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

Design and Deployment Guide

Published: December 2024

In partnership with:

COHESITY

About the Cisco Validated Design Program

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

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 HCI 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:

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.

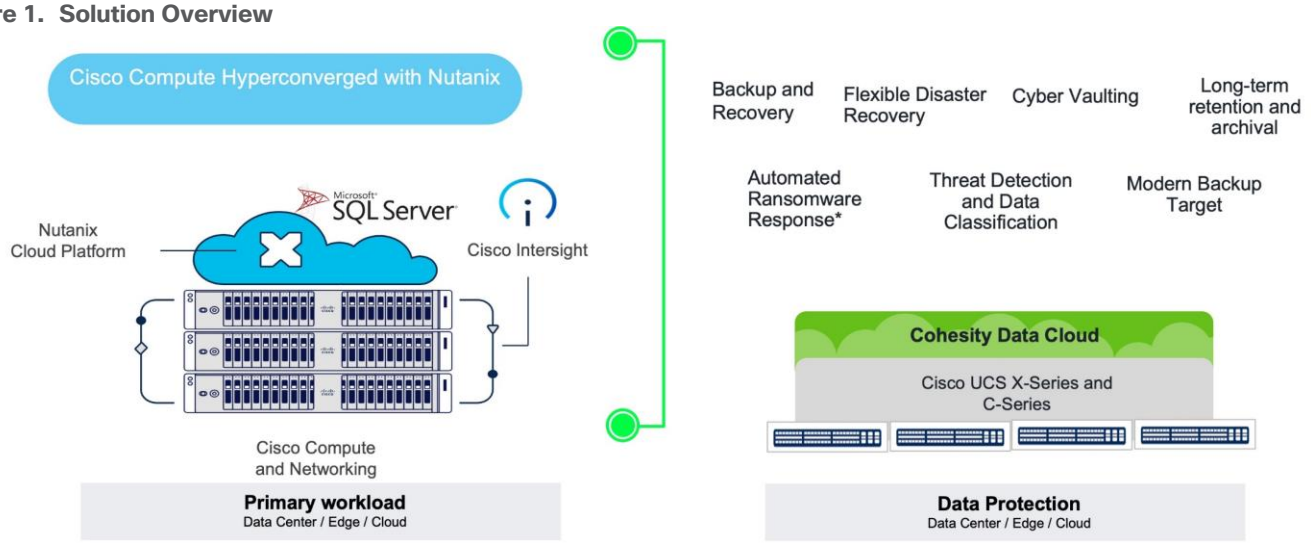
The key elements of this solution are as follows:

- 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



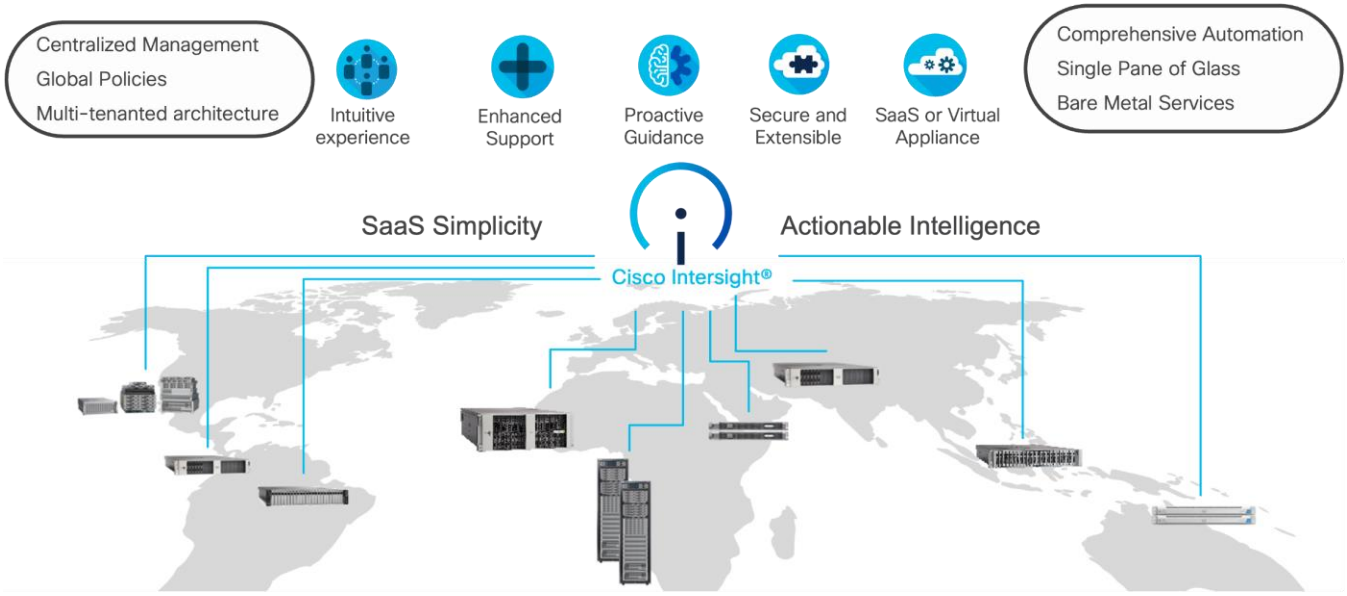
Technology Overview

This chapter contains the following:

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 cisco.com.

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.

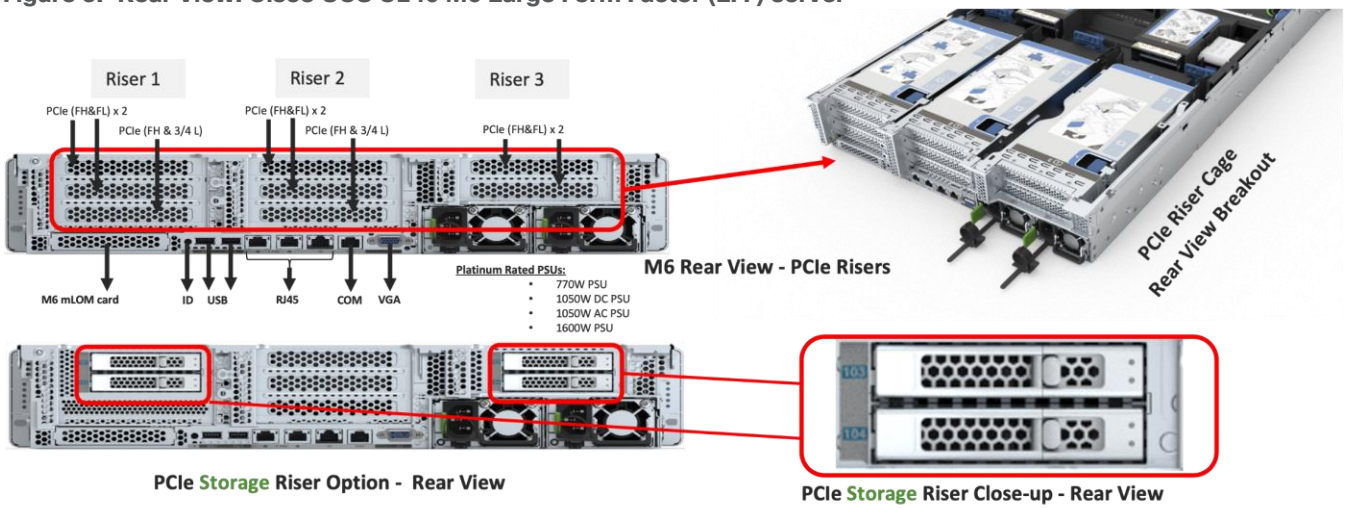
In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M6 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates 3rd Generation Intel Xeon Scalable processors, supporting up to 40 cores per socket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

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

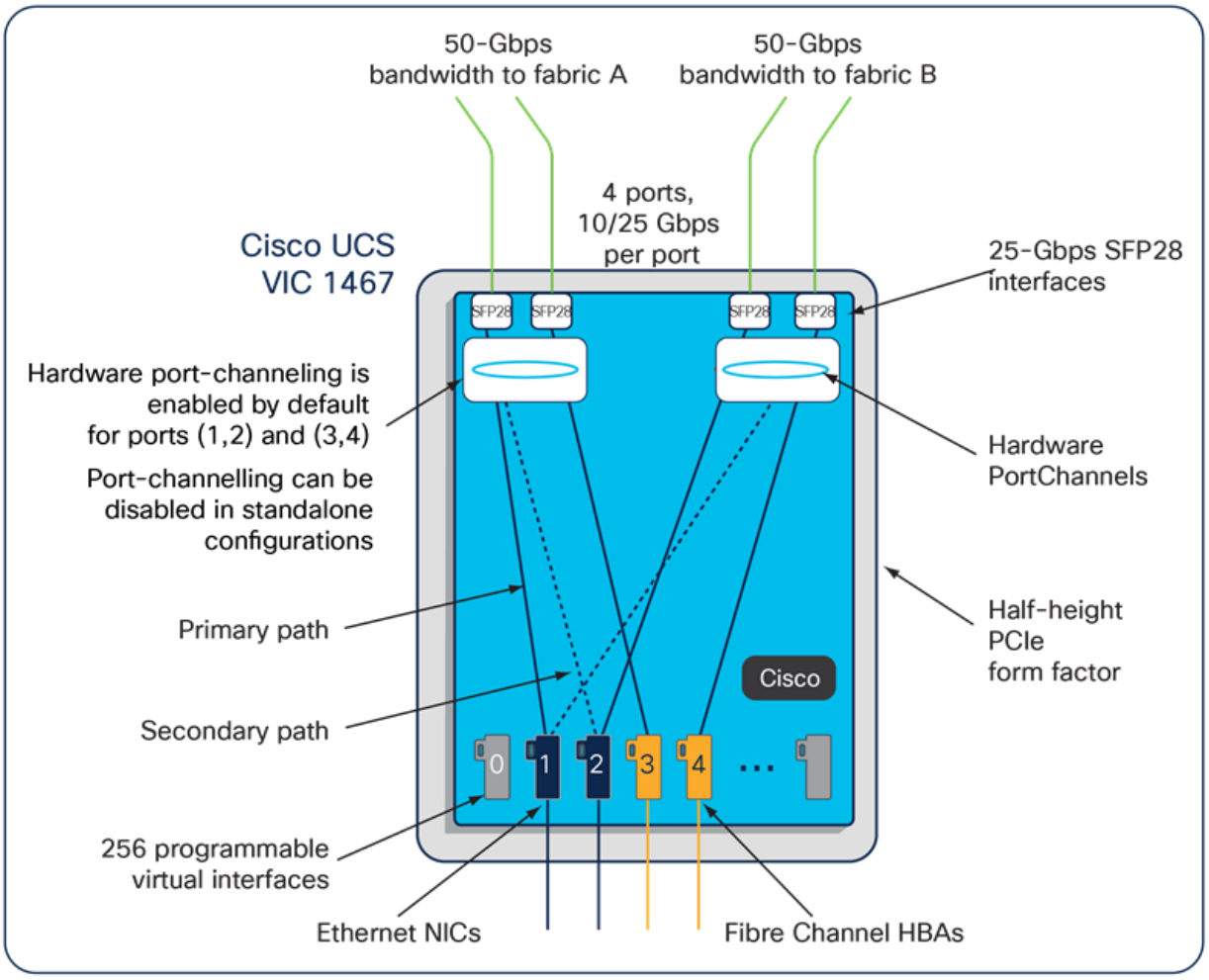
In the present configuration with the Cohesity Data Cloud, Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM with deployed on Cisco UCS C240 M6 LFF server.

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 PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBA. For more details visit, https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/unified-computing-system-adapters/datasheet-c78-741130.html

Figure 4. **Cisco UCS VIC 1467**

Figure 5. Cisco UCS VIC 1467 Infrastructure

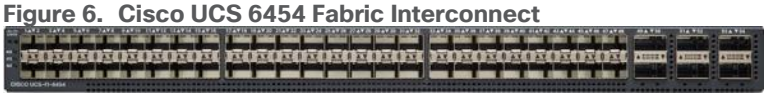


Cisco UCS 6400 Fabric Interconnects

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® Xeon® 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® Xeon® 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

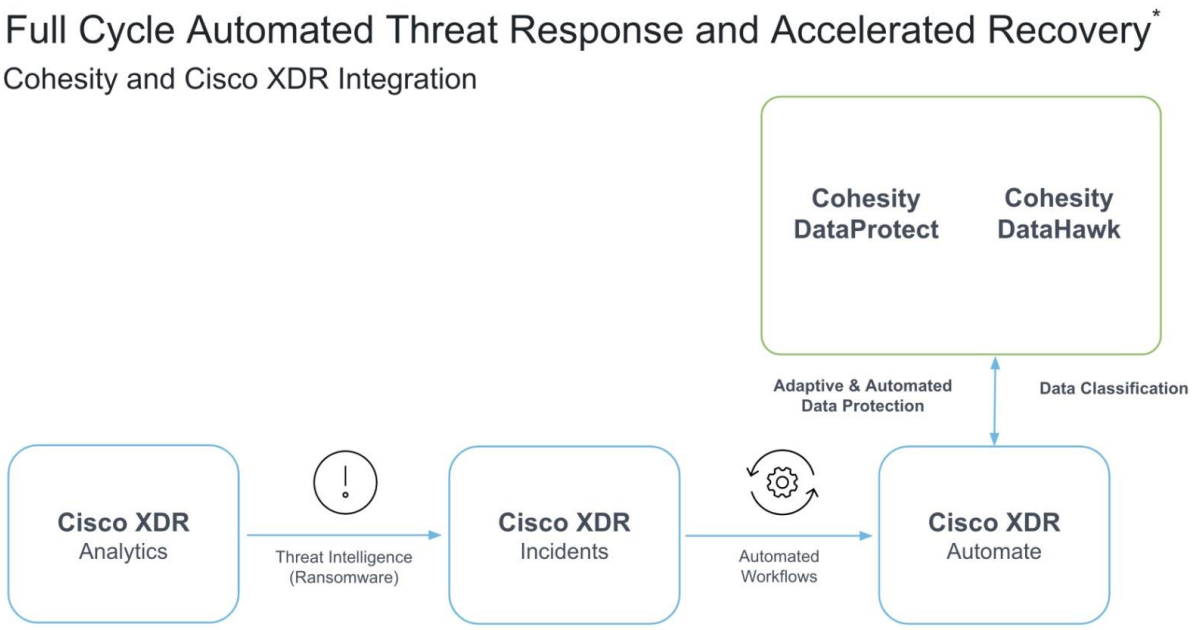
Figure 7. Front View: HCIAF240C M7 All-NVMe/All-Flash Servers

Cisco 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.

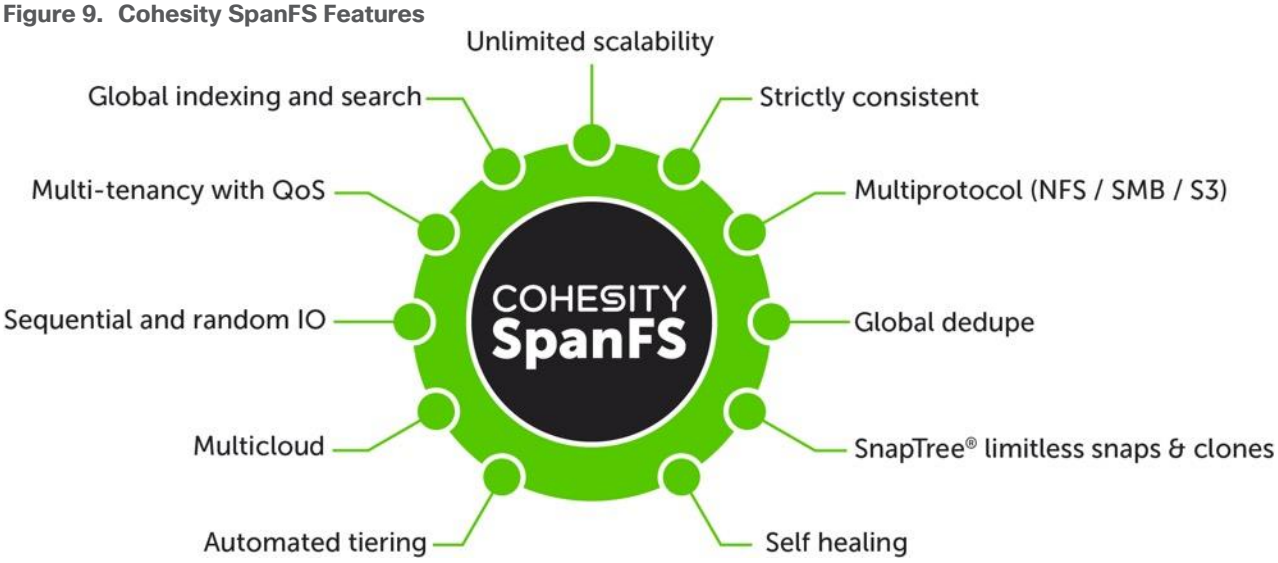
Helios is the user interface or control plane in which all customers interact with their data and Cohesity products. It provides a single view and global management of all your Cohesity clusters, whether on-premises, cloud, or Virtual Edition, regardless of cluster size. You can quickly connect clusters 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.

Figure 9. Cohesity SpanFS Features



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

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

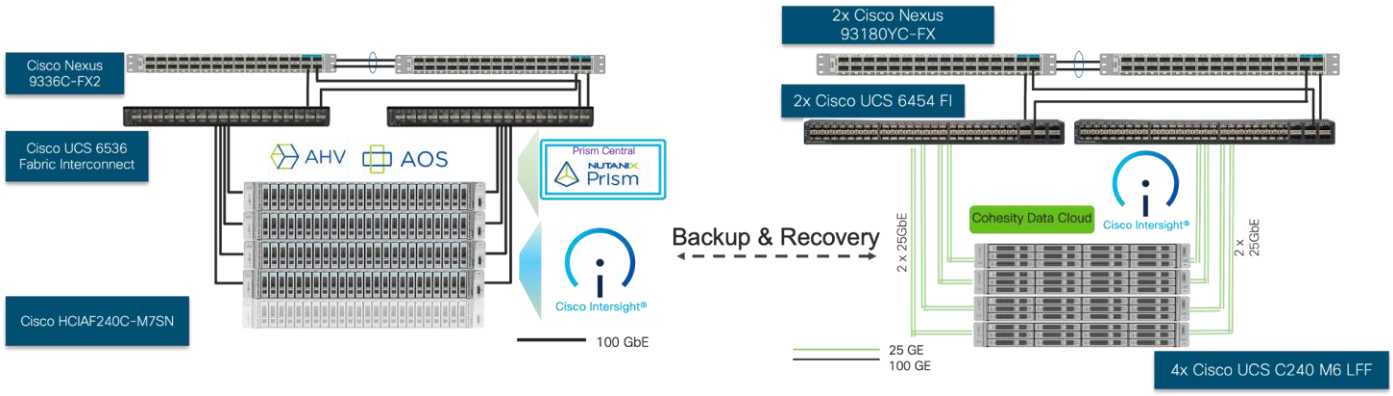
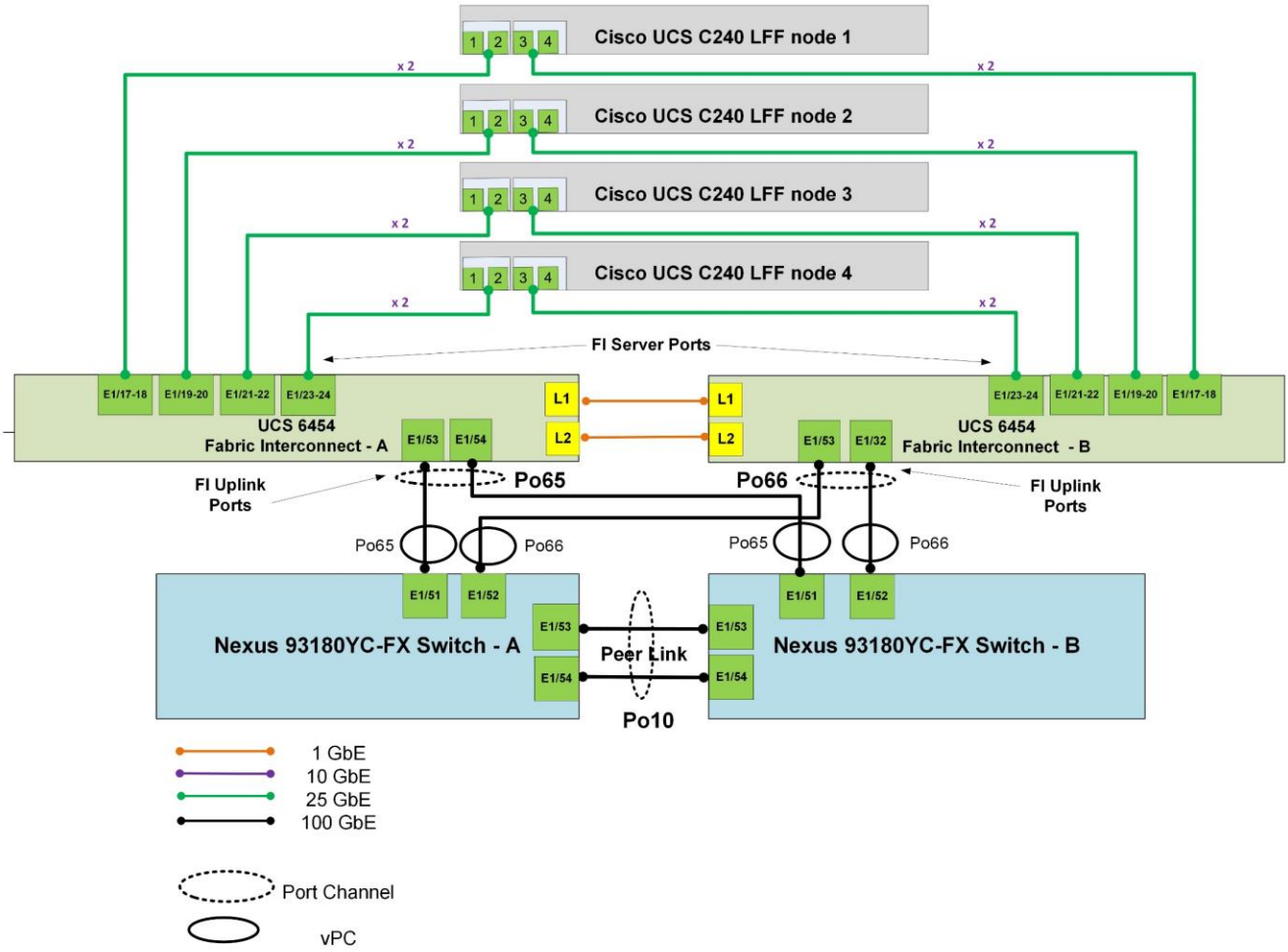


Figure 11 illustrates the cabling diagram for protection of SQL Server on CCHC with Nutanix through Cohesity on Cisco UCS C-Series servers.

Figure 11. Deployment Architecture Cabling



Note: Figure 11 does not showcase the CCHC with Nutanix cluster. Review the CVD for CCHC with Nutanix for SQL Server 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, SQL Server on Cisco Compute Hyperconverged with Nutanix

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 active-backup (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: 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

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: https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-infrastructure-service/licensing.html

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

Table 1 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.

Table 1. Software Components

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)
VirtIO Driver	1.2.3-x64

Solution Deployment

This chapter contains the following:

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 Device connector configuration 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: https://intersight.com/help/saas/resources/adding_OSimage). 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.

Table 2. Cohesity Cluster IP Addressing

Address Group:	UCS Management		Cohesity Cluster Nodes	
VLAN ID:			<<This should be native VLAN or tagged on the uplink 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				

Note: Table 3 is a true representation of configuration deployed during Solution Validation.

Table 3. Example Cohesity Cluster IP Addressing

Address Group:	UCS Management		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	<<blank>>
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	0.0.0.0

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 4. DNS Server Information

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

Item	Value	A Records
UCS Domain Name		
Cohesity Cluster Name		

Table 5. DNS Server Example Information

Item	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.

Table 8. VLAN Information

Name	ID
<<IN-Band VLAN>>	
<<cohesity_vlan>>	

Table 9. VLAN Example Information

Name	ID
<<IN-Band VLAN>>	1080
<<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
A		☐ Yes ☐ No	☐ LACP ☐ vPC		
		☐ Yes ☐ No			
		☐ Yes ☐ No			
		☐ Yes ☐ No			
B		☐ Yes ☐ No	☐ LACP ☐ vPC		
		☐ Yes ☐ No			
		☐ Yes ☐ No			
		☐ Yes ☐ No			

Table 11. Network Uplink Example Configuration

Fabric Interconnect Port		Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
A	1/53	☒ Yes ☐ No	☐ LACP ☒ vPC	61	Vpc61
	1/54	☒ Yes ☐ No			
		☐ Yes ☐ No			
		☐ Yes ☐ No			
B	1/53	☒ Yes ☐ No	☐ LACP ☒ vPC	62	Vpc62
	1/54	☒ Yes ☐ No			
		☐ Yes ☐ No			
		☐ Yes ☐ No			

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>>

Create Cisco Intersight Account

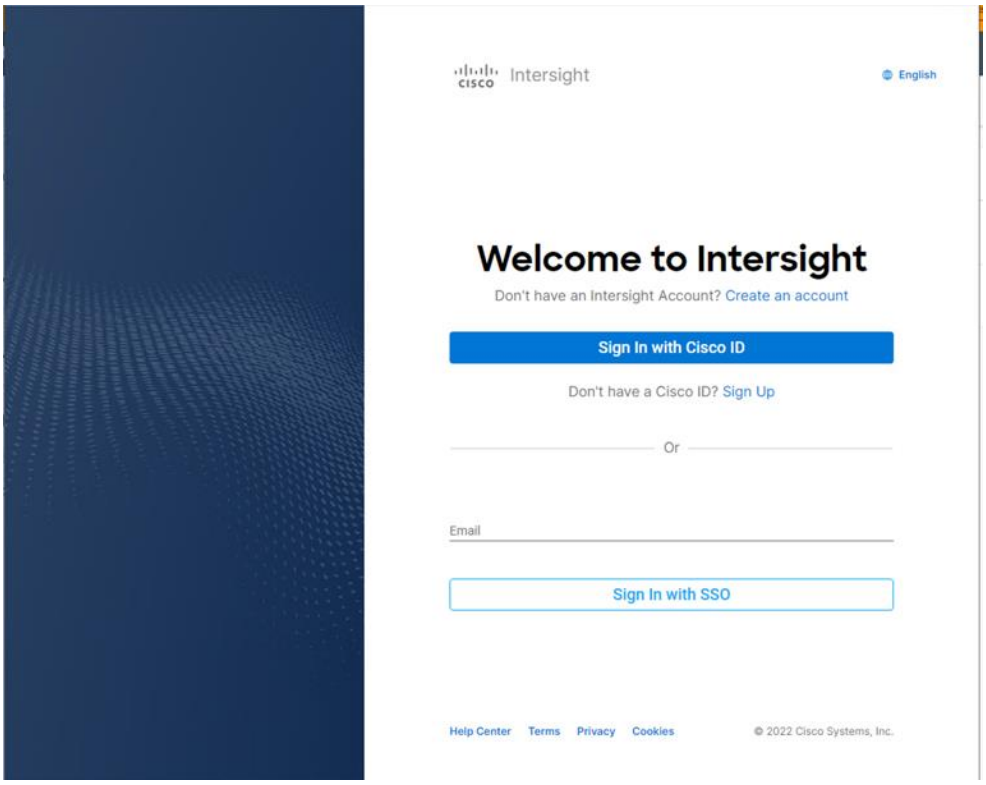
Procedure 1. Create an account on Cisco Intersight

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: https://intersight.com/help/saas/getting_started/create_cisco_intersight_account

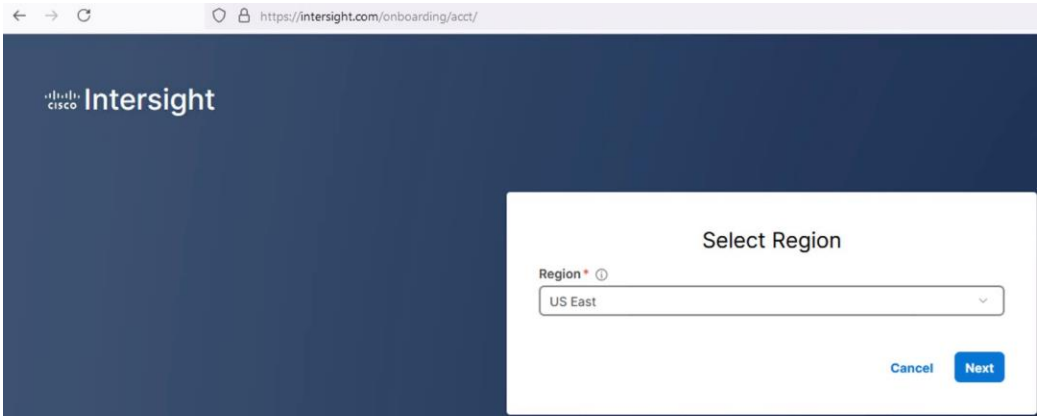
Step 1. Go to https://intersight.com/ to create your Intersight account. You must have a valid Cisco ID to create a Cisco Intersight account.

Step 2. Click Create an account.

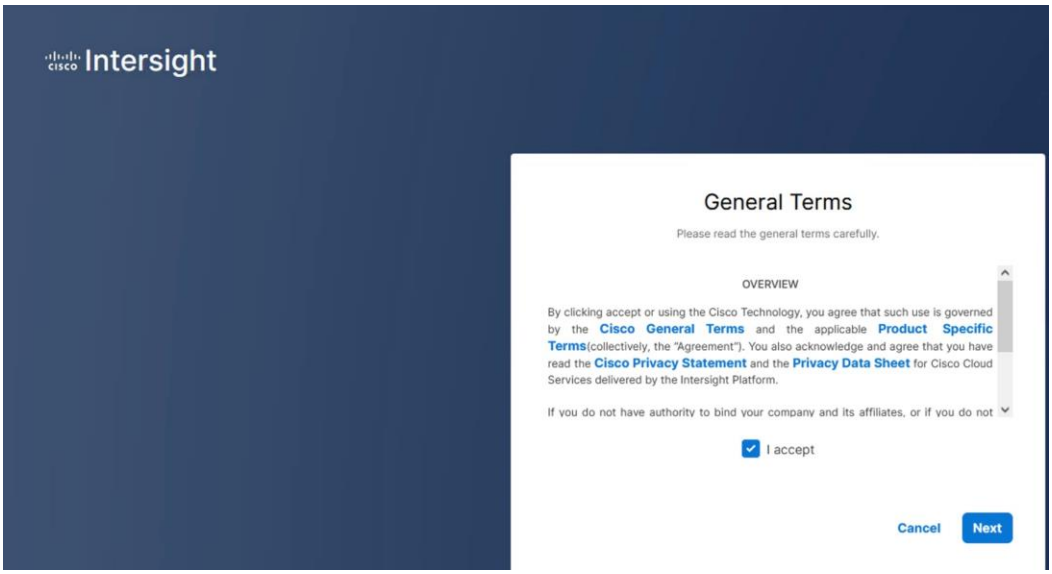


Step 3. Sign-In with your Cisco ID.

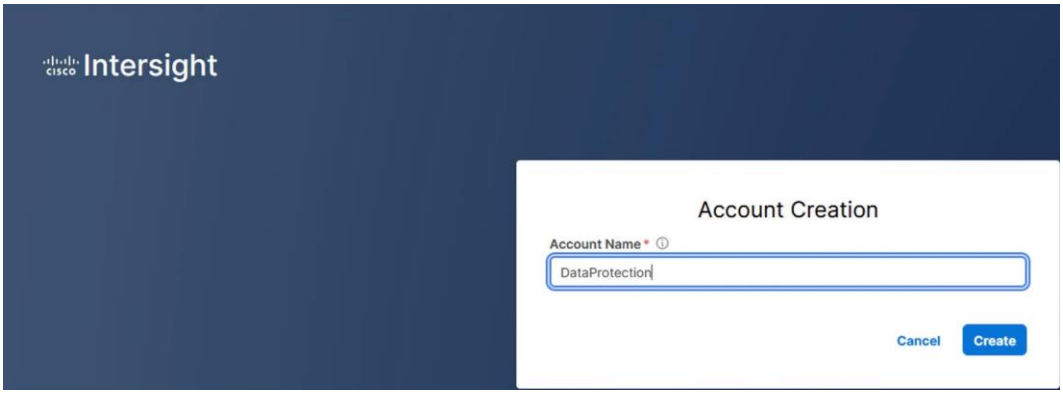
Step 4. Select Region



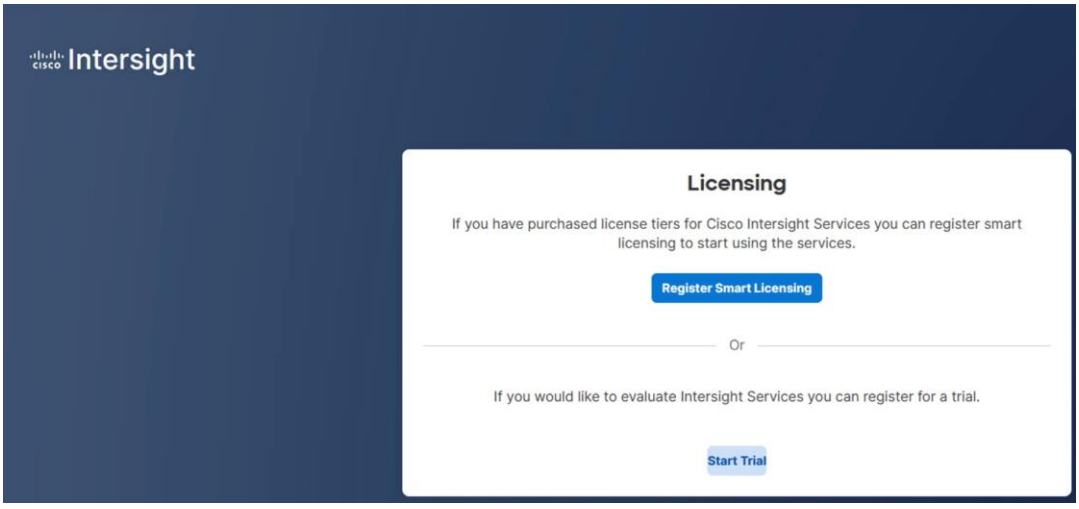
Step 5. Read the End User License Agreement and select I accept and click Next.



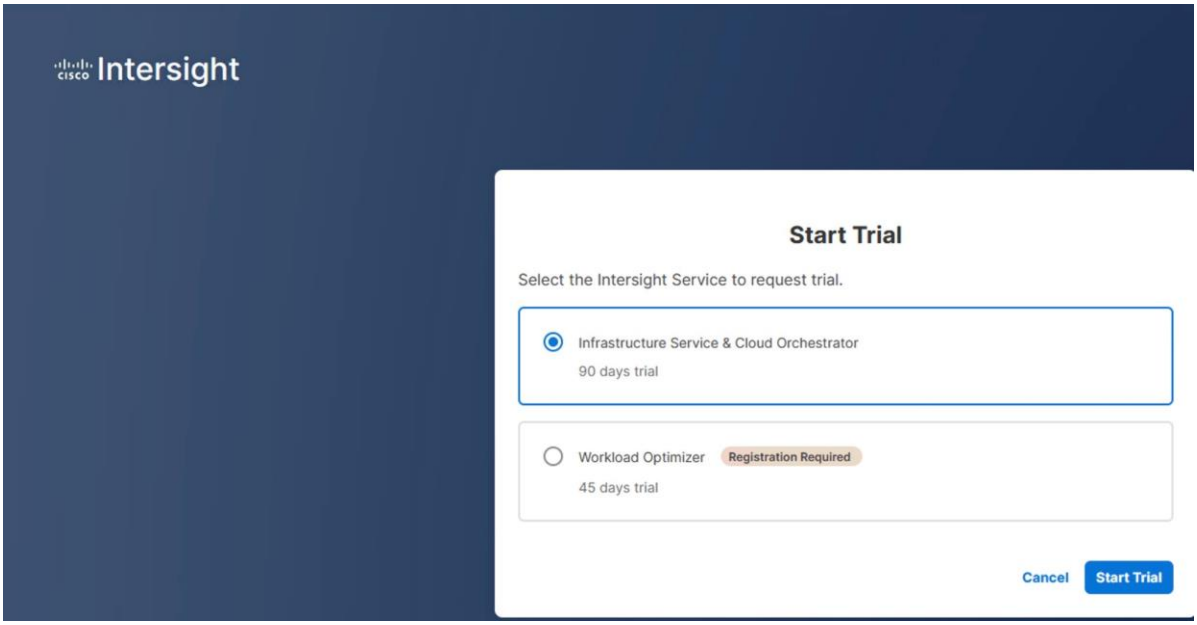
Step 6. Provide a name for the account and click Create.



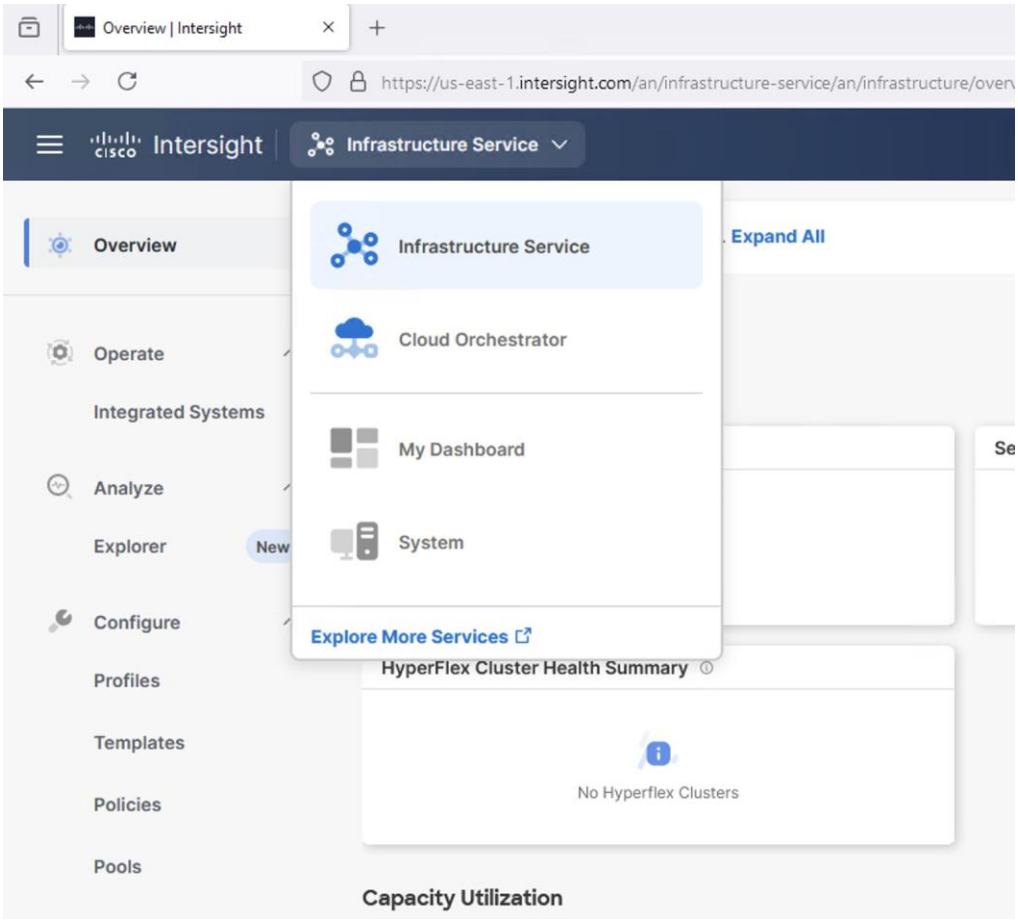
Step 7. Register for Smart Licensing or Start Trial.



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



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



Note: Go to: https://intersight.com/help/saas 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)? intersight

  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>

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

  Enter the system name:  <ucs-cluster-name>

  Physical Switch Mgmt0 IP address : <ucsa-mgmt-ip>

  Physical Switch Mgmt0 IPv4 netmask : <ucs-mgmt-mask>

  IPv4 address of the default gateway : <ucs-mgmt-gateway>

    DNS IP address : <dns-server-1-ip>

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

    Default domain name : <ad-dns-domain-name>

Following configurations will be applied:

    Management Mode=intersight
    Switch Fabric=A
    System Name=<ucs-cluster-name>
    Enforced Strong Password=yes
    Physical Switch Mgmt0 IP Address=<ucsa-mgmt-ip>
    Physical Switch Mgmt0 IP Netmask=<ucs-mgmt-mask>
    Default Gateway=<ucs-mgmt-gateway>
    DNS Server=<dns-server-1-ip>
    Domain Name=<ad-dns-domain-name>

  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

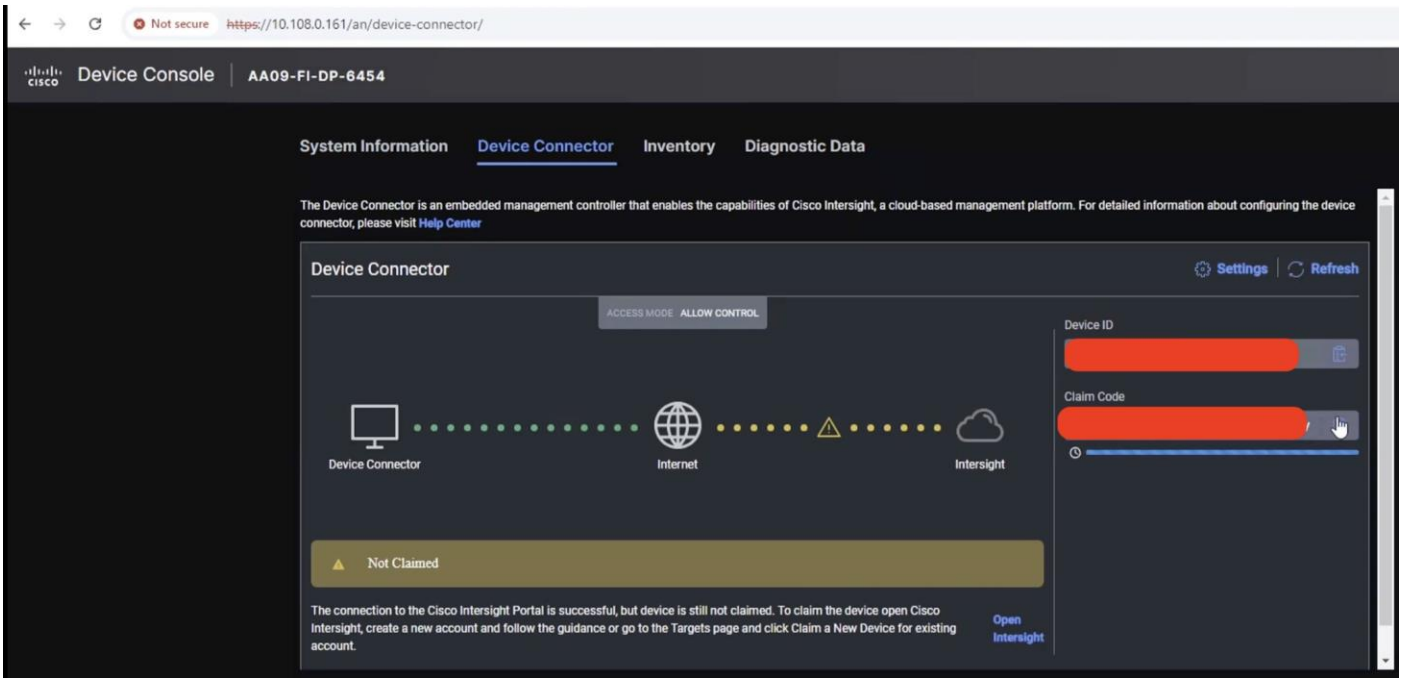
Note: In the present solution, “default” organization is used for all configurations. “Default” organization is automatically created once an Intersight account is created.

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.

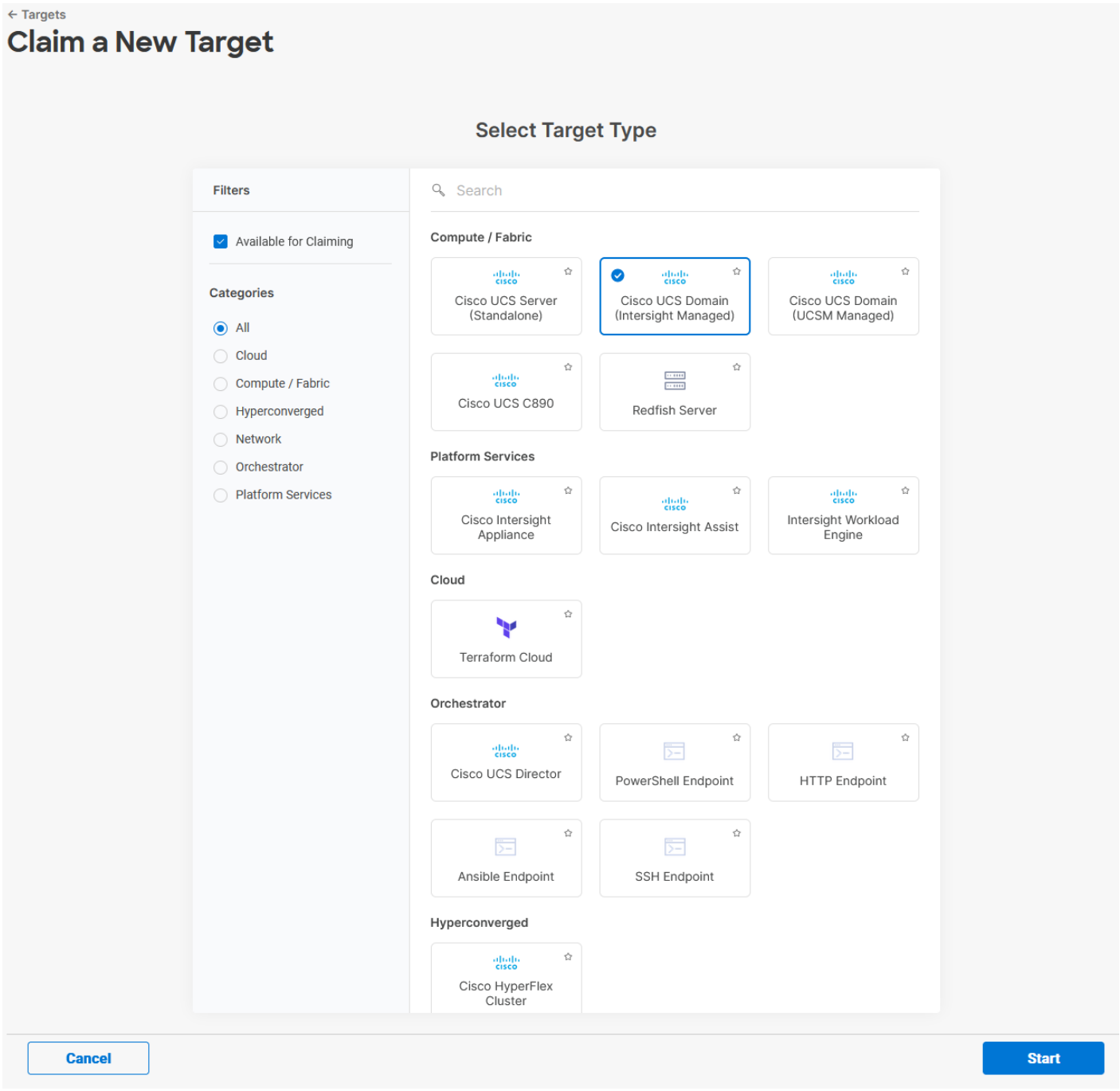


Step 3. Log into Cisco Intersight.

Step 4. Select System. Click Administration > Targets.

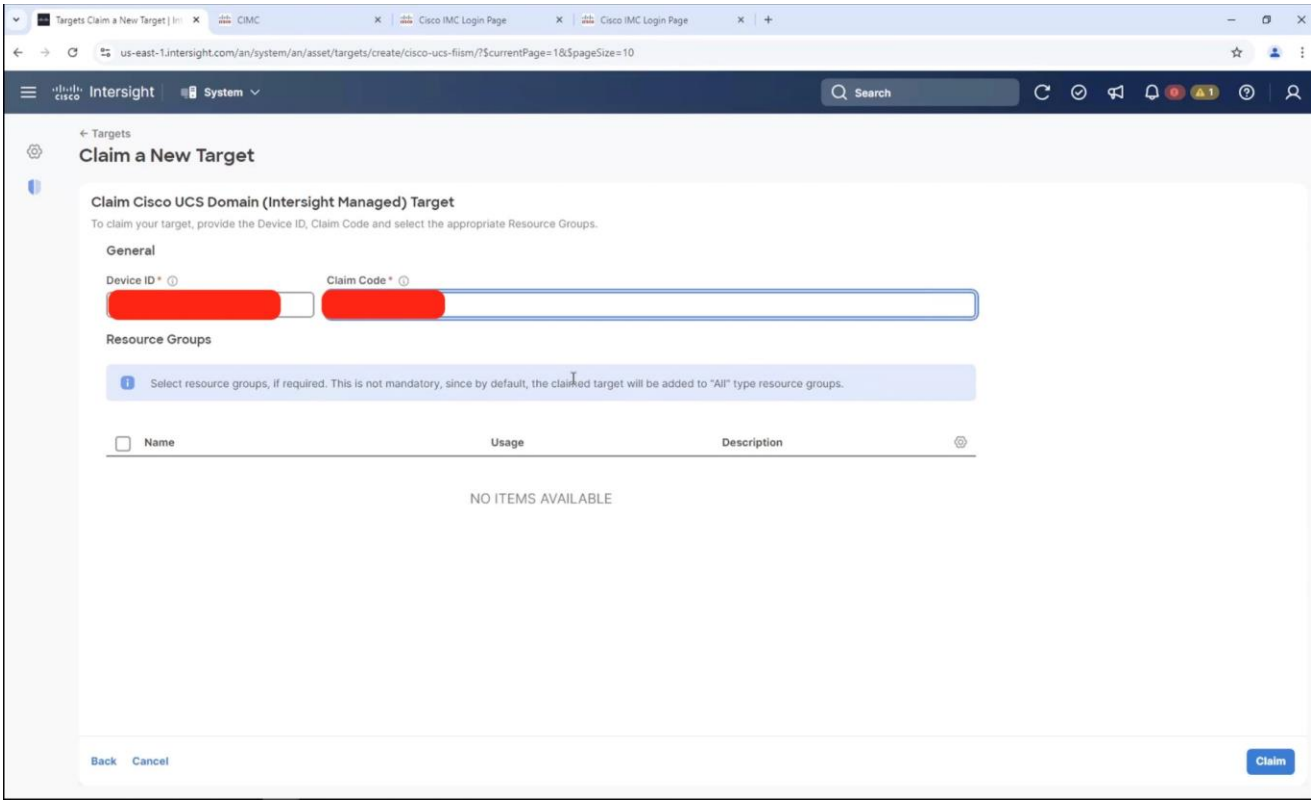
Step 5. Click Claim a New Target.

Step 6. Select Cisco UCS Domain (Intersight Managed) and click Start.

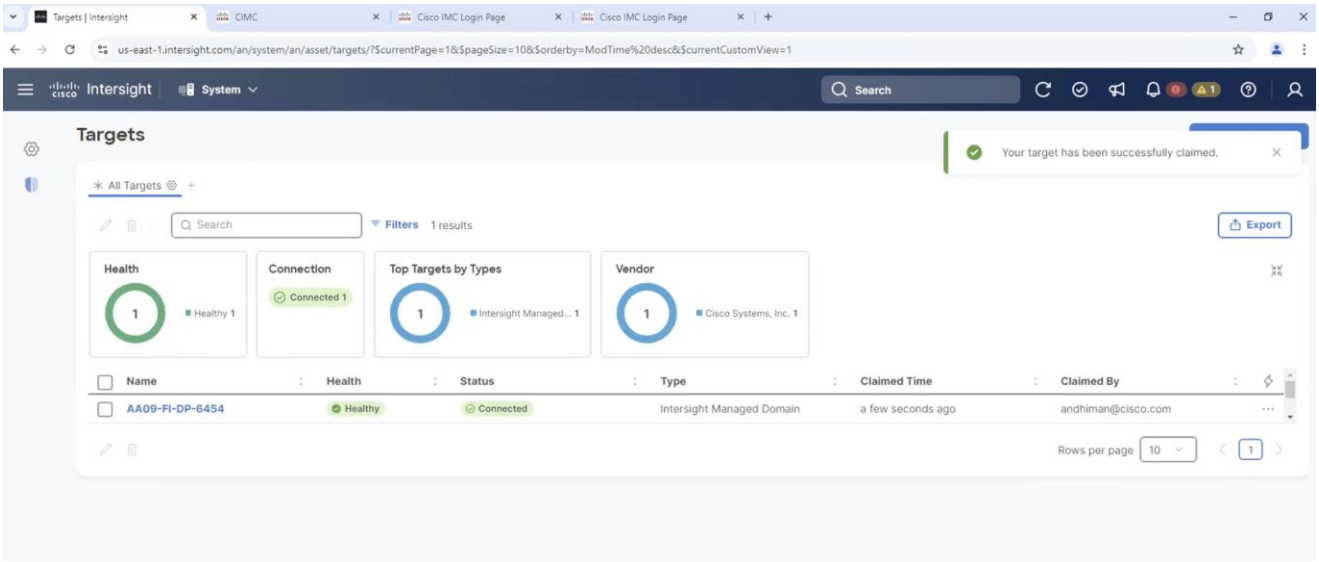


Step 7. Copy and paste the Device ID and Claim from the Cisco UCS FI to Intersight.

Step 8. Select the previously created Resource Group and click Claim.



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

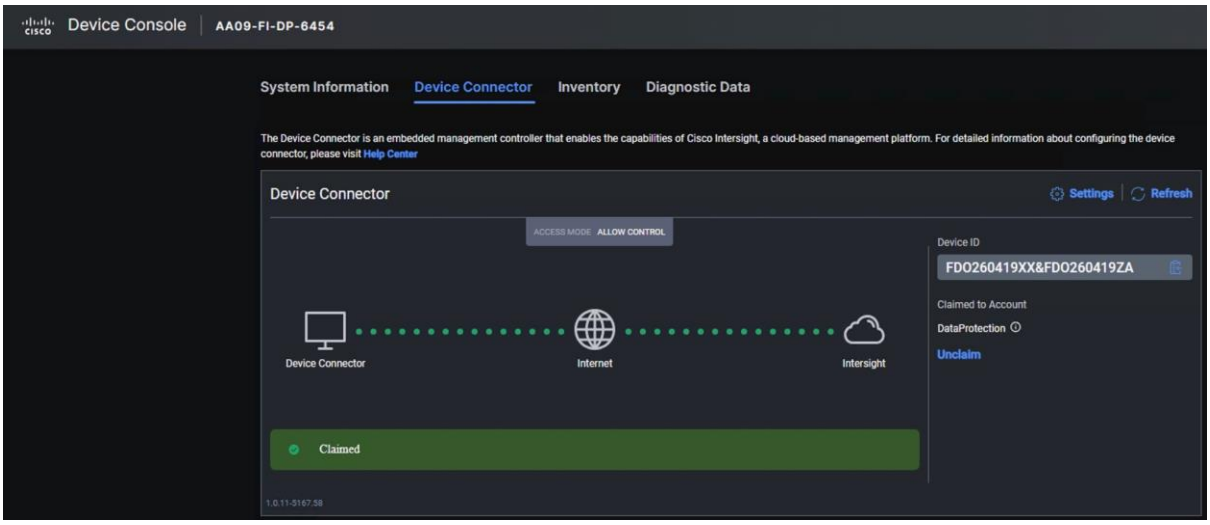


Step 10. In the Cisco Intersight window, click Settings and select Licensing. If this is a new account, all servers connected to the Cisco UCS domain will appear under the Base license tier. If you have purchased Cisco Intersight licenses and have them in your Cisco Smart Account, click Register and 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)

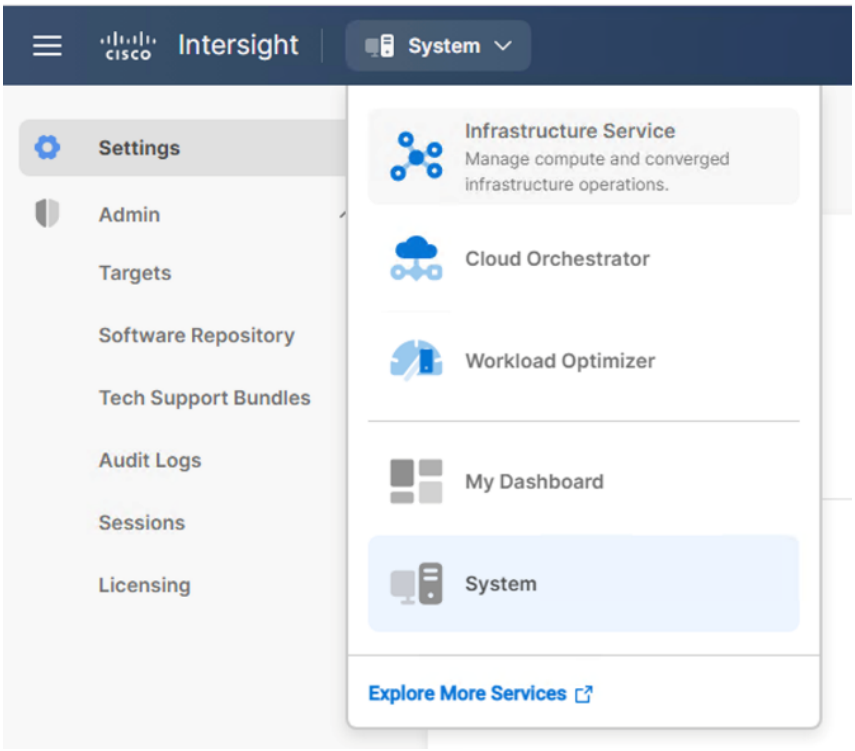
Procedure 4. Verify Addition of Cisco UCS Fabric Interconnects to Cisco Intersight

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

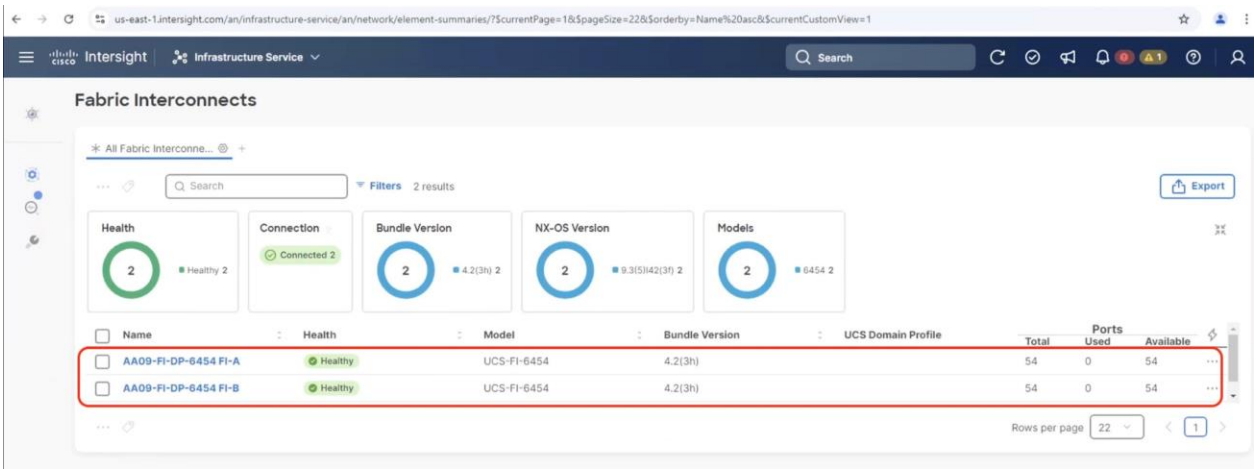
The fabric interconnect status should now be set to **Claimed**.



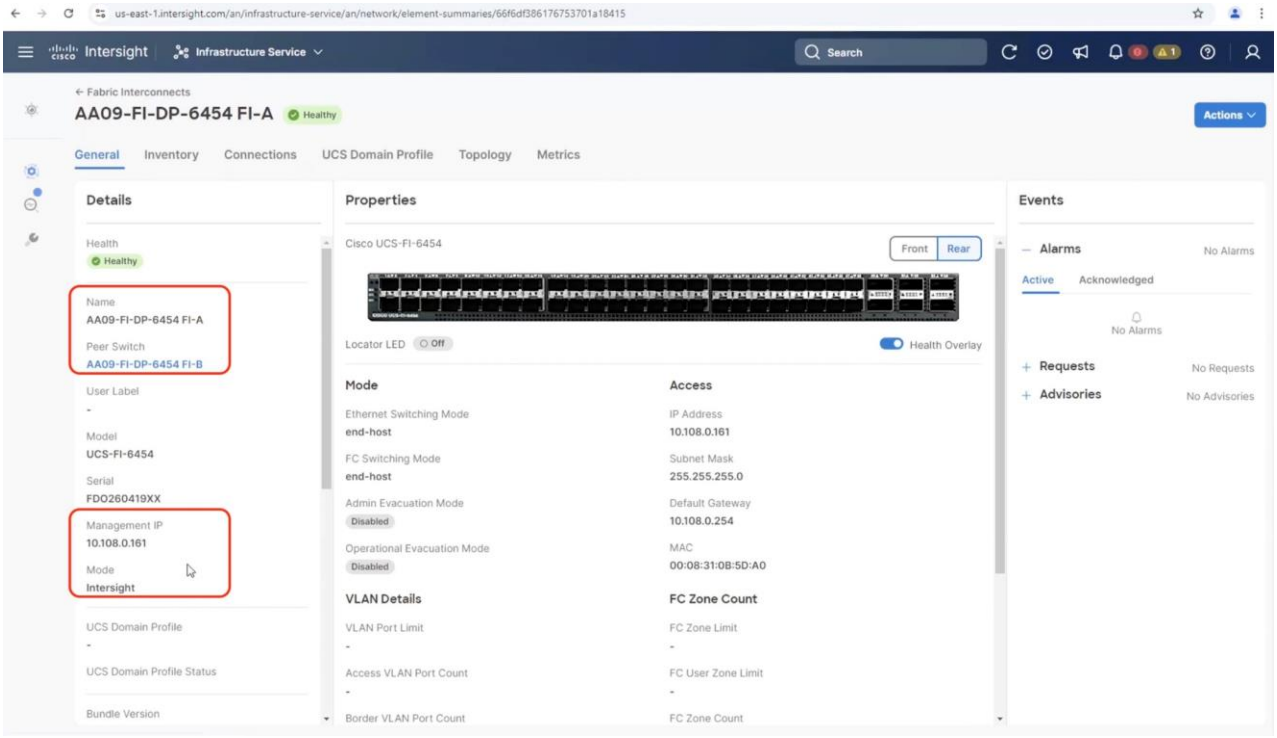
Step 2. Select Infrastructure Service.



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



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:



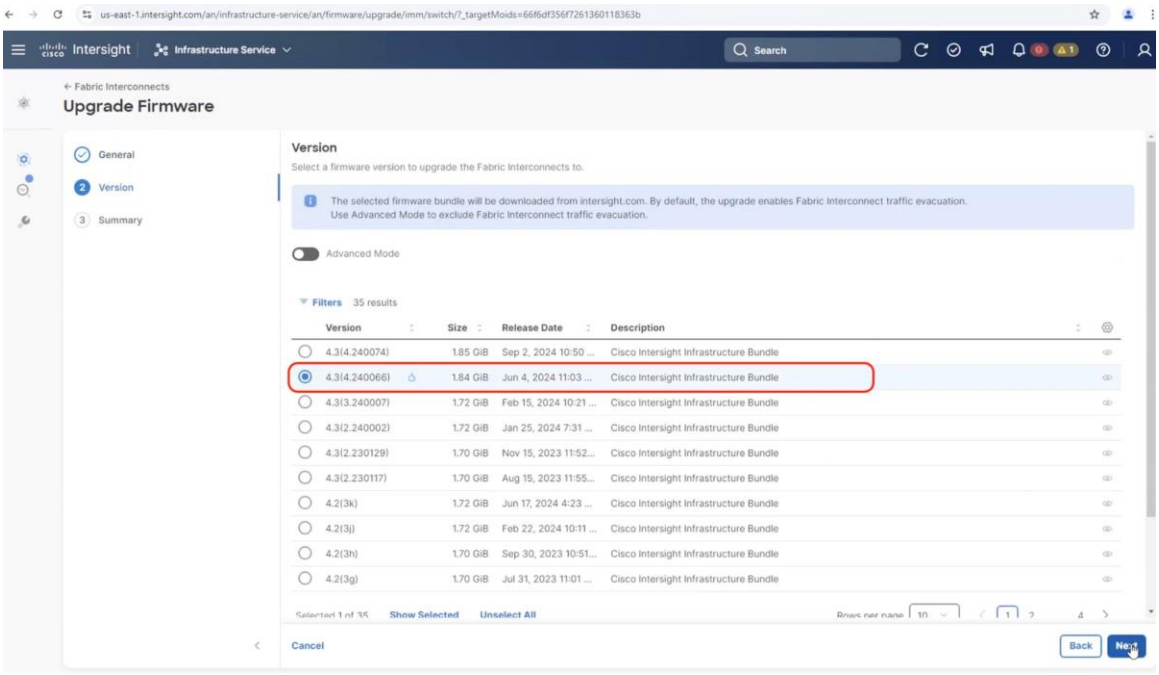
Procedure 5. Upgrade Fabric Interconnect Firmware using Cisco Intersight

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.

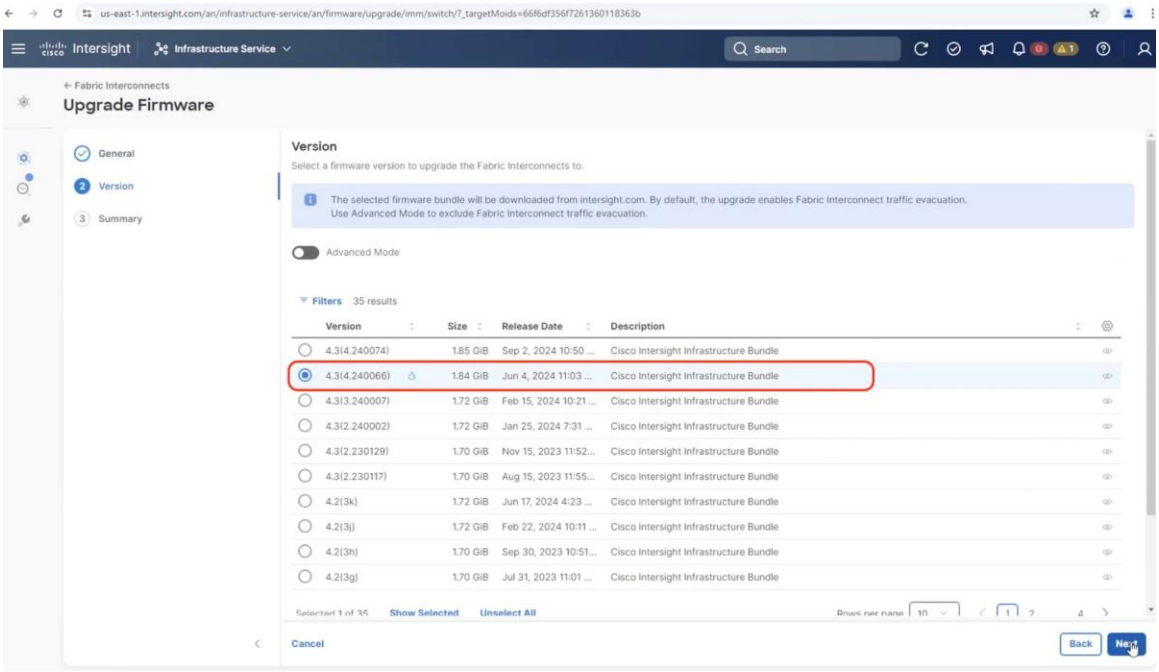
Step 3. Click the ellipses "..."for either of the Fabric Interconnects and select Upgrade Firmware.



Step 4. Click Start.

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

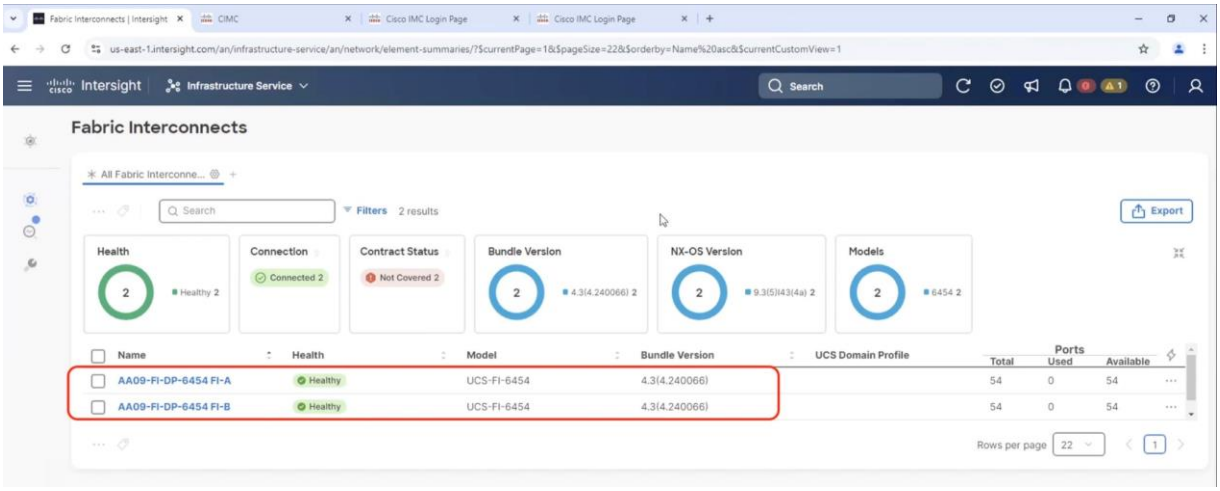
Step 6. Select 4.3(4.240066)) release (or the latest release which has the 'Recommended' icon) from the list and click Next.



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.



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-computing-system/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.

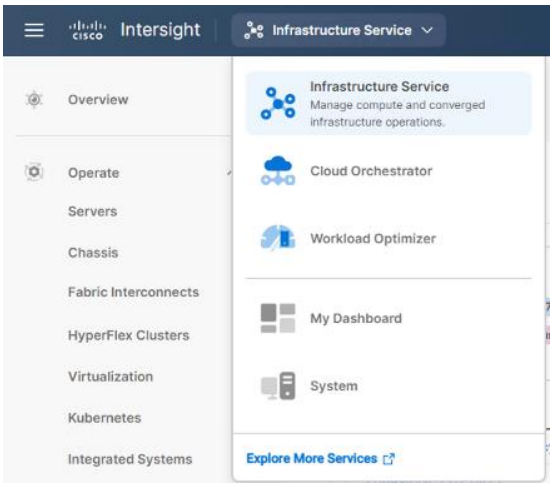
Table 13. Policies required for a Cisco UCS Domain Profile

Policy	Description
VLAN 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
Network Time Protocol (NTP) policy	

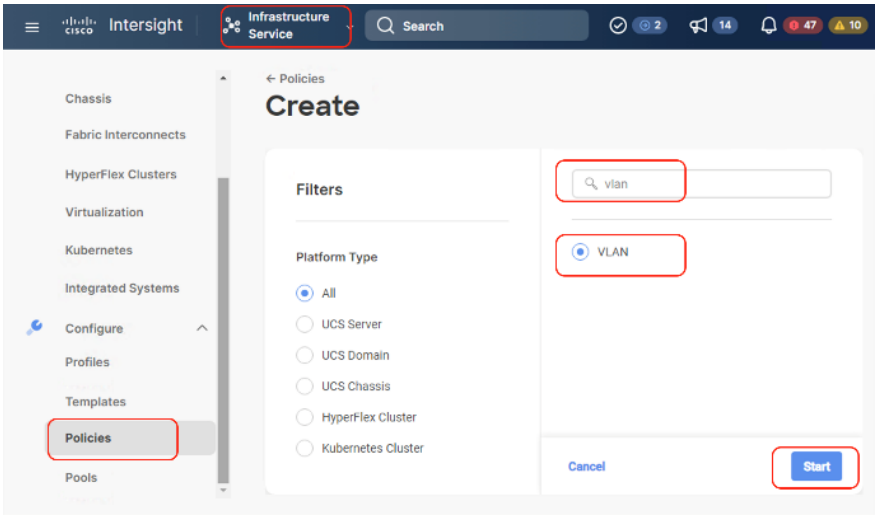
Policy	Description
Syslog policy	
System QoS	

Procedure 1. Create VLAN configuration Policy

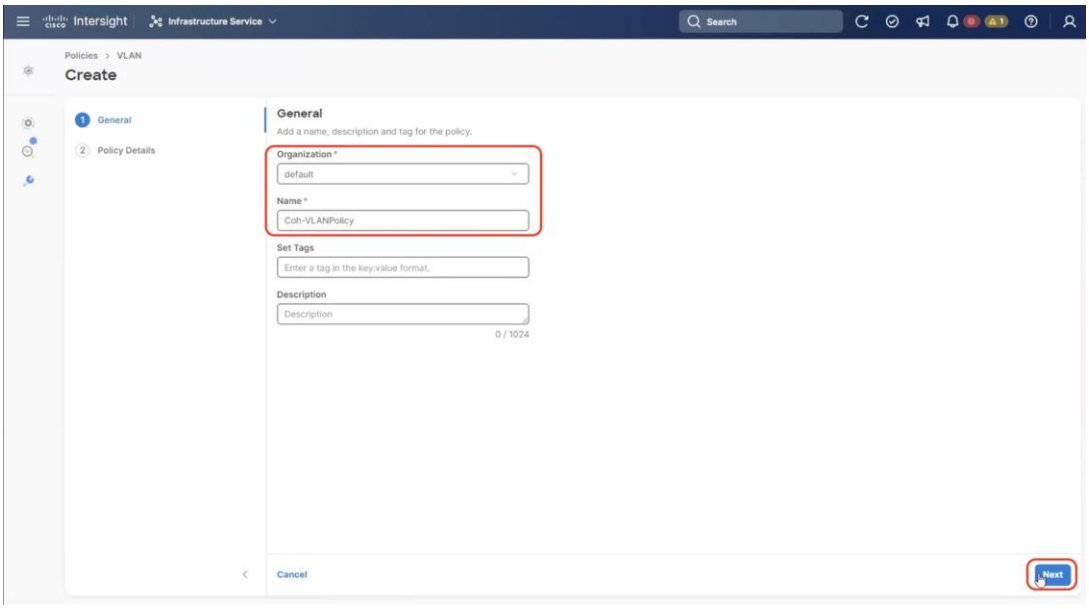
Step 1. Select Infrastructure Services.



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

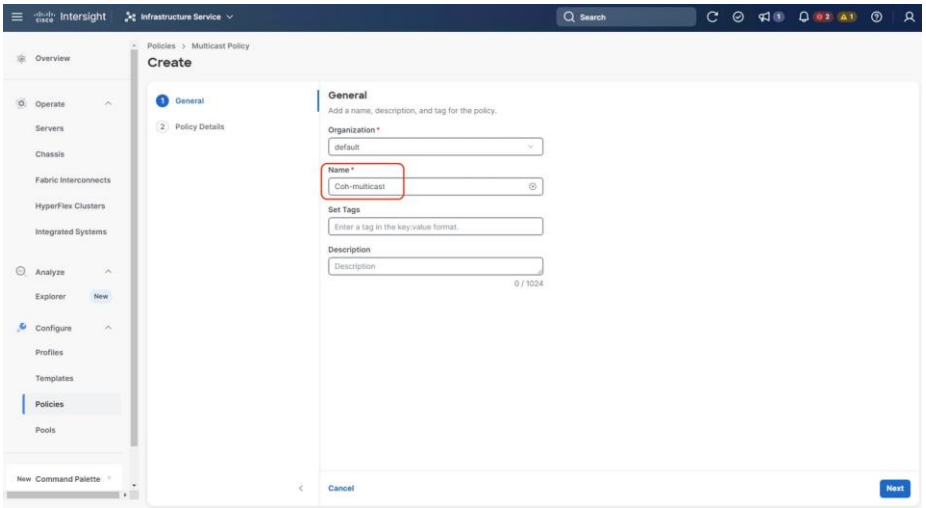


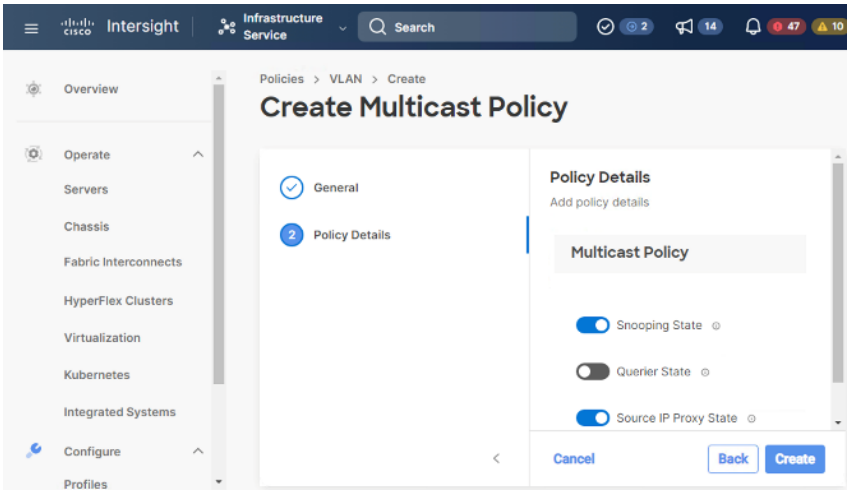
Step 3. Provide a name for the VLAN (for example, Coh-VLANPolicy) and click Next.



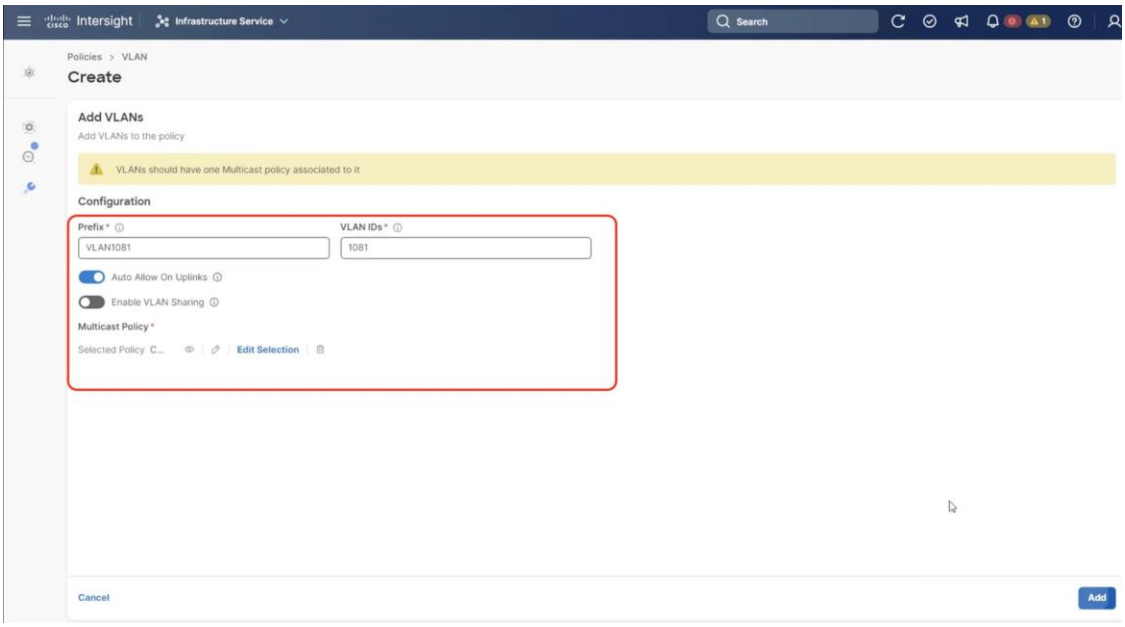
Step 4. Click Add VLANs to add your required VLANs.

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

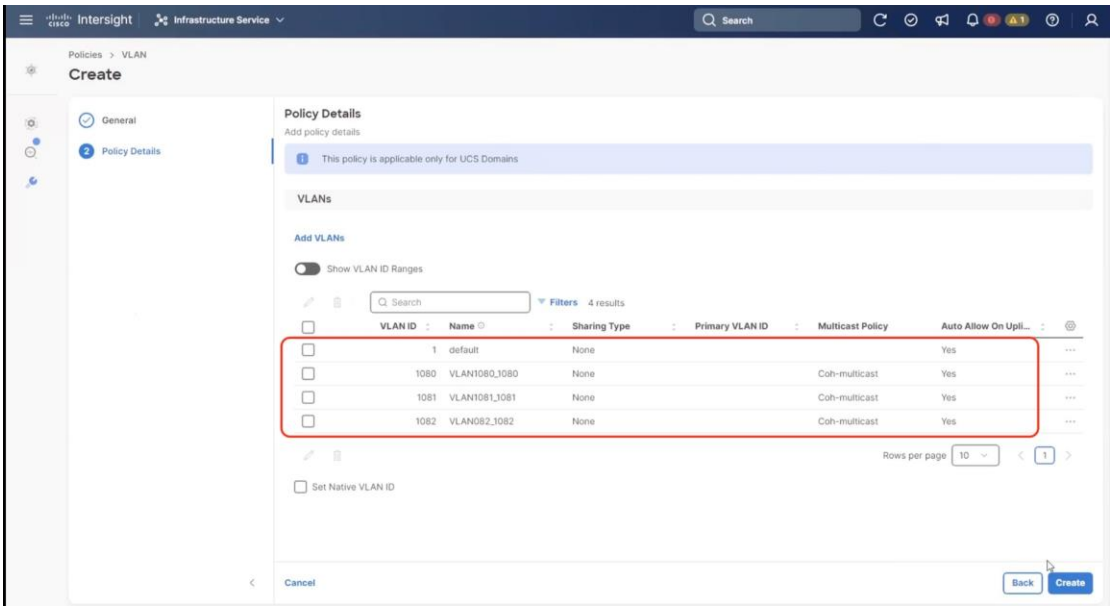




Step 6. Add VLAN as required in the network setup with default options and multicast policy, click Create.



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



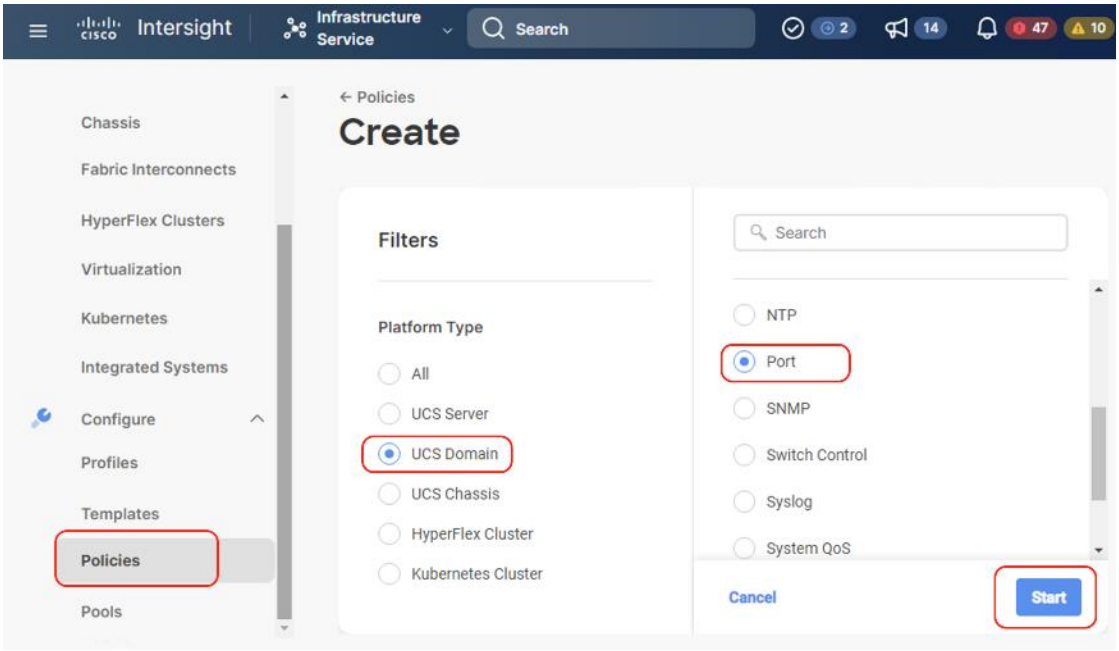
Note: If you will be using the same VLANs on fabric interconnect A and fabric interconnect B, you can use the same policy for both.

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.

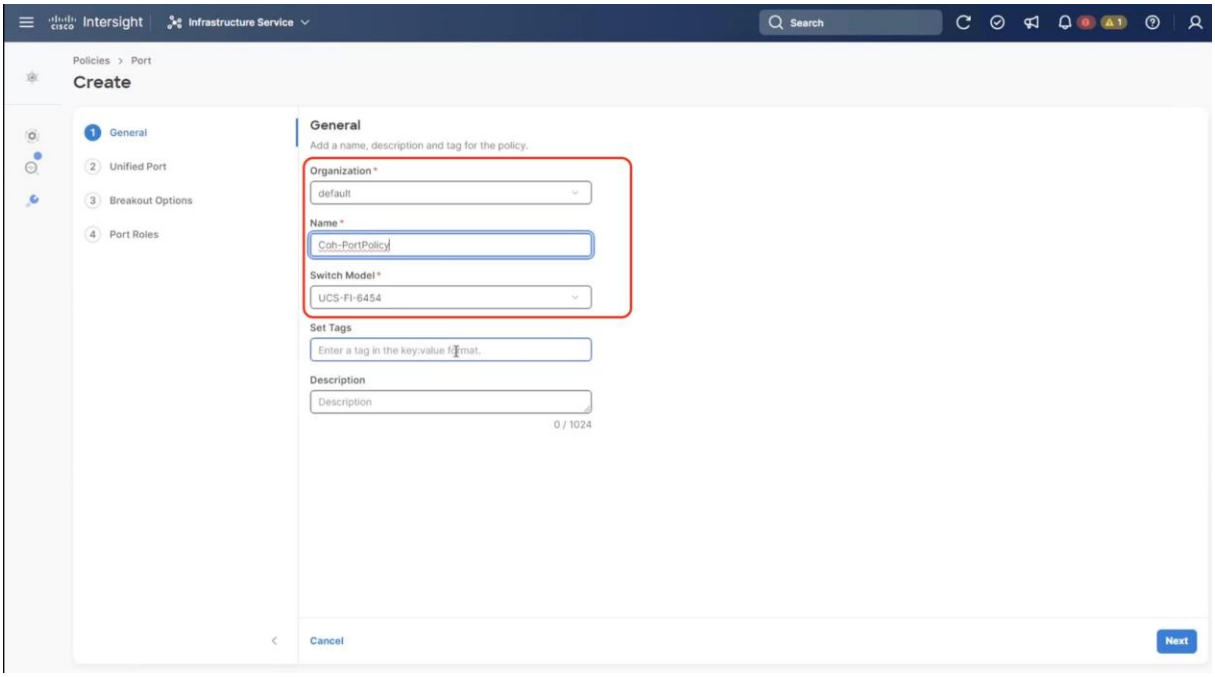
Procedure 2. Create Port Configuration Policy

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.

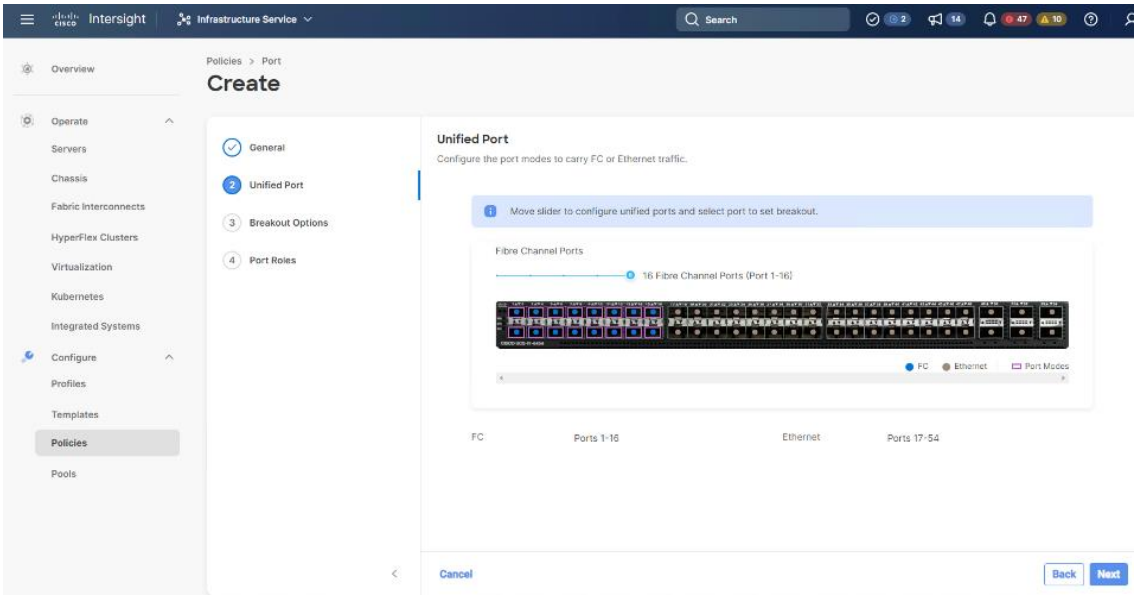


Step 3. Click Next. Define the port roles; server ports for chassis and server connections, Fibre Channel ports for SAN connections, or network uplink ports.

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.

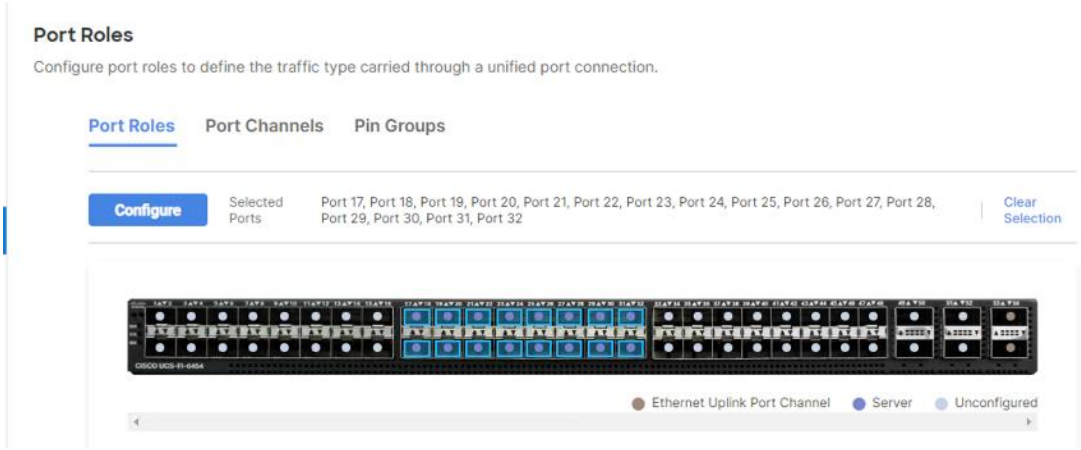
Note: Selection of FC ports should be confirmed with your administrators. In event customers are not looking to have FC connectivity , they can you Server Ports starting from Port 1



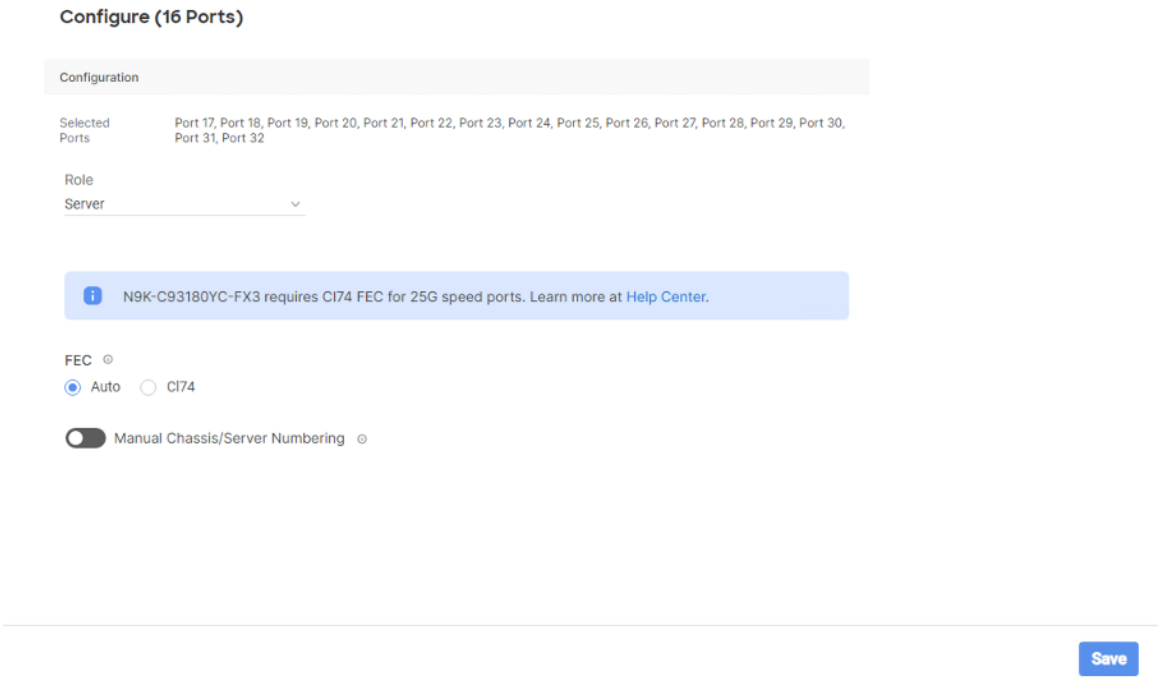
Step 6. Click Next.

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

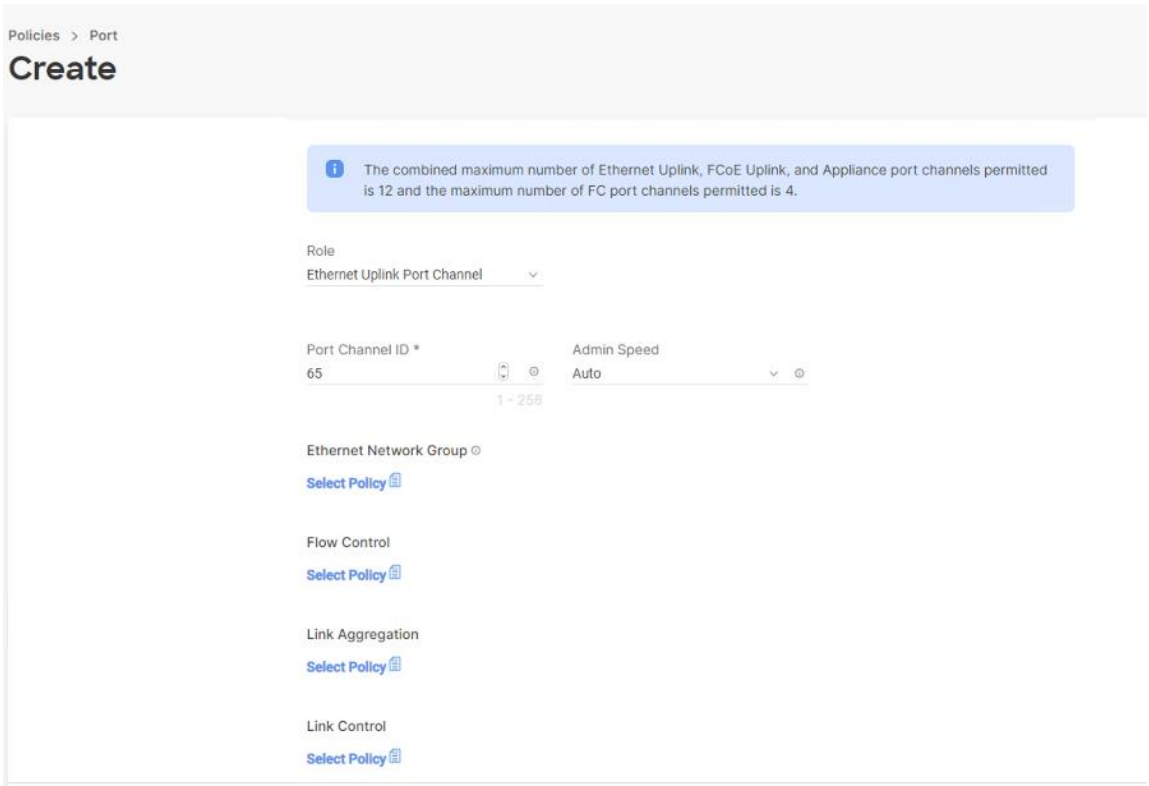
Step 8. To configure server ports, select the ports that have chassis or rack-mounted servers plugged into them and click Configure.

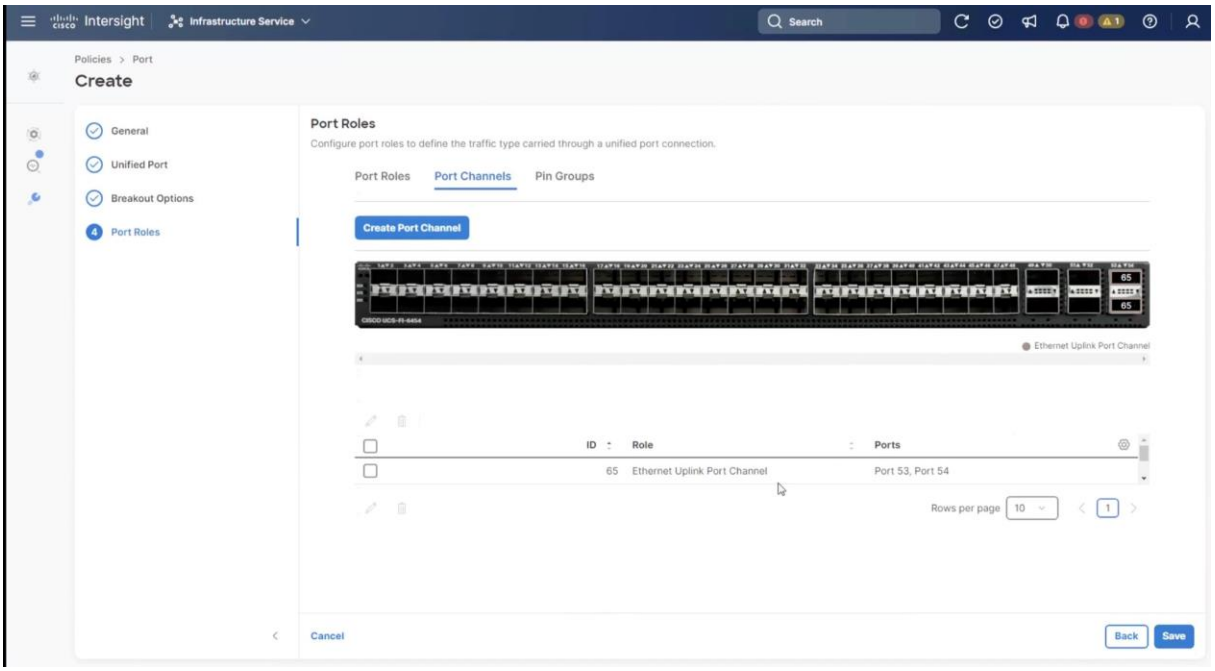


Step 9. From the drop-down list, select Server and click Save.

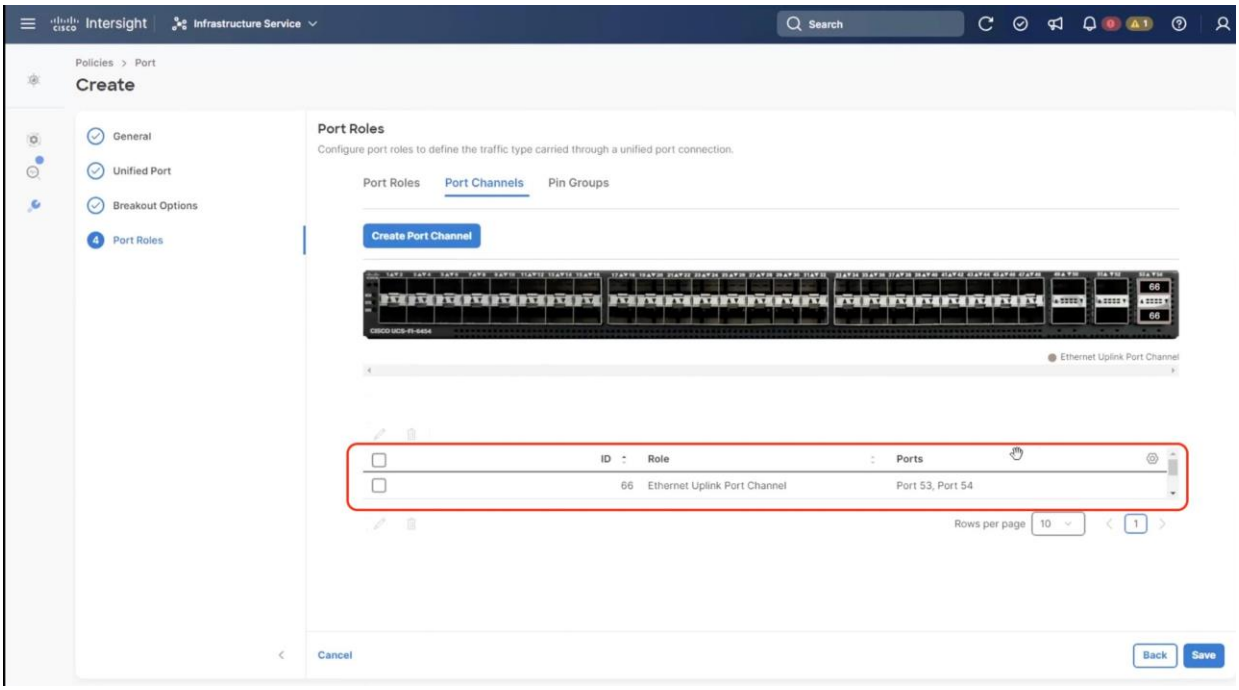


Step 10. Configure the uplink ports as per your deployment configuration. In this setup, port 53/54 are configured as uplink ports. Select the Port Channel tab and configure the port channel as per the network configuration. In this setup, port 53/54 are port channeled and provide uplink connectivity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



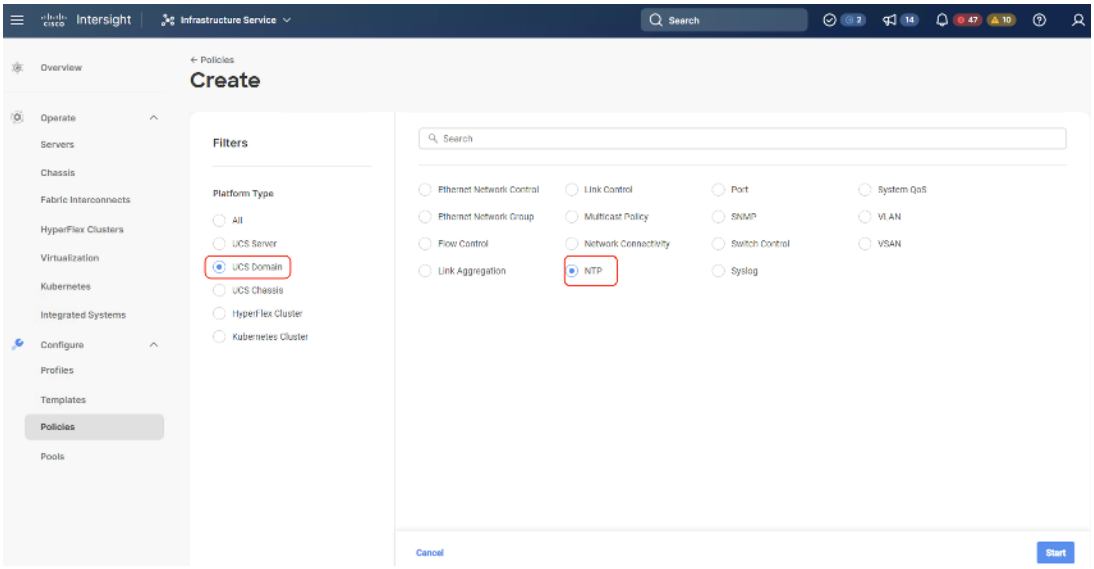


Step 11. Repeat this procedure to create a port policy for Fabric Interconnect B. Configure the port channel ID for Fabric B as per the network configuration. In this setup, the port channel ID 66 is created for Fabric Interconnect B, as shown below:



Procedure 3. Create NTP Policy

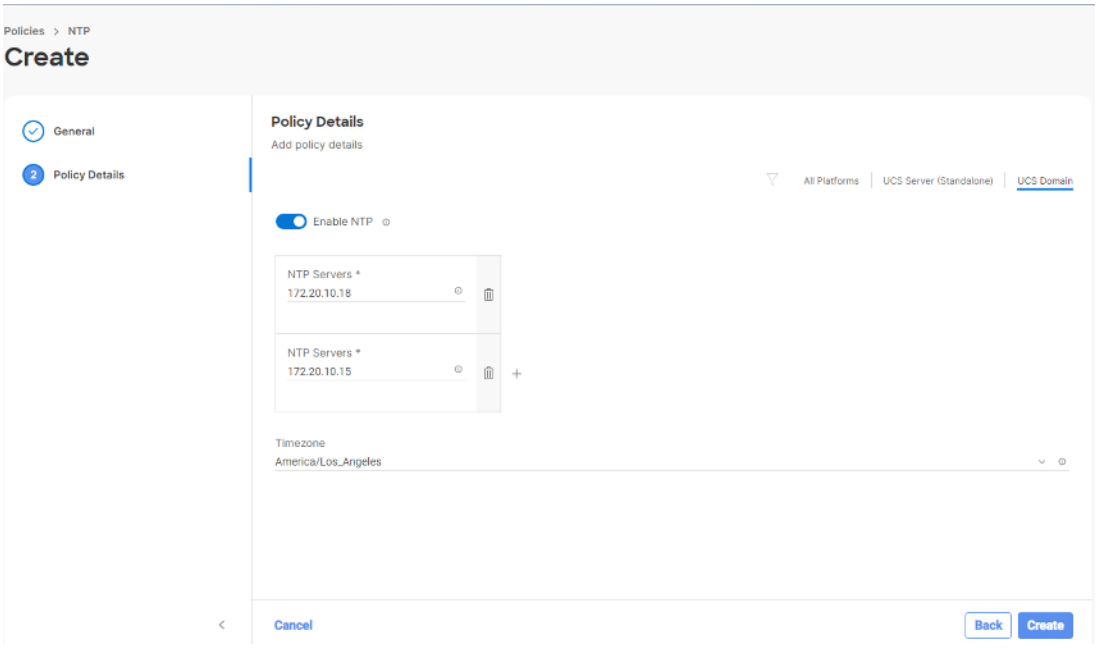
Step 1. Under Policies, select Create Policy, then select UCS Domain and then select NTP. Click Start.



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.

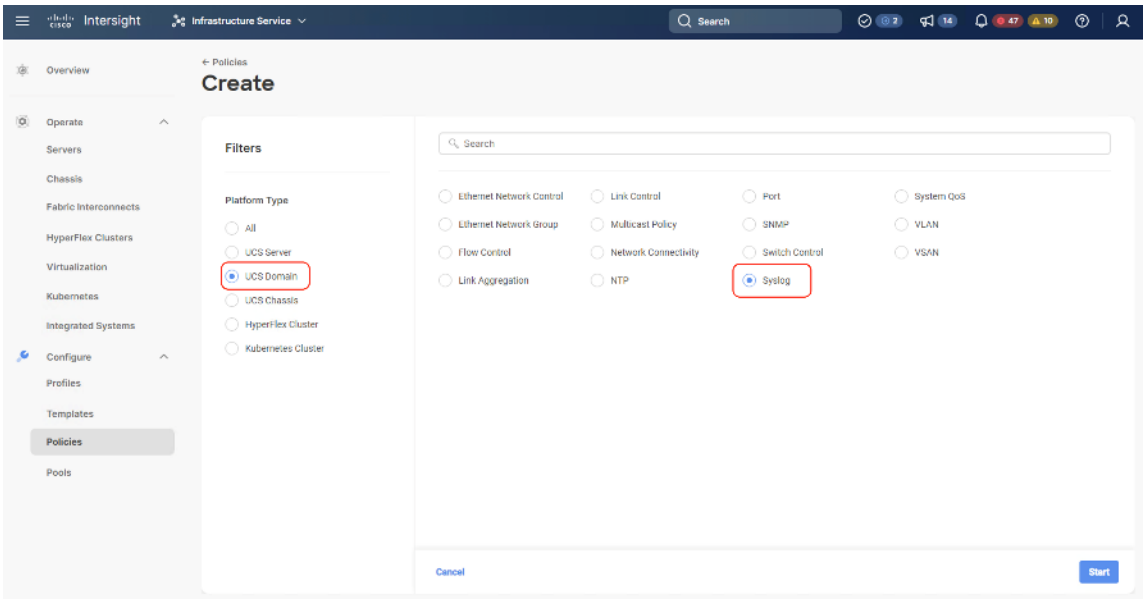


Step 5. Click Create.

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.



Step 2. Provide a name for the syslog policy.

Step 3. Click Next.

Step 4. Define the syslog severity level that triggers a report.

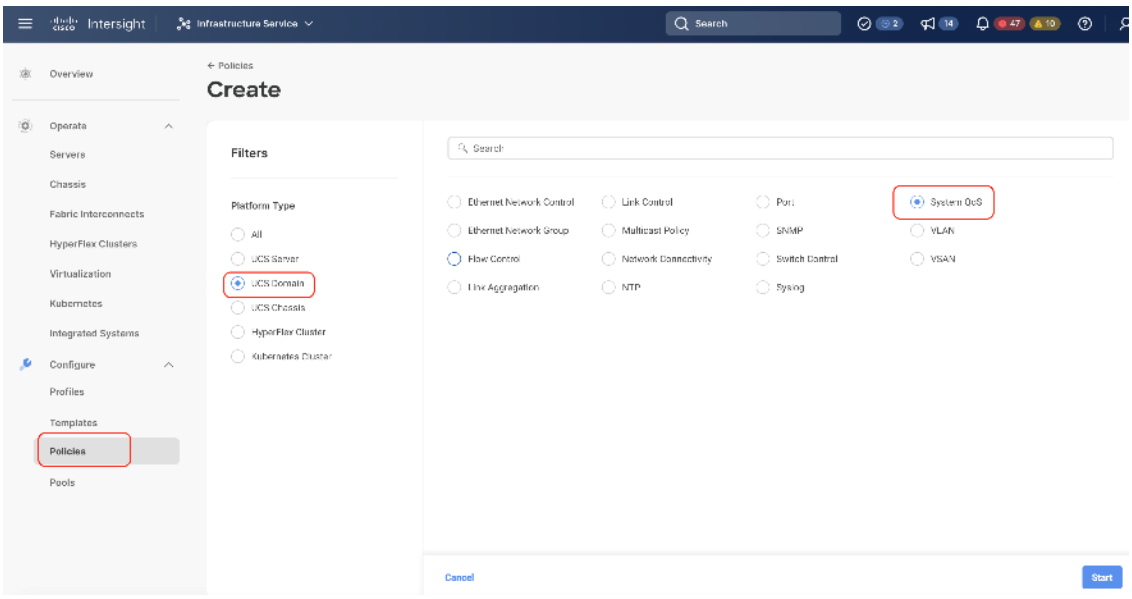
Step 5. Define the name or IP address for the syslog servers.

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.

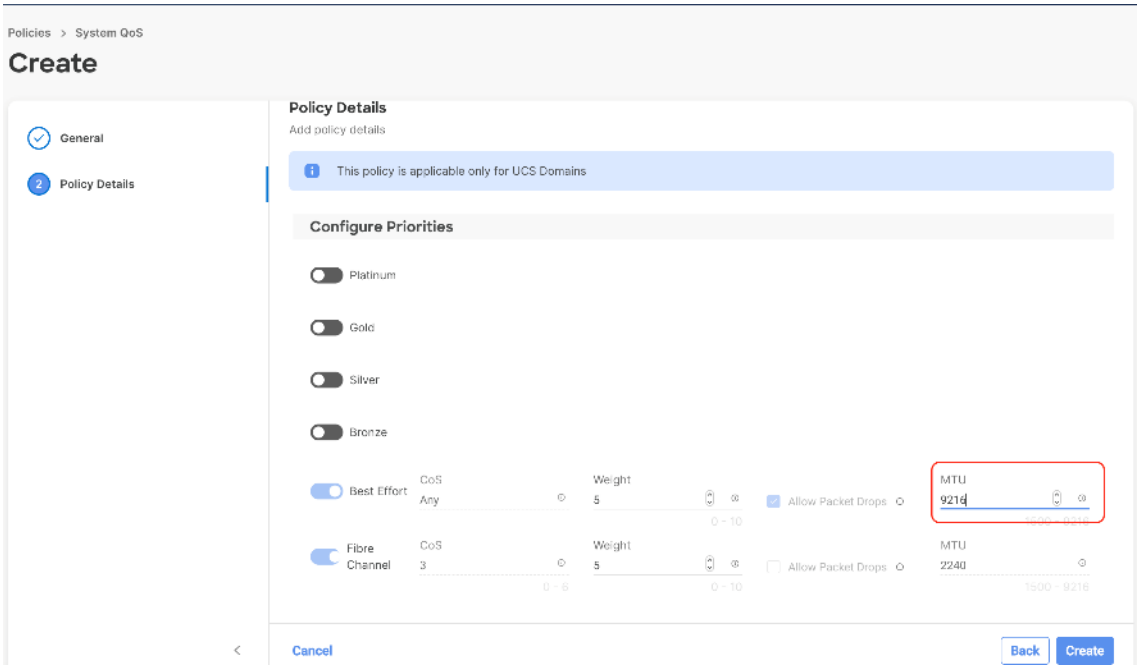
Step 1. Under Policies, select Create Policy, select UCS Domain, then select System QoS. Click Start.



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.

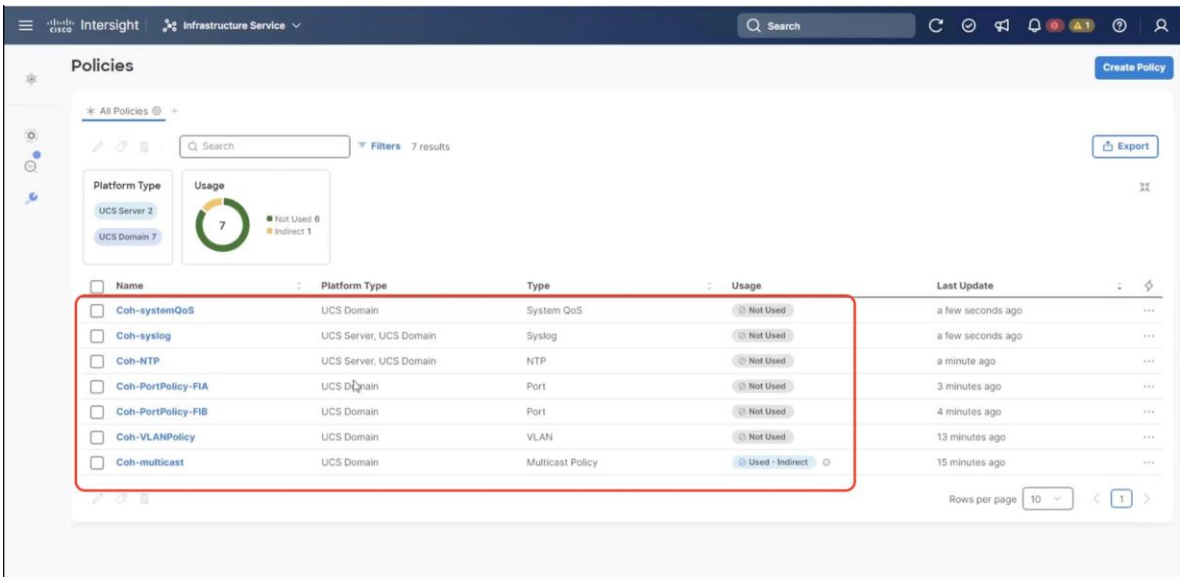


Note: All the Domain Policies created in this procedure will be attached to a Domain Profile. You can clone the Cisco UCS domain profile to install additional Cisco UCS Systems. When cloning the Cisco UCS domain profile, the new Cisco UCS domains use the existing policies for consistent deployment of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



Procedure 6. Create Domain Profile

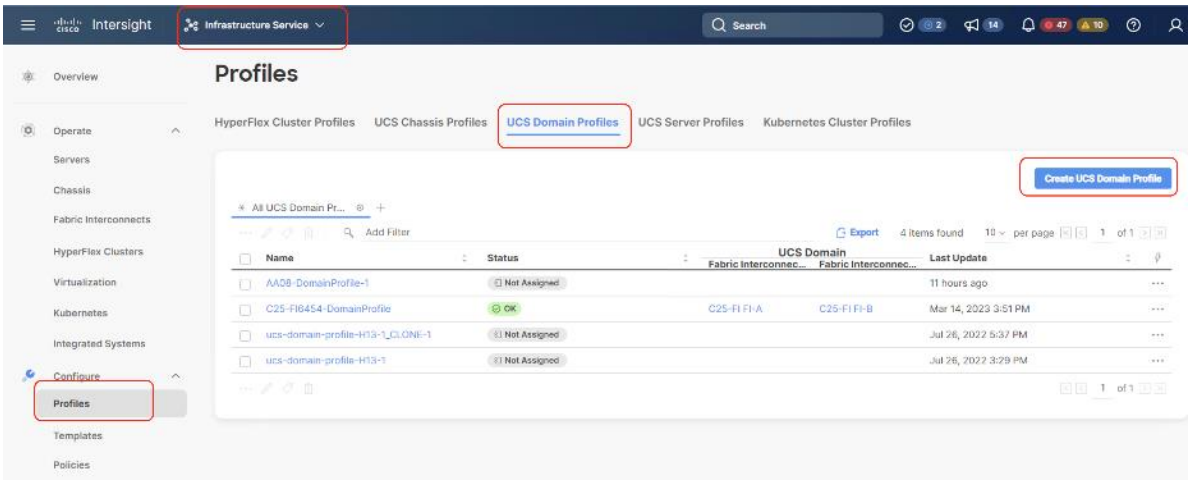
Note: All the Domain Policies created in this procedure will be attached to a Domain Profile. You can clone the Cisco UCS domain profile to install additional Cisco UCS Systems. When cloning the Cisco UCS domain profile, the new Cisco UCS domains use the existing policies for consistent deployment of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

Step 1. Prior to creating Domain Profile, please ensure the below Domain Policies are created.

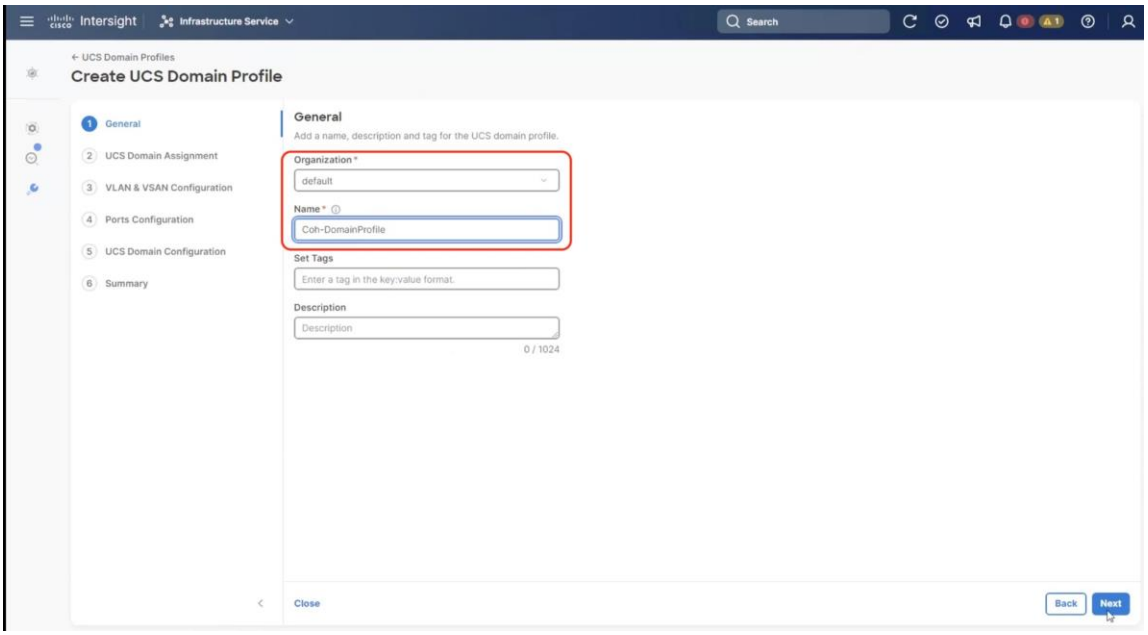
Step 2. Select the Infrastructure Service option and click Profiles.

Step 3. Select UCS Domain Profiles.

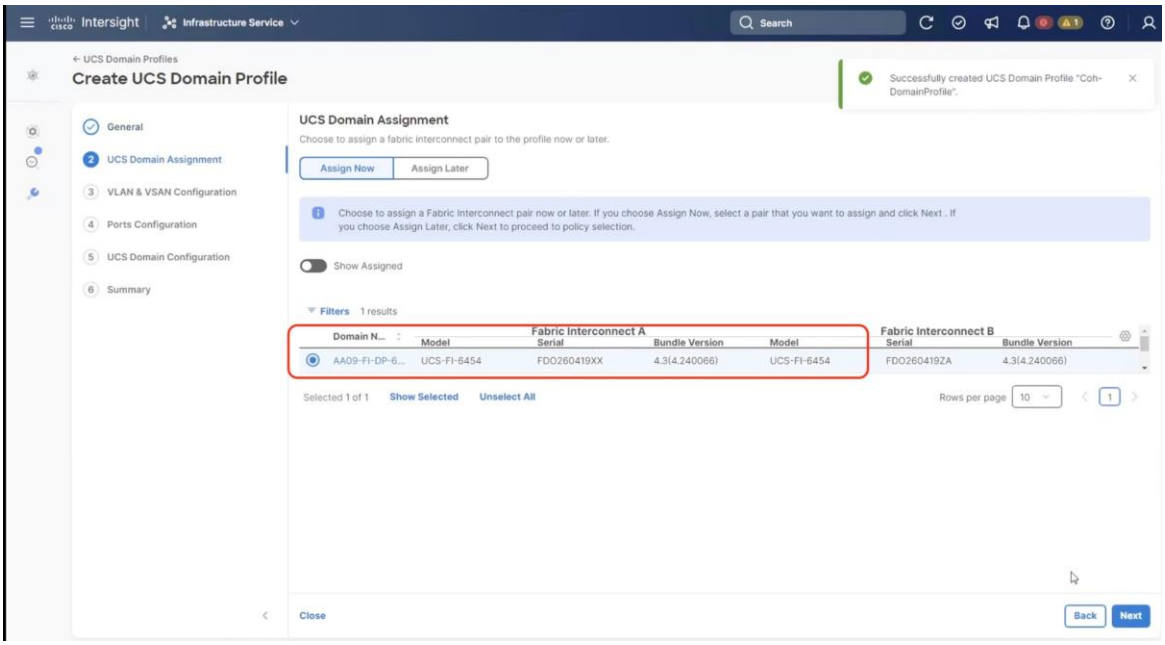
Step 4. Click Create UCS Domain Profile.



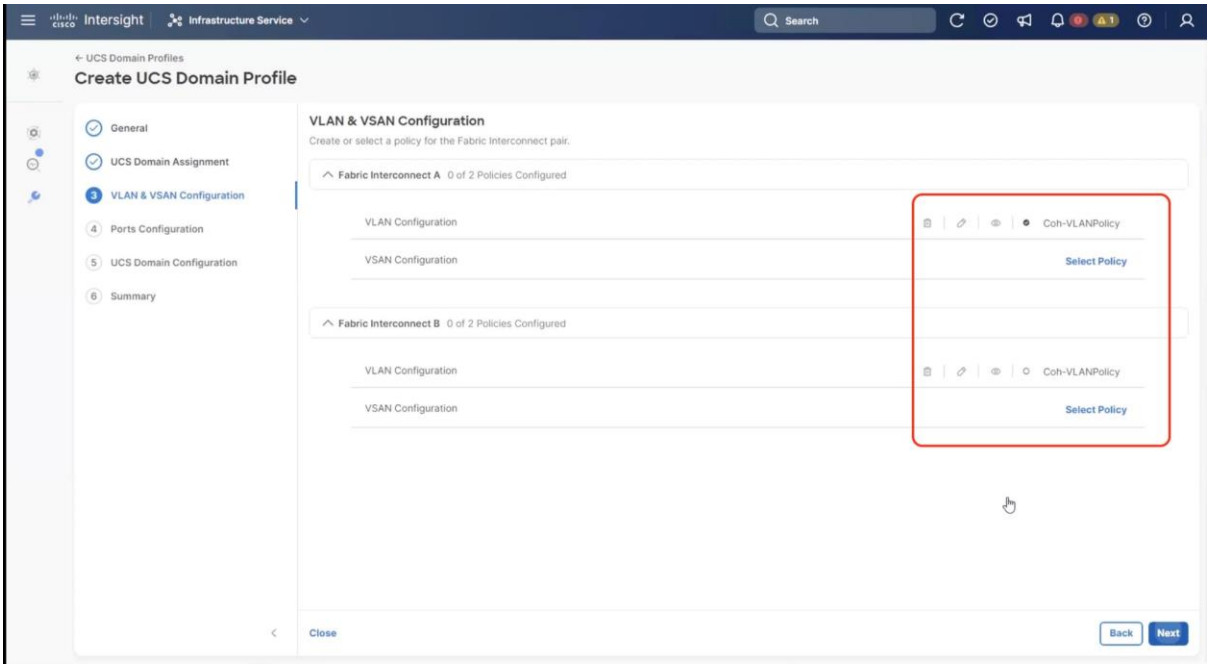
Step 5. Provide a name for the profile (for example, Coh-DomainProfile) and click Next.



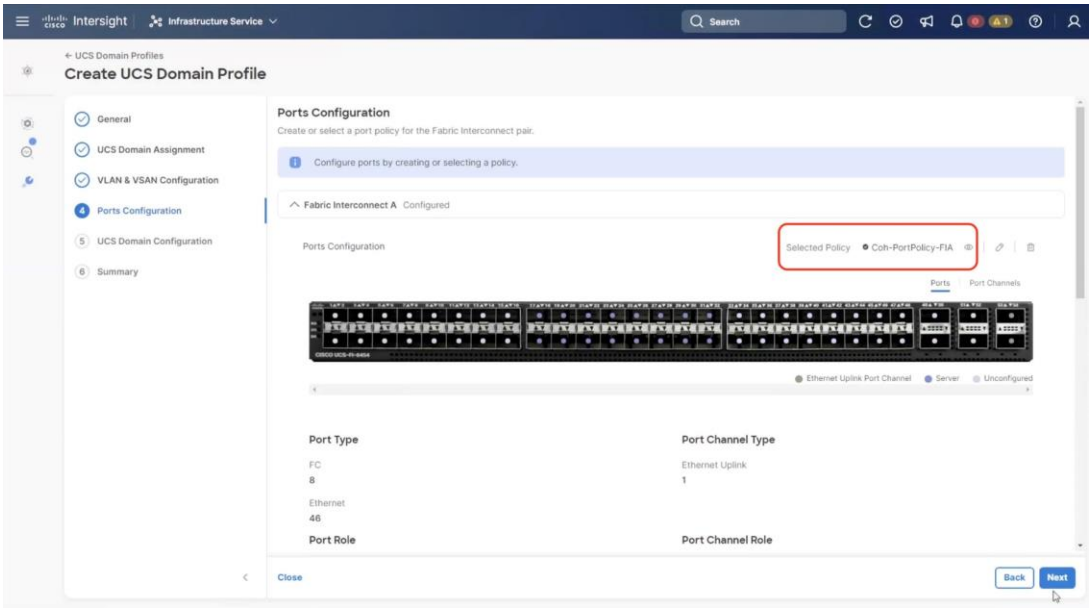
Step 6. Select the fabric interconnect domain pair created when you claimed your Fabric Interconnects.



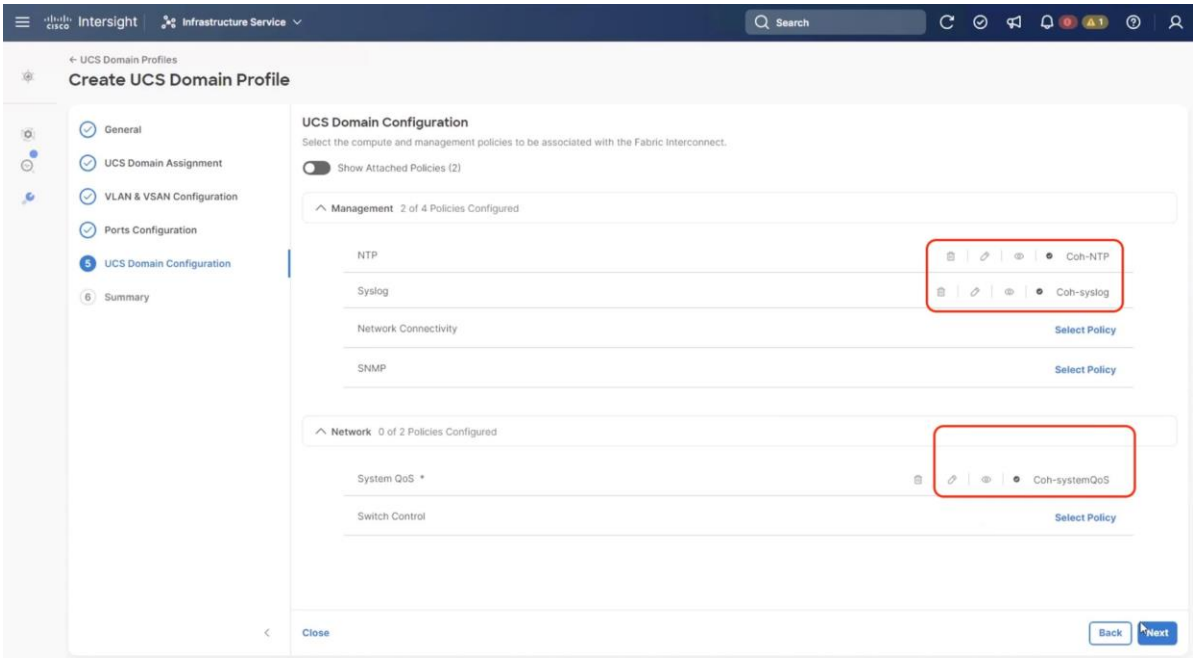
Step 7. Under VLAN & VSAN Configuration, click Select Policy to select the policies created earlier. (Be sure that you select the appropriate policy for each side of the fabric.) In this configuration the VLAN policy is same for both the fabric interconnects.



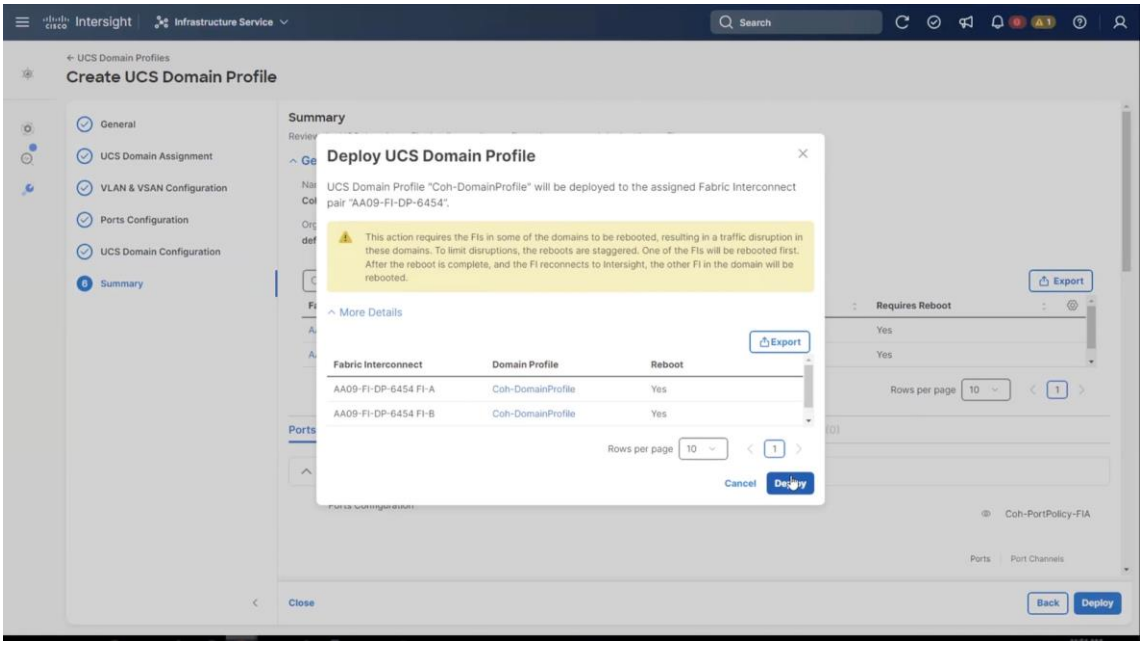
Step 8. Under Ports Configuration, select the port configuration policies created earlier. Each fabric has different port configuration policy. In this setup, only the port channel ID is different across both the Port Configuration Policy.



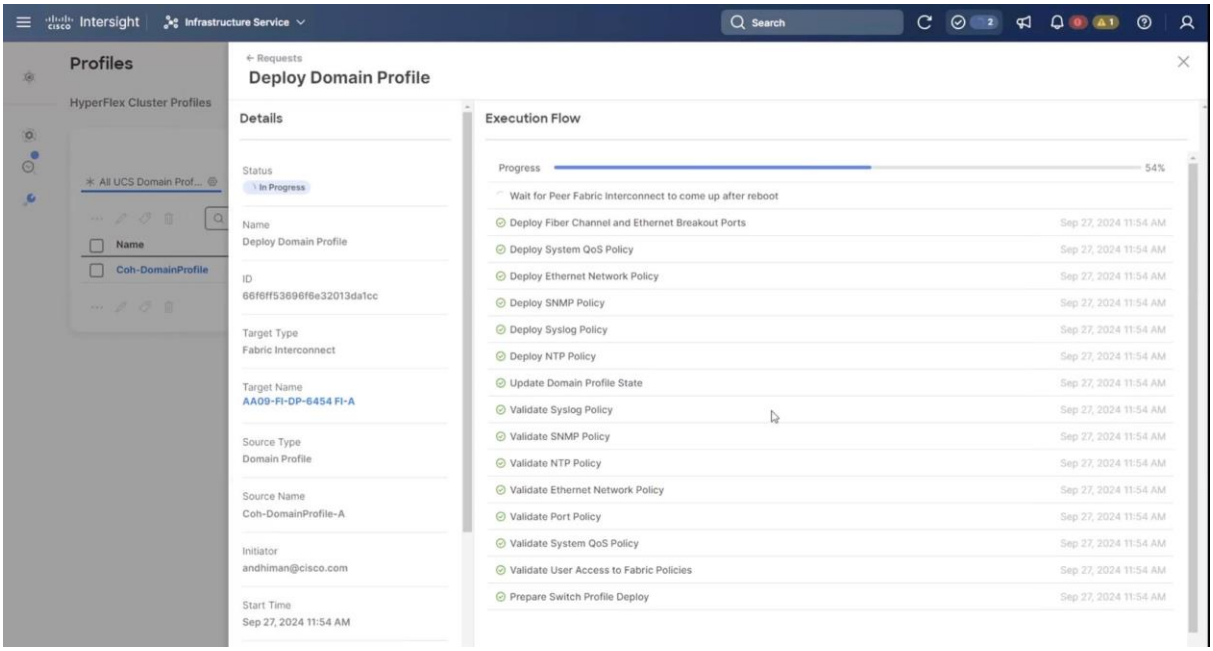
Step 9. Under UCS Domain Configuration, select syslog, System QoS, and the NTP policies you created earlier. Click Next.



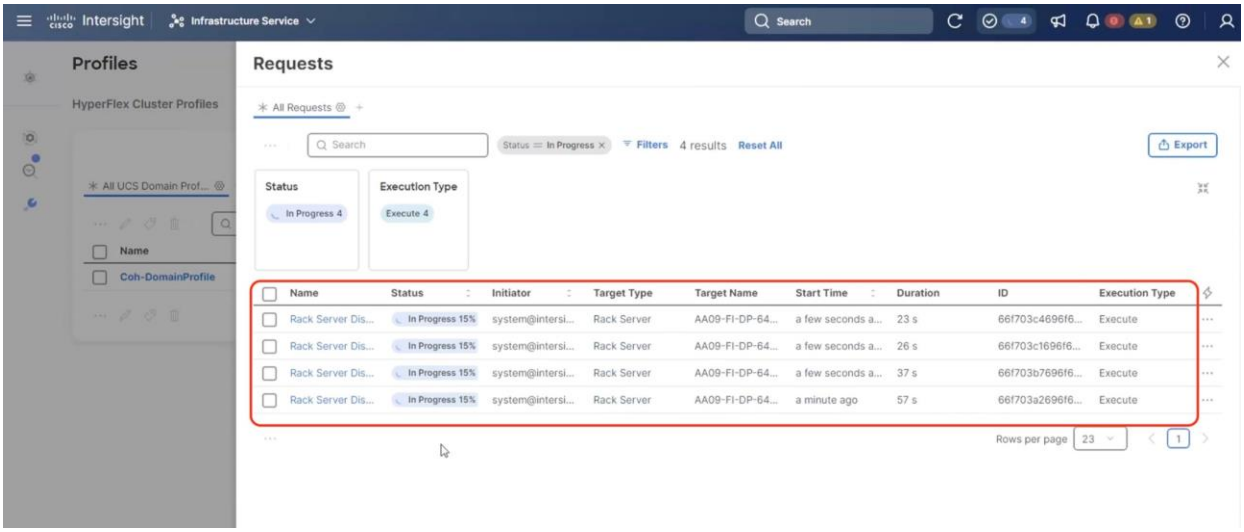
Step 10. Review the Summary and click Deploy. Accept the warning for the Fabric Interconnect reboot and click Deploy.

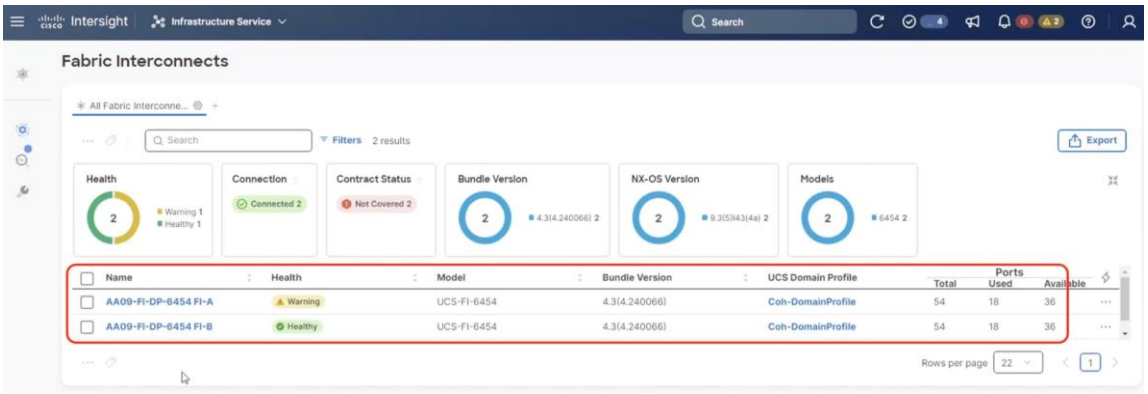


Step 11. Monitor the Domain Profile deployment status and ensure the successful deployment of Domain Profile.

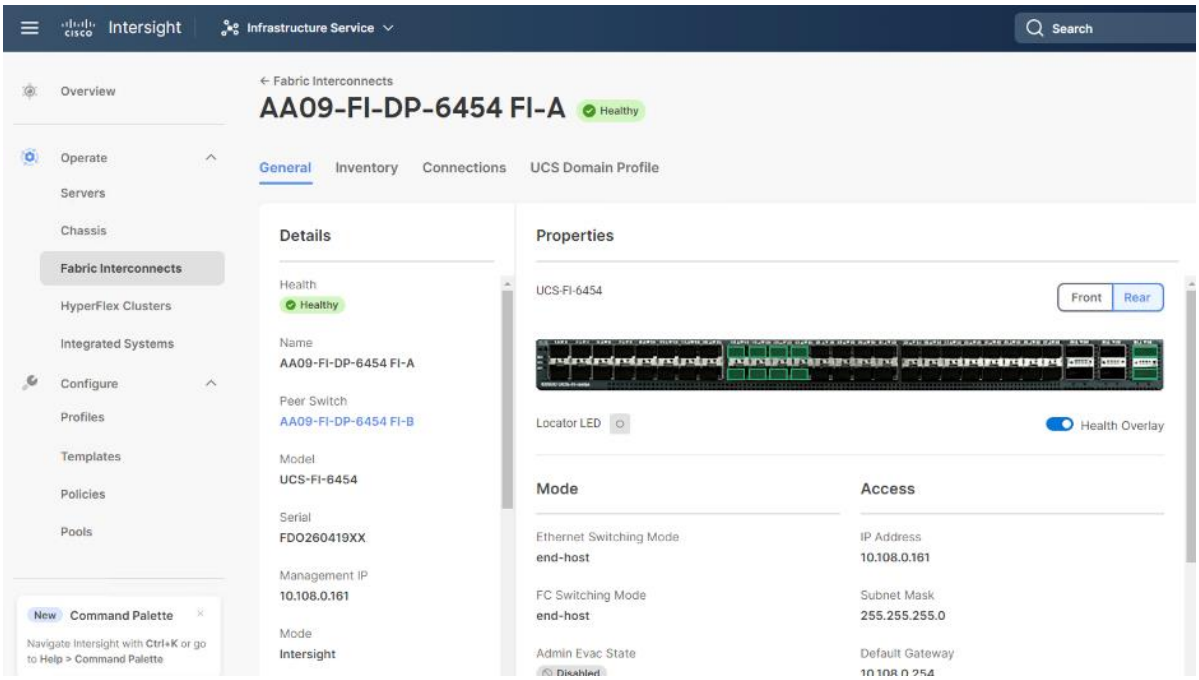


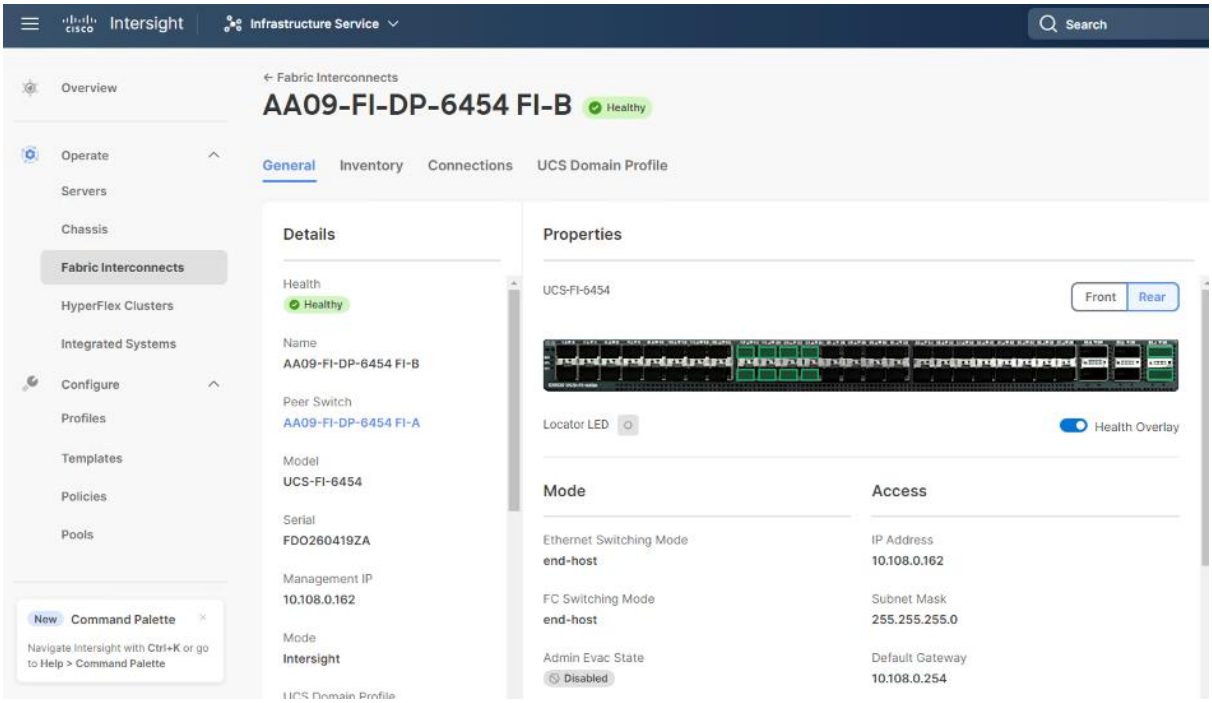
Step 12. In the event Cisco UCS Servers are already connected to server ports on Fabric Interconnect, they would be discovered in this process.





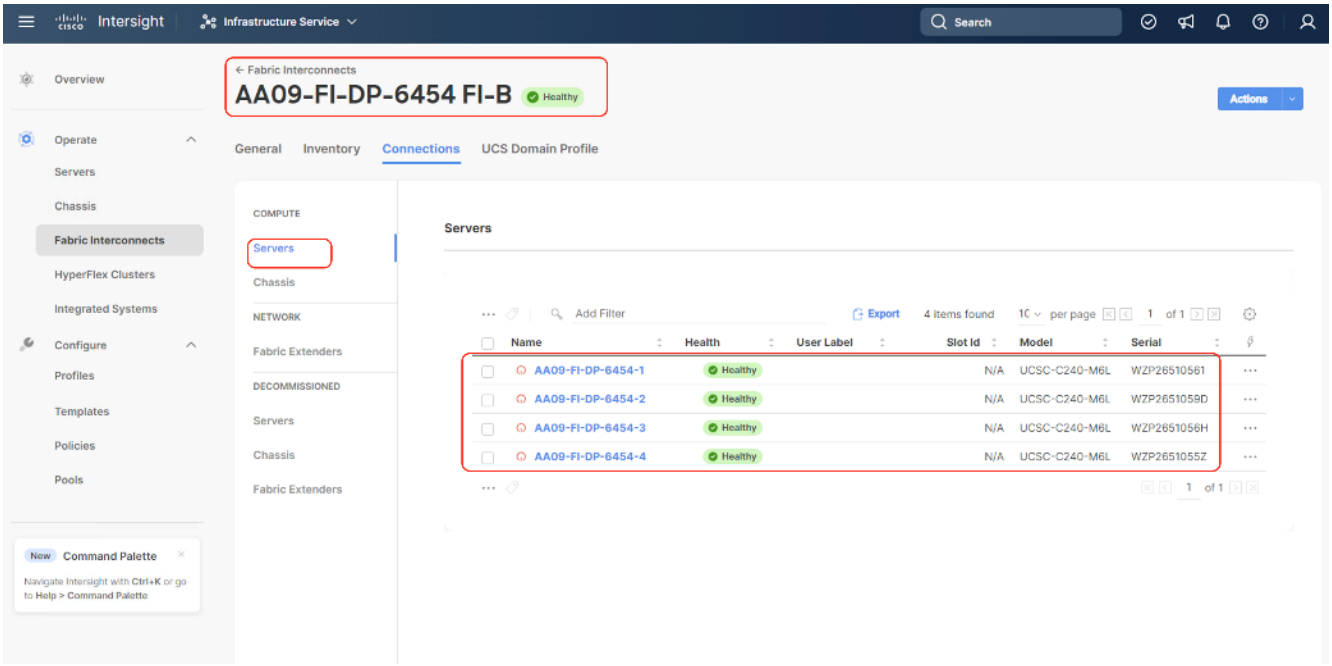
Step 13. Verify the uplink and Server ports are online across both Fabric Interconnects. In the event, the uplink ports are not green, please verify the configuration on the uplink Nexus switches.





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.



Manual Setup Server Template

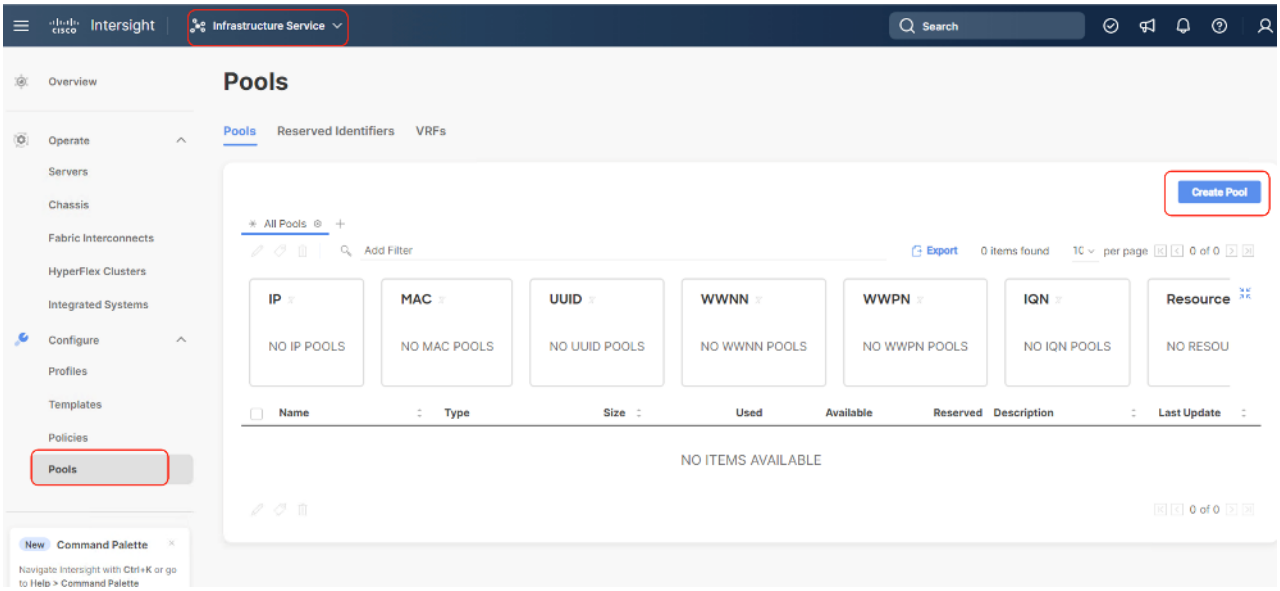
A server profile template enables resource management by simplifying policy alignment and server configuration. You can create a server profile template by using the server profile template wizard, which groups the server policies into the following categories to provide a quick summary view of the policies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

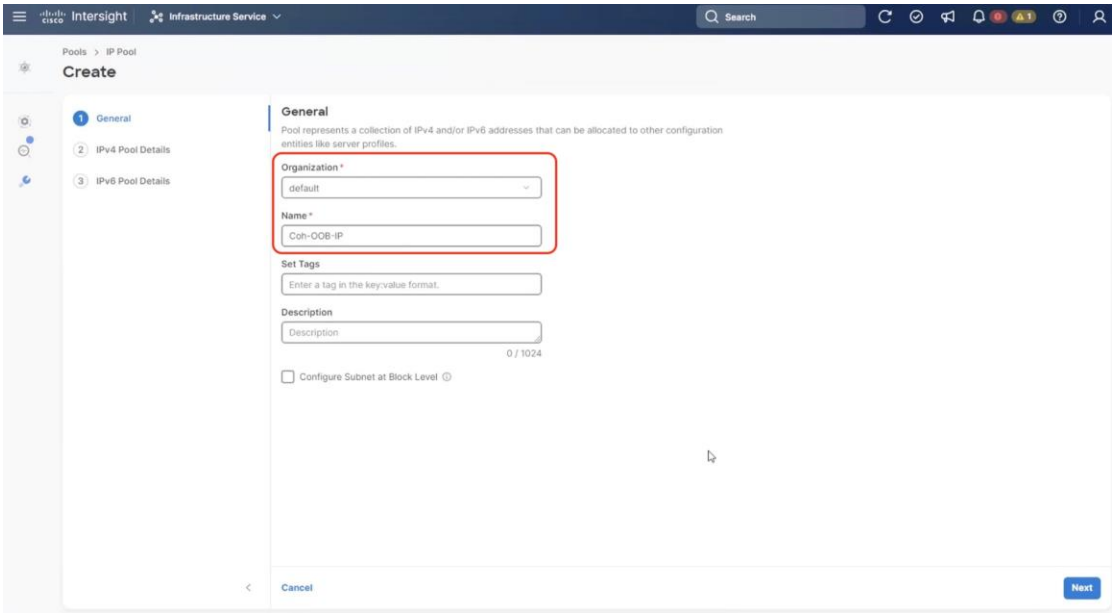
The IP Pool is a group of IP for KVM access, Server management of Cohesity certified nodes. The management IP addresses used to access the CIMC on a server can be out-of-band (OOB) addresses, through which traffic traverses the fabric interconnect via the management port.

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

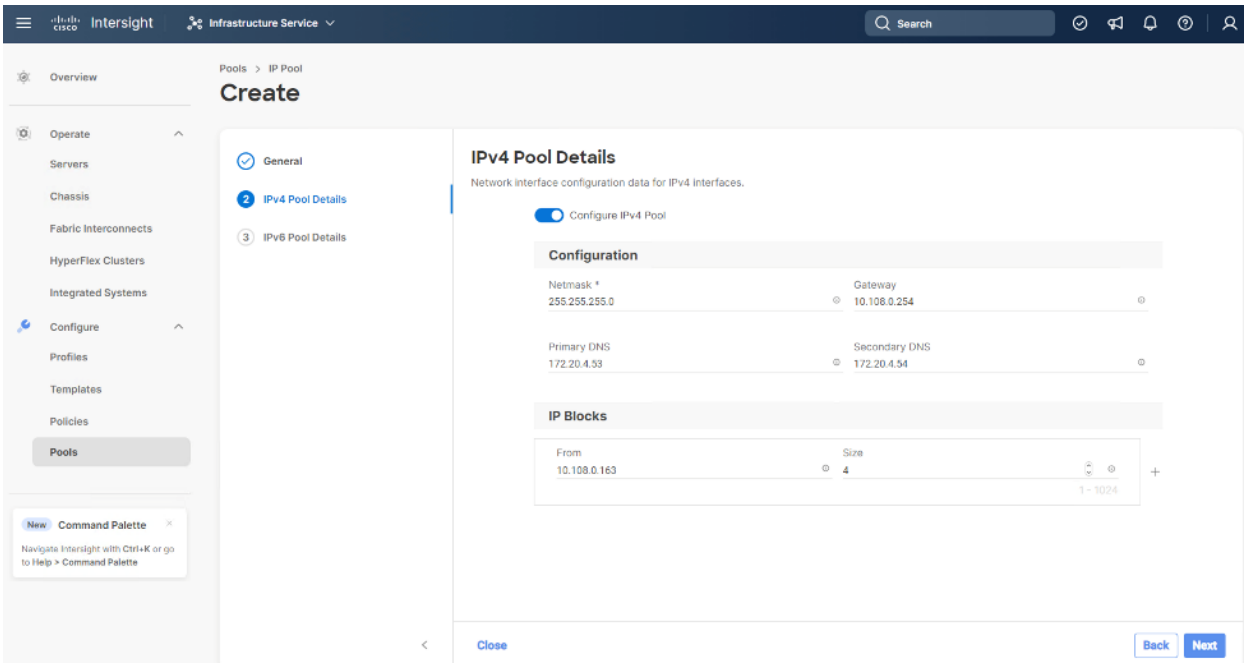


Step 2. Select IP and click Start.

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



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



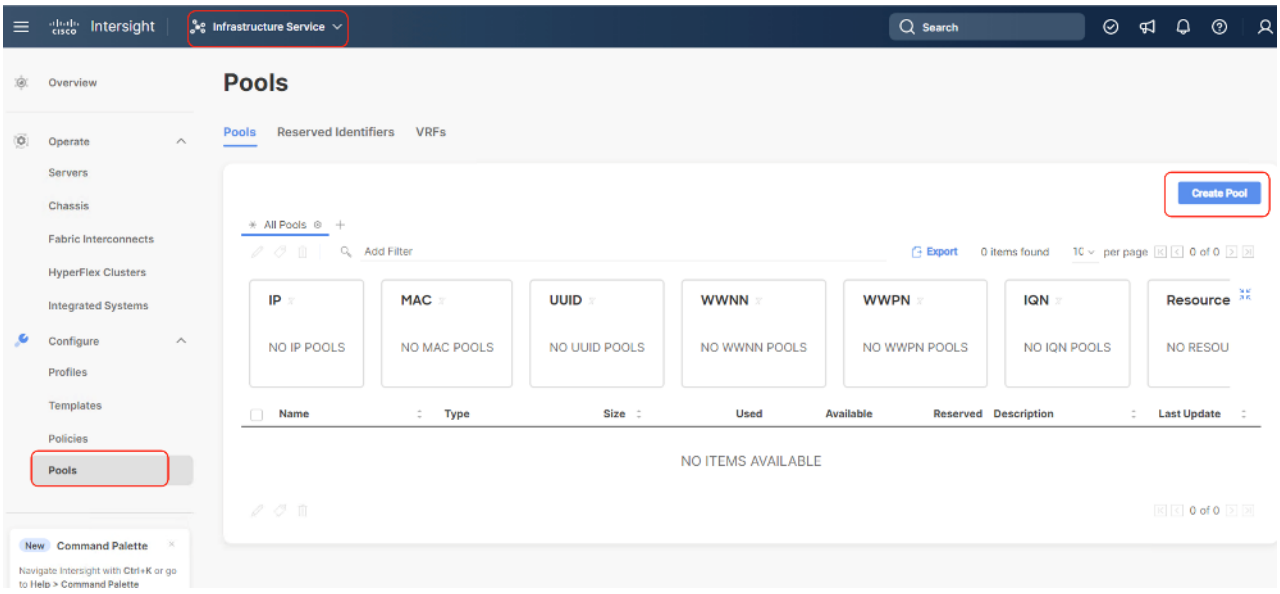
Step 5. Deselect the IPV6 configuration and click Create.

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.

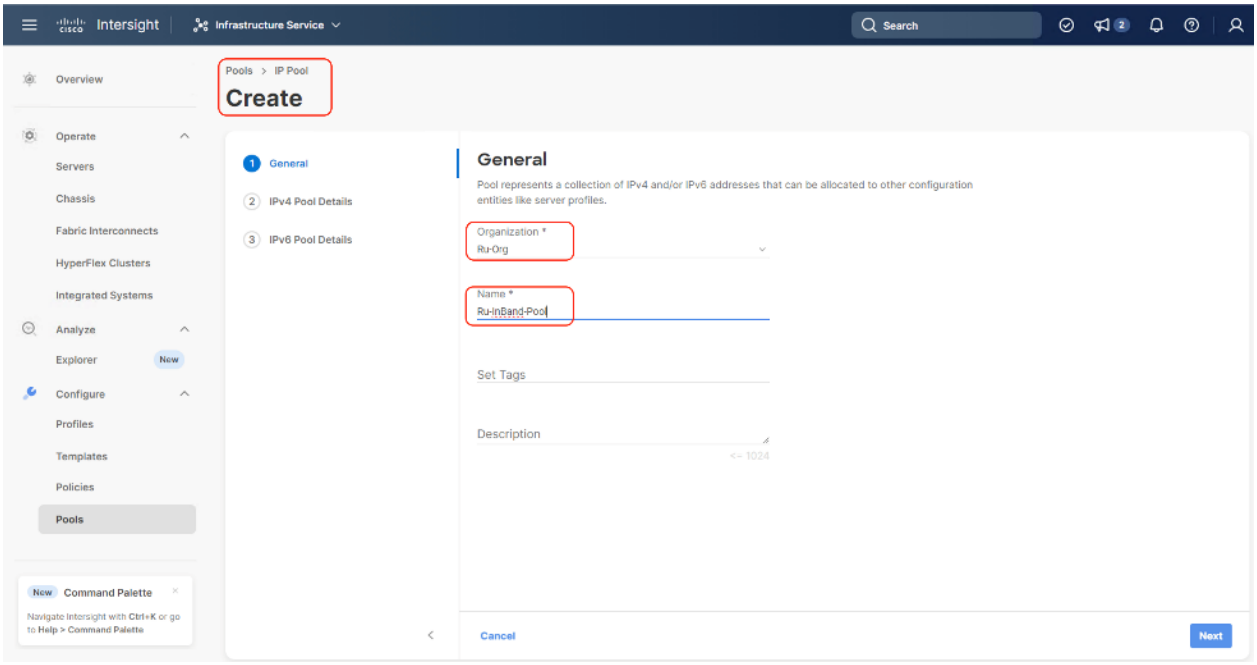
Note: Since vMedia is not supported for out-of-band IP configurations, the OS Installation through Intersight for FI-attached servers in IMM requires an In-Band Management IP address. For more information, go to: https://intersight.com/help/saas/resources/adding_OSimage.

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

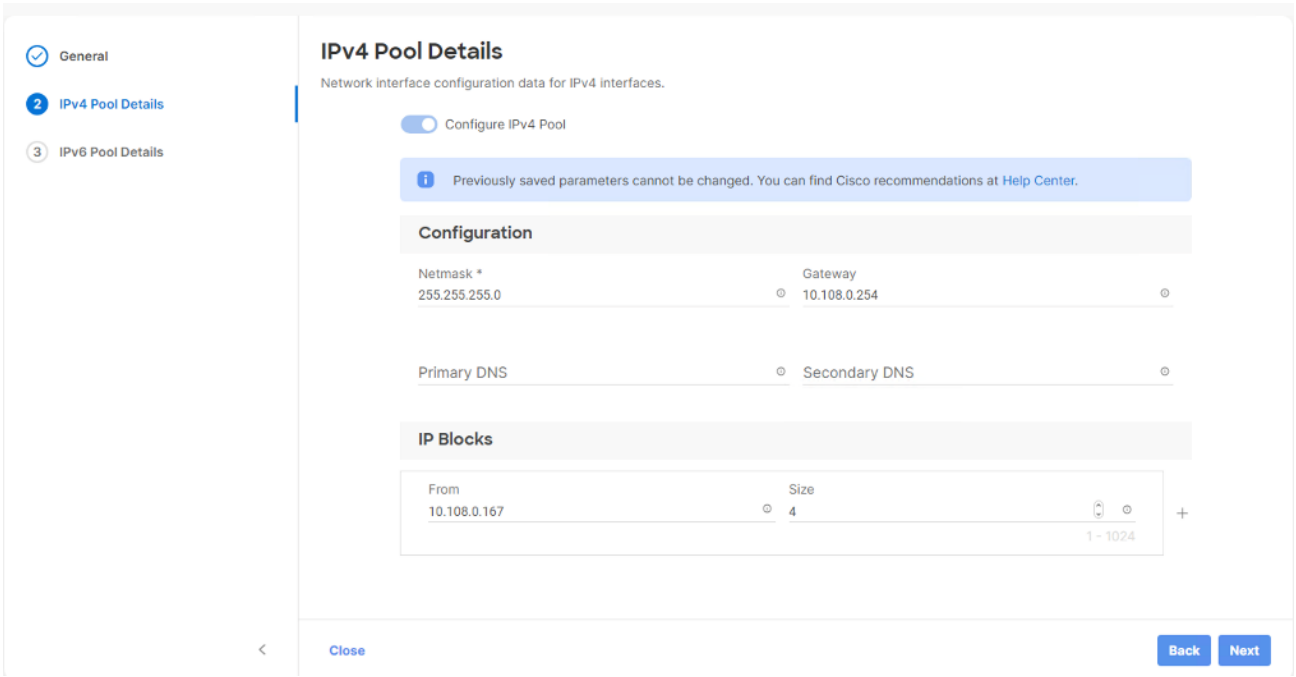


Step 2. Select IP and click Start.

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



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



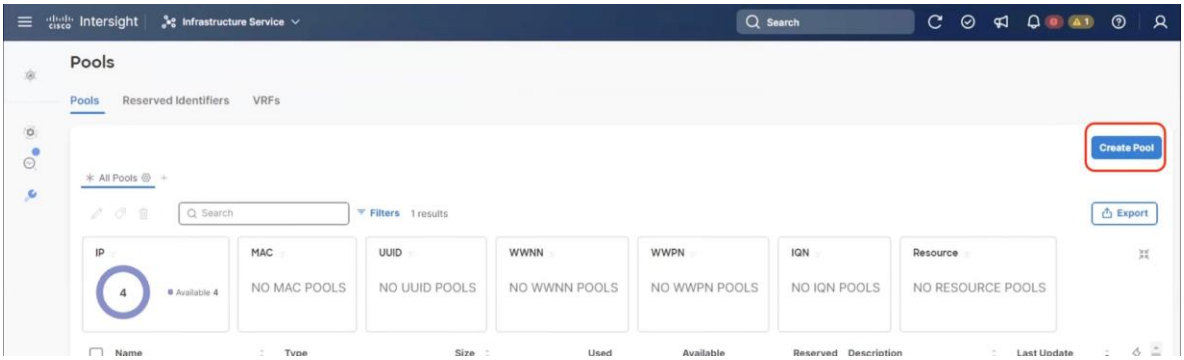
Step 5. Deselect the IPV6 configuration and click Create.

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.

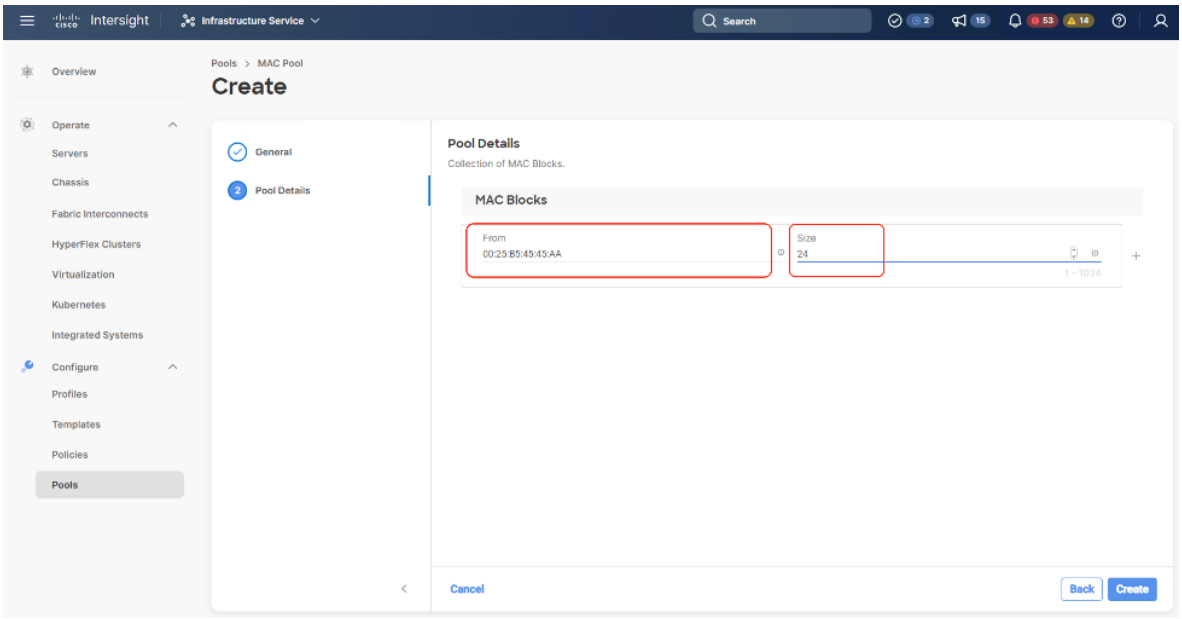
Step 6. Click Infrastructure Service, select Pool, and click Create Pool.



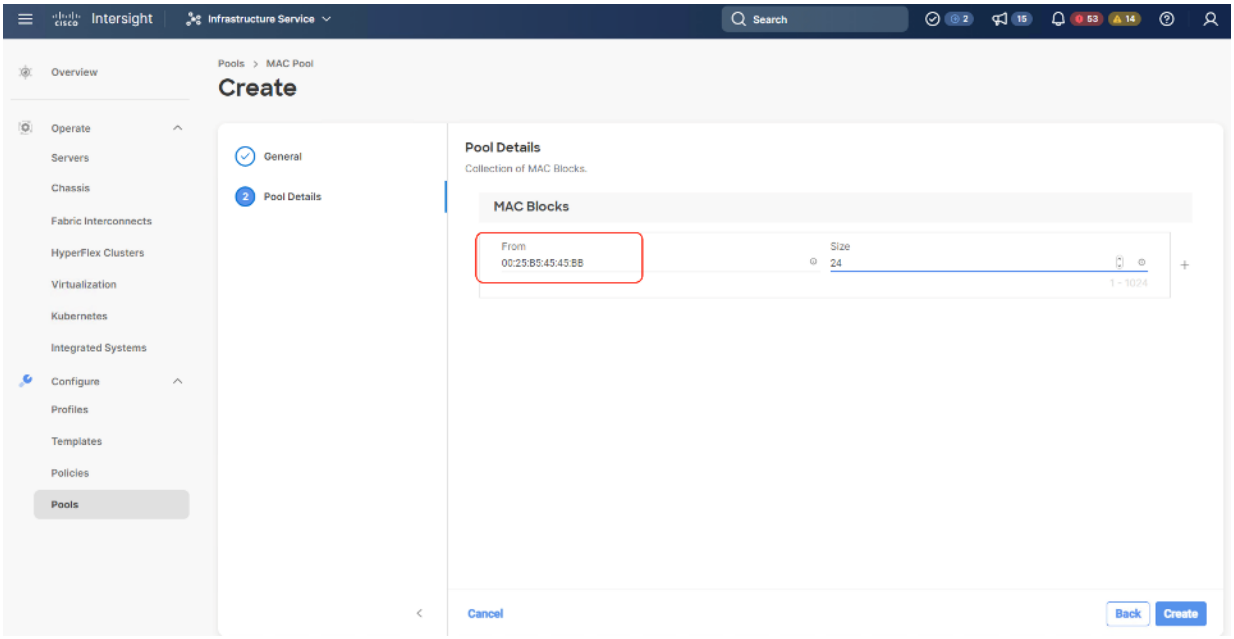
Step 7. Select MAC and click Start.

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.



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



Procedure 4. Create UUID Pool

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

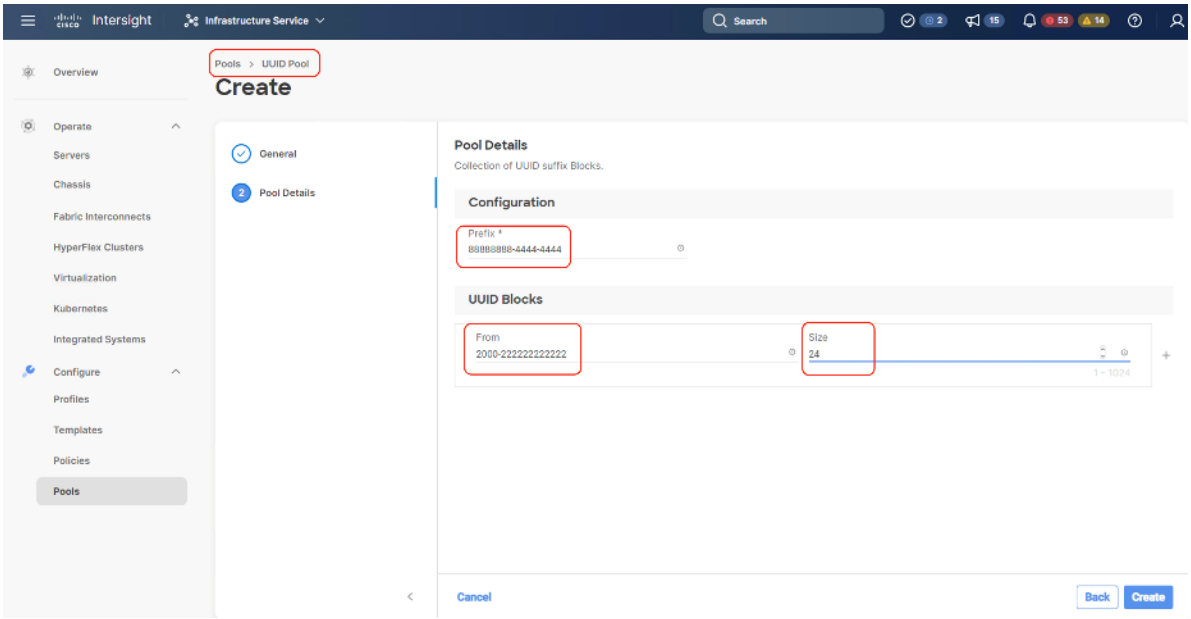
Step 2. Select UUID and click Start.

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 xxxxxxxx-xxxx-xxxx).

Step 5. Enter UUID Suffix (starting UUID suffix of the block must be in hexadecimal format xxxx-xxxxxxxxxxxx).

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



Create Server Policies

Procedure 1. Create BIOS Policy

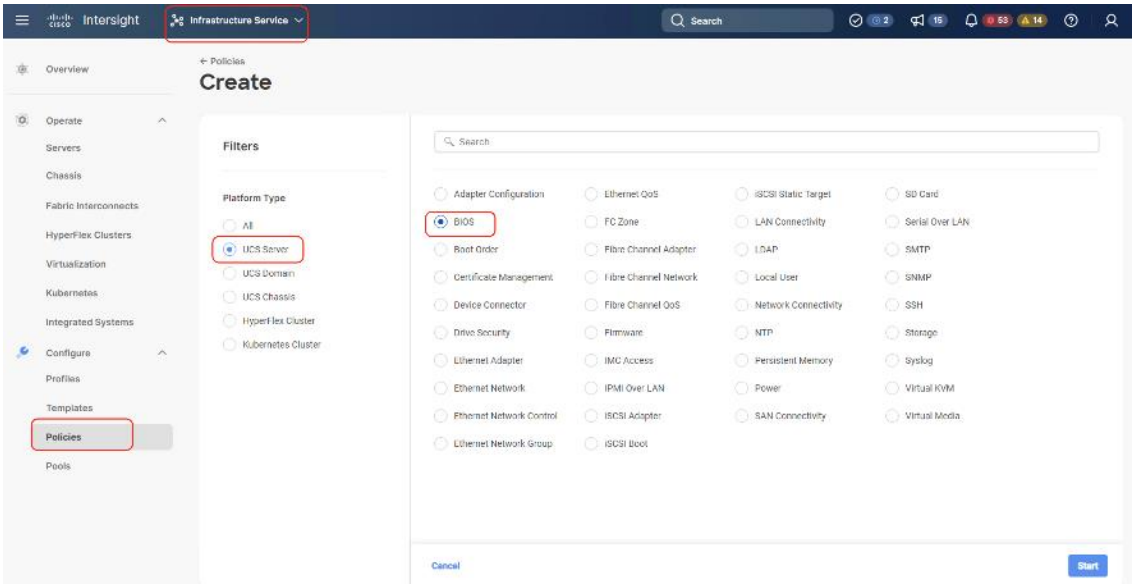
Table 14 lists the required polices for the BIOS policy.

Table 14. BIOS settings for Cohesity nodes

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.

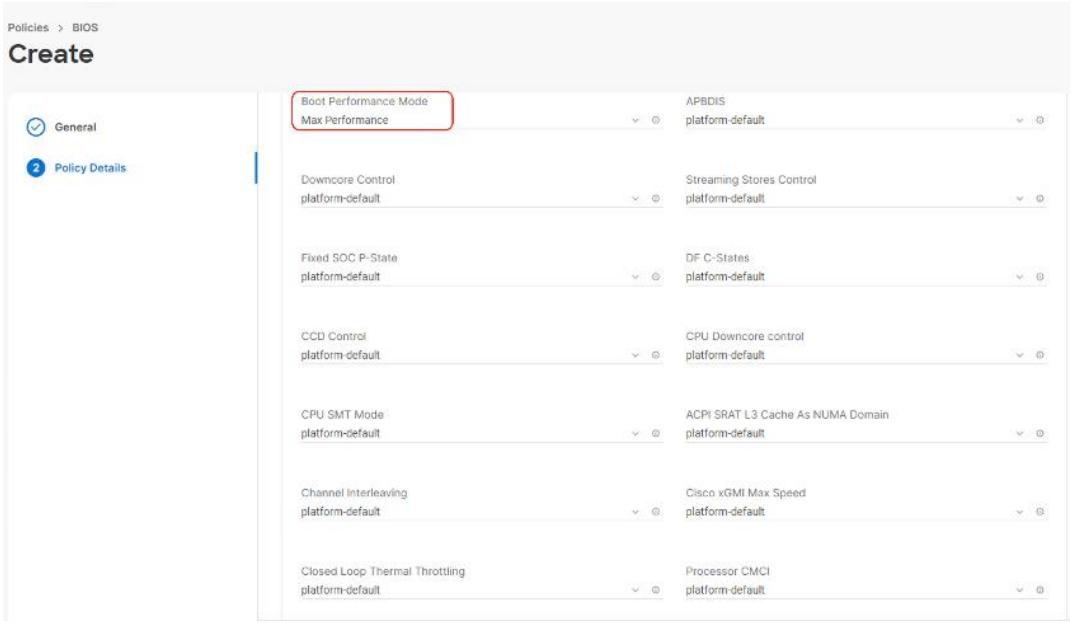
Step 2. Select UCS Server, BIOS and click Start.

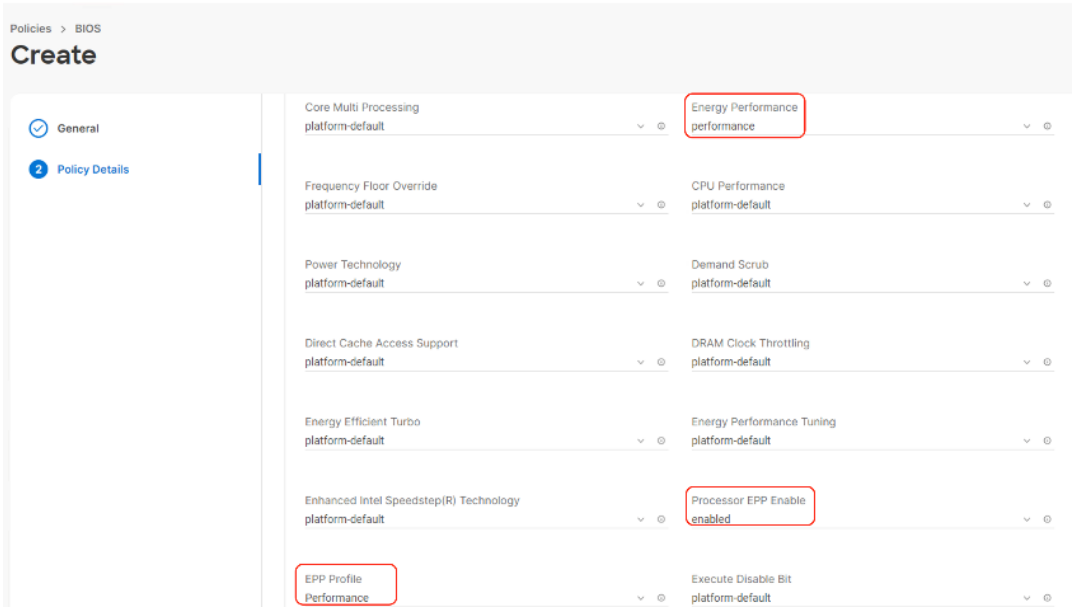


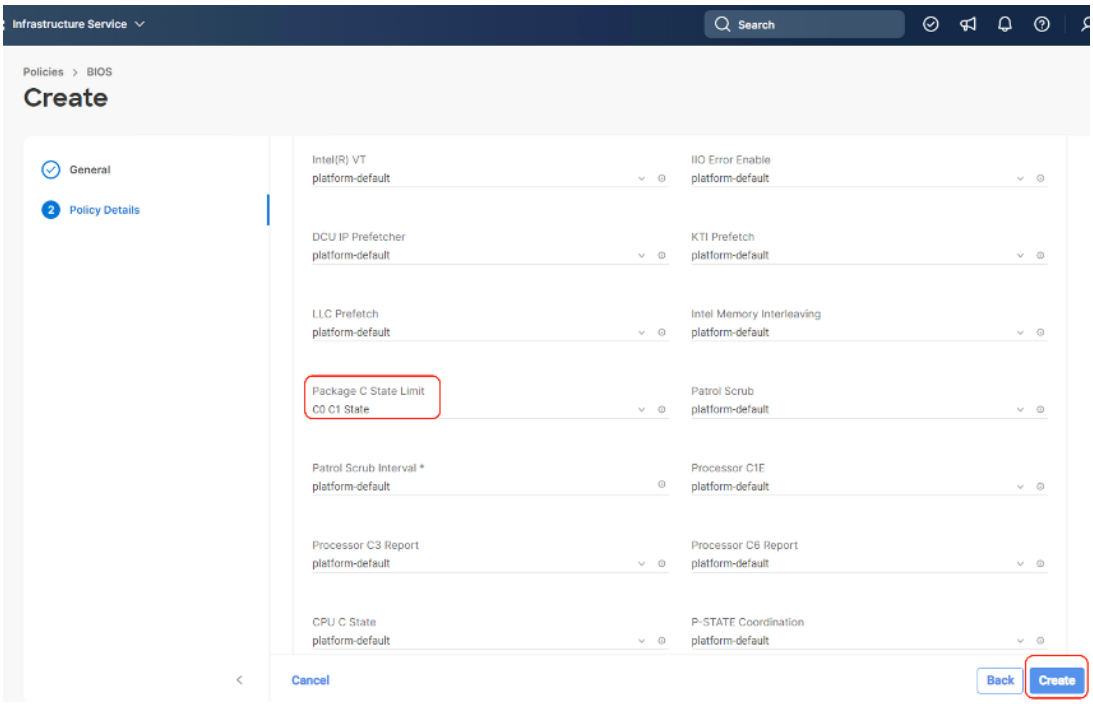
Step 3. Enter a Name for BIOS Policy.

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







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.

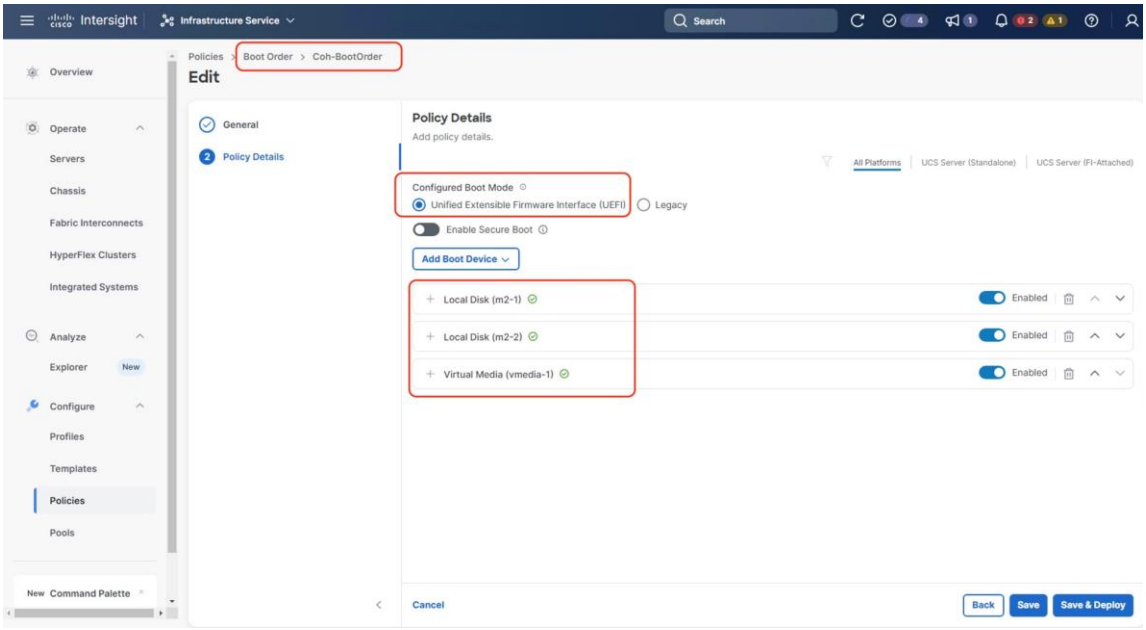
Step 4. Under Policy Detail, select UCS Server (FI Attached), and ensure UEFI is checked.

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:



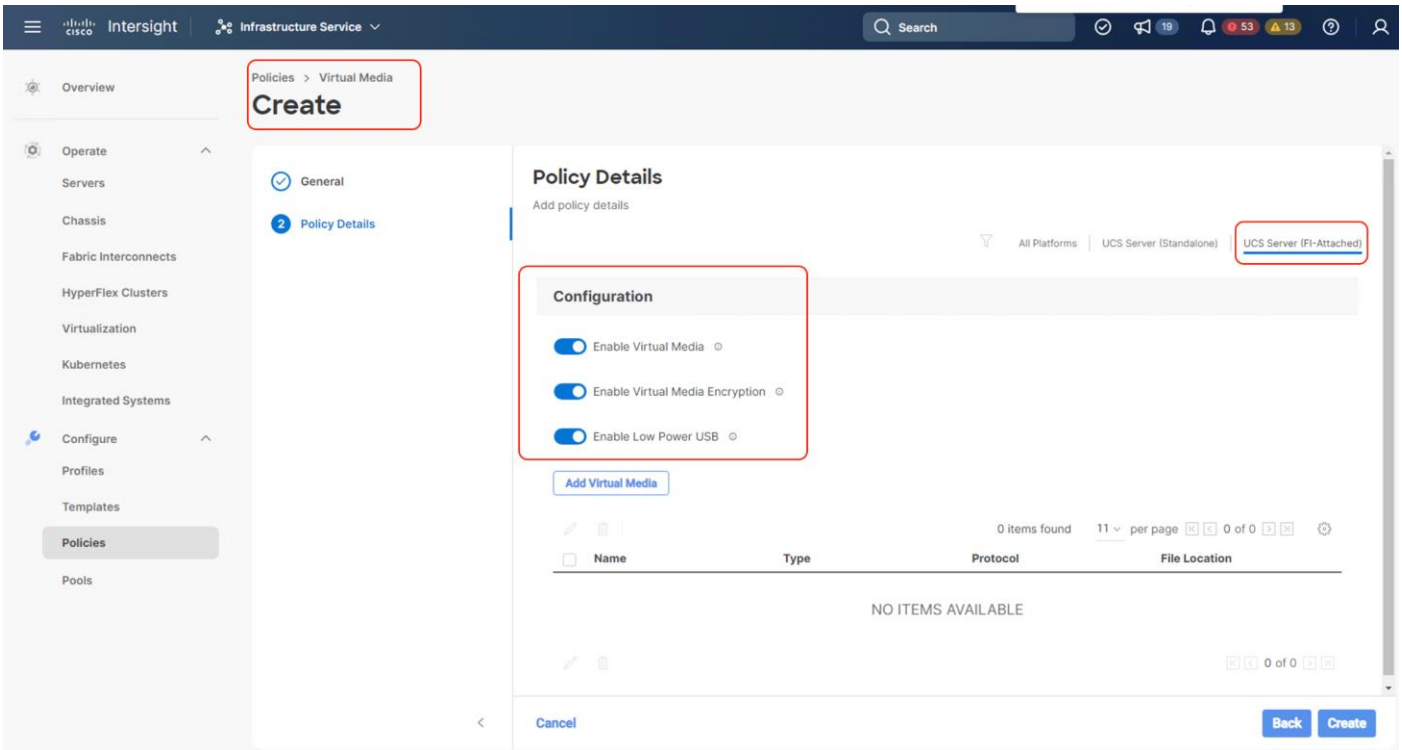
Procedure 3. Create Virtual Media Policy

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.



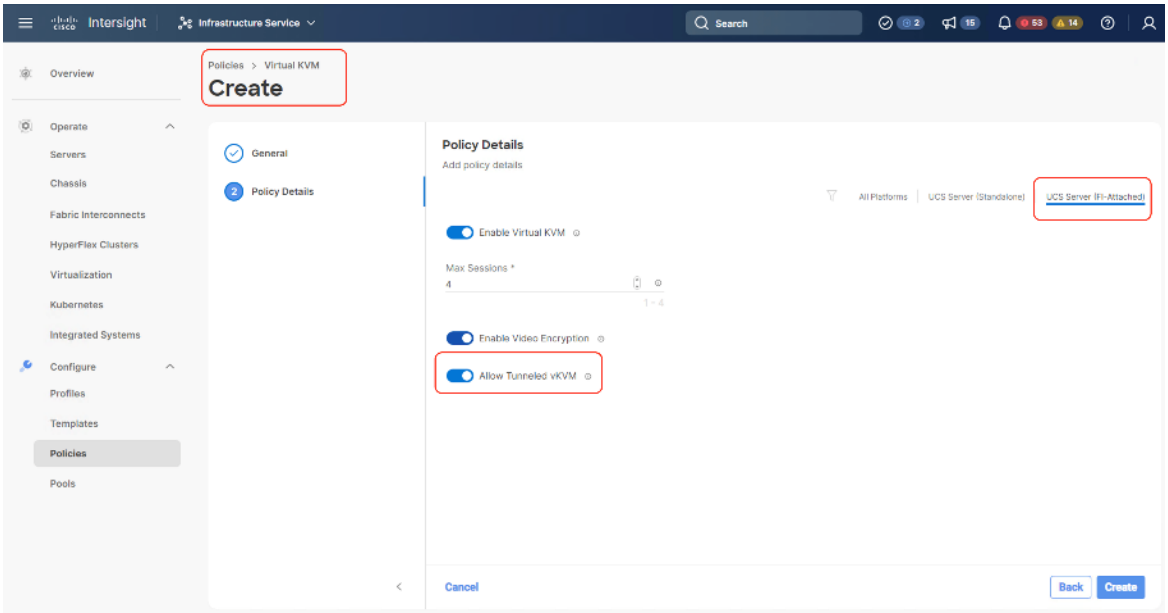
Procedure 4. Create virtual KVM Policy

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.



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.

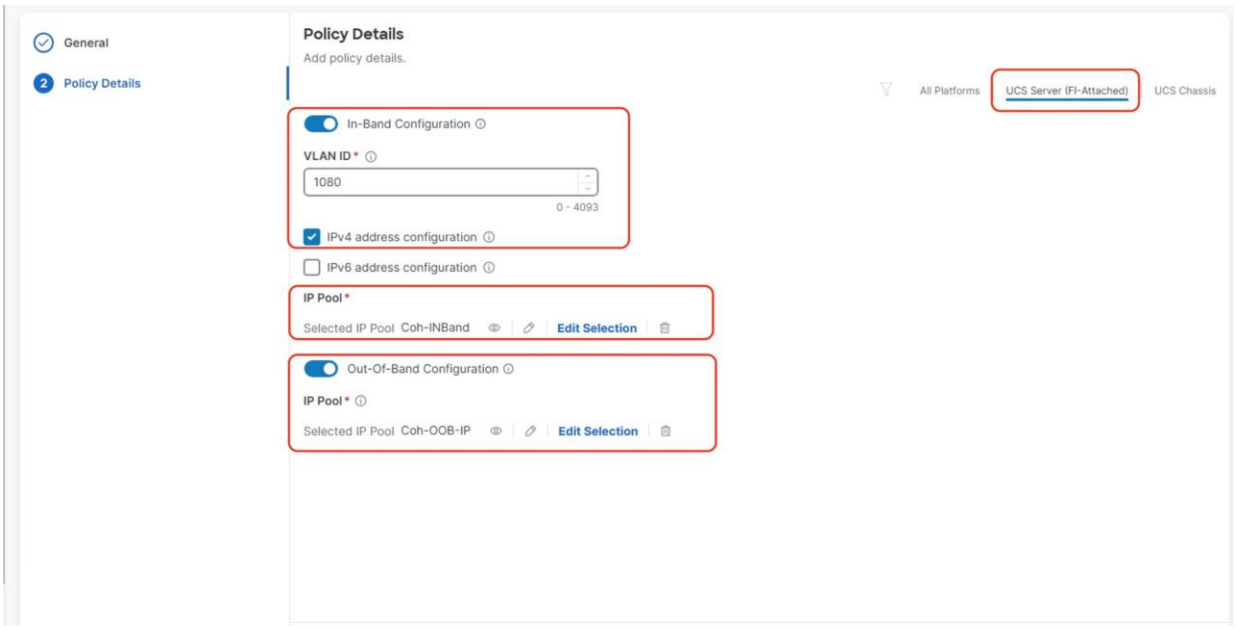
Step 4. Select UCS Server (FI-Attached).

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.



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.

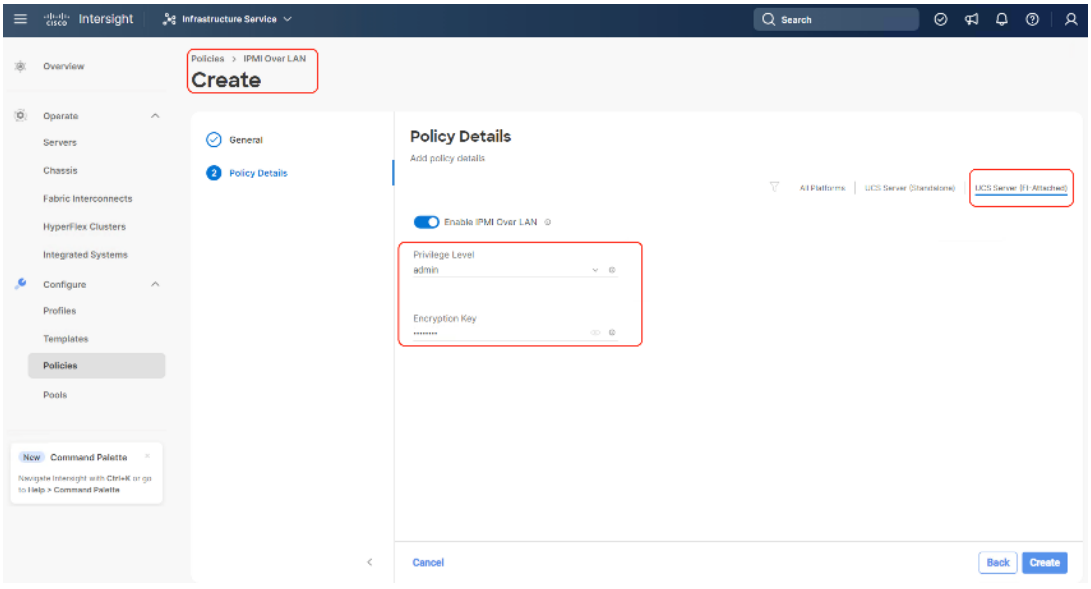
Step 1. Click Infrastructure Service, select Policies, and click Create Policy.

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.



Step 6. Click Save.

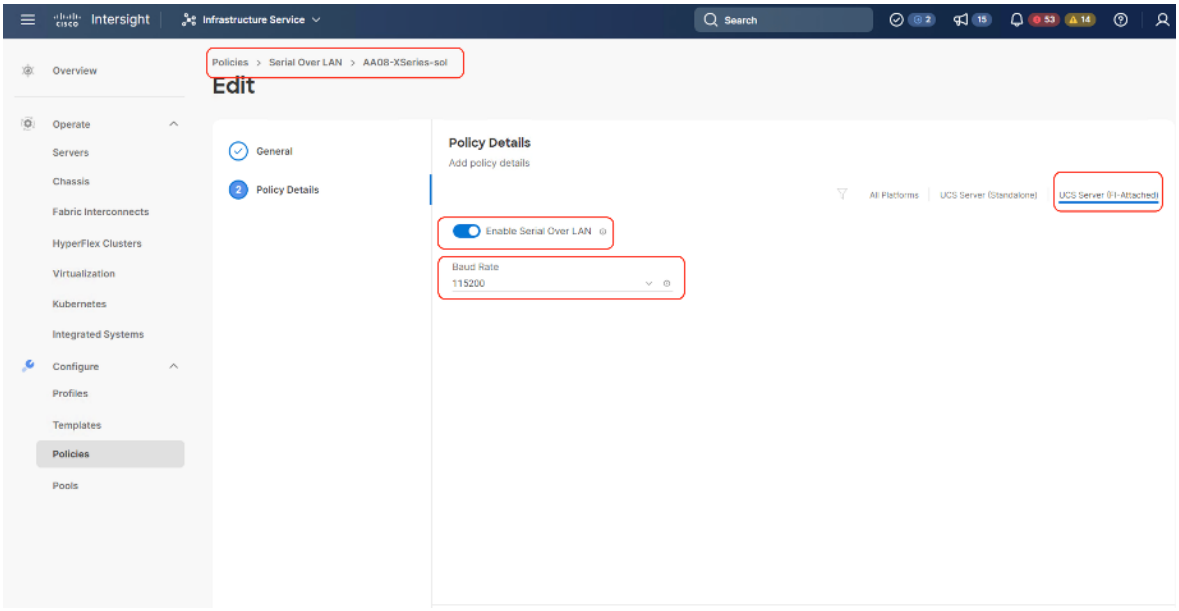
Procedure 7. Create Serial over LAN Policy

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.



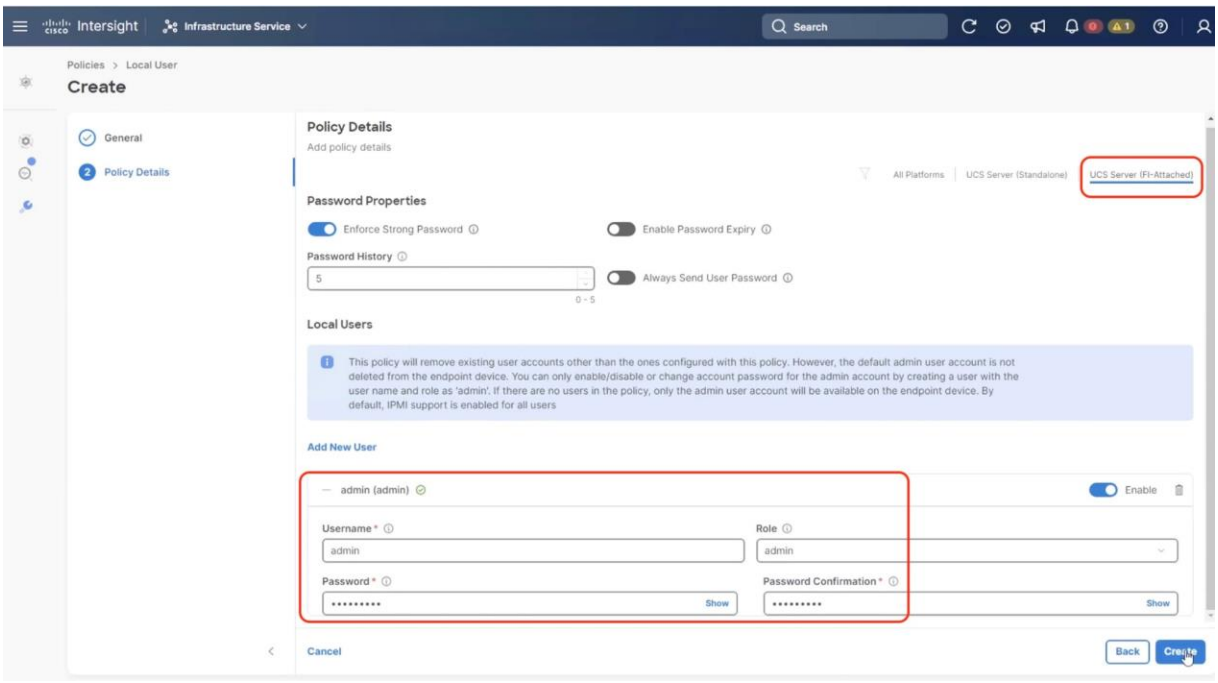
Procedure 8. Create Local User Policy

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.



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).

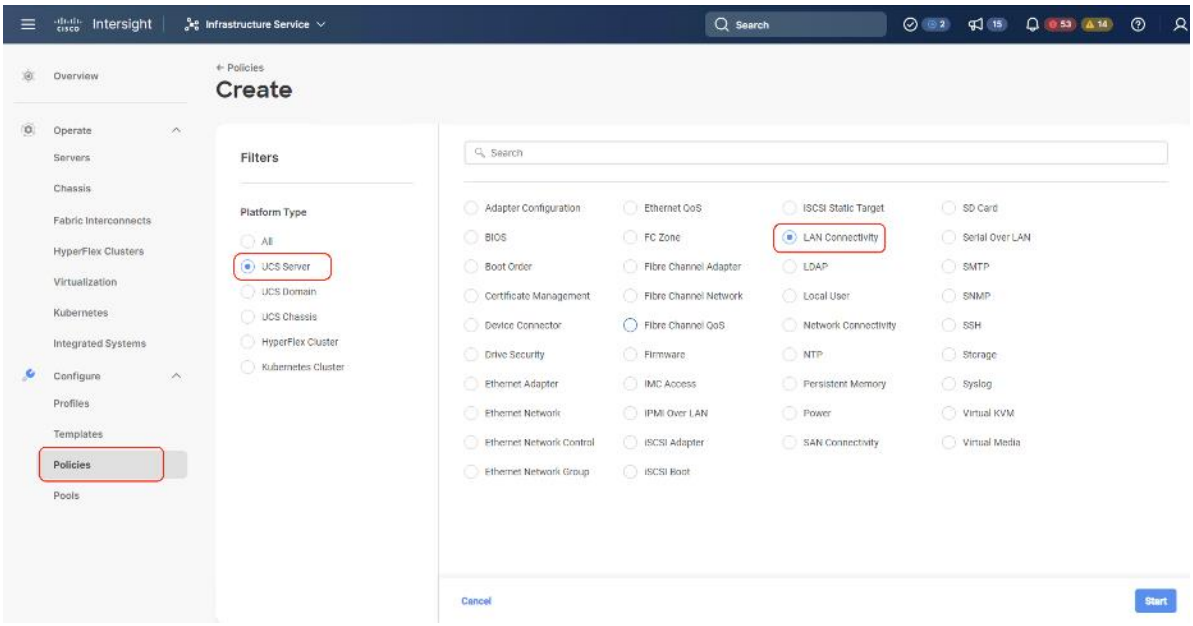
Note: The primary network VLAN for Cohesity should be marked as native or the primary network VLAN should be tagged at the uplink switch.

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.

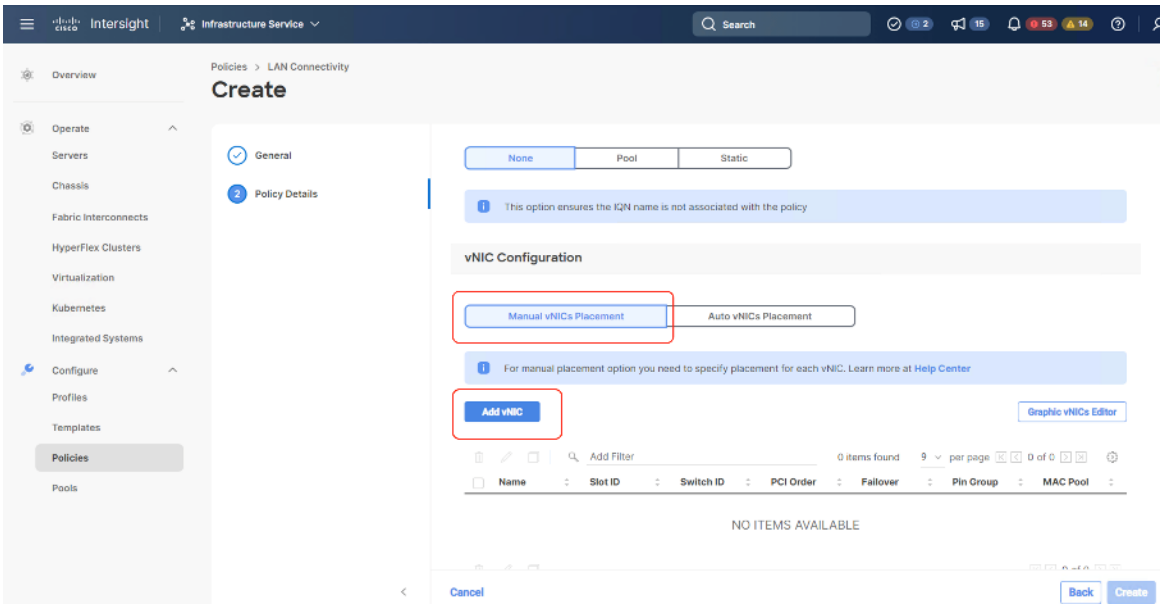
Step 1. Click Infrastructure Service, select Policies, and click Create Policy.

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



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

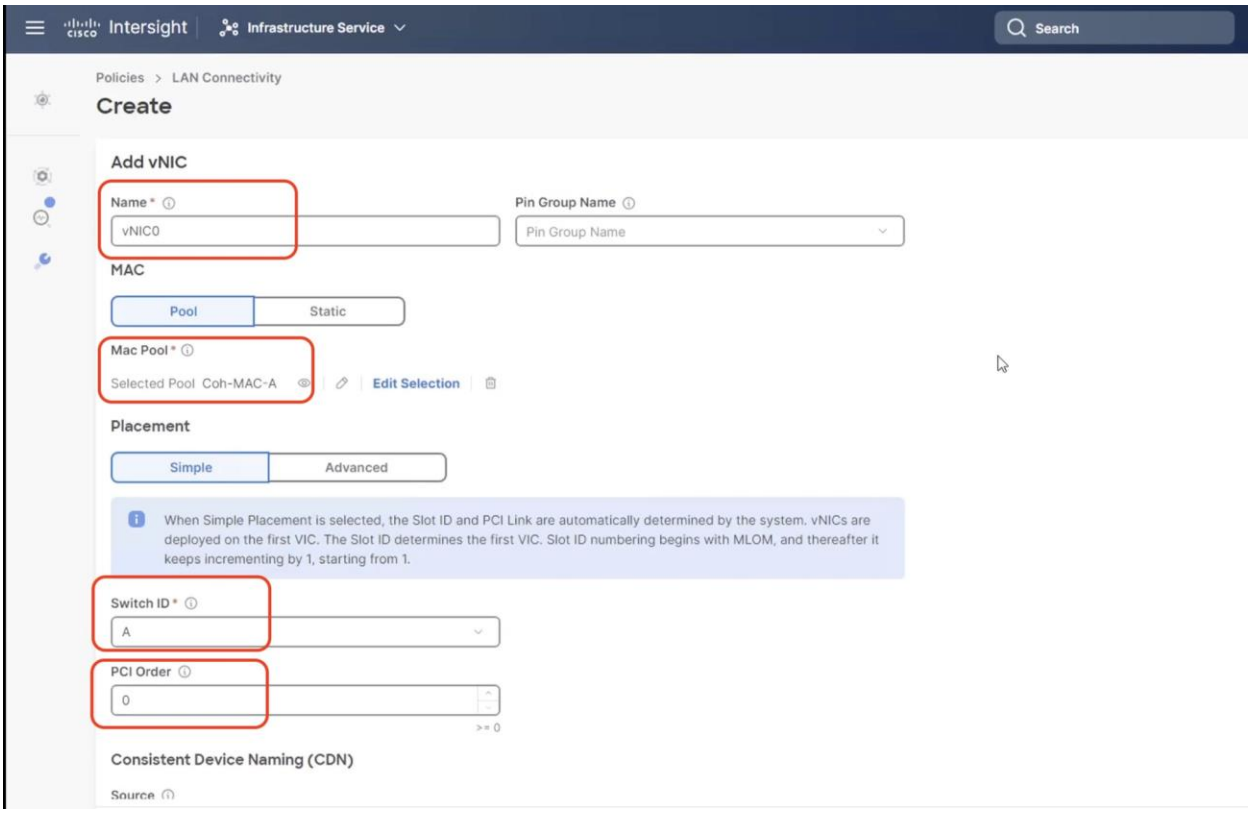
Step 4. Click Add vNIC.



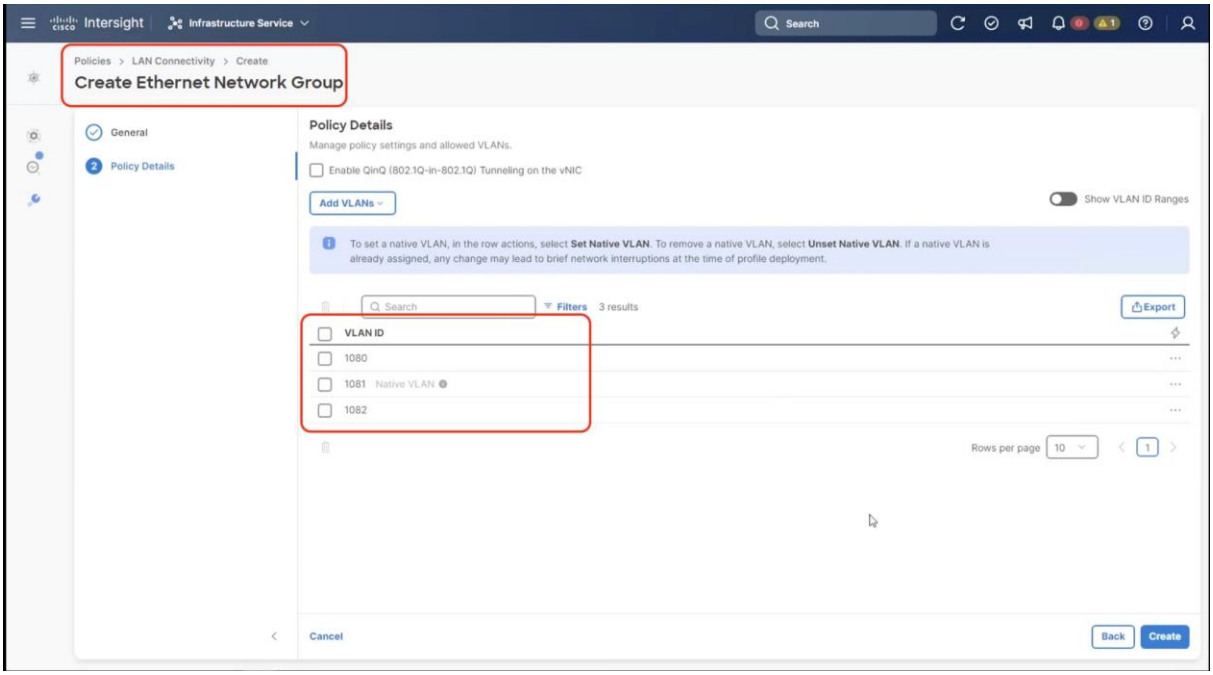
Step 5. Name the vNIC “vNIC0.”

Step 6. For the for vNIC Placement, select Advanced.

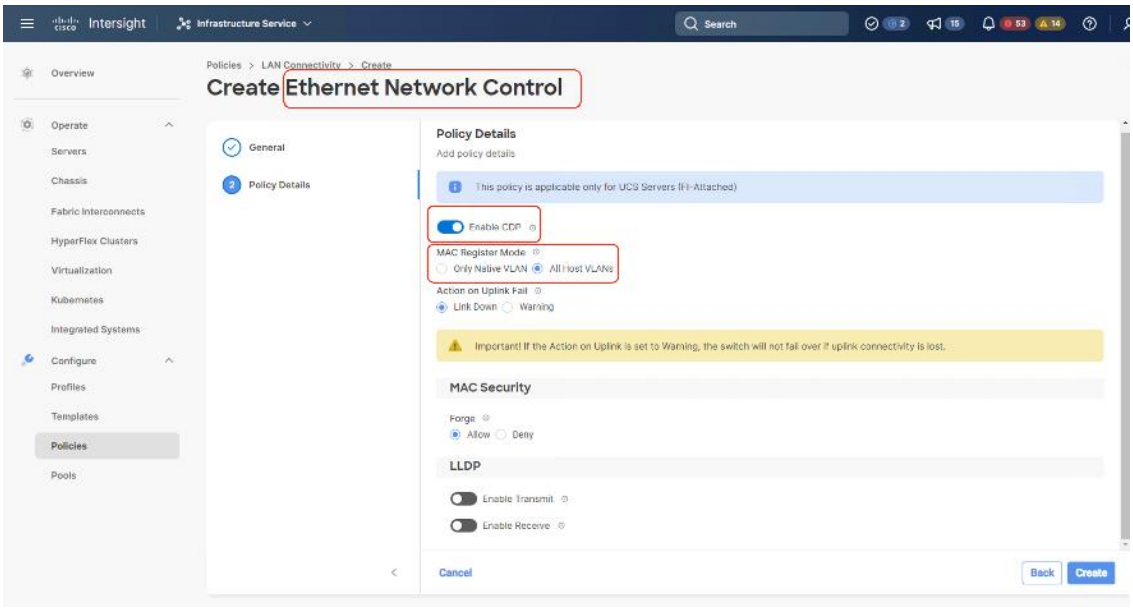
Step 7. Select MAC Pool A previously created, Switch ID A, PCI Order 0.



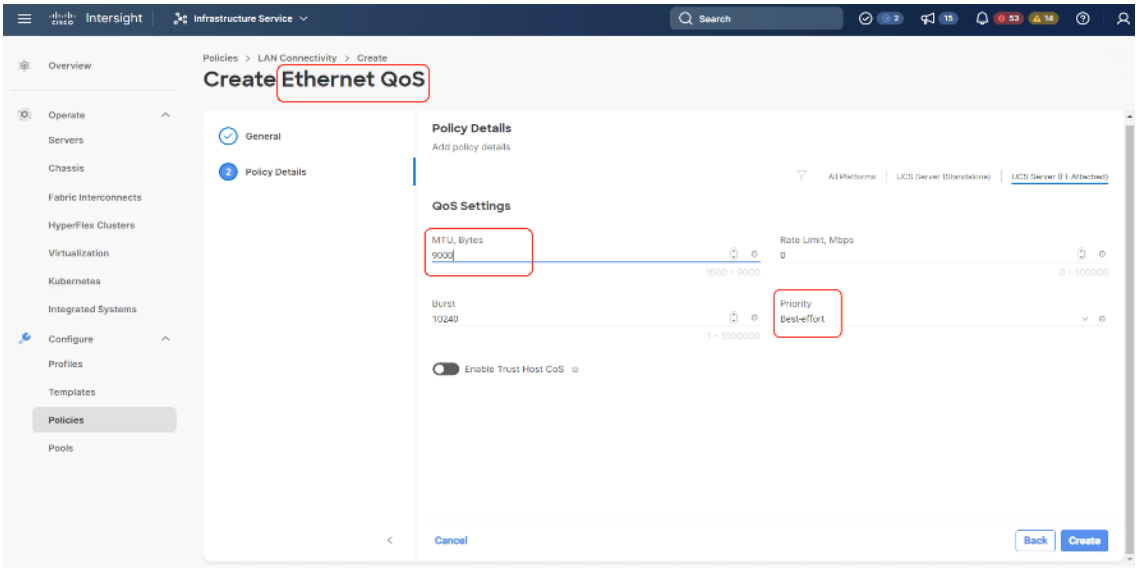
Step 8. Create the Ethernet Network Group Policy; add the allowed VLANs and add the native VLAN. The primary network VLAN for Cohesity should be marked as native or the primary network VLAN should be tagged at the uplink switch.



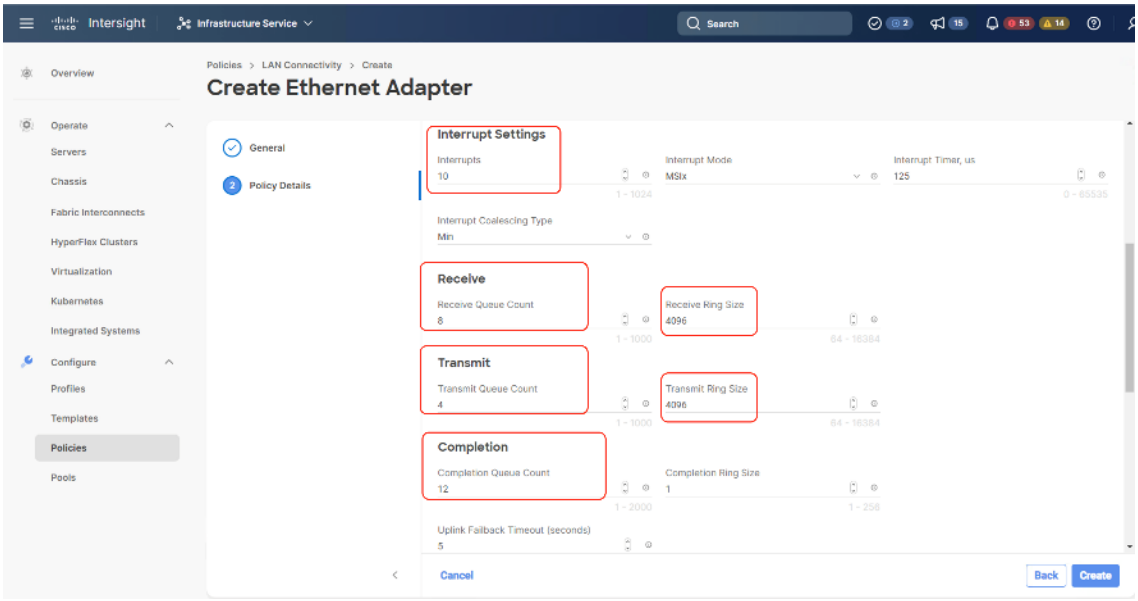
Step 9. Create the Ethernet Network Control policy; name the policy, enable CDP, set MAC Register Mode as All Host VLANs, and keep the other settings as default.



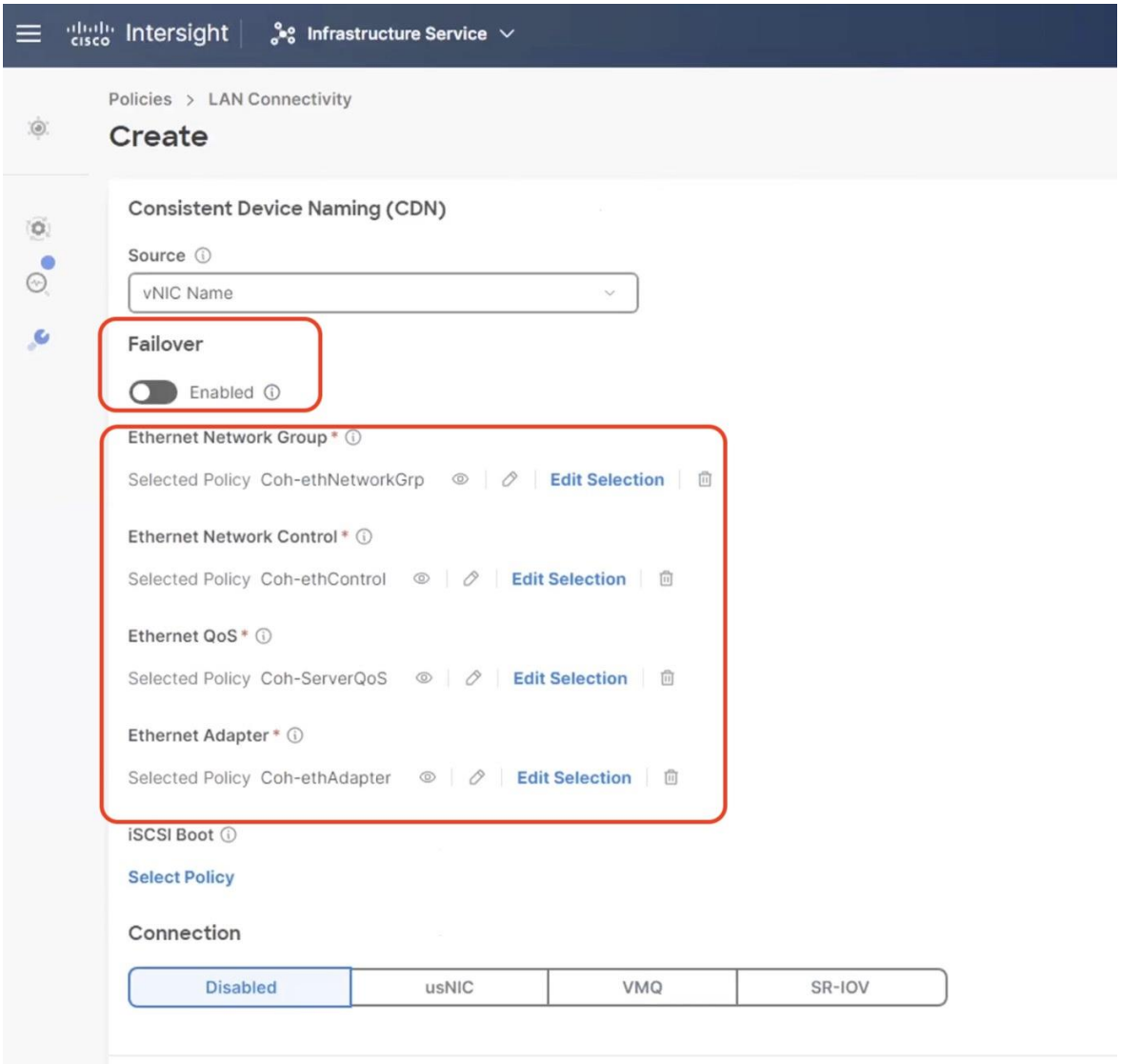
Step 10. Create the Ethernet QoS Policy; edit the MTU to 9000 and keep the Priority as best-effort.

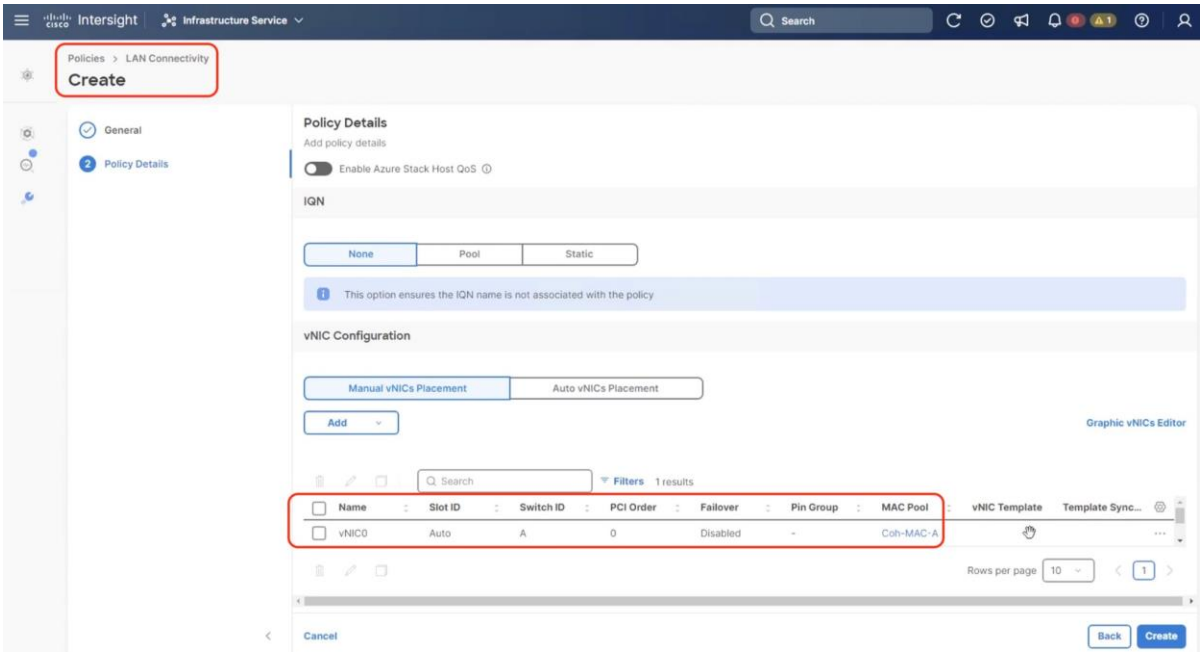


Step 11. Create the Ethernet Adaptor Policy; select UCS Server (FI-Attached), Interrupts=10, Receive Queue Count = 8 Receive Ring Size =4096, Transmit Queue Count = 4, Transmit Ring Size = 4096, Completion Queue = 12, keep the others as default, ensure Receive Side Scaling is enabled.



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



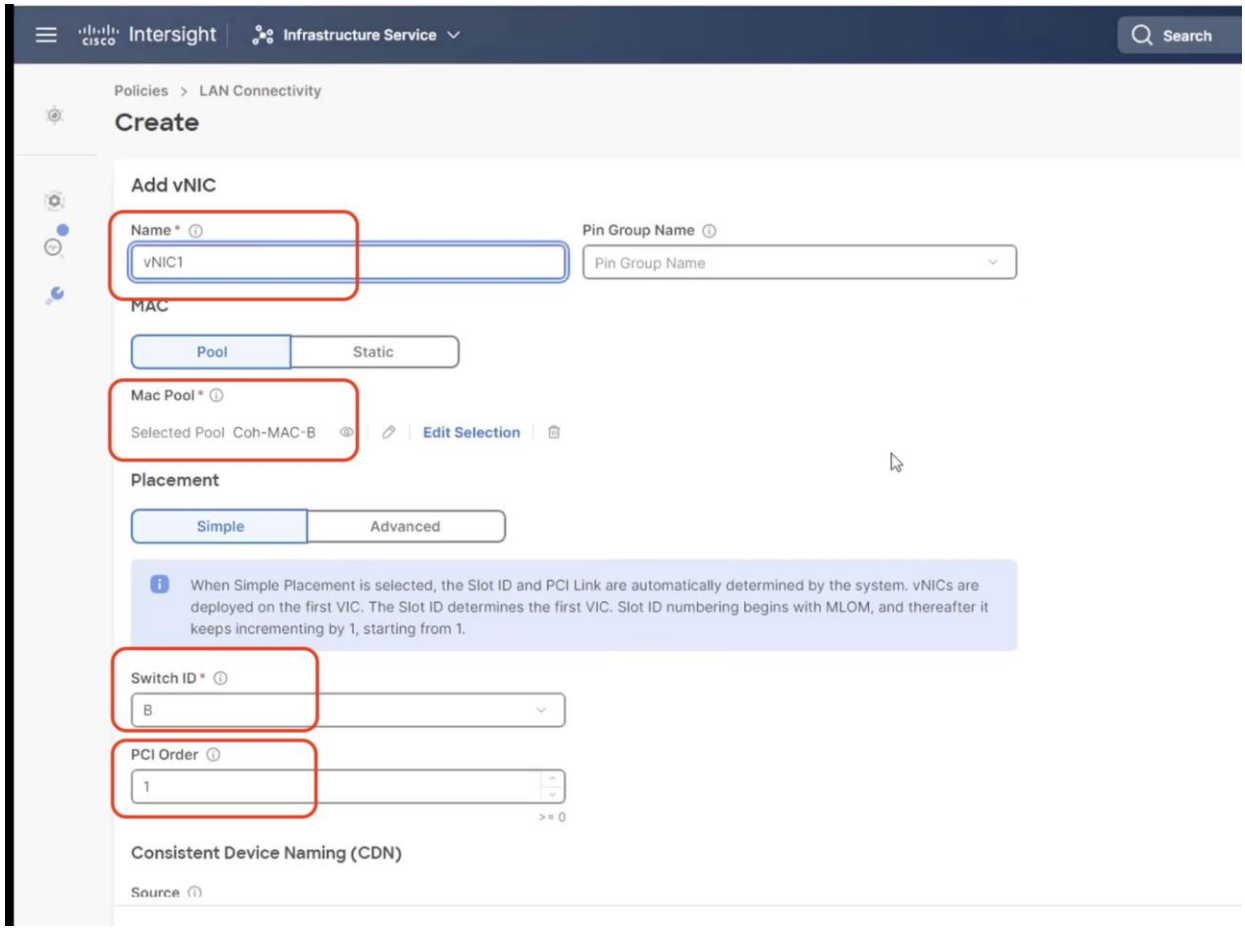


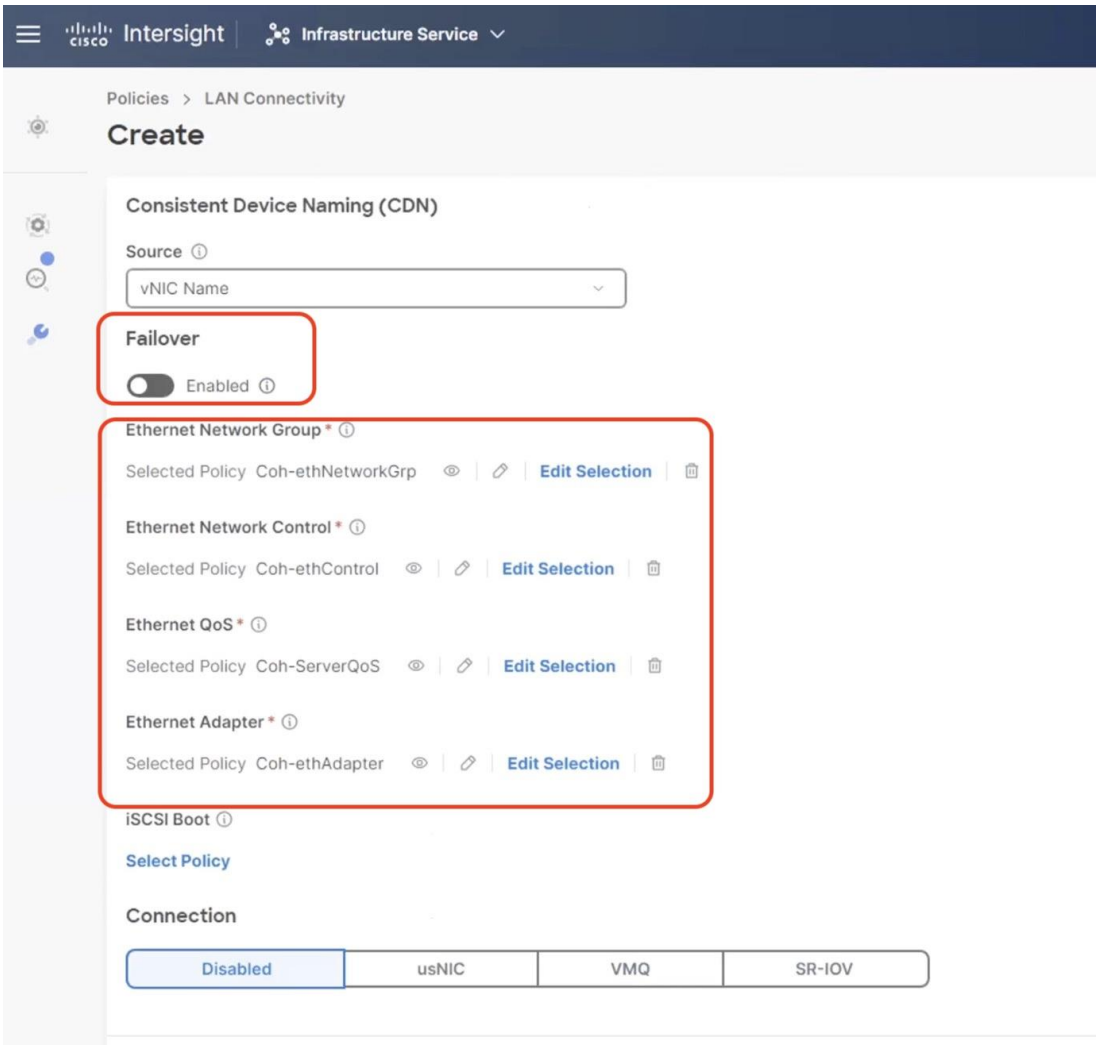
Step 13. Add vNIC as vNIC1. Select the same setting as vNIC0, the only changes shown below.

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

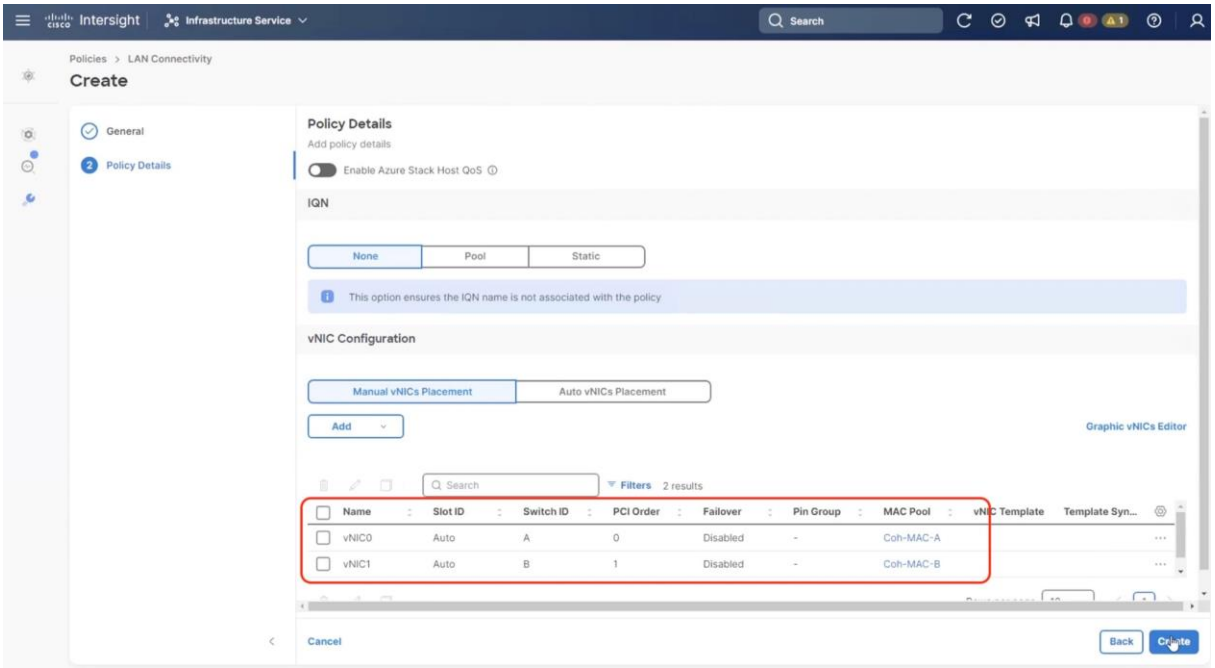
Step 15. Optional. The MAC Pool can be selected as the MAC Pool for Fabric B.

Step 16. Select the Ethernet Network Group Policy, Ethernet Network Control Policy, Ethernet QoS, and Ethernet Adapter policy as created for vNIC0 and click Add.





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



Create Server Profile Template

Procedure 1. Create Server Profile Template

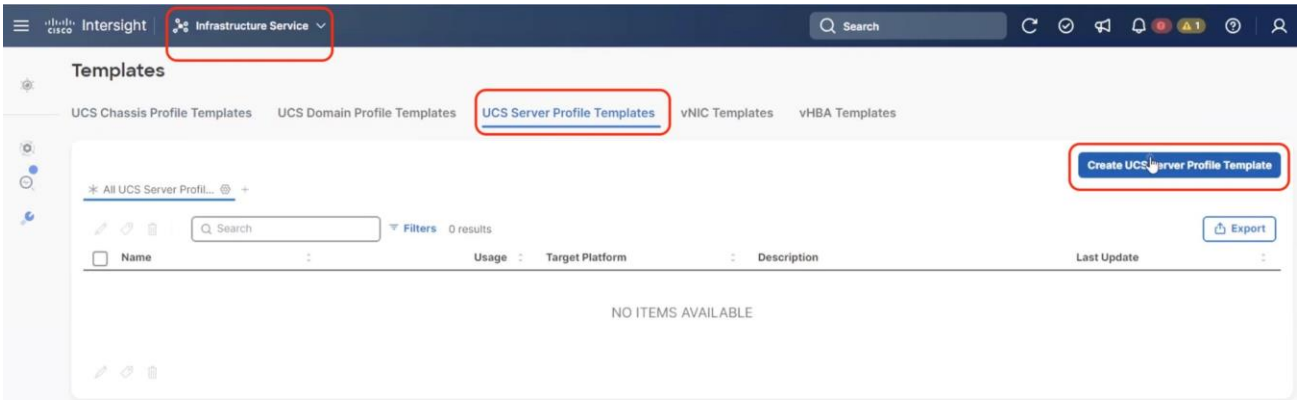
A server profile template enables resource management by simplifying policy alignment and server configuration. All the policies created in previous section would be attached to Server Profile Template. You can derive Server Profiles from templates and attach to Cisco UCS C-Series nodes for Cohesity.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

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

Table 15. Policies required for Server profile template

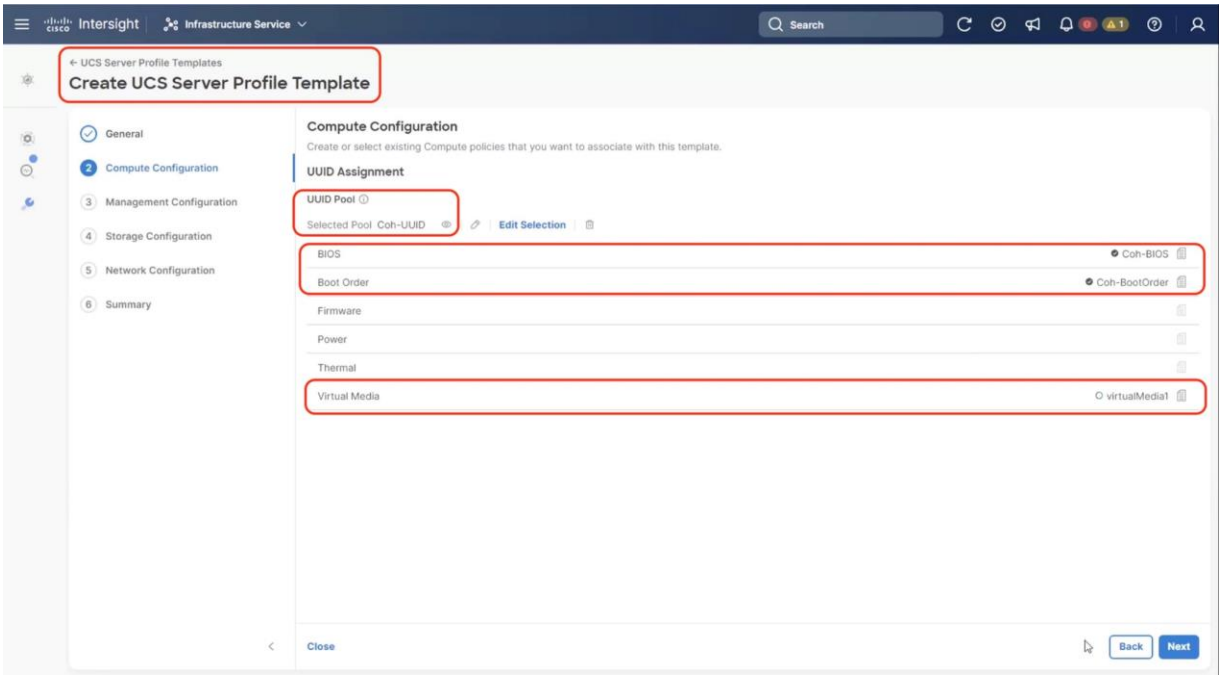
Pools	Compute Policies	Network Policies	Management Policies
KVM Management IP Pool for In-Band and Out-of-Band (OOB) Access	BIOS Policy	LAN Connectivity Policy	IMC Access Policy
MAC Pool for Fabric A/B	Boot Order Policy	Ethernet Network Group Policy	IPMI Over LAN Policy
UUID Pool	Virtual Media	Ethernet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

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

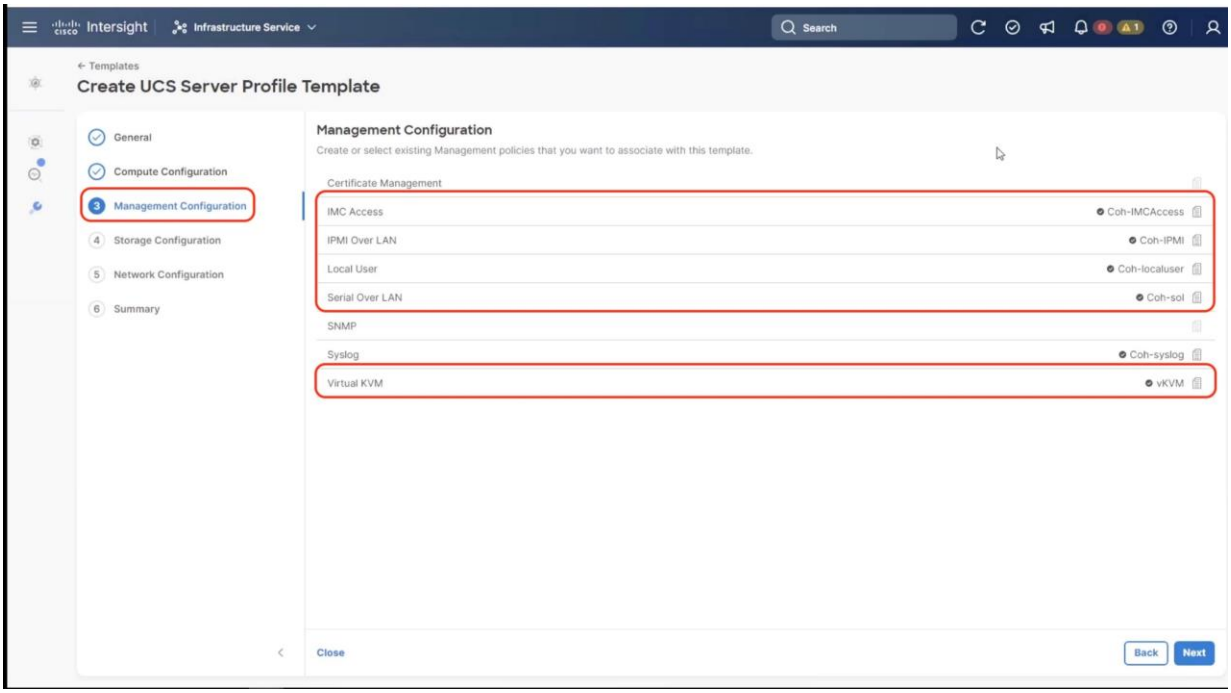


Step 2. Name the Server Profile Template, select UCS Sever (FI-Attached) and click Next.

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

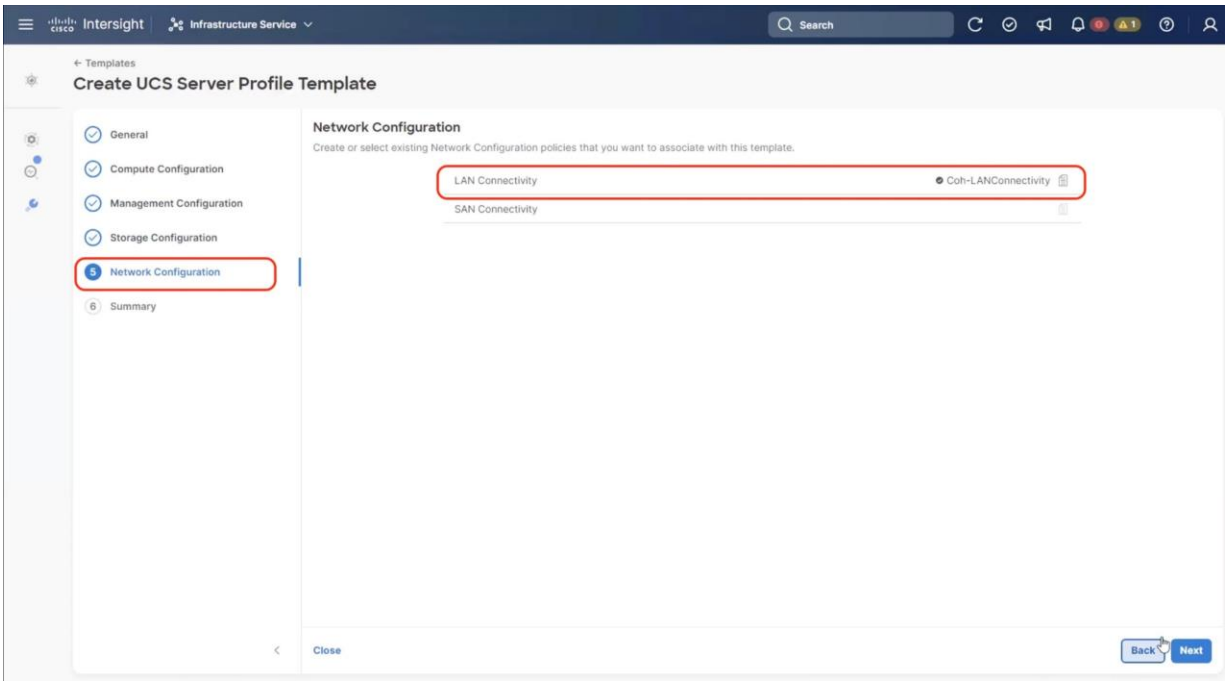


Step 4. Select all Management Configuration Policies and attach to the Server Profile Template.

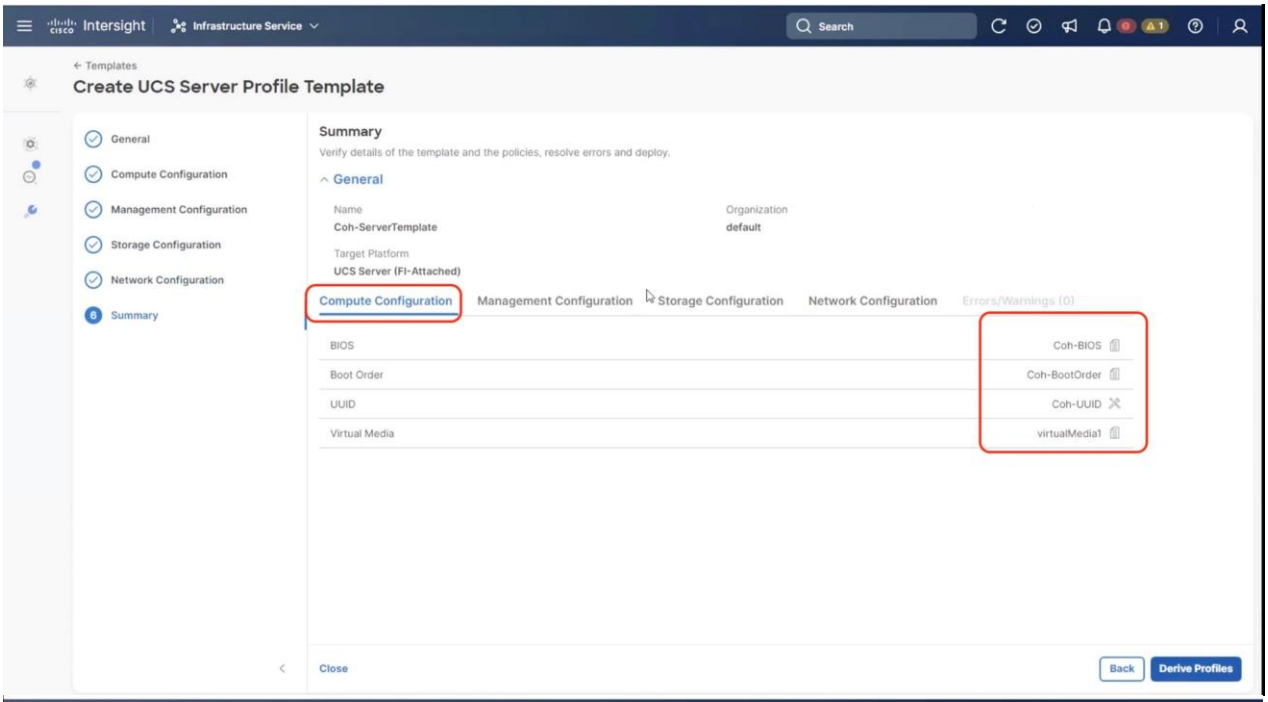


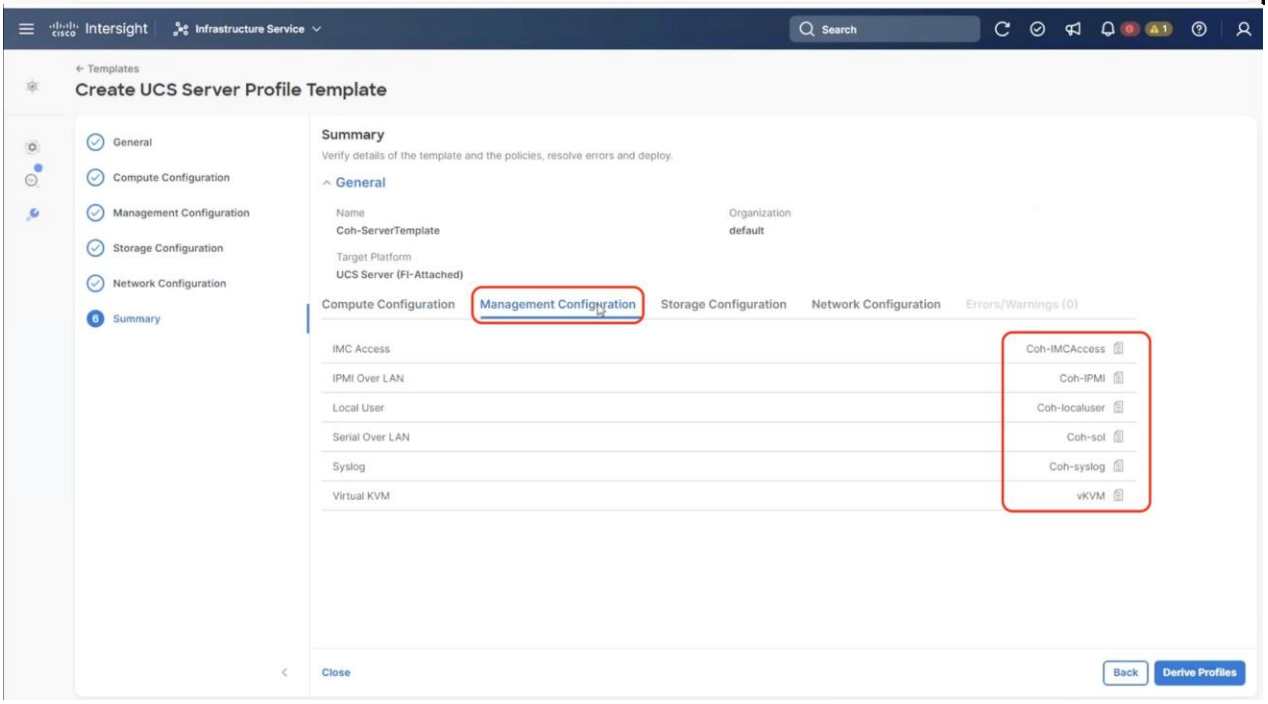
Step 5. Skip Storage Polices and click Next.

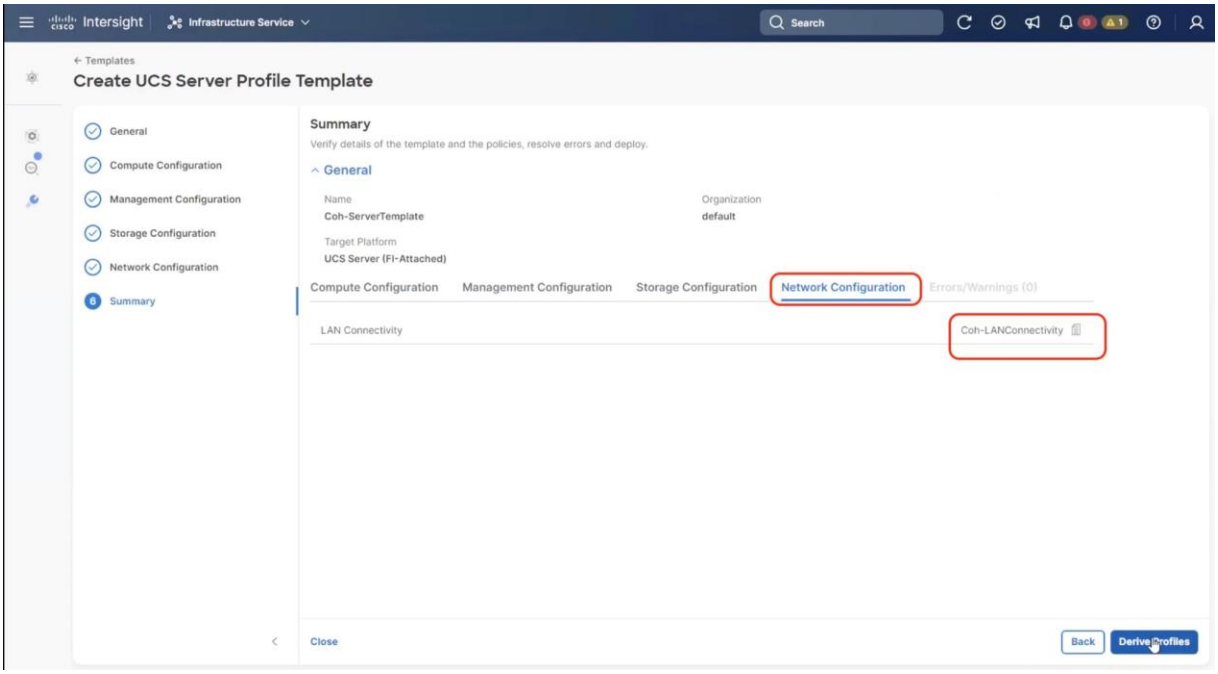
Step 6. Under Network Configuration, select the LAN connectivity Policy created in the previous section and click Next.



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.







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.

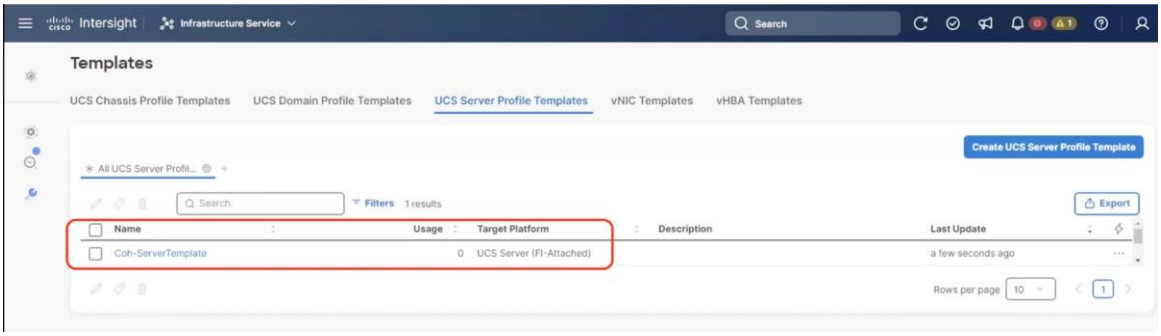
Derive and Deploy Server Profiles

Procedure 1. Derive and Deploy Server Profiles

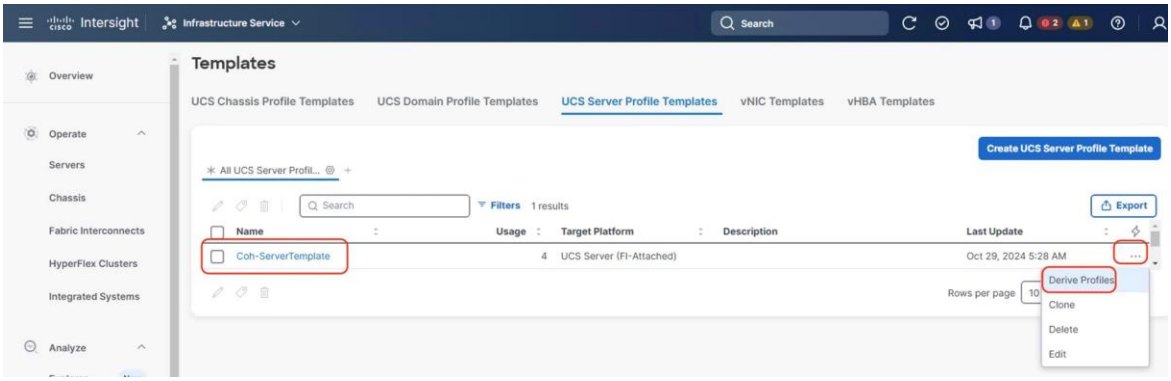
In this procedure, Server Profiles are derived from Server Profile Template and deployed on Cisco UCS C-Series nodes certified for the Cohesity Data Cloud.

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.

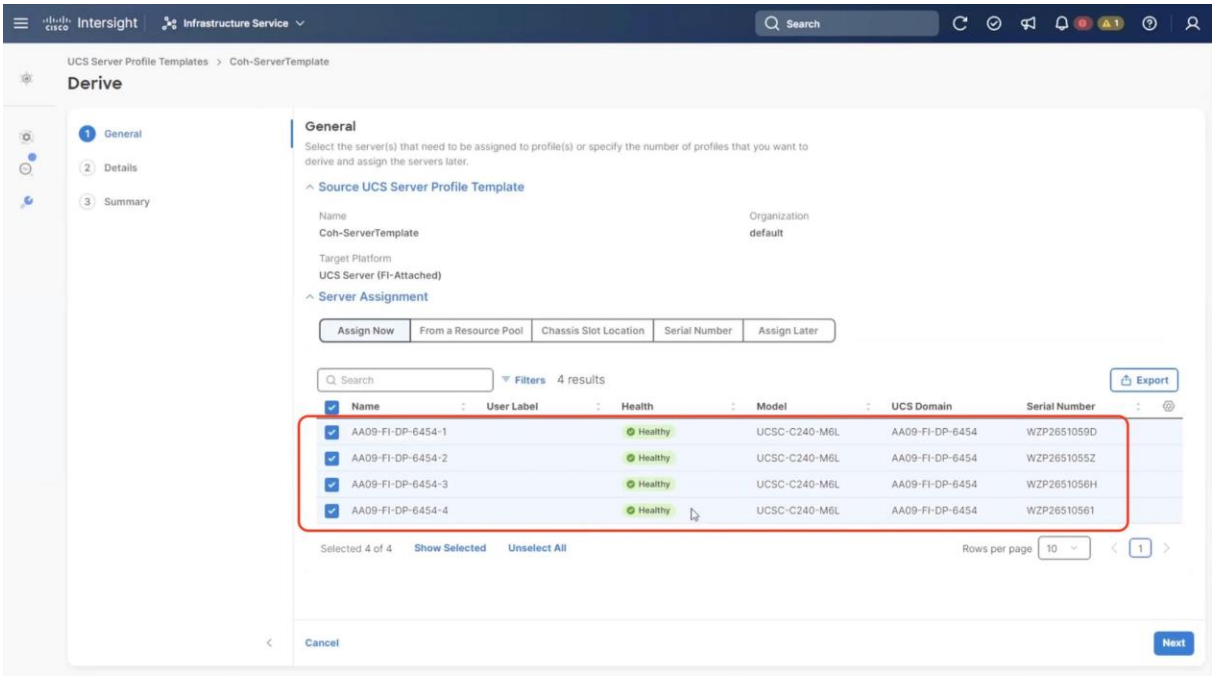
Step 1. Select Infrastructure Service, then select Templates and identify the Server Template created in the previous section.



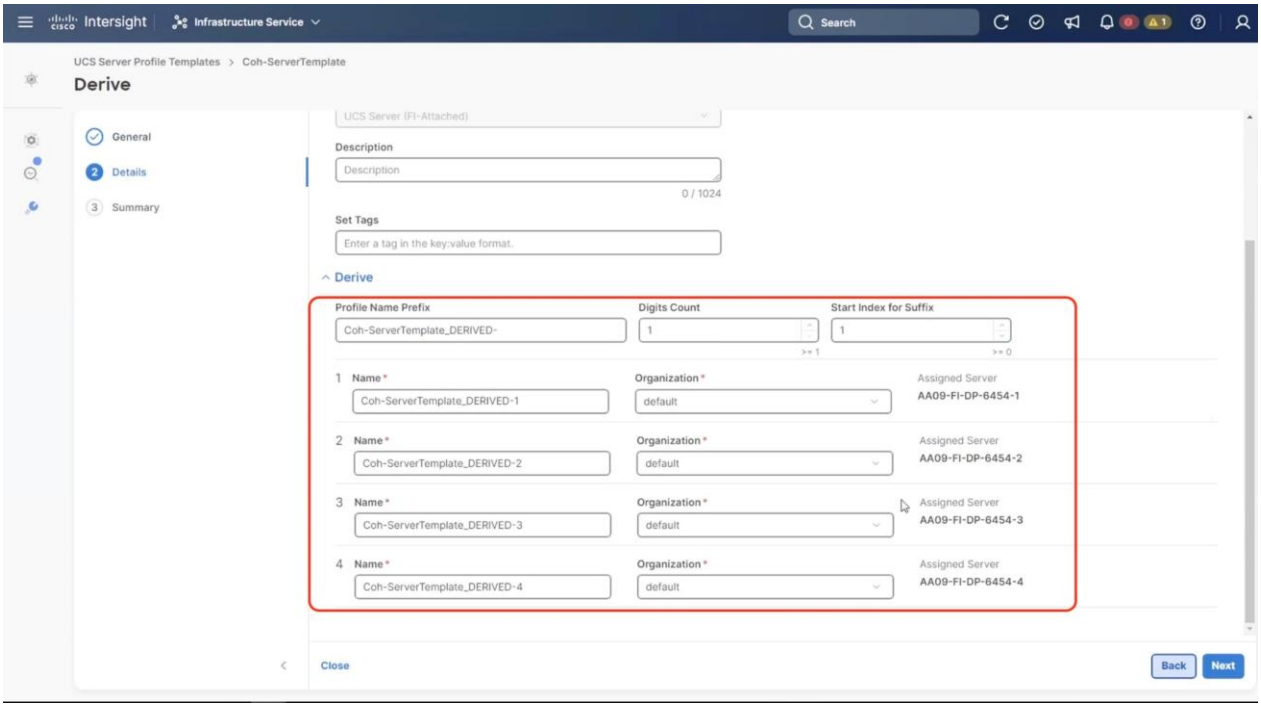
Step 2. Click the ... icon and select Derive Profiles.



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

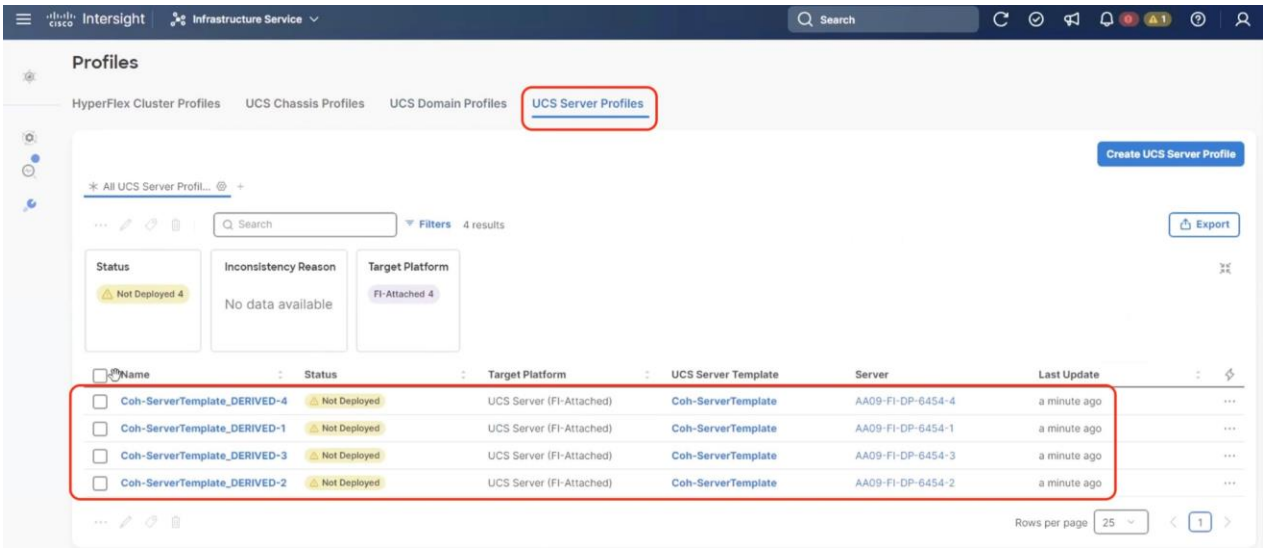


Step 4. Select organization (default in this deployment), edit the name of Profiles if required and click Next.

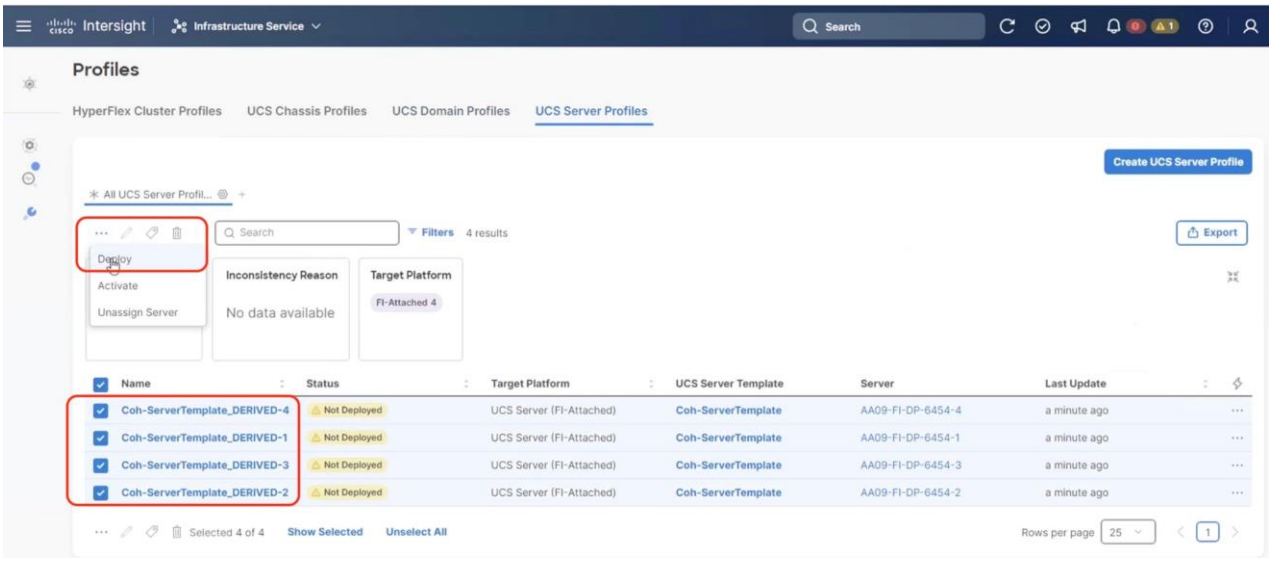


Step 5. All Server policies attached to the template will be attached to the derived Server Profiles. Click Derive.

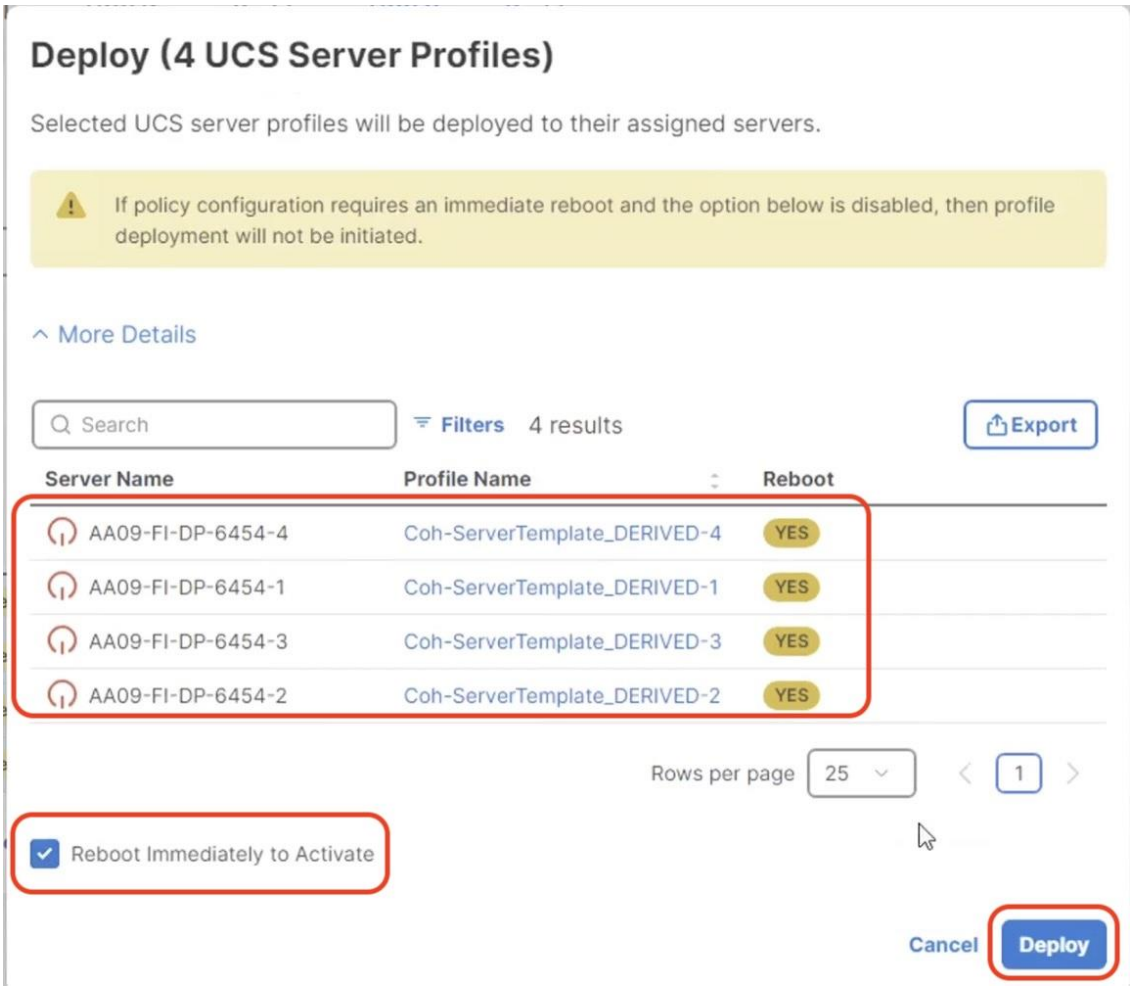
Step 6. The Server Profiles will be validated and ready to be deployed to the Cisco UCS C-Series nodes. A "Not Deployed" icon will be displayed on the derived Server Profiles.



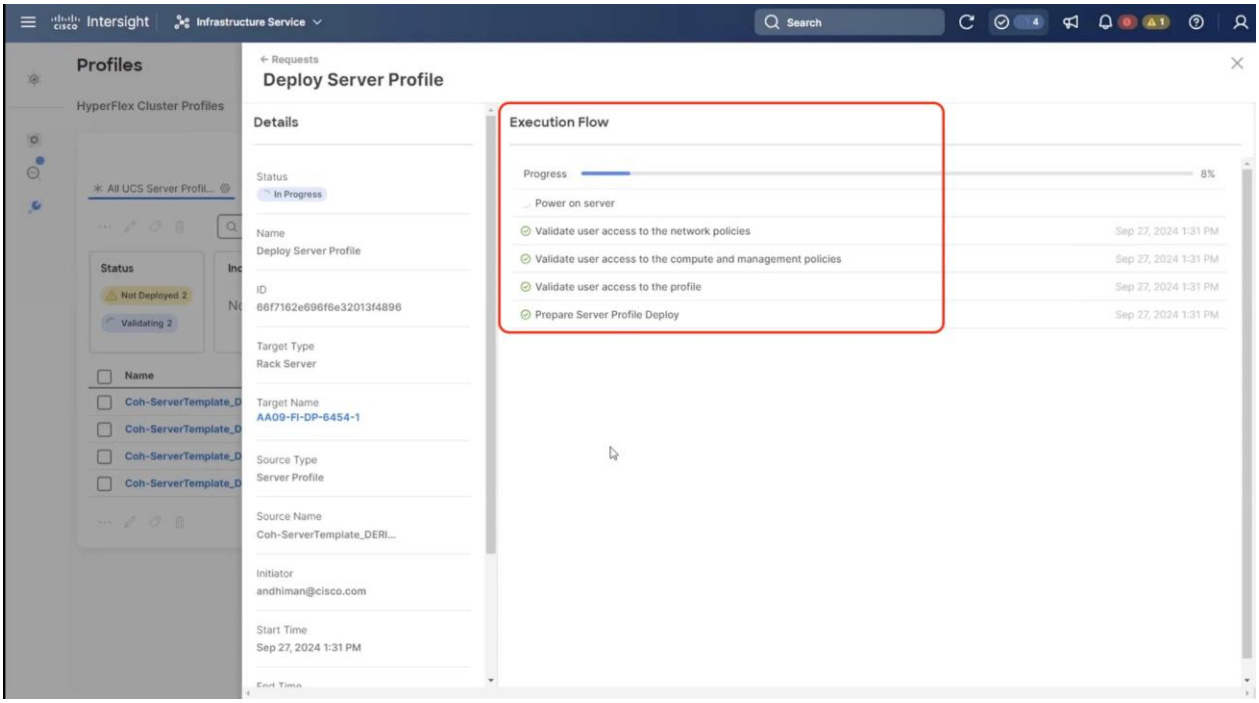
Step 7. Select the Not Deployed Server Profiles, click the ... icon and click Deploy.



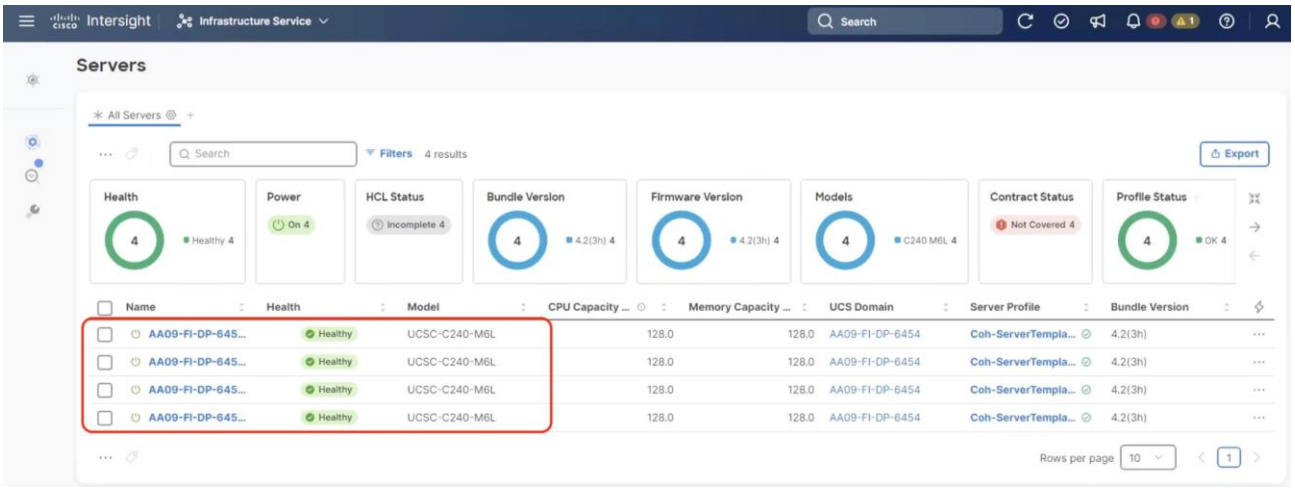
Step 8. Enable Reboot Immediately to Activate and click Deploy.



Step 9. Monitor the Server Profile deployment status and ensure the Profile deploys successfully to the Cisco UCS C-Series node.



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



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

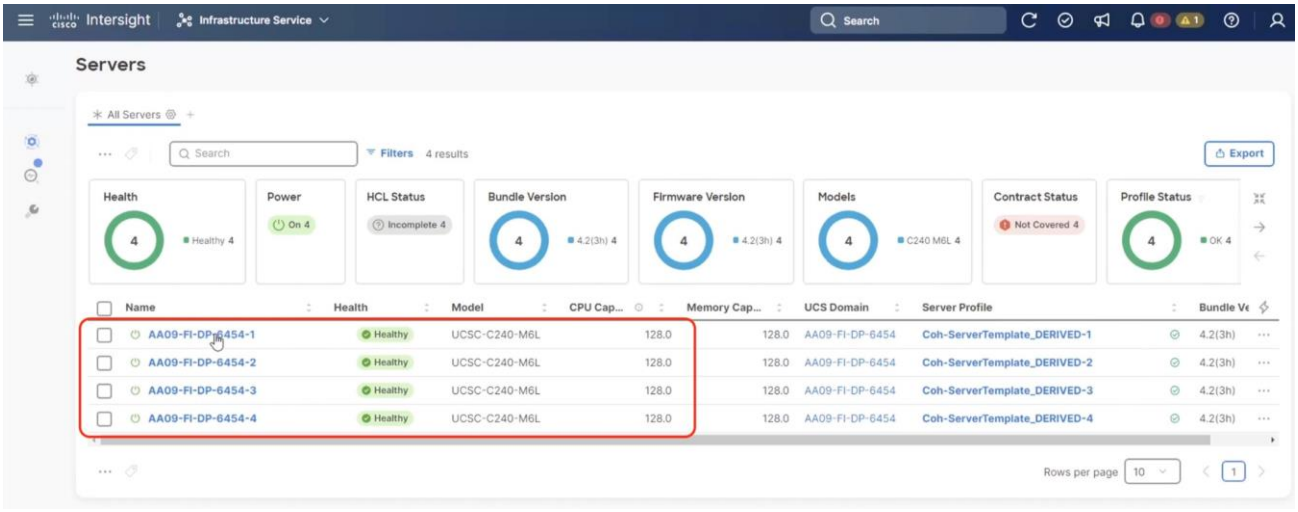
Prior to installing Cohesity OS, it is highly recommended to upgrade the Cisco UCS C-Series Firmware to the recommended Cisco UCS C-Series Firmware release. This procedure expands on the process to upgrade the Cisco UCS C-Series node firmware and should be executed only during the following scenarios:

1. During creating of a **new cohesity cluster** with Cisco UCS C-Series nodes.

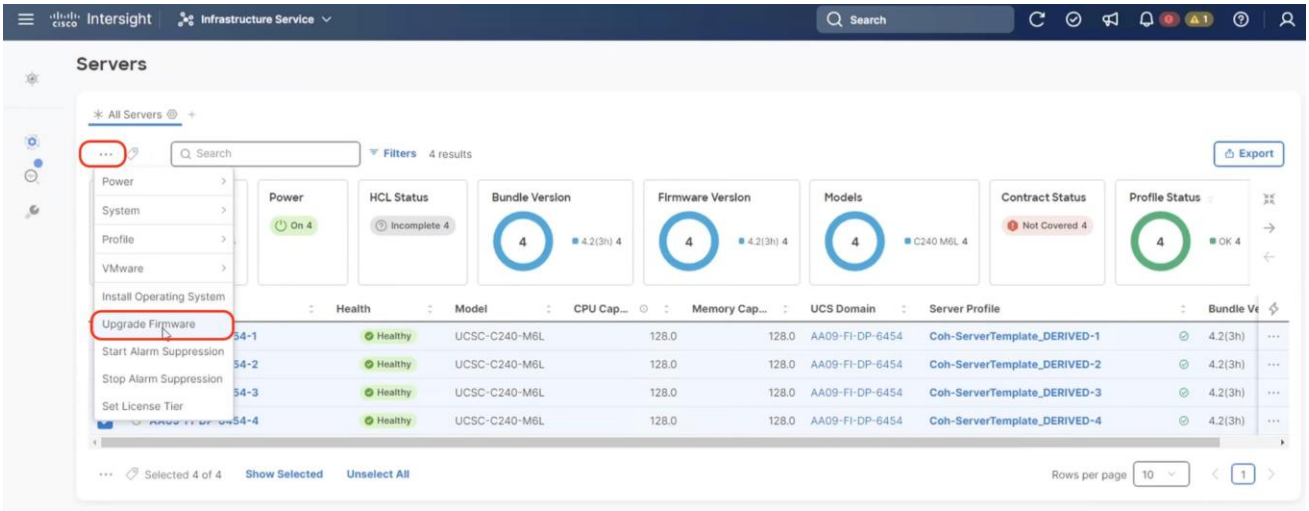
2. **Adding new nodes to cluster**. The firmware should be upgraded to new nodes before installing Cohesity OS.

3. Firmware upgrade of Cisco UCS C-Series nodes during **maintenance window**. This requires shutting down the entire Cohesity cluster.

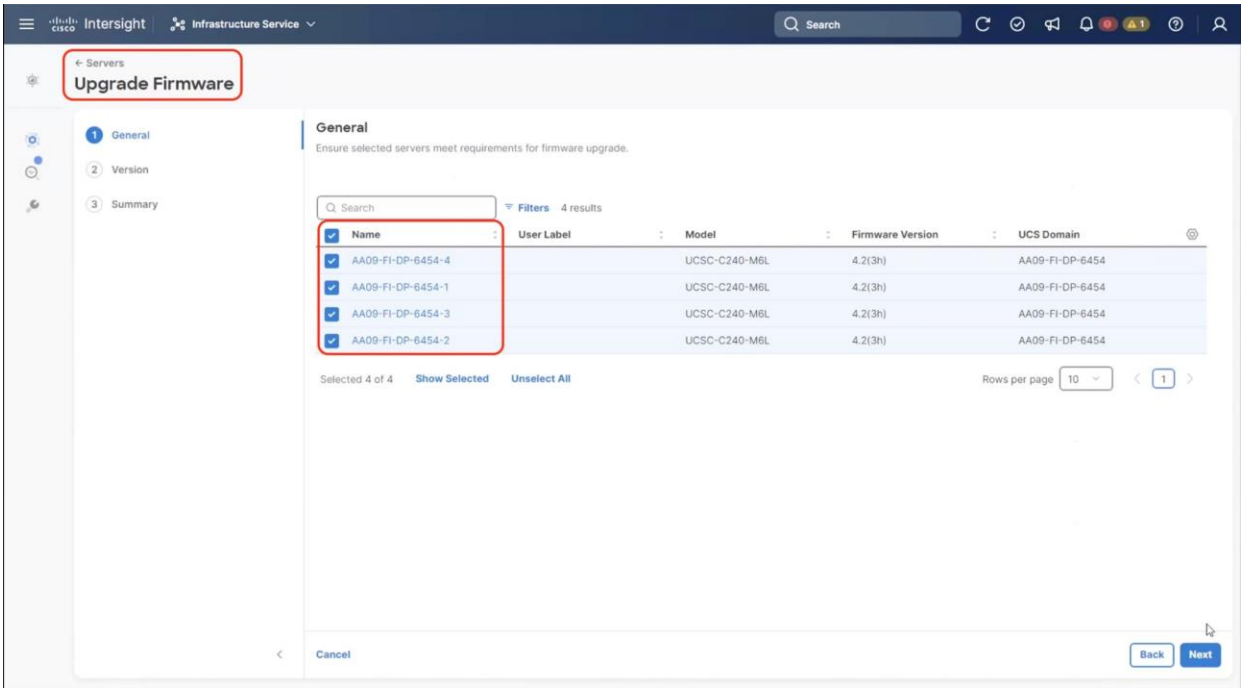
Step 1. Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster. Ensure Server Profile is successfully deployed to the Cohesity nodes



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

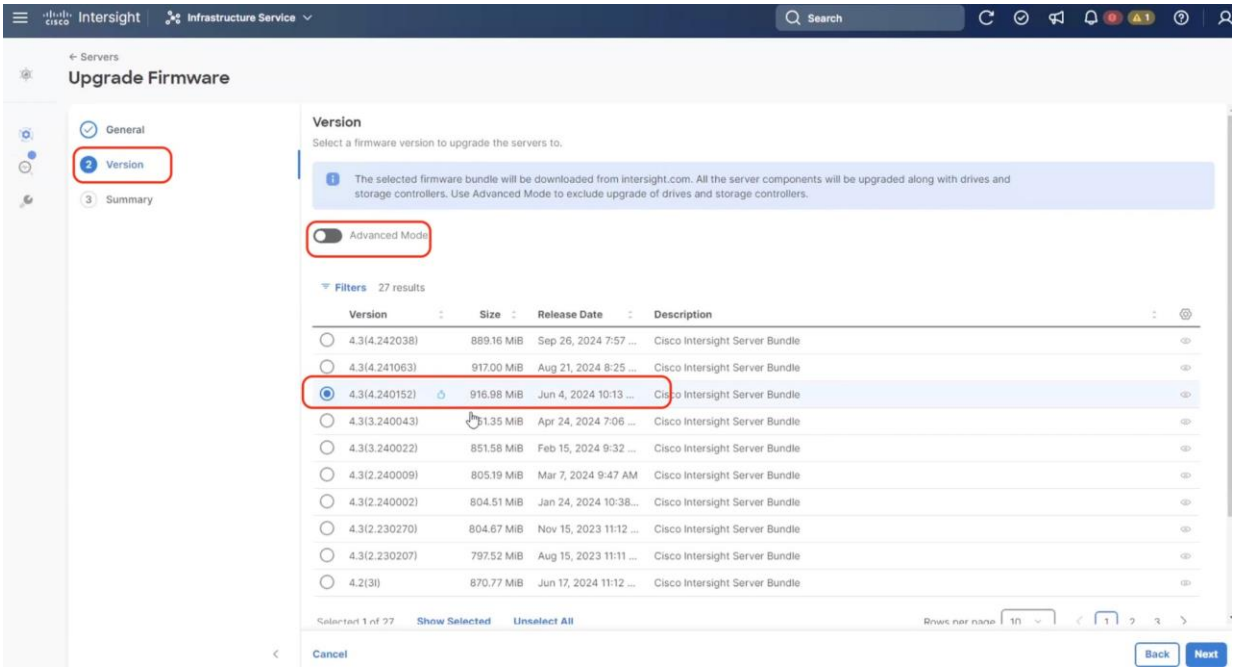


Step 3. Select Start Firmware upgrade and ensure the Cisco UCS C-Series nodes are selected. Click Next.

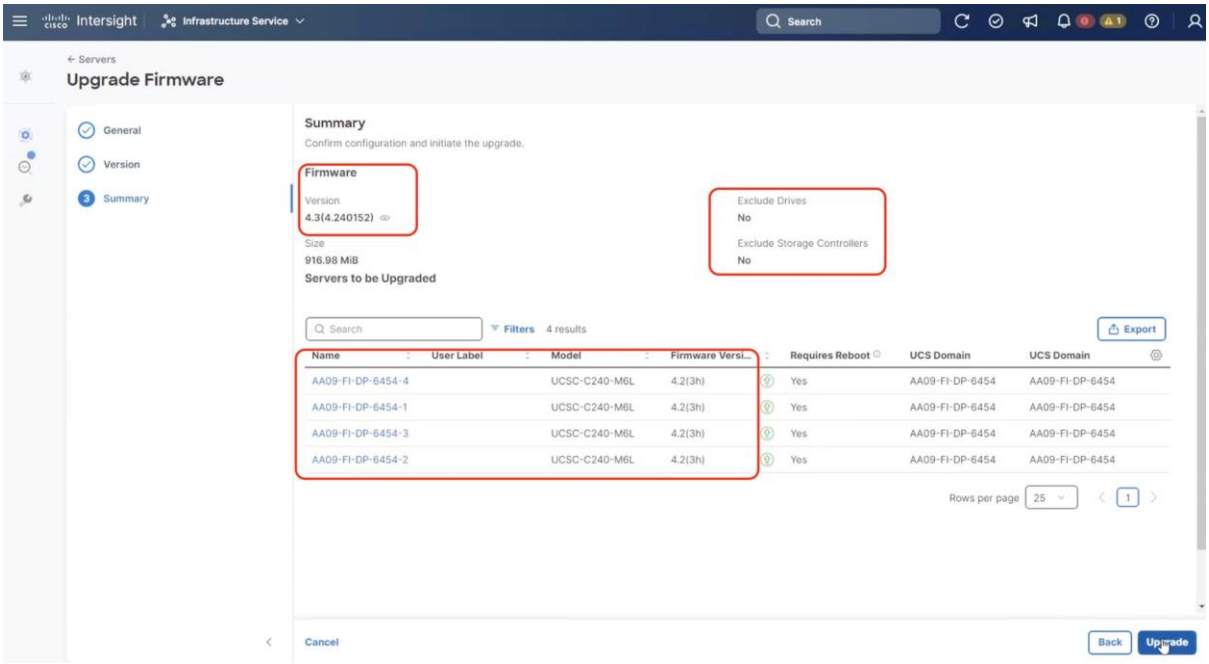


Step 4. Identify the recommended Firmware version. In general, the recommended sign is displayed on the firmware. Click Next.

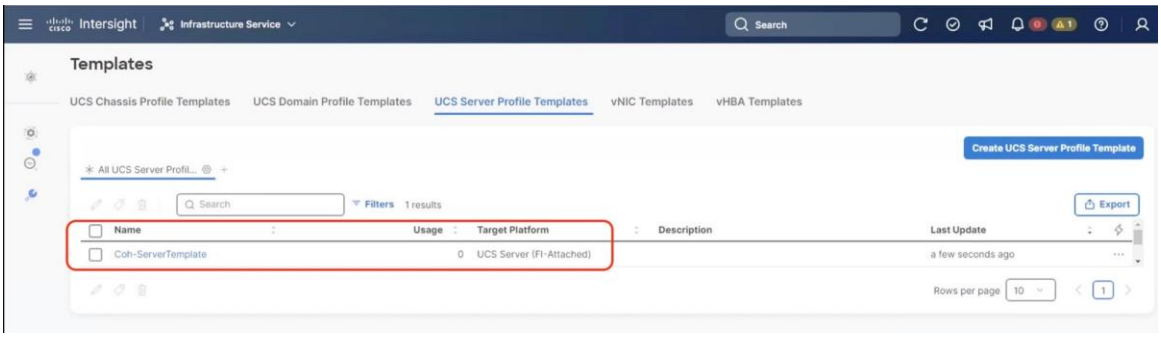
Note: By default the drive and storage controller firmware is also upgraded. To avoid drive failure and improve the resiliency of drives, it is recommended to upgrade drive firmware. Drives can be excluded from firmware upgrades, through 'Advanced Mode'.



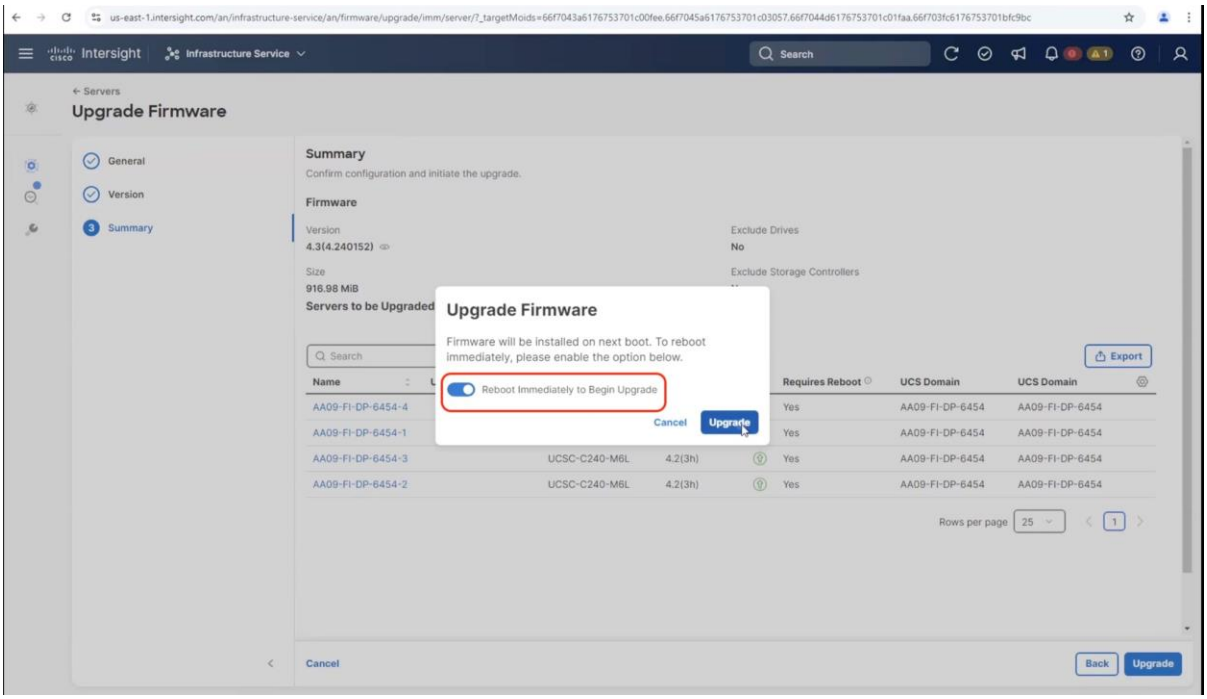
Step 5. Confirm the firmware version for upgrades on Cohesity nodes. Click Upgrade.



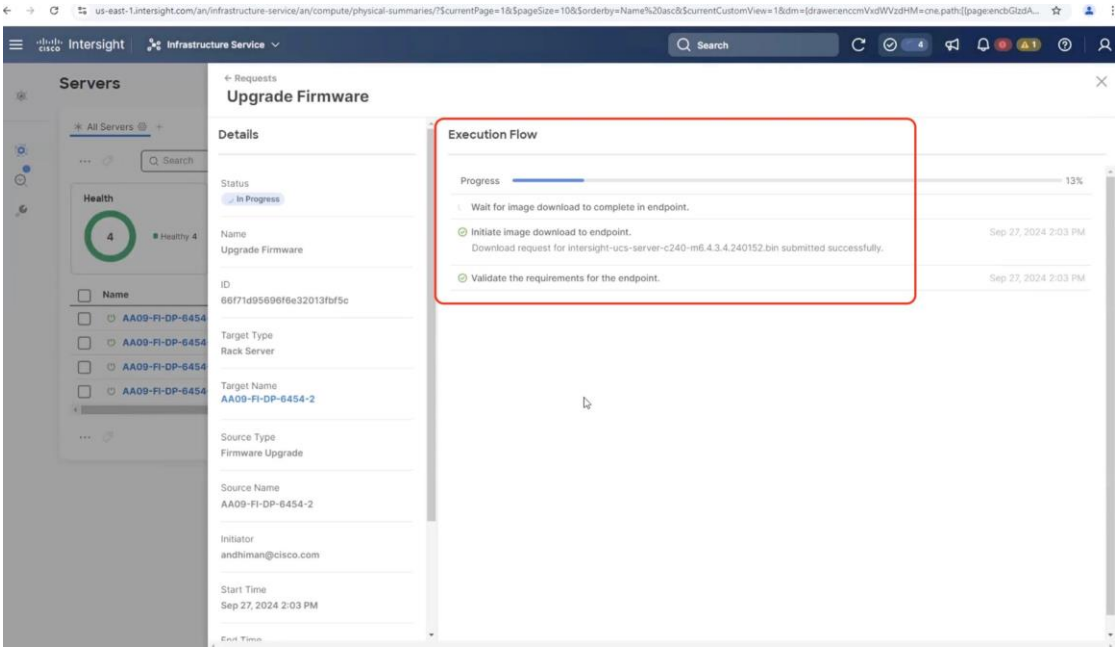
Step 6. On the Upgrade Firmware confirmation screen, enable Reboot Immediately to Begin Upgrade.



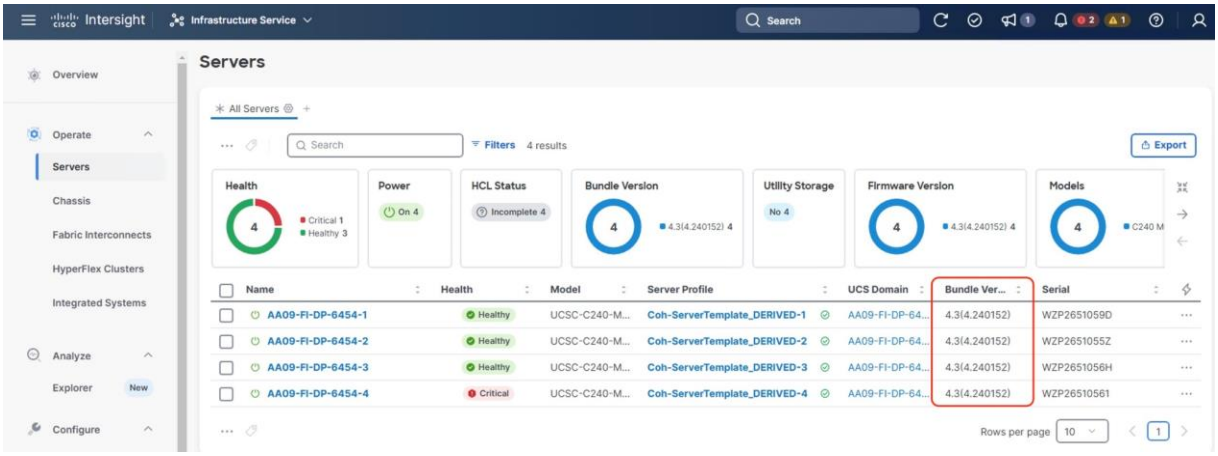
Step 7. Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster.



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



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

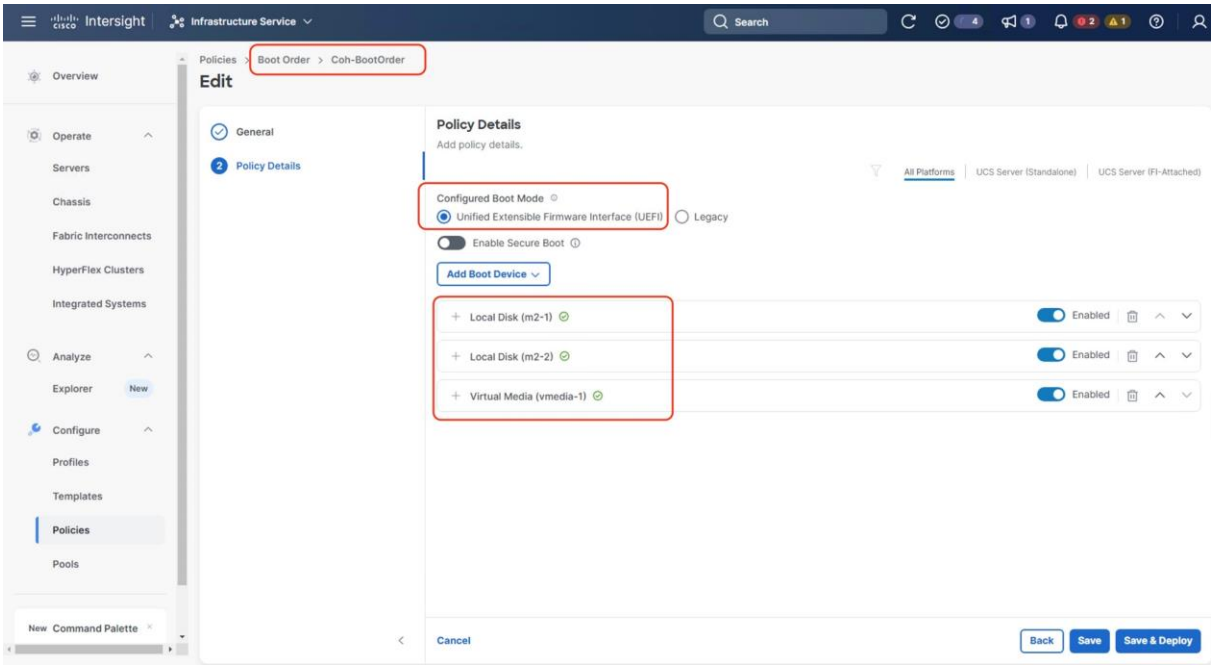


Cohesity OS installation through Cisco Intersight

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:



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

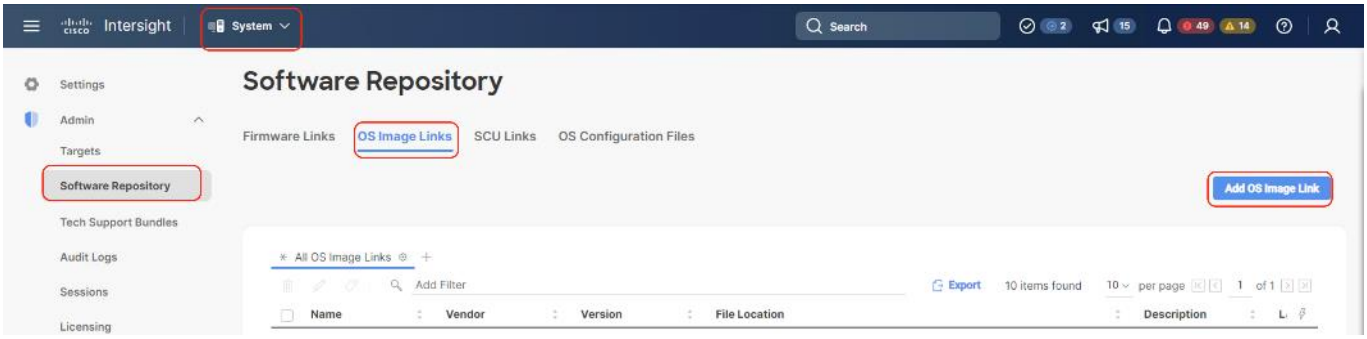
Note: Make sure the certified Cohesity Data Cloud ISO is available from a local repository, for example an HTTPS/NFS/CIFS server. This is a one-time process for each version of the Cohesity Data Cloud ISO.

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

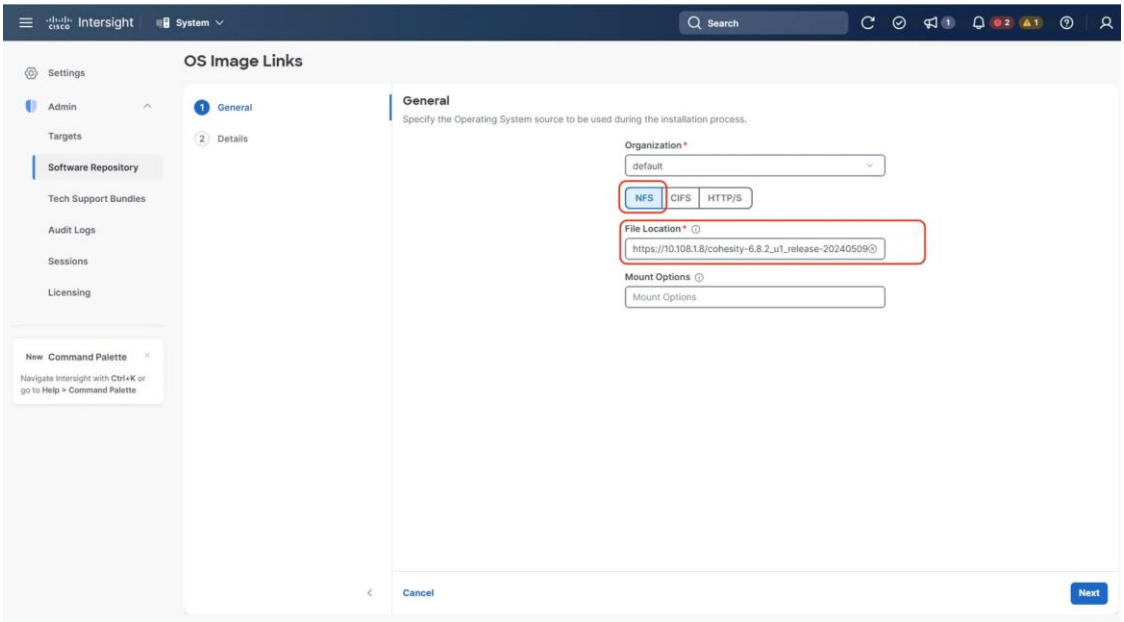
Step 1. Login to Cisco Intersight and click System.

Step 2. Click Software Repository and click the OS Image Links tab.

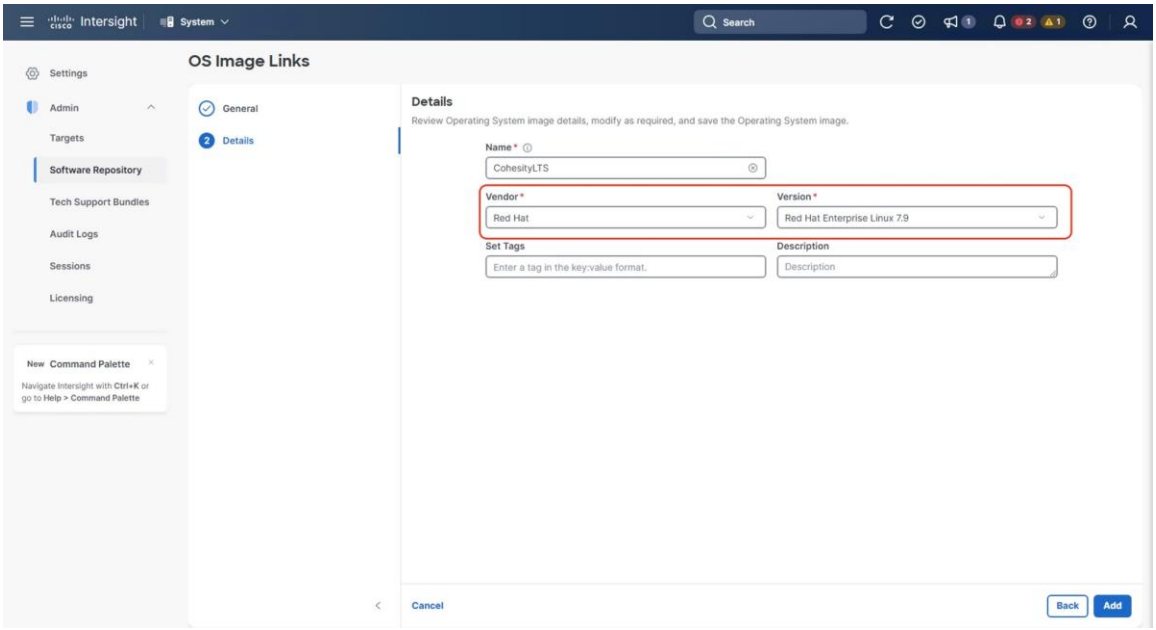
Step 3. Click Add OS Image Link.



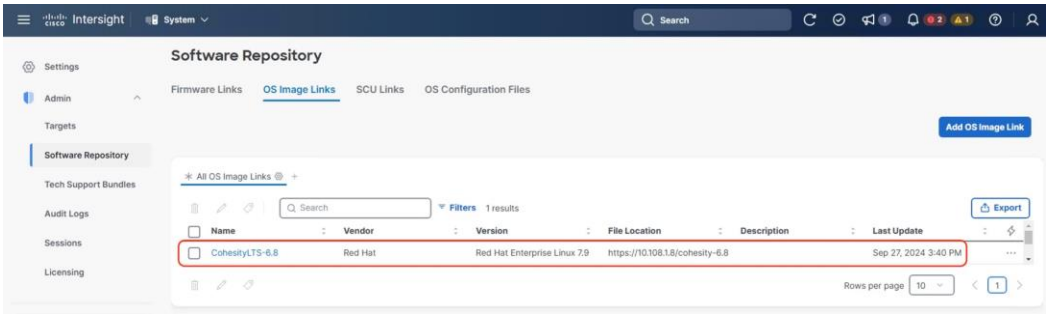
Step 4. Add the location of the Cohesity Data Cloud ISO (NFS/CIFS or HTTPS server) and click Next.



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

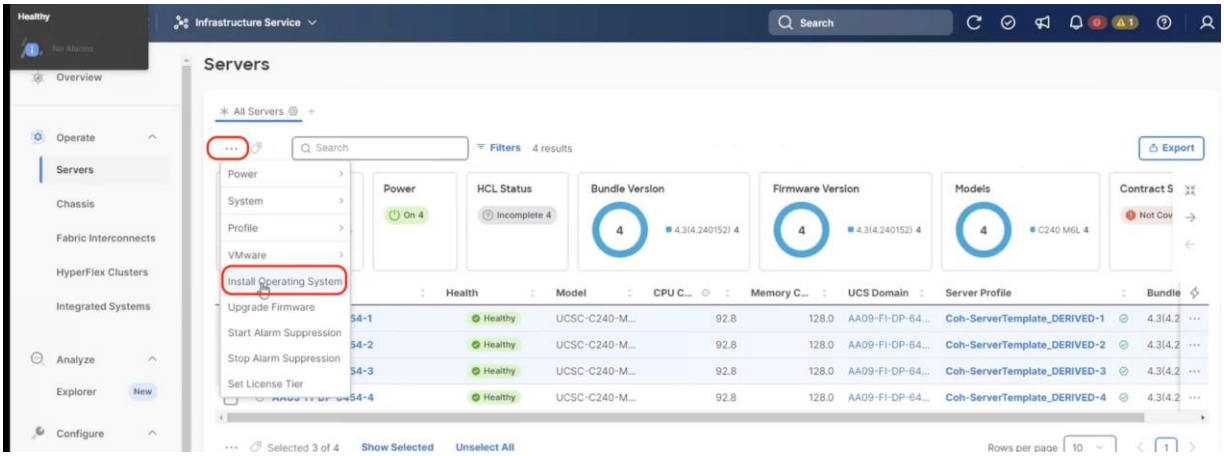


Step 6. Make sure the OS Repository is successfully created in Cisco Intersight.

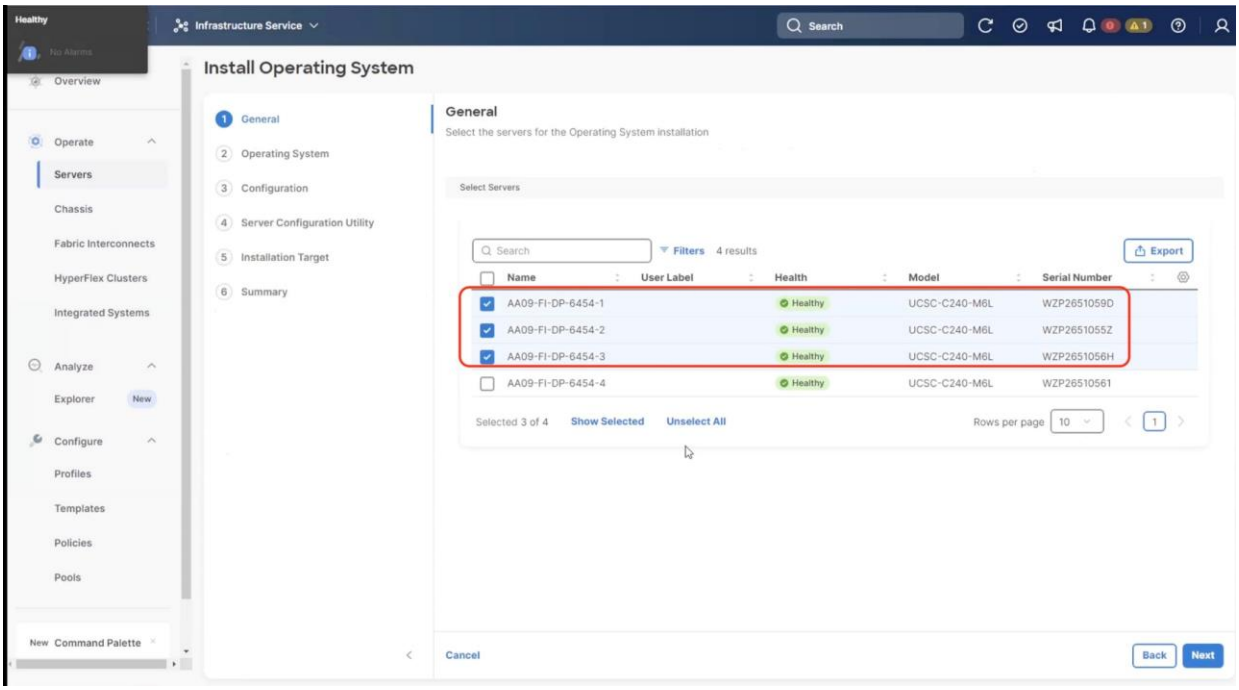


Step 7. From Cisco Intersight, click Infrastructure Service, then click Servers, and select the Cisco UCS C-Series nodes ready for the Cohesity Data Cloud installation.

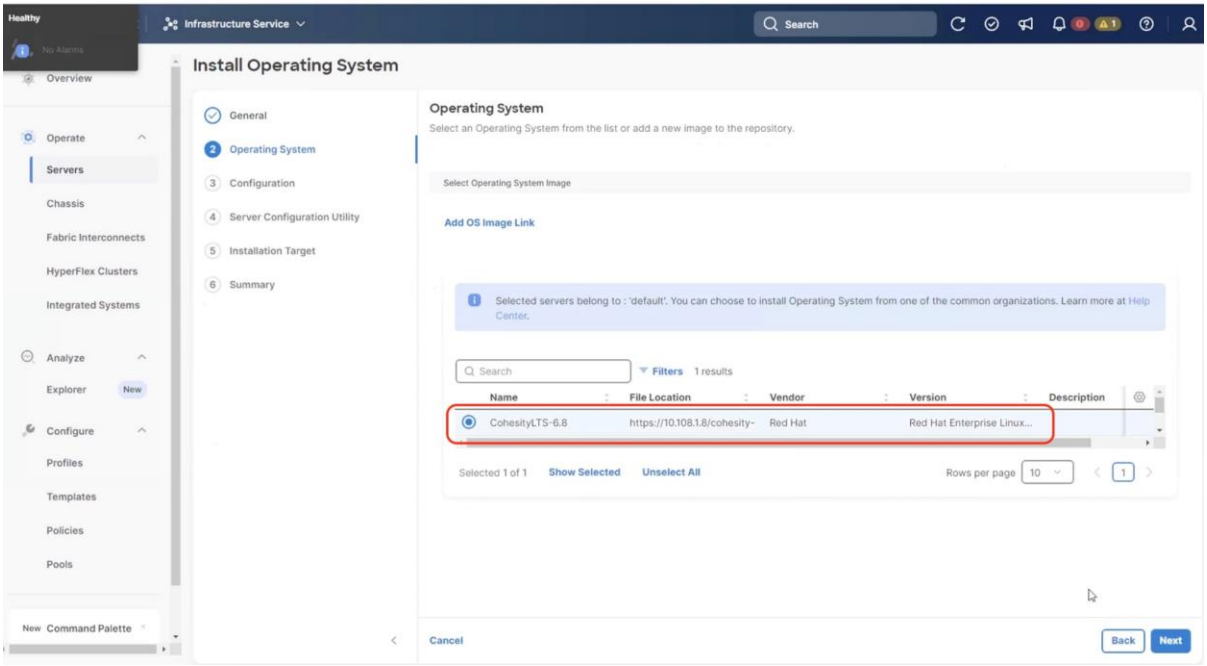
Step 8. Click the ... and select Install Operating System.



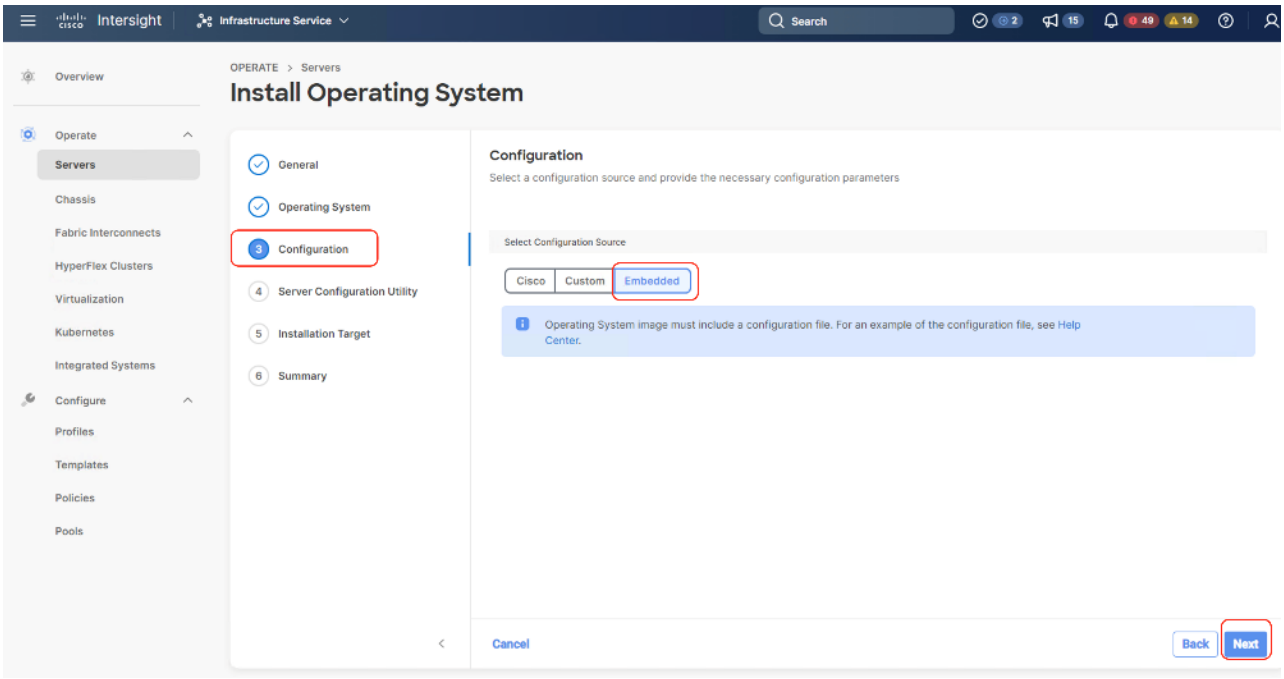
Step 9. Make sure the servers are already selected and click Next.



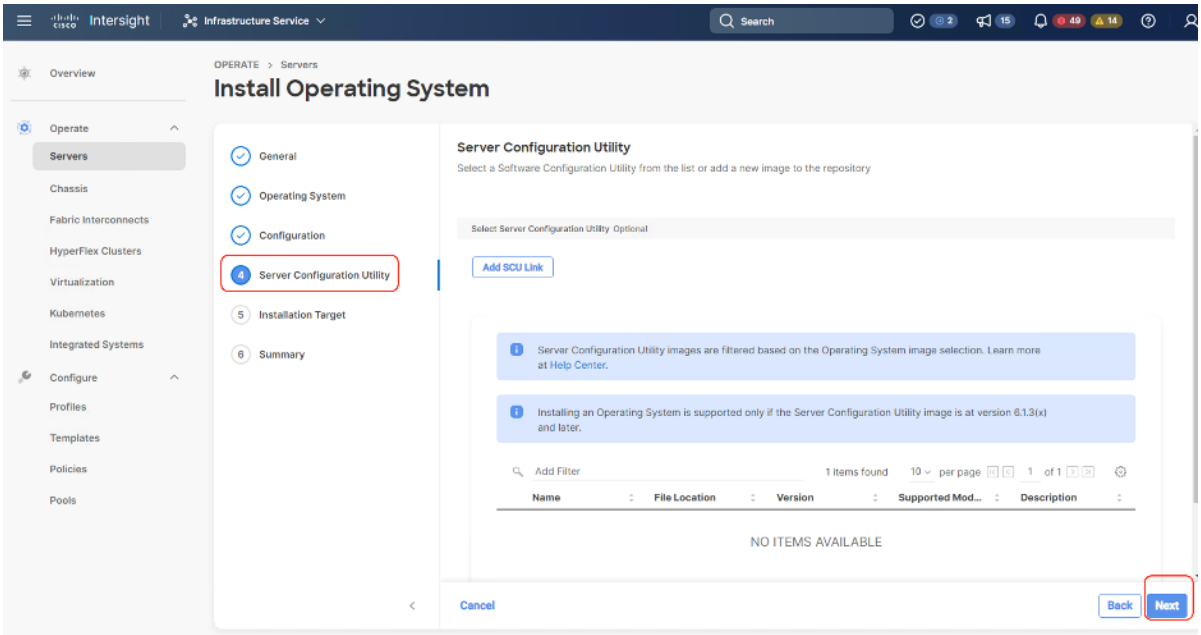
Step 10. Select the Operating System repository which was previously created with the Cohesity Data Cloud ISO and click Next.



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

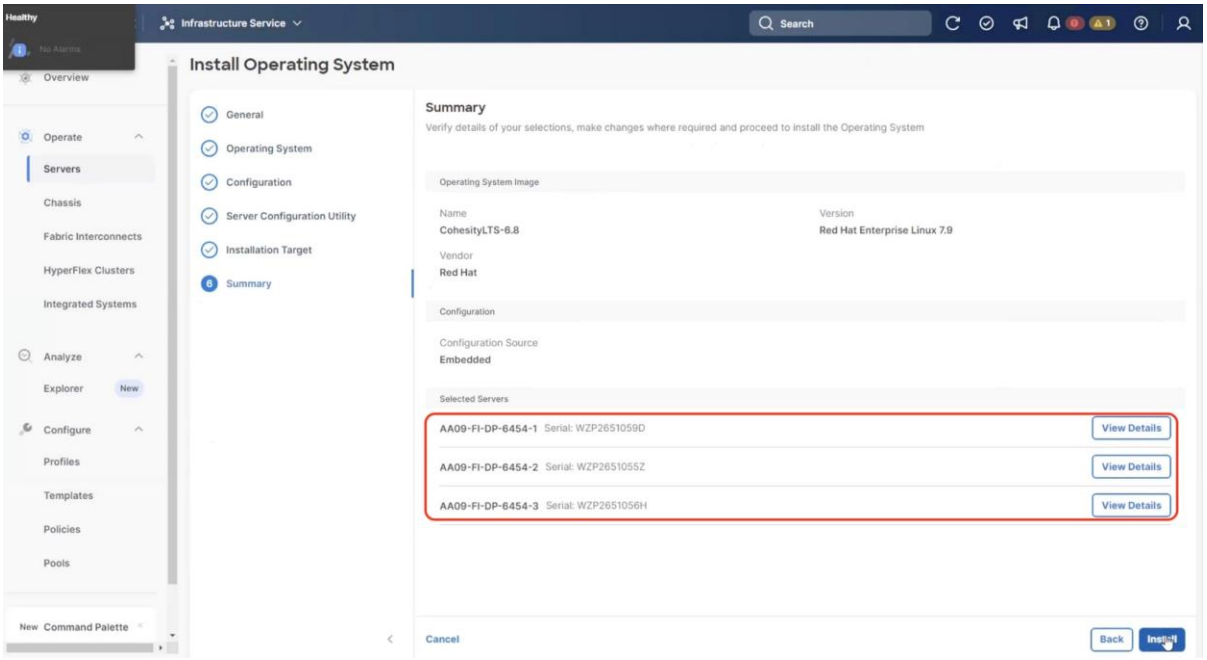


Step 12. Click Next.

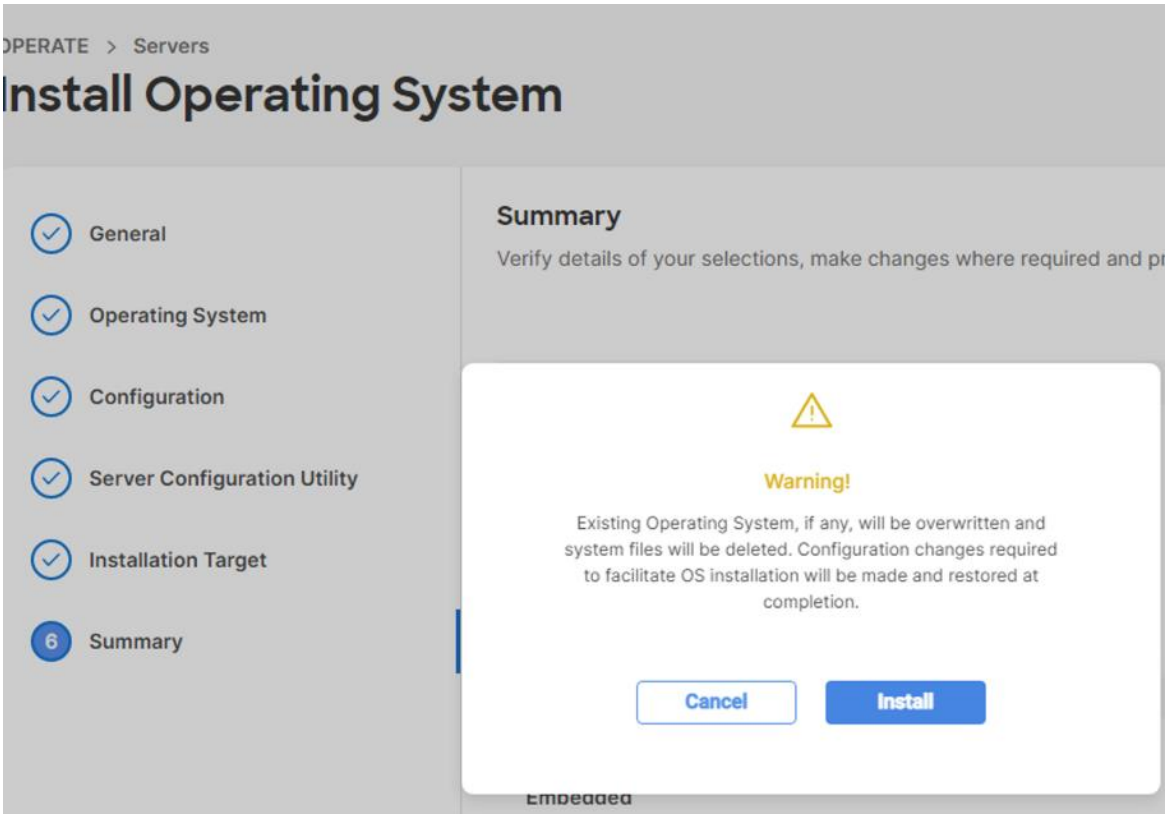


Step 13. Click Next from the Installation target. Cohesity ISO automatically identifies the Installation target as the 2x M.2 internal drives configured in the Boot Order Server Policy.

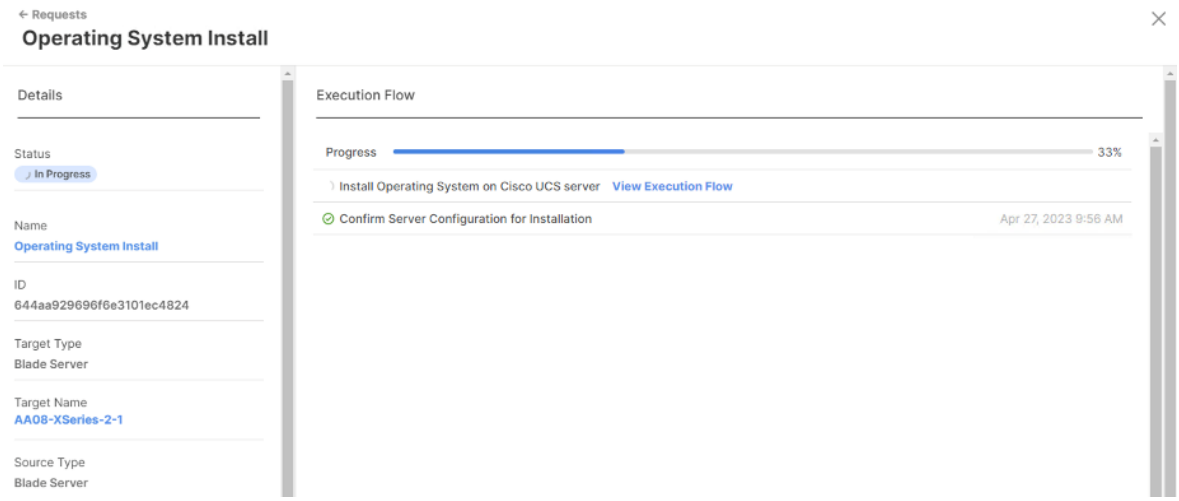
Step 14. Verify the summary and click Install.



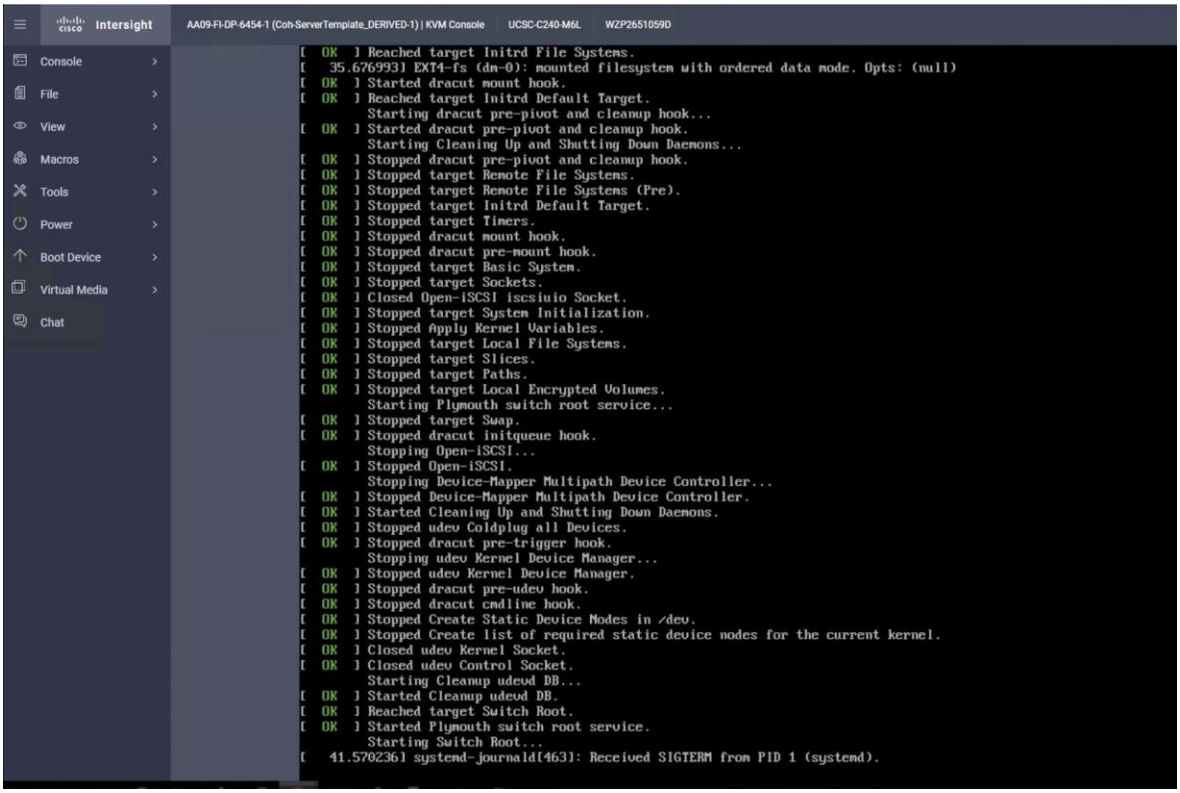
Step 15. Accept the warning for overwriting the existing OS image on the node and click Install.



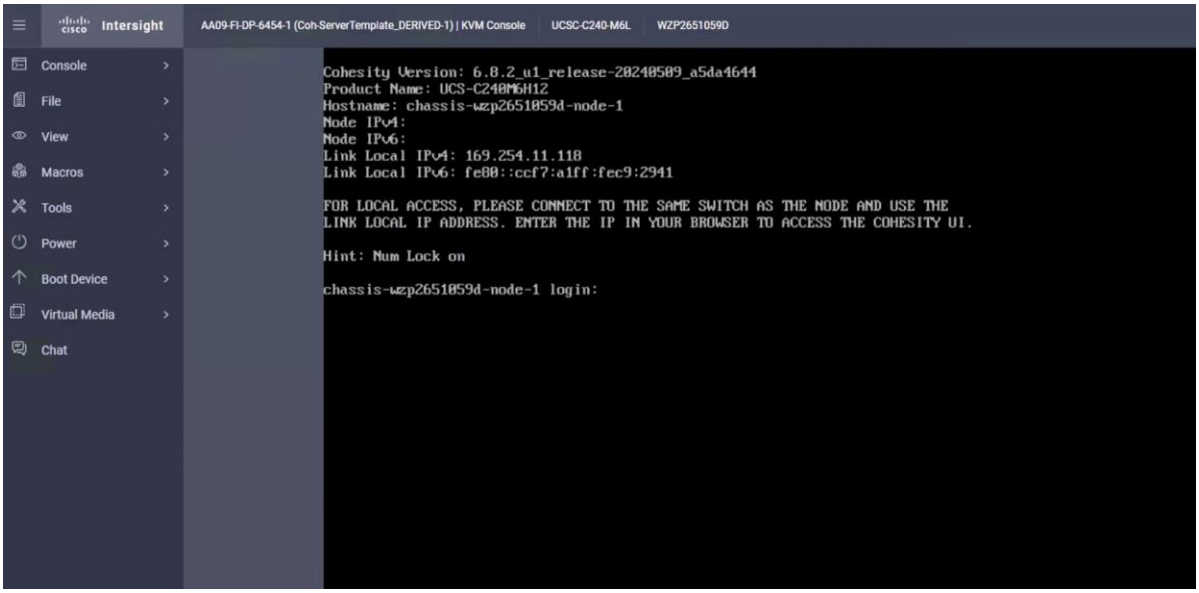
Step 16. Monitor the OS installation progress and wait for completion. Depending on the network bandwidth between the node management network and the repository network, it can take up to 45 minutes for the OS installation to complete.



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.



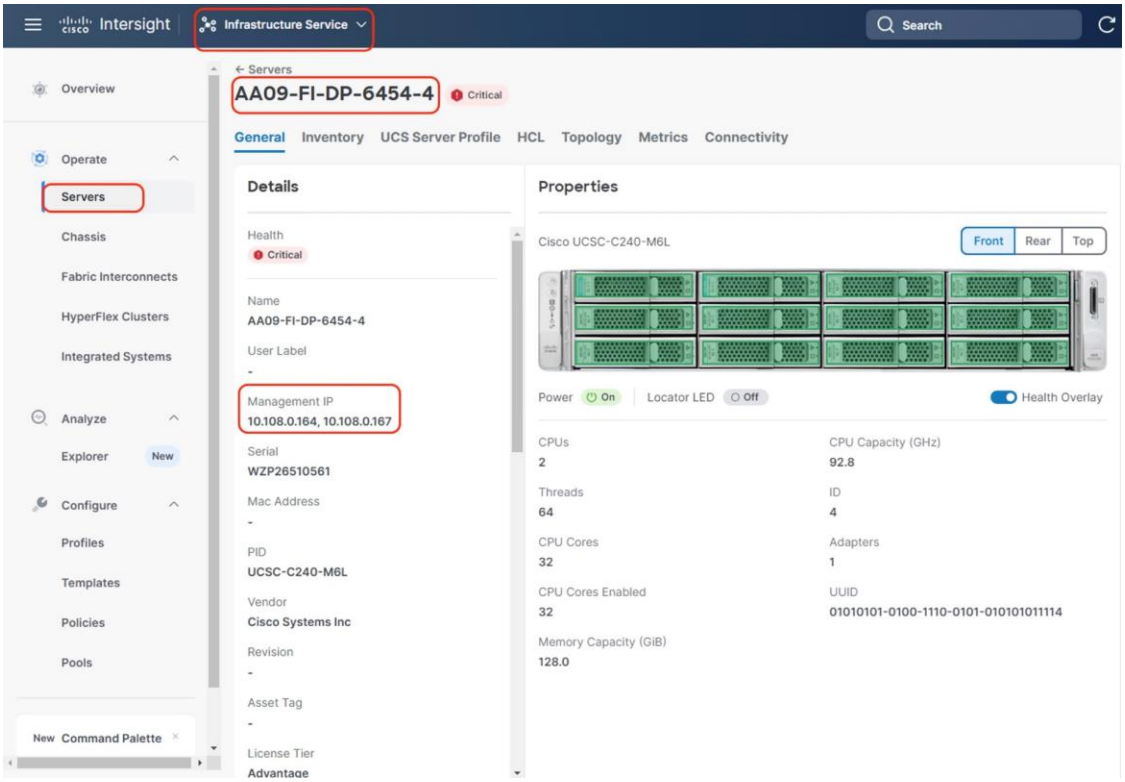
Install OS through Virtual Media

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.

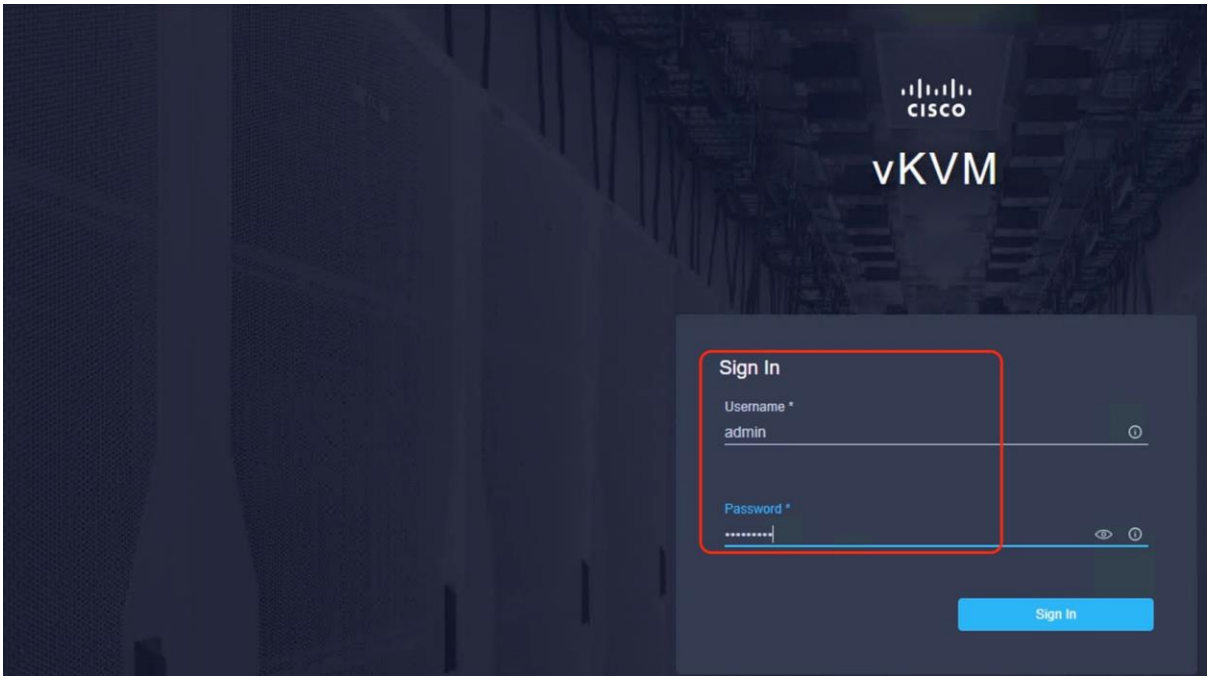
Note: During the OS installation, it is recommended to open vKVM through node management IP. Access the vKVM through the user created in useraccess policy (admin/<<password>>)

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

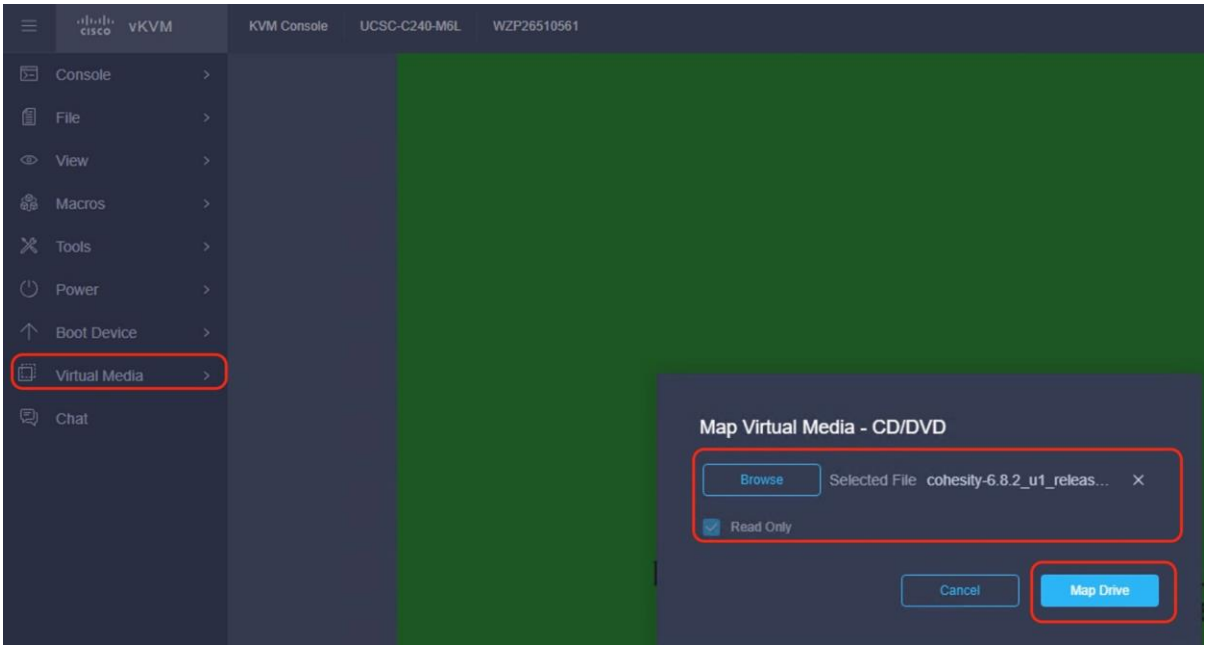


Note: The existing deployment displays two management IPs. These are IN-Band and Out of Bank management IPs as defined in the Cisco IMC Access Policy. If customers want to install the Cohesity OS only through KVM access then only Out of Band Management IP is required.

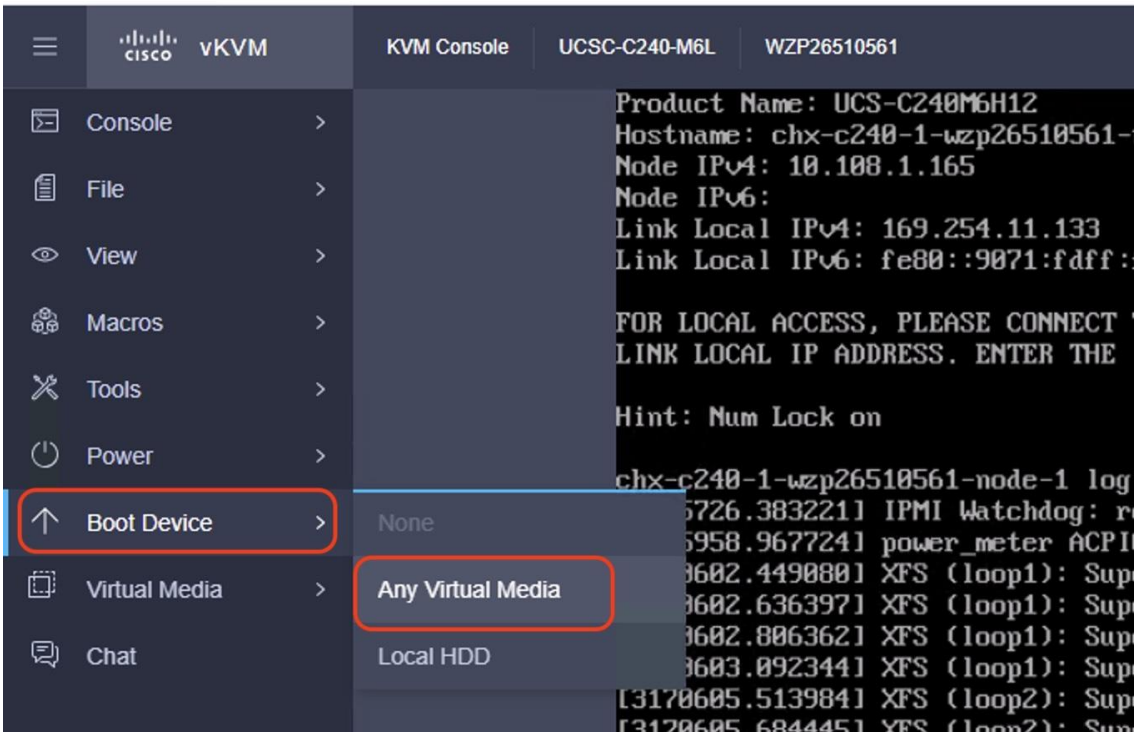
Step 2. Login to vKVM with the username/password as defined in the user access policy.



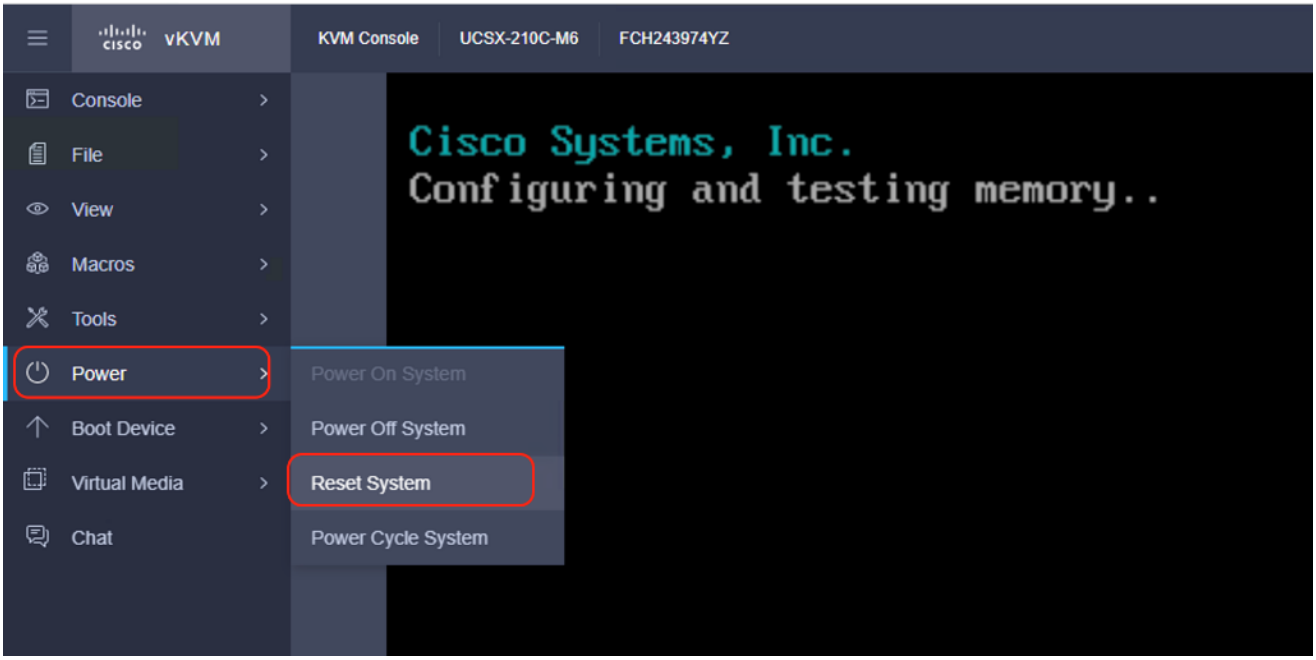
Step 3. Select the Cohesity Data Cloud ISO from your local file system and click Map Drive.



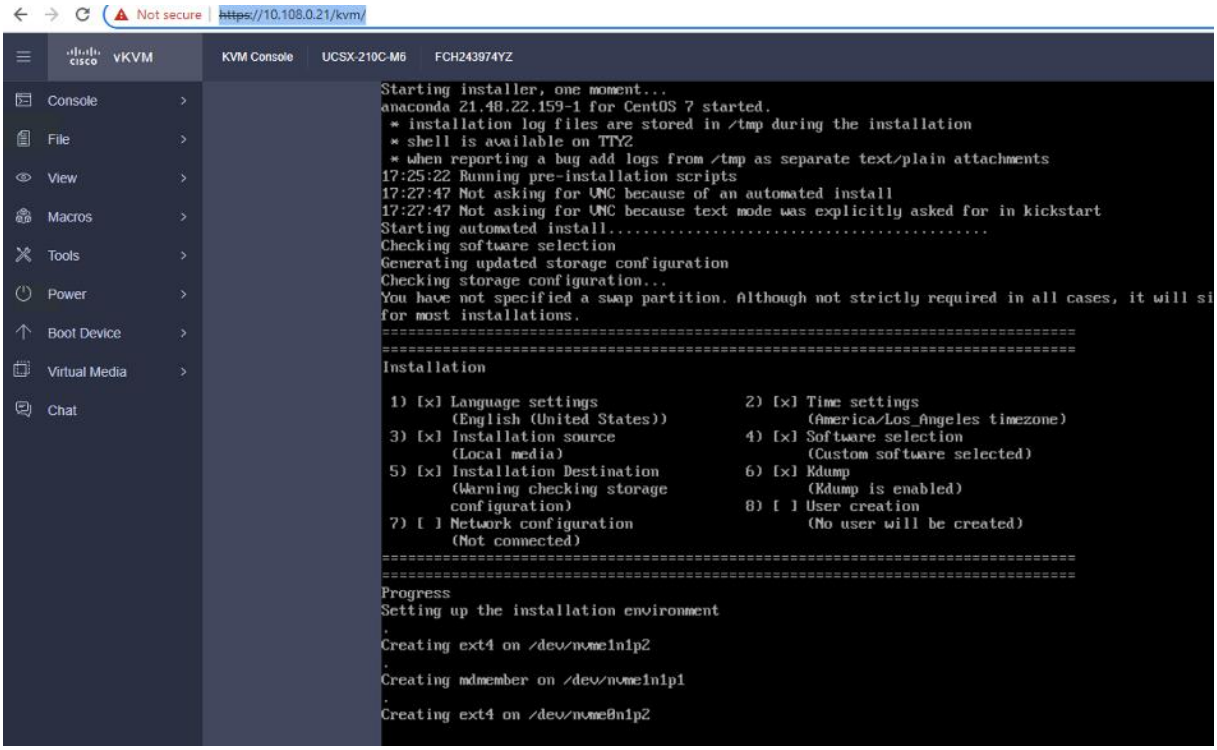
Step 4. Modify the Boot Device to Any Virtual Media , this will implement a one time boot through virtual media and override the default Boot Order Policy.



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.



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: 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)

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

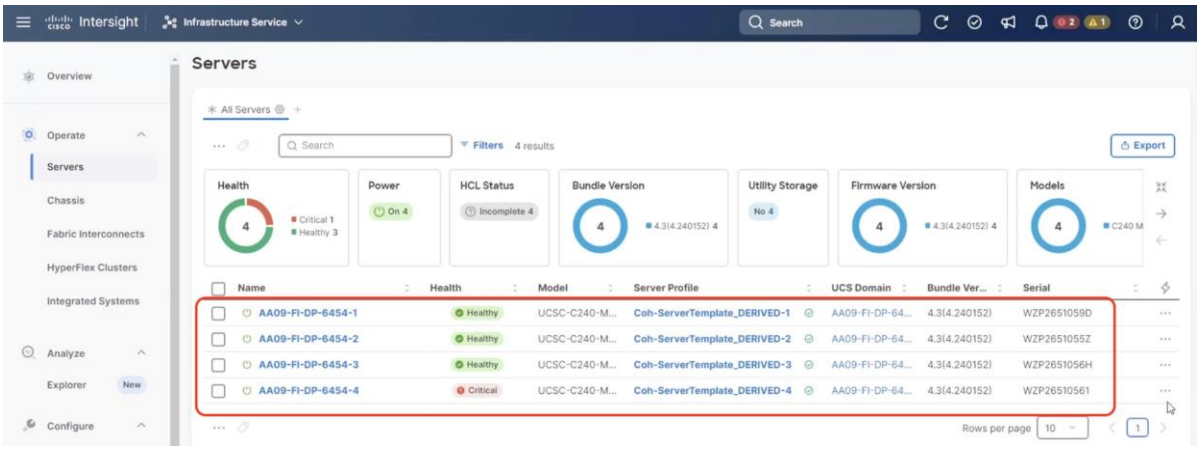
- Initial network configuration on 1x Cisco UCS C-Series node
- Cluster configuration across all Cisco UCS C-Series nodes

Configure First Node

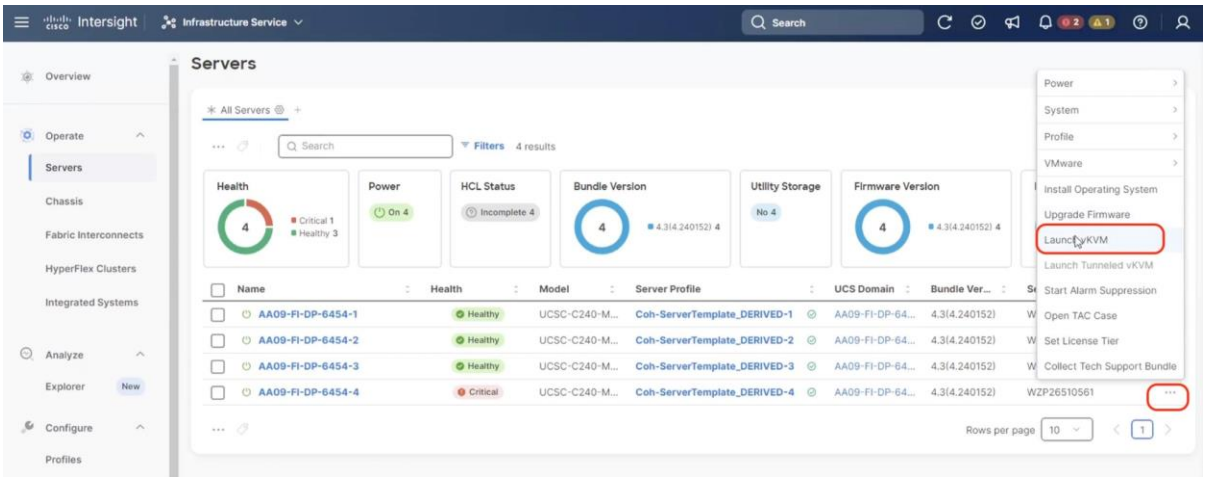
Procedure 1. Initial Network Configuration on 1x Cisco UCS C-Series Node

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

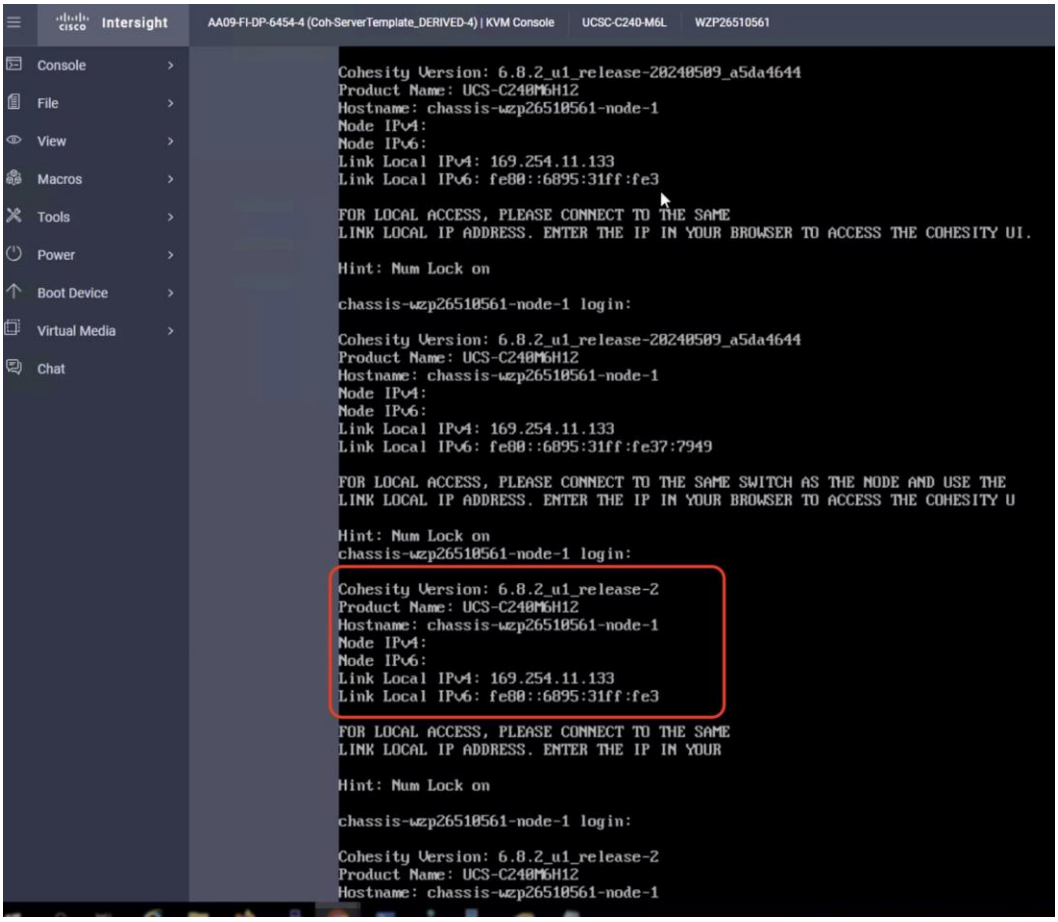
Step 1. Login to Cisco Intersight, click Infrastructure Service and click Servers. Identify the Cisco UCS C-Series nodes installed with the Cohesity ISO.



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



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.

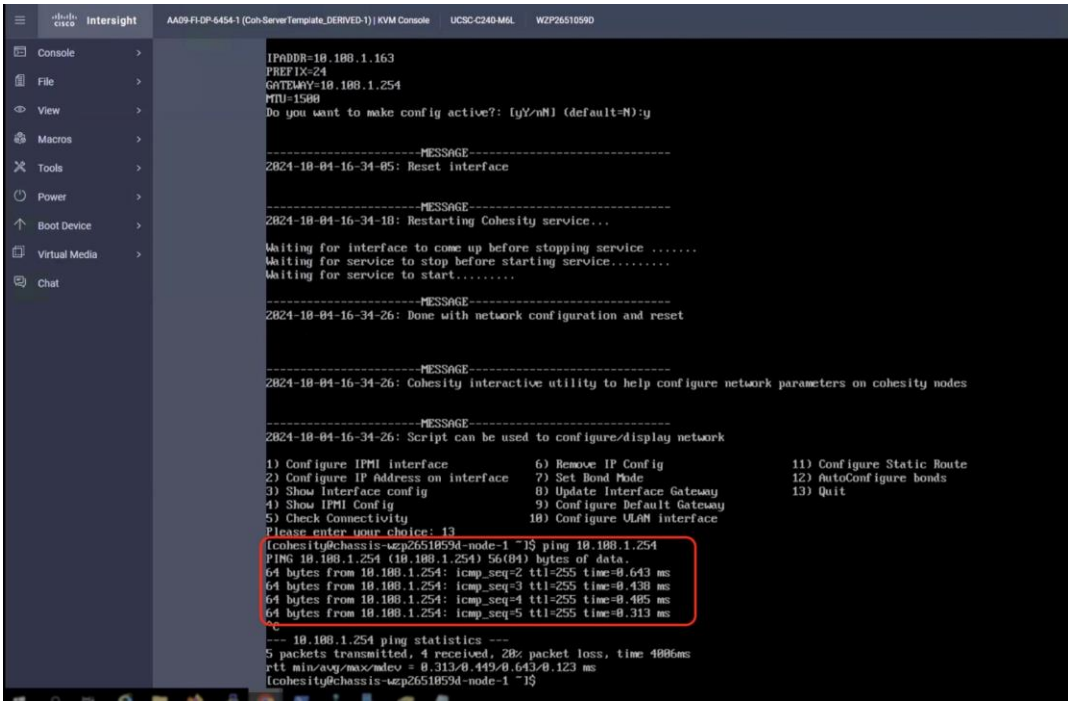
Step 10. Select Y/Yes to make the interface active.

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

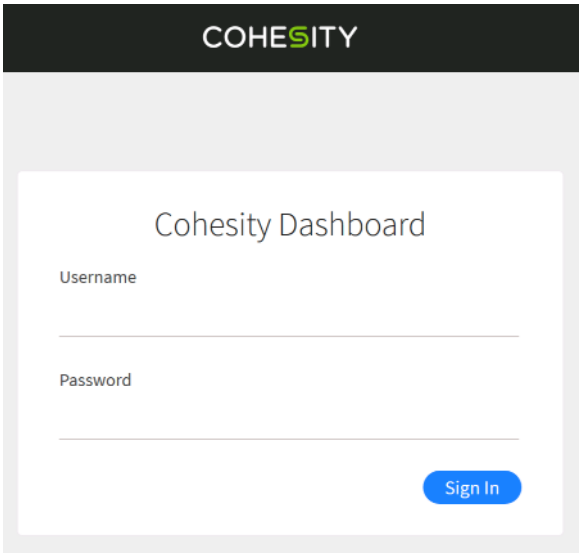
The initial setup of the Cohesity cluster is done through the configuration webpage, which is now accessible on the first node, at the IP address which was configured in the previous steps. Prior to beginning the initial cluster configuration, make sure that all Cohesity nodes which are to be included 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

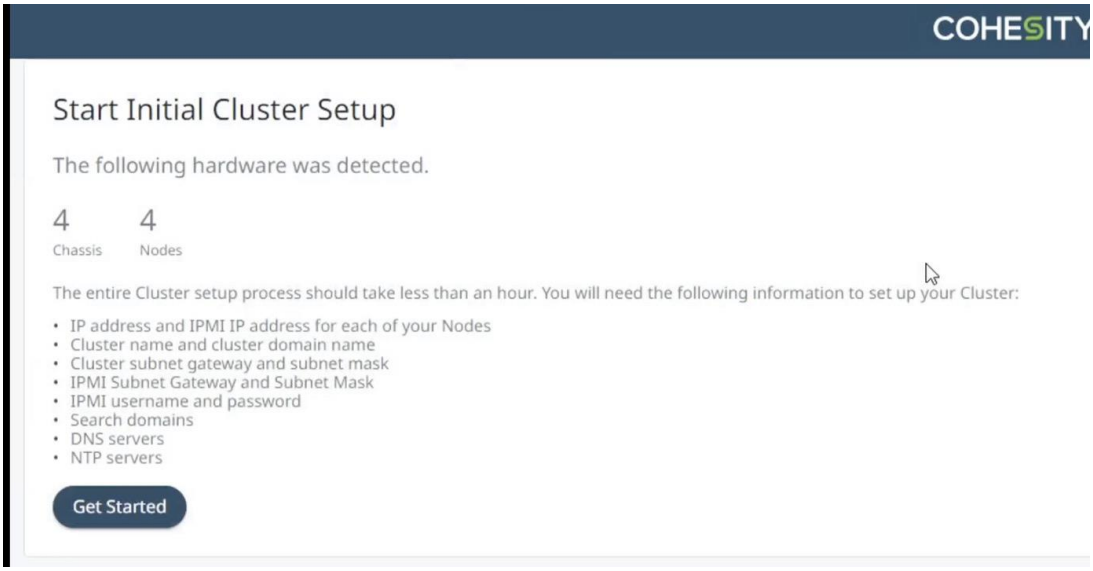
Step 2. Accept any SSL warnings or errors due to the default self-signed certificate on the server and proceed to the Cohesity Dashboard login screen.

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

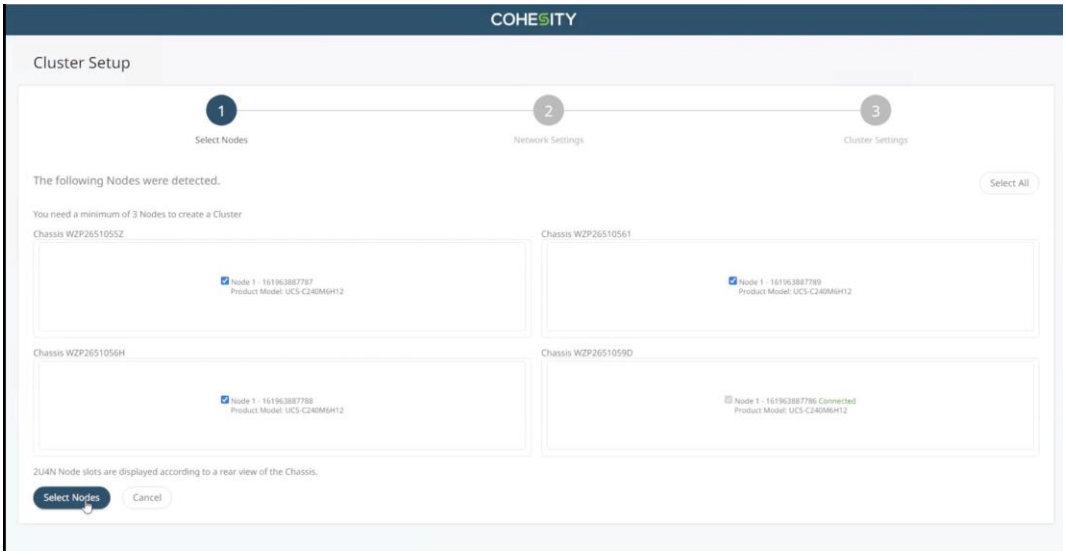
- Username: admin
- Password: <password>



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.

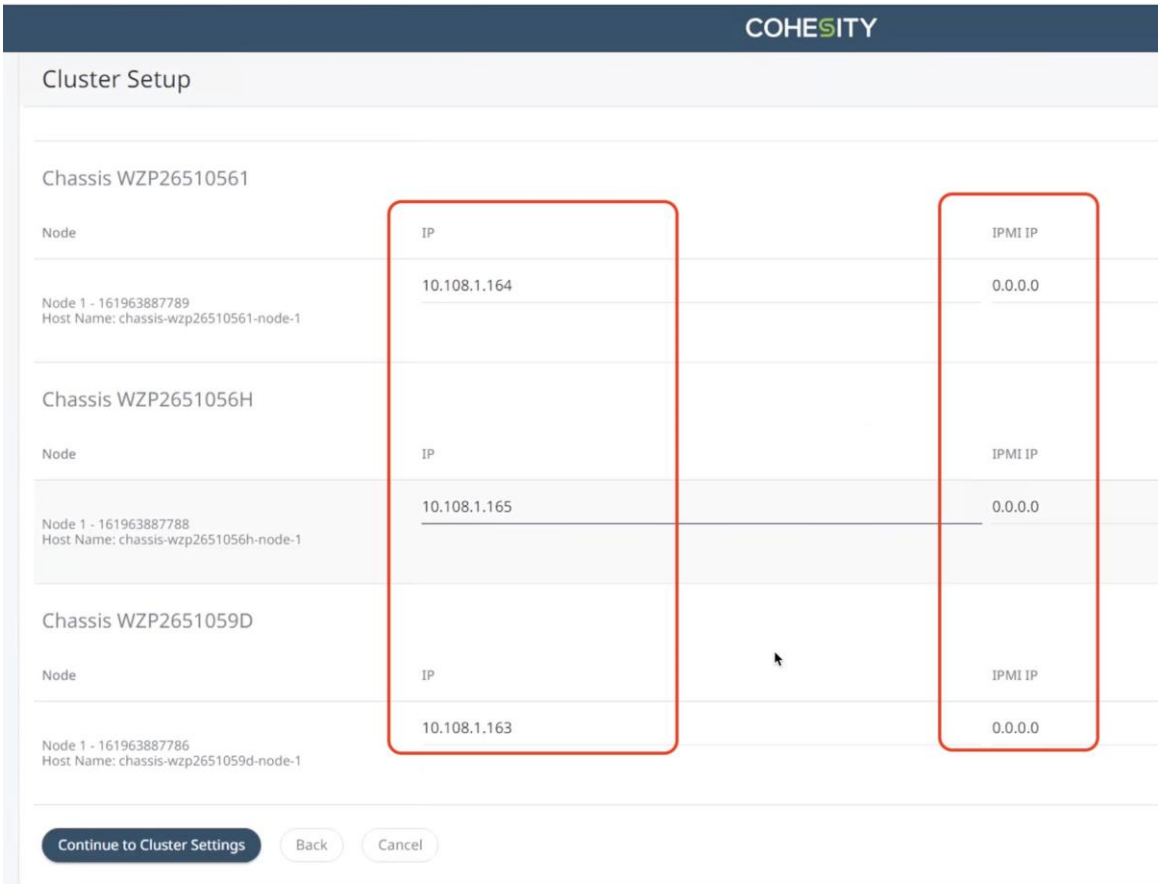


Step 5. Select the nodes to add to this initial cluster, then click Select Nodes.

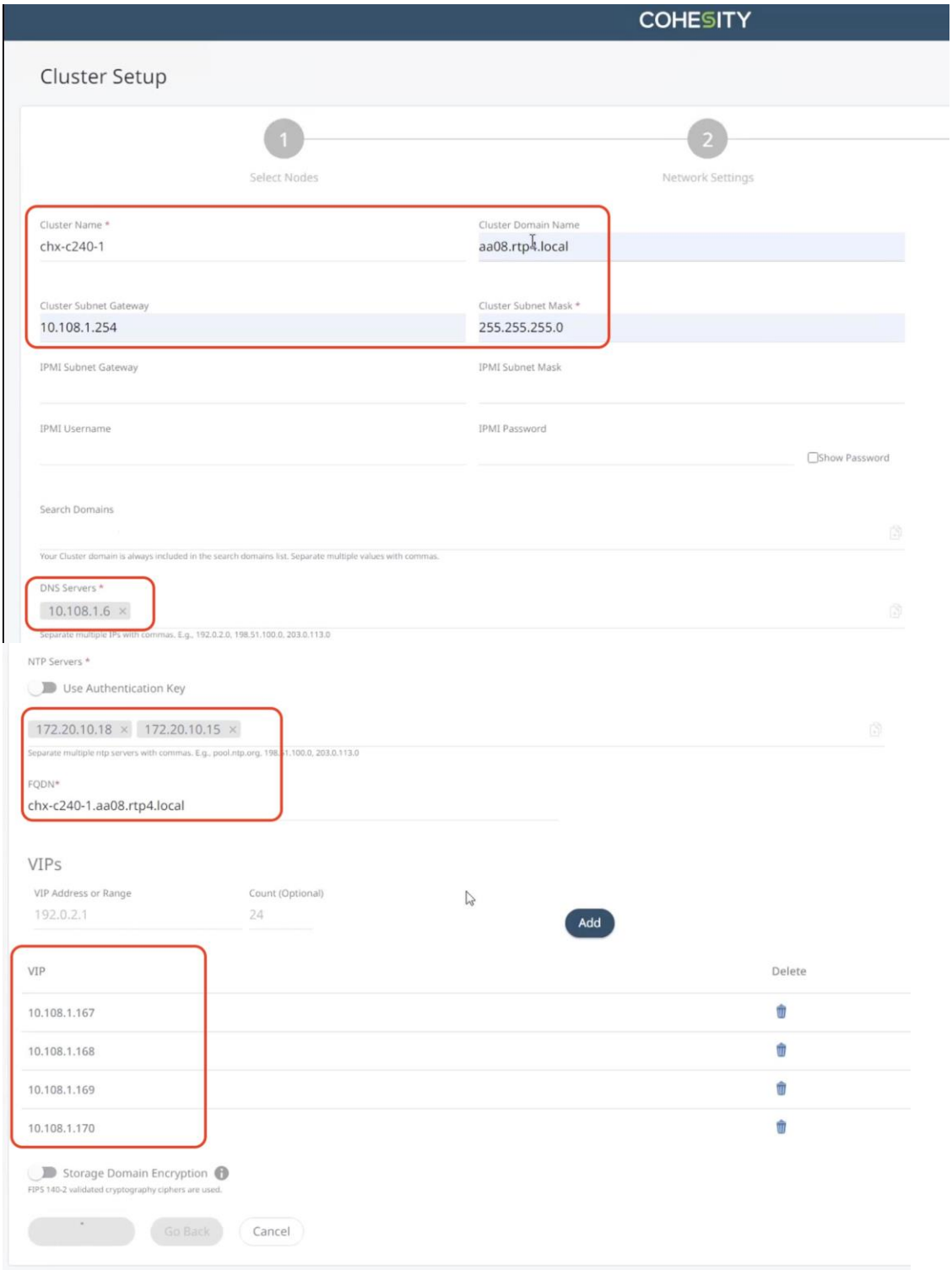


Step 6. Enter the OS IP determined for each node, The IPMI IP should be 0.0.0.0 for all nodes in the cluster

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.

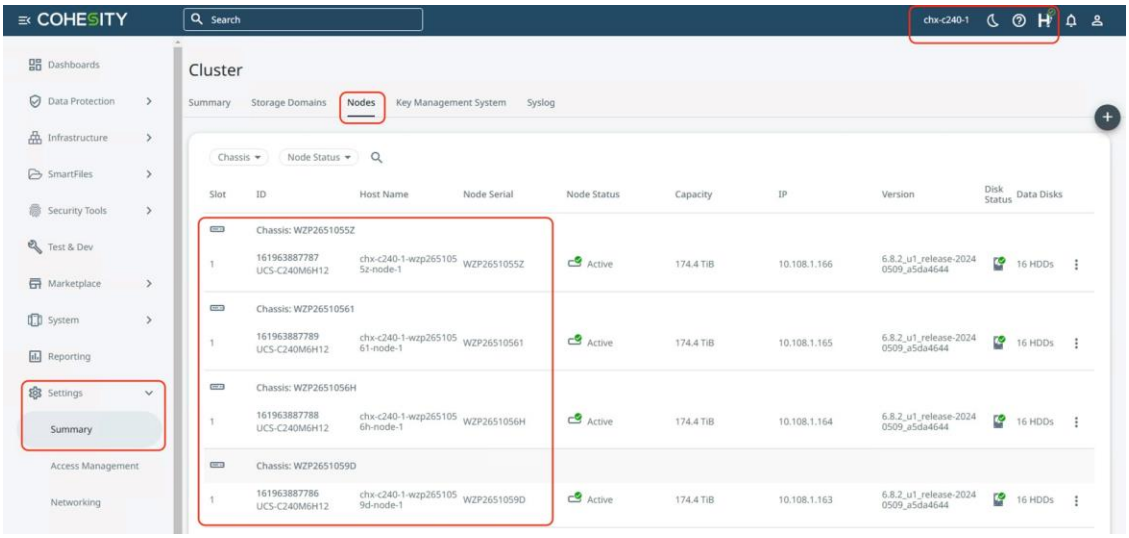


Step 7. Enter the Cluster Subnet, Gateway, DNS, NTP, Virtual IP and FQDN details and click Create Cluster.



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.



Cluster Expansion and Firmware Upgrades

This chapter contains the following:

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.

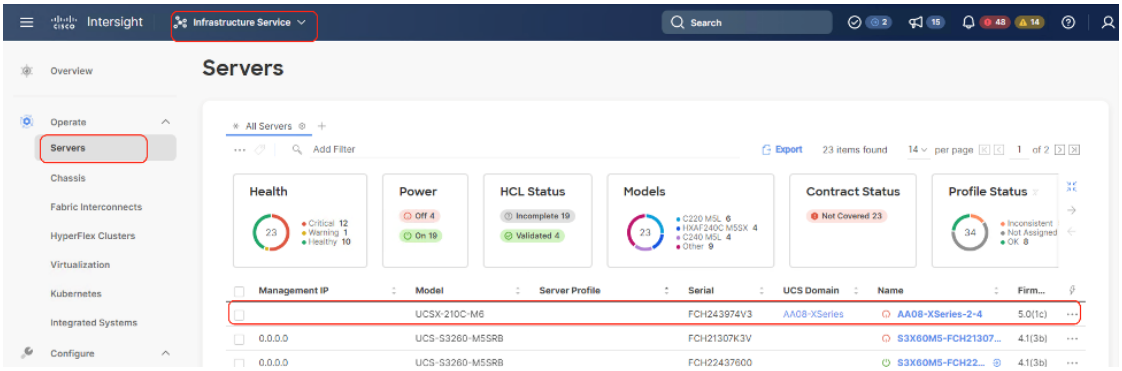
Procedure 1. Derive and Deploy Server Profile to New Node

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

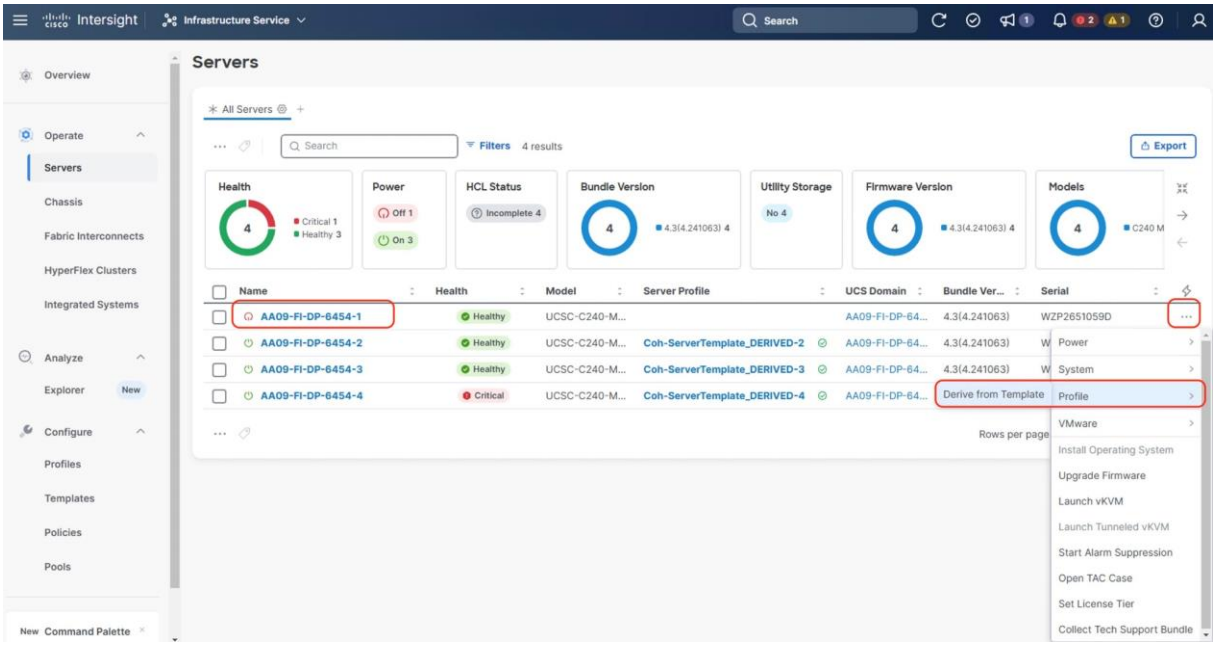
Step 1. Go to https://intersight.com/, click Infrastructure Service and click Server. Identify the new Cisco UCS C-Series node provisioned for the existing Cohesity cluster expansion.

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

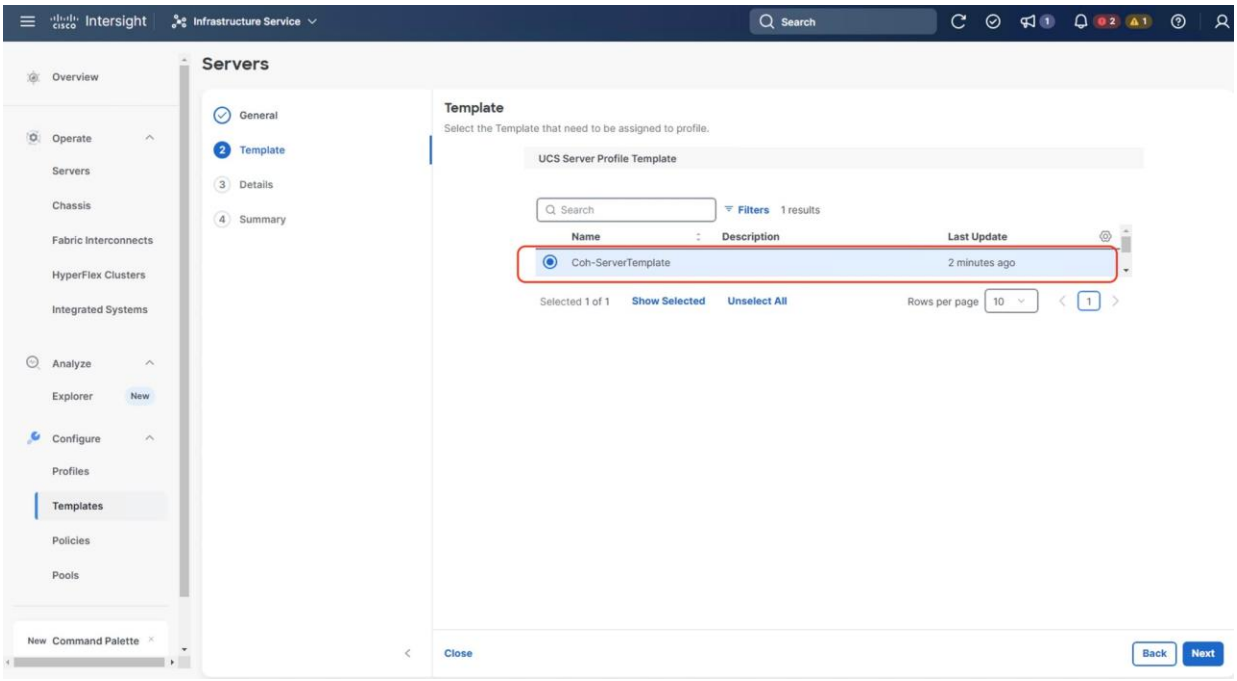
Note: The following screenshot demonstrates a Cohesity certified C-Series node which is discovered on Intersight and not assigned to any Server Profile.



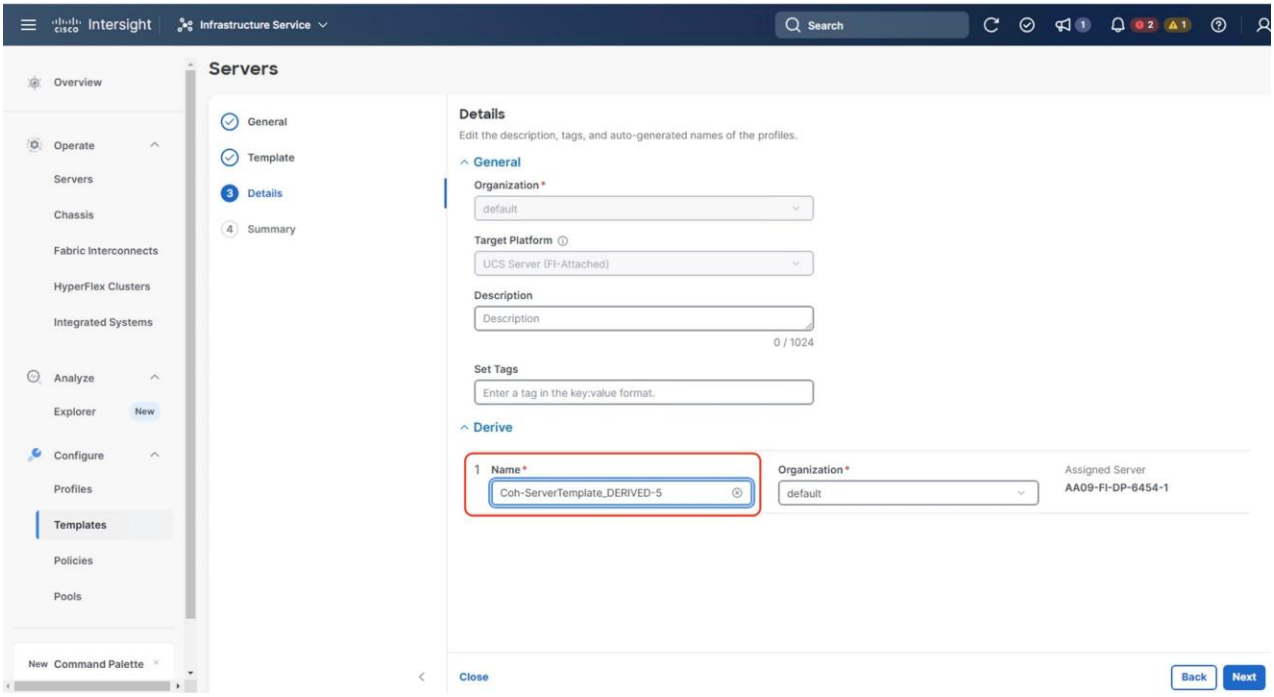
Step 2. Click "... ", select Profile and Derive Profile from the template.



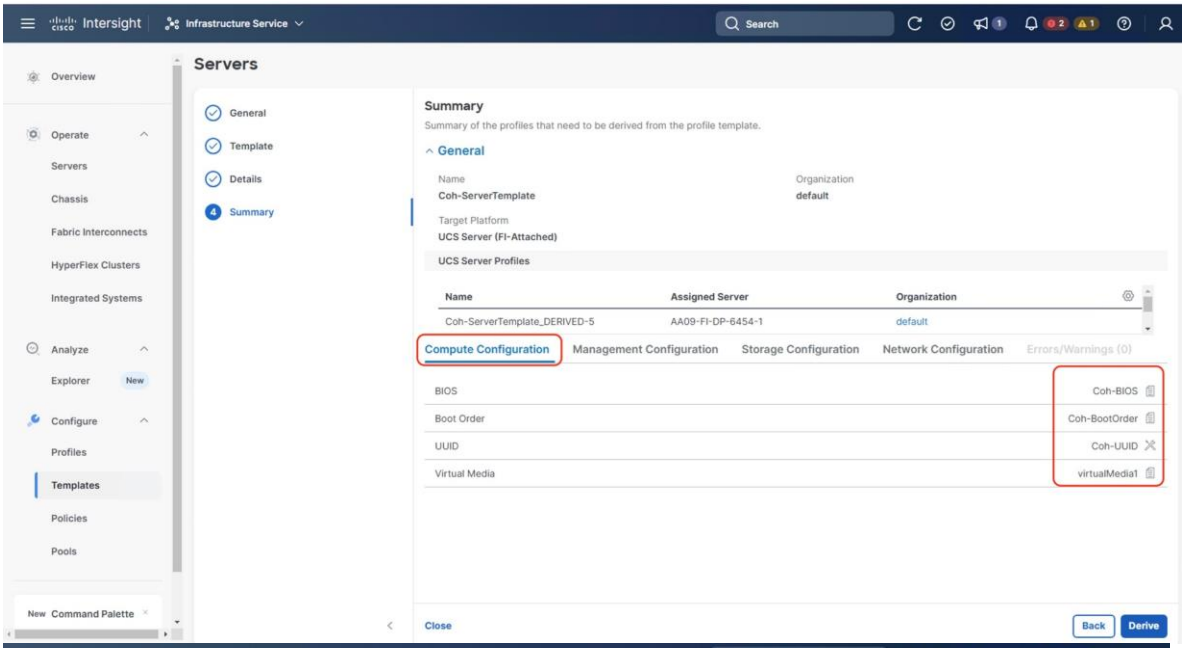
Step 3. Select the Server Profile template created to deploy the Cisco UCS C-Series node for the Cohesity cluster and click Next.

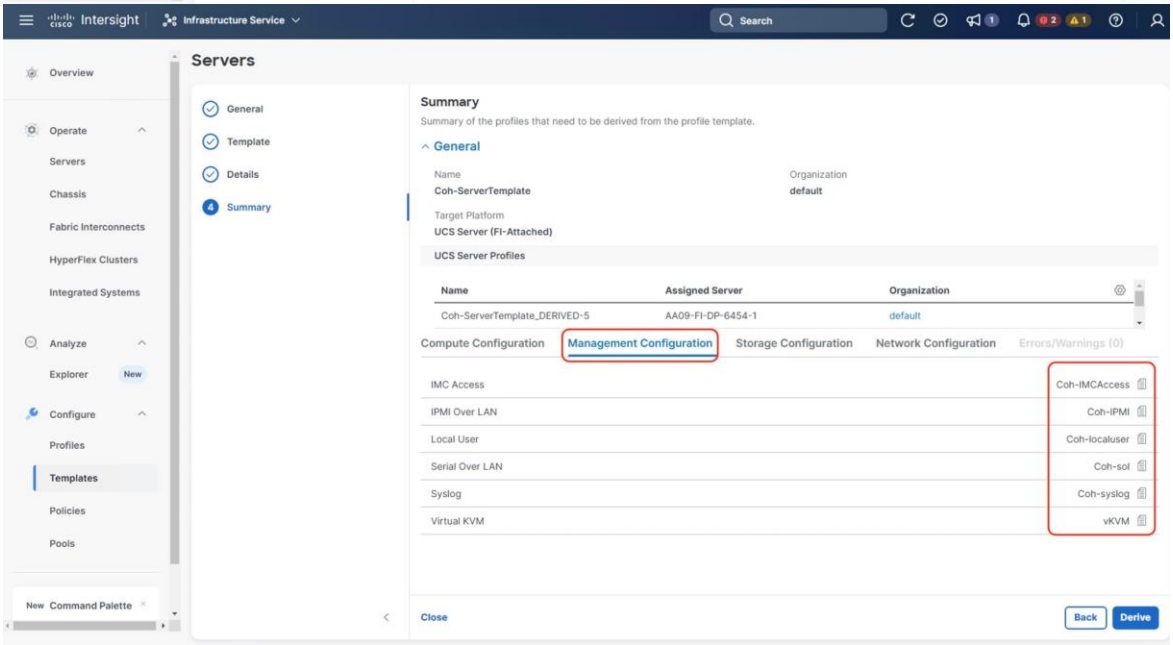


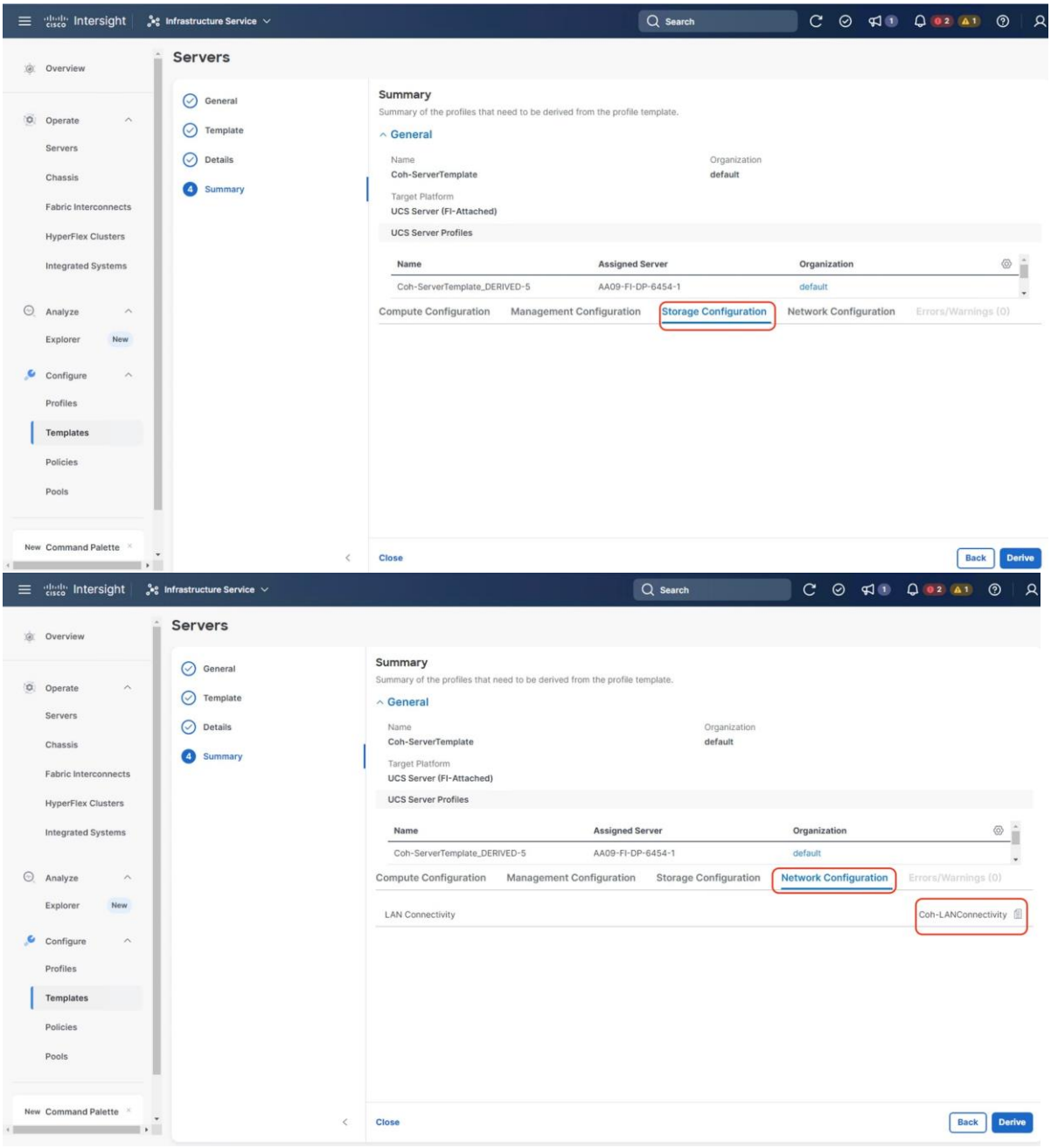
Step 4. Rename the Derive profile and click Next.



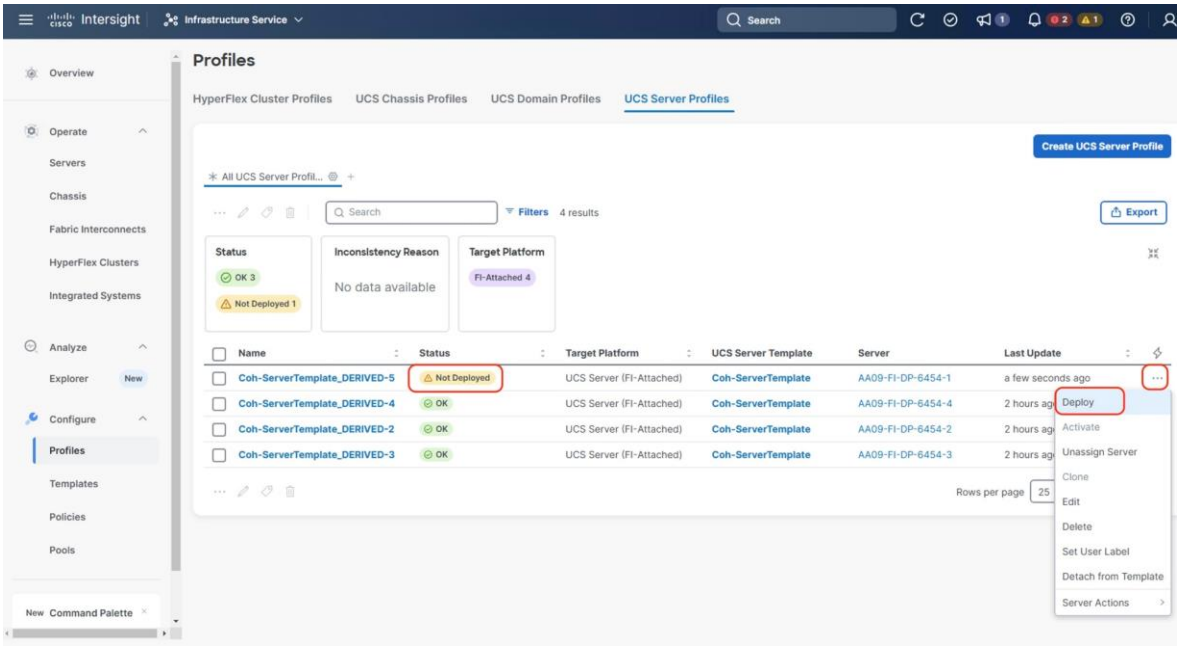
Step 5. Verify the policies and click Derive. As we are using the original Server Template to derive Server Profile, the policies would be exactly the same. To ensure consistency and avoid misconfigurations , it is recommended to use the same Server Template as that of original cluster.



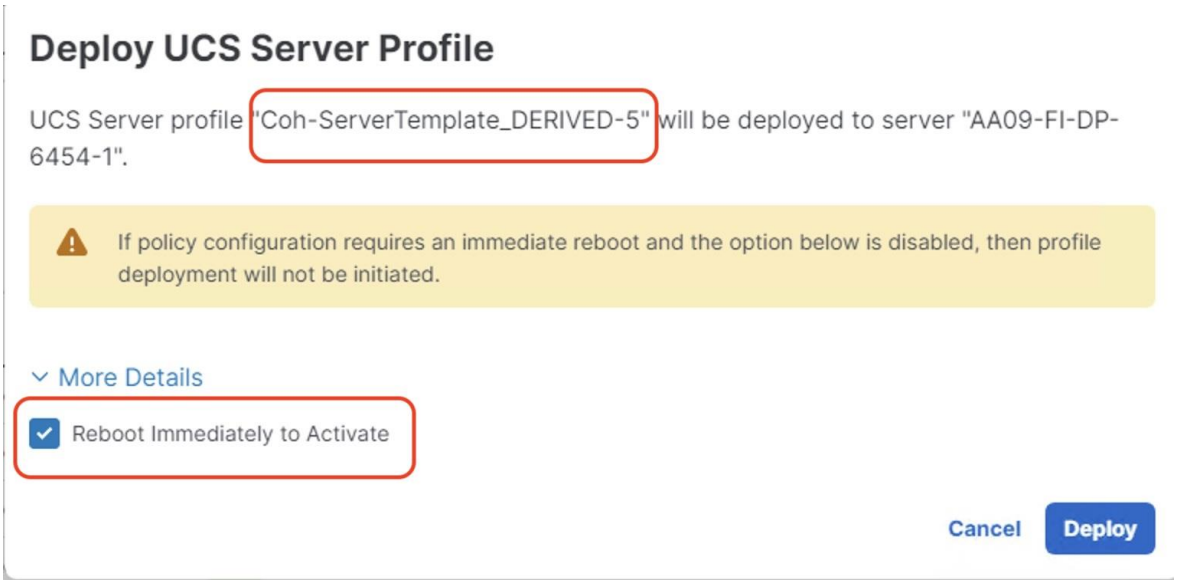




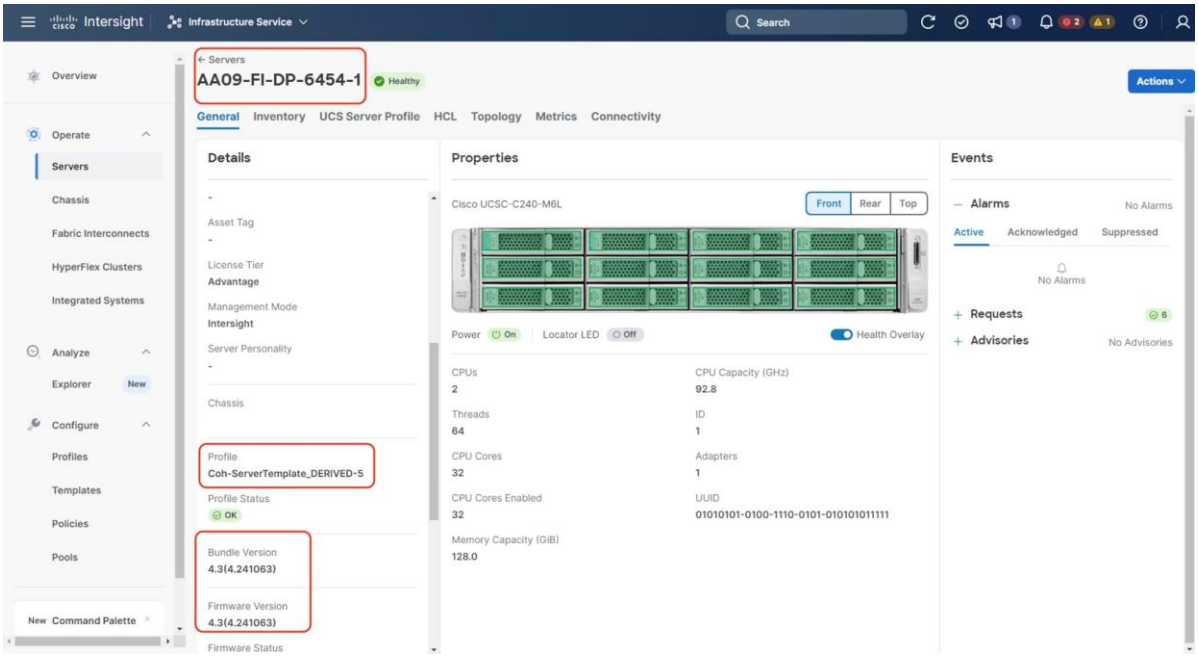
Step 6. When the Sever Profile is derived, go to the Servers tab, identify the Profile displayed as “Not Deployed,” click the “...” and select Deploy.



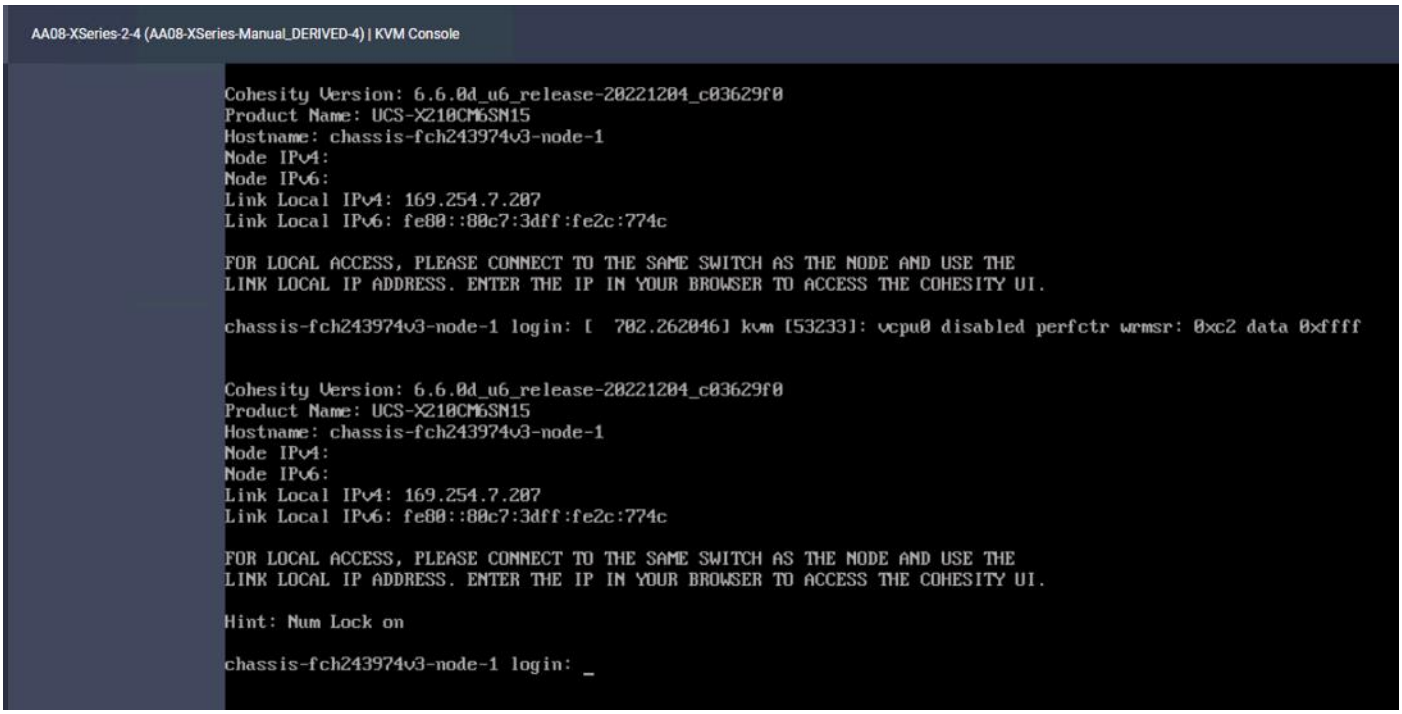
Step 7. On the Deploy Profile confirmation screen, enable Reboot Immediately to Activate and click Deploy.



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.



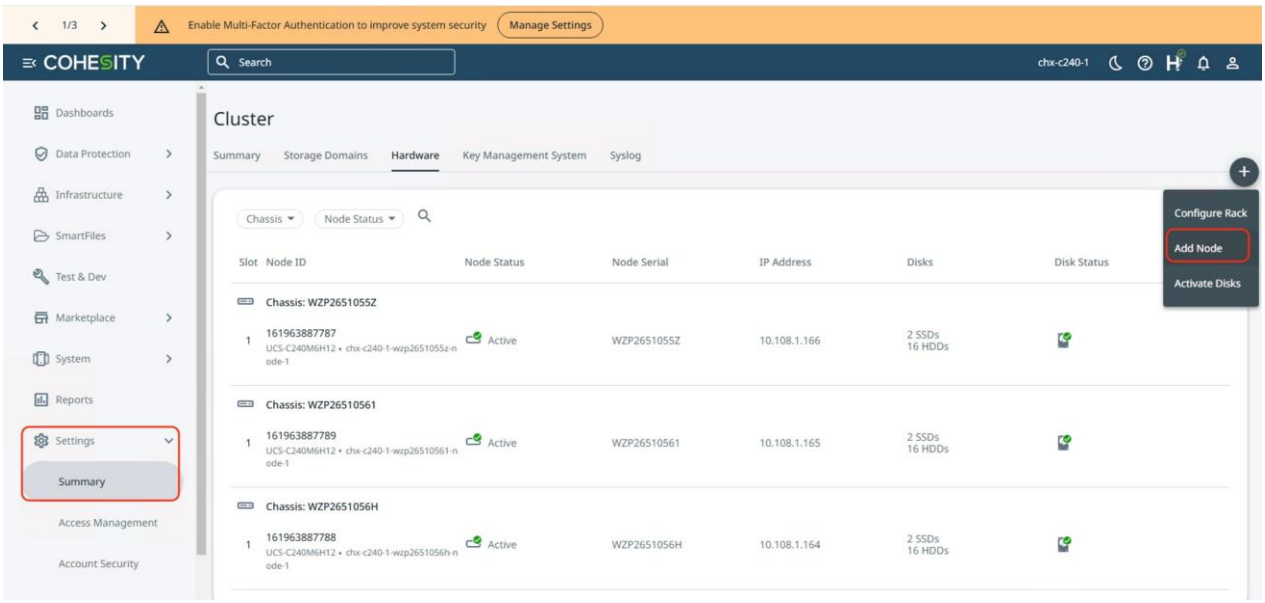
Step 9. Install the OS using Cisco Intersight or through vMedia, provided in section [Install Cohesity on Cisco UCS C-Series Nodes]The screenshot below displays on the OS deployed on the new Cisco UCS C-Series node.



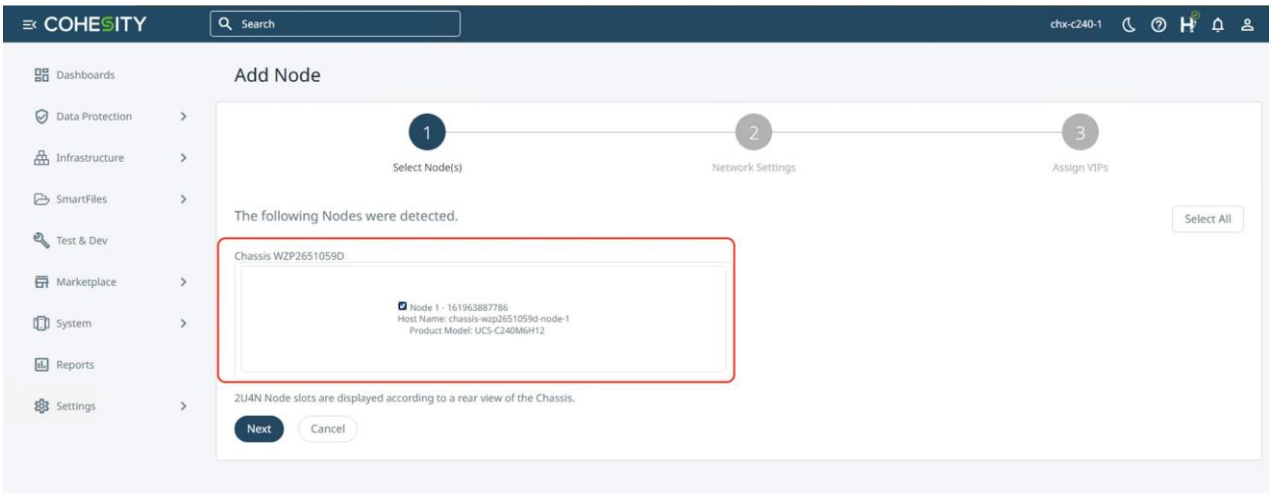
Procedure 2. Expand existing Cluster through Cohesity Helios

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.

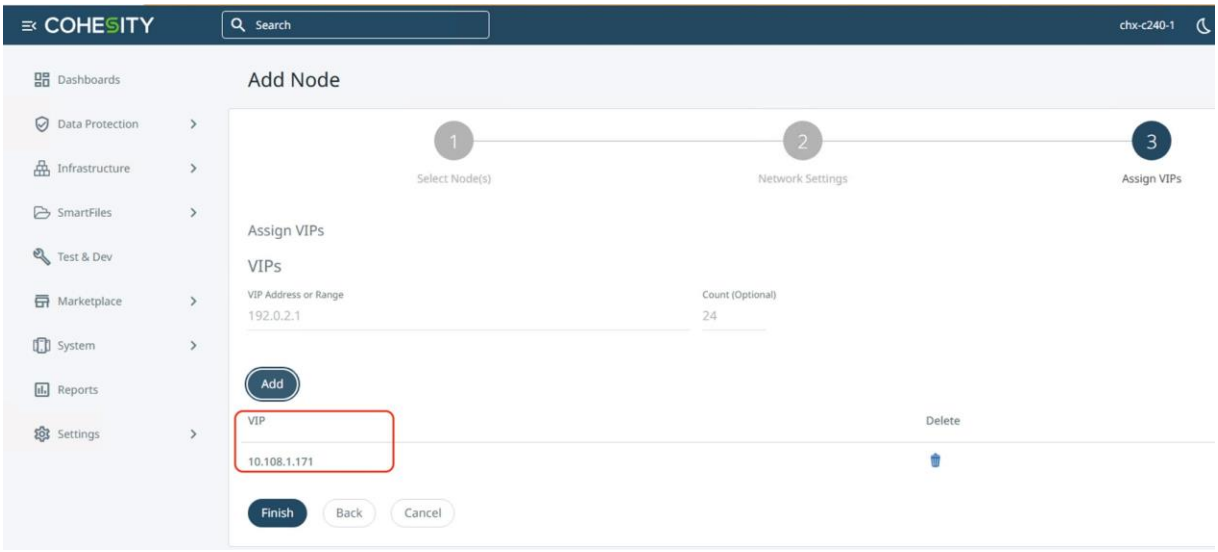


Step 2. The Cohesity cluster automatically identifies the new node. Confirm the serial number of the node, which was configured for the cluster expansion, select the node, and click Next.

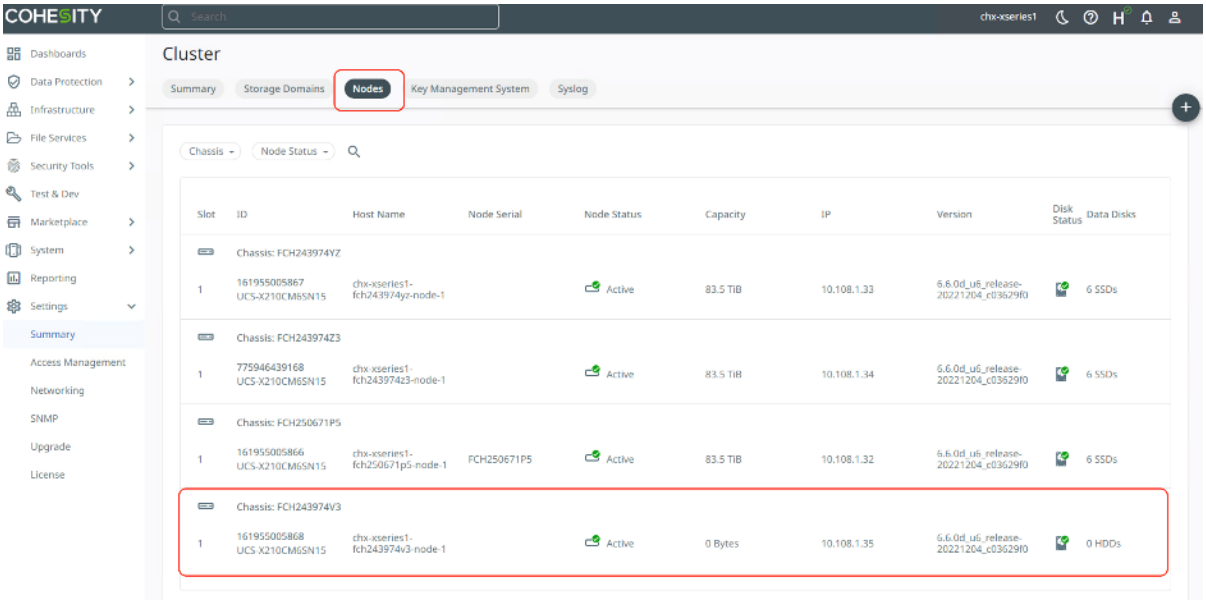


Step 3. Add the available Node IP and click Next.

Step 4. Add the Virtual IP as configured on DNS and click Finish.



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.



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: https://intersight.com/help/saas/resources/Upgrading_Fabric_Interconnect_Firmware_imm#procedure

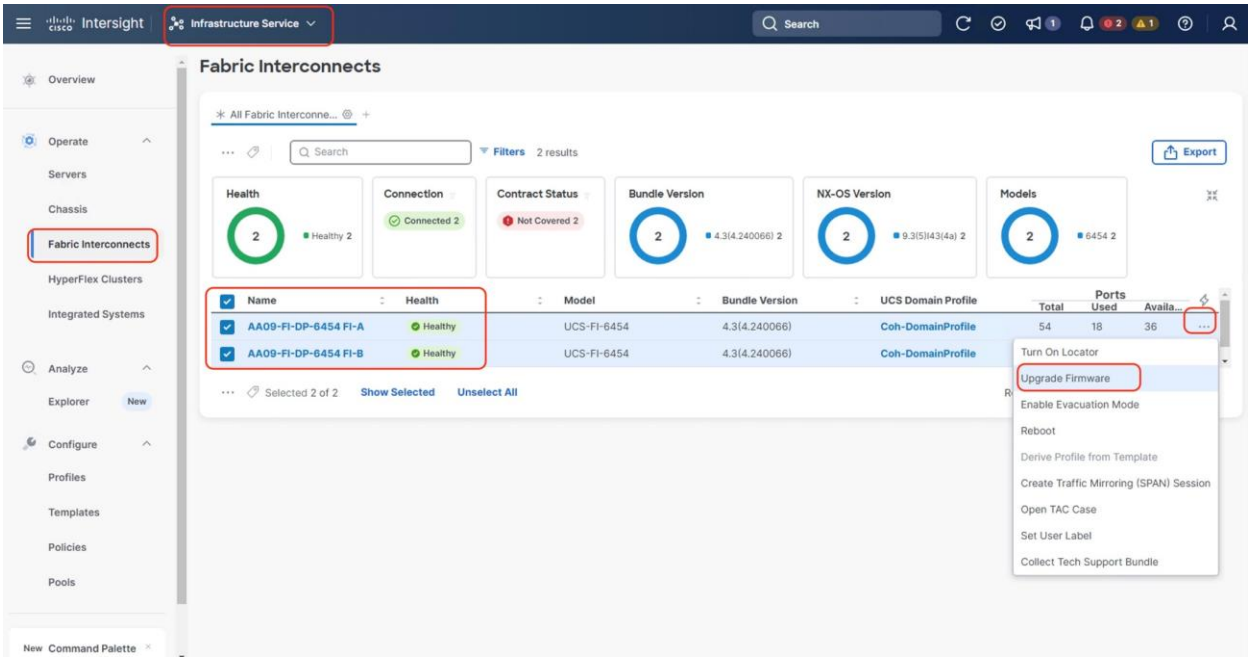
Note: During the upgrade of the Intersight Managed Fabric Interconnect, the fabric interconnect traffic evacuation is enabled by default. The fabric interconnect traffic evacuation evacuates all traffic that flows through the fabric interconnect from all servers attached to it, and the traffic will fail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

Upgrade Fabric Interconnect

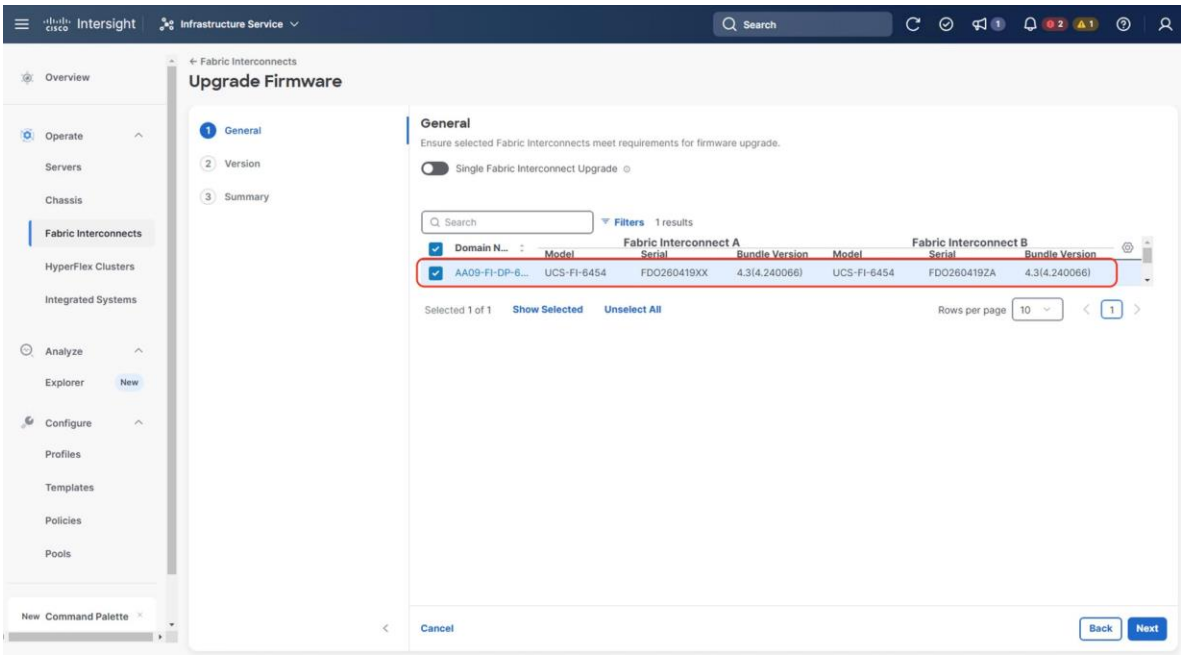
Procedure 1. Upgrade Cisco UCS Fabric Interconnect and Cisco UCSX 9108 IFM Firmware

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 https://Intersight.com, click Infrastructure Service, then click Fabric Interconnects, and select the Fabric Interconnect Pair (IMM) . Click "..." and select Upgrade Firmware.

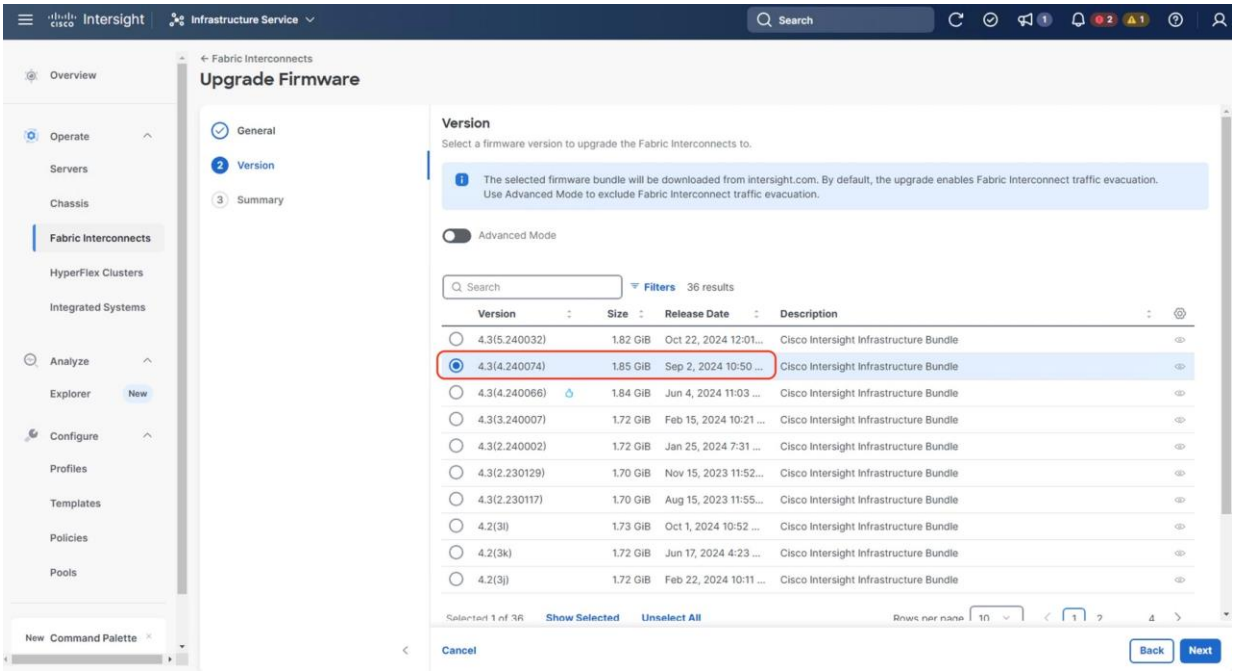


Step 2. Click Start and from Upgrade firmware make sure the UCS Domain Profile is selected and click Next.

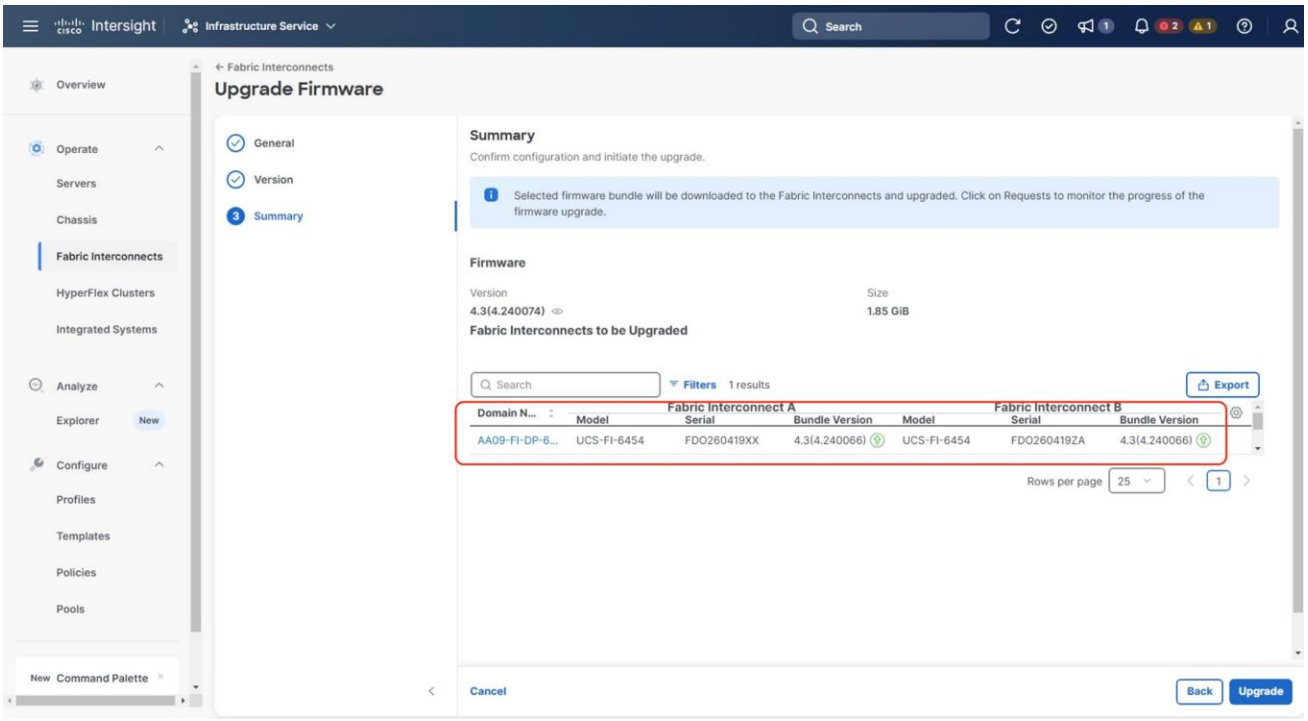


Step 3. Select the recommended Firmware release. By default, the upgrade enables the Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude the Fabric Interconnect traffic evacuation.

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.

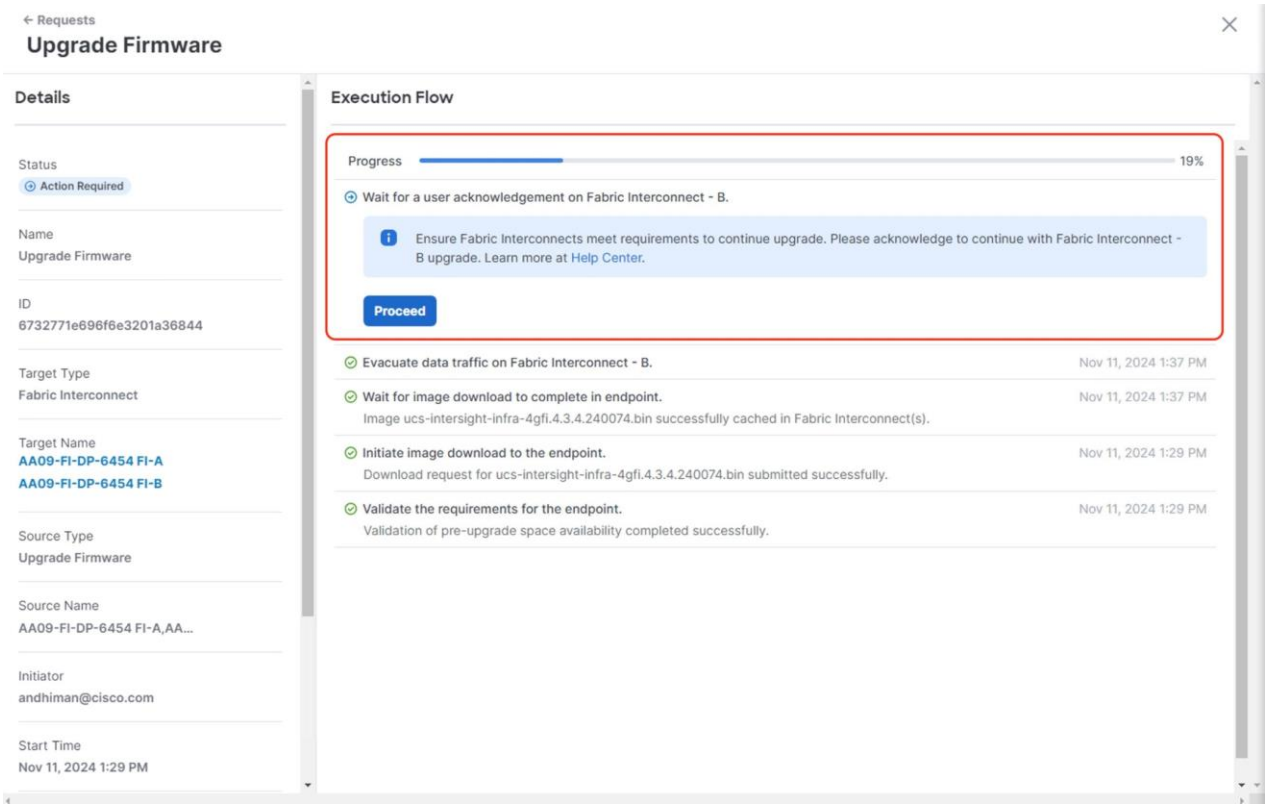


Step 4. On the Summary page, confirm the firmware to be upgraded and click Upgrade.

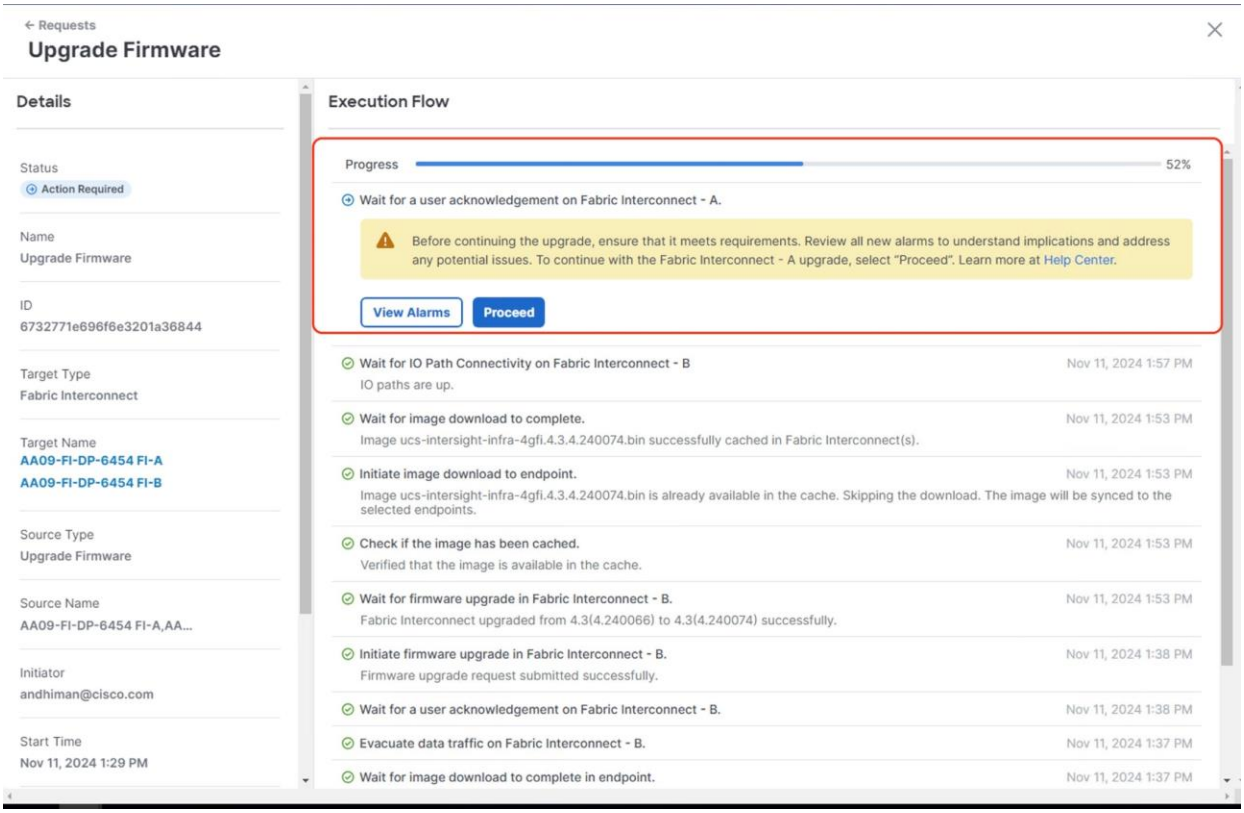


Step 5. Monitor the upgrade process and wait for it to complete.

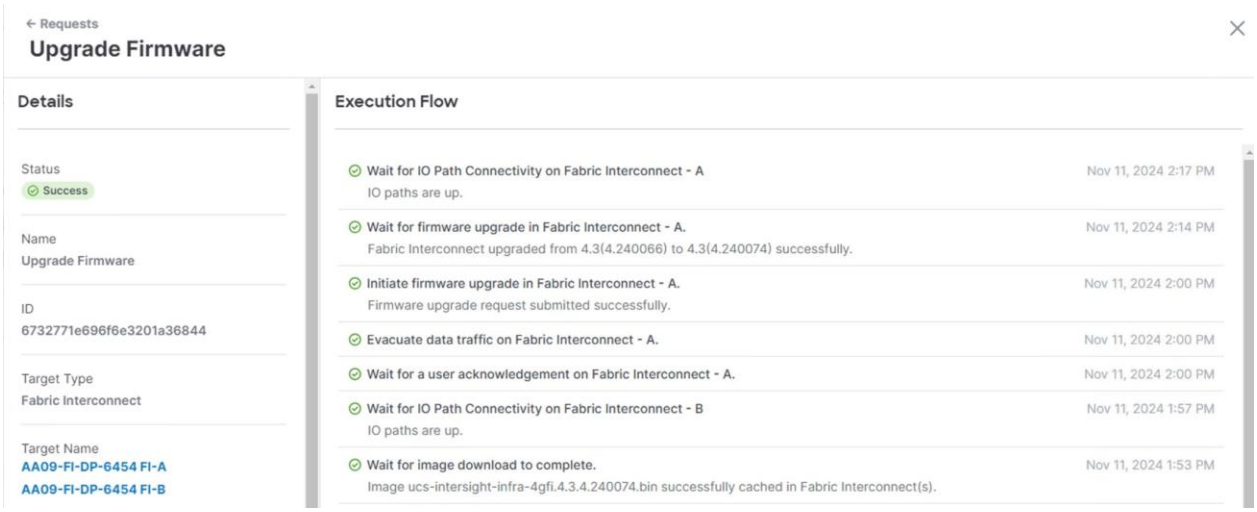
Step 6. When the Firmware downloads, acknowledge the Fabric Interconnect B upgrade, and click Continue.



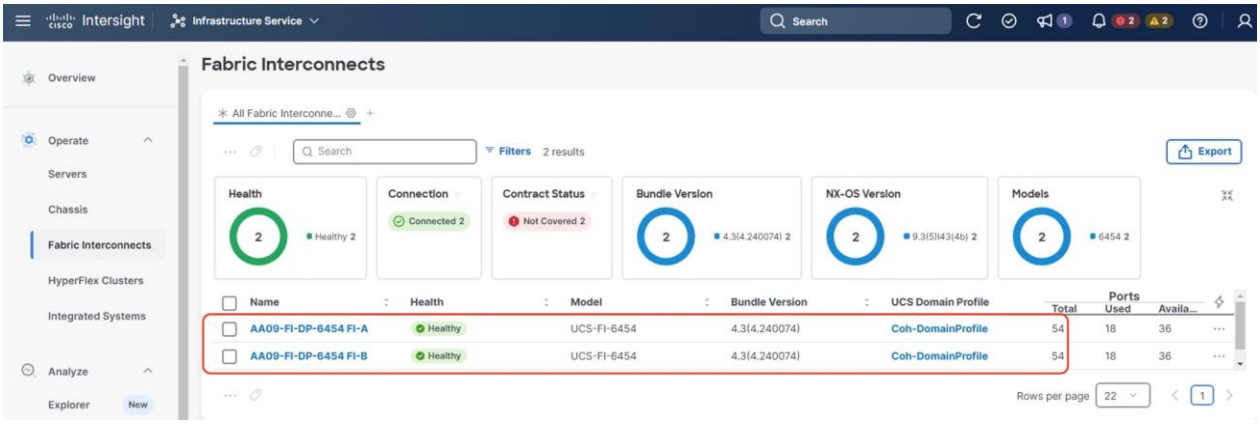
Step 7. When Fabric Interconnect –B is upgraded, acknowledge the alarms and Fabric Interconnect – A upgrade.



Step 8. Make sure the Firmware upgrade completed successfully.



Step 9. Verify the firmware upgraded on the Cisco UCS Fabric Interconnect.



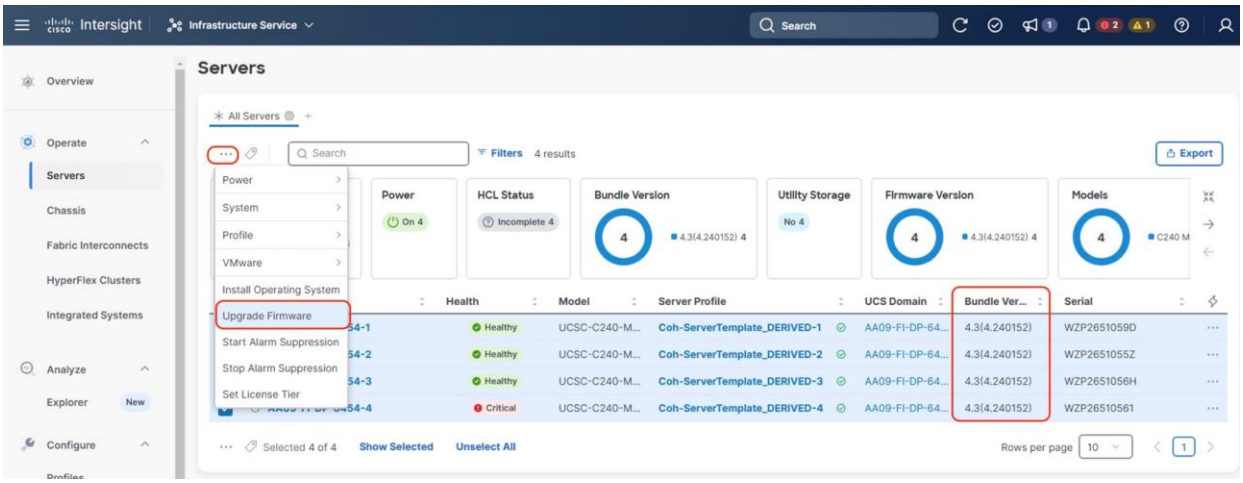
Rolling Upgrades (Node Firmware and Cohesity software)

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

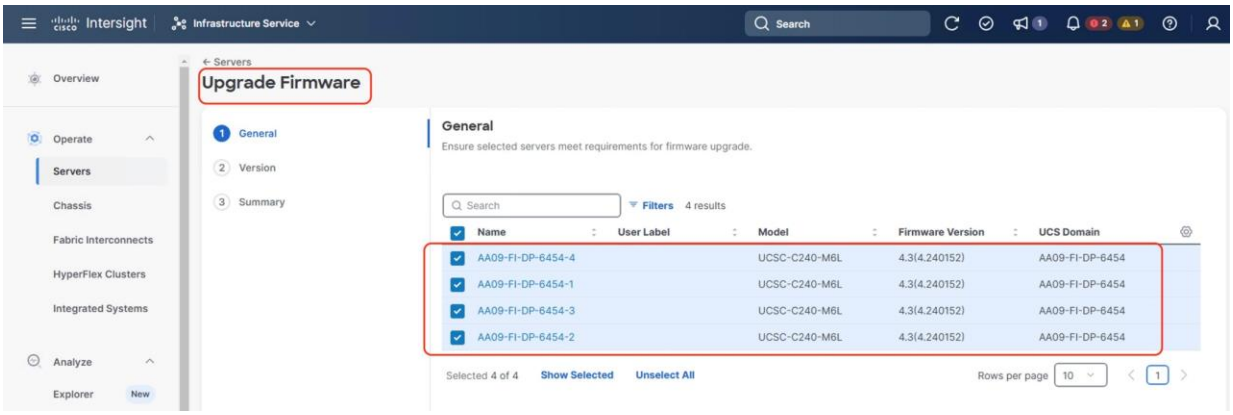
This procedure expands on the procedure to upgrade the firmware of Cisco UCS C-Series Cohesity certified nodes with Cohesity Cluster software upgrade.

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 https://Intersight.com, 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.

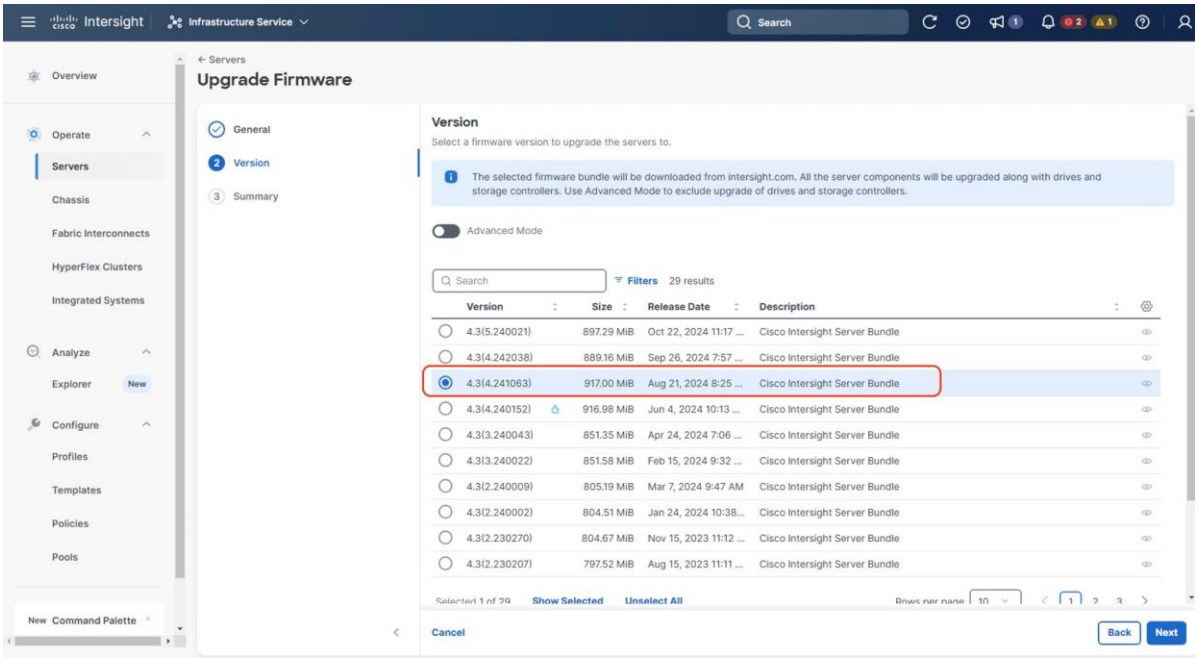


Step 2. Make sure all Cisco UCS C-Series nodes which are part of single Cohesity cluster are selected for upgrade. Click Next.

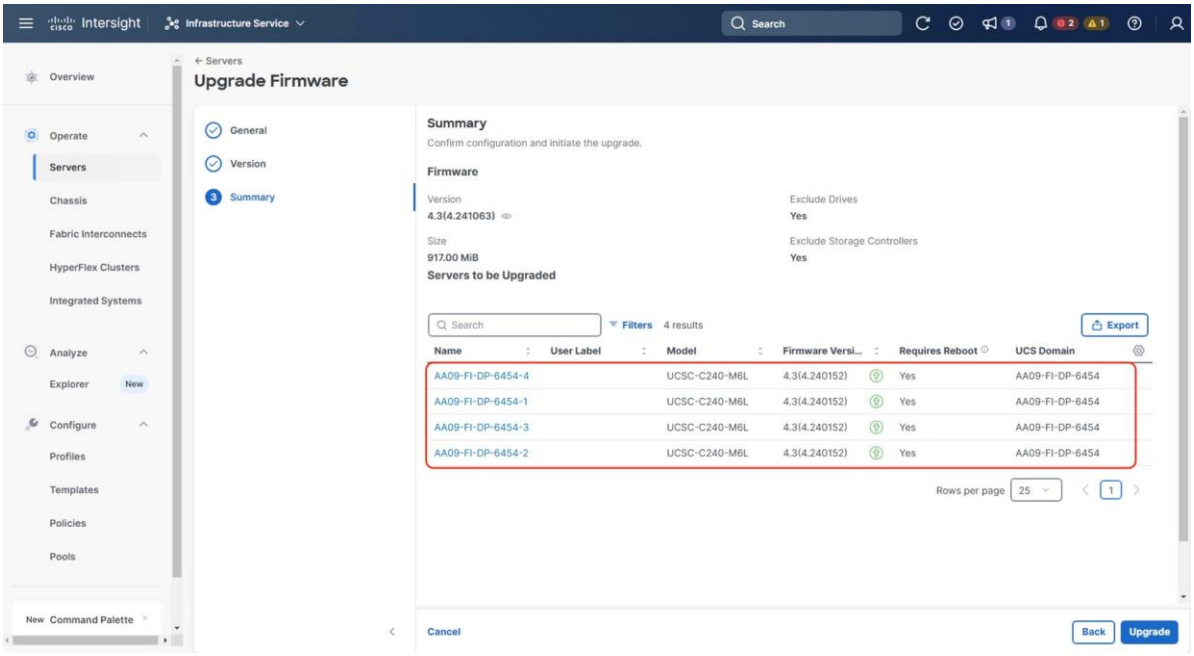


Step 3. Select the recommended Server Firmware version and click Next. At the time of publishing this guide, the suggested firmware was 4.3(4.240152). If the firmware upgrade does not require drive firmware updates, select Advanced Mode, and check the Exclude Drive option.

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.

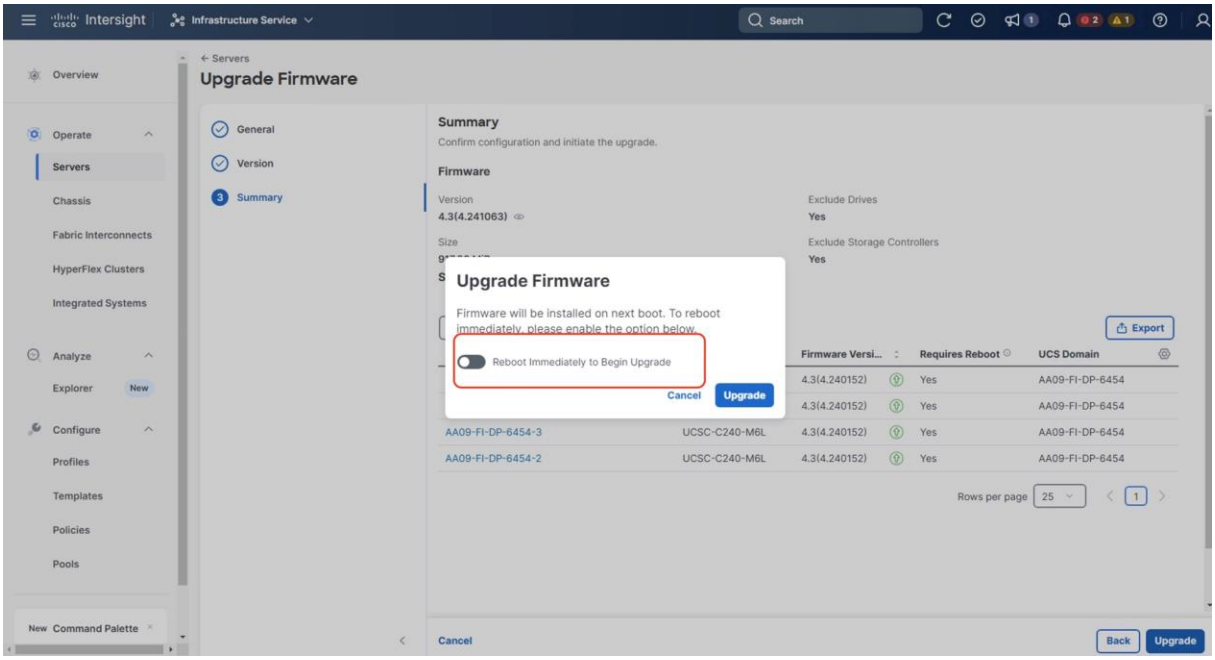


Step 4. Click Upgrade.

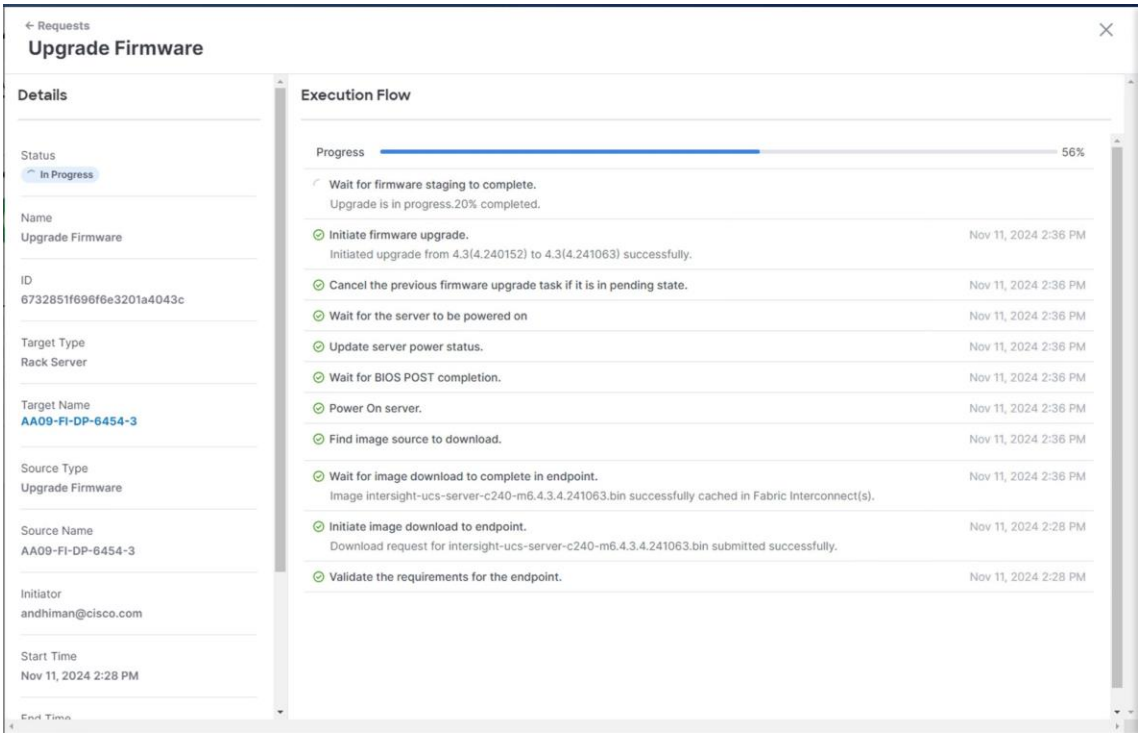


Step 5. Retain the Reboot Immediately to Begin Upgrade option as unselected. When the firmware is mounted and the reboot server message appears, start upgrading the Cohesity Cluster software which will ensure the serial reboots of each node (rolling reboots) and avoid any disruption of operations on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

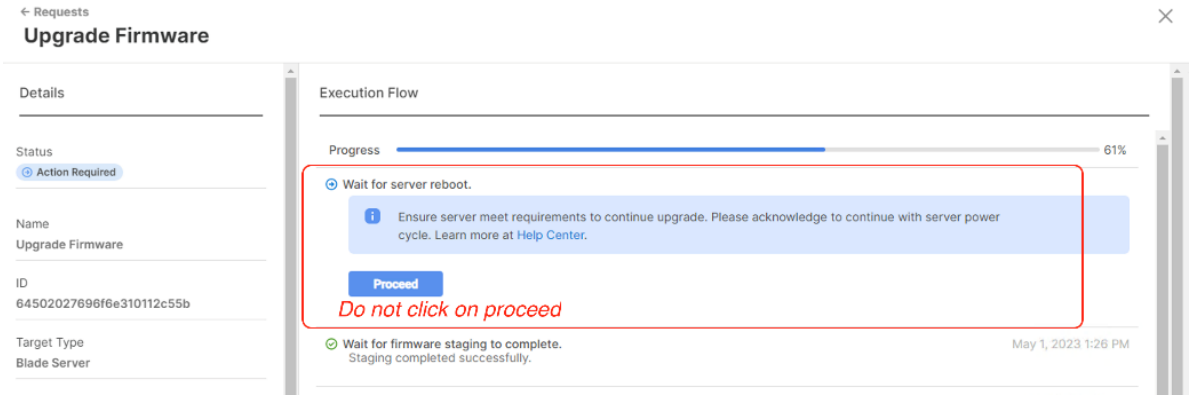
Step 6. Click Upgrade.

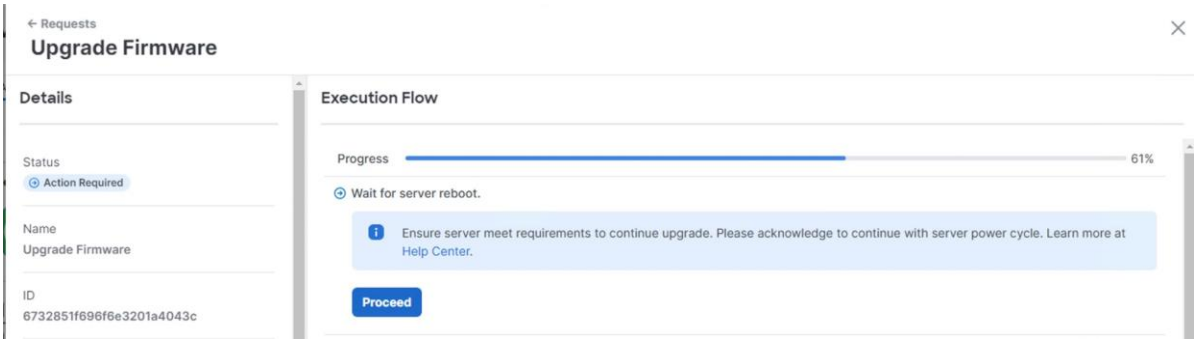


Step 7. The Firmware image is downloaded to the end point and staged to the respective node:



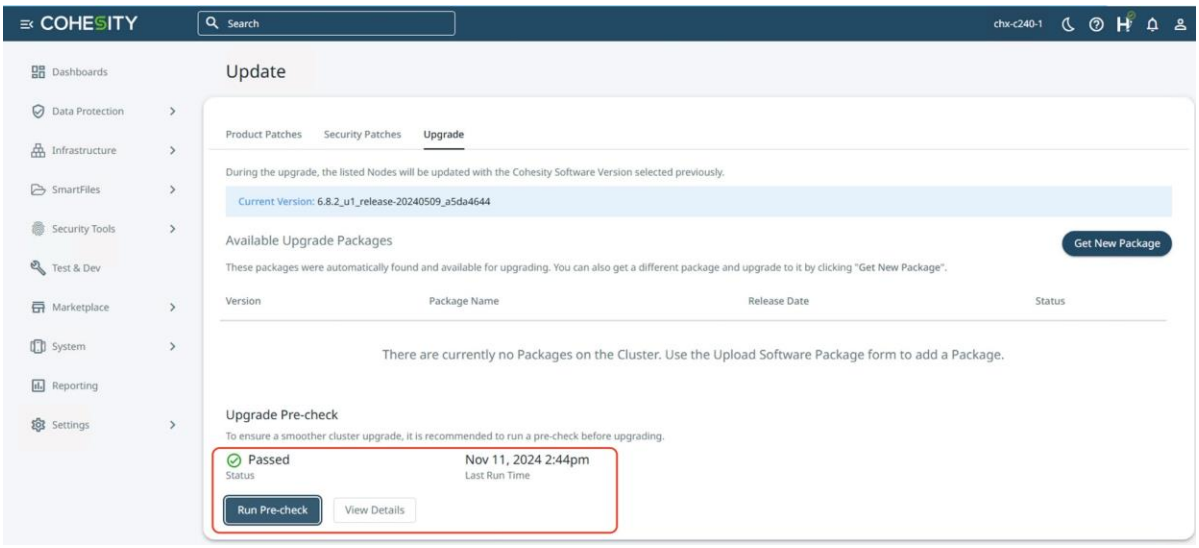
Step 8. Once the firmware staging completes, the Server Power cycle option is displayed, close the message, and do not click Proceed. Before proceeding to the next step, make sure all nodes are at this stage.



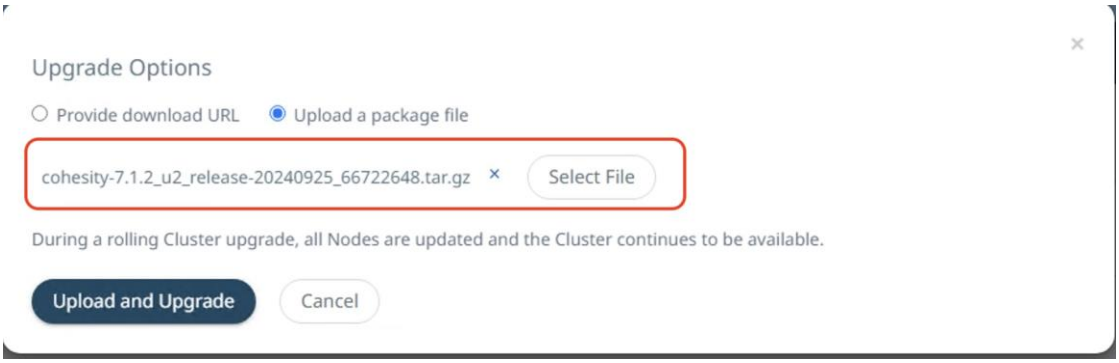


Step 9. Login to the Cohesity cluster dashboard and click Settings. Click Upgrade.

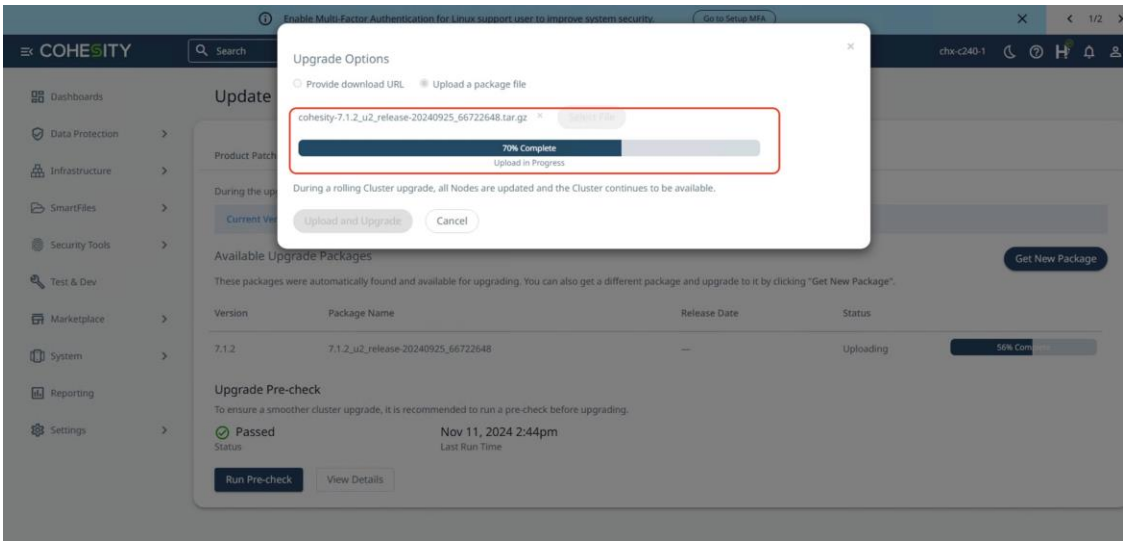
Step 10. Run a Pre-Check to ensure cohesity cluster is in a healthy state and compatible for upgrades.



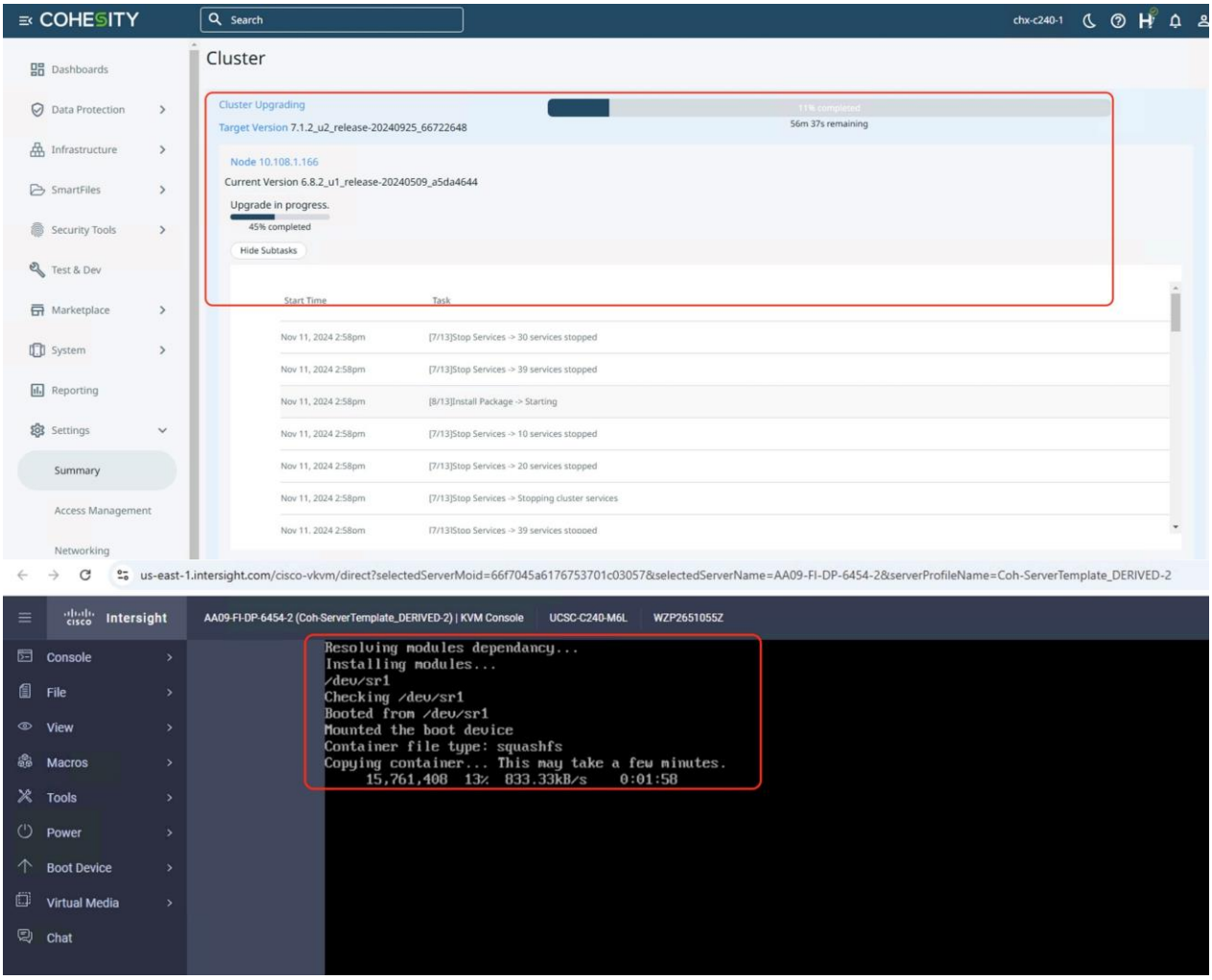
Step 11. Click on get New package, upload the latest version of Cohesity. At the time of writing this document cohesity was tested for upgrade to cohesity-7.1.2_u2_release-20240925_66722648. Click on upload and upgrade option.



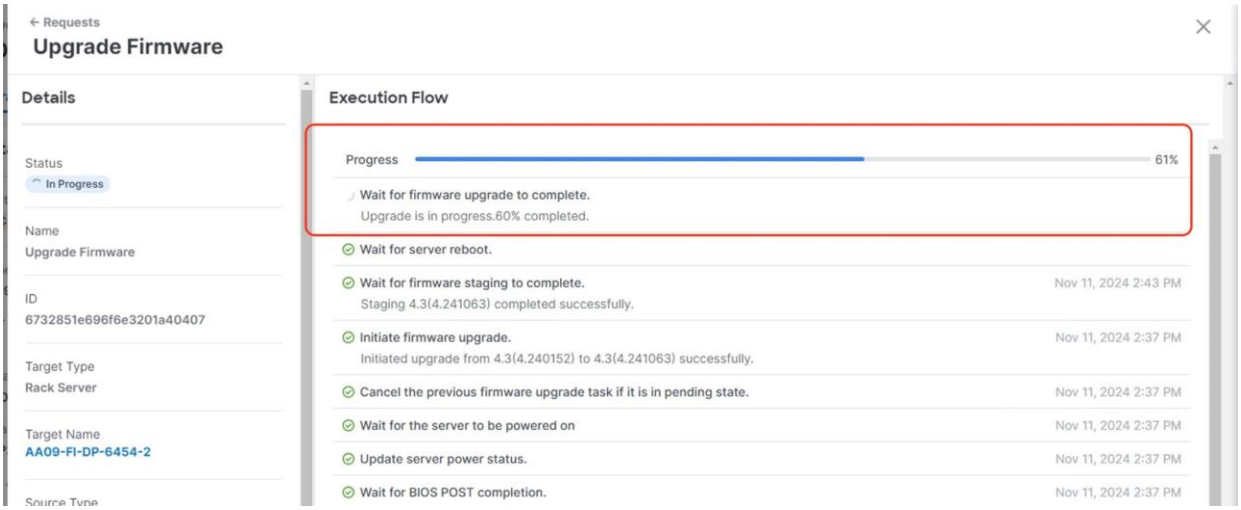
Step 12. This step of the upgrade process will take some time, about 20-30 minutes per node when the Cisco UCS C-Series nodes are rebooted and upgraded serially. It will take an additional 2-hours for the four node Cohesity Cluster rolling upgrade of the server firmware.



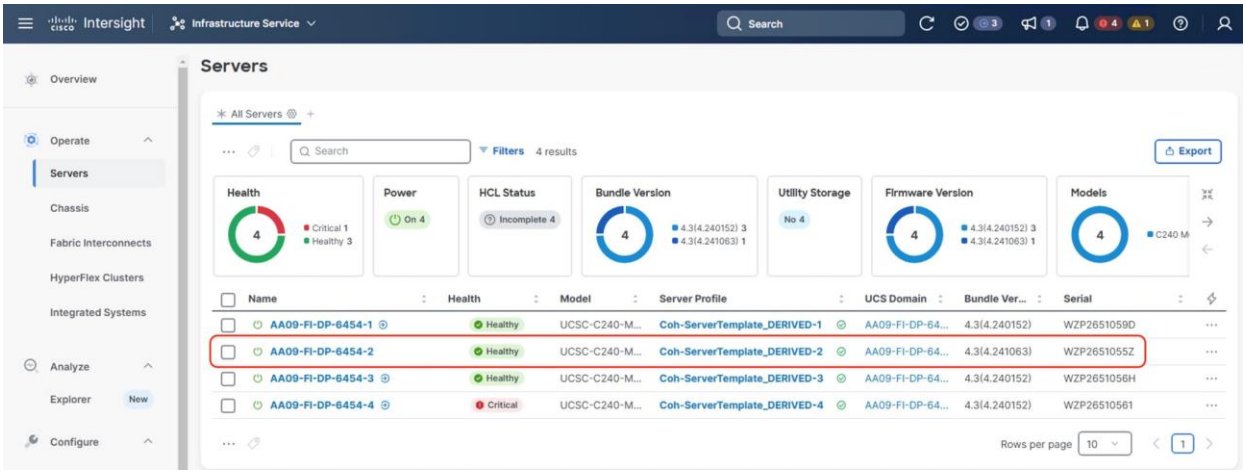
Step 13. During the Rebooting of Cohesity node executed through the Cohesity upgrade process, upgrade of Cisco UCS C-Series nodes is invoked through the staged UCS firmware from Intersight.

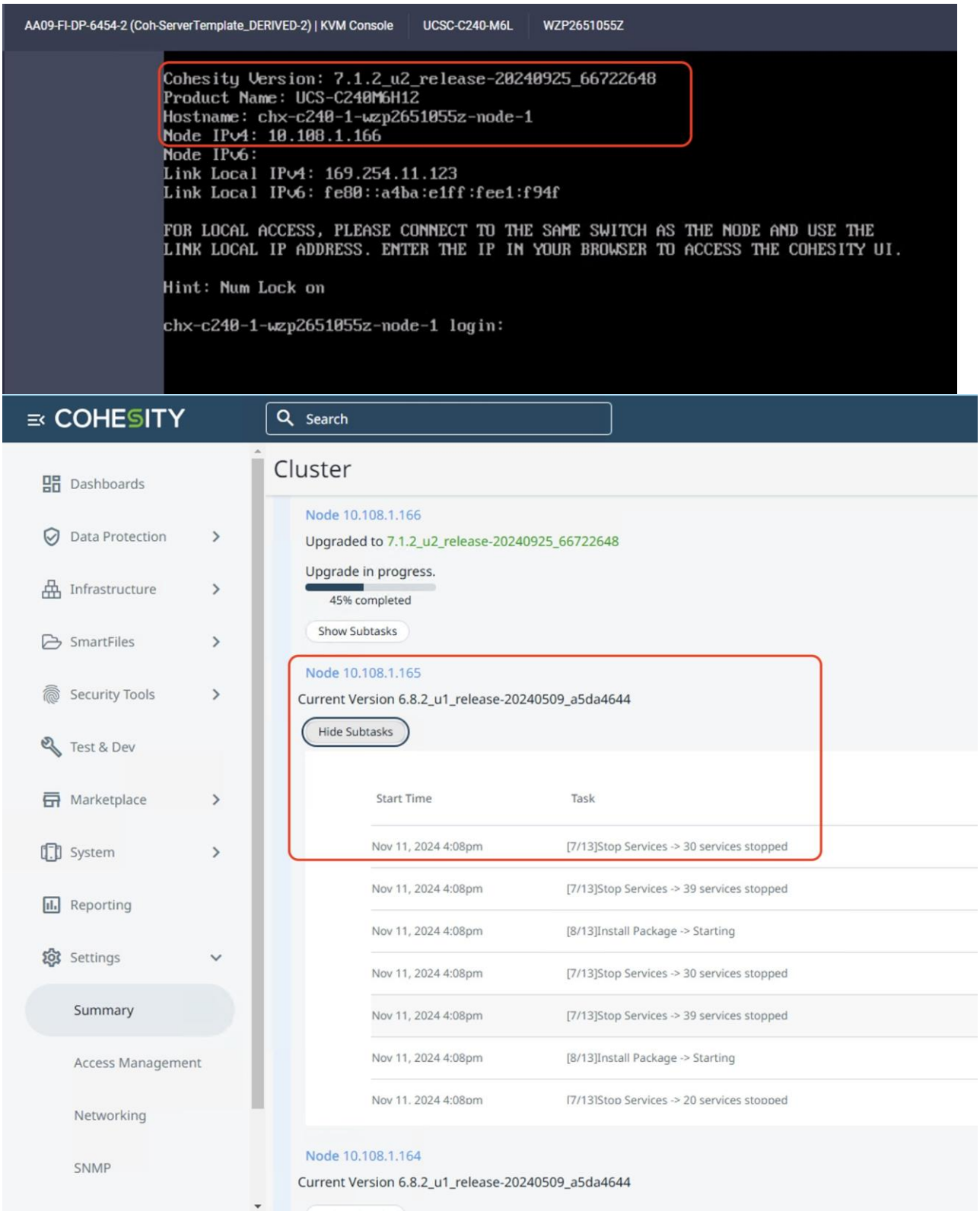


Step 14. You can also monitor the firmware upgrade status of the node with Cisco Intersight in Progress Request.

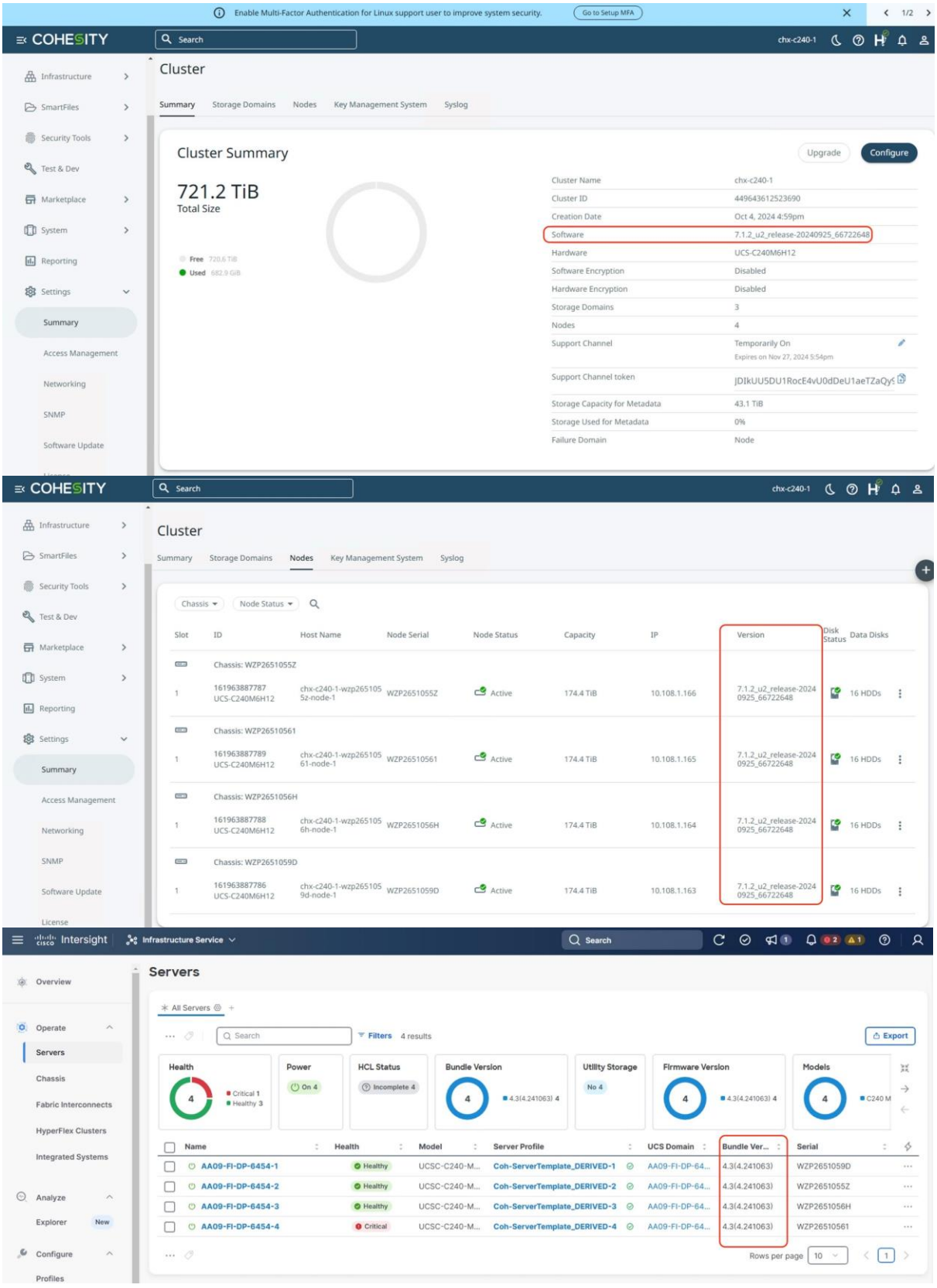


Step 15. The details of the firmware and software upgrade completing the first Cisco UCS C-Series node and the beginning of the upgrade procedure for the second Cisco UCS C-Series node initiated through the Cohesity Data Cloud is shown below:





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.



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.

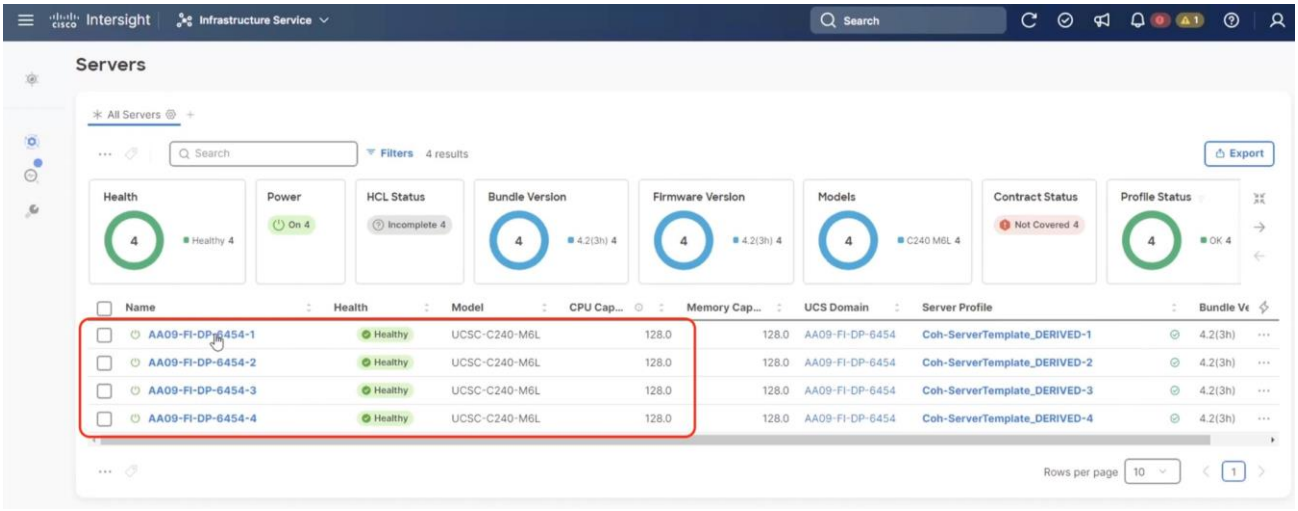
Note: Since the Cisco UCS C-Series node firmware upgrade requires a reboot, please initiate support of Cohesity to shut down the Cohesity cluster during the maintenance window.

This procedure is utilized in three key circumstances.

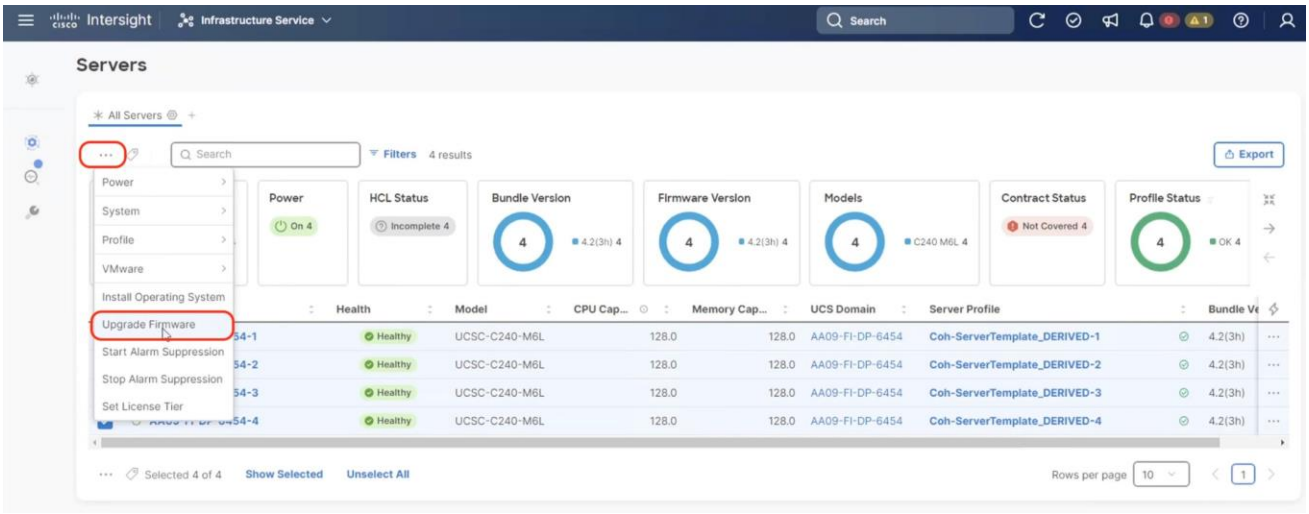
- Only the Cisco UCS C-Series node firmware requires an upgrade.
- You are comfortable with having a maintenance window for the Cohesity cluster downtime.
- Since the Rolling upgrade adds up to 20-30 minutes per node and is executed serially, it could be time consuming for Cohesity cluster with several 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 https://intersight.com and select the account registered to Cohesity C-Series nodes managed through Intersight.

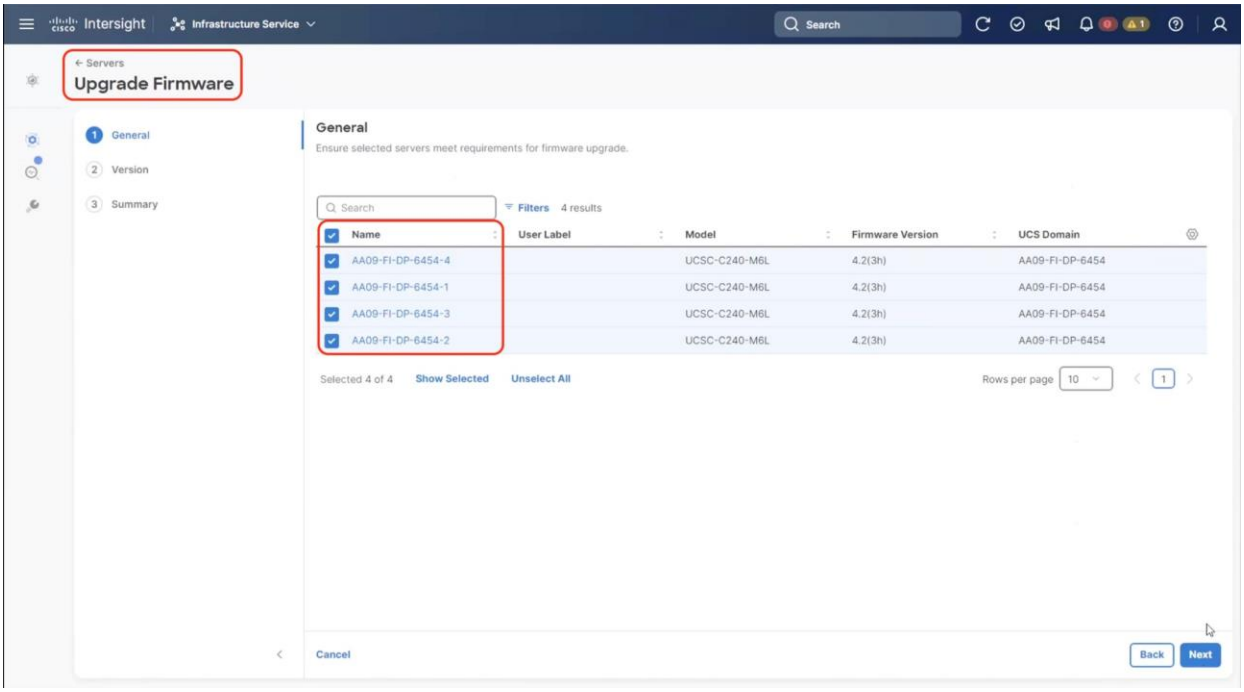
Step 2. Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster. Ensure Server Profile is successfully deployed to the Cohesity nodes.



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

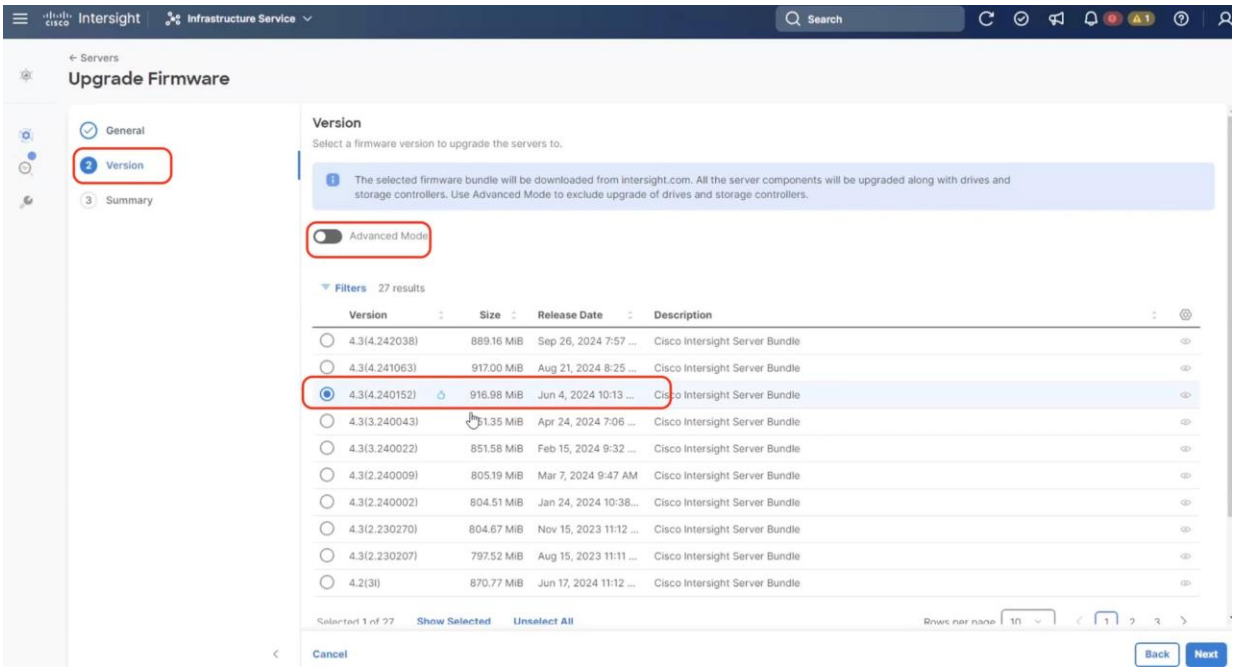


Step 4. Select Start Firmware upgrade and ensure the Cisco UCS C-Series nodes are selected. Click Next.

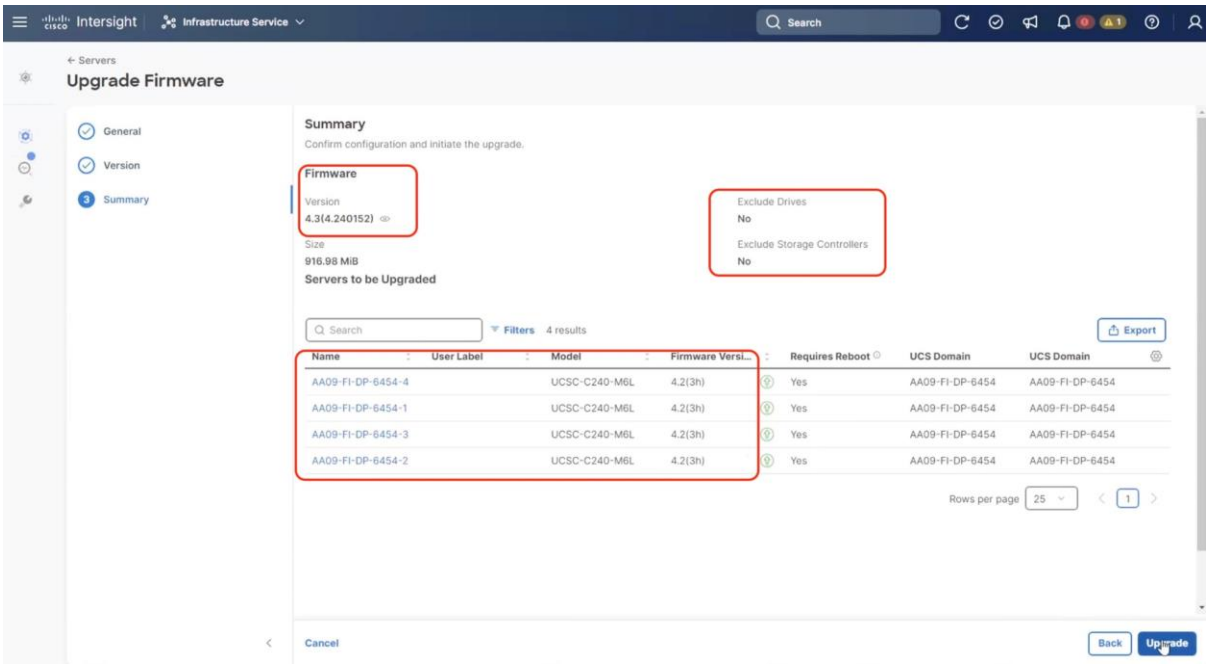


Step 5. Identify the recommended Firmware version. In general, the recommended sign is displayed on the firmware. Click Next.

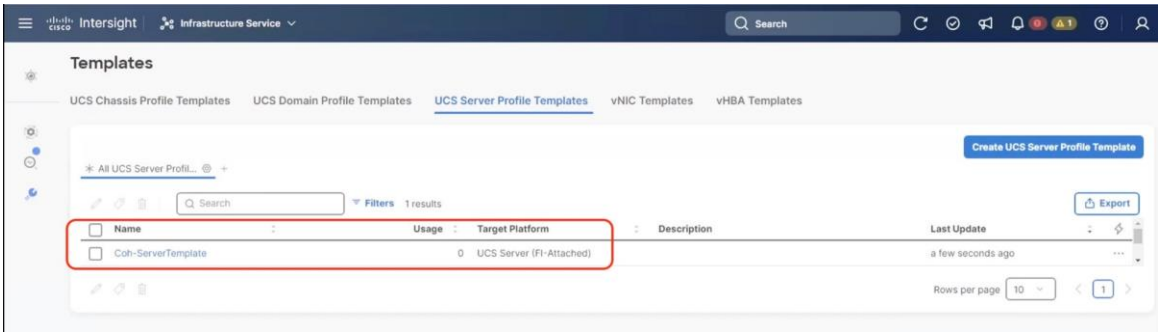
By default the drive and storage controller firmware is also upgraded. To avoid drive failure and improve the resiliency of drives, it is recommended to upgrade drive firmware. Drives can be excluded from firmware upgrades, through ‘Advanced Mode’.



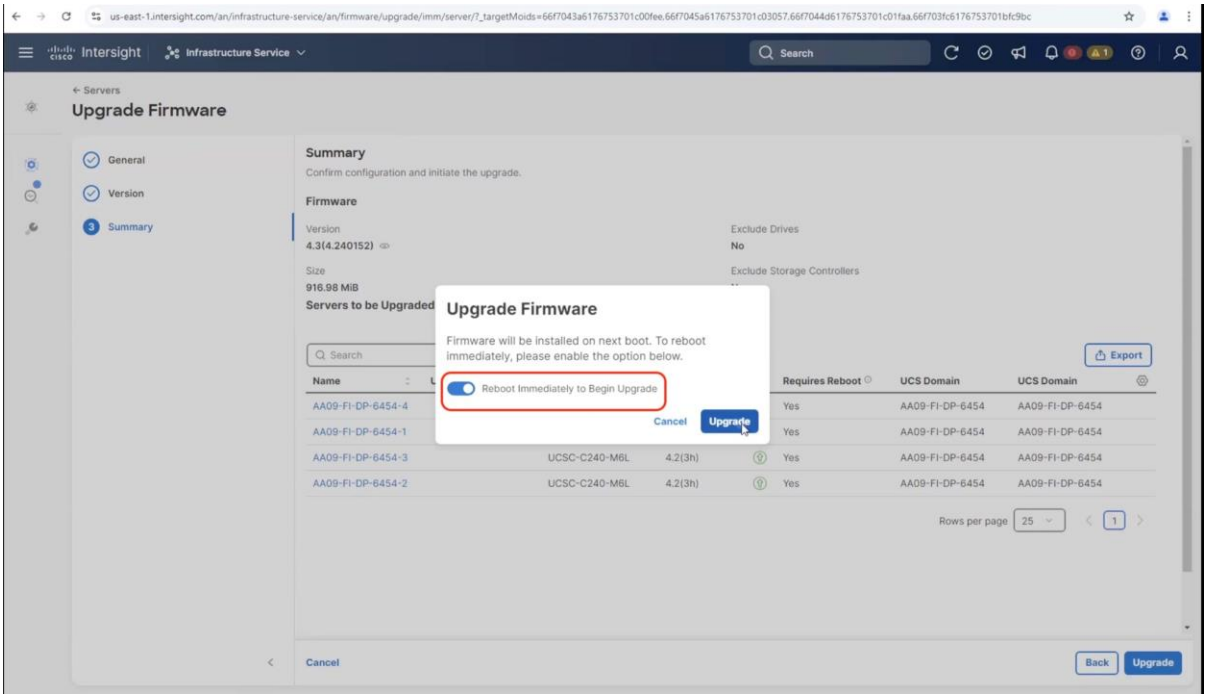
Step 6. Confirm the firmware version for upgrades on Cohesity nodes. Click Upgrade.



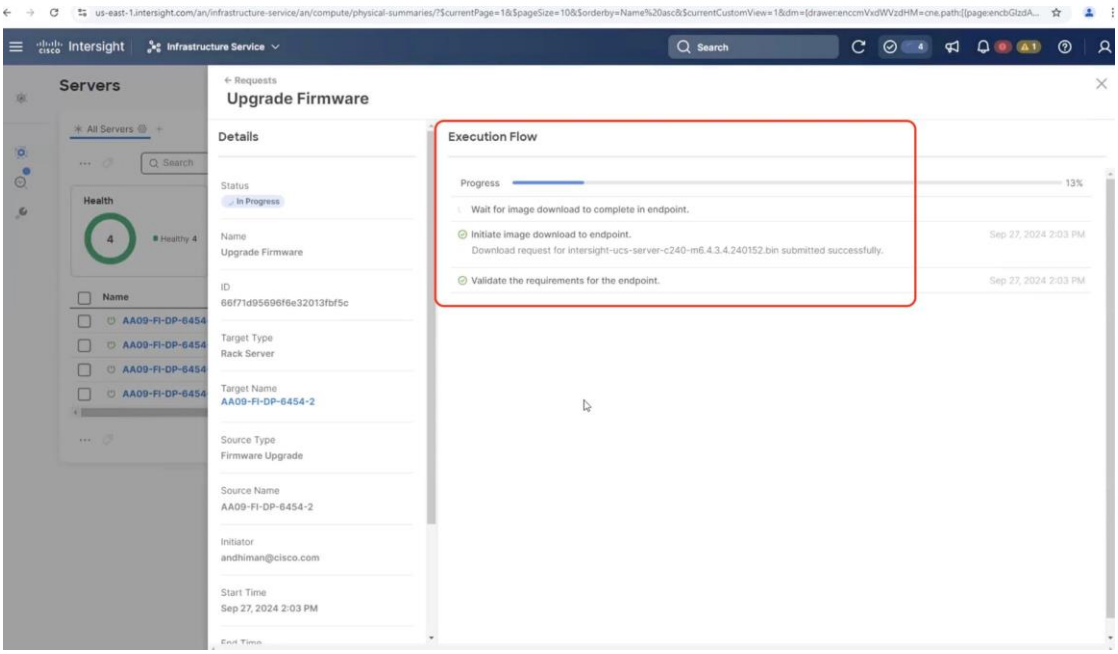
Step 7. On the Upgrade Firmware confirmation screen, enable Reboot Immediately to Begin Upgrade.



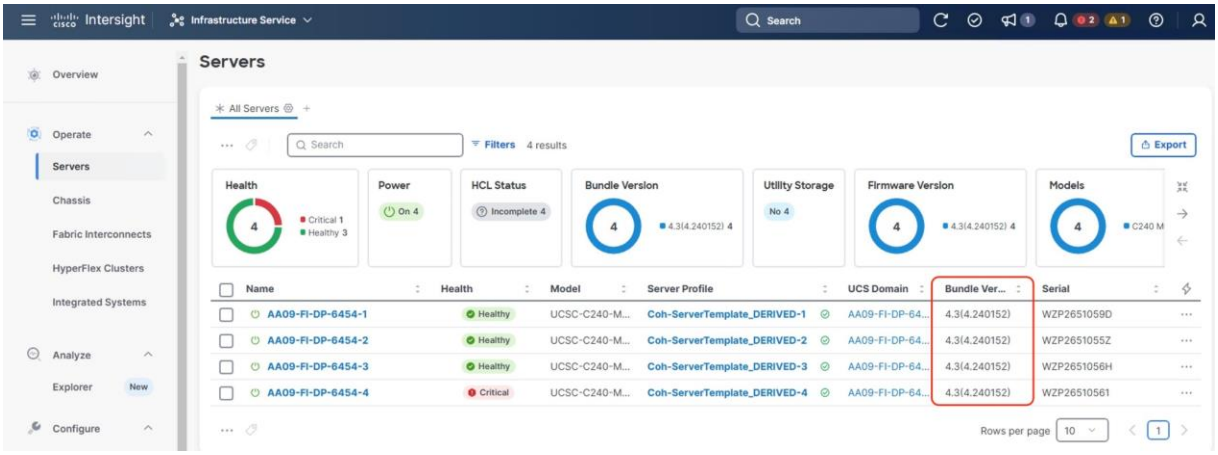
Step 8. Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster.



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



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



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
- Restore SQL Server with Cohesity File Based Protection Group

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 TPC 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 Cohesity documentation on protection of Microsoft SQL Server

Backup the SQL Server with Cohesity File-based Protection Group

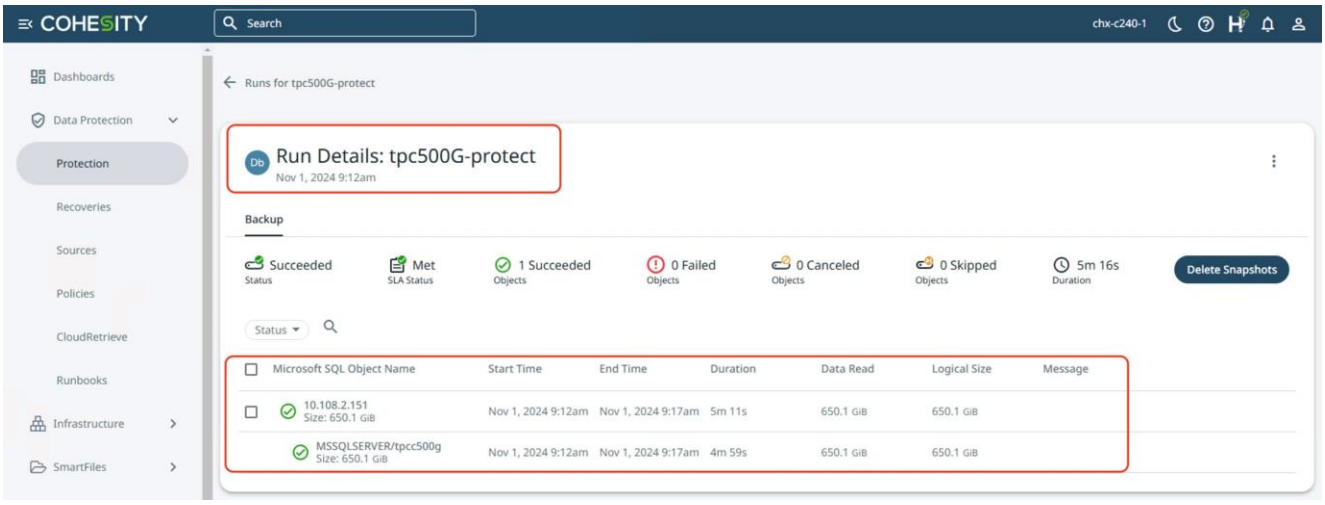
The objective of this test is to demonstrate protection of a large SQL server database deployed on a single AHV based VM on Cisco Compute Hyperconverged with Nutanix. Cohesity File-based Protection Groups protect only the specific MS SQL databases that you select.

Table 16 lists the test configuration details.

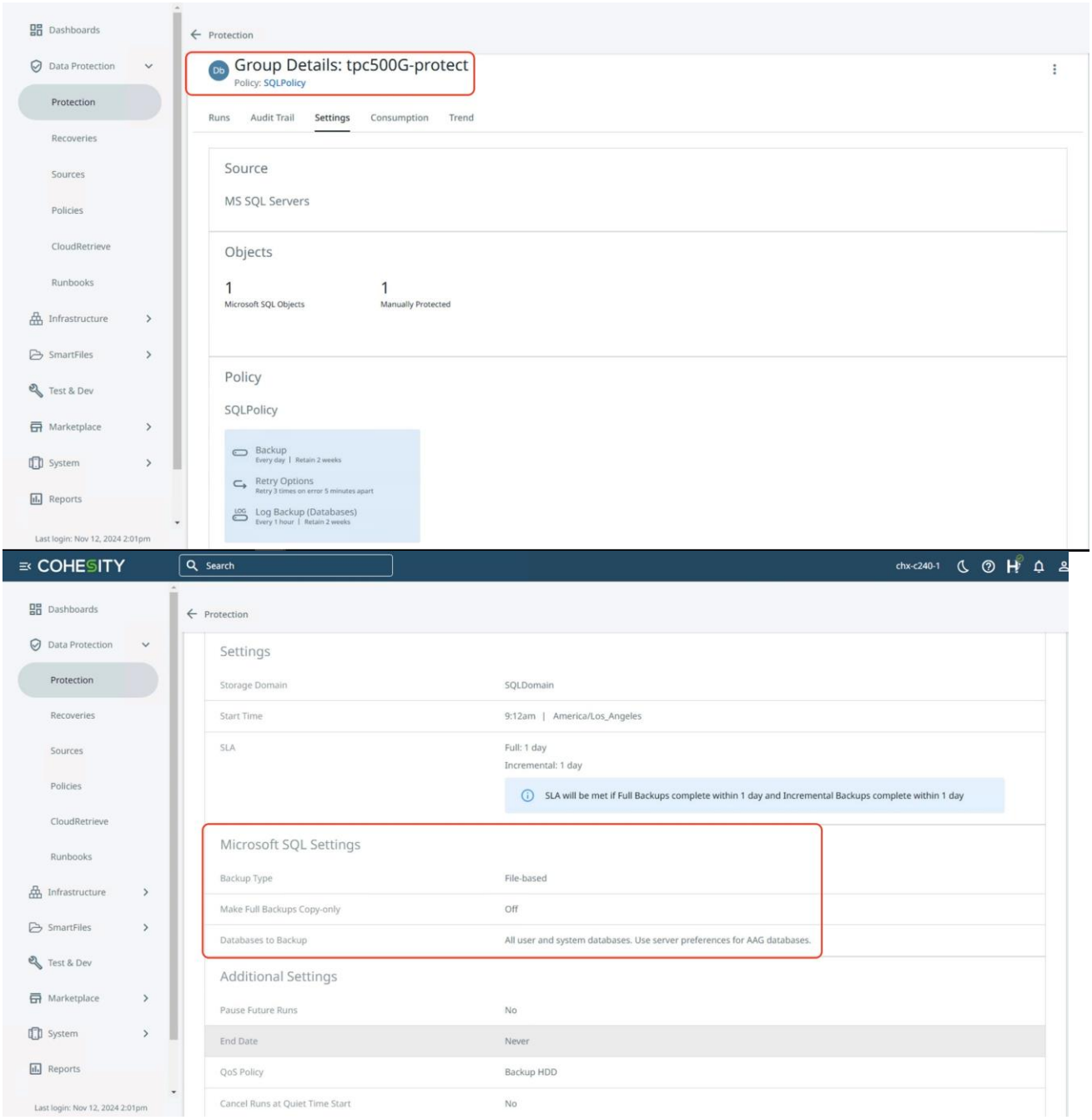
Table 16. File Based Backup configuration details

Component	Details
vCPUS	1
No of Cores	8
Memory	32GB
Storage Layout	1x 120G disk for Widows OS + SQL Binaries + System Databases Following disks are used for storing 500G user/test database 4x 200G disks for user Database data files 2x 300G disks for TempDB data files 1x 600G disk for user database and TempDB T-Log files 1x 800G disks for backup
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.



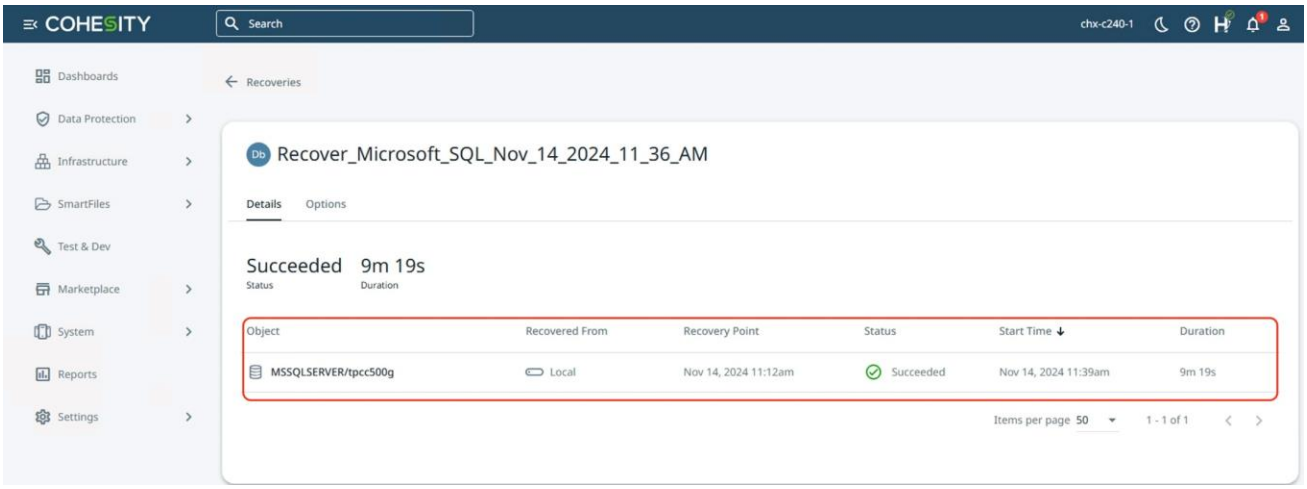
Cohesity protection group setting for the backup job is shown below:



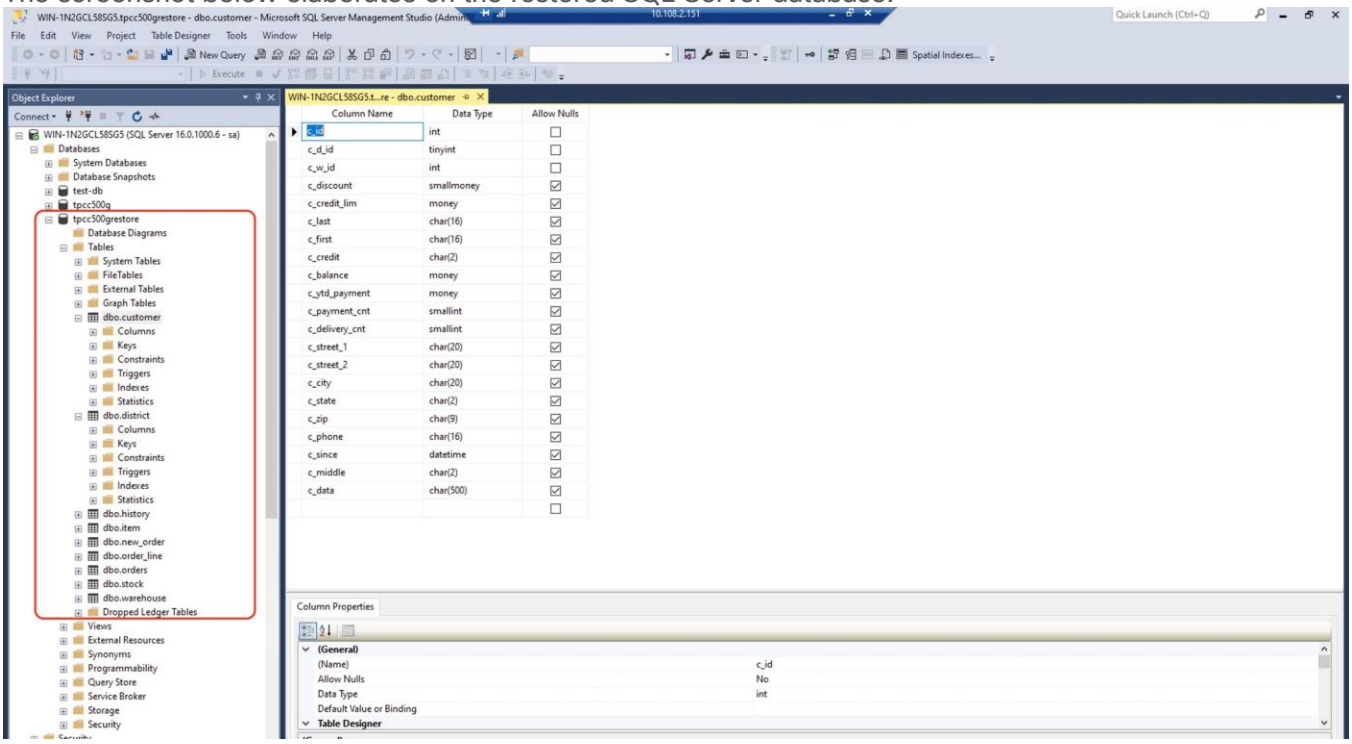
Restore SQL Server with Cohesity File Based Protection Group

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:



The screenshot below elaborates on the restored SQL Server database:



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-Nodes	Cisco UCS C240 M6 LFF Rack Server	12 TB	3.2 TB
		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 Rack Server	8 TB	1920 GB
		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 AI 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

Table 18 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.

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

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

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: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/cisco_nutanix_sql.html

Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Mode: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/CCHC_Nutanix_ISM.html

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-install-guide.html

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

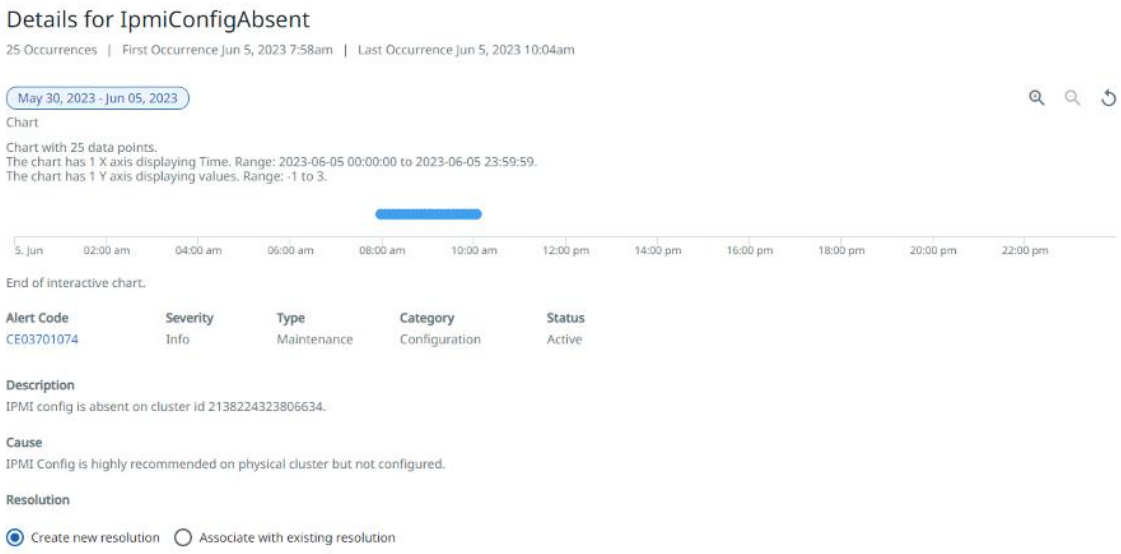
Cohesity Guide for Backup of Microsoft SQL Server: https://docs.cohesity.com/6_8_1/Web/UserGuide/Content/MSSQL/SQLProtection.htm?tocpath=Databases%7CMicrosoft%20SQL%20Server%7CBackup%20Microsoft%20SQL%20Server%7C_____0 and https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-Protect-SQL-Server-Databases.pdf

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:



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-install-guide.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-compute-solutions/intersight_cohesity_xseries_ansible/

Feedback

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

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**.