..|...|.. cisco

White Paper Public

Deploy Cohesity on Standalone Cisco UCS C-Series Rack Servers Managed by Cisco Intersight

Contents

Executive summary
Cisco Intersight platform
Cisco Intersight Virtual Appliance and Private Virtual Appliance
Solution design and deployment
Deployment hardware and software
Licensing requirements
Configuration constructs for Cisco Intersight mode7
Configure Cisco IMC network
Claim Cisco UCS C220 or C240 node in Cisco Intersight platform
Claim device in Cisco Intersight platform9
Configure server policies
Create organization policy12
Create adaptor configuration policy14
Create BIOS profile policy17
Create IPMI-over-LAN policy19
Create serial-over-LAN policy21
Create storage configuration policy23
Create boot-order policy24
Configure and deploy server profile for Cohesity nodes
Install the Cohesity operating system
Install the OS through the Cisco Intersight platform35
Install the OS through vMedia and one-time boot device42
Firmware upgrades
Conclusion
For more information
Products and solutions
Configuration guides

This document presents procedures and best practices for deploying Cohesity DataPlatform on standalone Cisco UCS[®] C-Series Rack Servers managed by the Cisco Intersight[™] platform.

Executive summary

Cohesity software on the Cisco Unified Computing System[™] (Cisco UCS[®]) is an end-to-end data management platform that delivers hyperscale simplicity, multicloud agility, and global visibility. It consolidates data silos across on-premises, cloud, and edge sites and simplifies IT operations. The platform empowers teams to take control of all their enterprise data, build data resilience, and streamline compliance processes and be more productive while achieving business outcomes. Cohesity and Cisco elevate data management strategies with an integrated platform for use cases that unify, protect, and unlock value from enterprise data across the data center core, cloud, and edge.

The Cisco Intersight[™] platform is a management solution delivered as a service with embedded analytics for Cisco[®] and third-party IT infrastructures. Cisco Intersight is a cloud operations platform that consists of optional, modular capabilities for advanced infrastructure, workload optimization, and Kubernetes services. Cisco Intersight infrastructure services include the deployment, monitoring, management, and support of your physical and virtual infrastructure. Cisco Intersight supports Cisco UCS and Cisco HyperFlex hyperconverged infrastructure (HCI) as well as third-party targets connected to the Cisco Intersight platform.

This document helps customers and business partners position and deploy Cohesity DataPlatform on standalone Cisco UCS C-Series Rack Servers through the Cisco Intersight platform. The Cisco Intersight platform works in conjunction with the Cisco Integrated Management Controller (IMC), providing a model-based configuration to provision servers. Using server profiles, IT staff can consistently align policy, server personality, and workloads. These policies can be created once and used to simplify server deployments, resulting in improved productivity and compliance and lower risk of failures due to inconsistent configuration.

The focus of this document is Cisco UCS C-Series standalone servers and the Cisco Intersight platform. Customers interested in understanding use cases, design and deployment details, and best practices for Cohesity on Cisco UCS should refer to the <u>Cisco Cohesity Data Management Solutions</u> page.

Cisco Intersight platform

The Cisco Intersight platform is a software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support services. With the Cisco Intersight platform, customers get all the benefits of SaaS delivery and the full lifecycle management of Cisco Intersight connected distributed servers and third-party storage systems such as NetApp across data centers, remote sites, branch offices, and edge environments (Figure 1).

The Cisco Intersight platform is designed to be modular, so customers can adopt services based on their individual requirements. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers and hypervisors to serverless applications, thereby reducing costs and mitigating risk. This unified SaaS platform uses a unified OpenAPI design that natively integrates with third-party platforms and tools.



Figure 1. Cisco Intersight overview

The main benefits of Cisco Intersight infrastructure services are summarized here:

- Simplify daily operations by automating many daily manual tasks.
- Combine the convenience of a SaaS platform with the capability to connect from anywhere and manage infrastructure through a browser or mobile app.
- Stay ahead of problems and accelerate trouble resolution through advanced support capabilities.
- Gain global visibility of infrastructure health and status along with advanced management and support capabilities.
- Upgrade to add workload optimization and Kubernetes services when needed.

Cisco Intersight Virtual Appliance and Private Virtual Appliance

In addition to the SaaS deployment model running on Intersight.com, on -premises options can be purchased 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 specifically designed for users who operate in disconnected (air gap) environments. The Private Virtual Appliance requires no connection to public networks or to Cisco to operate.

Solution design and deployment

This section discusses the infrastructure setup, software, and hardware requirements, and some of the design and deployment details for provisioning Cohesity DataPlatform on standalone Cisco UCS C-Series Rack Servers managed through the Cisco Intersight platform.

Figure 2 shows the deployment architecture for the solution.



Figure 2.

Cohesity on Cisco UCS server nodes

Deployment hardware and software

Table 1 and Table 2 list the deployment software and hardware requirements for the solution discussed in this document.

	Components	Software version
Computing and storage	Cisco Integrated Management Controller (IMC)	Release 4.1(3b)
Management	Cisco Intersight platform	-
Storage management	Cohesity DataPlatform	Release 6.6.0a

Table 1. Software requirements

Table 2. Deployment hardware

Component	Hardware required
Switches	2 Cisco Nexus® 9336C-FX2 Switches: This switch choice is optional; customers can deploy any network switch compatible with Cisco UCS Virtual Interface Card (VIC) 1457.
Servers	Minimum of 3 Cisco UCS C240 or C220 large-form-factor (LFF) rack servers: These nodes should be configured with hardware components certified by Cohesity.

Licensing requirements

The Cisco Intersight platform uses a subscription-based license with multiple tiers. You can purchase a subscription duration of one, three, or five 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 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 includes storage widgets and cross-domain inventory correlation across computing, storage, and virtual environments (VMware ESXi). It also includes OS installation for supported Cisco UCS platforms.
- Cisco Intersight Premier: In addition to the functions provided in the Advantage tier, Premier includes full subscription entitlement for Cisco UCS Director, providing orchestration across Cisco UCS and third-party systems.

Note: Servers in the deployment discussed in this document require at least the Essentials license. Deployment of the Cohesity operating system through the Cisco Intersight platform require an Advantage license. Customers with at least an Essentials license can deploy the Cohesity operating system on individual server nodes through virtual media (vMedia) using a one-time boot device. For more information about the features provided in the various licensing tiers, see

https://intersight.com/help/getting_started#licensing_requirements.

Configuration constructs for Cisco Intersight mode

At a high level, configuration of Cisco UCS C240 and C220 standalone nodes managed through Cisco Intersight mode consists of the steps shown in Figure 3. The details of these steps are presented in the following sections.



Configure Cisco IMC



Claim server node in Cisco Intersight platform



Configure server policies



Configure server template and profile



profile

Figure 3.

Steps to configure Cisco UCS server nodes using the Cisco Intersight platform

Configure Cisco IMC network

To configure the Cisco IMC network, follow these steps:

- Attach a keyboard and monitor to the USB ports on the rear panel of the Cisco UCS C220 or C240 Rack Server or use a keyboard, video, and mouse (KVM) cable (Cisco part number N20-BKVM) and connector to access the appliance console. Refer to the Cisco UCS C240 M5 Server Installation and Service Guide for details.
- 2. During bootup, press F8 when prompted to open the Cisco IMC Configuration Utility.
- 3. When prompted, enter the default IMC username (admin) and password (password).
- 4. When prompted, change the default IMC (Intelligent Platform Management Interface [IPMI]) username and password. You must enter a strong password.

Note: For all nodes in the Cohesity cluster, set the Cisco IMC (IPMI) user ID and password to the same values.

- 5. Enable the network interface card (NIC) mode Dedicated field by entering a space.
- 6. Enable either the IP (Basic) IPv4 field or the IP (Basic) IPv6 field according to your networking environment.
- 7. Move down to the IP (Basic) DHCP enabled field and enter a space to disable Dynamic Host Configuration Protocol (DHCP).
- 8. Move down to the NIC redundancy None field and enter a space to enable it.
- 9. Enter appropriate values for your network in the following fields:
 - · CIMC IP: Specify the IP address to access the IMC, which is similar to IPMI.
 - Prefix/Subnet: Specify the subnet mask for the IMC (IPMI) subnet.
 - Gateway: Specify the IP address of the subnet gateway for the IMC (IPMI) network interfaces.
 - Pref DNS Server: Specify the IP addresses of the preferred Domain Name System (DNS) server that the Cohesity cluster should use.

all Properties					
NIC mode			NIC redundancy		
Dedicated:	120			DQ	
Shared LOM:	[]		Active-standby:	[]	
Cisco Card:				[]	
	[]		VLAN (Advanced)		
	[]		VLAN enabled:	[]	
	[]		VLAN ID:		
Shared LOM Ext:	[]		Priority:		
IP (Basic)					
IPV4:	DCI	IPV6:	[]		
DHCP enabled	[]				
CIMC IP:					
Prefix/Subnet:					
Gateway:	10.1.0.1				
Pref DNS Server:	10.1.0.1				
Smart Access USB					
	[]				
Enabled	[]				

- 10. Select F10 to save the settings.
- 11. Repeats steps 1 through 10 for all the nodes deployed in the Cohesity DataPlatform cluster.

Claim Cisco UCS C220 or C240 node in Cisco Intersight platform

This section describes the process for claiming Cisco UCS C220 and C240 Rack Server nodes in the Cisco Intersight platform.

Note: This document assumes that customers already have a Cisco Intersight account. If you need to create a new account, refer to <u>Intersight Overview</u>.

Note: For more information about claiming a new device in the Cisco Intersight platform, refer to the videos for <u>starting Cisco Intersight Infrastructure Services</u>.

Note: Prepare device to claim in Cisco Intersight platform

Follow these steps to prepare the device that you want to claim in the Cisco Intersight platform:

- 1. Using a web browser, launch the Cisco IMC. In the browser address bar, enter the IMC (IPMI) IP address of the node.
- 2. Click the Toggle Navigation icon located in the top-left of the panel to view the left navigation pane.
- 3. Navigate to Admin > Device Connector.
- Verify that the status of server is Not Claimed and that connection to the Cisco Intersight portal is successful.

Eisco Integrated Management Controller	🔶 🔽 admin	@10.29.149.93 - C220-WZP24440A6Z
n / Admin / Device Connector *	Refresh Host Power Launch vKVM Pin	ig CIMC Reboot Locator LED 🔞
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 device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For detailed information about configure the device connector, please visit Help Central Control of Cisco Intersight, a cloud based management platform. For device control of Cisco Intersight, a cl	iter	
Device Connector		\textcircled{O} Settings $\mid \bigcirc$ Refresh
ACCESS MOCE ALLOW CONTROL	Device ID	E E
A Not Claimed The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Devices page and cick Claim a New Device Untersight 18-91323	e for existing account. Open	

- 5. Click Settings.
- 6. Verify that Device Connector is toggled to green and that Access Mode is set to Allow Control. These settings are enabled by default.

evice Connector is an em	bedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Cen
ttings	
eneral	
NS Configuration	When this option is ON, you can claim this system and leverage the capabilities of Cisco Intersight. If it is OFF, no communication will be allowed to Cisco Intersight. Learn More
TP Configuration	C Device Connector
roxy Configuration	Access Mode
ertificate Manager	Read-only Allow Control
	Configuration from Intersight only ⊙
	Tunneled vKVM

7. Register the claim ID and claim code that will be used to claim the device in the Cisco Intersight portal (shown here in red).

Cisco Integrated Management Controller	÷ 🔽	admin@10.29.149.93 - C220-WZP24440A6Z
A / Admin / Device Connector *	Refresh Host Power Launch	vKVM Ping CIMC Reboot Locator LED
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 device connector, please visit Help C	enter	
Device Connector		Settings C Refresh
Access Moor ALLow CONTROL	intersight	Device ID
Not Claimed		
Ine comection to the Use ontersignt nota is successful, out evice is still not carmed. To claim the evice open Claco Intersignt, create a new account and follow the guidance or go to the Derices page and cloc Claim a New Device is still not carmed. To claim the evice open Claco Intersignt, create a new account and follow the guidance or go to the Derices page and cloc Claim a New Device is still not carmed.	rice for existing account. Open	

8. Repeat steps 1 through 7 for all the nodes deployed in the Cohesity DataPlatform cluster.

Claim device in Cisco Intersight platform

This section describes the process for claiming devices in the Cisco Intersight platform.

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Admin > Targets > Claim a New Target.
- 3. Choose Available for Claiming, and for the target type, select Cisco UCS Server (Standalone). Click Start.

$\equiv \frac{dhalls}{cisco}$ Intersight	ADMIN > Targets > Claim Target	Q ■ 14 ▲4 B 441 Q Q () Anii Dhiman 🖉
110 MONITOR 録 OPERATE へ		Select Target Type	
Servers Chassis	Filters		
Fabric Interconnects HyperFlex Clusters Kubernetes	Available for Claiming Categories O All	Compute / Fabric	
CONFIGURE ^ Profiles Templates	Cloud Cloud Native Cloud Native Compater / Fabric Compater / Fabric	rinte ° Crisco UCS Demanyeti (UCSM	
Policies Pools	Council of Interest A an Hyperconverged Hypervisor Network	Platform Services	
Overview Plan Placement	⊖ Grobenizator ⊖ Platform Services ⊖ Storage	Elvest OS Process / APM	
More		Cisco AppOynamics	
Targets Software Repository	Canal		Diare
			oralt

4. Enter the device ID and claim code details from the Cisco IMC (Admin > Device Connector) of each Cisco UCS C-Series node, marked here in red.

onnector 🛧	Refi	resh Host Power Laune	ch vKVM Ping CIMC	Reboot Locator LED 🥊
Device Connector is an embedded r ut configuring the device connector,	nanagement controller that enables the capabil please visit Help Center	ities of Cisco Intersight, a clou	ud-based management plat	form. For detailed information
evice Connector				🕄 Settings 🛛 💭 Refresh
	ACCESS MODE ALLOW CONTROL		Device ID	_
				Ē
·····	••••	•••• 🛆	Claim Code	_
evice Connector	Internet	Intersight		Ē
			0	
Not Claimed				

5. Click Claim.

≡	،،ا،،،ا،، دısco Intersight	••• > Cisco UCS Server (Standalone)	Q 🗷 14 🔺 4 🛛 🗹 🛛 📢 1 🛛 Q	සී ⑦ Anil Dhiman گ
000	MONITOR			
	OPERATE ^	ξÕ.	Cisco UCS Server (Standalone) To claim your target, you must have the Device ID	
	Servers	℃	and Claim Code.	
	Chassis			
	Fabric Interconnects	Device ID *	Claim Code *	
	HyperFlex Clusters			
	Kubernetes			
≫	CONFIGURE ^			
	Profiles			
	Templates	l		
	Policies			
	Pools			
	OPTIMIZE ^			
	Overview	< Previous Cancel		Claim
	-	🔔 Communities	{} API Documentation	

6. Repeat steps 1 through 5 for all the nodes deployed for the Cohesity cluster. For example, the screen image here shows four nodes claimed in Cisco Intersight for Cohesity cluster deployment.

≡	cisco Intersight	ADMIN > Targets 📿	3 🗷 14 🛕 4 🛛 🔀 🙀 1 🖓 🤤	සී 🧿 Anil Dhiman 🖉
<u>00o</u>	MONITOR			Claim Target
	OPERATE ^			
	Servers	Connection Top Targets by Types		Ð
	Chassis	Connected 9 Standalone M UCS Domain WyperFlex Chi	5 S 8 1 ster 1	
	Fabric Interconnects			
	HyperFlex Clusters	2 前 O Add Eilter	10 itams found 10 x per page	
	Kubernetes		Turne Claimed Time	Claimed By
×	CONFIGURE ^		Standalana ME Saniar a faw sasanda aga	
	Profiles		a rew seconds ago	andniman@cisco.com ••••
	Templates	C220-WZP24440A7F OConnected	Standalone M5 Server a few seconds ago	andhiman@cisco.com •••
	Templates		Standalone M5 Server a minute ago	andhiman@cisco.com
	Policies	C220-WZP24440A6Z OCnnected	Standalone M5 Server 3 minutes ago	andhiman@cisco.com •••
	Pools		UCSM Managed Doma Mar 4, 2020 12:50 PM	andhiman@cisco.com ••••
	OPTIMIZE ^		Standalone M5 Server Mar 31, 2021 10:41 AM	andhiman@cisco.com ····
	Overview		Standalone M5 Server Jul 3, 2019 11:44 AM	andhiman@cisco.com •••

Configure server policies

Server policies in the Cisco Intersight platform provide various configurations for Cisco UCS servers, including BIOS settings, disk group creation, Simple Mail Transfer Protocol (SMTP), IPMI settings, and more. Once a policy is configured, it can be assigned to any number of servers to provide a configuration baseline. Policies in Cisco Intersight are native to the application and are not directly imported from Cisco UCS. Policy-based configuration with server profiles is a Cisco Intersight Essentials feature.

Note: For more information about Cisco Intersight server policies, refer to Server Policies.

Note: Customers should have at least an Essentials license to enable configuration of server profiles and policies for standalone Cisco UCS C-Series Rack Servers. For more information, refer to <u>Cisco Intersight</u> <u>Licensing Tiers</u>.

The main server policies required to configure Cisco UCS C220 and C240 server nodes for Cohesity DataPlatform through Cisco Intersight are listed here:

- Organization policy (optional)
- Adaptor configuration policy
- BIOS profile policy
- IPMI-over-LAN policy
- Serial-over-LAN policy
- Storage configuration policy
- Boot-order policy

The following sections describe the server policies created to deploy Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform.

Create organization policy

An organization is a logical entity that enables multitenancy through separation of resources. An organization allows you to divide the physical infrastructure or resources into logical entities, without requiring dedicated physical infrastructure for each organization. For more information about organizations, refer to <u>Introduction to Organizations</u>.

Follow these steps to create an organization:

- 1. Log in to the Cisco Intersight portal.
- 2. Click Settings (the gear icon) and choose Settings.



3. Click Organizations and click the Create Organization tab in the top-left corner.

≡	،راریرار، cisco Intersight	Settings	۵ 🛛	18 🔺 4 🛛 🗹	ç ‡1 Q		O Anil Dhima	in 🖉
	MONITOR OPERATE ^	없) GENERAL Account Details	Organizatio	ons				ion
	Servers Chassis Fabric Interconnects	Access Details [_&] AUTHENTICATION Single Sign-On	Use o Orga	organizations to manage a Inizations at Help Center.	access to your infra	structure. Learn mo	re about x	
	HyperFlex Clusters Kubernetes	Cisco ID	Add	1 Filter	und <u>10 v</u> pe	r page K <	I of 1	\$ }
×	CONFIGURE ^	IP Access Management Security & Privacy		lame 🌲	Memberships All	Usage 1 Roles	Descripti 💲 User in a Defa	<i>\$</i>
	Profiles Templates	Users Groups Rales			Custom		Ore for Interni	
	Policies	Organizations		li	Castom		$ \langle 1 \rangle of 1 \rangle$	 Ж
	OPTIMIZE ^ Overview	API Keys OAuth2 Tokens						

4. Under Memberships, select Custom, name the organization, select the nodes you claimed in the Cisco Intersight platform, and click Create.

	cisco Intersight	Organizations	; > Create		💭 18 🔺 4	⊡ 6 41	Q @ ()) Anil Dhiman 🖉
	MONITOR OPERATE ^	Nar org	^{me *} g-cohesity ©	Description				
	Servers Chassis	Mer	mberships					
	Fabric Interconnects HyperFlex Clusters		Custom Select targets to create a C	All	files and Policies that are	created within a Custom	Organization are	
×	Kubernetes CONFIGURE ^		applicable only to targets in	n the same Organization.				
	Profiles Templates	c	Add Filter		10 items found	10 ∨ per page	<of1 ≥="">> €</of1>	3
	Policies			Status	Type 🗘	IP Address	Target ID	
	Pools OPTIMIZE ^			Connected	Standalone Server	172.25.178.201	WZP22440AX5	
	Overview	C		Not Connected	HyperFlex Cluster	172.25.178.207	8370582135816828569:51.	
	Plan	0		Connected	UCSM Managed Do	10.29.149.11,10.29	FD022191E08 & FD022191	
	Placement	0		Connected	Standalone Server	10.41.2.131	WZP233414DG	
	More			Connected	Standalone Server	10.29.149.248	WZP24130MEV	
	ADMIN ^		C220-WZP24440A6Z	Connected	Standalone Server	10.29.149.34	WZP24440A6Z	
	Targets		C220-WZP24440A75	Connected	Standalone Server	10.29.149.35	WZP24440A75	
	Software Repository							Create

5. Verify that the organization was created successfully.

Create adaptor configuration policy

Adapter configuration policy configures the Ethernet and Fibre Channel settings for the VIC adapter.

Follow these steps to configure adaptor configuration policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.

≡	cisco Intersight		CONFI	GURE > Policies	¢	🛚 18 🔺 4 🛛 🗹	¶⊈1 Q €	පී 🧿 Anil Dhi	iman 🖉
<u>00o</u>	MONITOR							Create F	Policy
	OPERATE ^								
	Servers	1	Plat	form Type L	Jsage				Ð
	Chassis		Ну	perFlex Cluster 19	41 • Used 22 • Not Used 19				
	Fabric Interconnects								
	HyperFlex Clusters				litor	C 41 itema fai			
_	Kubernetes			Name	Platform Tune	41 Rems for	und 10 ♥ per page [N 		
×	CONFIGURE ^						, P		
	Profiles			con_ipmi	UCS Server	IPMI OVER LAN	الله الله	Mar 31, 2021 11:36 AM	
	Templates				UCS Server	Adapter Configuration	1 👩	Mar 31, 2021 11:28 AM	
\square	Policion	ור			UCS Server	Storage	1 慮	Mar 31, 2021 11:28 AM	
	Funcies				UCS Server	Serial Over LAN	1 👸	Mar 31, 2021 11:24 AM	
	Pools				UCS Server	Boot Order	1 🐻	Mar 31, 2021 11:22 AM	
	OPTIMIZE ^				UCS Server	BIOS	1 🐻	Mar 31, 2021 11:22 AM	
	Overview			cohesity_bootorder_c	UCS Server	Boot Order	1 👸	Oct 5, 2020 11:40 PM	

3. For Platform Type, select All. Select Adaptor Configuration and click Start.

Ξ	cisco Intersight	CONFIGURE > Policies > Create	다. 🖾 18 🛕 4 🛛 🦿 📢 1 🔍 🔅 🕜 Anil Dhiman ,	ይ
	MONITOR		Select Policy Type	
*	Servers Chassis Fabric Interconnects HyperFlex Clusters Kubernetes CONFIGURE OFIGIES Policies Policies OPTIMIZE	Filters PLATFORM TYPE All UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	Q, Search Adapter Configuration Link Control Add-ons Local User Auto Support Multicast Backup Configuration Network CIDR BIOS Network Connectivity Certificate Management Node IP Ranges Container Runtime Node OS Configuration Device Connector NTP Disk Group Persistent Memory 	
	Overview		Start	

- 4. On the adaptor configuration Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - For Name, enter coh-adaptor-config.
 - Click Next.

≡	ululu cisco Intersight	••• > Policies > Adapter Configuration > Create	- 🗘 🖪 18 🔺 4 🖸 ⊄ 1 ♀, 🔅 ⑦ Anil Dhiman &
<u>00o</u>	MONITOR	⊂ Progress	Step 1
	OPERATE ^		General
	Servers	General	Add a name, description and tag for the policy.
	Chassis	2 Policy Details	Organization *
	Fabric Interconnects		org-cohesity <u>v</u>
	HyperFlex Clusters		Name *
	Kubernetes		coh-adaptor-config
×	CONFIGURE ^		
	Profiles		Set Tags
	Templates		
	Policies		Description
	Pools		<= 1024
Ľ	OPTIMIZE ^		
	Overview		
	Plan		
	Placement		
	More		
Q	ADMIN ^		
			Next >

5. Under Policy Details, click Add VIC Adaptor Configuration.

≡	cisco Intersigh	it	••• > Policies > Adapter Configura	ation >	Cre	ate 🗘 🛛 24 ,	1 4	∑ 4	1 9 @	⑦ Ani	I Dhiman 🖉
1 <u>0o</u>	MONITOR		⊂ Progress					Step 2			
	OPERATE	^				{		Policy Detail	s		
	Servers		General				<u>}</u>	Add policy details			
	Chassis		2 Policy Details								
	Fabric Interconnects				о т	his policy is applicable only	for UCS	S Servers (Standalon	e)		
	HyperFlex Clusters			Ac	dapter	r Configurations					
	Kubernetes				Add	VIC Adapter Configuration					
*	CONFIGURE	^									ŝ
	Profiles					PCI Slot	LLDP			Port Channel	
	Templates										
	Policies										
	Pools										
~	OPTIMIZE										
	Overview										
	Plan										
	Placement										
	More										
Ð	ADMIN		< Back C							Cre	ate
											1.1

- 6. Enter the following details for the VIC configuration:
 - For PCIe Slot, specify MLOM.

- Disable the Enable Port Channel option. This setting allows all four 25 Gigabit Ethernet ports on the Cisco UCS VIC 1457. When you disable the port channel option, four virtual NICs (vNICs) and virtual host bus adaptors (vHBAs) are available for use on the adapter. When the port channel options is enabled, only two vNICs and vHBAs are available for use, and ports 0 and 1 are bundled as one port channel and ports 2 and 3 are bundled as the other port channel.
- The setup described here uses a 10-Gbps connection to uplink switches from the modular LAN on motherboard (MLOM), so leave FEC Mode set to the default, cl91.

Note: Using 25 Gigabit Ethemet mode typically requires the use of forward error correction (FEC), depending on the transceiver or the type and length of cabling selected. The Cisco UCS VIC 1400 platform by default is configured in CL91 FEC mode (FEC mode Auto, if available in the Cisco IMC user interface, is the same as CL91) and does not support automatic FEC negotiation. Certain switches will need to be manually set to match this FEC mode to bring up the link. The FEC mode must match on both the switch and the VIC port for the link to come up. If the switch in use does not support CL91, you can configure the VIC ports to use CL74 to match the FEC mode available on the switch. This will require a FEC mode change in the VIC configuration.

DOL OL-1 +			
PCI SIOT *			
MLOM			
Ethornot Cottingo			
Luternet Settings			
Enable LLDF			
Fibre Channel Settin	ıgs		
Enable FIP (
Port Channel Setting	gs		
Enable Port	Channel 🛈		
Enable Port	Channel 🛈	J	
Enable Port	S)	
Enable Port	S)	
DCE Interface 1	S	DCE Interface 2	
DCE Interface Setting	s	DCE Interface 2	
DCE Interface Setting	S	DCE Interface 2 FEC Mode *	
DCE Interface Setting DCE Interface 1 FEC Mode * cl91	s v 0	DCE Interface 2 FEC Mode * cl91	~ 0
DCE Interface Setting DCE Interface 1 DCE Interface 1 FEC Mode * cl91	s	DCE Interface 2 FEC Mode * cl91	~ 0
DCE Interface Setting DCE Interface 1 FEC Mode * cl91	s	DCE Interface 2 FEC Mode * cl91	~ 0
DCE Interface Setting DCE Interface 1 FEC Mode * cl91 DCE Interface 3	s	DCE Interface 2 FEC Mode * cl91 DCE Interface 4	v 0
DCE Interface Setting DCE Interface 1 FEC Mode * cl91 DCE Interface 3 EEC Mode *	s	DCE Interface 2 FEC Mode * cl91 DCE Interface 4 FEC Mode *	~ 0
DCE Interface Setting DCE Interface 1 FEC Mode * DCE Interface 3 FEC Mode * CI91	Channel © \$	DCE Interface 2 FEC Mode * cl91 DCE Interface 4 FEC Mode * cl91	~ 0

• Click the Add button.

7. Verify that the VIC adaptor configuration is updated, click the Create button, and verify that the adaptor configuration policy was created successfully.

≡	cisco Intersig	iht	••• > Policies > Adapter Configu	ration	> Cre	eate 🗘 🛚 2	20 🔺 4	ß	¶41 Q	\$ 0	Anil Dhiman 🚨
<u>100</u>	MONITOR		Œ Progress					Step 2			
	OPERATE	^	(1) General			ξÕ	2	Policy Det	tails		
	Servers					`~ d	ίςς Σ	Add policy det	2110		
	Chassis		2 Policy Details								
	Fabric Interconnects				0	I his policy is applicable	only for UC	S Servers (Stand	alone)		
	HyperFlex Clusters			4	Adapte	r Configurations					
	Kubernetes				Add	VIC Adapter Configurati					
≫	CONFIGURE	^									÷
	Profiles			ſ		PCI Slot	LLDP			Port Channel	
	Templates					MLOM	Enable	ed	Enabled	Disabled	
	Policies										
	Pools										
~	OPTIMIZE	^									
	Overview										
	Plan										
	Placement										
	More										
٩	ADMIN										
			< Back	Cancel							Create

Create BIOS profile policy

BIOS policy automates the configuration of BIOS settings on the managed devices. You can create one or more BIOS policies that contain specific groups of BIOS settings. If you do not specify a BIOS policy for a server, the BIOS settings remain as they are. If a BIOS policy is specified, the values that are specified in the policy replace any previously configured values on a server (including bare-metal server configuration settings). To apply the BIOS policy settings, you must reboot the server.

Follow these steps to configure BIOS policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight Platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.
- 3. For Platform Type, select All. Select BIOS and click Start.

≡	،،اب،اب دisco Intersight	CONFIGURE > Policies > Create	🗘 🗷 19 🛕 5 🛛 😭	1 Q 🔅 ⑦ Anil Dhiman 싶
	MONITOR OPERATE ^		Select Policy Type	
	Servers Chassis Fabric Interconnects	Filters Platform type	Q Search Adapter Configuration	Link Control Local User
×	Kubernetes CONFIGURE	UCS Server	Auto Support Backup Configuration BIOS	Multicast Network CIDR Network Configuration
	Profiles Templates	HyperFlex Cluster Kubernetes Cluster	Boot Order Certificate Management	Network Connectivity Node IP Ranges
	Policies		Container Runtime Device Connector	Node OS Configuration NTP
2	OPTIMIZE ^ Overview Plan		Disk Group DNS, NTP and Timezone Ethernet Adapter	Persistent Memory Port Replication Network Configuration
	Placement More		Ethernet Network Ethernet Network Control Ethernet Network Crown	SAN Connectivity SD Card Socurity
ē	ADMIN ^			Start

- 4. On the BIOS policy Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - Name the BIOS policy **coh-bios-config**.
 - Click Next.

≡	່ (Intersight	CONFIGURE > Policies > BIOS > Create	다. 🖬 19 🔺 5 🛛 🤤 📭 1 🔍 🐯 💮 Anil Dhiman 🕰
<u>00o</u>	MONITOR	⊂ Progress	Step 1
	OPERATE ^	General	General Adda arms description and the for the polling
	Servers		Adu a name, description and tag for the puncy.
	Chassis	2 Policy Details	Organization *
	Fabric Interconnects		org-cohesity ~
	HyperFlex Clusters		Name *
	Kubernetes		<u>coh-bios-config</u>
×	CONFIGURE ^		
	Profiles		set lags
	Templates		Description
	Policies		<= 1024
	Pools		
	Overview		
	Plan		
	Mare		
a			
- (<u>P</u>)			Next >

- 5. On the BIOS Policy Details page, do the following:
- Select the UCS Server (Standalone) tab.
- Select the Processor option and select the following options to enable optimal processor performance:
 - Energy Performance: Balanced performance
 - Energy Efficient Turbo: Disabled
 - Power Performance Tuning: OS
 - Package C State Limit: C0 C1 state
 - Hardware P state: performance
 - Processor EPP Enable: Enabled
 - EPP Profile: Performance
 - Workload Configuration: I/O Sensitive

- Processor			
DRAM Clock Throttling		Energy Efficient Turbo	
platform-default	× 0	disabled	~ 0
Power Performance Tuning		UPI Link Frequency Select	
<u>os</u>	<u>v 0</u>	platform-default	× 0
Package C State Limit		Patrol Scrub	
C0 C1 State	<u>~ 0</u>	platform-default	<u>~ 0</u>
Processor EPP Enable		EPP Profile	
enabled	~ 0	Performance	<u>* 0</u>
Uncore Frequency Scaling		Workload Configuration	
platform-default	~ 0	I/O Sensitive	¥ 0

• Select the Serial Port tab. Set Serial A Enable to enabled.

 Serial Port 	
Serial A Enable	
enabled	

• Click Create and verify that the BIOS policy was created successfully.

Create IPMI-over-LAN policy

IPMI-over-LAN policy defines the protocols for interfacing with a service processor that is embedded in a server platform. The IPMI enables an operating system to obtain information about the system health and control system hardware and directs the baseboard management controller (BMC) to perform appropriate actions to address a problem. You can create an IPMI-over-LAN policy to manage the IPMI messages through the Cisco Intersight platform. You can assign these user roles to an IPMI user by session.

Follow these steps to create IPMI-over-LAN policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.
- 3. For Platform Type, select All. Select IPMI Over LAN and click Start.
- 4. On the IPMI-over-LAN policy Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - Name the BIOS policy coh-ipmi-over-lan.
 - Click Next.

≡	راسان Intersight	CONFIGURE > Policies > IPMI Over LAN > 0	Steate 🗘 🖬 19 🔺 5 🛛 🔀 🛛 🕫 🖓 🖉 🖉 Anil Dhiman 🕰
<u>00o</u>	MONITOR	Progress	Sten 1
	OPERATE ^		General
	Servers	General	Add a name, description and tag for the policy.
	Chassis	2 Policy Details	Organization *
	Fabric Interconnects		cohesity_org ~
	HyperFlex Clusters		Name *
	Kubernetes		coh-ipmi-over-lan
≫	CONFIGURE ^		
	Profiles		Set Tags
	Templates		
	Policies		Description
	Pools		<= 1024
Ľ	OPTIMIZE ^		
	Overview		
	Plan		
	Placement		
	More		
ē	ADMIN ^		
	Torrata	Cancel	Next >

- 5. On the IPMI-over-LAN Policy Details page, do the following:
 - Select the UCS Server (Standalone) tab.
 - Verify that IPMI over LAN is enabled.
 - For Privilege Level, choose admin.
 - Create an encryption key. The encryption key to use for IPMI communication should have an even number of hexadecimal characters and not exceed 40 characters.
 - Click Create.

≡	cisco Intersight	CONFIGURE > Policies > I	MI Over LAN > Create 🗘 🖬 19 🛦 5 🔀 🙀 1 🔍 😳 🧿 Anil Dhiman 🔬
<u>00o</u>	MONITOR	Progress	Step 2
	OPERATE ^		Policy Details
	Servers	General	Add policy details
	Chassis	2 Policy Details	
	Fabric Interconnects		
	HyperFlex Clusters		Privilane Lavel
	Kubernetes		admin v O
×	CONFIGURE ^		
	Profiles		Encryption Key
	Templates		
	Policies		
	Pools	1	
⊵	OPTIMIZE ^		
	Overview		
	Plan		
	Placement		
	More		
ē	ADMIN ^	< Back	Cancel
	Taraete		

6. Verify that the IPMI-over-LAN policy was created successfully.

Create serial-over-LAN policy

Serial-over-LAN policy enables the input and output of the serial port of a managed system to be redirected over IP. You can create one or more serial-over-LAN policies that contain specific groups of serial-over-LAN attributes that match the needs of a server or a set of servers.

Follow these steps to create serial-over-LAN policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.
- 3. For Platform Type, select All. Select Serial Over LAN and click Start.
- 4. On the Serial-over-LAN policy Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - Name the BIOS policy **coh-serial-over-lan**.
 - Click Next.

≡	cisco Intersight	CONFIGURE > Policies > Serial Over LAN > Create	다. 🖪 19 🛦 5 🕝 🕫 1 오, 😨 🕜 Anil Dhiman 요
<u>00o</u>		⊂ Progress	Step 1
	OPERATE ^		General
	Servers	General	Add a name, description and tag for the policy.
	Chassis	2 Policy Details	Organization *
	Fabric Interconnects		org-cohesity <u> </u>
	HyperFlex Clusters		
	Kubernetes		coh-serial-over-lan
×	CONFIGURE ^		
	Profiles		Set Tags
	Templates		
	Policies		Description
	Pools		
Ľ	OPTIMIZE ^		
	Plan		
	Placement		
	More		
Ō	ADMIN ^		Next >

- 5. On the Serial-over-LAN Policy Details page, do the following:
 - Verify that Serial over LAN is enabled.
 - For COM Port, select com0.
 - For Baud Rate, select 115200.
 - Leave the solid-state-disk (SSD) port at the default setting.

≡	ւյիսի։ cisco Intersight		Dver LAN 🗲 Create 🛛 🚨 19 🔺 5	[·] 약⊄ 1 옥, ۞ Anil Dhiman 요
<u>00o</u>	MONITOR	🔄 Progress		Stan 2
	OPERATE ^		£ ` }	Policy Details
		General		Add policy details
	Chassis	2 Policy Details		All Platforms LICS Server (Standalone) LICS Server (FL-Attached)
	Fabric Interconnects			
	HyperFlex Clusters		COM Port	
	Kubernetes			
\times	CONFIGURE ^			
	Profiles		Baud Rate 115200	
	Templates			
	Policies		SSH Port * 2400	
	Pools		1024 - 65535	
Ľ	OPTIMIZE ^			
	Overview			
	Plan			
	Placement			
	More			
Q	ADMIN ^	< Back	Cancel	Create

6. Click Create and verify that the Serial-over-LAN policy was created successfully.

Create storage configuration policy

Storage configuration policy creates virtual drives, configures the storage capacity of a virtual drive, and associates the drive with a disk group policy. With the disk group policy, you can select and configure the disks to be used for a specific virtual drive. You must create a disk group policy before you add a virtual drive for a storage policy.

JBOD mode for local disks is enabled for Cisco UCS C220 and C240 nodes configured for Cohesity clusters.

Follow these steps to create storage policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.
- 3. For Platform Type, select All. Select Storage Policy and click Start.
- 4. On the storage policy Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - Name the policy coh-storage-policy.
 - Click Next.
- 5. On the Policy Details page, enable the JBOD option.

≡	cisco Intersight	CONFIGURE > Policies > Store	ye > Create 🗘 🖬 19 🛦 5 🗹 🕵 🤤 ⑦ Anil	Dhiman 🚨
000	MONITOR	⊂ Progress	Step 2 Policy Details	
Ŵ	OPERATE ^		Add policy details	
	Servers	General		
	Chassis	2 Policy Details	All Platforms UCS Server (Standalone) UCS Server (FI-A	ttached)
	Fabric Interconnects	1	 You must have a disk group policy to add virtual drives in a storage policy. (Note: This is not applicable for virtual drives for Cisco Boot optimized M.2 RAID controller) 	
	HyperFlex Clusters			
	Kubernetes		Drive Configuration	
×	CONFIGURE ^	l i	+ Global Hot Spares Enable	
	Profiles		Unused Disks State 0	
	Templates		Unconfigured Good	
	Policies			
	Pools	1	Retain Virtual Drives	
Ľ	OPTIMIZE ^		Add Virtual Drive	
	Overview	1		
	Plan		Virtual Drive Name Size (MB) Disk Group Expand to Availa Set as Boot	
	Placement	1		
	More			
Q	ADMIN ^	< Back	Cancel Crea	ate
	Targets			

6. Click Create and verify that the storage policy was created successfully.

Create boot-order policy

Boot-order policy configures the linear ordering of devices and enables you to change the boot order and boot mode. You can also add multiple devices under various device types, rearrange the boot order, and set parameters for each boot device type.

Note: This boot policy is specific to Cisco UCS C220 and C240 nodes with an M.2 hardware RAID controller. Verify that the node is installed with M.2 hardware RAID (Cisco part number UCS-M2-HWRAID).

Confirming the server RAID controller

To confirm that the Cisco UCS C220 or C240 Rack Server deployed for Cohesity is equipped with M.2 hardware RAID, follow these steps:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Server. Click any Cisco UCS C220 or C240 node used for Cohesity.

≡	cisco Intersight	OPERATE >	Servers > C220-WZP24440A6V) 🛛 19 🔺 5 🛛 🗹
000	MONITOR	General Inv	ventory UCS Server Profile HCL					
	OPERATE ^	Details		Properties				
L	Servers	Health	Critical	Cisco UCSC-C220-M5L			Front View	Rear View Top View
	Chassis	Name User Label	C220-WZP24440A6V					
	Fabric Interconnects	Management	IP 10.29.149.37					
	HyperFlex Clusters	Serial	WZP24440A6V	Power 🕐 Locator LED O				Health Overlay 🌉
	Kubernetes	PID	UCSC-C220-M5L					
×	CONFIGURE ^	Vendor	Cisco Systems Inc	CPUs				
20200	Orchestration	Revision		Threads	40	Adapters		
	Orchestration	Asset Tag	Unknown	CPU Cores		NIC Interfaces		
	Profiles	License Tier	Essentials	CPU Cores Enabled		HBA Interfaces		
	Templates	Contract Statu	JS Not Covered	Memory Capacity (GiB)	64.0		7B6EB596-0063-4D1B-9	C5F-657DCA6F81AB
		Management	Mode Standalone	CPU Capacity (GHz)	44.0			
	Policies	Chassis						
	Pools	LICS Server Pr	ofile Cohesity-Sever-					
\bowtie	OPTIMIZE ^		Template- 1_DERIVED-4					
	Overview	UCS Server Pr	ofile Status OK					
	Plan	Firmware Vers	sion 4.1(3b)					
	Placement	Firmware Stat						
	More	Organizations						

3. Click the Inventory tab and expand Storage Controller. Confirm that Controller MSTOR-RAID (M2HWRAID) is installed on the server.

	cisco Intersight	OPERATE > Servers > C220-WZP24	140A6V		🗘 🖬 19 🔺 5 🛛 🔀		
		General Inventory UCS Server Profile					Actions ~
		Expand All	Controller MSTOR-RAID (M2HWRAID)				
		Motherboard					
	Chassis	Boot	General Physical Drives Virtual Drives				
		СІМС	Configuration		Hardware		
		CPUs					
	HyperFlex Clusters	Memory	Firmware Version	2.3.17.1014	Controller ID		MSTOR-RAID
	Kubernetes	Network Adapters					MSTOR-RAID
	laborrietes	PCIe Devices			RAID Support		
×		Storage Controllers			Number Of Local Disks		
		Controller MSTOR-RAID					
	Orchestration	Controller MRAID (RAID)			Serial		FCH243374F5
	D. (1).	TPM				Cisco Boot optimi	zed M.2 Raid controller
	Promes						Marvell

Configuring boot-order policy

Now follow these steps to create boot-order policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Configure > Policies. Click Create Policy.
- 3. For Platform Type, select All. Select Boot Order Policy and click Start.
- 4. On the boot-order Create page, do the following:
 - For Organization, select org-cohesity, created in the previous section.
 - Name the policy coh-boot-order-policy.
 - Click Next.
- 5. On the boot-order Policy Details page, enable UEFI boot mode.

Note: UEFI boot mode for Cisco UCS C240 M5 Rack Servers with Cohesity DataPlatform is supported only by Cohesity Release 6.6.0a and later.

Note: UEFI boot mode for Cisco UCS C220 M5 Rack Servers with Cohesity DataPlatform is supported by all Cohesity releases.

Note: This boot policy is specific to Cisco UCS C220 and C240 nodes with an M.2 hardware RAID controller. Verify that the node is installed with M.2 hardware RAID (Cisco part number UCS-M2-HWRAID).

Note: Be sure that the slot is named as MSTOR-RAID.

- 1. Click Add Boot Device and select Local Disk.
- 2. Name the device m2-2. (This name can be any name defined by the user.)
- 3. Verify that the slot is named MSTOR-RAID. This name is fixed and must be the name used.

≡	cisco Intersight	CONFIGURE > Policies > Boot Orde	r > Create 🗘 🛚 19 🔺 5	<u>۲</u>	\$1 Q	© #	Anil Dhiman 🔔
nNa	MONITOR						
<u></u>	monitori	⊆ Progress	~~~~	Step 2			
ఱ	OPERATE ^	1 General	ζΟ)/2	Policy Deta	nils		
	Servers		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Add policy detail			
	Chassis	2 Policy Details			1000 0		
	Fabric Interconnects			All Platforms	UCS Server (Standal	one) UCS Se	rver (FI-Attached)
	HyperFlex Clusters		Configured Boot Mode ⊙				
	Kelenater		Legacy Legacy Unified Extensible Fin	mware Interface (UI	EFI)		
	Kubernetes		○ Enable Secure Boot ⊙				
×	CONFIGURE ^						
	Profiles		Add Boot Device ~				
	Templates						
ſ	Delision		— Local Disk (m2-2)			Enabled	
	Folicies		Device Name * m2-2		Slot MSTOR-RAID		
	Pools						
Ľ	OPTIMIZE ^						
	Overview						
	Plan		Bootloader Name		Bootloader Descrip	otion	
	Placement						
_							
	More		Bootloader Path				
Q	ADMIN ^						Create

- 4. Again click Add Boot Device and select Local Disk.
- 5. Name the device **m2-1**. (This name can be any name defined by the user.)
- 6. Verify that the slot is named MSTOR-RAID. This name is fixed and must be the name used.

Add Boot Device		
— Local Disk (m2-1)	Enabled 🗂	
Device Name * m2-1	Slot MSTOR-RAID	
Bootloader Name	Bootloader Description	

- 7. Again click Add Boot Device. Select Virtual Media.
- 8. Name the device **vmedia1**.

≡	cisco Intersight	CONFIGURE > Policies > Boot C	rder > Create 🗘 🖬 19 🛦 5 🔀 ⊄ 1	ද 😳 ල Anil Dhiman ዾ
<u>00o</u>	MONITOR	⊆ Progress	Share 2	
Ŷ	OPERATE ^	~	Policy Details	
	Servers	General	Add policy details	
	Chassis	Policy Details		100 Carrier (Classificity a)
	Fabric Interconnects			UCS Server (FI-Attached)
	HyperFlex Clusters		Configured Boot Mode ⊙ Configured Boot Mode ⊙ Legacy O Unified Extensible Firmware Interface (UEFI)	
	Kubernetes		_	
×	CONFIGURE ^		Enable Secure Boot	
	Profiles			
	Templates		- Virtual Media (ymedia1)	💽 Enabled 🏦 🔺 🗸
	Policies		Device Name *	-
	Pools		vmedia1 O	
	OPTIMIZE ^			
	Overview		Sub-Type None v O	
	Plan			

- 9. Verify that the boot order is defined as listed here. You can change the boot order with up and down arrow keys.
- 10. First device in the boot order is m2-1.
- 11. Second device in the boot order is m2-2.
- 12. Third device in the boot order is vmedia1.

=	cisco Intersight	CONFIGURE > Policies > Boot C	Order > coh-boot-order-policy > Edit				Q 🖬 19 🔺 5 🛛		
<u>00o</u>	MONITOR	😇 Progress				Step 2			
ø		General			{0}	Policy Details			
	Servers	Ĭ			~~~~~	and pointy details			
	Chassis	Policy Defails				V All Platforms	UCS Server (Standalone)	UCS Server (FI-	Attached)
	Fabric Interconnects			Configured Boot Mode					
	HyperFlex Clusters			C Legacy O Unified Extensible	Firmware Interface (U	JEFT)			
×	CONFIGURE ^			Enable Secure Boot O					
	Orchestration								
	Profiles			Add Boot Device					
	Templates			+ Local Disk (m2-1)			Cnable	4 🗈 🥂	
	Policies			+ Local Disk (m2-2)			Chable	a 🖬 🗸	
	Pools								
⊵	OPTIMIZE ^			+ Virtual Media (vmedia1)			Enable	• 🗊 ^	
	Overview								
	Placement								
	More								
জ্ঞা	ADMIN ^								

13. Click Create and verify that the boot-order policy was created successfully.

Configure and deploy server profile for Cohesity nodes

This section describes Cisco Intersight server profile templates and server profiles, which define the identity of the Cisco UCS C220 and C240 Rack Servers specific to Cohesity DataPlatform.

In Cisco Intersight, server profile templates enable the user to define a template from which multiple server profiles can be derived and deployed. Any property modification made in the template is synchronized in all the derived profiles. You can deploy these modified profiles individually. This feature facilitates quick and easy configuration because multiple profiles can be created and edited simultaneously. Server profile templates contain the configuration server policies created in the previous section.

Server profiles facilitate resource management by simplifying policy alignment and server configuration. You can create server profiles using the Server Profile wizard, or you can import the configuration details of a Cisco UCS C-Series server directly from the Cisco IMC. Using the Server Profile wizard, you can create profiles to provision servers, create policies to help ensure smooth deployment of servers, and eliminate failures that are caused by inconsistent configuration.

Note: Creation of a server profile template for Cohesity nodes is a one-time process generally performed during infrastructure provisioning. After a template has been created, you can instantiate server profiles and deploy them to the Cohesity nodes on Cisco UCS C220 and C240 Rack Servers, hence provisioning deployments at scale.

To create a server profile template, follow these steps:

1. Log in to the Cisco Intersight platform at https://intersight.com/.



2. Navigate to Operate > Configure > Templates. Click Create UCS Server Profile Template.

- 3. On the General page, do the following:
 - For Organization, choose org-cohesity (created in the previous section).
 - Name the template **Cohesity-Server-Template1**. (This name can be any name defined by user.)
 - For Target Platform, select UCS Server (Standalone).
 - Click Next.

≡	יוןייוןי cisco Intersight	CONFIGURE > Create UCS Server Profile Template	û 🖪 19 🔺 5 🛛 🖓 📢 1 🔍 🔅 💮 Anil Dhiman &
<u>00o</u>	MONITOR	Progress	
	OPERATE ^		General
	Servers	General	Enter a name, description, tag and select a platform for the server profile template.
	Chassis	2 Compute Configuration	
	Fabric Interconnects	3 Management Configuration	org-cohesity
	HyperFlex Clusters	4 Storage Configuration	
	Kubernetes	5 Network Configuration	Cohesity-Sever-Template-1 O
×	CONFIGURE ^	6 Summani	
	Profiles	Summary	Target Platform ⊙ ● UCS Server (Standalone)
	Templates		
	Policies		Set Tags
	Pools		
⊵	OPTIMIZE ^		Description
	Overview		<u>~</u> <= 1024
	Plan		
	Placement		
	More		
Ō	ADMIN ^		Next >

- 4. On the Compute Configuration page, select the server policies created earlier.
 - For BIOS, select coh-bios-policy.
 - For Boot Order, select coh-boot-order-policy.
 - Click Next.

≡	cisco Intersight	CONFIGURE 🗲 Create UCS Server Profile Template 🗘 🖬 19 🔺 5 🔀 📢 1 🔍 🔅 🕜 Anil D	
<u>00o</u>	MONITOR	⊆ Progress	
	OPERATE ^	Compute Configuration	
	Servers	Create or select existing compute policies that you want to associate with this template.	
	Chassis	Compute Configuration	
	Fabric Interconnects	3 Management Configuration	
	HyperFlex Clusters	4 Storage Configuration	
	Kubernetes	5 Network Configuration	
≫	CONFIGURE ^	6 Summary	
	Profiles	Virtual Media	
	Templates		
	Policies		
	Pools		
\succeq	OPTIMIZE ^		
	Overview		
	Plan		
	Placement		
	More		
Ō	ADMIN ^	Kack Close	
	Targets		

5. On the Managed Configuration page, select the appropriate policies.

- For IPMI Over LAN, select coh-ipmi-over-lan-policy.
- For Serial Over LAN, select coh-serial-over-lan.
- Click Next.

≡	cisco Intersight	CONFIGURE > Create UCS Server Profile Te	emplate 🗘 🖬 19 🛦 5 🖓 📢 1 🔍 🔅 🧭 Anil Dhiman 🖉
<u>00o</u>	MONITOR	⊆ Progress	Stan 3
	OPERATE ^ Servers Chassis	General Compute Configuration	Management Configuration Create or select existing Management policies that you want to associate with this template.
	Fabric Interconnects	Management Configuration	Show Attached Policies (2)
	HyperFlex Clusters	4 Storage Configuration	Device Connector
	Kubernetes	5 Network Configuration	IPMI Over LAN coh-ipmi-over-lan-policy 🗐
×	CONFIGURE ^	6 Summary	LDAP
	Profiles		Local User
	Templates		Network Connectivity
	Policies	_	NTP
	Pools		Serial Over LAN X 👁 coh-serial-over-lan 🗐
	OPTIMIZE ^		SMTP
	Overview		SNMP
	Plan		SSH
	Placement		Syslog
	More		Virtual KVM
ø	ADMIN ^		
			Next >

- 6. On the Storage Configuration page, do the following:
 - For Storage, select coh-storage-policy.
 - Click Next.



- 7. On the Network Configuration page, do the following:
 - For Adaptor Configuration, select coh-adaptor-config.
 - Click Next.

≡	uludu Intersight	CONFIGURE > Create UCS Server Profile Temple	ate 🗘 🖬 19 🛦 5 📝 📢 1 🔍 🛱	⑦ Anil Dhiman 요
<u>00a</u>	MONITOR	프 Progress	Step 5	
	OPERATE ^	General	Network Configuration	
	Servers		policies that you want to associate with this	
	Chassis	2 Compute Configuration	template.	
	Fabric Interconnects	3 Management Configuration	Show Attached Policies (1)	
	HyperFlex Clusters	4 Storage Configuration	dapter Configuration	coh-adaptor-config 📋
	Kubernetes	5 Network Configuration	AN Connectivity	
×	CONFIGURE ^	6 Summary	AN Connectivity	
	Profiles			
	Templates			
	Policies			
	Pools			
\bowtie	OPTIMIZE ^			
	Overview			
	Plan			
	Placement			
	More			
Ō	ADMIN ^			Next >
	¥20020			

8. Review the summary on the Summary page and verify the settings. Then click Derive Profiles.

≡	cisco Intersight	со	NFIGURE > Create U	ICS Server Profile Te	emplate	Q 🛛 19 🛕 5	⊡ ¶511 C			
<u>00o</u>	MONITOR	_ ∈	Progress				Step 6			
Ŵ	OPERATE ^		General			, , , , , , , , , , , , , , , , , , ,	Summary			
	Servers	Ĭ	General			✓= ,	resolve errors and deploy.	and the policies,		
	Chassis	2	Compute Configuratio	n						
	Fabric Interconnects	3	Management Configur	ration	General					
	HyperFlex Clusters	(4)	Storage Configuration		Template Na	Cohesity- Sever-	Organization	org-cohesity		
	Kubernetes	(5)	Network Configuration	1	Target Platfor	Template-1 UCS Server				
×	CONFIGURE					(Standalone)				
	Profiles									
	Templates				Compute Configuration	Management Configuration	Storage Configuration	Network Configuration		
	Policies				BIOS				ach bias config	a
	Pools				BIOS				con-bios-coning	
	OPTIMIZE				Boot Order			coh	i-boot-order-policy	
	Overview									
-	Plan									
	Plan Placement									
	Placement More									

- 9. After you click Derive Profiles, you can create server profiles that you can associate with Cohesity nodes claimed in Cisco Intersight. You can assign profiles either immediately or later.
 - You can assign server profiles to nodes already claimed in Cisco Intersight. For the purposes of this document, you assign the server to the derived server profiles.
 - You can select Assign Later and just create server profiles from the server profile template.

=	cisco intersigni	···· > Conesity-sever-rempiate-r > Der	
	MONITOR OPERATE ^ Servers Chassis	 Progress General 2 Details 	Step 1 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.
	Fabric Interconnects	3 Summary	UCS Server Profile Template
×	HyperFlex Clusters Kubernetes CONFIGURE ^		Name Cohesity- Organization org-cohesity Sever- Template-1 Target Platfor UCS Server (Standalone)
	Profiles		Server Assignment
	Templates		Assign Server Later
	Policies		
	Pools		
2	OPTIMIZE ^		
	Overview		Add Hiter
	Plan		Cooperative Cooperati
	Placement		
	More		
ē	ADMIN ^		<u> </u>
1	1	Cancel	Next >

10. Select Assign Server and select all the nodes claimed in Cisco Intersight for Cohesity cluster deployment. Click Next.

	ւլիսի։ cisco Intersight		> Derive					19 🔺 5		₽ \$1		
						Step 1						
Ŷ		General				General						
					_ _ 	profile(s) or spec want to derive an	ify the number of profile d assign the servers late	s that you ar.				
		2 Details	1100 00000	Deafile Template								
		3 Summary	uus server	Prome remplate								
			Name Target Plati	Cohesity	y-Sever-Template-1			org-cohes	sity			
×			Server Assi	ignment								
			Assig	In Server Ass								
	Templates											
				Add Filter								
										ZP24440A6		
										ZP24440A7		
										ZP24440A7		
				C220-WZP24440						ZP24440A6		
	Software Repository											

11. Edit the profile name prefix and click Next.

≡	cisco Intersight		ity-Sever-Template-1 > Derive	Q III 19 ▲ 5 🕑 9⊄1 Q 😳 0	
<u>00o</u>		œ Progress	of the pr		
9		General	General		
		2 Details	Organization * org-cohesity	Target Platform ✓ UCS Server (Standalone)	
	Chassis Fabric Interconnects	3 Summary			
			Description	Set Tags	
	Kubernetes				
×			Derive 4		
	Orchestration		Profile Name Prefix Cohesity-Sever-Template-1_DERIVED-		
	Templates			Assigne C220-WZP24440A6Z	
			Cohesity-Sever-Template-1_DERIVED-1		
	Pools			Assigne C220-WZP24440A75	
₽	OPTIMIZE ^		Cohesity-Sever-Template-1_DERIVED-2		
			2 Namet		
			Cohesity-Sever-Template-1_DERIVED-3	Assigne GZ20-WZP/2444UA/F	
	More		4 Name * Cohesity-Sever-Template-1_DERIVED-4	Assigne C220-WZP24440A6V	
ģ					
					Next >

12. Review the Summary page and confirm the settings. Then click Derive.

≡	cisco Intersight	CONFIGURE > UCS Server Profile Templates > Col	esity-Sever-Template-1 > Derive		۵ 🖪	19 🛕 5 🛛 🖂	¢‡1 Q,	© (0) Anil Dhiman 🔬
000		☑ Progress			Step 3				
•	OPERATE ^ Servers	General			Summary Summary of the profiles that need to be from the profile template.				
	Chassis	(2) Details	General					ř.	
	Fabric Interconnects	Summary		Cohesity-Sever-Template-1		org-cohesity			
	Kubernetes			UCS Server (Standalone)					
*	CONFIGURE ^		Server Selection					l,	
	Orchestration								
	Profiles		Cohesity-Sever-Ter	mplate-1_DERIVED-1	C220-WZP24440A6Z				
	Templates		Cohesity-Sever-Te	mplate-1_DERIVED-2	C220-WZP24440A75				
	Policies		Cohesity-Sever-Ter	mplate-1_DERIVED-3	C220-WZP24440A7F				
	Pools		Cohesity-Sever-Ter	mplate-1_DERIVED-4	C220-WZP24440A6V				
\bowtie	OPTIMIZE ^								
	Overview		Compute Configurat	ion Management Configuration					
	Plan								
	Placement		BIOS				coh-bios-config 📋		
	More		Boot Order			co	h-boot-order-policy		
ē	ADMIN ^								
	Targets							ſ	Derive

13. Navigate to Configure > Profiles and verify that the server profiles assigned to server nodes are in the Not Deployed state.

	alaala		232.000											
	cisco Intersight			IGURE > Profiles				■ 19 🛆 5 🕑 🥵 1		iman <u>Q</u>				
<u>00</u> e						erver Profiles Kubernetes Cluster Profi			Create UCS Server	Profile				
ø														
				2 7 🗊 🛛 🔍 Add Filter				Export 8 items found 16 -						
							UCS Server Template							
					🔺 Not Deployed	UCS Server (Standalone)			4 minutes ago					
ŕ					A Not Deployed	UCS Server (Standalone)			4 minutes ago					
					A Not Deployed	UCS Server (Standalone)			4 minutes ago					
×					A Not Deployed	UCS Server (Standalone)			4 minutes ago					
	Orchestration				19 Failed	UCS Server (Standalone)			May 21, 2021 12:10 PM					
					Dut of Sync	UCS Server (Standalone)			May 21, 2021 7:19 AM					
	Templates	1			Not Assigned	UCS Server (Standalone)								
					Not Assigned	UCS Server (Standalone)								
										N				
1														

14. Select the Cohesity profiles and click Deploy.

=	cisco Intersight	CONFIGURE > Profiles			🖬 19 🔺 5 🛛 🖓 📢 1		
<u>00o</u>			files UCS Domain Profiles UCS S	erver Profiles Kubernetes Cluster Profil		Create UCS Server F	rofile
ø				-			
×		··· / 🧷 🛍 🔍 Add Filter			Export 8 items found 16 ~	perpage K < 1 of 1 > >	
	Orchestration						
	Profiles	Unassign Server	A Not Deployed	UCS Server (Standalone)		4 minutes ago	
	Templates		A Not Deployed	UCS Server (Standalone)			
			A Not Deployed	UCS Server (Standalone)			
		Cohesity-Sever-Template-1_DERIVED-4	A Not Deployed	UCS Server (Standalone)		4 minutes ago	
Ł			E Failed	UCS Server (Standalone)		May 21, 2021 12:10 PM	
				UCS Server (Standalone)		May 21, 2021 7:19 AM	
			I Not Assigned	UCS Server (Standalone)		Apr 22, 2021 6:25 PM	
			I Not Assigned	UCS Server (Standalone)		Apr 22, 2021 6:25 PM	
	More						

15. A new window opens. Acknowledge the server reboot and click Deploy.



16. Monitor the deployment process. The state will transition from Validating to Configuring to OK.

≡	الافتان، Intersight		CONFIGURE > Profiles Q 11 Q, Q O Anith														nan 🔔
<u>00o</u>			HyperFlex Cluster Profiles UCS Clussis Profiles UCS Domain Profiles UCS Server Profiles Kubernetes Cluster Profiles UCS Server												S Server Pr	ofile	
Ŷ																	_
×				🖉 🖉 📋 🛛 🔍 Add Filter									16 v pr				۲
																	ş
																	•••
	Pools	Ľ		Cohesity-Sever-Template-1_DERIVED-4	O Validating		UCS Server (Standalone)		Cohesity-Sever-Template-1		C220-WZP24440A6V	l	٩	few seconds a	90		***

17. After all the profiles are in the OK state, the Cohesity server profiles on the Cisco UCS C220 and C240 nodes have been successfully deployed. You are ready to move on to Cohesity ISO file deployment, described in the next section.

\equiv	cisco Intersight	CONF	GURE > Profiles			۵	🗷 19 🛕 5 🛛 😭 📢 1	S O Anil Dhir	nan
<u>08a</u>					Server Profiles Kubernetes Cluster Profi			Create UCS Server P	rofile
0									
×			Add Filter				Export 8 items found 16 ~	per page (< < 1 of 1 > >	0
				© ок	UCS Server (Standalone)				
				O OK	UCS Server (Standalone)				
				Ø OK	UCS Server (Standalone)				
					UCS Server (Standalone)			a minute ago	
2	OPTIMIZE ^			0 Failed	UCS Server (Standalone)			May 21, 2021 12:10 PM	
				E Out of Sync	UCS Server (Standalone)				
				Not Assigned	UCS Server (Standalone)				
	Placement			C Not Assigned	UCS Server (Standalone)				
	More								

Install the Cohesity operating system

The section describes the deployment of the Cohesity ISO file on Cisco C220 and C240 standalone server nodes managed through the Cisco Intersight platform. The steps here are limited to installation of the Cohesity ISO file on Cisco UCS C220 and C240 Rack Server nodes and do not detail the procedure for configuring a Cohesity cluster. After the Cohesity OS is installed on each node, refer to the <u>Cohesity</u> standalone setup guide for information about how to configure Cohesity clusters. [[PLS PROVIDE LINK]]

Customers have a choice to install the Cohesity ISO file through either of the following processes:

- You can use the Cisco Intersight Install Operating System option. (This process requires at least a Cisco Intersight Advantage license.)
- You can install the operating system through vMedia and the one-time boot device feature. (This process requires at least a Cisco Intersight Essentials license.)

Install the OS through the Cisco Intersight platform

The Cisco Intersight platform introduces the capability to install vMedia-based operating systems on the managed servers in your data center. With this capability, you can perform an unattended OS installation on one or more Cisco UCS C-Series standalone servers from your central data center through a simple process. For more information, refer to <u>Installing an Operating System.</u>

The following section presents the main requirements and supported process for successfully installing the Cohesity ISO file through the Cisco Intersight Install Operating System feature. Cisco Intersight provides several options for installing the OS. For more information, refer to <u>Operating System Installation Guide.</u>

Note: To use the Install Operating System feature through the Cisco Intersight platform, you must have at least a Cisco Intersight Advantage license. For other Cisco Intersight license tiers, refer to Cisco Intersight Licensing Requirements.

Follow the high-level procedure presented here to install a Cohesity ISO file on Cisco UCS C220 and C240 Rack Servers:

- 1. Add the OS Image Link option in the Cisco Intersight Software Repository:
 - Log in to the Cisco Intersight platform at https://intersight.com/.
 - Navigate to Admin > Software Repository and select the OS Image Link tab.
 - Click the Add OS Image Link option in the top-right corner.

≡	cisco Intersigh	t A	ADMIN > Software Repository			다. 🖬 19 🔺 5 🖂 📢 1 오, 🤃 🕜 Anil Dhiman 요						
×			irmware Links OS Image Links		Add OS Image Link							
			🗓 🖉 🖉 🛛 🔍 _Add F	ilter		C Export 2 items found 10 v per page K < of 1 > > 🔅						
	Profiles							Last Update 🗧 🧳				
	Templates			CentOS	CentOS 7.9	http://10.29.149.95//cohes		May 26, 2021 3:42 PM ····				
				CentOS	CentOS 7.9	10.29.149.95/downloads/r		Mar 31, 2021 11:51 AM •••				
								মের 1 of1 সি সা				
		^										
ē	ADMIN	<u>^</u>										
	Targets											
	Software Repository											

 You can select Network File System (NFS), HTTP/S, or Common Internet File System (CIFS) to use to provide the location of the Cohesity ISO file to the Cisco Intersight Software Repository. This location will be accessed during OS installation. Click Next.

=	cisco Intersight	ADMIN > OS Image Links > Add	다. 🖸 19 🔺 5 🔽 📢 1 🔍 😳 🕜 Anil Dhiman 요
×		존 Progress	Step 1
	Orchestration	General	Specify the Operating System source to be used during the installation process.
	Profiles	2 Details	
	Templates		Organization *
	Policies		default <u>v</u>
	Pools		NFS CIFS HTTP/S
2	OPTIMIZE ^		File Location *
	Overview		9.95//cohesity-6.6.0a_release-20210209_d747dfca-centos.iso [©]
	Plan		
	Placement		Username 0
	More		
ē	ADMIN ^		Password
	Targets		
	Software Repository		
			Next >

 Add a name and specify CentOS as the vendor and Version 7.9. Click Add. This step will allow access to the Cohesity ISO file during OS installation.

≡	cisco Intersight	ADMIN > OS Image Links > Add	다 🖬 19 🛦 5 🖂 🥰 1 억, 🤃 💮 Anil Dhiman 🕰
×		⊡ Progress	Step 2
		General	Details Review Operating System image details, modify as required and save the Operating System image
		2 Details	
			Name *
			Cohesity 6.6 HTTP ISO O
Ł			CentOS CentOS CentOS 7.9
	Overview		
			Set Tags Description
Ō	ADMIN ^		
	Targets		
	Software Repository		
		< Back (ancel

- 2. Install the Cohesity operating system. Verify that the Cisco Intersight license tier is set to at least the Advantage tier.
- Log in to the Cisco Intersight platform at https://intersight.com/.
- Navigate to Operate > Servers and select the Cohesity nodes.
- Select the Install Operating System option.

≡	cisco Intersight						
<u>60o</u>	MONITOR	Health Power	HCL Status Models	Contract Status			
P	OPERATE ^	11 Critical 7	Incomplete 11	C220 MSL 6 C240 MSL 3	Failed 1 Out of Sync 1 Not Area		
	Servers				• OK 4		
	01						
	Chassis	••• 🖉 9, Add Filter					
							Upgrade Firmware
			Critical INot Covered	172.25.178 HXAF220C 50.4	384.0	HXEDge-2n 🗸	
			Healthy Not Covered	172.25 J HXAF2200 50.4	384.0	HXEDae-2n	
×	CONFIGURE ^						
	Orchestration		Healthy Not Covered	10.29.149 UCSC-C240 83.2		org-root/org-c	
	Drafilas		Healthy Not Covered				
			Healthy Not Covered				
	Templates		Critical Not Covered	10.41.2.131 UCSC-C220 22.8			
	Pools	C220-WZP24440A6Z		10.29.149.34 UCSC-C220 44.0			
⊵		C220.W7D24440475		10 20 140 25 1050,0220 44 0			
	Plan	C220-WZP24440A7F	Critical Not Covered	10.29.149.36 UCSC-C220 44.0	64.0	Cohesity 🥝	4.1(2a) ····

• Verify that all the nodes are selected. Click Next.

OF	PERATE > Servers > Instal	l Operating System				Q 🛛	19 🔺 5 🛛 🖓	ମ୍ଟୋ ଦ୍ 🗇	ි Anil Dhiman යූ
	Progress				Sel ins	ect the servers for the Operati allation	ng System		
1			Select	Servers					
	Operating System			Add Filter					
	Configuration								
	Server Configuration Utility			C220-WZP22440AZC			HXAF220C-M5SX	WZP22440AZC	
	Installation Target			C220-WZP22440AX5		Healthy	HXAF220C-M5SX	WZP22440AX5	
	Summary			C25-FI6454-1		Healthy	UCSC-C240-M5L	WZP22270066	
				C25-FI6454-2		Healthy	UCSC-C240-M5L	WZP2227005E	
				C25-FI6454-3		Healthy	UCSC-C240-M5L	WZP2227005C	
				C220-WZP233414DG			UCSC-C220-M5L	WZP233414DG	
				C220-WZP24130MEV	Cohesity ROBO	Critical	UCSC-C220-M5L	WZP24130MEV	
				C220-WZP24440A6Z			UCSC-C220-M5L	WZP24440A6Z	
				C220-WZP24440A75			UCSC-C220-M5L	WZP24440A75	
				C220-WZP24440A7F			UCSC-C220-M5L	WZP24440A7F	
									Next >

• Select the OS image link created in the previous workflow. Click Next.

cisco intersignt	OPERATE 7 Servers 7 Install Operating System			Anii Dhiman 🔬
	드 Progress	Step 2		
	1 General	Operating Sys	tem System from the list or add a	
Servers Chassis	Operating System	new image to the rep		
	3 Configuration	Select Operating System Image		
	4 Server Configuration Utility			
	5 Installation Target			
	6 Summary	 Selected servers belong to multiple common organizations: default, 'org-con the common organizations. Learn more at Help Center. 	esity'. You can choose to install Operating System from one of	
		V Add Filter 2 item	nstound 10 v perpage ℝ < 1 of 1 > >	
Templates				
		Cohesity HTTP ISO http://10.29.149.95//cohe CentOS	CentOS 7.9	
Pools		Selected 1 of 2 Show Selected Linselect All		
More	< Back Cancel			Next >

• Select the Embedded tab and click Next.

OPERATE > Servers > Install Operating System		💭 🔳 19 🛕 5	ା <u>ଜ</u> ାସ୍ଟା ସ୍କ	3 🔿 Anil Dhimar
🔄 Progress	~~~~	Step 3		
1 General		Configuration Select a configuration source and provide the necessary configuration parameters		
2 Operating System				
3 Configuration	Select Configuration Source			
4 Server Configuration Utility	Cisco	Custom	Embedded	
5 Installation Target	Operating System image must include a configuratio	n file. For an example of the configuration file, see He	elp Center.	
6 Summary				
K Cancel				Next >

- On the Server Configuration Utility screen, click Next.
- On the Select Installation Target screen, click Next. The Cohesity ISO file will automatically identify the M.2 drives to install the Cohesity operating system.

≡	cisco Intersight	OPERATE > Servers > Install Operating System	우 🖬 19 🔺 5 🛛 🖓 🗘	
<u>00</u> 0		⊡ Progress	Step 5	
Ŷ	OPERATE ^	1 General	Installation Target	
		Uperating System	Select Installation Target	
		(3) Configuration		
		4 Server Configuration Utility	 The configuration file of the selected operating system image must include the installation targets provided. Find examples and learn more about embedded configuration feature at Help Center. 	
	Kubernetes	Installation Target		
×	CONFIGURE ^	6 Summary		
	Pools			
Ľ	OPTIMIZE ^			
	More	< Back Cancel		Next >

• Verify the Cohesity nodes and Cohesity ISO target repository and click Install. Confirm the process in the warning window and click Install.

OPERATE > Servers > Install Operating System		Q 🖪 19 🔺 5 🛛 🔀	약다 1 🔍 🛞 ⑦ Anil Dhiman 요				
⊂ Progress	47	Step 6					
() General	Ŭ≣.	Summary Verify details of your selections, make changes where required and proceed to install the Operating					
2 Operating System		System					
3 Configuration	Selected Servers						
4 Server Configuration Utility	ရှိ Add Filter	3 items found 10 🗸 per page 🗹 🔇	1 of 1 🗵 🗵				
5 Installation Target	Name User Label	Health Model	Serial Number 🗧				
Summary	C220-WZP24440A6Z	Critical UCSC-C220-M5L	WZP24440A6Z				
	C220-WZP24440A75	Critical UCSC-C220-M5L	WZP24440A75				
	C220-WZP24440A7F	Critical UCSC-C220-M5L	WZP24440A7F				
			K C 1 of 1 > >				
	Operating System Image						
	Name Cohesity 6.6 HTTP ISO Vendor CentOS	Version CentOS 7	9				
	Configuration						
	Configuration Source Embedded						
K Back Cancel			Install				

• Verify the status of OS installation in the Progress window..

Health Power HCL 11 • Critical 7 • Healt. 4 00 ff 5	Status Models Contract Status Server Profiles Requests (11 * C120 MS, 6 * C120 MS, 3 * IOM/2200 M, 2 Contract Status Server Profiles Contract Status Server Profiles (* Server Profiles (* Status 1 * S					
	Install Operating System In Progress C220-W2P24440A7F a minute ago					
••• 🖉 9. Add Filter						
Requests > Install Operating System > Operating	System Install on Standalone Server 🗘 🖪 19 🛦 5 🔿 2 🛛 🕫 🖉 💮 Anil Dhirman 🧟					
Details	Execution Flow					
	Progress					
Name Operating System Install on Standalone Serve	r O Confirm Virtual Media Mapping					
ID 60b9206e696f6e2d3055ec0 Target Type Rack Serve	Oreate New Virtual Media Mapping Jun 9, 2021 11:33 AM Virtual media mapping created Jun 9, 2021 11:33 AM					
	r 💿 Validate Virtual Media Mapping Jun 3, 2021 11.33 AM					
Source Type Rack Serve						
Source Name C220-WZP24440A6	O Prepare Operating System Install Configuration Jun 3, 2021 11:33 AM Configuration file is prepared for Operating System: CentIOS 7.9, Configuration Source: Embedded					
Start Time Jun 3, 2021 11:33 AN	Configuration Jun 3, 2021 11:33 AM Configuration					
Duration 1 m 56 :	Oranfirm Secure Boot Configuration Jun 3, 2021 11:33 AM Secure Boot Configuration validated					
	t O Perform Scoped Inventory Jun 3, 2021 11:33 AM State synchronized.					

• Monitor the progress of the Cohesity ISO file installation through a virtual KVM (vKVM) session.

111111111111111111111111111111111111				
The Year Marces Tots Power Watardies Help: Image: Statistics configuration (Capital Marted States)) 10 Installation source (Capital Marted States)) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Installation source (Capital Marted States) 10 Ins	dialla cisco Intersight C220-WZP24440A6Z vKVM			Anil Dhiman 🚨
1) for Language strings (fullish (United States)) 2) for Time strings (fullish (United States)) 3) (a) Installation source (darming checking storage configuration) 2) for Time strings (fuer case case case case case case case case	File View Macros Tools Power Virtual Media Help		A 1 5	cisco UCS KVM
Creating ext4 on /dev/md/root Creating mdmember on /dev/sdh2	Fib Yew Macros Tools Power Vitual Media Help Installation 1) (x) Language settings (Feg) ib (United Stores)) 3) (x) United into Source (Local media) 5) (x) Installation Destination (Warning checking storage contiguration) 7) (1) Network configuration (Warning checking storage configuration) 7) (1) Network configuration (Warning checking storage configuration) 7) (1) Network configuration (Warning adverse) 7) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	 2) [x] Time settings (formite./us_ingples timezone) 1) [x] Software selection (Custom software selected) 6) [x] Kümg (Kümg) (Kümg) (seabled) 8) [1] User creation (No user will be created) 		diado UCS KVM
creating ext3 on /dev/md/boot	Greating minember on /dev/adhi Creating ext4 on /dev/ad/root Creating ext4 on /dev/adh/ Creating ext3 on /dev/ad/boot			

Verify that the Cohesity OS was installed successfully.

File	View	Macros	Tools	Power	Virtual Media Help
					Cohesity Version: 6.6.8a_release-28218209_d747dfca Product Name: UCS-C220H5H4 Hostname: chassis-wzp24440a7f-node-1 Node IPv4: Node IPv4: Link Local IPv4: 169.254.4.223 Link Local IPv6: fe00::e826:60ff:fed5:234c FOR LOCAL ACCESS, PLEASE CONNECT TO THE SAME SWITCH AS THE NODE AND USE THE LINK LOCAL IP ADDRESS. ENTER THE IP IN YOUR BROWSER TO ACCESS THE COHESITY UI.
					chassis-wzp24440a7f-node-1 login: [813.659190] kvm [149829]: vcpu0 disabled perfctr wrmsr: 0xc2 data 0xffff
					Cohesity Version: 6.6.8a_release-28218289_d747dfca Product Name: UCS-C220F5H4 Hostname: chassis-wzp24448a7f-node-1 Node IPv4: Node IPv6: Link Local IPv4: 169.254.4.223 Link Local IPv6: fe88::c826:68ff:fed5:234c
					FOR LOCAL ACCESS, PLEASE CONNECT TO THE SAME SWITCH AS THE NODE AND USE THE LINK LOCAL IP ADDRESS. ENTER THE IP IN YOUR BROWSER TO ACCESS THE COHESITY UI.
					chassis-wzp24440a7f-node-1 login:

- After Cohesity OS installation through the Cisco Intersight platform, the server profiles become out
 of sync. This loss of synchronization occurs because of the configuration of the one-time boot order
 to install the operating system.
 - Go to Configure > Profiles.
 - Select the out-of-sync profiles and click Deploy.

_		_						
≡	cisco Intersight		CONFI	IGURE > Profiles				û 🖬 19 🔺 5 ○ 1 🕵 1
<u>00o</u>	MONITOR		Нур	perFlex Cluster Profiles UCS Chassis Pro	ofiles UCS Domain Profiles UCS Serv	er Profiles Kubernetes Cluster Profiles		
Ŵ								
	Servers			Add Filter				Export 9 items found 18
	Chassis		Dep	pioy :			UCS Server Template	Server
	Fabric Interconnects		Una	assign Server ar-Template-1_C240-DERIV_	O OK	UCS Server (Standalone)		C240-WZP2227005W
	HyperFlex Clusters					UCS Server (Standalone)		C220-WZP24440A7F
	Kubernetes				Dut of Sync	UCS Server (Standalone)		C220-WZP24440A75
×	CONFIGURE ^	l			Out of Sync	UCS Server (Standalone)		C220-WZP24440A6Z
	Orchestration				© OK	UCS Server (Standalone)		C220-WZP24440A6V
(Profiles				E Failed	UCS Server (Standalone)		C220-WZP233414DG
	Templates				Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV
	Policies				2 Not Assigned	UCS Server (Standalone)		
	Pools				Not Assigned	UCS Server (Standalone)		
Ł				🖉 🖑 📋 Selected 3 of 9 Show				

• Confirm that the server profiles are in the OK state.

=	disco Intersight			GURE > Profiles						
<u>00o</u>						Server Profiles Kubernetes Cluster Pr			Create UCS Server	Profile
ø		Г								
		··· / / D D A Add Filter								۲
		L			Status :					
		ľ			O OK	UCS Server (Standalone)			a few seconds ago	
		П				UCS Server (Standalone)				
		L			ID OK	UCS Server (Standalone)			2 minutes ago	
×					⊜ OK	UCS Server (Standalone)			11 minutes ago	
	Orchestration	1			O OK	UCS Server (Standalone)				
						UCS Server (Standalone)			May 21, 2021 12:10 PM	
	Templates	L			Dut of Sync	UCS Server (Standalone)				
		L			Not Assigned	UCS Server (Standalone)				
		I			I Not Assigned	UCS Server (Standalone)				
R	OPTIMIZE ^	L	***	100					K (of 1	চাহ

• After the OS image installation succeeds, proceed to configuration of the Cohesity cluster.

Install the OS through vMedia and one-time boot device

Installation of the Cohesity ISO file through the one-time boot device feature requires customers to attach a vMedia policy for the Cohesity ISO file and install the Cohesity operating system. This process can be achieved by editing the boot-order policy and attaching the vMedia policy in the one-time boot device feature on the Cisco Intersight platform. Any user inputs during the installation process can be entered through the vKVM session.

These are some of the main steps to install the Cohesity OS through the Cisco Intersight one-time boot feature:

- Extend the vKVM timeout setting.
- Create and attach a new vMedia policy to the server profile template.
- Power the server off and on and assign the vMedia as the one-time boot device.
- Remove the vMedia configuration from the server profile template.

Note: Installation of the Cohesity operation system through the one-time boot device feature requires at least a Cisco Intersight Essential license.

Extending vKVM timeout

The Cohesity OS installation takes around 30 to 40 minutes, and thus it is important to increase the Cisco Intersight vKVM idle timeout value. To increase the Cisco Intersight idle timeout value, follow these steps:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Click the gear icon in the top-right corner and select Settings.
- 3. In the Account Details section, click Configure.

	cisco	Intersight	Settings	Q 🛛 19 🔺 5 🛛 🗹	📢 1 🔍 🕄 🕜 Anil Dhiman 🖉
<u>00o</u>	MONITOR		ⓒ3 general	Account Details	Configure
	OPERATE		Account Details		
	Servers		Access Details	Account Name	andhiman
	Chassis		န္တြ authentication	Account ID	5d1cf7a87564612d30f05a40
	Cabria Inter		Single Sign-On	Access Link	https://5d1cf7a87564612d30f05a40.intersight.com/

4. On the Configure Account Settings screen, change the default idle timeout value to 4000 seconds and click Save.

Set default values for Idl Concurrent Sessions set default settings during r	le Timeout, Session Timeout, and ttings. The values will be used as the ole creation.
Account Name *	
andhiman	
vood) ମିର
4000	200_18000
	300 - 18000
Default Session Timeout (Secc	onds)
57600	<u> </u>
	300 - 31536000
Mavimum Canaurrant Cassian	
	s per User (Sessions)
52	
	2 - 32
Cat Taga	

Creating and attaching a new vMedia policy to the server profile template

Follow these steps to create and attach a new vMedia policy to the server profile template:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Configure > Policies and click Create Policy.
- 3. For Platform Type, select UCS Server, and for Policy Type, select Virtual Media. Then click Start.

_						
=	cisco Intersight					
<u>a0</u> =						
ŵ			Select Policy Type			
	Servers					
	Chassis	Filters				
	Eshric Interrogenerts					
	HyperHex Clusters	UCS Server				
×	CONFIGURE ^	UCS Domain				
		HyperFlex Cluster				
	Templates					
ſ						
	Pools					
12	OPTIMIZE A					
	0					
	Overview					
Geo						
						Start

4. For Organization, select org-cohesity, and for the policy name, enter **vMedia-OS-Install**. Then click Next.

≡	cisco Intersight	CONFIGURE > Policies > Virtual Media > Create	다 🖬 19 🛦 5 🛛 🖓 📢 1 🔤 오, 🏷 💮 🖉 Anil Dhiman 요
<u>allo</u>		⊂ Progress	Step 1
ø			General
	Servers		Add a name, description and tag for the policy.
	Chassis	2 Policy Details	
	Fabric Interconnects		org-cohesity <u>v</u>
	HyperFlex Clusters		
×			vMedia-OS-Install
	Orchestration		
	Profiles		Set Tags
	Templates		
	Pools		
Ľ	OPTIMIZE ^		
	Overview		
	Plan		
	Placement		
	More		
ē	ADMIN ^		
	Targets		
	Software Repository		
		Cancel	Next >

- 5. Leave the configuration at the default settings and click Add Virtual Media.
- 6. On the Add Virtual Media screen, add the mount points of the Cohesity ISO file on the NFS, HTTP/HTTPS, or CIFS server. Click Add.

CONFIGURE > Policies > Virtual N	edia > Create			
1 General 2 Policy Details	Add Vii Virtual Me	rtual Media dia Type ⊙ ◯ HDD		
	Name * Cohesity	NFS	CIFS	HTTP/HTTPS
	File Locati ttp://10.2 Mount Q	on* 19.149.95//cohesity ptions	-6.6.0a_release-20	210209_d747dfca-centos.iso ©
	Usernam	e		
	Password	d		<u>@ 0</u>
				Cancel

7. Click Create to create the new vMedia policy.

≡	cisco Intersight	CONFIGURE > Policies > Virtual Media > Create		Q 🖬 19 🔺	େ 🛛 🖓 । କ୍	😧 💿 Anil Dhiman 🛓	
<u>allo</u>		🖂 Progress		Step 2			
ø	OPERATE ^	C Control	(O)	Policy Details			
	Servers		~~ କୁଡ଼	Aod porcy details			
	Chassis	Policy Details		All Platforms UCS Server			
	Fabric Interconnects		Configuration				
	HyperFlex Clusters		Contraction				
×	CONFIGURE ^		Cnable Virtual Media O				
	Orchestration		○ Enable Virtual Media Encryption ⊙				
	Profiles		Contraction In the second seco				
	Templates		Add Virtual Media				
	Policies			1 items found 10 v per page	হারি t of1 স সি 🔞		
	Pools						
Ľ	OPTIMIZE ^		CohesityISO CDD	HTTP/HTTPS	http://10.29.149.95//cohesit		
	Overview						
	Plan						
	Placement						
	More						
ģ	ADMIN ^						
	Targets						
	Software Repository						
		Cancel				Create	

- 8. After the vMedia policy has been created, edit the server profile template to add the new vMedia policy.
- 9. Navigate to Configure > Templates and select Cohesity-Server-Template-1. This server profile template was used to derive all the server profiles attached to Cohesity nodes.

	ماليتان المعمدتين			0	D 41	0 0	
_	cisco intersignt	CONFIGURE / Templates		φ μ Ιν Δ. ν	□ 41 1		
<u>01o</u>		UCS Server Profile Templates				Create U	CS Server Profile Template
	Servers	🖉 🖉 📋 🛛 🤤 Add Filter				10 🗸 per page 📧 🗉	
	Chassis						
	Fabric Interconnects		UCS Server (Standalone)				
	HyperFlex Clusters		UCS Server (Standalone)				
×	CONFIGURE						
	Orchestration						
	Profiles						
C							
	Policies						
	Pools						

10. From Actions in the top-right corner, select Edit.

≡ ^{-i i-i i-} Intersight		emplate-1	
			Actions v
© OPERATE ^	Details	Configuration	Edit
Servers	Name Cohesity-Sever-Template-1	Configuration Usage	
Chassis	Target Platform UCS Server (Standalone)		
	Last Update an hour ago	Compute	
Fabric Interconnects	Description	BIOS	oh-bios-config 📳
HyperFlex Clusters		Boot Order	ot-order-policy 🗐
🗶 CONFIGURE 🔷			
Orchestration	Taos Set	Management	
Desfine		IPMI Over LAN	over-lan-policy በ
Profiles		Serial Over LAN	serial-over-lan 🗐
Templates			

11. Click Next. On the Compute Configuration screen, select Virtual Media and click Select Policy.

≡	ະເທດ Intersight	CONFIGURE > Edit UCS Server Profile Template (Cohesity-Sever-Template-1)						
<u>00</u> 0		⊡ Progress				Step 2		
Ŷ		General			ξ Ο μ	Compute Configuration		
					~~~~	want to associate with this template.		
		2 Compute Configuration		Show Attached Policies				
		3 Management Configuration			-,			
		4 Storage Configuration		BIOS			coh-bios-con	fig 🗐
×	CONFIGURE ^	5 Network Configuration		Boot Order			coh-boot-order-poli	icy 📋
	Orchestration	Summary		Persistent Memory				
		o summery		Virtual Media				
	Templates							
	Policies							
	Policies Pools							

12. Select the vMedia-OS-Install policy created in the previous section.

CONFIGURE > Edit UCS Server Profile	Template (Cohesity-Sever-Template-1)	Q 🖪 19 🔺 5 🛛 [		
			Virtual Media	
1 General	the second s	Compute Configuration Create or select existing Compute policies that you	Policies 1	
	. ಆಗ್	want to associate with this template.		
2 Compute Configuration				
3 Management Configuration	Show Attached Policies (2)			
Storage Configuration				
	Boot Order			
5 Network Configuration	Persistent Memory			
6 Summary	Virtual Media			

13. Click Close. The server profile template will be configured with the vMedia policy.

=	cisco Intersight	CONFIGURE > Edit UCS Server Profile Template (Cohesity-Sever-Templa	s-1)	🗘 🖪 19 🛦 S		හි 🕜 Anil Dhiman 🚊
000		≅ Progress		Step 2		
ø			(O)	Compute Configuration		
			~ <b>~</b> \$\$	create or select existing compute policies that you want to associate with this template.		
		2 Compute Configuration	Charao Materia de Destadore (73)			
		3 Management Configuration	Show Atlacted Policies (3)			
		4 Storage Configuration	BIOS		coh-bios-config	
×		5 Network Configuration	Boot Order		coh-boot-order-policy	
		6 Summary	Persistent Memory			
			Virtual Media		vMedia-OS-Install	
	Templates					
Ŀ						
٩						
		< Back Close				Next >

14. Navigate to Configure > Profiles and verify that the server profiles deployed on Cohesity nodes have a status of Not Deployed Changes.

≡	cisco Intersight		CONFIGURE > Profiles								
<u>tilo</u>					iles UCS Domain Profiles UCS S	erver Profiles Kubernetes Cluster Profil			Create UCS Server	Profile	
ø											
		P 🖉 🖹   Q. Add Filter [ ] C Export 9 Items Sound   16 per page 🔣 C 1 of 1 2									
					A Not Deployed Changes	UCS Server (Standalone)					
					Not Deployed Changes	UCS Server (Standalone)					
X	CONFIGURE ^				Not Deployed Changes	UCS Server (Standalone)			a few seconds ago		
	Orchestration				A Not Deployed Changes	UCS Server (Standalone)			a few seconds ago		
ſ	Profiles				A Not Deployed Changes	UCS Server (Standalone)			a few seconds ago		
	Templates				E Faled	UCS Server (Standalone)			May 21, 2021 12:10 PM		
	Policies				Out of Sync	UCS Server (Standalone)			May 21, 2021 7:19 AM		
					I Not Assigned	UCS Server (Standalone)					
L2					I Not Assigned	UCS Server (Standalone)					
	Overview	2	1	Ø 1					<u>र ा</u> जग	হ স	

15. Select the Cohesity server profiles, Click the Options icon (...) and select Deploy. This action will deploy the vMedia changes to the Cohesity server profiles.

≡	cisco Intersight			rofiles				🖬 19 🔺 5 📝 🛛 🥵 1		iman ¿	
<u>00a</u>			HyperFer Cluster Profiles UCS Chassis Profiles UCS Samain Profiles UCS Samer Profiles Cluster Profiles Cluster Profiles CCS Gaves Prof								
ø											
			• / / 1	Add Filter				per page K < 1 of 1 > >	۲		
										Ş	
			Inassign Server								
		$\left  \right $									
×					A Not Deployed Changes	UCS Server (Standalone)			a few seconds ago		
		IL									
					E Failed	UCS Server (Standalone)			May 21, 2021 12:10 PM		
					Out of Sync	UCS Server (Standalone)			May 21, 2021 7:19 AM		
					Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM		
Ŀ					E Not Assigned	UCS Server (Standalone)					
										N	

16. Confirm the Deploy Alert message and verify that the changes have been deployed to the Cohesity nodes. The status changes from Validating to OK.

	1										
=	disco Intersight		Contribute > Profiles Q 😨 19 🔺 S 😰 👘 1 1 🔍 📀 💿 Ani Dhiman 🖇								
<u>ello</u>		I				erver Profiles Kubernetes Cluster Profi			Create UCS Server P	rofile	
ø		Г									
		/ / 🖉 📋 🔍 Add Filter 🕴 🕴 🕹 👘 🖓 Add Filter									
×											
	Orchestration	l				UCS Server (Standalone)					
					A Not Deployed Changes	UCS Server (Standalone)			10 minutes ago		
					Failed	UCS Server (Standalone)					
		L				UCS Server (Standalone)					
		L			🕄 Not Assigned	UCS Server (Standalone)					
P					I Not Assigned	UCS Server (Standalone)					
	Overview			🖉 🖉 📋 Selected 4 of 9 Show	Selected Unselect All				区 <u>1</u> of 1 [		

#### Installing the Cohesity OS through one-time boot device

Follow these steps to install the Cohesity operating system through the one-time boot device feature:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Servers. Select the Cohesity node on which to install the Cohesity OS.
- 3. Click the Options icon (...) at the right end of the server pane and select Power Cycle.

NUMBE       Normal State       Normal	cisco Intersight	OPERATE > Servers					■19 A 5 🕑 q4 1 Q	🕄 💿 Anil Dhiman 🔔		
All dist         Per dist         Mode         Control time	MONITOR									
Barren         (2)         : Statu / I         (2)         : Statu / I <th< td=""><td>OPERATE ^</td><td>Health Power</td><td>HCL Status Models</td><td></td><td>Contract Status Not Covered 12</td><td>Server Profiles</td><td>Requests (Last 24h)</td><td>Power Off</td></th<>	OPERATE ^	Health Power	HCL Status Models		Contract Status Not Covered 12	Server Profiles	Requests (Last 24h)	Power Off		
Constant         Image: Constant </td <td>Servers</td> <td>(12) • Criscal 7 • Heak_ 5 00 10</td> <td></td> <td><ul> <li>C220 MSL 6</li> <li>C240 MSL 4</li> <li>HXAF220C M. 2</li> </ul></td> <td></td> <td>9 Not Deployed Cha., 1 9 Out of Spice 1 9 Not Assigned 2</td> <td>(27) * Completed 25 Field 2</td> <td>Power Cycle</td>	Servers	(12) • Criscal 7 • Heak_ 5 00 10		<ul> <li>C220 MSL 6</li> <li>C240 MSL 4</li> <li>HXAF220C M. 2</li> </ul>		9 Not Deployed Cha., 1 9 Out of Spice 1 9 Not Assigned 2	(27) * Completed 25 Field 2	Power Cycle		
Add file <ul> <li></li></ul>	Chassis									
Normal         Normal<	Fabric Interconnects									
$ \begin{array}{                                    $	HyperFlex Clusters		Handha I. Caralana Ciatan			1100 Description		Shut Down Operating System		
<ul> <li></li></ul>	CONFIGURE		Heatin Contract Status	Manage. N		. Memory	HA GUDDET SETVET PT	Ubitty Stora Tum Off Locator		
0       0       0.000044000000000000000000000000000000	Contraction (		Critical Rot Covered	172.25.178.201 H	HXAF220C-M5_	50.4 384.0	HAEUge-2000_	Unorade Firmware		
Notice         O         C25146651         O         Distance         1231431         USC C264.0         B22         TB18         C556664         Opposite         Opposite         Instrument         Instrument <th< td=""><td></td><td></td><td>Heatiny     Not Covered</td><td>172.25.178.202 H</td><td>HXAF220C-M5</td><td>50.4 384.0</td><td>HXEDge-2nod_</td><td>Import Server Profile</td></th<>			Heatiny     Not Covered	172.25.178.202 H	HXAF220C-M5	50.4 384.0	HXEDge-2nod_	Import Server Profile		
Timestam         O         C2545852         Dietain         BietOmment         1031011         USCC20640.         822         7136         C556056         opport/opport         Linext-NN           Publics         O         C25468523         BietBitty         BietOmment         1231015         USCC20640.         822         7136         C556056         opport/opport         Linext-NN	Profiles		Healthy     Not Covered	10.29.149.14 U	UCSC-C240-M	83.2 128.0 C25-Fi6454	org-root/org-coh	Launch IMC		
Noise       © C5756633       © Methowed       1221015       UCC C2640.       B32       138       C576644       opport/opport       Description         Nois       © C256972334420       BCMiel       Methowed       1421131       UCC C2640.       B22       148       Columb C III       opport/opport       opport/o	Templates		Healthy     Not Covered	10.29.149.15 U	UCSC-C240-M_	83.2 128.0 C25-R6454	org-root/org-coh	Launch vKVM		
Prob         Construct         Red Kneet         16.412111         UCG CC294U,         2.28         4.48         Construct         gen RAC Case           OPTIMAZE         C         CC29647724153011400         RE Official         Red Kneet         16.21121         UCG CC294U,         2.38         4.48         Construct C         gen RAC Case         gen R			Healthy Kot Covered	10.29.149.16 U	UCSC-C240-M_	83.2 128.0 C25-F16454	org-root/org-coh	Lauren Terrated elCML e.		
OPTIMAZE         Image: Construct status			Critical R Not Covered	10.41.2.131 U	UCSC-C220-M_	22.8 64.0		Open TAC Case		
Openniew         College // 2019/07/44464/22         College // 446         College // 448			Critical E Not Covered	10.29.149.248 U	UCSC-C220-M_	33.6 64.0		Set License Tier		
Plan         C C20 M77 24448/35         E Chical         Imbit Normal         10.27 19.33         CCCC25M.         440         643         C Calmb 16 (0)         Set Upr 1.001           Pacement         0         C C20 M77 24448/37         E Chical         Imbit Normal         10.27 19.33         UCC C25M.         440         440         C calmb 16 (0)         410(1)			Critical Not Covered	10.29.149.34 U	UCSC-C220-M_	44.0 64.0		Set Asset Tags		
Placement         © C205/8779446607         © Ottes/         % Percent         15.2319.33         UCDCC25ML         44.0         64.8         Colemity 56.0         41(pc)            abre         0 C205/8779446667         © Ottes/         % Percent         15.2319.37         UCDCC25ML         44.0         64.8         Colemity 56.0         41(pc)            abre         0 C205/8779446667         © Ottes/         % Percent         15.2319.37         UCDCC25ML         44.0         64.8         Colemity 56.0         41(pc)            abre         0 C205/8779446667         © MetOwered         15.2319.37         UCDCC25ML         45.0         Colemity 56.0         41(pc)            abre         0 C205/8779446667         © MetOwered         15.2319.37         UCDCC25ML         45.0         Colemity 56.0         41(pc)            abre         0 C205/8779446667         © MetOwered         15.2319.31         UCDCC25ML         55.2         72.80         Colemity 56.0         41(pc)			Critical Not Covered	10.29.149.35 U	UCSC-C220-M_	44.0 64.0		Set User Label		
More         C 0 C209 H775446664//         Is 0 Clickel         Im Not Common         1522 16337         US2C C209 M.         44.0         64.0         Coloning field         410p0            LINEN                    410p0            LINEN	Placement		Critical I Not Covered	10.29.149.36 U	UCSC-C220-M_	44.0 64.0		4.1(3c)		
			Critical S Not Covered	10.29.149.37 U	UCSC-C220-M_	44.0 64.0		4.1(3c)		
			C Heathy R Not Covered	10.29.149.38 U	UCSC-C240-M_	83.2 128.0		4.1(3b)		
	Targets							লি বা পা বলি		

4. On the Power Cycle Server screen, enable One Time Boot Device and select vmedia1 as the boot device.

Power Cycle Se	erver	
Server 'C220-WZP2444	0A7F' will be Power Cycled.	
Set One Time E	loot Device 💿	
Boot Device		
vmedia1		
	Cancel	Power Cycle

- 5. After the server is power cycled, the server will boot through the vMedia mapped to the Cohesity operating system ISO file. This boot will initiate the Cohesity operating system installation process.
- 6. View the operating system installation progress by opening a vKVM session. User Inputs can be entered through the vKVM session.

cisco Intersight C220-WZP24440A7F   vKVM	
File View Macros Tools Power Virtual Media Help	
	Kickstant
	Use the ▲ and ▼ keys to change the selection. Press 'e' to edit the selected item, or 'c' for a command prompt.
	The selected entry will be started automatically in 70s.

7. Repeat steps 1 through 6 to install the Cohesity OS on other nodes.

#### Remove the vMedia configuration from the server profile template

After the operating system is installed, you should remove the vMedia policy from the server profile template. Follow these steps to remove the vMedia policy:

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- Navigate to Configure > Templates and select Cohesity-Server-Template-1, created for Cohesity nodes.
- 3. In the Action drop-down menu in the top-right corner, select Edit.

=	cisco Intersight	CONFIGURE > Templates > Cohesity-Sever-Te	mplate 1	Q 🖬 19 🔺 5	ß	ę\$ 1	٩	•	) Anil Dhiman 🔔
010	MONITOR								Actions v
ø		Details	Configuration						Edit
		Name Cohesity-Sever-Template-1	Configuration Usage						Cione
		Target Platform UCS Server (Standalone)							Delete
	Fabric Interconnects	Last Update Jun 14, 2021 4:59 PM	Compute						Derive Profiles
	Ihren Des Charlese		BIOS						coh-bios-config 🔟
	nypervex clusters		Boot Order					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	h-boot-order-policy 👔
	CONFIGURE ^	Organization org-cohesity	Virtual Media						vmedia-os-install 👔
	Orchestration	Tags Set	Management						
	Profiles								en la constant de la
	Templates							CONT	prinover sampoicy
	Policies		Serial Over LAN						coh-serial-over-lan 🔠
			Network						^
12	OPTIMIZE A		Adapter Configuration						coh-adaptor-config 🕼
-									
	Overview		Storage						^
			Storage						constorage policy
ø									
	Targets								
	Software Repository								

4. Go to the Compute Configuration screen and select the "X" on the policy attached to Virtual Media.

ι.
i i
i i
i i
i i
i i
Next >

5. Confirm that you want to detach the vMedia server policy from the Cohesity server profile template.

Progress			Step 2
General		۲ <b> </b>	Create or select ex want to associate v
		Show Attached Policies (3)	
Network Configuration		Boot Order	
		Persistent Memory	
		Detach Policy	) ×
		Policy "vmedia-os-install" will be detached from profile.	J
		Cancel	lach
	rogress Seneral Compute Configuration Aanagement Configuration Atorage Configuration Active Configuration Active Configuration	rogress seneral compute Configuration Aanagement Configuration storage Configuration storage Configuration storage Configuration	rogress several compute Configuration Aanagement Configuration storage Configuration tetwork Configuration tetwork Configuration Persistent Memory tetwork Configuration Cancel Detach Policy Tymedia-os-install* will be detached from profile. Cancel Detached Four profile. Cancel Detached Four Policy Cancel Deta

6. After the vMedia policy is detached, click Close on the Edit Server Profile Template screen.

≡	cisco Intersight	CONFIGURE > Edit UCS Server Pro	file Template (Cohesity-Sever-Template-1)			۱ 🗖 🗘	9 🔺 5 📄 🖸	3   951	۹ (۵	) Anil Dhiman 🔔
<u>©</u> ₽	MONITOR OPERATE ^	⊡ Progress			~~~ <b>~</b>	Step 2 Compute Configuration				
	Servers Chassis	Compute Configuration				Create or select existing Compute policies that want to associate with this template.	policies Ihat you e.			
	Fabric Interconnects	Management Configuration		Show Attached Policies (2)						
	HyperFlex Clusters	Storage Configuration		BIOS				coh-bios-con		
×	CONFIGURE ^	5 Network Configuration		Boot Order				coh-boot-order-pol	<b>a</b>	
	Orchestration	6 Summary		Victual Modia						
	Profiles									
	Templates									
Ľ										
	Overview									
	Plan									
	More									
(8)	ADMIN 0									
	Targets									
	Software Repository									
			Close							Dws Next >

## **Firmware upgrades**

Firmware upgrades in the Cisco Intersight platform, including infrastructure, server, and chassis firmware upgrades, are supported on the following devices:

- Cisco UCS C-Series and S-Series M4 and M5 servers that are configured in standalone mode.
- Cisco fabric interconnect-attached Cisco UCS B-Series, C-Series, and S3260 M3, M4, and M5 servers.
- Cisco fabric interconnect-attached Cisco UCS S3260 chassis
- Cisco UCS 6200, 6300, and 6400 Series Fabric Interconnects in a Cisco UCS domain

This feature requires a Cisco Intersight Essentials or higher-tier license.

For detailed instructions for performing firmware upgrades, see <u>Firmware Management in Intersight</u> and <u>Upgrading UCS C-Series Standalone Servers Firmware</u>.

Firmware for Cisco UCS C-Series servers deployed with Cohesity DataPlatform can be upgraded as described here for the two main use cases:

- Upgrade Cisco UCS C-Series firmware in combination with software upgrades of Cohesity DataPlatform. Cohesity nondistributive upgrades manage the sequential server reboot, allowing upgrades of Cisco UCS C-Series firmware during a Cohesity software upgrade. Because each node is upgrading sequentially, server firmware updating time will increase by about 25 to 30 minutes per Cohesity node.
- Upgrade Cisco UCS C-Series firmware independent of Cohesity DataPlatform software upgrades. In this process, customers need to manually reboot the server node and verify that the Cohesity node is back online after the server firmware upgrade. Verify that each node is rebooted serially, and that the first node comes back online and joins the Cohesity cluster before initiating a reboot on the second node.

Follow these steps to stage the server firmware on Cisco UCS C-Series nodes deployed for Cohesity DataPlatform. After the server firmware is staged, customers can either start a Cohesity DataPlatform upgrade or manually initiate a node reboot to upgrade the server firmware.

- 1. Log in to the Cisco Intersight platform at https://intersight.com/.
- 2. Navigate to Operate > Servers. Select the Cohesity nodes for server firmware upgrades.

=	cisco Intersight	OPERATE > Servers				Q 🖪 19	▲5 🛛 🖓 📢 1 🔤 Q
000	MONITOR	Health Power	HCL Status	Models	Contract Status	Server Profiles	Requests (Last 24h)
Ŷ		Off 2	Incomplete 12	C220 MSL 6		Failed 1 Out of Sync 1	
	Servers	12 • Healt_ 5 0 0n 10		12 • C240 MSL 4 • HXAF220C M. 2		9 • Not Assig_ 2 • OK 5	NO REQUESTS
te.	Chassis						
ų	Fabric Interconnects	··· 🧷 Q, Add Filter					cport 12 items found 16 ~ per p
í	HyperFlex Clusters	Power On :	Health Contract S		Model : CP ① :		HX Cluster Server P
×	CONFIGURE ^	Power Off			HXAF220C 50.4	384.0	HXEDge-2no
	Orchestration	Power Cycle	Healthy     Not		HXAF220C 50.4	384.0	HXEDge-2no
6	Profiles	Hard Reset	Healthy     Not	Covered 10.29.149.14	UCSC-C240 83.2		org-root/org-co
8	Templates	Shut Down Operating System	Healthy     Healthy	Covered 10.29.149.15	UCSC-C240 83.2		org-root/org-co
0	Policies	Turn On Locator	C Healthy Not		UCSC-C240 83.2		org-root/org-co
ti.	Pools	Turn Off Locator		Covered 10.41.2.131			Cohesity-C 🖬
⊵	OPTIMIZE ^	Install Operating System	Critical	Covered 10.29.149.248			coh_ServerProf
	Overview	Upgrade Firmware					Cohesity-S 🥥
	Plan	Set License Tier					Cohesity-S 🥹
	Placement	🖸 🕐 C220-WZP24440A7F					Cohesity-S 🥹
	More	🖸 🔘 C220-WZP24440A6V					Cohesity-S 🥥
Þ	ADMIN ^	C240-WZP2227005W	O Healthy	Covered 10.29.149.38	UCSC-C240 83.2		Cohesity-S 🥥
	Targets	···· 🧷 Selected 4 of 12 Show Select	d Unselect All				

3. Click the Options icon (...) and select Upgrade Firmware.

- 4. On the Upgrade Firmware screen, click Start.
- 5. Verify that the correct nodes are selected for the firmware upgrade and click Next.

=	Servers > Upgrade Firmware	다 🖬 19 🔺 5 🕞 😝 1 으, 🧿 🕥 Anil Dhiman 🔔
	臣 Progress	5kg 1
DOPERATE ^	General	General Ensure selected servers meet requirements for
Servers		fernivare upgrade.
Chassis		
Fabric Interconnects	3 Summary	Confirm Servers Selection 4 Selected
HyperFlex Clusters		
X CONFIGURE ^		
Orchestration		Name User Label Model Firmware Version Utility Storage
Profiles		C220-WZP24440A6Z UCSC-C220-MSL 4.1(36)
Templates		C220-WZP24440A75 UCSC-C229-MSL 4.1(36)
Policies		C220-W2P24440A7F UCSC-C220-MSL 41(3b)
Pools		C220-WZP2444046y UCSC-C220-MSL 41(36)
		Selected 4 of 4 Show Selected Unselect All (전 1 of 1 ) [전]
Overview		
Plan		
Placement		
More		
وَ admin ^		
Targets		
Software Repository		
	< Back Cancel	Next >

- 6. Select either Cisco Repository or Software Repository for the firmware image.
- 7. In the Cisco Repository, firmware is download to the utility storage. This option requires a 32-GB micro-SD card (UCS-MSD-32G) installed on the server node.
- 8. In the Software Repository, you can add images from NFS-, CIFS-, and HTTP/HTTPS-based network share repositories.
- Select Software Repository for the setup described in this document and click Add Firmware Link. You can enable thee Advanced Mode option to exclude drive and storage firmware. Drive and storage firmware upgrades are enabled by default.

— alala		
cisco Intersight	Servers > Upgrade Firmware	
	🔄 Progress	
📦 OPERATE 🛛 ^	General	Version Version
Servers		
Chassis	Version	
Fabric Interconnects	3 Summary	Select Firmware Bundle Advanced Mode 💽
HyperFlex Clusters		Cisco Repository Software Repository
Orchestration		Select the firmware bundle to upgrade. All the server components will be upgraded along with drives and storage controllers. Use Advanced Mode to exclude upgrade of drives and storage controllers.
Profiles		Exclude Drives
Templates		Exclude Storage Controllers
Policies		Add Firmware Link
Pools		
		QAdd Filter 1 items found 10 ✓ per page 문 < of 1 > >  ③
Overview		
Plan		Ucs-c220m5-huu-4.1.3b.iso         4.1(3b)         UCSC-C220 MSSX(5)         http://10.29.149.95/ucs-c220m5-huu-4.1.3b.iso         Image: Control of the second secon
Placement		

10. Add the location of the Cisco UCS C-Series Host Upgrade Utility (HUU). Click Next and then click Add.



11. On the Select Firmware Link screen, select the appropriate firmware for upgrade and click Next.

=	cisco Intersight	Servers > Upgrade Firmware	Q 🖬 19 🛦 5 🛛 🛛 😝 1 🔍 🔗 💮 🗍 Ani	Dhiman 🔔
<u>00</u> 0		든 Progress	5vp 2	
Ø	OPERATE ^	(1) General	Select a firmware version to upgrade the servers to.	
		🙁 Version		
		3 Summary	Select Firmware Bundle 🔹 Advanced Mode 🌑	
	HyperFlex Clusters		Cisco Repository Software Repository	
×	CONFIGURE ^		Select the firmware bundle to upgrade. All the server components will be upgraded along with drives and storage controllers. Use Advanced Mode to exclude	
			upgrade of drives and storage controllers.	
			Exclude Drives	
	Templates		Exclude Storage Controllers	
	Policies			
Ľ	OPTIMIZE ^		역, Add Filter 2 Items found 10 ~ per page 또 또 1 of 1 2 20 🗿	
	Overview			
			● ucs+c220m5+uu+4.1.3c.iso 4.1(3c) UCSC-C220-MSSX,(5) http://10.29.149.95/ucs+c220m5+uu+4.1.3c.iso ④	
			Uss-c220m5/hur-41.3b.iso         41(3b)         UCS0-C2204MSSX,(5)         http://10.29.149.95/uss-c220m5/hur-41.3b.iso         ©	
ģ				
	Targets			
		Ca		0

12. Confirm the firmware to be upgraded and click Upgrade.

=	cisco Intersight	Servers > Upgrade Firmware						🗘 🔳 19 🔺 5				Anil Dhiman 🔔
<u>00</u> 0		🖂 Progress					Step 3					
ø		Coneral					Summary					
		U Veneral				Ľ≡.Į	Contirm contiguration and inn	liate the upgrade.				
		Version										
		Summary	Firmv	vare								
×			Name	e uc	s-c220m5-huu-4.1.3c			age Controllers				
			Serve	ers to be Upgraded								
				me	: User Labe		Model :					
							UCSC-C220-M5L	4.1(3b)				
	Pools						UCSC-C220-M5L					
$\succeq$	OPTIMIZE ^						UCSC-C220-M5L					
							UCSC-C220-M5L					
(P)												
	Software Repository	C Back									-	Upprade
												obstance.

13. On the Upgrade Firmware screen that appears, **do not** enable the Reboot Immediately to Begin Upgrade option. Click Upgrade.

	4.1(3c) 💿	
<b>Upgrade F</b> i Firmware will be enable the optic	' <b>mware</b> installed on next boot. To reboot ir below.	nmediately, please
Reboot I	nmediately to Begin Upgrade	
	Cancel	Upgrade
		UCSC-C220-M5L

14. After the upgrade process begins, a server firmware upgrade request for a server reboot will be pending for each Cohesity node.

	ւյիսի։ cisco Intersight	OPERATE > Servers								
· <u>00o</u>	MONITOR									
	OPERATE ^	Health Power HCL Status Models	C220 M5L 6							
	Servers	12 • Critical 7 • Healt 5 © On 10	C220 M3E 8     C240 M5L 4     HXAF220C M 2							
,	Chassis									
	Fabric Interconnects	···· 🖉 🔍 Add Filter								
	HyperFlex Clusters	Name Health Contract Status	Manage 🗘 Model							
×	CONFIGURE ^	C220-WZP22440AZC	172.25.178.2 HXAF2:							
	Orchestration	C220-WZP22440AX5 C Healthy Not Covered	172.25.178.2 HXAF2:							
	Profiles	①         C25-FI6454-1         © Healthy         Image: Not Covered	10.29.149.14 UCSC-C							
	Templates	C25-FI6454-2 C25-FI6454-2 O Healthy O Not Covered	10.29.149.15 UCSC-C							
	Policies	C25-F16454-3 C Healthy Not Covered	10.29.149.16 UCSC-C							
	Pools	C220-WZP233414DG	10.41.2.131 UCSC-C							
	OPTIMIZE ^	C220-WZP24130MEV Requests	⊕ 1 C							
	Overview	Upgrade Firmware	Action Required							
	Plan	C220-WZP24440A75 € C220-WZP24440A6Z	2 minutes ago							
	Placement	C220-WZP24440A7F 🕤 🖪 Critical	10.29.149.36 UCSC-C							
	More	C220-WZP24440A6V	10.29.149.37 UCSC-C							
ē	ADMIN ^	①         C240-WZP2227005W         © Healthy         Image: Not Covered	10.29.149.38 UCSC-C							

_							
≡	cisco Intersight	Requests > Upgra					
<u>t0</u> 0		Details		Execution Flow			
ø		Status		Progress			
		Name	Upgrade Firmware	• Wait for the server reboot.			
		ID Turra Turr	60c10f9d696f6e2d309f8c3d	Please issue server power cycle to proceed further with firmware upgrade process.			
		Target Type	WZP24440A6Z	<ul> <li>Indata the server investory for out-of-hand components</li> </ul>			hen 0, 2021 12:00 PM
		Source Type	Firmware Upgrade	State synchronized.			
×		Source Name	C220-WZP24440A6Z	Initiate firmware upgrade. Unamedia are and boot account along a suscessfully. Up 10 20 3 40 05 Mars torus users: Demote a suscessfully.			
		Initiator	andhiman@cisco.com				
		Start Time End Time	Jun 9, 2021 11:59 AM				
		Duration					
		Organizations					
Ł							

15. At this point, the server firmware is staged on each Cohesity node deployed on the Cisco UCS C-Series Rack Servers. Users can proceed to upgrade the Cohesity software according to the guidelines suggested by Cohesity Support. After the Cohesity software upgrade is initiated, the server firmware will be upgraded automatically when the node reboots.

# Conclusion

The Cisco Intersight platform is a SaaS infrastructure lifecycle management solution that delivers simplified configuration, deployment, maintenance, and support. Cohesity DataPlatform on Cisco UCS is an end-to-end data management platform delivering hyperscale simplicity, multicloud agility, and global visibility. It consolidates data silos across on-premises, cloud, and edge sites and simplifies IT operations.

Integrating the Cisco Intersight platform for Cohesity on Cisco UCS provides global visibility of infrastructure health and status along with advanced management and support capabilities. The Cisco Intersight platform delivers a convenient SaaS solution with the capability to connect from anywhere and manage infrastructure through a browser or mobile app while allowing customers to stay ahead of problems and accelerate trouble resolution through advanced support capabilities.

# For more information

Consult the following references for additional information about the topics discussed in this document.

## **Products and solutions**

- Cisco Intersight platform: <u>https://www.intersight.com</u>
- Cisco Unified Computing System: <u>http://www.cisco.com/en/US/products/ps10265/index.html</u>
- Cisco UCS adapters:
   <u>http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html</u>
- Cohesity on Cisco UCS: <u>https://www.cisco.com/go/cohesity</u>
   https://www.cohesity.com/solutions/technology-partners/cisco/

# **Configuration guides**

- Cisco UCS with Cohesity Data Protection for Cisco HyperFlex™:
   <u>https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucsc240_cohesity_dp.</u>
   <u>html</u>
- Cisco UCS S3260 Storage Servers with Cohesity DataPlatform: <u>https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_s3260_cohesity_dataplatform.html</u>
- Setup Guide (Cisco UCS C240 M5) <u>https://docs.cohesity.com/hardware/PDFs/SetupGuideCiscoUCSC240M5.pdf</u>

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)

Printed in USA

221181.1 07/21