

Design and Deployment Guide Cisco Public

Rubrik CDM on Cisco UCS C-Series Rack Systems

Design and Deployment Guide

Published: March 2024



In partnership with:



About the Cisco Validated Design Program

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

Executive Summary

Digital transformation has brought significant benefits to organizations, including increased agility and flexibility, but it has also led to a rise in cyber attack vectors. 66 percent of organizations were hit with ransomware within the last year, according to a 2022 <u>Sophos survey</u>. The widespread adoption of cloud services and Software-as-a-Service (SaaS) applications has expanded the attack surface, making it more challenging to manage and secure data. Additionally, the increased use of mobile devices and remote work have made it easier for cybercriminals to launch attacks from anywhere, at any time.

Rubrik Security Cloud is the leading data security platform built upon a unique backup architecture that secures data. Rubrik is designed with zero trust principles to incorporate a logical air gap, secure protocols, native immutability, encryption, and access controls. The principal economic benefit of Rubrik is reduced costs associated with combating cyber threats. Data Protection safeguards data with secure backups. Data Threat Analytics makes it easy to monitor data risk and investigate threats faster. Data Security Posture helps to proactively reduce data exposure risk. Cyber Recovery helps restore business operations faster.

Rubrik Security Cloud on Cisco UCS C-Series systems, managed through Cisco Intersight provides an appliance-like deployment model. Business resilience, agility, flexibility, and orchestration of resources at scale across the edge, public, and private cloud environments are a key value differentiators of this joint solution.

This Cisco Validated Design and Deployment Guide provides prescriptive guidance for the design, setup, configuration, and ongoing use of the Rubrik Security Cloud on the Cisco UCS C-Series Rack System. Together, Cisco and Rubrik deliver the unified computing and Zero Trust Data Security capabilities you need to meet the demands for increased development agility and management of distributed environments, while ensuring your data is resilient against cyber-attacks, malicious insiders, and operational disruptions.

Solution Overview

This chapter contains the following:

- Audience
- Purpose of this Document
- Solution Summary

With Rubrik, organizations can be confident that their critical data is safe from deletion, compromise, or encryption. This is because air-gapped, immutable, access-controlled backups enable organizations to withstand cyberattacks, malicious insiders, and operational disruptions. Data is stored in an immutable format and cannot be read, modified, or deleted. Additionally, data is encrypted in-flight and at rest, and backup data is stored in a purpose-built append-only file system.

Lastly, backed up data is logically air-gapped so it's offline and not accessible through standard network protocols. System interfaces are secure, role-based, least privileged, and protected by multifactor authentication (MFA) to further reduce the risk of intrusion.

Data Resilience services include:

- Enterprise Data Protection to keep your enterprise data safe from attacks or disasters.
- Cloud Data Protection to ensure your cloud data is secure from compromise.
- SaaS Data Protection to secure your SaaS application data with automated protection.
- Unstructured Data Protection to protect, monitor, and rapidly recover unstructured data at petabytescale.

The Rubrik CDM joint solution with Cisco UCS, provides customers with a solution that is easy to deploy, manage and expand as per the growing demands of data protection workloads. Besides the best in class cyber security Rubrik solution, the security of the Cisco UCS platform starts with Cisco's value chain or supply chain security, through a layered approach to the manufacturing facilities – all to ensure that there's no tampering happening while the platform is being built. Cisco UCS products are designed and tested to Cisco's rigorous security framework, using the latest technologies for prevention, and following comprehensive cybersecurity programs.

The Cisco Intersight platform uses a layered security architecture that builds on industry-standard security technologies. It also encrypts data, complies with strict Cisco security and data handling standards, and separates management and IT production network traffic for additional isolation. As a result, you can have confidence that your cloud-based systems management platform offers the strong security you require.

Audience

The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, IT engineers, partners, and customers who are interested in learning about and deploying a secure, and scalable data protection solution for backup and recovery of workloads.

Purpose of this Document

This document describes the design, configuration, deployment steps for the Rubrik CDM on Cisco UCS C-Series platform managed through Cisco Intersight.

Solution Summary

This solution provides a reference architecture and validated deployment procedure for the Rubrik CDM on Cisco UCS C-Series platform managed through Cisco Intersight.

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 customers to get more value from hybrid IT investments by simplifying operations across on-prem and their 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.
- Rubrik Security Cloud Rubrik Security Cloud gives organizations a single place to secure their data wherever it lives—across enterprise, cloud, and SaaS applications.

Figure 1 illustrates the deployment overview of the Rubrik Security Cloud on Cisco UCS.



Figure 1. Solution Overview

Technology Overview

This chapter contains the following:

- <u>Cisco Intersight Platform</u>
- <u>Cisco UCS C240 M6 Large Form Factor (LFF) Rack Server</u>
- Rubrik Security Cloud

These components deployed in this solution are configured using best practices from both Cisco and Rubrik to deliver an enterprise-class data protection solution deployed on Cisco UCS C-Series Rack Servers. The upcoming sections provide a summary of the key features and capabilities available in these components.

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 HyperFlex, 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 customers 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 customers 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.

In this solution, Cisco Intersight provides a single global SaaS platform allowing management of Cisco C-Series Rack servers running the Rubrik CDM deployed across multiple data centers, edge, or remote sites. The life cycle management capabilities that Cisco Intersight offers allows easier Day 0 deployment, continuous monitoring of infrastructure, proactive RMAs, firmware upgrades and easier expansion of Rubrik CDM Clusters.

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.

Cisco Intersight Assist

Cisco Intersight Assist helps you add endpoint devices to the Cisco Intersight platform. A datacenter could have multiple devices that do not connect directly with the platform. Any device that the Cisco Intersight platform supports but does not connect with directly must have a connection mechanism, and Cisco Intersight Assist provides it. In FlashStack, VMware vCenter and Pure Storage FlashArray connect to the Intersight platform with the help of the Cisco Intersight Assist virtual machine.

Cisco Intersight Assist is available within the Cisco Intersight virtual appliance, which is distributed as a deployable virtual machine contained within an OVA file format. Later sections in this paper have more details about the Cisco Intersight Assist virtual-machine deployment configuration.

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, see:

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

For more details and specification, go to: <u>https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m6-lff-specsheet.pdf</u>

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

1 Con 0		
-their Exco		

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 this configuration with Rubrik CDM, Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM with deployed on Cisco UCS C240 M6 LFF server.

Cisco UCS VIC 1467

The Cisco UCS VIC 1467 is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for Cisco UCS C-Series M6 Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE. The card can present PCle standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBA. For

more details, go to: <u>https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/unified-</u> <u>computing-system-adapters/datasheet-c78-741130.html</u>



Figure 4. Cisco UCS VIC 1467

Figure 5. Cisco UCS VIC 1467 Infrastructure



Cisco UCS 6400 Fabric Interconnects

The Cisco UCS fabric interconnects provide a single point for connectivity and management for the entire Cisco UCS system. Typically deployed as an active-active pair, the fabric interconnects of the system integrate all components into a single, highly available management domain that Cisco UCS Manager or the Cisco Intersight platform manages. Cisco UCS Fabric Interconnects provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, storage-area network (SAN), and management traffic using a single set of cables (Figure 6).

```
Figure 6. Cisco UCS 6454 Fabric Interconnect
```

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

Rubrik Security Cloud

Cyberattacks are increasing in frequency and sophistication. Despite large investments in infrastructure security tools, bad actors are finding their way through to the data. And they know legacy backup tools are vulnerable, so they are increasingly targeting backup data. When a cyberattack takes down data, it takes down businesses. It's time for a new approach. One that marries the investments made in infrastructure security with data security.

Rubrik is on a mission to secure the world's data. With Rubrik Security Cloud, you can automatically protect data from cyberattacks, continuously monitor data risks, and quickly recover data and applications across the enterprise, in the cloud, and in SaaS applications.

• Data Protection: Keep Data Readily Available

Ensure data integrity and availability with automated, secure, and access-controlled backups that are designed to withstand cyberattacks, malicious insiders, and operational disruptions.

• Data Threat Analytics: Monitor Data Risk and Investigate Faster

Continuously monitor for threats to data, including ransomware, data destruction, and indicators of compromise.

• Data Security Posture: Proactively Reduce Risk of Data Exposure

Proactively identify and monitor sensitive data exposure and use intelligent insights to mitigate risks to data.

Cyber Recovery: Restore Business Operations Faster

Quickly return to business as usual within hours or days, not weeks or months. Orchestration and quarantining enable you to contain threats and rapidly recover your apps, files, or objects while avoiding malware reinfection.



Architecture and Design Considerations

This chapter contains the following:

- Deployment Architecture for Cisco UCS C240 with Rubrik
- Network Bond Modes with Rubrik and Fabric Interconnect Managed Systems
- Licensing
- <u>Physical Components</u>
- <u>Software Components</u>

Deployment Architecture for Cisco UCS C240 with Rubrik

The Rubrik CDM 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 Rubrik CDM. The entire deployment is managed through Cisco Intersight.

Each Cisco UCS C240 M6 LFF node is equipped with:

- 2x Intel 5318N 2.1GHz/150W 24C/36MB DDR4 2667MHz
- 384 GB DDR4 memory
- 2x 240GB M.2 card managed through M.2 RAID controller, for Rubrik operating system
- 1x 1.6 TB NVMe
- 12x 12TB,12G SAS 7.2K RPM LFF HDD (4K) managed through 1x Cisco M6 12G SAS HBA

Figure 7 illustrates the deployment architecture overview of Rubrik on Cisco UCS C-Series nodes.

Figure 7. Deployment Architecture as captured through Cisco Intersight

≡	diale Inters	sight 🎝	a Infrastructure Service 🗸	Q Search	0 4 0	ଡ ନ
.@.	Overview		Fabric Interconnects AA09-FI-DP-6454 FI-A Ø Heatthy			Actions -
0	Operate Servers	^	General Inventory Connections UCS Domain Profile Topology			
	Chassis		AA09-FI-DP-6454 FI-A	Last Refresh Tin	ne la few seconds age	o Refresh
	Fabric Intercon	nects				82
	HyperFlex Clush	ters				K 3
	Integrated Syst	ems		19070309090503090 2003020 2007020		-
Q	Analyze	^	AA03-FLDP-4643 FLA 🗶 🛇	AA09-FI-DP-6654 FI-B 🥥 🗇		• +
	Explorer	New				
,e	Configure	^				(
	Profiles		Y Y	Y Y		Q
	Templates					0
	Policies		AA09-FLDP-665-L 🔮 🕜 🛛 AA09-FLDP-665-L 🧶 🛇	AA09-FI-DP-6454-3 🥥 🕜 AA09-FI-DP-6454-4 🔮 💮		
	Pools					

Figure 8 illustrates the cabling diagram for Rubrik on the Cisco UCS C-Series Rack Servers.



Figure 9 illustrates the cabling topology as captured through Cisco Intersight.

Figure 9. Cabling topology as captured through Cisco Intersight



The reference hardware configuration includes:

- Two Cisco Nexus 93360YC-FX Switches in Cisco NX-OS mode provide the switching fabric.
- Two Cisco UCS 6454 Fabric Interconnects (FI) provide the chassis connectivity. One 100 Gigabit Ethernet port from each FI, configured as a Port-Channel, is connected to each Cisco Nexus 93360YC-FX.
- Four (4) Cisco UCS C240 LFF nodes. Each node is equipped with Cisco UCS 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. Port 1-2 are connected to Server ports on Fabric Interconnect A and Port 3-4 are connected to Server ports on Fabric Interconnect B.
- Cisco Intersight as the SaaS management platform for Cisco UCS Fabric Interconnects and Cisco UCS C-Series Rack Servers.

Note: Do not connect port 1 of the VIC 1467 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.

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

Network Bond Modes with Rubrik and 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 and Cisco 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 UCS Fabric Interconnects. This type of configuration is unsupported.

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

Cisco UCS Servers with Linux Operating System and managed through fabric interconnects, support activebackup (mode 1), balance-tlb (mode 5) and balance-alb (mode 6). The networking mode in the Rubrik operating system (Linux based) deployed on Cisco UCS C-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-bladeservers/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.

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

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

- Configuration of Domain and Server Profiles for Rubrik on Cisco UCS C-Series Rack Servers.
- Rubrik OS installation on Cisco UCS C-Series nodes through Cisco Intersight. This requires enabling an NFS/SMB/HTTPS repository which has the certified Rubrik CDM software.

Physical Components

This section details the physical hardware, software revisions, and firmware versions required to install Rubrik CDM Clusters running on Cisco Unified Computing System. A Rubrik on-premises cluster requires a minimum of four physical nodes deployed either on Cisco UCS C-Series Rubrik-certified nodes.

<u>Table 1</u> lists the required hardware components and disk options for the Rubrik CDM on Cisco UCS C-Series Rack Servers.

Component		Hardware
Fabric Interconnects		Two (2) Cisco UCS 6454 Fabric Interconnects
Server Node		4x Cisco UCS C240 M6 LFF Server Node for Intel Scalable CPUs
Processors		Each server node equipped with two Intel 5318N 2.1GHz/150W 24C/36MB
Memory		Each server node equipped with 384 GB of total memory using twelve (12) 32GB RDIMM DRx4 3200 (8Gb)
Disk Controller		Cisco M6 12G SAS HBA
Storage (each server node)	OS Boot	2x M.2 (240GB) with M.2 HW RAID Controller
Caching		1x 1.6 TB NVMe
Storage		12x 12TB 12G SAS 7.2K RPM LFF HDD (4K)
Network (Each Server node)		Cisco UCS VIC 1467 4x25G mLOM

		~ ~ .		e		
Table 1.	Cisco UCS	C-Series	nodes	for the	Rubrik	CDM

Software Components

<u>Table 2</u> lists the software components and the versions required for the Rubrik CDM and Cisco UCS C-Series nodes managed through Cisco UCS Fabric Interconnect in Intersight Managed mode (IMM), as tested, and validated in this document.

Table 2. Software Components

Component	Version
Rubrik CDM	rubrik_os_8.1.3-p6-25150_iv_3.5.0-138
Cisco Fabric Interconnect 6454	4.2 (3h)
Cisco UCS C240 M6 LFF servers	4.2 (3h)

Solution Deployment

This chapter contains the following:

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

This chapter describes the solution deployment for Rubrik CDM 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 beginning the installation activities, complete the following necessary tasks and gather the required information.

IP addressing

IP addresses for the Rubrik CDM on Cisco UCS, 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.
- Cisco UCS C240 M6 LFF node management: Each Cisco UCS C240 M6 LFF server/node, is managed through an IMC Access policy mapped to IP pools through the Server Profile. Both In-Band or 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 Rubrik 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
- Rubrik Operating System IP: These addresses are used by the Linux OS on each Rubik node. One IP addresses per node required from the same subnet. Rubrik node is configured with bond0 and bond1 as two separate networks. Both bond0 and bond1 networks support active-passive failover mode. Only bond0 network should configured for Cisco C-Series nodes connected to Cisco Fabric Interconnect. Once the Rubrik CDM software is installed on each node, Both Rubrik Management and Rubrik Data network are allocated in the same VLAN and configured in bond0 network.
- Once Rubrik cluster is configured, Customers have the option to configure sub-interfaces for Rubrik nodes. This allows accessibility to **multiple networks** through different VLANs.

<u>Figure 10</u> elaborates on the network port (bond0). Only bond0 port should be configured for Cisco C-Series nodes connected to Cisco Fabric Interconnect.

Checking networking	ponts								
Port I	Device	1	Driver	ı	State	ı	Link	I	Speed
(bond0]		i		i	up	i	ues	i	50000Mb/s
bond1		İ.		Ì	down	Ì	no	Ì	Unknown!
eth0	Cisco VIC NIC (rev a2)	i	enic	i	down	i	no	i	Unknown!
eth1	Cisco VIC NIC (rev a2)	i i	enic	i	down	Ì	no	i	Unknown!
rketh0	Intel 10G X550T	Î.	ixape	Î	down	Ì	no	Î	Unknown!
rketh1	Intel 10G X550T	Î.	ixqbe	Î	down	Ì	no	Ì	Unknown!
rketh2	Cisco VIC NIC (rev a2)	1	enic	I	սթ	I	yes	I	50000Mb/s
rketh3	Cisco VIC NIC (rev a2)	1	enic	I	սթ	I	yes	I	50000Mb/s
Bondl Mode is fault Bondl bond port: Current active j WARNING: Bondl has	-tolerance (active-backup) s are: rketh0 rketh1 port is None no active ports and is not 	ope	erational	l.					
Checking for MCEs /var/log/mcelog is (clean								
FRU Replacement Sum All FRUS in the m RC240WZP2649215W >> RC240WZP2649215W >>	mary: ode are healthy.								

Figure 10. Network Port configuration for Rubrik nodes

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

Note: Rubrik CDM deployed on Cisco UCS C-Series Servers and attached to Cisco UCS Fabric Interconnect **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 below table the IPMI IPs are configured as 0.0.0.x

Note: Administrators deploying Rubrik CDM on standalone Cisco C-Series servers (not attached to Cisco Fabric Interconnect) can use the node CIMC address as the IPMI IP.

Note: Use the following tables to list the required IP addresses for the installation of a 4-node Rubrik CDM cluster and review an example IP configuration.

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

Address Group:	UCS Mana	gement	Rubrik CE)M Nodes
VLAN ID:	KVM Management Addresses (Out of Band)	KVM Management Addresses (In-Band)	Node IP	Node IPMI IP
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				
Rubrik Node #1				
Rubrik Node #2				
Rubrik Node #3				
Rubrik Node #4				

Table 3. Rubrik Cluster IP Addressing

Note: <u>Table 4</u> is a true representation of configuration deployed during Solution Validation.

Address Group:	UCS Management		Rubrik CD)M Nodes
VLAN ID:	KVM Management Addresses (Out of Band) KVM Management I		Node IP	Node IPMI IP
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0	0.0.0.0
Gateway:	10.108.0.254	10.108.1.254	10.108.0.254	0.0.0
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			
Rubrik Node #1	10.108.0.163	10.108.0.167	10.108.1.163	0.0.0.1
Rubrik Node #2	10.108.0.164	10.108.0.168	10.108.1.164	0.0.0.2
Rubrik Node #3	10.108.0.165 10.108.0.169		10.108.1.165	0.0.0.3
Rubrik Node #4	10.108.0.166	10.108.0.170	10.108.1.166	0.0.0.4

Table 4. Example Rubrik Cluster IP Addressing

VLANs

Prior to the installation, the required VLAN IDs need to be documented, and created in the upstream network if necessary. In present deployment the Rubrik Management and Backup Data traffic exist in the same VLAN on bond0 network. Customers can segregate Rubrik Management and Backup Data traffic by defining separate VLAN for Rubrik Management and Backup Data. Once the Rubrik cluster is bootstrapped and registered, customers can create sub-interfaces to segregate management and backup traffic.

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

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

Name	ID
< <rubrik-management-vlan>></rubrik-management-vlan>	1081
< <rubrik-data-vlan>></rubrik-data-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.

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

Table 6. Network Uplink Configuration

Table 7. Network Uplink Example Configuration

Fabric Interconnec	t Port	Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
	1/53	🖾 Yes 🗆 No	□ LACP		
	1/54	🖾 Yes 🗆 No	⊠ vPC		
A		🗆 Yes 🗆 No		61	Vpc61
		🗆 Yes 🗆 No			
	1/53	🛛 Yes 🗆 No	LACP		
2	1/54	🛛 Yes 🗆 No	🖾 vPC		
в		🗆 Yes 🗆 No		62	Vрс62
		🗆 Yes 🗆 No			

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: <u>https://intersight.com/help/saas/getting_started/create_cisco_intersight_account</u>

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

Step 2. Click Create an account.

cisco Intersight © English
Welcome to Intersight Don't have an Intersight Account? Create an account Sign In with Cisco ID
Don't have a Cisco ID? Sign Up Or Email
Sign In with SSO
Help Center Terms Privacy Cookles @ 2022 Cisco Systems, Inc.

- **Step 3.** Sign-In with your Cisco ID.
- Step 4. Read the End User License Agreement and select I accept and click Next.

ीत्र Intersight	
	End User License Agreement
	Please read the end user license agreement carefully.
	OVERVIEW
	By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.
	If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms.
	I accept
	Cancel Next

Step 5. Provide a name for the account and click Create.

ഷം Intersight	
	Account Creation Account Name * Ru-DataProtection
	Cancel

Step 6. Register for Smart Licensing or Start Trial.

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

Step 7. Select Infrastructure Service & Cloud Orchestrator and click Start Trial.

Start Trial		
Infrastructure Service & Cloud Orchestrator 90 days trial		
Workload Optimizer Registration Required 45 days trial		
	Cancel	Start Trial

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

Set up Intersight Managed Mode (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

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>
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 : <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]: n
Default 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>
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 Resource Groups

A Resource Group represents a collection of resources. You can create a Resource Group to classify and manage resources. Resource Groups can be used for assigning resources to an organization. For more information, go to: <u>https://intersight.com/help/saas/resources/RBAC#role-based_access_control_in_intersight</u>

Note: In Cisco Intersight, all the resources and configurations in existing user accounts will automatically be placed in a default Resource Group, titled default Resource Group.

In this procedure, a Cisco Intersight organization is created where all Cisco Intersight Managed Mode configurations, including policies, are defined.

Step 1. Log into the Cisco Intersight portal.

Step 2. Select System. Click Settings (the gear icon).

Step 3. Click Organizations.

Step 4. Click + Create Resource Groups.

\equiv $\frac{1}{2}$	System V			Q Search		চি ৫	Q (0	1.
O Settings	Settings							
Admin Targets Software Repository Tech Support Bundles Audit Logs	Single Sign-On Domain Names Cisco ID Trusted Certificates	Resource Groups	is whowing you to light-ally group the recours	ces. You can create multiple R oups in Help Center.	+ Croups *	eate Resource	Group	
Sessions	ACCESS & PERMISSIONS IP Access Management Security & Privacy	Resource Groups +	Used Organizations	1 Items found Membership	10 - per page E Description	€ <u>1</u> of	()))) ()))	
New Command Palette × Navigate Intercipit with Ctrl+K or go to Help > Command Palette	Usera Groups	2 B	Constitu	All	The Defaur	Resource u.		
	Roles Organizations Resource Groups							
	API Keys DAuth2 Tokens Webhooks							

Step 5. Provide a name for the Resource group and click Create

≡ -thedo- cosco Intersight	🛢 System 🗸			Q Search	0 4 0 0
D Settings	Settings				
Admin Admin Aragets Software Repository Tech Support Bundles Audit Logs Sessions	Single Sign-On Domain Names Claca ID Trusted Certificates ACCESS & PEMASSIONS	Resource Groups Bissource Groups are new avoider wrd associate with the Organizet * Resource Groups @ +	is strending you to logically group the resource and	cas. Yeu can create multiple oups in Help Center.	+ Crieste Resource Group a Resource Croups ×
Licensing	IP Access Menagement Security & Privacy	Add Filter Name	Used Organizations	2 items found Membership	10 - per page 1 of 1 1 : Description : ₽
New Command Palette * asigate Intersight with Ofri+K or go Help > Command Palette	Users Groups	Ru-resourcegroup		Custom	The Denduit Tension Co.
	Roles Organizations Resource Groups API API Kays				
	OAuth2 Tokens Webhooks				

Procedure 3. Set Up Cisco Intersight Organization

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.

Note: Administrators can use "default" organization. "Default" organization is automatically created once an Intersight account is created.

In this procedure, a Cisco Intersight organization is created where all Cisco Intersight Managed Mode configurations, including policies, are defined.

- **Step 1.** Log into the Cisco Intersight portal.
- **Step 2.** Select System. Click Settings (the gear icon).
- Step 3. Click Organizations.
- Step 4. Click + Create Organization
- Step 5. Provide a name for the organization (for example, Ru-Org).
- Step 6. Select the Resource Group created in the last step (for example, Ru-ResourceGroup).
- Step 7. Click Create.

antersight	System 🗸			Q Search	R @ 4 P @
O Settings	Settings				
Admin ^ Targets Software Repository	Single Sign-On Domain Names	Organizations			+ Create Organization
Tech Support Bundles Audit Logs Sessions	Cisco ID Trusted Certificates	Use organizations to mana- create an Organization and Center.	ge access to your infrastructure. Organizati associate with one or more Resource Grau	on now includes Resource Group select as. For more information, see Organizat	llon. You can Llions in Help X
Licensing	IP Access Management Security & Privacy	* Organizations © +	: Usage	2 items found 10 Resource Groups	> per page ≥ 1 of 1 > Description :
New Command Palette * Navigate Intersight with Ctrl+K or go to Help > Command Palette	Users Groups Roles	default	-	default Ru-resourcegroup	User in a Default Organi
	Organizations Resource Groups API API Keys OAuth2 Tokens				

Procedure 4. 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.

CISCO DEVICE CONSOLE AA08-XSeries	0	[
SYSTEM INFORMATION DEVICE CONNECTOR INVENTORY DIAGNOSTIC DATA		
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the dev please visit Help Center	ice connector	2
Device Connector	C Refres	
Device Connector ALLOW CONTROL Internet Intersight	Ē	
Not Claimed The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a Open new account and follow the guidance or go to the Targets page and click Claim a New Device for existing account. Intersight 1.0.11-3179		

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

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

Step 7. Copy and paste the Device ID and Claim from the Cisco UCS FI to Intersight, select the Resource Group created in previous section and click Claim.

≡ "lisco Intersight 📲 System	n ×		Q Search	₽ ©	Q ()	۹
Settings Admin ^	aim a New Target					
Software Repository Tech Support Bundles	Claim Cisco UCS Domain (Intersight Manag to claim your target, provide the Device ID, Claim Code and select the approp	ed) Target rlate Resource Groups.				
Audit Logs	General					
Sessions Licensing	Device ID * Claim Code *	1		G	2	
	Resource Groups					
New Command Palette × Navigate Intersight with Ctrl+K or go to Help > Command Palette	Select the Resource Groups if required. However, th Group type is 'All'. The claimed target will be part of	is selection is not mandatory as all Organizations with the Resour	one or more Resource rce Group type 'All'.			
			1 tems found 10 v per p	ace K (1 of 1)) &	3	
	Vame	Usage	Descript	ion	,	
	Ru-resourcegroup	Ru-Org			_	
	Selected 1 of 1 Show Selected Unselect All			🗷 < 1 of 1 🔉		
	Back Cancel				Claim	

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

≡	cisco Intersight	tem 🗸			Q Search	0 F1 C	0	A
0	Settings	Fargets				С	aim a New	Target
	Targets Tech Support Bundles	* All Targets ● +			G Export 1 items found	10 - yer page 🔣 🔇 1	of 1 🔉 🛛	
	Audit Logs Sessions Licensing	Connection Connected 1	Top Targets by Types	Vendor 1 • Cisco Systems, Inc. 1			3	ĸ
Ne	w Command Palette ×	Name	: Status	: Туре	Claimed Time	Claimed By	: (3
Navi to H	igate Intersight with Ctrl+K or go elp > Command Palette	AAU9-FI-DP-8454	(g) connected	intersignt Managed Domain	a tew seconds âgo	andnimangicisco.com	of 1 🗵 🗄	Я

Step 8. 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 run the Cisco UCS C-Series platform in Intersight Managed Mode (IMM).

Procedure 5. 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.

≡	diada Intersight	\$e Infrastructure Service ∨ Q Search	Ø \$	Q @ A
:@:	Overview	Fabric Interconnects		
0	Operate Servers	★ All Fabric Interconn ◎ + ⊘ Q, Add Filter G: Export 2 it	items found 12 - per page 📧 🔇	1 of 1 > >
	Chassis Fabric Interconnects	Health Connection Bundle Version NX-OS Version Mod	odels	94 26
,c	HyperFlex Clusters Configure	2 • Healthy 2 No Versions 2 • 7.0(3)N2(4.13)) 2 2	2 • 6454 2	
	Profiles	Name : Health : Model : Bundle Version : UCS Domai	ain Profile Ports Total Used	Availa
	Templates	AA09-FI-DP-6454 FI-A O Healthy UCS-FI-6454	54 0	54
	Policies	AA09-FI-DP-6454 FI-B O Healthy UCS-FI-6454	54 0	54
	Pools			1 of 1 ≥ ∋

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:

	ີ Intersight 🤅	° Infrastructure Service ∨		Q Search	h
@:	Overview	← Fabric Interconnects	FI-A O Healthy		
Ø.	Operate ^ Servers	General Inventory Connections	UCS Domain Profile		
	Chassis	Details	Properties		
	Fabric Interconnects				
	HyperFlex Clusters	Health A	UCS-FI-6454	Fro	ont Rear
C	Configure ^ Profiles Templates	Name AA09-FI-DP-6454 FI-A Peer Switch AA09-FI-DP-6454 FI-B	Locator LED	andarskarskarskarskarskarskarskarskarskarsk	lealth Overlay
	Policies Pools	Model UCS-FI-6454	Mode	Access	
		Serial FDO260419XX	Ethernet Switching Mode	IP Address 10.108.0.161	
Nev	Command Palette	Management IP			
Navig to He	gate Intersight with Ctrl+K or go elp > Command Palette	10.108.0.161	FC Switching Mode end-host	Subnet Mask 255.255.255.0	
		Intersight	Admin Evac State	Default Gateway	
		UCS Domain Profile	O Disabled	10.108.0.254	
			Oper Evac State	MAC	
		UCS Domain Profile Status	S Disabled	00:08:31:0B:5D:A0	
		COS Domain Prome Status			

Procedure 6. Upgrade Fabric Interconnect Firmware using Cisco Intersight

Note: If your Cisco UCS 6454 Fabric Interconnects are not already running firmware release 4.2(2c), upgrade them to 4.2(3d) or to the recommended release.

Note: If Cisco UCS Fabric Interconnects were upgraded to the latest recommended software using Cisco UCS Manager, this upgrade process through Intersight will still work and will copy the Cisco UCS firmware to the Fabric Interconnects.

Note: By default, Fabric Interconnect upgrades through Intersight are enabled with 'Fabric Interconnect Traffic Evacuation. Since the present procedure is a new setup with no Domain Profile associated, Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.

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. Enable Advanced Mode and uncheck Fabric Interconnect traffic evacuation. This is only for new setup of Fabric Interconnects.

Step 7. Select 4.2(3d) release (or the latest release which has the Recommended icon) from the list and click Next.

Step 8. Verify the information and click Upgrade to start the upgrade process.

Step 9. 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 10. Wait for both the FIs to successfully upgrade.

Step 11. Snap shot below details in the Fabric Interconnect upgrade to firmware version 4.2(3d)

≡	dials Intersight	.**	Infrastructu	re Service 🗸						Q Search	0	¢	¢	0	R
:\$:	Overview		Fabr	ric Interconi	nects										
0	Operate Servers	^	* 1	All Fabric Interconn ©	+				G	Export 2 items found 12 v	per pag	e K <	1 of	1 > স	
	Chassis			Health	Connection		Contract Statue		Rundle Version	NY-OS Version		Mod	lole		
	Fabric Interconnects				Connected 2		Not Covered 2					Piot	1013		
	HyperFlex Clusters			2 • Healthy 2					2 • 4.2(3d) 2	2 • 9.3(5)142(3c)	2	C) ·	645-	
.0	Configure														
	Profiles			Name	: Health	÷	Model	÷	Bundle Version	UCS Domain Profile	Total	Ports Used	Avai	a 9	_
	Templates			AA09-FI-DP-6454 FI-A	C Healthy		UCS-FI-6454		4.2(3d)		54	0	54		
	Policies			AA09-FI-DP-6454 FI-B	Healthy		UCS-FI-6454		4.2(3d)		54	0	54		
	Pools												1 of	1 🤉 🛛	

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 for Rubrik 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. <u>Table 8</u> lists the policies required for the solution described in this document.

Table 8. 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	
Syslog policy	
System QoS	

Procedure 1. Create VLAN configuration Policy

Step 1. Select Infrastructure Services.

	disco Intersight	📽 Infrastructure Service 🗸
@:	Overview	Anage compute and converged infrastructure operations.
ŝ)	Operate	Cloud Orchestrator
	Servers	
	Chassis	Workload Optimizer
	Fabric Interconnects	
	HyperFlex Clusters	My Dashboard
	Virtualization	System
	Kubernetes	
	Integrated Systems	Explore More Services 17

Step 2. Under Policies, select Policy, then select UCS Domain, select the VLAN policy option and click Start.
≡	diala Intersight Service	ce Q Search	Ø ◎ 2 ⊈ 14	Q 047 A 10
	Chassis C	Policies		
	HyperFlex Clusters	Filters	Q, vian	
	Kubernetes Integrated Systems	Platform Type	VLAN	
,c	Configure ^ Profiles Templates	UCS Server UCS Domain UCS Chassis HyperFlex Cluster		
(Policies Pools	Kubernetes Cluster	Cancel	Start

Step 3. Select organization, provide a name for the VLAN (for example, Ru-VLAN) and click Next.

=	diale Intersight	🖧 Infrastructure Service 🗸	Q Search	⊘	₽	٥	0	R
.(\$).	Overview	Policies > VLAN Create						
0	Operate ^		General					
	Servers	General General	Add a name, description and tag for the policy.					
	Fabric Interconnects	2 Policy Details	Organization * Ru-Org		~			
	HyperFlex Clusters		Name *					
.0	Configure ^		RU-VLAN		_			
	Profiles Templates		Set Tags					
	Policies							
	Pools		Description		<i>a</i> 024			
Ner	Command Palette	•	< Cancel				Nex	đ

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:

≡	Intersight	🎥 Infrastructure Service 🗸	Q Search	
nàn -	Dverview	Policies > VLAN > Create		
p		Create Multicast Po	licy	
0	Operate ^	· · · · · · · · · · · · · · · · · · ·		
:	Servers	1 General	General Add a name, description and tag for the policy.	
(Chassis	2 Policy Details	Organization *	
1	Fabric Interconnects		Ru Org	
	Popfiques		Nama * Ru-multicast	
F	Profiles		Partituitivaar	
1	Templates		Set Tags	
F	Policies			
ł	Pools		Description	
New	Command Palette		Canad	
avigat	e Intersight with Ctrl+K or	`		
_	during Intersight	o Infrastructure Q Search	Ø 0 2 ⊈ 14 Δ 0 47 Δ 10	
	cinco	Service		
ġ:	Overview	Policies > VLAN > Create		
		Create Multic	ast Policy	
0	Operate	^	·	
	Servers	General	Policy Details Add policy details	
	Chassis	2 Policy Details		
	Fabric Interconnects		Multicast Policy	
	HyperFlex Clusters			
	Virtualization		Snooping State ©	
	Kubernetes		Querier State 💿	
	Integrated Systems			
6	Configure		Source IP Proxy State 💿 🖕	
~	Profiles	•	Create	
Ξ	disco Intersight	🖧 Infrastructure Service 🗸	Q Search 🥝 📢	0 Q
à	Overview	 Policies > VLAN 		
		Create		
0	Operate	^ Add VI ANs		
	Servers	Add VLANs to the policy		
	Chassis			
	Fabric Interconnects	A VLANs should have	one Multicast policy associated to it	
	HyperFlex Clusters	Configuration		
0	Configure	Computation		
	Drofilee	Name / Prefix * VLAN1080	VLAN IDs * © 1080	G
	Tampleta			
	remplates	Auto Allow On Up	plinks O	
	Policies			
	Pools	Enable VLAN Sha	anng u	
		Multicast Policy *		
Net	Command Palette	× Selected Policy Ru-mul	Iticast X ©	-
Navi	gate intersight with Ctrl+K	or • Cancel		Add

Step 6. Add additional VLANs as required with same multicast policy in the network setup and click Create.

| A

Overview Policies > VLAN Cperate Create Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure Profiles Templates Policies <	Overview Policies > VLAN Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure Pofiles Templates Policies Policies Policies VLANs Policies		Sec Infrastructure Service V	Q Search 🥝 🛱 🗘	0
Operate Servers Chassis Pabric Interconnects HyperFlex Clusters Configure Profiles Templates Policies	Operate Servers Chassis Chassis Pabric Interconnects HyperFlex Clusters Configure Pofiles Templates Policies Policies <	Overview	Policies > VLAN		
Servers	Servers Servers Chassis 2 Policy Details Add VLANs Fabric Interconnects Show VLAN Ranges HyperFlex Clusters Sitems found Configure Sitems found Profiles Add Filter Templates VLAN None Policies 1 Policies 1 Policies 1 1 1080 VLAN None Ru-m Yes 1 1081 VLAN None Ru-m Yes	Operate ^			
Chassis 2 Policy Details Fabric Interconnects HyperFlex Clusters Configure Profiles Templates Policies Add VLANs Add VLANs Add VLANs Show VLAN Ranges Image: Show VLAN Ranges	Chassis 2 Policy Details Fabric Interconnects HyperFlex Clusters Configure Profiles Templates Polices Polices Polices Polices 1 default 1 1 default 1 1 080 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081 1 081	Servers	General	VLANs	
Fabric Interconnects HyperFlex Clusters Configure Profiles Templates Policies Show VLAN Ranges I default None Yes I default None Ru-m., Yes	Fabric Interconnects Biter HyperFlex Clusters Show VLAN Ranges Configure 5 items found 1	Chassis	2 Policy Details	Add VLANs	
HyperFlex Clusters Image: State of the s	HyperFlex Clusters	Fabric Interconnects		Show VII AN Deserve	
Configure ^ 5 items found 1 of 1 > > Profiles	Configure Sitems found 1 c per page 1 of 1 P Profiles Add Filter Add Filter P Image: I			STOW VEAN BALGES	
Profiles V : N : S : P : Multic Auto Ø Templates 1 default None Yes ···· Policies 2 VLAN None Ru-m Yes ····	Profiles N. : N. : S. : P. : Multic Auto Ø Templates - 1 default None Yes ···<	HyperFlex Clusters		Show VLAN Ranges	
V N S P Multic Auto Ø Templates 1 default None Ves	Image: Pointing of the second seco	HyperFlex Clusters		Show VLAN Ranges	
Templates 1 default None Yes ···· Policies 2 VLAN None Ru-m Yes ····	Templates 1 default None Yes Policies 2 VLAN None Ru-m Yes 1 1080 VLAN None Ru-m Yes 1 1081 VLAN None Ru-m Yes	HyperFlex Clusters		Show VLAN Ranges Ø 5 items found 1C ∨ per page I of 1 Q Add Filter) (3)
Policies 2 VLAN None Ru-m Yes ····	Policies 2 VLAN None Ru-m Yes ··· Pools 1080 VLAN None Ru-m Yes ··· 1081 VLAN None Ru-m Yes ···	HyperFlex Clusters Configure Profiles		Show VLAN Ranges Image: 5 items found 10 per page Q Add Filter Image: V V N S P Multic))) }
	Pools 1080 VLAN None Ru-m Yes 1081 VLAN None Ru-m Yes	HyperFlex Clusters Configure Profiles Templates		Show VLAN Ranges Sitems found 1C v per page Q Add Filter V N 1 default None Yes	9
Pools 1080 VLAN None Ru-m Yes ····	1081 VLAN None Ru-m Yes ····	HyperFlex Clusters Configure Profiles Templates Policies		Show VLAN Ranges Image: Show VLAN Ranges	9
1081 VLAN None Ru-m Yes ····		HyperFlex Clusters Configure Profiles Templates Policies Pools		Show VLAN Ranges 5 items found 1C v per page Add Filter V N 1 default 2 VLAN 1080 VLAN None Ru-m Yes 1080 VLAN	¢
	1082 VLAN None Ru-m Yes ***	HyperFlex Clusters Configure Profiles Templates Policies Pools		Show VLAN Ranges Sitems found 1C v per page Add Filter I default None Yes 2 VLAN 1080 VLAN None Ru-m Yes 1080 VLAN None Ru-m Yes 1081 VLAN None Ru-m Yes	¢
	Pools 1080 VLAN None Ru-m 1081 VLAN None Ru-m	HyperFlex Clusters		5 items found 10 v per page C]_1_of1 [>

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.

≡ "disco" Intersight	Service Q Search	
Chassis Fabric Interconnects	← Policies Create	
HyperFlex Clusters	Filters	Q Search
Kubernetes	Platform Type	
Integrated Systems	All UCS Server	SNMP
Profiles Templates	UCS Chassis	Switch Control
Policies	HyperFlex Cluster Kubernetes Cluster	System QoS Cancel Start

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.

≡	روانيان Intersight	📽 Infrastructure Service 🗸	Q Search	Ø	\$	¢	0	<u> </u>
(.).	Overview	Policies > Port						
0	Operate ^	1 General	General					ľ
	Chassis	2 Unified Port	Add a name, description and tag for the policy. Organization *					
	Fabric Interconnects HyperFlex Clusters	Breakout Options A Port Roles	Ru-Org Name *		<i>v</i>			
.0	Configure ^		Ru-PortPolicy					
	Templates Policies		UCS:FI-6454	0	~			
	Pools		Set Tags					
Ne	w Command Palette		Description				_	
Nav	igate Intersight with Ctrl+K or		< Cancel				Ne	ext

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

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

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

	ense Intersight	🔩 Infrestructure Service 🗸		والمتناف المتحدي	Q Search	0 002	F	Q (0 47) (A 10)	0	۶
	Overview	Policies > Port								
0) •	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Virtualization Kubernetes Integreted Systems Configure Profiles Templates	 General Unified Port Breakout Options Port Roies 	Unified I	Port the port modes to carry FC or Ethernet traff Move slider to configure unified ports Fibre Channel Ports I & Fibre I & Fib	ic. and select port to set breakout.	6.000 0.000 0.000	FG. • Ether	et Part Modes		
	Policies		< Cancel	Ports 1-16	Lithernet	Ports 1	7-54	Bac	k Ne	xt

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.

1	Port Roles	Port Channe	els Pin Groups		
1	Configure	Selected Ports	Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32		Clear Selectio
				•	0

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

Configure (16 Ports)

Configuration	
Selected Ports	Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32
Role Server	~
і пэк	-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.
FEC © Auto () CI74
Manu Manu	al Chassis/Server Numbering 💿

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 ID 65 (or as defined in your configuration table) as per the network configuration. In this setup, port 53/54 are port channeled and provide uplink connectivity to the Cisco Nexus switch.

Policies > Port	1.00			10	-	
1010103 / 1011	Port	>:-	es	IIC	PO	

	The combined maximum number of Ethernet Uplink, FCoE Uplink, and Appliance port channels permitted is 12 and the maximum number of FC port channels permitted is 4.
	Role Ethernet Uplink Port Channel v
	Port Channel ID * Admin Speed 65 C © Auto < © 1 - 255 1 - 255
	Ethernet Network Group ⊙ Select Policy 🗐
	Flow Control Select Policy
	Link Aggregation Select Policy
	Link Control Select Policy
icies > Port	
eale	
General Unified Port	Port Roles Configure port roles to define the traffic type carried through a unified port connection. Port Roles Port Channels Pin Groups
General Unified Port Breakout Options Port Roles	Port Roles Configure port roles to define the traffic type carried through a unified port connection. Port Roles Port Channels Pin Groups
General Unified Port Breakout Options Port Roles	Port Roles
General Unified Port Breakout Options Port Roles	Port Roles Create Port Channels Pin Groups Create Port Channel Create Port Channel Create Port Cha
 General Unified Port Breakout Options Port Roles 	Port Roles Center port coles to define the traffic type carried through a unified port connection. Port Roles Ort Roles Port Roles Port Channels Port Roles Port Channels Port Roles Port Channels Port Roles Port Channels Port Roles Port Channel Port Roles Port Roles <p< td=""></p<>

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:

General	Port Roles	
Unified Port	Configure port roles to define the traffic type carried through a unified port connection.	
Breakout Ontions	Port Roles Port Channels Pin Groups	
Breakout Options		
Port Roles	Create Port Channel	
	100 test have been here have have many many starts, starts ward many many many many many gark many parts ward day	1.654748.614748_ #14.758_ 814.750_ 514.756
		1974 1974 2003 2006 2007
	OBCOURS-Press	
	*	Ethernet Uplink Port Channel
	ℓ ■ 1 items found 10 × per per	ge 📧 🤇 1 of 1 🗩 🖗
	Items found 10 ∨ per parts ID Role 2	ge 🗷 🤇 1 of 1 🔊 🖗

Procedure 3. Create NTP Policy

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

≡	the Intersight	📚 Infrastructure Service 🗸		Q Sear	ch	Ø @2 ⊄1 ™	Q 047 A 10	0	8
×.	Overview	← Policies Create							
¢	Operate P Servers P Fabric Interconnects P Hype/Filex Clusters P Kubernetes P Integrated Systems P Profiles P Templates P Pools P	Filters Platform Type All UCS Server UCS Domain UCS Chassis Hyper Tex Cluster Kuberneiers Cluster	Q, Search Pthemet Network Control Ptharnet Network Group Flow Control Unk Aggregation	Link Control Multicast Policy Network Connactivity NTP NTP	Port SNMP SNMCh Control Styllog	System Qal			
			Cancel					Star	n

- **Step 2.** Provide a name for the NTP policy.
- Step 3. Click Next.
- **Step 4.** Define the name or IP address for the NTP servers. Define the correct time zone.

Policies > NTP Create			
General Policy Details	Policy Details Add policy details		
	Enable NTP The Servers * 172.20.10.18 NTP Servers *	D	
	172.20.10.15 © (i Timezone America/Los_Angeles	h +	× 0
<	Cancel		Back Create

Step 5. Click Create.

Procedure 4. Create syslog Policy

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

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

≡	tisco Intersight	📲 Infrastructure Service 🗸		Q sea	rch	⊗ 💷 🕫 📧	Q @47 (A10)	ଡ ନ
)(Ø)(Overview	 Policies Create 						
, , , ,	Operata ^ Servers Chassis Fabric Intercennects HyperFlex Clusters Virtualization Kubernetas Integrated Systems Configure ^ Profiles Posicies Posicies	Fitters Platform Type All UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	C, Search Ethemet Network Control Uthemet Network Group Flow Control Unix Aggregation	Lisk Control Multicast Policy NEtwork Connectivity NTP	Port SHMP Switch Control Systog	System QoS VLAN VSAN		
			Cancel					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 Rubrik 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.

≡	and Intersight	$_{g}$ infrastructure Service $$		Q Search		⊘ <u>⊚</u> 2 ⊄1 14 £	. 💶 🖓	ଡ ନ
XÂX	Overview	 Policies Create 						
(<u>)</u>	Operate A Servers Chassis Chas	Filters Platform Type All UCS Satvar UCS Choasis HyperFlay Cluster Subernates Dustar	Search Ethermet Neswork Control Ethermet Neswork Group Have Control Thirk Aggregation	Link Control Multicast Polcy Notwork Danacetivity NTP	Pari SvMP Svitch Dantral Systog	System OcS VLAN VISAN)	
			Cancel					Start

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

Step 3. Click Next.

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

Policies > System QoS Create								
	Policy Details							
General	Add policy details							
2 Policy Details	This policy is ap	oplicable only for UC:	S Domain:	5				
	Configure Prior	rities						
	Platinum							
	Gold							
	Silver							
	Bronze							
	Best Effort	CoS Any	©	Weight 5) a	Allow Packet Drops O	мти 9216	() a
	Fibre	CoS		Weight			MTU	
	Channel	3	0	5	() ()	Allow Packet Drops	2240	0
<	Cancel						[Back Create

Note: All the Domain Policies created in this procedure will be attached to a Domain Profile. You can clone the Cisco UCS domain profile to install additional Cisco UCS Systems. When cloning the Cisco UCS

domain profile, the new Cisco UCS domains use the existing policies for consistent deployment of additional Cisco Systems at scale.

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

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

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

	disco Intersight	ှိမိုး Infrastruc	cture Service 🗸			Q Sear	ch ⊘ ⊄	<u>م ۞ </u>
:@:	Overview	Pol	icies					Create Policy
0	Operate A Servers Chassis Fabric Interconnects HyperFlex Clusters		All Policies +	Filter Usage (7) •Not Used 6 •N/A 1		🔁 Export	7 items found 10 v per page 🗷 🤇] 1 of1 ≥ ≫
,c	Configure /		Name	 Platform Type 	Туре	÷.	Usage Last Update	÷ 4
	Templates		Ru-syslog	UCS Server, UCS Domain	Syslog	0 🐻	a few seconds ago	
(Ru-NTP	UCS Server, UCS Domain	NTP	6 O	a few seconds ago	
U	Policies		Ru-System-QoS	UCS Domain	System QoS	0 []	5 minutes ago	
	Pools		Ru-PortPolicy-B	UCS Domain	Port	0 (5	12 minutes ago	
			Ru-PortPolicy	UCS Domain	Port	0 👩	16 minutes ago	
Ne	Command Palette		Ru-VLAN	UCS Domain	VLAN	0 [8	29 minutes ago	
Navi	gate Intersight with Ctrl+K or go		Ru-multicast	UCS Domain	Multicast Policy	© N/A	31 minutes ago	
to H	elp > Command Palette		101			-		. 1 of 1 > >

Procedure 6. Create Domain Profile

- Step 1. Select the Infrastructure Service option and click Profiles.
- Step 2. Select UCS Domain Profiles.
- Step 3. Click Create UCS Domain Profile.

≡	dialla Intersight	🎗 Infrastructure Service 🗸	Q Search	0	41 Q	ଡ ନ
:@:	Overview	Profiles				
0	Operate	HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles UCS Server Profiles				
	Servers			Cre	ate UCS Don	ain Profile
	Fabric Interconnects	* All UCS Domain Pr ⊕ + ···	Export 0 items found 10	v per pag	e K < 0	of 0 돈 🗵
.0	HyperFlex Clusters	Name Status - U	CS Domain Last Update			+
(Profiles	NO ITEMS AVAILABLE				
	Policies				0 [2] [9]	of 0 [2] [2]
	Pools					
No	w Command Palette ×					
Nav to H	gate Intersight with Ctrl+K or go elp > Command Palette					

Step 4. Provide a name for the profile (for example, AA08-XSeries-DomainProfile) and click Next.

≡	diala Intersight 🌲 In	nfrastructure Service 🗸		Q Search	\odot	F I (0 (<u>୍</u>
:@:	Overview	← Profiles Create UCS Domain	Profile					1
© ,© Nava to I	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure Profiles Policies Pools	 Ceneral UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration Summary 	Ceneral Ad a name, description and tag for the UCS domain profile. Organization * RrOrg ✓ Name * RrDomainProfile-AA00 © Set Tags Description \checkmark <= 1024					
		<	Close			В	ack Ne	at

Step 5. Select the fabric interconnect domain pair created when you claimed your Fabric Interconnects.

=	dialitic Intersight	📽 Infrastructure Service 🗸		Search	Ø 9	a Q	0	A
\$	Overview	<pre>← Profiles</pre> Create UCS Domain	n Profile					
S Nav to F	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure Profiles Policies Pools w Command Palette	 Ceneral UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration UCS Domain Configuration Summary 	UCS Domain Assignment Choose to assign a fabric interconnect pair now or later. Assign Now Assign Later Image: Choose to assign a fabric interconnect pair now or later. If you choose Assign went to assign and click Next. If you choose Assign Later, click Next to proce Image: Show Assigned Image: Add Filter Image: Domain Name Fabric Interconnect A Image: Add Filter Image: Add Filter	Now, select a pair that y ed to policy selection. 1 items found <u>10</u> ersion <u>Model</u> UCS-FI-6454	vou ✓ per page € € € Fabric Interconn- Serial 4 FD0260419ZA	1 of 1 Bundlet 4.2(34 1 1	e Version 0 of 1	3
		< c	Close			Bac	c Nex	xt

Step 6. Under VLAN 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.

≡	distle Intersight	📽 Infrastructure Service 🗸		Q Search	0 4 0 0 A
:¢:	Overview	 Profiles Create UCS Domain 	Profile		
)) , , ,	Operate ^ Servers. / Chassis / Fabric Interconnects / HyperFlex Clusters / Configure ^ Profiles / Templates /	 Ceneral UCS Domain Assignment VLAN & VSAN Configuration VLAN & Configuration Orts Configuration UCS Domain Configuration Summary 	VLAN & VSAN Configuration Create or select a policy for the fabric interconnect pair.	× Ø	⊕ Ru-VLAN Select Policy
Nav Nav to H	Pools Command Palette × Qate Intersight with Ctri-K or go elp > Command Palette		VLAN Configuration VSAN Configuration	× Ø	C Ru-VLAN
		<	Close		Back Next

Step 7. Under Ports Configuration, select the port configuration policies created earlier. Each fabric has different port configuration policy with only the port channel ID different across both the Port Configuration Policy. Therefore, you need to select separate Port Policy for each Fabric Interconnect.

enersight 🍂	Infrastructure Service 🗸		Q Search	0 4 4 0
Overview	← Profiles Create UCS Domain	Profile		
Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Configure ^ Profiles Templates Policies Policies Policies Policies Policies Policies	 General UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration UCS Domain Configuration Summary 	Ports Configuration Create or select a part policy for the fabric interconnect pair. Configure ports by creating or selecting a policy. Parts Configuration Ports Configuration	- Selected Policy R	I-PortPolicy × 👁 🖋
		Port Type	Port Channel Type	
allado Intersight 🔪 Overview	t Infrastructure Service ↓ ← Profiles Create UCS Domain	n Profile	Q Search	0 A Q Ø
Overview Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure Profiles	 Infrastructure Service Profiles Create UCS Domain © General © UCS Domain Assignment © VLAN & VSAN Configuration Ports Configuration © UCS Domain Configuration © UCS Domain Configuration 	n Profile Ports Configuration Create or select a port policy for the fabric interconnect pair. Configure ports by creating or selecting a policy. Fabric Interconnect A Configured Fabric Interconnect B Configured	Q Search	0 A C 0
Untersight Intersight Overview Image: Comparison of the second s	 Infrastructure Service Profiles Create UCS Domain General UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration Summary 	n Profile Create or sated: a port policy for the fabric interconnect pair. Configure ports by creating or selecting a policy. Configure ports by creating or selecting a policy. Fabric Interconnect & Configured Ports Configuration	C Selected Policy R Selected Policy R Type R C Selected Policy R	Uncertified and a series of the series of t

Step 8. Under UCS Domain Configuration, select syslog, System QoS, and the NTP policies created earlier. Click Next.

≡	diala Intersight	📲 Infrastructure Service 🗸	Q	Search 🛛 🖓 🗘	0 9
:@:	Overview	← Profiles Create UCS Domain	n Profile		
0	Operate ^ Servers Chassis Fabric Interconnects	General	UCS Domain Configuration Select the compute and management policies to be associated with the fabric intercom Show Attached Policies (3)	ect.	
,e	HyperFlex Clusters Configure ^ Profiles	VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration	Management 2 of 4 Policies Configured NTP	× 2 0 Ru-NTP	
	Templates Policies	6 Summary	Syslog Network Connectivity	× Ø Tru-syslog B Select Policy B	j
	Pools		SNMP	Select Policy 🗐	
Nav Nav to H	w Command Palette × igate Intersight with Ctrl+K or go lelp > Command Palette		Network 1 of 2 Policies Configured		
			System QoS * Switch Control	× 🖉 🕸 Ru-System-QoS 📓	J

Step 9. Review the Summary and click Deploy. Accept the warning for the Fabric Interconnect reboot and click Deploy.



Step 10. Monitor the Domain Profile deployment status and ensure the successful deployment of Domain Profile.

etails	Execution Flow	
atus	Progress	52%
In Progress) Wait for Peer Fabric Interconnect to come up after reboot	
me	O Deploy Fiber Channel and Ethernet Breakout Ports	Jul 5, 2023 9:26 PM
ploy Domain Profile	O Deploy System QoS Policy	Jul 5, 2023 9:26 PN
	O Deploy Ethernet Network Policy	Jul 5, 2023 9:26 PM
a61831696f6e33016deb68	⊘ Deploy Sysiog Policy	Jul 5, 2023 9:26 PM
get Type	O Deploy NTP Policy	Jul 5, 2023 9:26 PN
and interconnect	⊘ Update Domain Profile State	Jul 5, 2023 9:26 PM
get Name 09-FI-DP-6454 FI-B	⊘ Validate Syslog Policy	Jul 5, 2023 9:26 PM
	⊘ Validate NTP Policy	Jul 5, 2023 9:26 PM
main Profile	⊘ Validate Ethernet Network Policy	Jul 5, 2023 9:26 PM
urce Name	⊘ Validate Port Policy	Jul 5, 2023 9:26 PM
-DomainProfile-AA09-B	⊘ Validate System QoS Policy	Jul 5, 2023 9:26 PM
iator	⊘ Prepare Switch Profile Deploy	Jul 5, 2023 9:26 PM
Jhiman@cisco.com		
art Time		

Step 11. After the Cisco UCS domain profile has been successfully created and deployed, the policies, including the port policies, are pushed to Cisco UCS fabric interconnects. Screenshot below details successful configuration of Domain Profile on Cisco UCS Fabric Interconnect in IMM mode (Intersight Managed Mode).

≡	cisco Intersight	*	Infrastructure Service $$				Q Search	ତ) ¢1 (2 @ A
	Overview		Profiles							
	Operate	^	HyperFlex Cluster Profiles	UCS Chassis Profiles	UCS Domain Profiles	UCS Server Profiles				
	Servers								0	and Barth
	Chassis								Create UCS I	Domain Profile
	Fabric Interconnects			+ .dd Filter			C Export 1 items found	10 v per p	age 🖂 <	1 of 1 ≥ >
	HyperFlex Clusters		Name	0 Sta	itus	Fabric Interconnec	Domain Fabric Interconnec Last Up	date		с <i>ў</i>
	Integrated Systems		Ru-DomainProfile-AA0	9 @	ок	AA09-FI-DP-6454	AA09-FI-DP-6454 an hour	ago		
.9	Configure	^								1 of 1 ≥ ≥
	Profiles									
	Templetes									

Step 12. 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 Rubrik deployment were already attached to these ports. The Servers are automatically discovered when the Domain Profile is configured on the Fabric Interconnects.

Step 13. To view the servers, go to the Connections tab and select Servers from the right navigation bar.

≡	-ili-ili- cisco Intersight 🍂	Infrastructure Service 🗸		Q Search	R @ 4 4 @ R
.(¢).	Overview	← Fabric Interconnects	5454 FI-B e Healthy		Actions
0	Operate ^ Servers	General Inventory	nnections UCS Domain Profile		
	Chassis	COMPUTE			
	Fabric Interconnects	Servers	Servers		
	HyperFlex Clusters	Chassis			
	Integrated Systems	NETWORK	🖉 🔍 Add Filter 🕒 Export	4 items found 10 ~ per page	K < 1 of 1 > H 🔅
φ,	Configure ^	Fabric Extenders	Name : Health : User Label :	Slot Id 💠 Model	t Serial t β
	Profiles	DECOMMISSIONED	AA09-FI-DP-6454-1 AE02 FI-DP-6454-1 AE02 FI-DP-6454-1	N/A UCSC-C240-M6	3L WZP26510561
	Templates	Servers	AA09-FI-DP-6454-2 O Resitty	N/A UCSC-C240-M	6L WZP2651056H ····
	Policies	Chassis	○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	N/A UCSC-C240-M6	SL WZP2651055Z ····
	Pools	Fabric Extenders	Ø		K < 1 of1 ≥ ≫
Nev Navi to H	Command Palette × gate Intersight with CtrI+K or go alp > Command Palette				

Manual Set up 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 policy.
- 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 for RAID1 configuration of internal M.2 cards. This is required for Rubrik OS installation.
- Management policies: IMC Access Policy for Rubrik certified Cisco C240 M6 LFF node, Intelligent Platform Management Interface (IPMI) over LAN; local user policy.

Create Pools

Procedure 1. Create Out of Band IP Pool

The IP Pool is a group of IP for KVM access, Server management and IPMI access of Rubrik 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.

≡	aliada Intersight	*	Infrastructure Service 🗸				Q Search	Ø	41 Q (୭ A
:¢:	Overview		Pools							
0	Operate	^	Pools Reserved Identi	fiers VRFs						
	Servers Chassis Fabric Interconnects		* All Pools © +	Add Filter			🔁 Export 0 i	items found 10 √ per pa	Creat	Pool
	HyperFlex Clusters Integrated Systems		IP x	MAC #		WWNN #	WWPN *	IQN #	Resourc	e ^{se}
,e	Configure Profiles	^	NO IP POOLS	NO MAC POOLS	NO UUID POOLS	NO WWNN POOLS	NO WWPN POOLS	NO IQN POOLS	NO RESC	U
	Templates		Name	: Туре	Size :	Used	Available Reserved	Description :	Last Update	
(Policies Pools					NO ITEMS AVAILABLE	I			
									(전 of C	
Navi to He	w Command Palette gate Intersight with Ctrl+K or g elp > Command Palette	ю К								

Step 2. Select IP and click Start.

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

≡	diality Intersight	🖧 Infrastructure Service 🗸	Q Search	Ø	₽	φ	0	۹
:@:	Overview	Pools > IP Pool Create						
© S New New New New New New New New New New	Operate A Servers A Chassis A Fabric Interconnects A HyperFiter Clusters A Configure A Poofiles A Poofiles A Poolicles A Poolicles A Poole A	Concrat Prv4 Pool Details IPv6 Pool Details	Ceneral Indicating the server profiles. Organization " Name * Nume * Set Tags Description < < < < < </th <th></th> <th></th> <th></th> <th></th> <th></th>					
		<.	Cancel				Next	

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

≡ dualte Intersigh	t 💦 🖓 Infrastructure Service 🗸	Q Search	ତ ସ ନ ଡ ୧
ŵ Overview	Pools > IP Pool Create		
 Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Templates Pools 	 General IPv4 Pool Details IPv6 Pool Details 	IPv4 Pool Details Network Interface configuration data for IPv4 Interfaces. Configure IPv4 Pool Configuration Netmask * Cateway 255255.255.0 0 Gateway 255255.255.0 0 IO.108.0.254 Primary DNS 172.20.4.33 0 172.20.4.54 IP Blocks From Size	0
New Command Palette Navigata Intersight with Ctrl+K to Heip > Command Palette	× arga	10.108.0.163 • 4	

Step 5. Deselect the IPV6 configuration and click Create.

Procedure 2. Create In-Band IP Pool

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

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

≡	-lindin Intersight	😪 Infrastructure Service 🗸				Q Search	0	R 0 0 R
:¢:	Overview	Pools						
0	Operate ^	Pools Reserved Ident	ifiers VRFs					
	Servers Chassis Fabric Interconnects	<u>* All Pools ⊛</u> +	Add Filter			🕒 Export 0 i	tems found 10 v per pa	Create Pool
	HyperFlex Clusters Integrated Systems	IP ×	MAC #		WWNN ×	WWPN #	IQN #	Resource
,0	Configure ^	NO IP POOLS	NO MAC POOLS	NO UUID POOLS	NO WWNN POOLS	NO WWPN POOLS	NO IQN POOLS	NO RESOU
	Templates	Name	: Туре	Size :	Used	Available Reserved	Description	Last Update
(Policies Pools				NO ITEMS AVAILABLE	I		
								K < 0 of 0 ≥ ≥
Nev Navi	Command Palette Section 2014 Section 2014							

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

Step 2. Select IP and click Start.

≡	tited: Intersight 88 In	nfrastructure Service 🗸	Q Search Ø 4 @ Q
:@:	Overview	Pools > IP Pool Create	
0	Operate ^	1 General	General
	Chassis	2 IPv4 Pool Details	Pool represents a collection of IPv4 and/or IPv6 addresses that can be allocated to other configuration entities like server profiles.
	Fabric Interconnects HyperFlex Clusters	3 IPv6 Pool Details	Organization * Ru-Org
0	Integrated Systems		Name * Ru-inBand-Pool
Q	Analyze A Explorer New		
,0	Configure ^		Set lags
	Profiles		Description d <- 1024
	Policies		
	Pools		
Ne	Command Palette		
Navi to H	jate Intersight with Ctrl+K or go Ip > Command Palette	<	Cancel Next

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

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

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



Procedure 3. Create MAC Pool

Note: Best practices mandate that MAC addresses used for Cisco UCS domains use 00:25:B5 as the first three bytes, which is one of the Organizationally Unique Identifiers (OUI) registered to Cisco Systems, Inc. The remaining 3 bytes can be manually set. The fourth byte (for example, 00:25:B5:xx) is often used to identify a specific UCS domain, meanwhile the fifth byte is often set to correlate to the Cisco UCS fabric and the vNIC placement order.

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

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

- Step 2. Select MAC and click Start.
- Step 3. Select organization, Enter a Name for Mac Pool (A) and click Start.

Step 4. Enter the last three octet of MAC address and the size of the Pool and click Create.

=	disco Intersight	📽 Infrastructure Service 🗸		Q Search	A 0 0 A
:@:	Overview	Pools > MAC Pool			
© ,© Navi to H	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Templates Policies Pools Command Palette	Ceneral Cenera	Pool Details Collection of MAC Blocks. MAC Blocks From 002585555AA	0 Stee 24	() o 1-1024 +
		<	Cancel		Back Create

Step 5. Repeat this procedure for the MAC Pool for the vNIC pinned to Fabric Interconnect B, shown below:

≡	cisco Intersight	📲 Infrastructure Service 🗸		Q Search	ତ 4 ନ ତ
:@:	Overview	Pools > MAC Pool Create			
(0)	Operate ^ Servers Chassis Pabric Interconnects HyperFlex Clusters Integrated Systems Configure ^ Profiles Pools w Command Palette ×	 ceneral Pool Details 	Pool Details Collection of MAC Blocks. MAC Blocks From 0025:85:55:58	© Size 24	() o 1 - 1024 +
		<	Cancel		Back Create

The screenshot below details two MAC Pool for each virtual NIC (vNIC) pinned to each Fabric Interconnect:

≡	tiste Intersight	📌 Infrastructure Service 🗸			Q Search	Ø 4 ₽ @ A
iĝi	Overview	Pools				
(0)	Operate	Pools Reserved Identifiers VRFs				
,c	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles	* All Pools ● + Add Filter IP = MA	C 7 Wuld 7 No Uuid Pools	WWNN = NO WWNN POOLS	C Expert 3 items found 10 WWPN = NO WWPN POOLS	Create Pool → per page K (1 of 1) K IQN 7 NO IQN POOLS ←
	Templates	Name C Type	Size 0	Used Available	Reserved Description	🗧 Last Update 💈 🖗
	Policies	MAC-B MAC	24	0 24	0	a few seconds a ···
	Pools	MAC-A MAC	24	0 24	0	2 minutes ago ····
		Ru-IP-Pool IP	4	0 4	0	7 minutes ago ····
New Navk to He	Command Palette × gate Intersight with Ctrl +K or go tp > Command Palette					6 t <u>1</u> d1 5 9

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. Select Organization, Enter a Name for UUID Pool and click Next.
- Step 4. Enter a UUID Prefix (the UUID prefix must be in hexadecimal format xxxxxxx-xxxx).
- **Step 5.** Enter UUID Suffix (starting UUID suffix of the block must be in hexadecimal format xxxx-xxxxxxxxx).
- Step 6. Enter the size of the UUID Pool and click Create. The details are shown below:

≡	eisco Intersight 🦂 🖧 In	frastructure Service 🗸		Q Search	Ø	Ъ	¢	0	R
:¢:	Overview								
©	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Policies Pools	 Ceneral Pool Details 	Pool Details Collection of UUID suffix Blocks. Prefix * 9999999:5555 5555 • UUID Blocks From 3000 53335333353	e Size 24			0 1 - 102	0 24	+
			Cancel				Back	Creat	•

Create Server Policies

Procedure 1. Create BIOS Policy

Table 9 lists the required polices for the BIOS policy.

Table 9.	Policies	required	for	domain	profile
Table 5.	1 0110103	requireu	101	uomann	prome

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

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

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

=	diade Intersight	}8 Infrastructure Service ∨		Q Searc	h	⊘ ◎ 2 ⊄1 15 ♀ ● 58 6	10 Ø A
÷.	Overview	+ Policies Create					
0	Operate Servers Chassis Fabric Interconnects HyperFlek Clusters Virtuslization Kubarnetes Integrated Systems Configure	Filters Platform Type Al © UCS Server UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernettes Cluster	Adapter Configuration Adapter Configuration Brost Brost Certificate Management. Device Connector Drive Security Libernel Adapter	Ethermet QoS PC Zone Plan Channel Adspter Fibre Channel Melwork Fibre Channel OoS Firmware M/G Access	ISCSI Static Target LAN Connectivity LDAP LOCal User Network Connectivity NTP Persistent Memory	SD Card Serial Over LAN SMTP SNMP SSH Sterage Oyslog	
(Profiles Templates Pedicies Pools		Ditrinet Network Fitnemet Network Control Uthernet Network Group	IPAIl Over LAN ISCSI Adopter ISCSI Boot	SAN Connectivity	Vinusi Koka	Start

Step 3. Select Organization and 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

			A Management	
	Boot Performance Mode Max Performance	× 0	APBDIS platform-default	
General				
Policy Details				
	Downcore Control platform-default	~ 0	streaming Stores Control platform-default	
	Fixed SOC P-State		DE C-States	
	platform-default	~ ©	platform-default	
	CCD Control		CPU Downcore control	
	platform-default	~ 0	platform-default	
	CPU SMT Mode		ACPI SRAT L3 Cache As NUMA Domain	
	platform-default	× ©	platform-default	
	Channel Interleaving		Cisco xGMI Max Speed	
	platform-default	v ©.	platform-default	
	Closed Loop Thermal Throttling		Processor CMCI	
s > BIOS	Closed Loop Thermal Throttling platform-default	~ 0	Processor CMCI platform-default	
	Closed Loop Thermal Throttling platform-default	~ 0	Processor CMCI platform-default	
s → BIOS eate	Closed Loop Thermal Throttling platform-default	~ @	Processor CMCI platform-default	
s → BIOS ∋ate General	Closed Loop Thermal Throttling platform-default	~ 0	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default	v 0 v 0	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override	v 0 v 0	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default	~ 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default	× 0 × 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default	
s > BIOS Deate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology	× 0 × 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default Demand Scrub	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default	× 0 × 0 × 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default Demand Scrub platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default	v 0 v 0 v 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default Demand Scrub platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support	× 0 × 0 × 0	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support platform-default	· 0 · 0 · 0 · 0	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support platform-default	· 0 · 0 · 0 · 0	Processor CMCI platform-default Energy Performance performance CPU Performance platform-default Demand Scrub platform-default DRAM Clock Throttling platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support platform-default Energy Efficient Turbo	· • •	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support platform-default Energy Efficient Turbo platform-default	· • •	Processor CMCI platform-default	
s > BIOS eate General Policy Details	Closed Loop Thermal Throttling platform-default Core Multi Processing platform-default Frequency Floor Override platform-default Power Technology platform-default Direct Cache Access Support platform-default Energy Efficient Turbo platform-default	· • •	Processor CMCI platform-default	

structure Service 🗸		Q Search	0 4 6 0
icies > BIOS			
reate			
General	Intel(R) VT	IIO Error Enable	
-	platform-default	v o platform-default	~ O
2 Policy Details			
	DCU IP Prefetcher	KTI Prefetch	
	platform-default	v o platform-default	~ 0
	LLC Brefeteb	latel Mamori Istados és s	
	platform-default	 o platform-default 	~ ©
	Package C State Limit	Patrol Scrub	
	(co or state	 o protronmocrasic 	
	Patrol Scrub Interval *	Processor C1E	
	platform-default	 platform-default 	~ ©
	B		
	platform-default	Processor C6 Report ✓ Ø platform-default	× 0
		Provide a series of the series of	
	CPU C State	P-STATE Coordination	
	platform-default	✓ ◎ platform-default	✓ ②

Step 5. Click Create.

Procedure 2. 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.

≡	eisco Intersight 🍂	Infrastructure Service 🗸		Q Search	0 4 0 0 A
:8:	Overview				
© ,•	Oparata ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure ^ Profiles Templates	General Policy Details	Policy Details Ad policy datalis Privilegia Level admi	∀ A1Flatforms UCS Server 0	Standslane)
Nev Nev to H	Pools Command Palatta pole Interrupt with Christ or on abo - Command Palatte	<	Cancel		Back Create

Step 6. Click Save.

Procedure 3. Create Storage Policy

The Storage policy allows you to create drive groups, virtual drives, configure the storage capacity of a virtual drive, and configure the M.2 RAID controllers.

In this configuration, Rubrik certified C240 M6 LFF nodes are configured with:

- 2x M.2 SSDs managed through M2 RAID Controller. A RAID1 configuration would be created across these drives.
- 12x Large Form Factor (LFF) drives managed through pass through SAS controller. These drives are configured in JBOD mode.
- Step 1. Click Infrastructure Service, select Policies, and click Create Policy.
- Step 2. Select UCS Server, Storage and click Start.
- **Step 3.** Select Organization, Name the Storage policy, then click Next.
- Step 4. Select UCS Server (FI-Attached).
- Step 5. Change the Default Drive State' to JBOD
- **Step 6.** Enable M.2 RAID Configuration and select MSTOR-RAID-1 (MSTOR-RAID). (All Changes are marked in RED).

= 앱ata Intersight	🚓 Infrastructure Service 🗸		Q Search	0 4 4 6
Overview	Policies > Storage Create			
Operate Servers	Ceneral	General Configuration	V All Platforms UCS Set	ver (Standalone) UCS Server (FI-Attach
Fabric Interconnects HyperFlex Clusters	2 Policy Details	Use JBOD drives for Virtual Drive creation © Unused Disks State		
Integrated Systems Configure	^	Na Change	~ 0	
Templates Policies		Secure JBOD Disk Slots	0	
Pools		M.2 RAID Configuration		
New Command Palette	× 10	Slot of the M.2 RAID controller for virtual drive creation MISTORRAID-1 (MISTORRAID) V 0		
		Cancel		Back

Step 7. Click Create.

LAN Connectivity Policy

LAN Connectivity Policy determines the connections, and the network communication resources between the server and the LAN on the network. Some of the key best practices which should be considered before creating a LAN Connectivity Policy for Rubrik nodes are explained below:

- To allow network access to Rubrik nodes, the LAN connectivity policy is used to create (four)4x virtual network interfaces (vNICs); vNIC0, vNIC1, vNIC2, VNIC3. vNIC0 and vNIC1 are pinned to Switch ID A and Switch ID B respectively, similarly vNIC2 and vNIC3 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.
- Even though (four) 4x vNICs only (two)2 vNICs (vNIC2 and vNIC3) were created and are configured through Rubrik OS. vNIC0 and vNIC1 are never used by Rubrik OS. Four vNICs are created to ensure compatibility of configuration between C-Series nodes connect to Cisco Fabric Interconnect and standalone Cisco UCS C-Series nodes which allow Cisco UCS VIC directly connected to a uplink switch such as Cisco Nexus 9000 series.
- The primary network VLAN for Rubrik should be marked as native or the primary network VLAN should be tagged at the uplink switch.
- The two vNICs (vNIC2/vNIC3) managed by Rubrik for all UCS Managed mode or Intersight Managed mode (connected to Cisco UCS Fabric) should be in Active-Backup mode (bond mode 1). C-Series nodes connected to Cisco Fabric Interconnect does not support Active-Active mode (802.3ad / mode 4). Ref. <u>https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-b-series-blade-</u> <u>servers/200519-UCS-B-series-Teaming-Bonding-Options-wi.html</u>

Figure 11 shows the mapping of VNIC2 and vNIC3 created in LAN connectivity Policy to network ports as identified on Rubrik nodes.

	King ports							
Port I	Device	Driver	I	State	I	Link	I	Speed
bond0 l			I	սք	I	yes	I	50000 Mb /s
bond1	I		I	down	I	no	I	Unknown !
eth0	Cisco VIC NIC (rev a2)	enic	I	down	I	no	I	Unknown !
eth1	Cisco VIC NIC (rev a2)	enic	I	down	I	no	I	Unknown !
rketh0	Intel 10G X550T	ixgbe	I	down	I	no	I	Unknown !
rketh1	Intel 10G X550T	ixgbe	I	down	I	no	I	Unknown !
rketh2	Cisco VIC NIC (rev a2)	enic	I	սք	I	yes	I	50000Mb/s
rketh3	Cisco VIC NIC (rev a2)	enic	I	սք	I	yes	I	50000Mb∕s
Bond1 Mode is fo Bond1 bond Current act WARNING: Bond1	ault-tolerance (active-backup) ports are: rketh0 rketh1 ive port is None has no active ports and is not o	operational						
Checking for MC /var/log/mcelog	Es is clean							

Figure 11. vNIC2 mapped with network ports on Rubrik node

Table 10 lists the policy details which would be created through Intersight.

Table 10. LAN connectivity Policy details

Network Port	Mac Pool	Switch ID	PCI Order	OS mapping
vNIC0	MAC Pool A	А	0	eth0
vNIC1	MAC Pool B	В	1	eth1
vNIC2	MAC Pool A	А	2	rketh2
vNIC3	MAC Pool B	В	3	rketh3

Procedure 4. Create LAN Connectivity Policy

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

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

E disco Intersight 3	💲 Infrastructure Service 🗸		Q Sear	ch (⊘ ⊈ (Q (053) (A 14)	0
C Overview	+ Policies Create						
Operate ^	Filters	G, Search					
Enassis Fabric Interconnects HyperFlex Clusters Virtualization Kubernetes Integrated Systems Configure Profiles Templates Policies Pools	Platform Type All US Sorver UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	Adapter Configuration BIOS Boot Order Certificate Management Device Connector Drive Security Ethernet Adapter Ethernet Network Ethernet Network Ethernet Network Orostral	Ethernet GoS FC Zone Fibre Channel Adapter Fibre Channel Network Fibre Channel GoS Fibre Channel Adapter ISCSI Adapter ISCSI Boot	I SCSI Static Target LAN Connectivity LDAP Local User Network Connectivity NTP Persister: Memory Prower SAN Connectivity	SD Card Serial Over LAA SAMP SAMP SSH Storage Systog Virtual KVM Virtual Media		
		Cancel					Start

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

Step 4. Click Add vNIC.

≡	dials Intersight	🖧 Infrastructure Service 🗸	Q Search 🥥 (0.2 qC) 15 Q (0.53 (A.14) (?)
:@:	Dverview	Policies > LAN Connectivity	
0	Operate ^		
	Servers	General	None Pool Static
	Chassis	2 Policy Details	
	Fabric Interconnects		This option ensures the New name is not associated with the policy
	HyperFlex Clusters		vNIC Configuration
	Virtualization		
	Kubernetes		Manual vNICs Placement Auto vNICs Placement
	Integrated Systems		
,0	Configure ^		For manual placement option you need to specify placement for each vNIC. Learn more at Help Center
	Profiles		Add WICE Editor
	Templates		
	Policies		□ / □ Q. Add Filter 0 items found 9 ∨ per page 12 C 0 of 0 3 32
	Pools		Name Slot ID Switch ID PCI Order Pailover Pin Group MAC Pool
			NO ITEMS AVAILABLE
		<	Cancel Back Create

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

Policies > LAN Connectivity						
Create						
Add vNIC						
	Constal					
	General					
	Name * vNIC0 © Pin Group Name	~ 0				
	MAC					
	Pool Static					
	MáC Bool * 0					
	Selected Pool MAC-A × @ Ø					
	Placement					
	Simple Advanced					
	When Simple Placement is selected, the Slot ID and PCI Link are automatically determined by the systi vNICs are deployed on the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1. Simple assignment is not applicable 13xx series VICs that support dual-link.	em. N				
Infrastructure Service 🗸	Q Search		Ø	₽	¢	0
Policies > LAN Connectivity						
	Switch ID *					
	A ~ 0					
	PCI Order					
	0 () 0					

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

≡	👷 🖓 🕺	Infrastructure Service 🗸		Q Search	Ø @2 ⊄1 15	Q 053 A14	0	Я
*	Overview	Policies > LAN Connectivity > Create	twork Group					
ة بر ا	Operate > Servers > Chassis > Fabric Interconnects > HyperFlax Clustars > Virtualization > Kubarnates > Integrated Systems > Configure > Porfiles > Podicies > Pools >	General Policy Details	Policy Details Add colley defaits VLAN Settings Allowed VLANs 1080,1001,1002	€ Native VLAN 1091			2 <u>0</u> - 4093	
		<	Cancel			Back	Create	

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.

E	the Intersight	🍂 Infrastructure Service 🗸		Q Search	0 000 43 10	Q 000 A10 (2	۶ (
÷	Overview	Policies > LAN Connectivity > Create	twork Control				
0	Operate Servers Chassis Fabric Interconnecta HyperFlex Clusters Virtualization Kubernetes Integrated Systems Configure Profiles Templates Pools	 General Policy Datails 	Policy Details Add policy details This policy is applicable only for (Prable CD® @ MAC flegister Mode @ MAC flegister Mode @ MAC flegister Mode @ MAC flegister Mode @ Lith Down Warning Mac Security Progs @ Advo Deny LLDP Enable frammal @ Enable frammal @ Enable frammal @	UCS Servers (FI-Attaches)	Dirk connectivity is lost,		
		<	Cancel			Back Crea	ate

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

≡	and Intersight	🖧 Infrastructure Service 🗸		Q Search	Ø@≥ ⊈1®	Q 053 A14	ଡ
:@:	Overview	Policies > LAN Connectivity > Create	6				7
0	Operate	General Policy Details	Policy Details Add policy details QoS Settings	ал У	Platforms UCS Server (Stended	one) LCS Server ()1 A	(Inched)
ş	HyperFlex Clusters Virtualization Kubernetes Integrated Systems Configure Profiles	•	MTU, Bytes 9000 Burst 10240 Enable Trust Host CoS ©	C 0 8000 1500 - 6000 0 0 C 0 Priority L 0 DestetFlort			00000 V 0
	Templates Policies Pools		Cancel			Back	reate

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.

≡	the Intersight	📽 Infrastructure Service 🗸		Q Search	Ø@2 ¢1 16 Ç	053 🛯 🕐 🖓
X\$K	Overview	Policies > LAN Connectivity > Create	apter			
0	Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters	General Policy Details	Interrupt Settings Interrupts 10 Interrupt Coalescing Type Min	Interrupt Mode MStx	interrupt Timer, us V 0 125	() e 0 - 65535
۵,	Virtualization Kubernetes Integrated Systems Configure ^ Profiles		Receive Receive Queue Count 8 Transmit Toescell Queue Count	Receive Ring Size	(; D 64 - 16364	
	Tempistes Policies		4 Completion	Completion Size	(\$) © 64 - 16384	
	Pools	K	Usinguistion Quistue Count 12 Uplink Failback Timeout (seconds) 5 Cancel	Orpuston King Size 1	(; ● 1 - 258	Back Create

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

Infrastructure Service 🗸		Q Search	\odot	₽	¢	0	۶
Policies > LAN Connectivity							
Create							
	Consistent Device Naming (CDN)						
	Source						
	vNIC Name 🗸 🛇						
	Failover						
	Enabled ©						
	Ethernet Network Group Policy * O						
	Selected Policy Ru-ethernet-netgroup						
	Ethernet Network Control Policy * ©						
	Selected Policy Ru-ethernet-networkcontrol × © 🖉						
	Ethernet QoS * 0						
	Selected Policy Ru-ethernetQoS X						1
	Selected Policy Ru-ethernet-adapter						
-							
Cancel						Add	

Dicies > LAN Connectivity															
		No.													
General															
2 Policy Details			None	1	001	St	atic)							
		-													
		U	This option	ensures the IC	N name is	not associate	ed with the p	olicy							
	Ň		Configura	tion											
	\ (Configura Manual vN	tion ICs Placemen	t	Auto	vNICs Place	ement							
	(Manual vN For manual	tion ICs Placemen placement op	t ion you nee	Auto ed to specify	vNICs Place	ement or each v	NIC. Learn mor	re at Help Cer	nter				
		NIC C	Manual vN For manual	tion ICs Placemen placement op	t ion you nee	Auto ed to specify	vNICs Place	ement or each v	NIC. Learn mor	re at Help Cer	ater	Gr	aphic vi	NICs Ed	itor
		NIC C	Manual vN For manual vNIC	tion ICs Placement placement op	t ion you nee	Auto ed to specify	vNICs Place	ement or each v	NIC. Learn mor	re at Help Cen 10 ∽ per j	nter page 🕑 <	Gr	sphic vi	NICs Ed	itor
		Add	Configura Manual vN For manual vNIC	CS Placement placement op Q. Add Fi S Stot ID	t ion you new ter	Auto ed to specify Switch ID	vNICs Place placement fc	ement or each v	NIC. Learn mor 1 items found Failover	re at Help Cen 10 ~ per i 2 Pin G	nter page (K) < Sroup ÷	Gr 1 MAG	of 1 D	NICs Ed	itor © §
			Manual VN For manual VNIC	tion ICs Placement placement op Q Add Fi Siot ID Auto	t ion you nee ter 2	Auto ed to specify Switch ID A	vNICs Place placement fo : PCI Or 0	ement or each v	NIC. Learn mor 1 items found Failover Disabled	re at Help Cer 10 ∽ per j : Pin 0 -	nter page 또 도 Sroup :	Gr 1 MAC	of 1 D C Pool	NICs Ed	itor © 9

Step 13. Add vNIC as vNIC1. Select the same setting as vNIC0.

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

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

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

Policies > LAN Connectivity	
Create	
Add vNIC	
	General
	Name *
	vNIC1 O Pin Group Name v o
	MAC
	Pool Static
	MAC Pool * 0
	Selected Pool MAC-B X OP
	Placement
	Simple Advanced
	When Simple Placement is selected, the Slot ID and PCI Link are automatically determined by the system.
	vNICs are deployed on the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1. Simple assignment is not applicable for 19 marchine NICs that waves the determines the first VIC.
	i six series vius that support qual-link.
	Switch ID *
	PCI Order
	1 () 0
	Consistent Device Naming (CDN)
	Source
	wild Name
	Fallouar
	Fallover
	Enabled ©
	Ethernet Network Group Policy * ©
	Selected Policy Ru-ethernet-netgroup X @ 🧷
	Ethernet Network Control Policy * O
	Selected Policy Ru-ethernet-networkcontrol × Φ 🖉
	Ethernet QoS * O
	Selected Policy Ru-ethernetQoS × Φ 🖉
	Ethernet Adapter * O
	Selected Policy Ru-ethernet-adapter × Φ Ø
	ISSERAND C
	Select Policy 🗄
	Connection
Cancel	Add

Step 17. Repeat steps 1 – 16 to add vNIC2 and vNIC3.

Step 18. vNIC2 and vNIC3 will have the same Ethernet Network Group Policy, Ethernet Network Control Policy, Ethernet QoS, and Ethernet Adapter policy as created for vNIC0 and VNIC1.

- vNIC2 needs to be pinned to Switch ID A, with AMC Pool B and PCI Order as 2.
- vNIC2 needs to be pinned to Switch ID B, with MAC Pool B and PCI Order as 3, select B, and the PCI Order should be 1.

Step 19. Ensure the LAN connectivity Policy is created as shown below with 4x vNIC and click Create.

t	-LANConnectivity_4vNit	J								
Ganaral	0	This optic	on ensure	s the IQN nan	me is not associa	ed with the policy				
Policy Details	VNIC	: Configu	ration							
		Manual	vNICs Pla	cement	Aut	o vNICs Placemen	t			
	0	For manu	al placem	ent option yo	ou need to specif	placement for each	ch vNIC. Learn mor	a at Help Center		
	Ad	d vNIC						(Graphic vNICs E	Editor
			Q	Add Filter		🕒 Export	4 items found	13 🗸 per page 🗵 🔇	1_of1 ≥ ⊠	\odot
		Name	÷ 5	Slot ID	Switch ID	C PCI Order	C Failover	C Pin Group	MAC Pool	Ģ
		VNIC1	1	Auto	В	1	Disabled	-	MAC-B	
		vNIC3	ļ	Auto	В	3	Disabled	-	MAC-B	
		vNIC0	Å	Auto	A	0	Disabled	-	MAC-A	
		VNIC2	1	Auto	A	2	Disabled	-	MAC-A	

Procedure 5. Create Boot Order Policy

The boot order policy is configured with the Unified Extensible Firmware Interface (UEFI) boot mode. The following are the Boot Order mapping for Rubrik nodes:

- PXE Boot
- Virtual Media to mount ISO
- Virtual Drive with RAID1 created across (two)2x M.2 boot drives. Rubrik OS is installed on this Virtual Drive.
- **Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.
- Step 2. Select UCS Server, Boot Order, and click Start.
- **Step 3.** Select Organization, 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 select local disk and enter device name as 'os' and Slot as 'MSTOR-RAID.'

Policies > Boot Order Create				
General	Add policy details		C All Platforms UCS Server (Standalone)	UCS Server (FI-Attached)
2 Policy Details	Configured Boot Mode Unified Extensible Firmware Interface (UEFI) Legacy Enable Secure Boot Add Boot Device			
	- Local Disk (os)		En	abled 🗊 \land 🗸
	Device Name * os	٥	Slot MSTOR-RAID	٥
	Bootloader Name	٥	Bootloader Description	٥
	Bootloader Path	٥		

Step 6. Select Add Boot Device and click vMedia and name the 'vmedia-1' device name.

Policies > Boot Order Create			
 General Policy Details 	Add policy details Configured Boot Mode	V All Platforms UCS Server (S	itandalone) UCS Server (FI-Attached)
	+ PXE Boot (PXE-boot)	None	Enabled

Step 7. Select Add Boot Device and select PXE Boot, enter device name as 'PXE-boot' and interface name as vNICO.
	Add policy details		
General		All Platforms UCS Server (itandalone) UCS Server (FI-Attached
Policy Details	Configured Boot Mode ① Unified Extensible Firmware Interface (UEF) Legacy Enable Secure Boot		
	Add Boot Device ~		Enabled III · · · · ·
	Device Name * PXE-boot	IP Type D None	v ©
	Interface Name * vNIC0	0	

Step 8. Ensure the boot Device Order is as provided in the following screenshot, with 1st Boot Order as PXE boot, 2nd Boot Order as vMedia and 3rd Boot Order as os(local disk). Click Create.

Policies > Boot Order Create		
 General Policy Details 	Add policy details Configured Boot Mode	All Platforms UCS Server (Standalone) UCS Server (FI-Attached)
	Add Boot Device > + PXE Boot (PXE-boot) + Virtual Media (vMedia1) + Local Disk (os)	Enabled 1 A V Enabled 1 A V Enabled 1 A V
<	Cancel	Back Create

Procedure 6. 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 Rubrik 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.

≡	aliala Intersight 🏻 縄 Infr	rastructure Service 🗸	Q search 🥝 🕫 2 Q 😨 A
	Overview	Policies > IMC Access	
0	Operate ^ Servers Chassis	General Policy Details	All Platforms UCS Server (FI-Attached) UCS Chassis A minimum of one configuration must be enabled. Policies like SNMP, vMedia, KMIP and Systog are supported via Out-Of-Band. Check here
	Fabric Interconnects HyperFlex Clusters Integrated Systems		for more info, Help Centre
<u>ی</u>	Analyze A Explorer New Configure A Profiles		IPv4 address configuration IPv6 address configuration
	Templates Policies Pools		IP Pool * Selected IP Pool Ru-InBand-Pool Image: Control - Band Configuration @
Ne Nav to H	Command Palette × gate Intersight with Ctrl+K or go elp > Command Palette	<	IP Pool * ⊙ Selected IP Pool Ru-IP-Pool X Ø Ø Ø Ø Cancel Back Create

Procedure 7. Create Local User Policy

Note: Local User Policy creates local user and password for access to KVM through Server Management IP allocated through IMC Access Policy. For example, access to server console through https://<<KVM-IP>>/kvm/.

- **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. Select Organization, Name the Local User policy and click Next.

Step 4. Change the password history to '0', Add a local user with the name 'RUBRIK' and role as admin and enter a password. This is used to access the server KVM through KVM IP. Click Create. You can create multiple Local Users as required.

cisco Intersignt and Infrastructure Service V	Q search O 🕫 🗘 🕐
Overview Policies > Local User Create	
Operate ^ Servers Or General	Password Properties
Chassis 2 Policy Details	Enforce Strong Password
Fabric Interconnects	Password History Always Send User Password ©
HyperFlex Clusters	0-5
Integrated Systems	
Analyze	Local users
Explorer New	This policy will remove existing user accounts other than the ones configured with this policy. However, the default admin user account is not deleted from the endpoint device. You can only enable/disable or change account password for the admin account by creating a user with the user name and note as 'admin'. If there are no users in the policy, only the admin user account will be available on the endpoint of the adminument of the time.
Configure ^	device, by default, invit support is enabled for all users
Configure ^ Profiles	Add New User
Configure ^ Profiles Templates	device, by default, in Mi support is enabled for all users Add New User
Configure ^ Profiles Templates Policies	Advice. by default, in Mit support is enabled for all users Add New User - RUBRIK (admin) Ø
Configure ^ Profiles Templates Policies Pools	Add New User - RUBRIK (admin) @ Username * Role RUBRIK
Configure ^ Profiles Templates Policies Pools	Add New User

Create Server Profile

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 new Cisco UCS C-Series nodes deployed for Rubrik cluster. For more information, go to: <u>https://www.intersight.com/help/saas/features/servers/configure#server_profiles</u>

The pools and policies attached to Server Profile Template are listed in Table 11.

Pools	Compute Policies	Network Policies	Management Policies	Storage Policy
KVM Management IP Pool for In-Band and Out-of-Band (OOB) Access	BIOS Policy	LAN Connectivity Policy	IMC Access Policy	Rubrik storage policy for RAID1 configuration across 2x M.2 cards. This is utilized for Rubrik OS installation
MAC Pool for Fabric A/B	Boot Order Policy	Ethernet Network Group Policy	IPMI over LAN	
UUID Pool		Ethernet Network Control Policy	Local User Policy	
		Ethernet QoS Policy	Serial Over LAN Policy	
		Ethernet Adapter Policy		

Table 11. Policies required for Server profile template

≡	else Intersight	🏂 Infrastructure Service 🗸	Q Search	0 \$ \$ @ \$
:\$:	Overview	Templates		
0	Operate	UCS Server Profile Templates		Create UCS Server Profile Template
	Servers Chassis	* All UCS Server Prof	G Export 0 items found	10 v per page 📧 🤇 D of C 🗦 🗩
	Fabric Interconnects HyperFlex Clusters	Name : Usage Target Platform : Description		Last Update :
	Integrated Systems	NO ITEMS AVAILABLE		
9	Configure			K ≤ 0 of 0 ≥ ≥
	Profiles Templates			
	Policies			
	Pools			
Ne	Command Palette			
Navi to H	gate Intersight with #+K or go elp > Command Palette			
Novi to H	gate Intersight with № 4K or go elp > Command Palette			

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

≡	ahala Intersight 🍂	Infrastructure Service 🗸		Q Search	Ø	FJ 🔹	٥	0	8
	Overview	← Templates Create UCS Server	Profile Template						
(0) (0)	Operate Servers Chassis Pabric Interconnects HyperFlex Clusters Integrated Systems Analyze Analyze Configure Profiles	 General Compute Configuration Management Configuration Storage Configuration Network Configuration Summary 	General Enter a name, description, tag and select a platform for th Organization * Rubrik Templato 1 Target Platform © UUSS Server (F)-Attached Out Temp	ne server profile template.					
(Ne Nec To H	Templates Policies Pools Command Palette Command Palette Policies Pools Command Palette Policies Pool	•	Set rags Description <10 Close	26 26				Nex	

Step 3. Select UUID Pool and all Compute Policies (BIOS and Boot Order Policy) created in the previous section. Click Next.

≡ ::!:::l: Intersight	€ Infrastructure Service ∨	Q Search	ତ ସ ହ ତ ହ
Ø. Overview	← Templates Create UCS Server F	Profile Template	
 Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze Analyze Configure Profiles Templates Pools 	 Compute Configuration Management Configuration Storage Configuration Network Configuration Summary 	Compute Configuration Create or select existing Compute policies that you want to associate with this template. UUID Assignment UUID Pool Selected Pool Ru-UUID × • • • • • BIOS Boot Order Firmware Power Themal Virtual Media	Ru-BloS (E) Ru-BootOrder (E) []
New Command Palette × Navigate Intersight with Ctrl+K or go to Help > Command Palette	<	Close	Back Next

Step 4. Select all Management Configuration Policies (IMC Access, IPMI over LAN and Local User policies) and attach to the Server Profile Template.

=	elise Intersight 🏻 🍰	; Infrastructure Service 🗸	Q Search	⊘	¢1 (2) () ()	A
	Overview	← Templates Create UCS Server P	rofile Template					
0 0 9	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze Analyze Configure Pooflies Poolicies	 Compute Configuration Compute Configuration Management Configuration Storage Configuration Network Configuration Summary 	Management Configuration Create or select existing Management policies that you want to associate with this template. Certificate Management IMC Access IPMI Over LAN Local User Serial Over LAN SNMP Syslog Virtual KVM			© IMC. © Io	Access-1 Ru-IPM caluser-1	
Nav to H	igate Intersight with Ctrl+K or go elp > Command Palette	<	Close			в	ack	Next

Step 5. In the next screen, under Storage Configuration, Select Storage Policy and click Next.

≡ dualta Intersight	နိုင္ငံ Infrastructure Service 🗸	٩	Search	ର ଏବ ତ ଓ ଓ ୪
ê: Overview	← Templates Create UCS Server	Profile Template		
Operate Operate Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze Analyze Analyze Configure Profiles Templates Pools New Kow Command Palette *	 Ceneral Compute Configuration Management Configuration strage Configuration Network Configuration Network Configuration Summary 	Storage Configuration Create or select existing Storage poticles that you want to associate with this temp Drive Security SD Card Storage	Nate.	ا Ru-storage ا
Navigate Intersight with Ctrl+K or go to Help > Command Palette	<	Close		Back Next

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

≡	المعنية: Intersight	Infrastructure Service 🗸	Q Search	0	¢1 🔹 I) ()	A
:@:	Overview	← Templates Create UCS Server P	Profile Template				
0	Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters	General Compute Configuration Management Configuration	Network Configuration Create or select existing Network Configuration policies that you want to associate with this template. LAN Connectivity SAN Connectivity	Ru-LANConne	ectivty_4vNIC	1	
©.	Integrated Systems Analyze Explorer Kew Configure	Storage Configuration Network Configuration Summary					
	Profiles Templates Policies Pools						
Ne Navi to H	Command Palette X Gate Intersight with Ctrl+K or go elp > Command Palette	K	Close			ack N	Vext

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

← Templates Create UCS Server Profile Template

 General Compute Configuration Management Configuration Storage Configuration Network Configuration 	Summary Verify details of the templ General Template Name Rubrik-Template-1 Target Platform UCS Server (FI-Attach	ate and the policies, resolve erro	ors and deploy. Organization Ru-Org					
3 Summary	Compute Configuration BIOS Boot Order UUID	Management Configuration	Storage Configuration	Network Configuration	E ((rrors/Warn D) Ru-Boo R	u-BIOS () DtOrder () u-UUID X	
<	Close				E	Back Dei	rive Profiles	8
Infrastructure Service 🗸			Q Search		⊚≮	I 🔹 🗘	0	<u>م</u>
← Templates Create UCS Server I	Profile Templ	ate						
General Compute Configuration Management Configuration	Summary Verify details of the temp ~ General Template Name Rubrik-Template-1	plate and the policies, resolve erro	ors and deploy. Organization Ru-Org					

Storage Configuration	Rubrik-Template-1 Target Platform	chad)	Ru-Org		
6 Summary	Compute	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)
	IMC Access				IMCAccess-1
	IPMI Over LAN				Ru-IPMI
	Local User				localuser-1
	Close				Back Derive Profiles

Infrastructure Service $$			Q Search		⊘ ⊈2	Q ()	
← Templates Create UCS Server P	rofile Templat	е					
 Ceneral Compute Configuration Management Configuration Storage Configuration Network Configuration Summary 	Summary Verify details of the template General Template Name Rubrik-Template-1 Target Platform UCS Server (FI-Attached) Compute Configuration Storage	and the policies, resolve error Management Configuration	rs and deploy. Organization Ru-Org Storage Configuration	Network Configuration	Errors, (0)	Warnings Ru-storage	
<	Close				Back	Derive Prof	iles
Infrastructure Service $$			Q Search		⊘ ⊈⊇	Q ()	A
← Templates Create UCS Server P	rofile Templat	e					
 General Compute Configuration Management Configuration Storage Configuration Network Configuration 	Summary Verify details of the template General Template Name Rubrik-Template-1 Target Platform UCS Server (FI-Attached	e and the policies, resolve erro	rs and deploy. Organization Ru-Org				
3 Summary	Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors (0) Ru-LANConr	/Warnings ectivty_4vNIC	

Back Derive Profiles

Install Rubrik CDM on Cisco UCS C-Series Nodes

Rubrik OS can be installed on Rubrik certified Cisco UCS C240 M6 LFF nodes with one of two options:

• Install OS through Intersight OS installation.

This allows installing the Rubrik CDM 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 C-Series nodes provisioned for the Rubrik CDM cluster.
- It reduces Day0 installation time by avoiding mounting the ISO as Virtual Media on the KVM console for each node deployed for Rubrik 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 C-Series nodes certified for the Rubrik CDM.

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

≡	diada Intersight	💃 Infrastructure Service 🗸	Q Search	A @ 0 #
:¢:	Overview	Templates		
0	Operate ^	UCS Server Profile Templates		
	Servers			Create UCS Server Profile Template
	Fabric Interconnects		Export 2 items found	10 v perpage K < 1 of 1 > ×
	HyperFlex Clusters	Name : Usage : Target Platform : Description		Last Update the second
	Integrated Systems	Rubrik-Template-1 0 UCS Server (FI-Attached)		Dec 22, 2023 3:38 PM
Ø.	Analyze o	Ru-SP-Template-1 3 UCS Server (FI-Attached)		Oct 18, 2023 7:38 PM
	Explorer	201		
۹,	Configure ^			
	Profiles			
	Templates			
	Policies			
	Pools			

Step 2. Select the Server Template created in previous section, click the ... icon and select Derive Profiles.

≡	ntersight	At Infrastructure Service V Q. Search	୍ ତ ସ ହ ତ ହ
:@:	Overview	Templates	
	Operate ^	UCS Server Profile Templates	
	Servers Chassis	* All UCS Server Prof., © +	Create UCS Server Profile Template
	Fabric Interconnects HyperFlex Clusters	Image: Comparison of the second se	10 v perpage K < 1 of 1 > >
	Integrated Systems	Name Osage larger Hattorm Description Rubrik-Template-1 0 UCS Server (FI-Attached)	Dec 22, 2023 3:38 PM
Q	Analyze ^ Explorer New	Image: Server (Fi-Attached) Image: Optimized content of the selected of the select	Oct 18, 2023 7:38 PM ···· Derive Profiles
.0	Configure ^		Clone Delete
	Templates		Edit
	Policies		

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

	General
General	Select the server(s) that need to be assigned to profile(s) or specify the number of profiles that you want to derive and assign the servers later.
Details	∧ UCS Server Profile Template
Summary	Name Organization
	Ru-SP-Template-1 Ru-Org
	Tamet Blatform
	VCS Server (FI-Attached)
	UCS Server (FI-Attached) ^ Server Assignment Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Q Add Filter C Export 4 items found 1f > per page (C) Image: C Export 4 items found 1f > per page (C) 1
	UCS Server (FI-Attached) ^ Server Assignment Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Q Add Filter Q Add Filter Image: Comparison of the serial Number 11 × per page Image: Name 1 + Health USEr Label Model USE Domain Serial Num
	UCS Server (FI-Attached) Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Add Filter Add Filter Health : User Label : Model : UCS Domain Serial Nu : AA09-FI-DP-6454-1 Chasting UCSC-C240-M AA09-FI-DP-B WZP26510561
	UCS Server (FI-Attached) Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From Assign Now Fro
	UCS Server (FI-Attached) Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Add Filter Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From a Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From A Resource Pool Chassis Slot Location Serial Number Assign Later Assign Now From Assign Now From A Resource Pool Chassis Slot Location Serial Num Chasse Slot Location Num Chasse Slot Locatio

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

erive			
General	Details		
2 Details	A General	ted names of the profiles.	
3 Summary	Organization * Ru-Org	Target Platform → UCS Server (FI-Attached)	~ D
	Description	<u>کی محمد Set Tags</u>	
	^ Derive		
	1 Name * Ru-SP-Template-1_DER/VED-1	Assigned Server AA09-FI-DP-6454-1	

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

General	Summary Summary of the prof	les that need to be derived from the	e profile template.		
Details	∧ General				
Summary	Template Name Ru-SP-Template- Target Platform UCS Server (FI-Al	1 ttached)	Organization Ru-Org		
	UCS Server Profil	es	Assigned S	Server	
	UCS Server Profil Name Ru-SP-Template	es	Assigned S AA09-FI-D	Server P-6454-1	
	UCS Server Profile Name Ru-SP-Tomplate Compute Configuration	es -1_DERIVED-1 Management Configuration	Assigned 5 AA09-FI-D Storage Configuration	Server P-6454-1 Network Configuration	Errors/Warnings (0)
	UCS Server Profil Name Ru-SP-Template Compute Configuration BIOS	es -1_DERIVED-1 Management Configuration	Assigned S AA09-FI-DI Storage Configuration	Server P-6454-1 Network Configuration	Errors/Warnings (0) Ru-BIOS
	UCS Server Profil Name Ru-SP-Tomplate Compute Configuration BIOS Boot Order	es -1_DERIVED-1 Management Configuration	Assigned S AA09-FI-D Storage Configuration	Server P-8454-1 Network Configuration	Errors/Warnings (0) Ru-BIOS (Ru-BootOrder)

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

.©.	Overview	Profiles		
Ö	Operate	HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles		
	Servers			Create UCS Server Profile
	Fabric Interconnects	+ ALUCS Server Prof ◎ + / ◇	G Export 1 items found	9 ∨ perpage < < 1 of1 ≥ ≥
	HyperFlex Clusters Integrated Systems	Status Inconsistency Reason Target Platform		3 K
	Configure	A Not Deployed 1 (FI-Attached 1) No data available		
l	Templates	Name - Status - Target Platform - UCS Server Template	Server	Last Update ^ &
	Policies	Kunne Content Con	AA09-FI-DP-6454-1	a few seconds ago
	Pools	··· / () (F		বি[ব] 1 of 1 চি চি
New Navi to He	Command Palette × gata Intensight with SK+K or go sip > Command Palette			

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

≡	the Intersight	ွိန်ဖို့ Infrastructure Service 🗸	Q Search	2 A Q 🚥 🚥 🤉 X
:@:	Overview	There are 1 Critical, 1 Warring slerts. Expand All		×
0	Operate A Servers Chassis	Profiles HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles UCS Server Profi	flies	
	Fabric Interconnects HyperFlex Clusters Integrated Systems	* All UCS Server Prof_ © +	C Export 4 items found	Create UCS Server Profile
¢	Profiles Templates Policies	Activate Unassign Server No data available		X
	Pools	Name : Status : Target Platform : UCS	S Server Template Server	Last Update \ddagger
		Ru-SP-Template-1.DERIVE 🛆 Not Deployed UCS Server (FI-Attached) Ru-S	SP-Template-1 AA09-FI-DP-6454-4	7 hours ago ····
N	ew Command Palette	Ru-SP-Template-LDERIVE (A Not Deployed) UCS Server (FI-Attached) Ru-SP-Template-LDERIVE	SP-Template-1 AA09-FI-DP-6454-3	7 hours ago ····
Na	vigate Intersight with Ctrl+K or go	Ru-SP-Template-1_DERIVE (A Not Deployed) UCS Server (FI-Attached) Ru-S	SP-Template-1 AA09-FI-DP-6454-2	7 hours ago ····
to	Help > Command Palette	Ru-SP-Template-1_DERIVE @ 0X UCS Server (FI-Attached) Ru-S	-SP-Template-1 AA09-FI-DP-6454-1	8 hours ago ····
		/ 🖉 🗓 Selected 3 of 4 Show Selected Unselect All		K C 1 af1 5 3

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

Deploy (3 UCS Server Profiles)
Selected UCS server profiles will be deployed to their assigned servers.
If policy configuration requires an immediate reboot and the option below is disabled, then profile deployment will not be initiated.
Reboot Immediately to Activate ③ ^ More Details
G 3 it Deploy (3 UCS Server Profiles) age K < 1 of 1 >> 3 Add Filter Server Profile Name Server Name Reboot
Ru-SP-Template-1_DERIVED-4 AA09-FI-DP-6454-4 YES
Ru-SP-Template-1_DERIVED-3 AA09-FI-DP-6454-3 YES
Ru-SP-Template-1_DERIVED-2 AA09-FI-DP-6454-2 YES
Cancel Deploy

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

 Requests Deploy Server Profile 								×	
Details	Execution Flow								
Status	Progress	Completion						5%	
Marra	Ø Prepare Server Profil	e Deploy					Jul 7, 2023 11:5	i5 AM	
Name Deploy Server Profile	O Power On Server						Jul 7, 2023 11:5	i5 AM	
ID 64a85fa7696f6e330197478a									
Target Type Rack Server									
Target Name AA09-FI-DP-6454-1									
Source Type Server Profile									
Source Name Ru-SP-Template-1_DERIVE									
Initiator andhiman@cisco.com									
Start Time Jul 7, 2023 11:55 AM									
End Time									
Requests									>
* All Requests ◎ + ···	Filter			×	GE	xport 3 items for	ound 12 v per pag	ge 🗵 < _1_ of 1	
Status Executi	on Type								<u>як</u> 24
C In Progress 3 Execute 3									
Name Status	≎ Initiator ≎	Target Type	Target Name	Start Time	÷	Duration	ID	Execution Type	Ģ
Deploy Server P) In Progress :	andhiman@cisc	Rack Server	- AA09-FI-DP-64	7 hours ago		7 h 12 m 2 s	64a9913e696f6	Execute	
Deploy Server P) In Progress	andhiman@cisc	Rack Server	AA09-FI-DP-64	7 hours ago		7 h 12 m 2 s	64a9913e696f6	Execute	
Deploy Server P) In Progress	5% andhiman@cisc	Rack Server	AA09-FI-DP-64	7 hours ago		7 h 12 m 3 s	64a9913e696f6	Execute	
)		K < 1 of 1	

Step 10. Once the Server Profile deployment completes successfully, you can proceed to the Rubrik CDM deployment on the Cisco UCS C-Series nodes.

 \times

				CC CLEAR		0 N	0
Overview	Profiles						
Operate ^	HyperFlex Cluster Pro	files UCS Chassis Profiles UC	CS Domain Profiles	rofiles			
Servers Chassis Fabric Interconnects HyperFlex Clusters	* All UCS Server Pr	of () + , Add Filter		G Export	4 items found 12 v	Create UCS Serve	er Profile
Integrated Systems	Status	Inconsistency Reason	Target Platform				35
	C OV A		FI-Attached 4				
Analyze ^ Explorer New	O OK 4	No data available					
Analyze ^ Explorer New Configure ^	Name	No data available	: Target Platform	UCS Server Template S	erver	Last Update	÷ \$
Analyze ^ Explorer New Configure ^ Profiles	Name	No data available : Status ate-1_DERIVED-2 ② OK	: Target Platform UCS Server (FI-Attacher	UCS Server Template S 1) Ru-SP-Template-1 /	ierver M09-FI-DP-6454-2	Last Update Dec 5, 2023 4:47 PM	÷ 5
Analyze A Explorer New Configure A Profiles Templates	Name	No data available : Status atte-1_DERIVED-2 @ OK tto-1_DERIVED-4 @ OK	: Target Platform UCS Server (FI-Attacher UCS Server (FI-Attacher	UCS Server Template S I) Ru-SP-Template-1 // I) Ru-SP-Template-1 //	ierver 1409-FI-DP-6454-2 1409-FI-DP-6454-4	Last Update Dec 5, 2023 4:47 PM Dec 5, 2023 4:49 PM	÷ ۶
Analyze A New Configure A Profiles Policies	Name Ru-SP-Templa Ru-SP-Templa Ru-SP-Templa	No data available : Status ste-1_DERIVED-2 @ OK ste-1_DERIVED-4 @ OK ste-1_DERIVED-3 @ OK	: Target Platform UCS Server (FI-Attacher UCS Server (FI-Attacher UCS Server (FI-Attacher UCS Server (FI-Attacher	UCS Server Template S NRU-SP-Template-1 NRU-SP-Template-1 RU-SP-Template-1 RU-SP-Template-1	ierver X09-FI-DP-6454-2 X09-FI-DP-6454-4 X09-FI-DP-6454-3	Last Update Dec 5, 2023 4:47 PM Dec 5, 2023 4:49 PM Dec 5, 2023 4:49 PM	÷ ۶
Analyze A Explorer New Configure A Profiles Policies	Name Ru-SP-Templi Ru-SP-Templi Ru-SP-Templi Ru-SP-Templi Ru-SP-Templi	No data available : Status ate-1_DERIVED-2 @ 0K ate-1_DERIVED-4 @ 0K ate-1_DERIVED-3 @ 0K ate-1_DERIVED-1 @ 0K	: Target Platform UCS Server (FI-Attache UCS Server (FI-Attache UCS Server (FI-Attache UCS Server (FI-Attache	UCS Server Template S Ru-SP-Template-1 // Ru-SP-Template-1 // Ru-SP-Template-1 // S) Ru-SP-Template-1 //	A09-FI-DP-6454-2 A09-FI-DP-6454-4 A09-FI-DP-6454-3 A09-FI-DP-6454-3	Last Update Dec 5, 2023 4:47 PM Dec 5, 2023 4:49 PM Dec 5, 2023 4:49 PM Dec 5, 2023 6:32 PM	÷ 5 ⁵

Step 11. Access KVM with KVM username > kvm-user (RUBRIK) 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.



Install OS through Intersight

Procedure 1. Install Rubrik CDM through Cisco Intersight OS Installation feature

This procedure details the process to install the Rubrik CDM operating system through the Cisco Intersight OS installation feature.

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

Note: Make sure the certified Rubrik CDM 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 Rubrik CDM ISO.

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

≡	cisco Intersight	∥∰ System ∨	Q search
Ø	Settings	Software Repository	
•	Admin ^	Firmware Links OS Image Links OS Configuration Files	
l	Software Repository Tech Support Bundles		Add OS Image Link
	Audit Logs	* All OS Image Links +	
	Sessions	🗋 🥒 🖉 🔍 Add Filter	Export 3 items found 10 ∨ per page K < 1 of 1 > >
	Licensing	Name : Vendor : Version : File Lo	cation C Description C Last Update C 🖗
	-	rubrik-OS1 Ubuntu Ubuntu Server 18.04.4 LTS https://	10.108.1.8/rubrik_os_8 Dec 4, 2023 5:20 PM
		rubrik_os_8.1.3-p5-25046 Ubuntu Ubuntu Server 18.04.4 LTS https://	10.108.1.8/rubrik_os_8 Nov 3, 2023 3:16 PM ····
Ne	w Command Palette	Rubrik81 Ubuntu Ubuntu Server 18.04 LTS https://	10.108.1.8/rubrik_os_8 Oct 18, 2023 7:54 PM ····
Navi to H	gate Intersight with Ctrl+K or go elp > Command Palette		e c <u>1</u> of 1 2 9

Step 4. Select organization, add the location of the Rubrik CDM ISO (NFS/CIFS or HTTPS server) and click Next.

=	tisco Intersight	🖥 System 🗸	Q Search	0	¢] 😢	٥	0	R
@ •	Settings	Software Repository	,					
	Targets Software Repository Tech Support Bundles Audit Logs Sessions Licensing	 General 2 Details 	General Specify the Operating System source to be used during the installation process. Organization * Ru Org NFS CIFS HTTP/S File Location * https://10.108.1.8/rubrik_os_8.1.3-p6-25150_iv_3.5.0-138.ii @					
Nav to I	ex Command Palette × vigate Intersight with Ctri+K or go Help > Command Palette		Username o Password o o					

Step 5. Enter a name for the Repository, for the Vendor enter Ubuntu, and for the Version enter Ubuntu 18.04 Click Add.

≡ "dhah: Intersight System ~			Q Search	⊗ ⊄	2 () @	A ا
Softv	ware Repository						
Targets C Get Software Repository 2 Det Tech Support Bundles Audit Logs	neral Det Raview	tails w Operating System image details, modify as required, and save the Op Name * Rubrik 813 ©	erating System image.				
Sessions		Vendor * Ubuntu ~	Version * Ubuntu Server 18.04 LTS		J		
New Command Palette × Navigata Intercipt with Ctrl+K or go to Help > Command Palette		Set Tags	Description			đ	
	< Cance	el			ľ	ack A	dd

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

≡	uludu Intersight	System ∨	Q Search	A © C • P ©
0	Settings	Software Repository		
U	Admin ^	Firmura Links OC Image Links SCILLinks OS Configuration Filos		
	Targets	So Links OS coniguration Files		
	Software Repository			Add OS Image Link
	Tech Support Bundles			
	Audit Logs	* All OS Image Links		
	Sessions	📋 🖉 🔗 🗛 Add Filter	Export 4 items found	10 ∨ per page K < 1 of 1 > >
	Licensing	Name C Vendor C Version C File Location	C Description	≎ Last Update ≎ 🖇
	-	Rubrik 813 Ubuntu Ubuntu Server 18.04 LTS https://10.108.1.8/rub	rik_os_8	a few seconds ago

Step 7. From Cisco Intersight, click Infrastructure Service, then click Servers, and select the Cisco UCS C-Series nodes ready for the Rubrik CDM OS installation. Click the ... and select Install Operating System. Click the ... and select Install Operating System.

≡	ntersight 🔐	Infrastructure Service 🗸				Q Search	⊙ ⊈ 2	Q 0 A
(Ø)	Overview	Servers						
10	Operate ^ Servers	* All Servers (a) +				C Export 4 items found	d 10 ~ perpage 📧 💽	1 of 1 🖂 🖂
	Chassis Fabric Interconnects	Power > System >	Power	HCL Status	Models	Contract Status	Profile Status	Rec 👯
	HyperFlex Clusters	Profile > Install Operating System	Cont		4 • C240 M6L 4		4 • OK 4	No1 ÷
O,	Analyze ^	Upgrade Firmware Start Alarm Suppression	Health	- Model - Ç	P 🛈 💈 Memo 🤤	UCS D : Serve : F.	A. : Serial	: Mana 🖗
	Explorer New	Stop Alarm Suppression 4-1	O Hes	ithy UCSC-C24	128.0 384.0	AA09-FI-D Ru-SP @ 4.2(3	f) No WZP26510561	10,108
,o	Configure ^	Set License Tier	O Hea	ithy UCSC-C24	128.0 384.0	AA09-FI-D Ru-SP @ 4.2(3	f) No WZP2651059D	10.108
	Profiles	 O AA09-FI-DP-6454-3 O AA09-FI-DP-6454-4 	© Hes	itthy UCSC-C24	128.0 384.0 128.0 384.0	AA09-FI-D Ru-SP ⊗ 4.2(3 AA09-FI-D Ru-SP ⊗ 4.2(3	e No WZP2651056H !f) No WZP2651055Z	10.108
	Templates							

Step 8. In the General tab, ensure the nodes are selected. Click Next.

≡	alialia Intersight 🍂	Infrastructure Service 🗸	Q. Search 🕑 📢	2 Q 0
.¢.	Overview	Install Operating Sys	em	
	Operate ^ Servers Chassis	Ceneral Operating System G Configuration	General Select the servers for the Operating System installation Select Servers	
	HyperFlex Clusters	Server Configuration Utility SInstallation Target	Q ₆ Add Filter G Export 4 items found <u>10</u> ∨ per page (F. C. <u>1</u> of	1 🗵 🔅
2	Analyze ^ Explorer New	6 Summary	Name : Health : User Label : Model : Serial Ø AA09-FI-DP-6454-1 Ø Healthy UCSC-C240-M6L WZP24 AA09-FI-DP-6454-1 Ø Healthy UCSC-C240-M6L WZP24 AA09-FI-DP-6454-2 Mealthy UCSC-C240-M6L WZP24	Number : 5510561
	Configure ^		WARDS FILDP-6454-3 Weathy UCSC-C240-M6L WZP24 AA09-FILDP-6454-3 O Healthy UCSC-C240-M6L WZP24 AA09-FILDP-6454-4 O Healthy UCSC-C240-M6L WZP24	551056H 651055Z
	Templates		Selected 4 of 4 Show Selected Unselect All	1_of1 > >
	Pools			
Nev aviç He	Command Palette × gate Intersight with Ctrl+K or go alp > Command Palette	<	Cancel	Back

Step 9. Select the Operating System repository which was previously created for Rubrik CDM ISO and click Next.

=	diada Intersight	$\sigma^{\rm lag}$ Infrastructure Service $ \lor $		Q Search	ତ ୟ 🔹	0 Q	۶
:@:	Overview	Install Operating Sys	tem				
0	Operate /	General	Operating System Select an Operating System from the list or add a new image to the repository.				
	Fabric Interconnects HyperFlex Clusters Integrated Systems	Configuration Server Configuration Utility Installation Target	Select Operating System Image Add OS Image Link				
O.	Analyze Explorer New	6 Summary	Selected servers belong to multiple common organizations: 'd' from one of the common organizations. Learn more at Heip Ce	efault', 'Ru-Org'. You can choose to inst enter.	all Operating System	'n	
,0	Profiles	×	Q. Add Filter 4 it Name 2 File Location 2 Vendor	tems found 10 ∨ per page 🗷 3	☐ 1 of 1 ≥ ≫ Description	© :	
	Templates Policies		Rubrik81 https://10.108.18/rubrik_ Ubuntu rubrik_os_8.1.3-p5-, https://10.108.1.8/rubrik_ Ubuntu	Ubuntu Server 18.04 Ubuntu Server 18.04			
	Pools		rubrik-OS1 https://10.108.1.8/rubrik, Ubuntu e Rubrik 813 https://10.108.1.8/rubrik, Ubuntu	Ubuntu Server 18.04 Ubuntu Server 18.04			
Nev Navi to He	Command Palette × gate Intersight with Ctrl+K or go elp > Command Palette	K	Selected 1 of 4 Show Selected Unselect All		K < 1_ of 1	Back N	ext

Step 10. From Configuration, click Embedded and click Next (the OS configuration file is already part of Rubrik CDM ISO). Click Next

≡ المعانية: المtersight المعانية: المعانية:	Infrastructure Service 🗸	Q Search Ø	¢1® Q ® }
) Overview	Install Operating Sys	stem	
Operate Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Ceneral Coperating System Configuration Configuration Server Configuration Utility S Installation Target	Configuration Select a configuration source and provide the necessary configuration parameters Select Configuration Source Cisco Custom Embedded Operating System Image must include a configuration file. For an example of the configuration file, see Help Center.	
Analyze Analyze New	6 Summary		
Configure ^ Profiles Templates Policies Pools New Command Palette ×			
Navigate Intersight with Ctrl+K or go to Help > Command Palette	<	Cancel	Back Next

Step 11. Click Next on the Server Configuration Utility (SCU) tab.

=	the Intersight	📌 Infrastructure Service 🗸	Q Search 🛛 🖓 💿 🖓 🚺 Q 🚳 🗛 🖓	2
:@:	Overview	OPERATE > Servers	tem	
0	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Virtualization Kubernets	Ceneral Operating System Configuration Server Configuration Utility Installation Target	Server Configuration Utility Select a Software Configuration Utility from the list or add a new image to the repository select Server Coefiguration Utility Optional Add SCU Link	
,o	Integrated Systems	6 Summary	Server Configuration Utility images are filtered based on the Operating System image selection. Learn more at Help Center.	
	Profiles Templates		Installing an Operating System is supported only if the Server Configuration Utility image is at version 6.1.3(x) and later.	
	Policies Pools		Q, Add Filter 1 Items found 10 v par page E 1 of 1 2 0 Name : File Location : Version : Supported Mod : Description : NO ITEMS AVAILABLE	
		<	Cancel Back Ne	a)

Step 12. Click Next from the Installation target. Rubrik CDM ISO automatically identifies the Installation target as the RAID1 virtual drive created across 2x M.2 internal drives configured in the Boot Order Server Policy.

Step 13. Verify the summary and click Install.

Writer Sight Intrastructure Service Install Operating System Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Integrated Systems Integrated Systems Integrated Systems Integrated Systems Summary Configuration Target Summary	_
Install Operating System Operate Servers Chassis Fabric Interconnects HyperFiex Clusters Integrated Systems Integrated Systems Surver New	=
Operate Chasis Chasis Chiguration Fabric Interconnects Configuration HyperFlex Clusters Configuration Utility Integrated Systems Configuration Utility Integrated Systems Installation Target Configuration Configuration Surce Explorer New	:(¢);
	0
Configure A Profiles Selected Servers Templates AA09-FI-DP-6454-1 Serial: WZP2651059D Policies AA09-FI-DP-6454-2 Serial: WZP2651059D Pools View D New Command Palette × AA09-FI-DP-6454-4 Serial: WZP2651055Z Newsylate Intersight with Ctri-K or go View D In bieley Command Palette Kerkel	S Nev Nav

Step 14. Accept the warning for overwriting the existing OS image on the node and click Install.

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

Step 15. The OS installation for Rubrik on Cisco UCS C-Series nodes require few confirmations. Therefore, you need to open a vKVM window for each of the nodes wherein Rubrik OS is getting installed. The node will reboot for OS installation and the ISO would be automatically mounted.



Step 16. Confirm the Rubrik CDM version.

Ready to install 8.1.3–p6–25150:
Platform: c240m6 Serial: RC240WZP2649Z182
Installer: 18.04.5~3.5.0–138
Would you like to proceed?
< Yes > <abort></abort>

Rubrik Installer will verify the hardware compatibility.

Platform:C240mb Serial:RC240w2P26492182 Software:8.1.3-p2-24912	Installer:18.04.5 3.5.0-130
Bios and BMC configuration (system may reboot)	[In Progress]
Hardware Validation	[Not Started]
Prepare for Install	[Not Started]
Install Kubrik Uperating System Prepare for Stage 2 and Reboot	[Not Started]
	[Not otdited]
Clean up install	[Not Started]
Finish Installation	[Not Started]
Prepare for normal startup	[Not Started]
Ruppell Produces	

Step 17. When the verification completes, confirm the errors detected. Ignore the NIC count, CPU and SSD model check errors.

Following error(s) detected. Would you like to proceed?
TPM version check
< Yes > < No >

Next, the stage 2 of installation proceeds.



Step 18. When the OS is installed, login to each node (admin/rubrik) and verify the hardware health. Execute 'cluster hw_health' on each node to confirm on any hardware issue and the node is healthy.

	ports					
Port I	Device	Driver I	State I	Link	I	Speed
bond0 l			աթ I	yes	I	50000Mb/s
bond1 l			down I	no	I	Unknown !
eth0	Cisco VIC NIC (rev a2)	enic l	down I	no	I	Unknown !
eth1	Cisco VIC NIC (rev a2)	enic l	down I	no	I	Unknown!
rketh0	Intel 10G X550T	ixgbe l	down I	no	I	Unknown !
rketh1	Intel 10G X550T	ixgbe l	down I	no	I	Unknown!
rketh2	Cisco VIC NIC (rev a2)	enic l	սթ I	yes	I	50000Mb/s
rketh3	Cisco VIC NIC (rev a2)	enic l	up l	yes	I	50000Mb/s
Bond1 Mode is fault- Bond1 bond ports Current active p WARNING: Bond1 has n	tolerance (active-backup) are: rketh0 rketh1 port is None no active ports and is not	operational.				
Checking for MCEs /var/log/mcelog is c	lean					

Note: Ensure the bond0 is created across rketh2 and rketh3 and the network port status is up.

Install OS through Virtual Media

Procedure 1. Install Rubrik CDM OS through Virtual Media

This procedure details the process to install the Rubrik CDM 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: If you are installing the OS through virtual media and it times out, please use a different browser such as Mozilla Firefox.

Step 1. Login to virtual KVM, click Virtual Media and click vKVM-Mapped DVD.

≡	cisco Intersight	AA09-FI-DP-6454-1 (Ru-SP-Templa
5	Console	
] (1	File >	
0	View	
	Macros	
*	Tools	
Ċ	Power	
\uparrow	Boot Device >	[8335.786224] blk_updat
	Virtual Media	Create Image
, Ę	Chat	vKVM-Mapped vDVD

Step 2. Select the Rubrik CDM ISO from your local file system and click Map Drive.

Browse	Selected File rubrik_os_8.1.3-p6-25150
DIOTISC	
Read Only	

Step 3. Click Boot Device and then select Any Virtual Media as a one time boot device. This ensures the next boot of the node attaches to the ISO mounted on the Virtual Media.

≡	cisco Intersight	AA09-FI-DP-6454-1 (Ru-SP-Templa
5	Console >	
1	File >	
0	View >	
6 6	Macros >	
×	Tools >	
\bigcirc	Power >	
\uparrow	Boot Device >	None
	Virtual Media >	LAN
Ð	Chat	Any Virtual Media

Step 4. Click Power and then click Reset System to reset the power cycle on the node. The Rubrik CDM ISO automatically loads.

Ready to install 8.1.3-p6-25150:	
Platform: c240m6 Serial: RC240WZP2649Z182	
Installer: 18.04.5~3.5.0–138	
Would you like to proceed?	
< Yes >	<abort></abort>

Step 5. The entire installation takes about an hour. When all the nodes are installed with Rubrik ISO, you can proceed to configure the Rubrik cluster.

Rubrik Installer will verify the hardware compatibility.

AA09-FI-DP-6454-1 (Ru-SP-Template-1_DERIVED-1) KVM Console	UCSC-C240-M6L WZP26510561	
Rubrik Installer (Stag		
Platform	:c240m6_Secial:RC240WZP26497182_Software:8_1_3-p2-24912_Installer:18_04	5"3 5 0-130 1
Rice and	DWC configuration (custom mou paboat)	[To Prograss]
Hardware	Validation	[Not Started]
Prepare Install	for Install Rubrik Operating System	[Not Started] [Not Started]
Prepare	for Stage 2 and Reboot	[Not Started]
Clean up	install	[Not Started]
Prepare	nstallation for normal startup	[Not Started]
Uvera	0%]

Step 6. When the verification completes, confirm the errors detected. Ignore the NIC count, CPU and SSD model check errors.



Next, the stage 1 of installation will proceed. It may take about 70-80 minutes for completion of stage 1.

≡	cisco Intersight	AA09-FI-DP-6454-1 (Ru-SP-Template-1_DERIVED-1) KVM Console UCSC-C240-M6L WZP26510561 🕮 1	
Ŀ	Console >		
1	File >	Rubrik Installer (Stage 1 of 2)	
θ	View >		
8	Macros >		
×	Tools >		
0	Power >		
\uparrow	Boot Device >	Platform:c240m6 Serial:RC240WZP26492182 Software:8.1.3-p6-25150 Installer:18.04.5~3.5.0-138]
Q	Virtual Media >	Bios and BMC configuration (system may reboot) [Succeed Hardware Validation [Succeed Prepare for Install [Succeed Install Rubrik Operating System [In Progr Prepare for Stage 2 and Reboot [Not Star	ed] ed] ed] ess] ted]
		Clean up install [Not Star Finish Installation [Not Star Prepare for normal startup [Not Star	ted] ted] ted]
		Overall Progress 20%	

Step 7. When Stage 1 is complete, the installer will reboot the system and proceed to Stage 2.



Step 8. When Stage2 is complete and installation succeeds, the node would be ready for normal setup and cluster configuration.

ik Installer (Stage 2 of 2)	
Platform:c240m6 Serial:RC240WZP2649Z157 Software:8.1.3-p6-25150	Installer:18.04.5~3.5.0-138
Bios and BMC configuration (system may reboot)	[Succeeded
Hardware Validation	[Succeeded
Prepare for Install	[Succeeded
Install Rubrik Operating System	[Succeeded
Prepare for Stage 2 and Reboot	[Succeeded
Clean up install	[In Progress
Finish Installation	[Not Started
Prepare for normal startup	[Not Started
·····	
Overall Progress	
65%	



Step 9. Login to each node (admin/rubrik) and verify the hardware health. Execute 'cluster hw_health' on each node to confirm on any hardware issue and the node is healthy.

Checking networking ports... Port Device Driver | State | Link | Speed I up I yes I 50000Mb/s bond0 I bond1 | down I no l Unknown ! Cisco VIC NIC (rev a2) Cisco VIC NIC (rev a2) Unknown! eth0 | down I enic I no l eth1 | I enic I down I no Unknown? Intel 10G X550T Unknown! rketh0 | no I ixgbe l down I no I Unknown! rketh1 | Intel 10G X550T ixgbe | down I Cisco VIC NIC (rev a2) up I yes I 50000Mb/s rkethZ enic I Cisco VIC NIC (rev a2) | rketh3 | enic I սթ I yes | 50000Mb/s Bond0 Mode is fault-tolerance (active-backup) Bond0 bond ports are: rketh2 rketh3 Current active port is rketh3 Bond1 Mode is fault-tolerance (active-backup) Bond1 bond ports are: rketh0 rketh1 Current active port is None WARNING: Bond1 has no active ports and is not operational. Checking for MCEs... /var/log/mcelog is clean FRU Replacement Summary: All FRUS in the node are healthy. RC240WZP2649Z15W >> RC240WZP2649Z15W >> RC240WZP2649215W >> RC240WZP2649Z15W >>

Note: Ensure the bond0 is created across rketh2 and rketh3 and the network port status is up.

Step 10. Repeat this procedure for all Cisco C-Series nodes to be configured for the Rubrik CDM cluster.

Configure Rubrik CDM Cluster

This section elaborates on the configuration of the Rubrik CDM Cluster on Cisco UCS C-Series nodes. The existing deployment is deployed with four (4) Cisco UCS C240 M6 LFF servers.

Note: Make sure the Rubrik CDM ISO is installed on each Cisco C-Series nodes.

Note: The network bonding mode on the Rubrik operating systems with Cisco UCS C-Series servers connected to Cisco UCS Fabric Interconnect, 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)

Note: The following section is for reference; make sure to involve Rubrik support during cluster configuration.

The Rubrik CDM cluster configuration is a three-step process:

- Verify node network status and change node to UCS Managed (UCSM) mode
- Bootstrap cluster
- Register Cluster

Verify node network status and change node to UCS Managed (UCSM) mode.

Procedure 1. Verify network active status

In this procedure, administrators should verify the network status of each Cisco UCS C-Series server to be configured as part of Rubrik CDM cluster

Step 1. Ensure Rubrik CDM OS is installed on each node. Login to each node (admin/rubrik) and execute cluster hw_health to verify the node health and network status. The following screenshot displays the output of cluster hw_health. The active network is Bond0 with ports as rketh2 and rketh3 with active-backup fault tolerance mode. These network ports are mapped to vNIC2/vNIC3 created in the LAN Connectivity Policy for Server Profile of Cisco UCS C-Series server. This was created in the <u>Create Server Profile</u> template section.

Checking for PCI No PCIe errors fo	e errors ound.					
Checking network	ing ports					
Port I	Device	l Driver	I State	l Lir	ık I	Speed
bond0 l		I	I up	l ye	s	50000Mb/s
bond1 I		1	l down	l r	no I	Unknown!
eth0 I	Cisco VIC NIC (rev a2)	l enic	l down	l r	no I	Unknown!
eth1 I	Cisco VIC NIC (rev a2)	l enic	l down	l r	no I	Unknown!
rketh0	Intel 10G X550T	l ixgbe	l down	l r	no I	Unknown!
rketh1	Intel 106 X550T	ixgbe	l down	l r	no l	Unknown!
rketh2	Cisco VIC NIC (rev a2)	l enic	I up	l ye	s	50000Mb/s
rketh3	Cisco VIC NIC (rev a2)	l enic	I սր	l ye	s	50000Mb/s
Bond0 hode is fat Bond1 Mode is fat Bond1 Mode is fat Bond1 bond po Current activ WARNING: Bond1 ha	orts are: rketh3 rketh2 we port is rketh3 ult-tolerance (active-backup) orts are: rketh0 rketh1 we port is None as no active ports and is not	operational				
Checking for MCEs /var/log/mcelog	s is clean					
FRU Replacement S All FRUS in the RC240WZP26492182	Summary: e node are healthy. >>					

Procedure 2. Convert to UCS Managed node

Step 1. Convert each node in UCS Managed mode. Execute cluster change_cisco_UCS_mode. The following screenshot displays the output. This should be executed across each node which would be configured in Rubrik CDM cluster. This is required for all Cisco UCS C-Series servers configured as Rubrik CDM nodes and connected to Cisco UCS Fabric Interconnect in Intersight Managed Mode (IMM).

RC240U2P2649215U logint admin
Helesse to Bubyik Clint
Type neip or ! to fist commanas
Type commands list to list all available commands
It is recommended to use the Rubrik CDM web UI for cluster setup, Please use this URL "https://fe80::225:b5ff:fe55:55c1]" to an
cess the UI from inside the same submet. Alternatively, use the "cluster setupmetwork" command on the CLI to assign a routable
Put address to any of the nodes and then access the UI via IPut
RC240WZP2649215W >> cluster change_cisco_UCS_mode
Node is set to managed mode.
RC240WZP2649215W >>

Bootstrap Rubrik Cluster

Note: The following section is for reference. Customers and administrators should contact Rubrik support to bootstrap and register Rubrik Cluster.

Note: This section explains the bootstrap process using the CLI method. To bootstrap Rubrik cluster through the UI, please refer to Setting up a Rubrik cluster using the UI in the <u>Rubrik CDM Install and</u> <u>Upgrade Guide</u>.

This section details the cluster bootstrap process. All IP address details should be pre-populated as provided in <u>Table 3 Rubrik Cluster IP Addressing</u>. It is recommended to involve Rubrik support during this process.

Procedure 1. Bootstrap cluster

Step 1. Login to any Rubrik node (admin/rubrik).

Step 2. Execute 'cluster bootstrap' Once the general inputs such as cluster name, DNS, NTP are entered, all the nodes pre-installed with Rubrik CDM OS will be discovered.

The following screenshots display the user inputs, marked in RED. All user inputs are detailed <u>Table 3 Rubrik</u> <u>Cluster IP Addressing</u>.

RC240W2P2649215T >> cluster bootstrap Waiting for Rubrik API to become available
Select your role from the following options: 1 Customer 2 Support 3 Rubrik Professional Service 4 Partner 5 Sales Engineer
User configuration
Input your role: 1 E-mail: Password: Re-enter Password: Re-entered password does not match Password: Re-enter Password:
Cluster configuration
Cluster name: ru-chx-02
DNS Nameservers [8.8.8.8]: 10.108.1.6,172.20.4.53 DNS Search Domains (Optional - press [Enter] to continue): NTP Servers [pool.ntp.org]: 172.20.10.18,172.20.10.15
Management Gateway: 10.108.1.254 Management Subnet Mask: 255.255.255.0 Management VLAN (Optional - press [Enter] to continue):
IPMI Gateway: 0.0.0.0 IPMI Subnet Mask: 0.0.0.0
Data Subnet Mask (Optional - press [Enter] to continue):
Enable Software Encryption (y/n) (Optional - press [Enter] to continue) [y]:
Node configuration ====================================
Node configuration
======================================
Discovered nodes: 1: RC240WZP26492157 2: RC240WZP2649215T 3: RC240WZP2649215W 4: RC240WZP26492182 Tupe a node index or name to configure. Tupe θ to find more nodes or hit Enter to begin bootstrap
Select node: (Optional - press [Enter] to continue): _

1: RC240WZP26492157* 2: RC240WZP2649215T 3: RC240WZP2649215W
4: RC240WZP26492182 Type a node index or name to configure. Type 0 to find more nodes or hit Enter to begin bootstrap Select node: (Optional - press [Enter] to continue): 2 Configuring node RC240WZP2649215T Management IP [10.108.1.164]: IPMI IP [0.0.0.2]:
Discovered nodes: 1: RC240WZP26492157* 2: RC240WZP2649215T* 3: RC240WZP2649215W 4: RC240WZP26492182 Type a node index or name to configure. Type 0 to find more nodes or hit Enter to begin bootstrap Select node: (Optional - press [Enter] to continue): 33 Invalid index
Discovered nodes: 1: RC240WZP26492157* 2: RC240WZP2649215T* 3: RC240WZP2649215W 4: RC240WZP26492182
Type a node index or name to configure. Type 0 to find more nodes or hit Enter to begin bootstrap Select node: (Optional - press [Enter] to continue): 3 Configuring node RC240W2P2649215W Management IP [10.108.1.165]: IPMI IP [0.0.0.3]:
Discovered nodes: 1: RC240WZP26492157* 2: RC240WZP2649215T* 3: RC240WZP2649215W* 4: RC240WZP26492182
Type a node index or name to configure. Type 0 to find more nodes or hit Enter to begin bootstrap Select node: (Optional - press [Enter] to continue): 4 Configuring node RC240W2P26492182 Management IP [10.108.1.166]: IPMI IP [0.0.0.4]:
Discovered nodes: 1: RC240WZP26492157* 2: RC240WZP2649215T* 3: RC240WZP2649215W* 4: RC240WZP26492182* Tume 0 to find more nodes on hit Enter to begin bootstran
Select node: (Optional - press [Enter] to continue): _


Step 3. When the bootstrap is successful, proceed to registering the cluster to Rubrik Security Cloud (RSC) instance.

Procedure 2. Rubrik Cluster Registration

Note: Ensure you have a Rubrik Security Cloud Instance created for your Rubrik account.

Step 1. Open a browser and login to Rubrik node with the Node OS IP address configured during the bootstrap process.

← → C ONot secure https://10	0.108.1.163/web/onboarding/					
RackTables 🕜 DMZ vCenter						
		R		— \$ —		⊘
		Discover Nodes	Configure	Bootstrap	Register Cluster	Initiate Access
Be	ootstrap Comple	te!				
Pla	asso login with password	you created earlier to f	inich the registration			
Fit	ase login with password	you created earlier to r	insir the registration.			
Use	ername					
Bat	reuord					
		assword				
	LOG IN					

Step 2. Enter the Rubrik Security Cloud URL (RSC) and sign in to Rubrik.

	Disc	over Nodes	Configure	🥸 Bootstrap	Register Cluster	Initiate Access	
R	egister your cluster w	rith Rubrik				Node Count: 3 Platform Type: third	party
Cc wi m Le	omplete the registration process Il connect your cluster to your Re anaging clusters with your purch earn More @	to enable multi-c ubrik account, fro aased manageme	cluster managemen om where you could nt plan.	ıt. Rubrik İ start			
Yo re	our company's Rubrik domain ad gistration.l don't have a domain	dress and Log in or credentials @	credentials are nee	ded for			
In	put your Rubrik domain URL:	ciscocvd.my.rut	brik.com	SIGN	IN TO RUBRIK		
u u	nable to access RSC from this loc	ation? Register h					
A	dvanced Settings 🗸						
St W	ill having issues with connection e will help instruct you to open S	? You can contact upport Tunnel	t Rubrik Customer S	Support.			

Step 3. Enter your Rubrik Security Cloud instance login and password.



Step 4. Select the SaaS instance service type and confirm the cluster details for registration, click Next.

Online Cluster Registration **Choose Service Type** Your account has multiple orders of different service types. Rubrik Security Cloud (SaaS) CDM (Software) Latest order Enable centralized data management through Manage your clusters locally. Rubrik Security Rubrik Security Cloud's single interface only. Cloud may already be available to you. You can register a Rubrik cluster using this limited-time option, which allows you manage your cluster in dual management mode (CDM and RSC). Confirm the cluster that will be granted registration permission: Cluster Name: ru-cluster-03 Cluster ID: 2bbcfa26-f3e2-4a2b-9ced-17d2e317f9e4 Cluster Address: 10.108.1.163 NEXT

Step 5. Cluster registration may take few minutes, confirm the successful cluster registration to Rubrik Security Cloud instance.





Cluster Expansion and Firmware Upgrades

This chapter contains the following:

- Rubrik Cluster Expansion
- Upgrade Cisco UCS C-Series Node Firmware

Note: Rubrik support should be involved for both Cluster Expansion and Cisco C-Series Firmware Upgrades.

Rubrik Cluster Expansion

Cluster Expansion is a two-step process:

- 1. Derive, Deploy Server Profile, and Install Rubrik CDM operating system.
- 2. Add node through Rubrik management console.

Derive-Deploy Server Profile

Procedure 1. Derive and Deploy Server Profile to new node

Step 1. Go to <u>https://intersight.com/</u>, click Infrastructure Service and click Server.

Step 2. Verify the Cisco UCS Fabric Interconnect port assigned for the new C-Series node is enabled and has the role as Server. This can be confirmed by viewing the 'port policy' assigned to Domain Profile

≡	cisco Intersight	📲 Infrastructure Service 🗸	Q Search		⊘ ⊄1 ② ↓ ⑦ A
	Overview	Starting on January 25, 2024, any notifications will be high, if your inf	arget disconnected for more than 5 minutes will generate an alarm. This new feature means that initial rastructure has many disconnected targets. As usual, acknowledge alarms to dismiss them.		×
0	Operate /	← UCS Domain Profiles Ru-DomainProfile-	AA09		Actions
	Fabric Interconnects	Details	Policies	⊒	Port Details
	HyperFlex Clusters Integrated Systems	Status © OK	Port Configuration VLAN & VSAN Configuration UCS Domain Configuration	- Î	General Name
œ,	Analyze	Name Ru-DomainProfile-AA09	^ Fabric Interconnect A Configured		Ru-PortPolicy Organization
	Explorer New	Fabric Interconnect A	General		Ru-Org
ب (Configure /	Fabric Interconnect B AA09-FI-DP-6454	Port Ru-PortPolicy 🗑		Policy Details Collapse All Device Model UCS-FI-6454
	Policies	Last Update Jul 7, 2023 2:54 PM	Port 1/21		 Ports Port 1/1 (Unconfigured)
	Pools	Organizations Ru-Org	ADDETUTED AND ADDETUTED A EXTERNA ADDETUTED ADDETUT		Role Unconfigured Type

Step 3. Ensure additional Cisco UCS C-Series nodes for Rubrik Cluster is cabled to the Sever Port on Cisco UCS Fabric Interconnect. The following screenshot displays the cabling to Cisco UCS Fabric Interconnect.

≡	elterin Intersight	Infrastructure Service V	Q Search	0 4 2 Q	୭
(0)	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minutes will gen notifications will be high, if your infrastructure has many disconnected targets. As usual	arate an alarm. This new feature means that initial acknowledge alarms to dismiss them.		×
0	Operate Servers Chassis Fabric Interconnects	Ceneral Inventory UCS Server Profile HCL Statistics Topology			Actions 🗸
	HyperFlex Clusters	AA09-FI-DP-6454-4	Lat	t Refresh Time a few seconds ago	Refresh
©.	Analyze Analyz				1 + 1 C Q 0
Nevi Navi to H	Command Palette Sequence of the seque		aasargaalaa 🕢		

Step 4. Ensure there is an available IP in 'IP Pool Policy' assigned to Server Profile Template. This is required for CIMC access to the new Cisco UCS C-Series node.

	cisco Intersight	🗚 Infrastructure Service 🗸	Q search 🕑 🕫 2 🗘 💿 🔉
:@:	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minutes will generate an alarm. This new feature notifications will be high, if your infrastructure has many disconnected targets. As usual, acknowledge alarms to dismiss	means that initial × them.
0	Operate ^ Servers	Pools	
	Chassis	Pools Reserved Identifiers VRFs	
	Fabric Interconnects		
	HyperFlex Clusters		Create Pool
	Integrated Systems	* All Pools @ +	
	integrated bystems		
O,	Analyze ^		G Export 5 items found 10 ∨ per page K 1 of 1 >
Q	Analyze ^ Explorer New	IP x MAC x UUID x WWNN x	G Export 5 items found 10 ∨ per page 1 1 2 WWPN T IQN X
୍	Analyze ^ Explorer New Configure ^	Add Filter Add Filter MAC = UUID = WWNN = Output to the state of t	G Export 5 items found 10 ∨ per page K < 1 of 1 > 1 WWPN = IGN = × >
© ,•	Analyze ^ Explorer New Configure ^ Profiles	$\begin{array}{c c c c c c c c c c c c c c c c c c c $	G Export 5 items found 10 ∨ per page ≤ 1 of 1 > 0 WWPN = IQN = XX NOLS NO IQN POOLS XX
୍	Analyze ^ Explorer New Configure ^ Profiles Templates	IP Q, Add Filter IP IP ID Used 8 ID Used 8 ID Used 22 ID Available 26 ID ID ID ID ID Used 8 ID Used 8 ID ID ID ID	€ Export 5 items found 10 ∨ per page € 1 of 1 > N WWPN 〒 IQN 〒 ↓ NOLS NO WWPN POOLS NO IQN POOLS ×
୍	Analyze ^ Explorer New Configure ^ Profiles Templates Policies	IP IP <td< th=""><th>€ Export 5 items found 10 → per page € 1 of 1 > N WWPN ▼ IQN ▼ X NO WWPN POOLS IQN POOLS X Reserved Description : Last Update Ø</th></td<>	€ Export 5 items found 10 → per page € 1 of 1 > N WWPN ▼ IQN ▼ X NO WWPN POOLS IQN POOLS X Reserved Description : Last Update Ø
©.	Analyze ^ Explorer New Configure ^ Profiles Templates Policies	IP = IP = III = IIII = IIIII = IIIII = IIIII = IIIII = IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	C Export 5 items found 10 ∨ per page € < 1 of 1 > 1 WWPN ₹ IQN ₹ NO WWPN POOLS NO IQN POOLS Reserved Description : Last Update \$ 0 a few seconds a

Step 5. Identify the new Cisco UCS C-Series server node, click the ellipses "... ", select Profile and Derive Profile from the template.

≡	dialle Intersight	🖫 Infrastructure Service 🗸	Q Search	ତ ସ ହ ୦ ୦ ୦୦
(@);	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minutes will generate an alarm. This new feature notifications will be high, if your infrastructure has many disconnected targets. As usual, acknowledge alarms to dismise	r means that initial s them.	×
0	Operate A	Servers		
	Chassis Fabric Interconnects		G Export 4 items found 10 ∨	Power >
	HyperFlex Clusters	Health Power HCL Status Models	Derive from Template Contract Status Profile	Profile Profile Install Operating System
۵,	Analyze	(4) • Healthy 4 (6) Off 1 (6) Incomplete 4 (4) • C240 M6L 4	Not Covered 4	Upgrade Firmware Launch vKVM
,c	Configure	Name : Health : Model : CP () : Memo : UCS D	. : Serve : F : A. :	Launch Tunneled vKVM Start Alarm Suppression
	Profiles	C AA09-FI-DP-6454-1 @ Healthy UCSC-C24 128.0 384.0 AA09-FI	I-D Ru-SP 😔 4.2(2f) No	Open TAC Case
	Templates	(¹) (¹) AA09-FI-DP-6454-2 (② Healthy) UCSC-C24 128.0 384.0 AA09-FI	I-D Ru-SP @ 4.2(2f) No	Set License Tier
	Policies	C AA09-FI-DP-6454-3 C Healthy UCSC-C24 128.0 384.0 AA09-FI	I-D Ru-SP @ 4.2(3e) No	Collect Tech Support Bundle
	Pools	G AA09-FI-DP-6454-4 @ Healthy UCSC-C24 128.0 384.0 AA09-FI	I-D 4.2(2f) No	WZP2651055Z

Step 6. The Cisco UCS C-Series node is displayed, click Next.

≡	tisco Intersight	° Infrastructure Service V	Q Search	D	2 🗘	0	R
(Ø)	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minutes will generate an alarm. This new fe notifications will be high, if your infrastructure has many disconnected targets. As usual, acknowledge alarms to disconnected targets.	eature means that initial ismiss them.				×
0	Operate ^ Servers	Templates					
	Chassis Fabric Interconnects HyperFlex Clusters	General General Please confirm the Server selection Confirm Server 1					
Q	Integrated Systems Analyze ^	3 Details Selection selected 4 Summary Add Filter C II Image: Selection Selected Name Image: User Label	Export 1 items found 10 v per pag lealth : Model : UC3	ge ℝ < _1_o S Domain	f 1 > 🗵 Serial Nu	0	
,e	Explorer New Configure ^ Profiles	AA09-FI-DP-6454-4	Healthy UCSC-C240 AAC	09-FI-DP-6 K <	WZP265105	5Z	
	Templates						
	Pools						
Ne	w Command Palette ×						
to H	Help > Command Palette	Cancel				Nex	ct 🛛

Step 7. Select the Server Profile template created to deploy the Cisco UCS C-Series node for the Rubrik CDM cluster and click Next.

≡	المانية، Intersight	🚓 Infrastructure Service 🗸			Q se	arch	Ø	₽] 2	Ф @) A
.@:	Overview	 Starting on January 25, 2024, any tai notifications will be high, if your infra 	jet disconnected for more than 5 tructure has many disconnected t	ninutes will generate an alarr argets. As usual, acknowledg	n. This new feature means th e alarms to dismiss them.	at initial				×
0	Operate A	Templates								
	Chassis Fabric Interconnects	General	Template Select the Template that nee	t to be assigned to profile.						
	HyperFlex Clusters	3 Details	UCS Server	rofile Template Filter	2 items found	10 v per page 📧 <	1 of 1 🗵))		
O,	Analyze Replorer New	4 Summary	Nam	e : I	Description	Last Upd	late 2023 3:38 F	PM		
.0	Configure /		Ru-S	P-Template-1		Oct 18, 2	023 7:38 P	M		
	Templates		Selected 1	r 2 Show Selected	Unselect All		C C _	ori D D		
	Policies									
New Navig to He	Command Palette × gate Intersight with Ctrl+K or go tip > Command Palette	¢	Close						Back	Next

Step 8. Rename the Derive profile and click Next.

≡	altado Intersight 🌲	Infrastructure Service 🗸		Q Search	0	#1 🔹 🗘	0	<u> </u>
:@:	Overview	 Starting on January 25, 2024, any targ notifications will be high, if your infrast 	jet disconnected for more than 5 minutes will generate an alarm. This ne tructure has many disconnected targets. As usual, acknowledge alarms	aw feature means that initial to dismiss them.				×
0	Operate ^ Servers	Templates						
	Chassis Fabric Interconnects HyperFlex Clusters	General Template	Details Edit the description, tags, and auto-generated names of the profile A General	15.				Î
Ø	Integrated Systems	3 Details	Organization * Ru-Org	Target Platform V UCS Server (FI-Attached)			~ 0	
6	Explorer New	0	Description	Cot Togo				
	Profiles		Jeschpaon	& <= 1024				
	Policies		∧ Derive					
	Pools		1 Name * Ru SP-Template 1_DERIVED-1	Organization * Ru-Org	~	Assigned Serv AA09-FI-DP-0 4	ver 3454-	
Nev Nav to H	w Command Palette × igste Intersight with Ctrl+K or go elp > Command Palette	<	Close			Baci	K Ne:	×t

Step 9. Verify the policies and click Derive.

≡	۰۱۱۰۰۱۱۰۰ Intersight	📌 nfrastructure Service $ \lor $			Q Search	⊘ ⊈⊇	Q ()	<u>ା</u>
.(¢).	Overview	 Starting on January 25, 2024, any ta notifications will be high, if your infra 	rget disconnected for more than 5 minu structure has many disconnected targe	tes will generate an alarm. This new featur ts. As usual, acknowledge alarms to dismis	e means that initial is them.			×
0	Operate Servers	Templates						
	Chassis Fabric Interconnects HyperFlex Clusters	General	General Template Name Ru SD-Template 1	a to be derived norm the prome template.	Organization			
©,	Integrated Systems	 Details Summary 	Target Platform UCS Server (FI-Attached)		nu-org			
ې	Explorer New Configure	^	UCS Server Profiles	Assimud Server	Organization			
	Profiles		Ru-SP-Template-1_DERIVED	1 AA09-FI-DP-6454-4	Ru-Org			
	Templates Policies		Compute M Configuration C	anagement Storage onfiguration Configu	Network ration Configuration	Errors/W (0)	arnings	
	Pools		BIOS				Ru-BIOS	
			Boot Order			Ru-	BootOrder	
Ne	w Command Palette		L					L .
Navi to H	igate Intersight with Ctrl+K or ge lelp > Command Palette	<	Close			l	Back	erive

Step 10. When the Sever Profile is derived, go to the Servers tab, identify the Profile displayed as "Not Deployed," click the ellipses"..." and select Deploy.

≡	🔐 🔐 Intersight	nfrastructure Service $$	Q Search	. ⊘ 🧣	ជា 🔹 🕻	0	8
(Ø)	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minu notifications will be high, if your infrastructure has many disconnected target	utes will generate an alarm. This new feature means that initial tts. As usual, acknowledge alarms to dismiss them.				×
(0)	Operate ^ Servers	Profiles					
	Chassis	HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Prof	files UCS Server Profiles				
	HyperFlex Clusters				Deploy		
	Integrated Systems	* All UCS Server Prof + Add Filter	C Export 5 items found	10 v per pag	Activate Unassign	Server	
O,	Analyze ^				Clone		
	Explorer New	Status Inconsistency Reason	Target Platform		Edit		
,c	Configure ^	OK 3 Not Assigned 1	FI-Attached 5		Delete		
ſ	Profiles	No data available			Set User	Label	
C	Templates				Detach fr	om Templat	e
	remplates	Name Status	Target Platform CUCS Server Template Server	Last U	Server Ad	tions	>
	Policies	Ru-SP-Template-1_DERIVED-5	UCS Server (FI-Attached) Ru-SP-Template-1 AA09-FI-DP-6454-4	a few s	seconds ago	, <u> </u>	

Step 11. On the Deploy Profile confirmation screen, enable Reboot Immediately to Activate and click Deploy.

Deploy UCS Server Profile

UCS Server profile "Ru-SP-Template-1_DERIVED-4" will be deployed to server "AA09-FI-DP-6454-4".

If policy configuration requires an immediate reboot and the option below is disabled, then	
profile deployment will not be initiated.	

Reboot Immediately to Activate ③		
	Cancel	Dep

Step 12. Monitor the Sever Profile Deployment task and ensure profile is deployed successfully.

	Execution Flow	
tus	Progress	13%
In Progress	Usit For BIOS POST Completion	
ne	⊘ Power On Server	Jan 19, 2024 12:56 PM
loy Server Profile	⊘ Validate user access to the storage policies	Jan 19, 2024 12:56 PM
	 Validate user access to the network policies 	Jan 19, 2024 12:56 PM
ab7cc696f6e3301db2e4e	⊘ Validate user access to the compute and management policies	Jan 19, 2024 12:56 PM
get Type	⊘ Validate user access to the profile	Jan 19, 2024 12:56 PM
a server	Prepare Server Profile Deploy	Jan 19, 2024 12:56 PM
get Name 0 9-FI-DP-6454-4		
исе Туре		
ver Profile		
irce Name		
SP-Template-1_DERIVE	_	
ator		
niman@cisco.com		

Step 13. When the profile is successfully deployed, install the OS using Cisco Intersight 'OS installation' feature or by mounting the Rubrik ISO to KVM console .Once Rubrik OS is installed, verify the node with cluster hw_health.

loy

Checking networking	ports								
Port I	- Device	I	Driver	I	State	I	Link	I	Speed
bond0 l		I		I	սթ	I	yes	I	50000Mb/s
bond1 l		I		I	down	I	ົາວ	I	Unknown !
eth0	Cisco VIC NIC (rev a2)	I	enic	I	down	I	no	I	Unknown!
eth1	Cisco VIC NIC (rev a2)	I	enic	I	down	I	no	I	Unknown?
rketh0	Intel 10G X550T	I	ixgbe	I	down	I	no	I	Unknown !
rketh1	Intel 10G X550T	I	ixgbe	I	down	I	no	I	Unknown !
rketh2	Cisco VIC NIC (rev a2)	I	enic	I	սք	I	yes	I	50000 M b/s
rketh3 I	Cisco VIC NIC (rev a2)	I	enic	I	սք	I	yes	I	50000 M b/s
Bond1 Mode is fault- Bond1 bond ports Current active p WARNING: Bond1 has r	ort is rketh3 -tolerance (active-backup) s are: rketh0 rketh1 port is None no active ports and is not	; oj	perational						
Checking for MCEs /var/log/mcelog is c	lean								
FRU Replacement Summ All FRUS in the no RC240WZP2649Z15W >> RC240WZP2649Z15W >> RC240WZP2649Z15W >> RC240WZP2649Z15W >>	nary: ode are healthy.								

Procedure 2. Add Node through Rubrik Management Console

When the Rubrik CDM operating system is installed and the cluster hw_health is 'healthy, contact Rubrik support to add the new node to existing cluster.

Note: The Add Node process demonstrates an expansion from three node cluster to four node cluster. Rubrik recommends having a minimum of four node in the cluster. Rubrik support should be involved for both Cluster Expansion and Cisco UCS C-Series Firmware Upgrades.

Note: Ensure the new node has Rubrik OS installed as detailed in the previous section.

Step 1. Ensure the existing cluster is an healthy state.

Data Protection	DASHBOARD V CLUS	TERS INVENTORY V SLA DOMAINS EVI	INTS V REPORTS LIVE MOUNTS	Q L © III
ers > ru-cluster-03				
-cluster-03 🏾 💩 Sync up to dat	e 🔵 👩 RSC Managed			··· VISIT CLUSTER
DVERVIEW 🔆 NODES 🚳 NETWO				
Performance and Tasks Pa	ist 24 hours 🔻		Events Past 24 hours 👻	
Performance		L.	0	O autora
				Replication failed
\land		не 4% сеџ	0	0
	\smile \sim	747.53 kB Data Received	O out of 0 Backup failed	Archiving failed
		736.03 kB Data Transmitted		
Tasks			Hardware Health	
			Power Supply Status	Network Status
		-O- Q Falled		
		0 Completed	OIMM Status	 Disk Status
		O Canceled	Chassis Status	Node Status

Step 2. Go to the Node tab. It displays a three node cluster. Click Add Node.

lusters > ru-cluster-0	a → All Nodes 03 @ Sym	: up to date 🕜 RSC-Managed		Pinned All Data Center					··· VISIT CL	USTER (
ime Range		Network DetAils (2) CLUST	Management IP	Brik ID	CPU Utilization	Data Received	ADD		earch by node, host, or ap	pliance
Past 1 hour		* RC240WZP26492157		WZP2651056H				Read: 13 Write: 115	Read: 277 kB/s Write: 41 MB/s	
 Past 7 days Past 30 days 		* RC240WZP2649Z15W	10.108.1.164	WZP2651059D		164 kB/s	234 kB/s	Read: 13 Write: 116	Read: 272 kB/s Write: 37 MB/s	
iata		* RC240WZP2649Z182		WZP26510561				Read: 13 Write: 173	Read: 278 kB/s Write: 50 MB/s	

Step 3. Existing cluster automatically identifies the new node. Enter available Node IP address. In present configuration Cisco UCS C-Series nodes are attached to Cisco Fabric Interconnect and do not utilize IPMI configuration. Therefore, the IPMI IPs are configured as 0.0.0.x. Click Next.

IPMI	
	1 node
	IPMI 0004

Step 4. Enter the subnet mask and Gateway. In present configuration Cisco UCS C-Series nodes are attached to Cisco Fabric Interconnect and do not utilize IPMI configuration. Therefore, the IPMI Gateway and subnet are 0.0.0.0. The node is registered to the cluster.

Add Node	<>──2	×
Check or edit the follo	wing fields to add nodes to this cluster.	
Default Gateway		
Gateway IP	10.108.1.254	
Gateway Network	💿 Management Network 🔵 Data Network 🔵 VLAN	J
Management Netw	ork	
Subnet Mask	255.255.255.0	
Management VLAN (Optional)	Type the Management VLAN	
ІРМІ		
Subnet Mask	0.0.0.0	
IPMI Gateway	0.0.0.0	
New IPMI Password	d	
	1 node selected	BACK ADD

Step 5. It takes about 10-15 minutes for the new node to be visible in the cluster. The screenshot below confirms the addition of new node to the existing cluster:

ru-cluster-0 ລາຍສາຍສາຍ	3 Syn	c up to date 💦 🕐 RSC Managed	FR DETAILS						··· VISIT CLL	ISTER [
me Range	_	Nade Neme A	Management IP	Brik ID	CPU Utilization	Data Received	ADD N Deta Sent		earch by node, host, or ap	pliance
Past 1 hour		* RC240WZP2649Z15T		WZP2651055Z				Read: Write:	Read: Write:	
) Past 7 days Past 30 days								Read: 13 Write: 104	Read: 277 kB/s Write: 24 MB/s	
ta		* RC240WZP2649215W		WZP2651059D				Read: 13 Write: 86	Read: 273 kB/s Write: 27 MB/s	

Upgrade Cisco UCS C-Series Node Firmware

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 upgrade of Cisco UCS C-Series nodes connected to Cisco UCS Fabric Interconnect is a two-step process. Administrators should upgrade the Cisco UCS Fabric Interconnect Firmware, thereafter, upgrade the Cisco UCS C-Series node firmware.

Note: Firmware upgrade of Cisco UCS Fabric Interconnect is non-disruptive, but firmware upgrade of Cisco UCS C-Series node is disruptive, administrators should have a maintenance window in which the Rubrik cluster is shutdown. Please contact Rubrik support to provision a maintenance window.

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 Firmware

This procedure details the high-level procedure to upgrade firmware of the Cisco UCS Fabric Interconnect in Intersight Managed Mode (IMM). For more details, go to: https://intersight.com/help/saas/resources/Upgrading Fabric Interconnect Firmware imm#before you begin

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

≡	ntersight	Infrastructure Service 🗸			Q Search	Ø	¢] 💈	Q 🚥 🛆	0	<u>8</u>
.¢.	Overview	Starting on January 25, 202 notifications will be high, if y	4, any target disconnected for rour infrastructure has many	r more than 5 minutes will generate a disconnected targets. As usual, ackn	in alarm. This new feature means owledge alarms to dismiss them.	that initial				×
0	Operate ^ Servers	Fabric Intercon	nects							
C	Chassis Fabric Interconnects	* All Fabric Interconn ©	ŧ		G Exp	port 2 items found 1	0 v per p	age 🗵 🔍 1 d	#1 🗵 🕅	
0	HyperFlex Clusters Integrated Systems	Health	Connection	Contract Status	Bundle Version	NX-OS Version	ul 2	Models	31	
,c	Explorer New Configure	Name	: Health	- Model -	Bundle Version	UCS Domain Profile	Total	Ports		
	Profiles Templates	AA09-FI-DP-6454 FI-A	C Healthy	UCS-FI-6454 UCS-FI-6454	4.2(3d) 4.2(3d)	Ru-DomainProfile-AA09 Ru-DomainProfile-AA09	54 54	18 36 um On Locator		
	Policies	Selected 2 of 2 Show	Selected Unselect All				Ű	pen TAC Case pgrade Firmware		
							R	eplace UCS Domai ollect Tech Suppor	1 t Bundle	

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

	distle Intersight	📽 Infrastructure Service 🗸		Q se	earch	⊘ ধ্বা ⊗	Q 🐽 🛛	0	1 8
(i)	Overview	Starting on January 25, 2024, any targ notifications will be high, if your infras	et disconnected for more than 5 minutes will ructure has many disconnected targets. As	ll generate an alarm. This new featu usual, acknowledge alarms to dismi	are means that initial iss them.				×
0	Operate ^ Servers Chassis	 ← Fabric Interconnects Upgrade Firmware 							
	Fabric Interconnects HyperFlex Clusters Integrated Systems	General Version	General Ensure selected Fabric Interconnects on Confirm Fabric Interconnects Selection	eet requirements for firmware upgr I Selected	ada.				
Q	Analyze ^ Explorer New	3 Summary	Infrastructure firmware upgrad	e can be performed only on a pair o	of Fabric Interconnects at once 1 items found 10	v per page 📧	R 1 of 1 5	DE C	9
,e	Configure ^ Profiles Templates		O Add Filter Image: Comparing Name Million Image: Comparing Name Million Image: Comparing Name Million Image: Comparing Name Million Image: Comparing Name Million	Fabric Interconnec odel Serial 25-FI-6454 FD0260419XX	t A Bundle Version Model 4.2(3d) UCS-FI-64	Fabric Inte Serial	rconnect B Bund 419ZA 4.2(3/	e Version	1
	Policies Pools		Selected 1 of 1 Show Selected	Unselect All			1	of 1	
Net Navi to He	Command Palette * gate Intersight with Ctrl+K or go etp > Command Palette	c.	Cancel				в	ack I	Next

Step 3. Select the recommended Firmware release (currently 4.2(3h)). By default, the upgrade enables the Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude the Fabric Interconnect traffic evacuation.

=	disclo Intersight	🖋 Infrastructure Service 🗸	Q search 🥝 🕫 2 🗘 🧕	ە 🔊
þ:	Overview	Starting on January 25, 2024, any t notifications will be high, if your info	arget disconnected for more than 5 minutes will generate an alarm. This new feature means that initial astructure has many disconnected targets. As usual, acknowledge alarms to dismiss them.	
	Operate /	 ← Fabric Interconnects Upgrade Firmware 		
	Fabric Interconnects HyperFlex Clusters	General	Version Select a firmware version to upgrade the Fabric Interconnects to.	
	Integrated Systems	Version	Select Firmware Bundle Advanced	Mode O
		2 Summary		
	Analyze	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.	evacuation.
	Analyze Explorer Naw Configure	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page II C 1 of 3 II	evacuation.
	Analyze / Kew Explorer New Configure / Profiles	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page II C 1 of 3 2 Version : Size : Release Date : Description	evacuation.
	Analyze / Kaw Explorer New Configure / Profiles Templates	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page II c 1 of 3 2 Version : Size : Release Date : Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Clicco Intersight Infrastructure Bundle	evacuation.
	Analyze	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page II of 3 v Version z Size z Release Date z Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Clisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Clisco Intersight Infrastructure Bundle	evacuation. D C C C C C C C C C C C C C
	Analyze A Explorer New Configure A Profiles Templates	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page III of 3 v Version z Size z Release Date z Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Clisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Clisco Intersight Infrastructure Bundle 4.2(3h) 1.70 GiB Sep 30, 2023 1:51 Clisco Intersight Infrastructure Bundle	evacuation.
	Analyze A Explorer New Configure A Profiles Polícies Pools	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page IIII of 3 v Version Size t Release Date Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Gisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Cisco Intersight Infrastructure Bundle 4.2(3h) 1.70 GiB Sep 30, 2023 1:51 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB Jul 31, 2023 2:01 PM Cisco Intersight Infrastructure Bundle	evacuation.
	Analyze A Explorer New Configure A Profiles Polícies Polícies	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page I C 1 of 3 v Version Size t Release Date Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Gisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB Jug 10, 2023 2:01 PM Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB Jug 30, 2023 1:51 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB Jug 31, 2023 2:01 PM Cisco Intersight Infrastructure Bundle 4.2(3e) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle	evacuation.
	Analyze A Explorer New Configure A Profiles Policies Policies	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page 1 of 3 Version Size Release Date Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Gisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Gisco Intersight Infrastructure Bundle 4.2(3h) 1.70 GiB Sep 30, 2023 1:51 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3g) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle	evacuation.
	Analyze Analyz	3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic Use Advanced Mode to exclude Fabric Interconnect traffic evacuation. Add Filter 28 items found 10 v per page 1 of 3 v Version Size Release Date Description 4.3(2.230129) 1.70 GiB Nov 15, 2023 2:52 Gisco Intersight Infrastructure Bundle 4.3(2.230117) 1.70 GiB Aug 16, 2023 2:55 Gisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB Sep 30, 2023 1:51 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16, 2023 2:57 Cisco Intersight Infrastructure Bundle 4.2(3p) 1.70 GiB May 16,	evacuation.

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

≡	diada Intersight	Infrastructure Service 🗸		Q Search	Ø	\$	Q 03 (A)	0	R
(Ø.	Overview	Starting on January 25, 2024, any target notifications will be high, if your infrastruct	Sisconnected for more than 5 minutes ture has many disconnected targets. J	will generate an alarm. This new feature means that initial As usual, acknowledge alarms to dismiss them.					×
0	Operate Servers Chassis	 ← Fabric Interconnects Upgrade Firmware 							
Ø	Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze	General Version Summary	Summary Confirm configuration and initiate the Selected firmware bundle w firmware upgrade.	e upgrade. ill be downloaded to the Fabric Interconnects and upgraded. Click or	n Reques	ts to monite	or the progress of t	he	
,e	Explorer New Configure ^ Profiles Templates		Firmware Version 4.2(3h) © Fabric Interconnects to be Upgraded	Size 1.70 GIB					
Ne	Policies Pools w Command Palette		Q Add Filter Domain N : Model AAG9-FI-DP-6 UCS-FI-6454	C: Export 1 items found 13 Fabric Interconnect A Serial Bundle Version Model FD0260419XX 4.2(3d) ④ UCS-FI-6454	 per p Fabric Seria FDO: 	age 💽 🔄 Interconnel 260419ZA	1 of 1 2 1 ect B Bundle Version 4.2(3d)	on ©)
Navi to H	igste intersight with Ctri+K or go ielp > Command Palette	¢	Cancel				Back	Upgra	de

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.

Upgrade Firmware			
Details	Execution Flow		
itatus	Progress	26%	6
Action Required	 Wait for a user acknowledgement on Fabric Interconnect - B. 		
√ame Jpgrade Firmware	Ensure Fabric Interconnects meet requirements to continue upgrade. Please acknowledge to con B upgrade. Learn more at Help Center.	ntinue with Fabric Interconnect -	
D 35aac302696f6e3301dbb6a2	Proceed		
Farget Type Fabric Interconnect	Wait for MAC address synchronization on Fabric Interconnect - B. MAC address synchronization is complete.	Jan 19, 2024 1:57 PM	4
arget Name	© Evacuate data traffic on Fabric Interconnect - B.	Jan 19, 2024 1:52 PM	A,
A09-FI-DP-6454 FI-B	Wait for image download to complete in endpoint. Image ucs-intersight-infra-4gfi.4.2.3h.bin successfully cached in Fabric Interconnect(s).	Jan 19, 2024 1:52 PM	A
iource Type irmware Upgrade	Initiate image download to the endpoint. Download ucs-intersight-infra-4gfi.4.2.3h.bin request is submitted successfully.	Jan 19, 2024 1:44 PM	A
ource Name A09-FI-DP-6454 FI-A,AA	 Validate the requirements for the endpoint. Validation of pre-upgrade space availability completed successfully. 	Jan 19, 2024 1:44 PM	A
vitiator			



← Requests Upgrade Firmware		
Details	Execution Flow	
Status Action Required	Progress O Wait for a user acknowledgement on Fabric Interconnect - A.	58%
ame pgrade Firmware	Firmware upgrade for Fabric Interconnect - B is complete. Ensure Fabric Interconnects meet require Please acknowledge to continue with Fabric Interconnect - A upgrade. Learn more at Help Center.	ements to continue upgrade.
5aac302696f6e3301dbb6a2	Proceed	
rget Type bric Interconnect	Wait for image download to complete. Image ucs-intersight-infra-4gfi.4.2.3h.bin successfully cached in Fabric Interconnect(s).	
rget Name A09-FI-DP-6454 FI-A A09-FI-DP-6454 FI-B	Initiate image download to endpoint. Image ucs-intersight-infra-4gfi.4.2.3h.bin already available in a cache, skipping the download. Image will be endpoints.	Jan 19, 2024 2:11 PM synced to the selected
urce Type mware Upgrade	Oheck if the image has been cached. Verified that image is available in the cache.	Jan 19, 2024 2:11 PM
urce Name (09-FI-DP-6454 FI-A,AA	 Wait for firmware upgrade in Fabric Interconnect - B. Successfully upgraded Fabric Interconnect. 	Jan 19, 2024 2:11 PM
liator dhiman@cisco.com	Initiate firmware upgrade in Fabric Interconnect - B. Firmware upgrade request submitted successfully.	Jan 19, 2024 1:58 PM
art Time	⊘ Wait for a user acknowledgement on Fabric Interconnect - B.	
in 19, 2024 1:44 PM	 Wait for MAC address synchronization on Fabric Interconnect - B. MAC address synchronization is complete. 	Jan 19, 2024 1:57 PM

Step 8. Make sure the Firmware upgrade completed successfully.

Overview			ß
Operate ^	Details F:	Execution Flow	
Servers Chassis	Status Success	Wait for firmware upgrade in Fabric Interconnect - A. Successfully upgraded Fabric Interconnect.	l9, 2024 2:31 PM
Fabric Interconnects HyperFlex Clusters	Name Upgrade Firmware	Initiate firmware upgrade in Fabric Interconnect - A. Jan Firmware upgrade request submitted successfully.	19, 2024 2:18 PM
Integrated Systems	ID 65aac302696f6e3301dbb6a2	Wait for MAC address synchronization on Fabric Interconnect - A. MAC address synchronization is complete.	19, 2024 2:18 PM
Analyze ^	Target Type	Several data traffic on Fabric Interconnect - A. Jan	19, 2024 2:13 PM
Explorer New	Fabric Interconnect	Wait for a user acknowledgement on Fabric Interconnect - A.	
Configure ^	Target Name AA09-FI-DP-6454 FI-A AA09-FI-DP-6455 FI-B	 Wait for image download to complete. Jan Image ucs-intersight-infra-4gfi.4.2.3h.bin successfully cached in Fabric Interconnect(s). 	19, 2024 2:11 PM
Tempiates	Source Type Firmware Upgrade	Initiate image download to endpoint. Image ucs-intersight-infra-4gfi.4.2.3h.bin already available in a cache, skipping the download. Image will be synced to the s endpoints.	19, 2024 2:11 PM elected
Pools	Source Name AA09-FI-DP-6454 FI-A,AA	Check if the image has been cached. Jan Verified that image is available in the cache.	19, 2024 2:11 PM
Command Delete	Initiator andhiman@cisco.com	Wait for firmware upgrade in Fabric Interconnect - B. Successfully upgraded Fabric Interconnect.	19, 2024 2:11 PM
igate intersight with Ctrl+K or go elp > Command Palette	Start Time Jan 19, 2024 1:44 PM	Initiate firmware upgrade in Fabric Interconnect - B. Jan Firmware upgrade request submitted successfully.	i9, 2024 1:58 PM
		- O Wait for a user acknowledgement on Fabric Interconnect - B.	

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

≡	ៅក្រៅក Intersight ្រំ៖	Infrastructure Service V	Q Search	⊘ ⊈ ≥	ር ር ଦ୍ ଦ୍ ଦ୍ ଦ୍ ନ୍ ନ୍ ନ୍			
:@:	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minute notifications will be high, if your infrastructure has many disconnected targets	will generate an alarm. This new feature means that initial As usual, acknowledge alarms to dismiss them.		×			
0	Operate ^ Servers	-abric Interconnects						
	Chassis	★ All Fabric Interconn ⊕ +						
	Fabric Interconnects	I Q. Add Filter	Export 2 items found	d 9 v perr	bage 데이지 이 1 이 기			
	HyperFlex Clusters							
	Integrated Systems	Health Connection Contract	Status Bundle Version NX-OS Vers	sion	Models			
Q	Analyze ^	2 • Healthy 2	2 • 4.2(3h) 2 2 • 9:	3(5)142(3f) 2	2 • 6454 2			
	Explorer New							
.0	Configure ^	Name t Health t Model	Bundle Version C UCS Domain Profil	e Total	Used Availa			
	Profiles	AA09-FI-DP-6454 FI-A O Healthy UCS-FI-64:	4 4.2(3h) Ru-DomainProfile-	AA09 54	18 36			
	Templates	AA09-FI-DP-6454 FI-B O Healthy UCS-FI-64	4 4.2(3h) Ru-DomainProfile-	AA09 54	18 36 …			
	Policies	Ç						

Upgrade Cisco UCS C-Series Node Firmware

This section details the procedure to upgrade the firmware of only Cisco UCS C-Series Rubrik certified nodes. The Rubrik CDM software upgrade is not part of this procedure.

Note: Since the Cisco UCS C-Series firmware upgrade requires a reboot, contact Rubrik support to shut down the cluster during the maintenance window.

This section is utilized in two key circumstances.

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

Procedure 1. Upgrade Cisco UCS C-Series Node Firmware

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

	diale Intersight	💱 Infrastructure Service 🗸	Q Search	ଡ ≰120 ¢	ଡ ନ
XQR.	Overview	Starting on January 25, 2024, any target disconnected for more than 5 minutes will generate an alarm. This new featu notifications will be high, if your infrastructure has many disconnected targets. As usual, acknowledge alarms to dismi	ure means that initial iiss them.		×
	Operate A	Servers			
	Chassis Fabric Interconnects		G Expert Alternational 10		44 N N
	HyperFlex Clusters	Power HCL Status Models	Contract Status Prof	ile Status x	Rec 3X
O,	Analyze	Profile > (C On 4) (O Incomplete 4)	Not Covered 4) • OK 4	¢ ÷
	Explorer New	Install Operating System			
9,	Configure A	Start Alarm Suppression CHealth C Model C CP C C Memo C UCS C	D 🌣 Serve 🔅 F 🗧 A. 🗧	Serial 🗧 N	łana ∮
	Profiles	Stop Alarm Suppression 4-1 @ Healthy UCSC-C24 128.0 384.0 AA09-	-FI-D Ru-SP @ 4.2(2f) No	WZP26510561 1	0.108
	Templates	Set License Tier 4-2 @ Healthy UCSC-C24 128.0 384.0 AA09	-FI-D Ru-SP @ 4.2(2f) No	WZP2651059D 10	D.108 ···
	Policies	AA09-FH-DP-6454-3 O Healthy UCSC-C24 128.0 384.0 AA09 O AA09-FH-DP-6454-4 O Healthy UCSC-C24 128.0 384.0 AA09	-FI-D Ru-SP @ 4.2(3e) No	WZP2651056H 10	0.108
	Pools				

Step 2. Make sure all Cisco UCS C-Series nodes are selected for upgrade. Click Next.

Ξ	cisco Intersight	Infrastructure Service 🗸		Q Search	Ø 412 Q	୭ ୧
÷.	Overview	Starting on January 25, 2024, any target notifications will be high, if your infrastru	disconnected for more than 5 minutes will generate an alarm. This new fee :ture has many disconnected targets. As usual, acknowledge alarms to dis	ature means that initial miss them.		×
0	Operate ^ Servers	+ Servers Upgrade Firmware				
©,	Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze ^	 General Version Summary 	General Ensure selected servers meet requirements for firmware upgrade. Confirm Servers Selection 4 Selected	4 items found 10 ∨ per p	age E C 1 of 1 5 M	Q
o,	Explorer New Configure ^ Profiles Templates Policies		Q Add Filter Image: Second Seco	Firmware Version -C240-M6L 4.2(2f) -C240-M6L 4.2(3e) -C240-M6L 4.2(2f) -C240-M6L 4.2(2f)	UCS Domain AA09-FI-DP-8454 AA09-FI-DP-6454 AA09-FI-DP-6454 AA09-FI-DP-6454 AA09-FI-DP-6454	
Nev Nav to F	Pools Command Palette S gate Intersight with Ctrl+K or go elp > Command Palette	ć	Selected 4 of 4 Show Selected Unselect All		R I of 1 Back	Next

Step 3. Select the recommended Server Firmware version and click Next. At the time of publishing this guide, the suggested firmware was 4.2(3h) If the firmware upgrade does not require drive firmware updates, select Advanced Mode, and check the Exclude Drive option.

≡	cisco Intersight	🚴 Infrastructure Service 🗸				Q Search	0	¢] (2)	٥	0	R
æ	Overview	Starting on January 25, 2024, any targ notifications will be high, if your infras	get disconnected for more than 5 m tructure has many disconnected to	minutes will gene argets. As usual,	rate an alarm. This n acknowledge alarms	ew feature means that initial to dismiss them.					×
0	Operate ^ Servers Chassis	 Servers Upgrade Firmware 									
Q.	Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze	 Qeneral Version Summary 	Version Select a firmware version to u Select Firmware Bundle The selected firmwar storage controllers. L	upgrade the serv re bundle will be Use Advanced M	ers to. downloaded from ini lode to exclude upgra	iersight.com. All the server comp de of drives and storage control	enents will be upgräded ald	Advanced	^{1 Mode} C		
,c	Explorer New Configure		Q Add Filter	Size : R	elease Date	18 items found	10 👻 për page 🗟 🔄	1 of 2 [10	(i) ș	
	Promes		4.3(2.230270)	804.67 MiB N	ov 15, 2023 2:12	Cisco Intersight Server Bundle			3	90	
	Templates		4.3(2.230207)	797.52 MiB	ug 16, 2023 2:11	Cisco Intersight Server Bundle				0	
	Policies		O 4.2(3l)	854.30 MIB N	ov 7, 2023 1:26 PM	Cisco Intersight Server Bundle	_			db	
	Pools		(a) 4.2(3h)	854.30 MiB S	ep 30, 2023 2:19	Cisco Intersight Server Bundle	J			•	
			O 4.2(3g)	828.34 MiB Ji	ul 31, 2023 2:36 PM	Cisco Intersight Server Bundle				C22	
Ner	Command Palette		() 4.2(3e)	828.18 MiB M	lay 16, 2023 2:41	Cisco Intersight Server Bundle				00	
Navie to He	gate Intersight with Ctri+K or go #p > Command Palette	<	Càncel	823.63 MiB M	lar 22, 2023 12:2	Cisco Intersight Server Bundle			Back	Next	j

Step 4. Click Upgrade.

≡	📲 🔐 🕹	infrastructure Service 🗸		Q Search	Ø 4 [®] C Ø A
۲	Overview	Starting on January 25, 2024, any targe notifications will be high, if your infrastr	t disconnected for more than 5 minutes will generate an alarm. Thi icture has many disconnected targets. As usual, acknowledge alar	is new feature means that initial rms to dismiss them.	×
0	Operate ^ Servers Chassis	 Servers Upgrade Firmware 			
Q	Fabric Interconnects HyperFlex Clusters Integrated Systems Analyze	 General Version Summary 	Summary Confirm configuration and initiate the upgrade. Firmware Version 4.2(3h) @	Size 854.30 MiB	
,c	Configure ^ Profiles Templates		Servers to be Upgraded Q. Add Filter Name : User Label : Model	G Export 4 items found 13 Firmware Versi : F	3 ∽ perpage III 1 of 1 III ©. Requires Reboot © UCS Domain
	Policies Pools		AA09-FI-DP-6454-2 UCSC-C240 AA09-FI-DP-6454-3 UCSC-C240 AA09-FI-DP-6454-1 UCSC-C240	0-M6L 4.2(21) (§) Y 0-M6L 4.2(3e) (§) Y 0-M6L 4.2(21) (§) Y	AA09-FI-DP-6454 Yes AA09-FI-DP-6454 Yes AA09-FI-DP-6454
Ner Naoś to He	Command Palette	K	AA09-FI-DP-6454-4 UCSC-C240	0-M8L 4.2(2f) 🛞 Y	Res AA09-FI-DP-6454

Step 5. Select the Reboot Immediately to Begin Upgrade option. This initiates the firmware upgrade across all Cisco UCS C-Series Rubrik certified nodes.

≡	ہ Intersight ،	° Infrastructure Service $$		Q Search	Ø	\$12 Q	?	ጸ
:@:	Overview	Starting on January 25, 2024, any targe notifications will be high, if your infraste	t disconnected for more than 5 minutes will generate an alarm. This new ucture has many disconnected targets. As usual, acknowledge alarms to	r feature means that initial dismiss them.				×
(0)	Operate ^	← Servers						
	Servers	Upgrade Firmware						
	Chassis Fabric Interconnects HyperFlex Clusters	General	Summary					Ì
	Integrated Systems	Version	Upgrade Firmware					
Q	Analyze ^	3 Summary	Firmware will be installed on next boot. To reboot immediately, please enable the option below.	Size 854.30 MiB				
	Explorer New		Reboot Immediately to Begin Upgrade					
,c	Configure ^		Cancel Upgrade					
	Profiles		Q, Add Filter	Export 4 items found	13 🗸 per page 🖂 <	1_of1 ≥ >	$\langle \hat{j} \rangle$	
	Templates		Name C User Label C Model	C Firmware Versi C	Requires Reboot ①	UCS Domain		
	Policies		AA09-FI-DP-6454-2 UCSC-C240-M6I	4.2(21)	Yes	AA09-FI-DP-6454	4	
	Pools		AA09-FI-DP-6454-3 UCSC-C240-M6I	4.2(3e) 🛞	Yes	AA09-FI-DP-6454	4	
			AA09-FI-DP-6454-1 UCSC-C240-M6I	4.2(2f) 🛞	Yes	AA09-FI-DP-645	4	
			AA09-FI-DP-6454-4 UCSC-C240-M6I	4.2(2f) 💮	Yes	AA09-FI-DP-645	4	
Ne	w Command Palette ×							÷
to H	igate Intersight with Ctrl+K or go elp > Command Palette	<	Cancel			Back	Upgrad	•

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

← Requests Upgrade Firmware		×
Details	Execution Flow	
Status > In Progress	Progress Vait for image download to complete in endpoint. 0% completed.	13%
Name Upgrade Firmware	 Initiate image download to endpoint. Download intersight-ucs-server-c240-m6.4.2.3h.bin request is submitted successfully. 	Jan 19, 2024 5:45 PM
ID 65aafb74696f6e3301dee8cb	⊘ Validate the requirements for the endpoint.	Jan 19, 2024 5:45 PM
Target Type Rack Server		
Target Name AA09-FI-DP-6454-4		
Source Type Firmware Upgrade		
Source Name AA09-FI-DP-6454-4		
Initiator andhiman@cisco.com		
Start Time Jan 19, 2024 5:45 PM		
End Time		

Step 6. Confirm the firmware upgrade across all Cisco UCS C-Series nodes is complete.

≡	ologia cisco Intersight 🍰 Infrast	structure Service 🗸		Q Search	Ø 4 0 9
)ĝi	Overview	 Starting on January 25, 2024, any target disc notifications will be high, if your infrastructure 	onnected for more than 5 minutes will generate an alarm. 1 shas many disconnected targets. As usual, acknowledge a	his new feature means the Last Login The Last Login IP Last Login IP	ine : Jan 19, 2024 2:37 PM : 192.133.242.70
0	Operate ^				
	Servers	ervers			
	Chassis				
	Fabric Interconnects	* All Servers © +		Export 4 items found	10 v perpage K < 1 of 1 > 河
	HyperFlex Clusters				
	Integrated Systems	Health Power	HCL Status Models	Contract Status	Profile Status 🗉 🛛 F 💥
Q	Analyze ^	(1) On 4	(1) Incomplete 4	Not Covered 4	▲ • OK 4
	Explorer New				\sim
,0	Configure ^	Name	Health : Model : CP () : Memo	: UCS D : Serve : Fi :	A.: Serial : P 🖗
	Profiles	AA09-FI-DP-6454-1 40-	G Healthy UCSC-C24 128.0 3	84.0 AA09-FI-D Ru-SP @ 4.2(3h)	No WZP26510561 1 ···
	Templates	AA09-FI-DP-6454-2 40	C Healthy UCSC-C24 128.0 3	84.0 AA09-FI-D Ru-SP- @ 4.2(3h)	No WZP2851059D 1 ···
	Policies	AA09-FI-DP-6454-3 40	O Healthy UCSC-C24 128.0 3	84.0 AA09-FI-D Ru-SP @ 4.2(3h)	No WZP2651056H 1 ···
	Policies	AA09-FI-DP-6454-4 -05	© Healthy UCSC-C24 128.0 3	84.0 AA09-FI-D Ru-SP @ 4.2(3h)	No WZP2651055Z 1 …

Step 7. Once the firmware across all Cisco UCS C240 LFF nodes are upgraded, restart the Rubrik CDM Cluster.

Rubrik Certified Cisco UCS Nodes

This solution utilizes 4x Cisco UCS C240 M6 LFF nodes configured with Rubrik CDM. Along with this configuration, Cisco and Rubrik have certified solutions with different capacity points available on Cisco UCS C-Series Rack Servers .This allows you to select your configuration based on key characteristics such as:

- Total Capacity
- Cluster Resiliency
- Performance requirements.

Note: Customers should contact Rubrik Sizing Team or Rubrik Sales Specialist for identification of Rubrik Cluster configuration.

Table 12 lists the Rubrik-certified nodes on Cisco UCS Platform.

Solution Name	Cisco UCS Platform	Capacity per Node	Caching SSDs/NVMe per Node
Rubrik-C240M6 LFF	Cisco UCS C240 M6 LFF Rack Server with 12 drive options	48 TB (12x 4TB)	1.6 TB
		96 TB (12x 8TB)	1.6 TB
		144 TB (12x 12TB)	1.6 TB
		168 TB (12x 14TB)	1.6 TB
		192 TB (12x 16TB)	1.6 TB
		240 TB (12x 20TB)	1.6 TB
		264 TB (12x 22TB)	1.6 TB

Table 12. Rubrik Certified Cisco UCS Nodes

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 12 years, Anil has authored several Cisco Validated Designs for enterprise solutions on Cisco data center technologies. Currently, Anil's focus is on Cisco's portfolio of hyperconverged infrastructure and data protection solutions.

Acknowledgements

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

- Urshila Lohani, Product Manager, Cisco Systems Inc.
- Matt Tangvald, Director of Product Management at Rubrik
- Khush Nezam, Product Manager at Rubrik
- Ken Chao, Manufacturing Operations Support Engineer at Rubrik
- Rui Xiao, Staff Hardware Engineer at Rubrik
- Venkat Nitin P., Sr Software Engineer at Rubrik
- Daryl Stanbery, Senior, Director of Alliances at Rubrik

Appendices

This appendix is organized into the following sections:

- Appendix A Bill of Materials
- Appendix B References Used in this Guide

Appendix A - Bill of Materials

<u>Table 13</u> provides an example the Bill of Materials used for four (4) node Rubrik CDM cluster deployed on a single Cisco UCS C-Series systems, along with a pair of Cisco Fabric Interconnects, used in the testing and reference design described in this document.

Table 13. Cisco UCS Bill of Materials

Cisco C-Series estimate (4x C240 M5 LFF nodes) for Rubrik CDM Cluster				
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	
1.2	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	UCSC-M-V25-04	Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM	4	
1.2.2	CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	4	
1.2.3	UCS-M2-240G	240GB SATA M.2	8	
1.2.4	UCS-M2-HWRAID	Cisco Boot optimized M.2 Raid controller	4	
1.2.5	UCSX-TPM-002C	TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, for M6 servers	4	
1.2.6	N20-BKVM	KVM local IO cable for UCS servers console port	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	12	

1.2.9	UCS-DIMM-BLK	UCS DIMM Blanks	80
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-I5318N	Intel 5318N 2.1GHz/150W 24C/36MB DDR4 2667MHz	8
1.2.17	UCS-MR-X32G2RW	32GB RDIMM DRx4 3200 (8Gb)	48
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-NVMEI4-I1600	1.6TB 2.5in U.2 Intel P5600 NVMe High Perf Medium Endurance	4
1.2.21	UCSC-PSU1-1600W	UCS 1600W AC PSU Platinum (Not EU/UK Lot 9 Compliant)	8
1.2.22	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	8
1.2.23	UCS-SID-INFR-OI	Other Infrastructure	4
1.2.24	UCS-SID-WKL-OW	Other Workload	4
1.3	UCSX-FI-6454-U	UCS Fabric Interconnect 6454	2
1.3.0.1	CON-OSP-UCSXUFI6	SNTC-24X7X4OS UCS 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-C14-3M-IN	Power Cord Jumper, C13-C14 Connectors, 3 Meter Length, India	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 this 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 UCS Manager

http://www.cisco.com/en/US/products/ps10281/index.html

Cisco UCS C-Series Rack Servers

https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m6-lff-specsheet.pdf

Rubrik CDM

https://www.rubrik.com/products/cloud-data-management

Feedback

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

CVD Program

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS X-Series, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trade-marks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW_P2)

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

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

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