White Paper
Public

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

Contents

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 Cisco Cohesity Data Management Solutions 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.

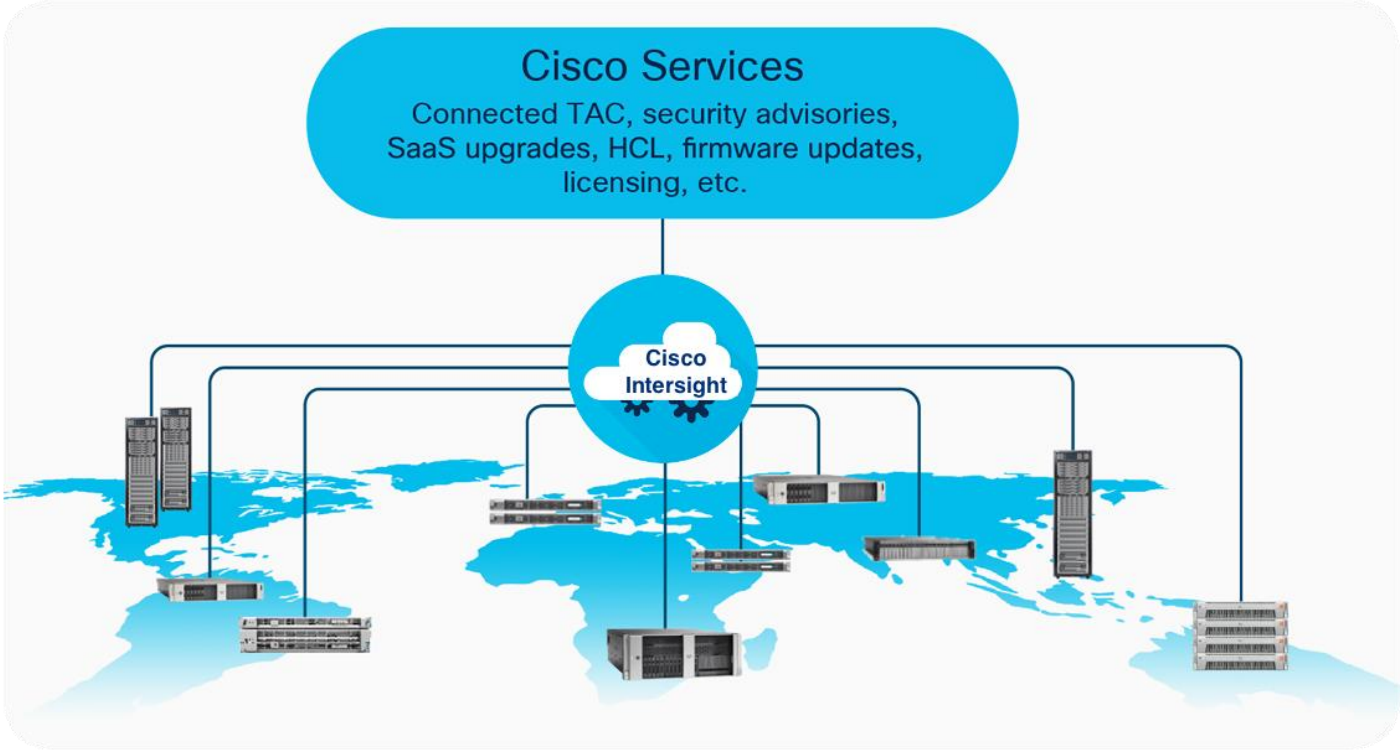

Cisco Services
Connected TAC, security advisories, SaaS upgrades, HCL, firmware updates, licensing, etc.
Cisco Intersight

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.

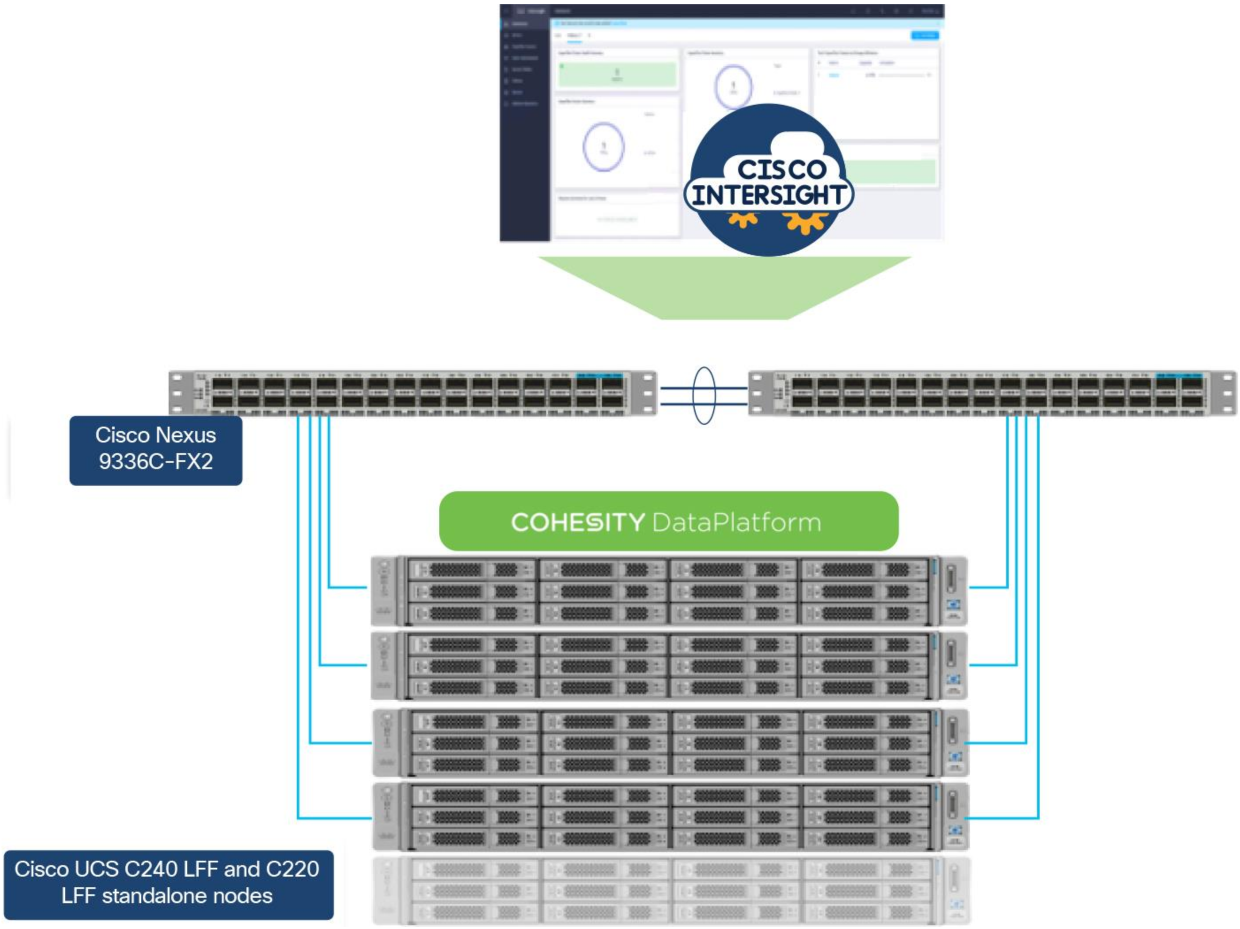


Figure 2.
Cohesity on Cisco UCS server nodes

Deployment hardware and software

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

Table 1. Software requirements

	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 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.

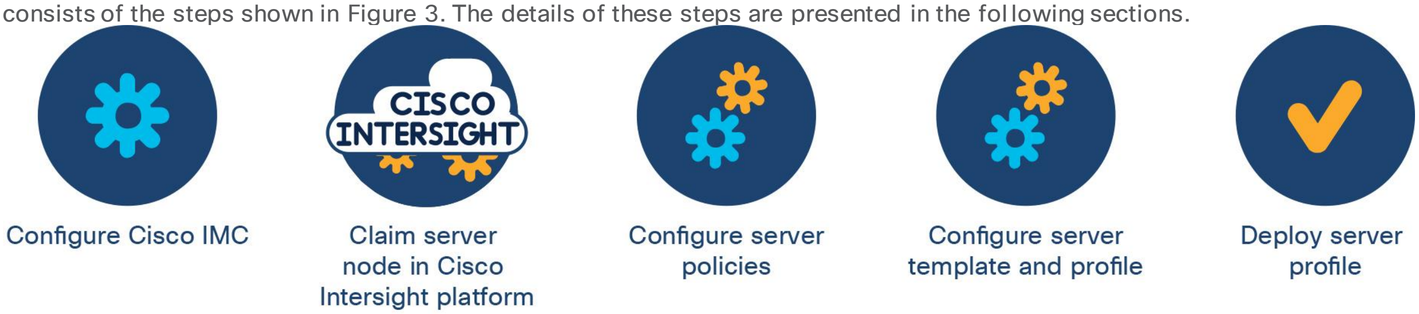

CISCO INTERSIGHT
Configure Cisco IMC
Claim server node in Cisco Intersight platform
Configure server policies
Configure server template and profile
Deploy server profile

Figure 3.
Steps to configure Cisco UCS server nodes using the Cisco Intersight platform

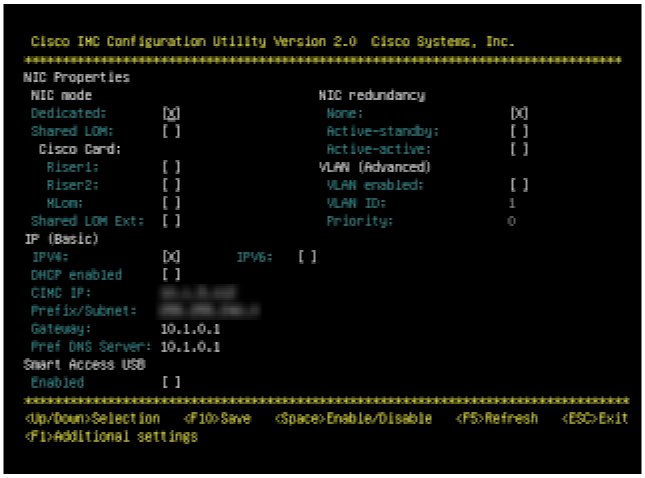
Configure Cisco IMC network

To configure the Cisco IMC network, follow these steps:

1. 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.



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*****************************************************************************
NIC Properties
 NIC mode                               NIC redundancy
 Dedicated:        [X]                   None:                     [X]
 Shared LOM:       [ ]                   Active-standby:           [ ]
  Cisco Card:                            Active-active:            [ ]
   Riser1:         [ ]                  VLAN (Advanced)
   Riser2:         [ ]                   VLAN enabled:             [ ]
   MLom:           [ ]                   VLAN ID:                  1
 Shared LOM Ext:   [ ]                   Priority:                 0
IP (Basic)
 IPV4:             [X]       IPV6:    [ ]
 DHCP enabled      [ ]
 CIMC IP:          [redacted]
 Prefix/Subnet:    [redacted]
 Gateway:          10.1.0.1
 Pref DNS Server:  10.1.0.1
Smart Access USB
 Enabled           [ ]
*****************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```

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 Intersight Overview.

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

Note: Prepare device to claim in Cisco Intersight platform

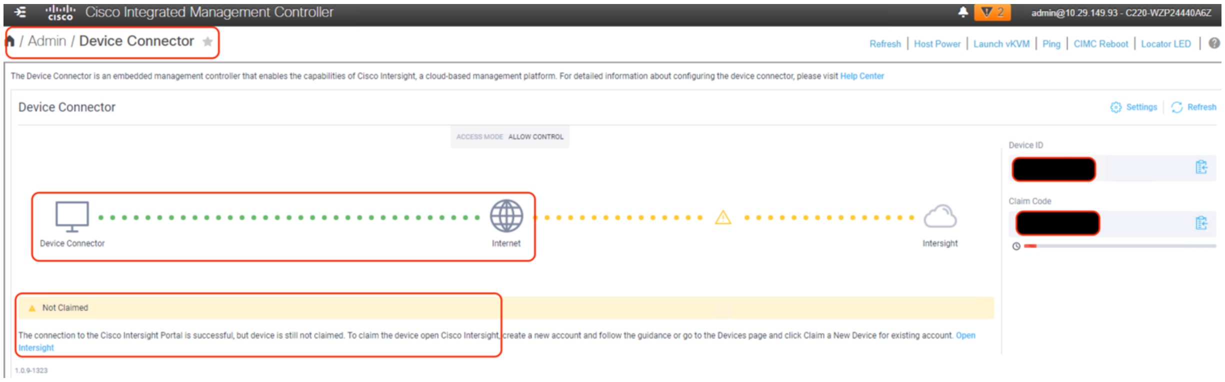
Follow these steps to prepare the device that you want to claim in the Cisco Intersight platform:

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.

4. Verify that the status of server is Not Claimed and that connection to the Cisco Intersight portal is successful.



Cisco Integrated Management Controller
2
admin@10.29.149.93 - C220-WZP24440A6Z
/ 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 Center

Device Connector

Settings | Refresh
ACCESS MODE ALLOW CONTROL
Device Connector
Internet
Intersight

Device ID [redacted]

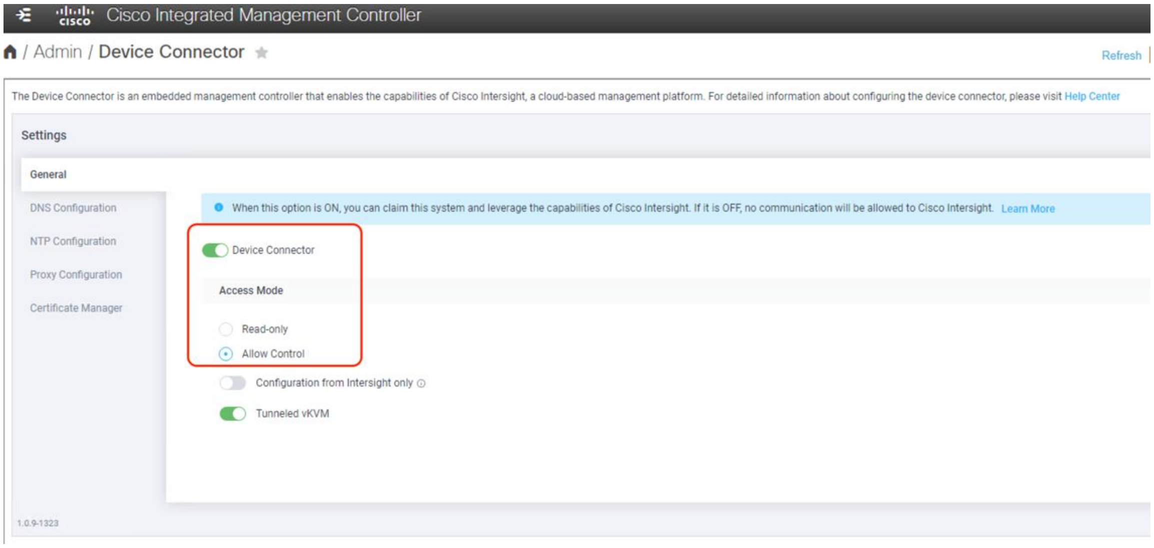
Claim Code [redacted]

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 click Claim a New Device for existing account. Open Intersight

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.



/ Admin / Device Connector ☆ Refresh

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 Center

Settings

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

Device Connector: ON

Access Mode

○ Read-only

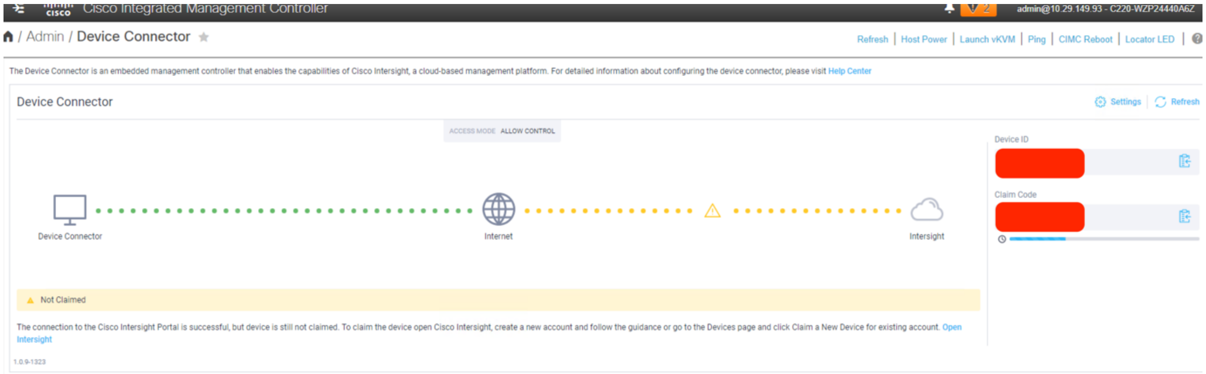
● Allow Control

Configuration from Intersight only: OFF

Tunneled vKVM: ON

1.0.9-1323

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

/ 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 Center

Device Connector

ACCESS MODE ALLOW CONTROL

Device Connector
Internet
Intersight

Device ID: [redacted]

Claim Code: [redacted]

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 click Claim a New Device for existing account. Open Intersight

1.0.9-1323

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

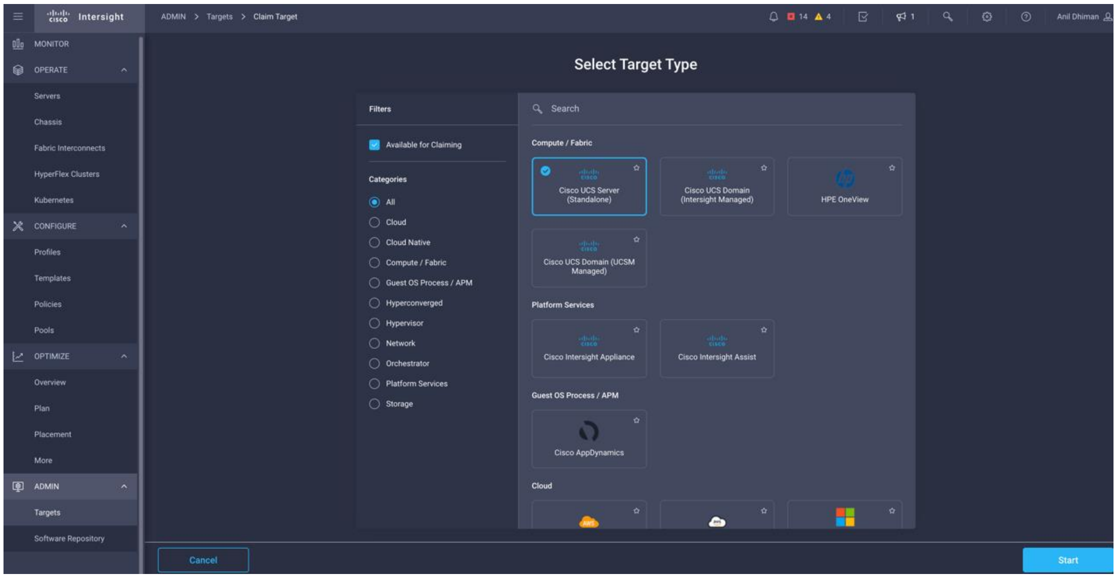
Claim device in Cisco Intersight platform

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.



Select Target Type

Filters

☑ Available for Claiming

Categories

● All
○ Cloud
○ Cloud Native
○ Compute / Fabric
○ Guest OS Process / APM
○ Hyperconverged
○ Hypervisor
○ Network
○ Orchestrator
○ Platform Services
○ Storage

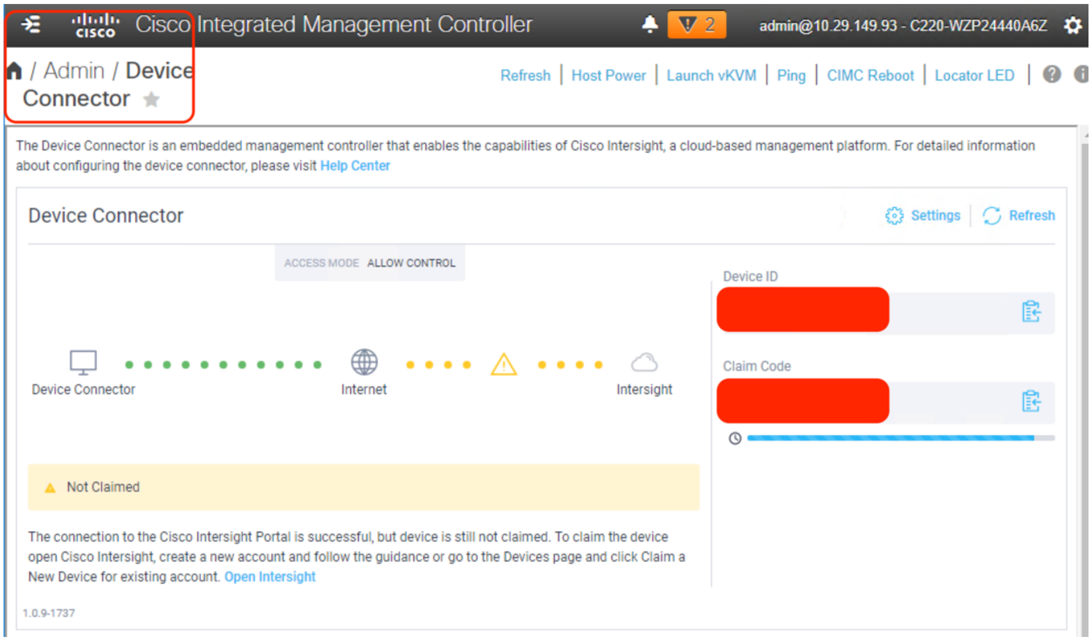
Compute / Fabric: ✓ Cisco UCS Server (Standalone)

Platform Services

Guest OS Process / APM

Cloud

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.



/ Admin / Device Connector

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 Center

Device Connector

ACCESS MODE ALLOW CONTROL

Device ID
[redacted]

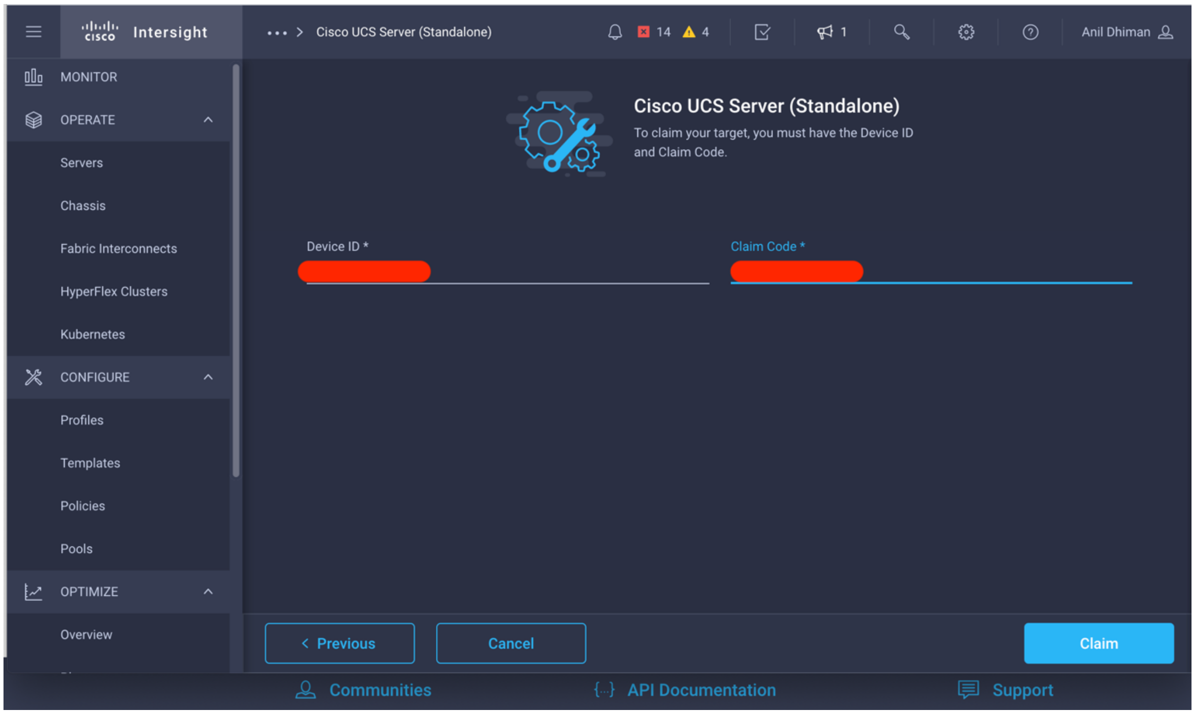
Claim Code
[redacted]

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 click Claim a New Device for existing account. Open Intersight

1.0.9-1737

5. Click Claim.



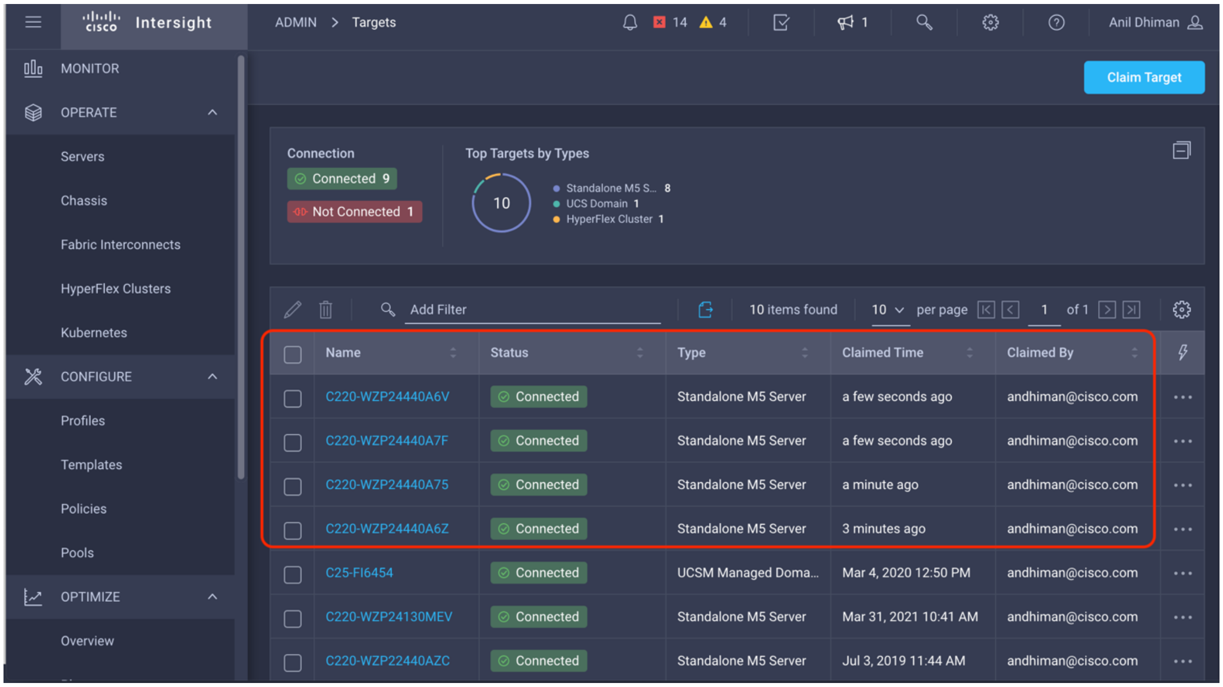
Cisco UCS Server (Standalone)

To claim your target, you must have the Device ID and Claim Code.

Device ID * [redacted]

Claim Code * [redacted]

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.



Connection: Connected 9, Not Connected 1

Top Targets by Types: 10 — Standalone M5 S... 8, UCS Domain 1, HyperFlex Cluster 1

Name	Status	Type	Claimed Time	Claimed By
C220-WZP24440A6V	Connected	Standalone M5 Server	a few seconds ago	andhiman@cisco.com
C220-WZP24440A7F	Connected	Standalone M5 Server	a few seconds ago	andhiman@cisco.com
C220-WZP24440A75	Connected	Standalone M5 Server	a minute ago	andhiman@cisco.com
C220-WZP24440A6Z	Connected	Standalone M5 Server	3 minutes ago	andhiman@cisco.com
C25-FI6454	Connected	UCSM Managed Doma...	Mar 4, 2020 12:50 PM	andhiman@cisco.com
C220-WZP24130MEV	Connected	Standalone M5 Server	Mar 31, 2021 10:41 AM	andhiman@cisco.com
C220-WZP22440AZC	Connected	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 Cisco Intersight Licensing Tiers.

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

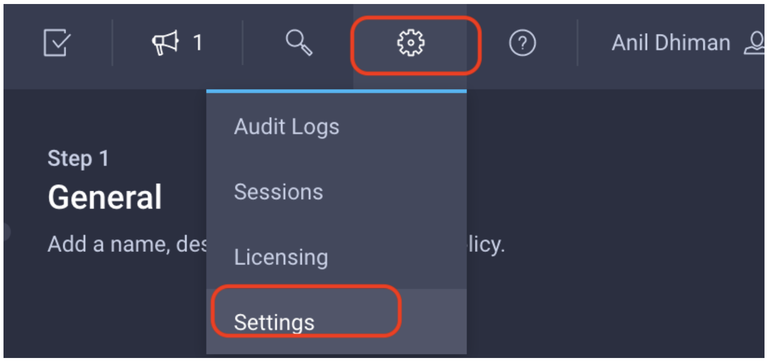
The following sections describe the server policies created to deploy Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform.

Create organization policy

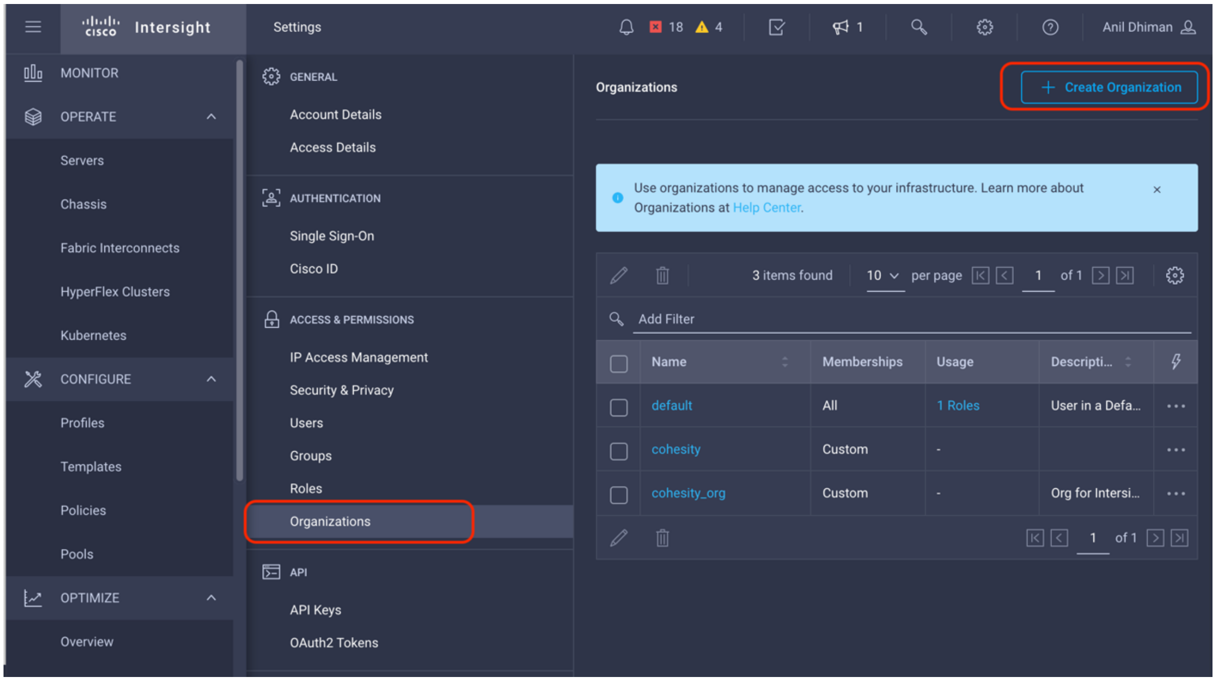
An organization is a logical entity that enables multitenancy through separation of resources. An organization allows you to divide the physical infrastructure or resources into logical entities, without requiring dedicated physical infrastructure for each organization. For more information about organizations,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

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.



Organizations

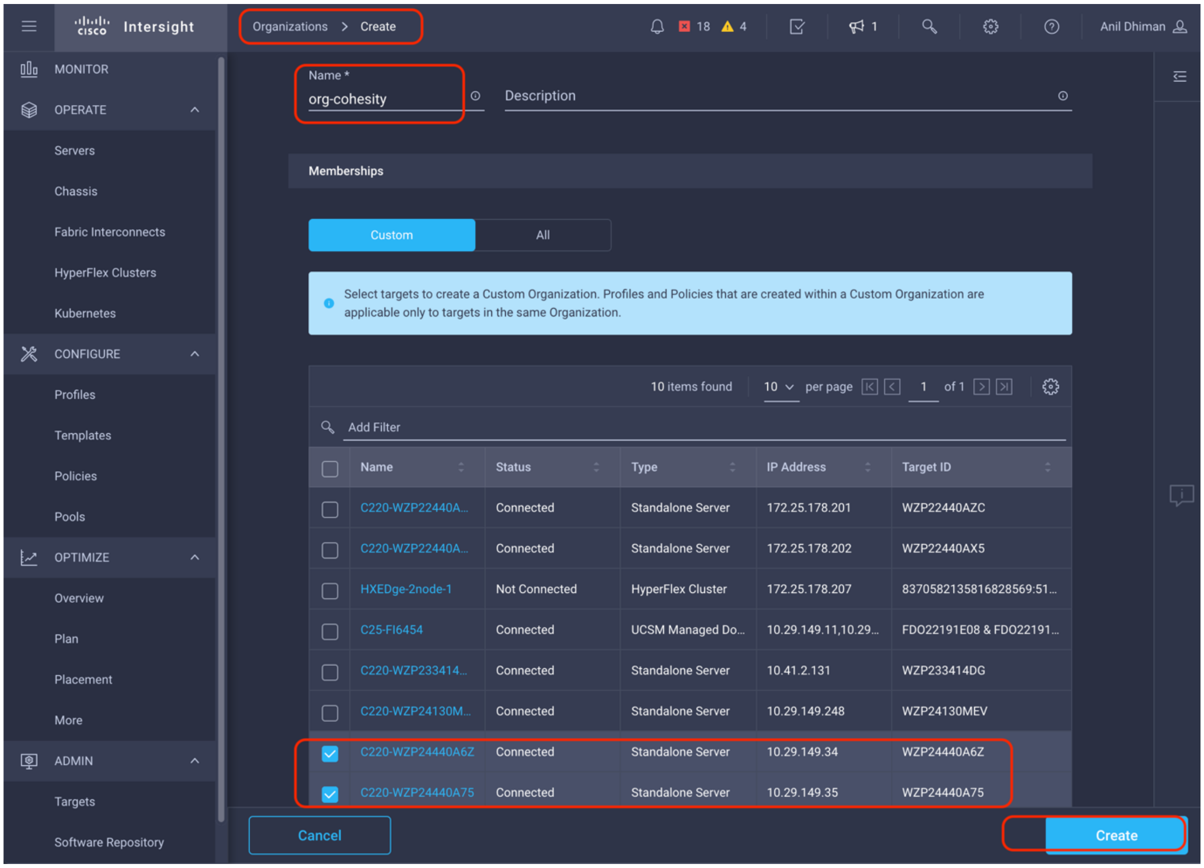
Use organizations to manage access to your infrastructure. Learn more about Organizations at Help Center.

3 items found 10 per page 1 of 1

Add Filter

Name	Memberships	Usage	Descripti...
default	All	1 Roles	User in a Defa...
cohesity	Custom	-	
cohesity_org	Custom	-	Org for Intersi...

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



Name * org-cohesity

Description

Memberships

Custom | All

Select targets to create a Custom Organization. Profiles and Policies that are created within a Custom Organization are applicable only to targets in the same Organization.

10 items found 10 per page 1 of 1

Add Filter

	Name	Status	Type	IP Address	Target ID
☐	C220-WZP22440A...	Connected	Standalone Server	172.25.178.201	WZP22440AZC
☐	C220-WZP22440A...	Connected	Standalone Server	172.25.178.202	WZP22440AX5
☐	HXEDge-2node-1	Not Connected	HyperFlex Cluster	172.25.178.207	8370582135816828569:51...
☐	C25-FI6454	Connected	UCSM Managed Do...	10.29.149.11,10.29...	FDO22191E08 & FDO22191...
☐	C220-WZP233414...	Connected	Standalone Server	10.41.2.131	WZP233414DG
☐	C220-WZP24130M...	Connected	Standalone Server	10.29.149.248	WZP24130MEV
☑	C220-WZP24440A6Z	Connected	Standalone Server	10.29.149.34	WZP24440A6Z
☑	C220-WZP24440A75	Connected	Standalone Server	10.29.149.35	WZP24440A75

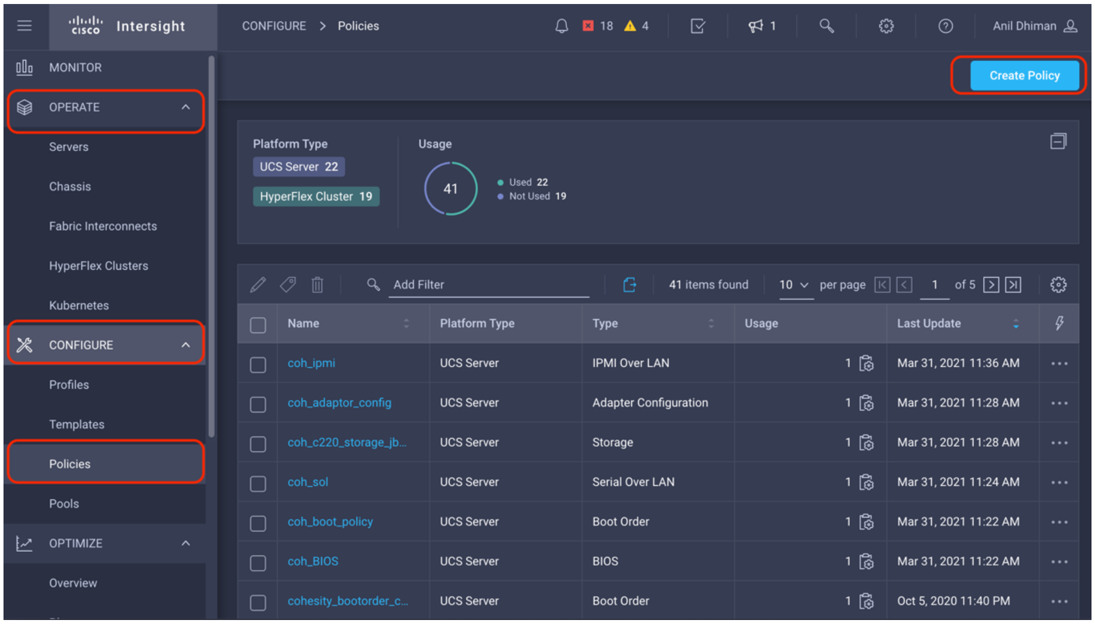
5. Verify that the organization was created successfully.

Create adaptor configuration policy

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

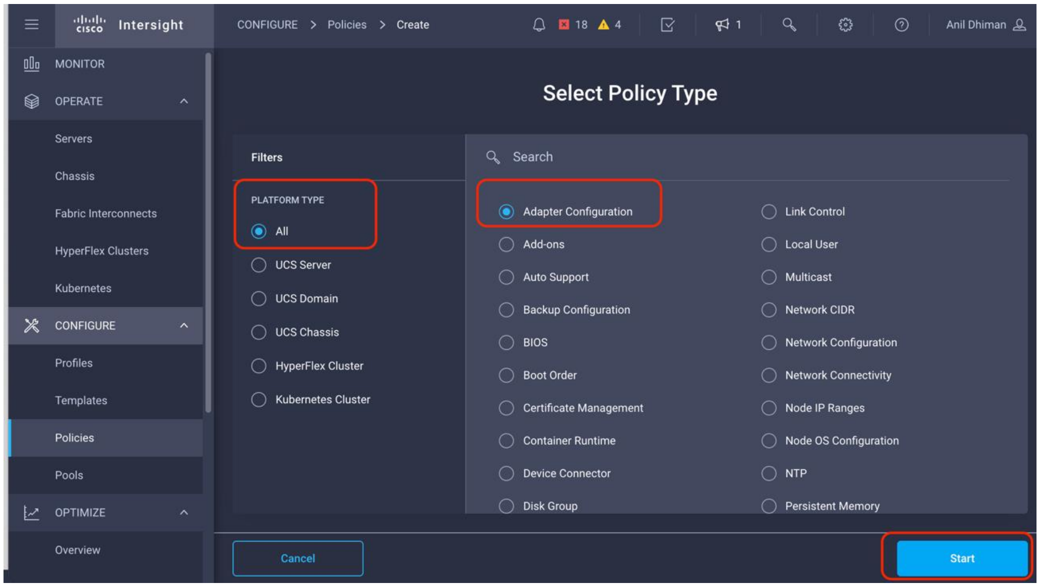
Follow these steps to configure adaptor configuration policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

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

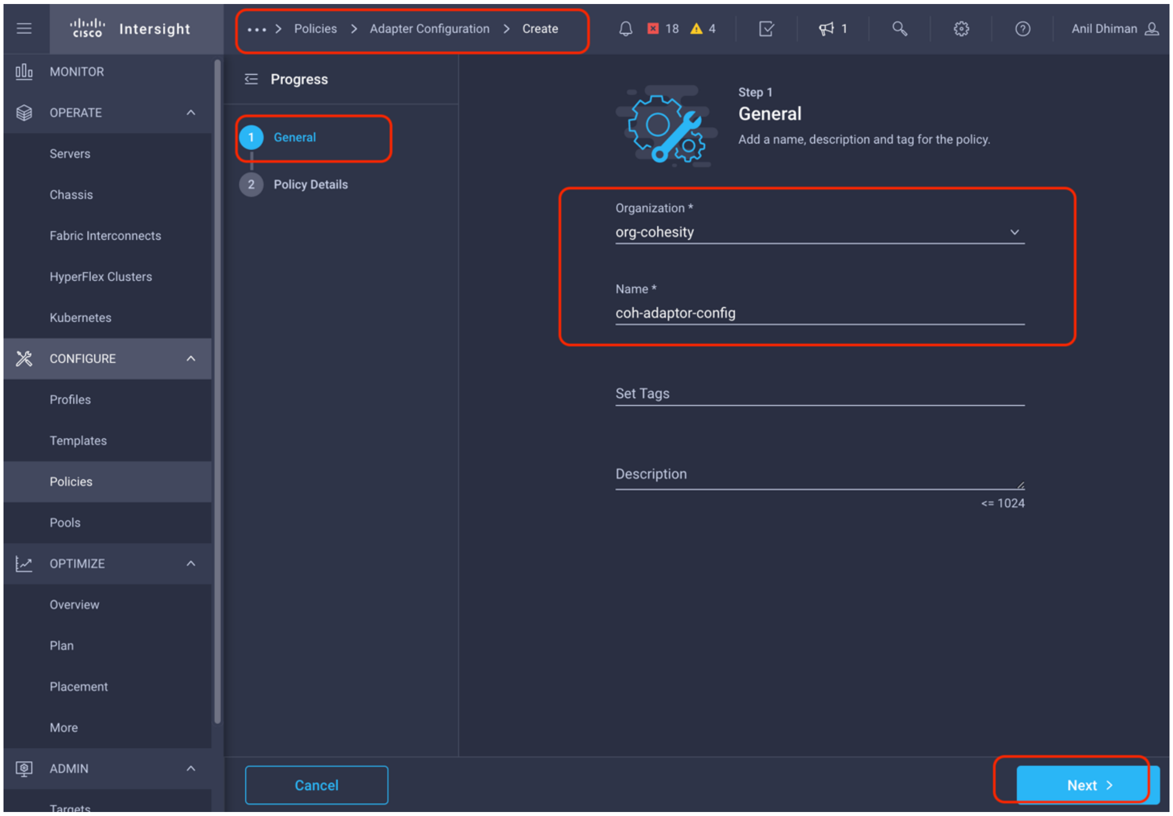


Name	Platform Type	Type	Usage	Last Update
coh_ipmi	UCS Server	IPMI Over LAN	1	Mar 31, 2021 11:36 AM
coh_adaptor_config	UCS Server	Adapter Configuration	1	Mar 31, 2021 11:28 AM
coh_c220_storage_jb...	UCS Server	Storage	1	Mar 31, 2021 11:28 AM
coh_sol	UCS Server	Serial Over LAN	1	Mar 31, 2021 11:24 AM
coh_boot_policy	UCS Server	Boot Order	1	Mar 31, 2021 11:22 AM
coh_BIOS	UCS Server	BIOS	1	Mar 31, 2021 11:22 AM
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.



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.



Step 1

General

Add a name, description and tag for the policy.

Organization *

org-cohesity

Name *

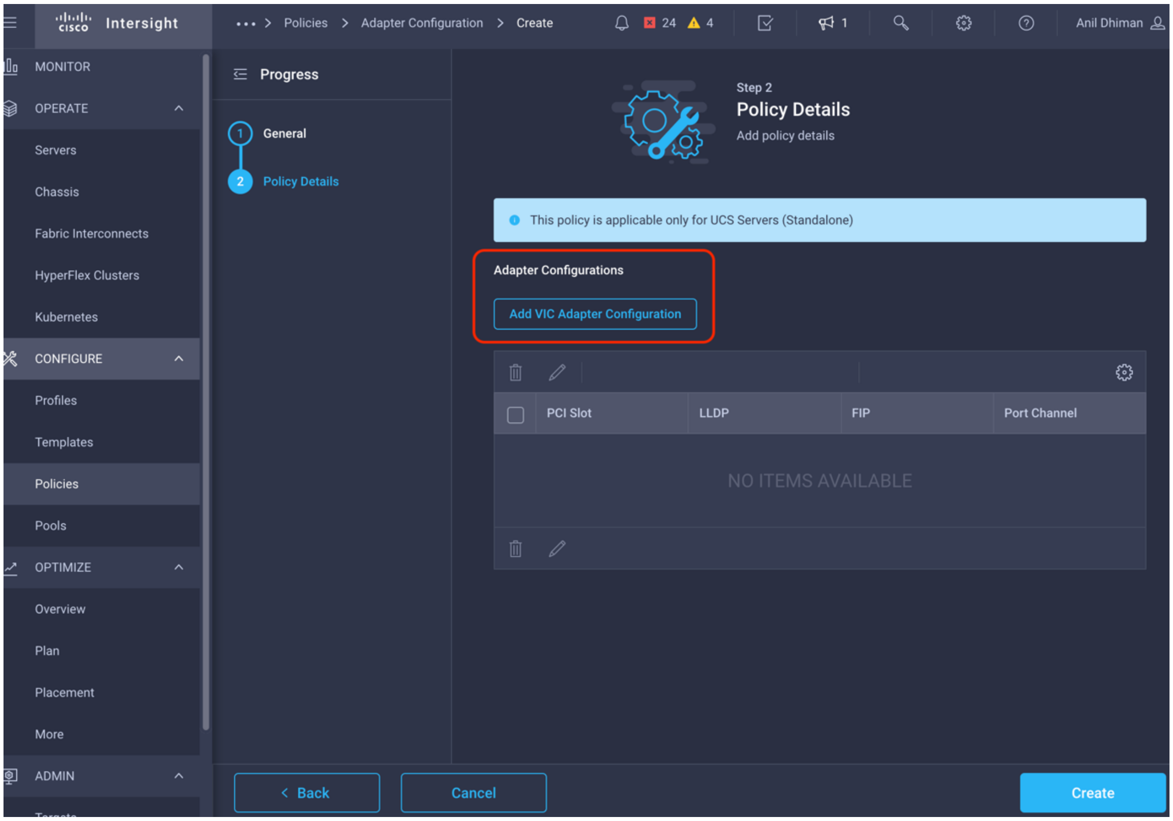
coh-adaptor-config

Set Tags

Description

<= 1024

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



Step 2

Policy Details

Add policy details

This policy is applicable only for UCS Servers (Standalone)

Adapter Configurations

□	PCI Slot	LLDP	FIP	Port Channel

NO ITEMS AVAILABLE

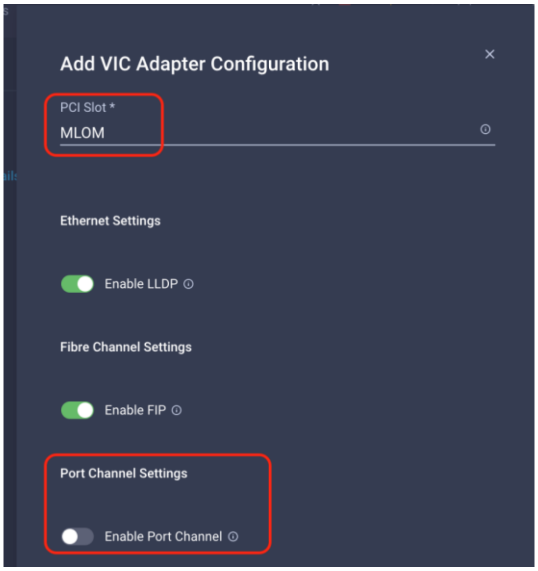
6. Enter the following details for the VIC configuration:

   - 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 Ethernet 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.

- Click the Add button.



Add VIC Adapter Configuration

PCI Slot *: MLOM

Ethernet Settings

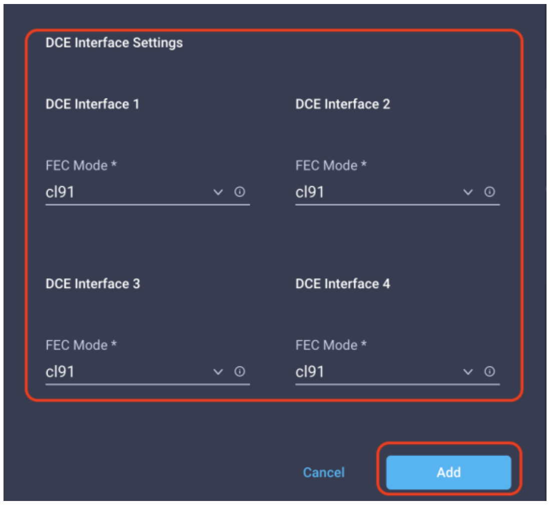
Enable LLDP: on

Fibre Channel Settings

Enable FIP: on

Port Channel Settings

Enable Port Channel: off



DCE Interface Settings

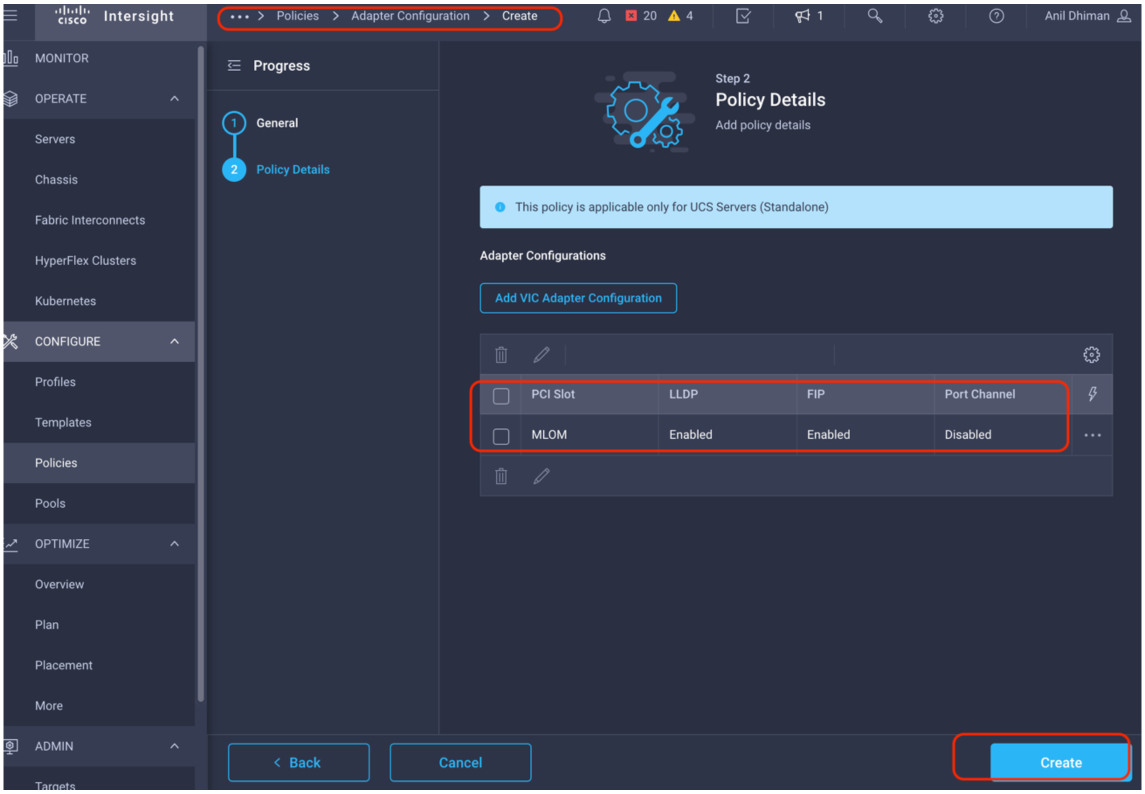
DCE Interface 1 — FEC Mode *: cl91

DCE Interface 2 — FEC Mode *: cl91

DCE Interface 3 — FEC Mode *: cl91

DCE Interface 4 — FEC Mode *: cl91

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



Step 2
Policy Details
Add policy details

This policy is applicable only for UCS Servers (Standalone)

Adapter Configurations

Add VIC Adapter Configuration

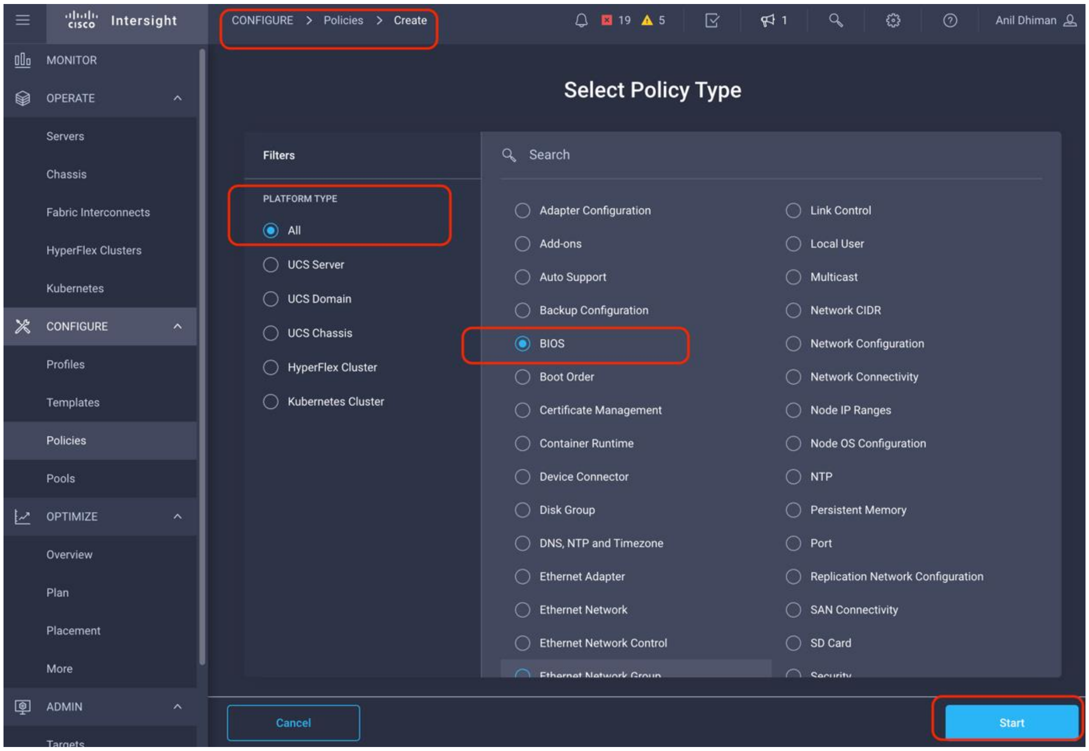
PCI Slot	LLDP	FIP	Port Channel
MLOM	Enabled	Enabled	Disabled

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:

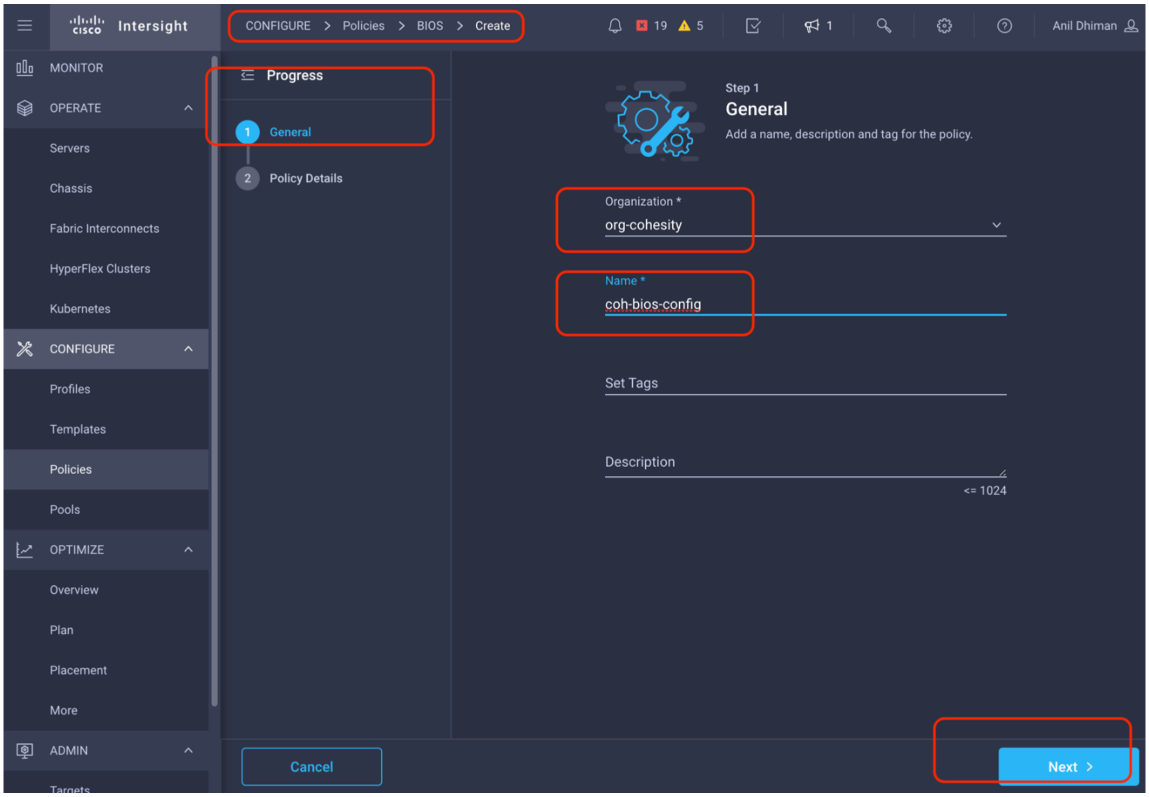
1. Log in to the Cisco Intersight Platform at https://intersight.com/.
2. Navigate to Operate > Configure > Policies. Click Create Policy.
3. For Platform Type, select All. Select BIOS and click Start.



PLATFORM TYPE: ● All

● BIOS

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.



Step 1

General

Add a name, description and tag for the policy.

Organization *: org-cohesity

Name *: coh-bios-config

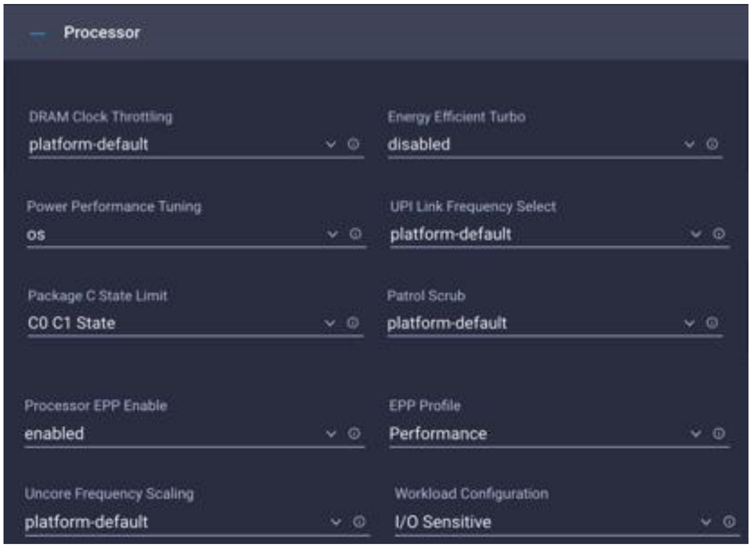
Set Tags

Description

<= 1024

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: platform-default

Energy Efficient Turbo: disabled

Power Performance Tuning: os

UPI Link Frequency Select: platform-default

Package C State Limit: C0 C1 State

Patrol Scrub: platform-default

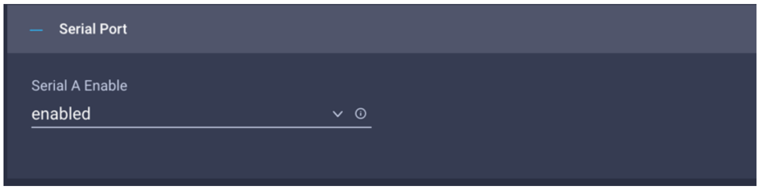
Processor EPP Enable: enabled

EPP Profile: Performance

Uncore Frequency Scaling: platform-default

Workload Configuration: I/O Sensitive

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



Serial Port

Serial A Enable: enabled

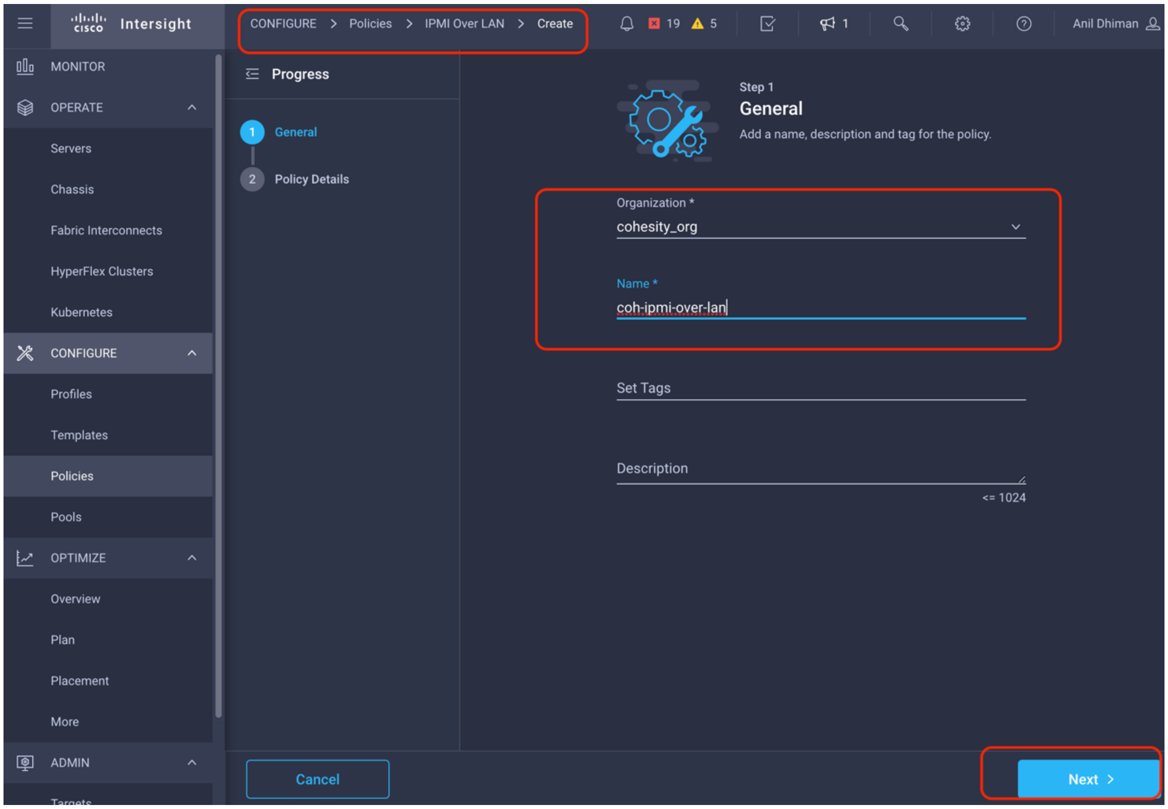
- Click Create and verify that the BIOS policy was created successfully.

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.



CONFIGURE > Policies > IPMI Over LAN > Create

Step 1

General

Add a name, description and tag for the policy.

Organization * cohesity_org

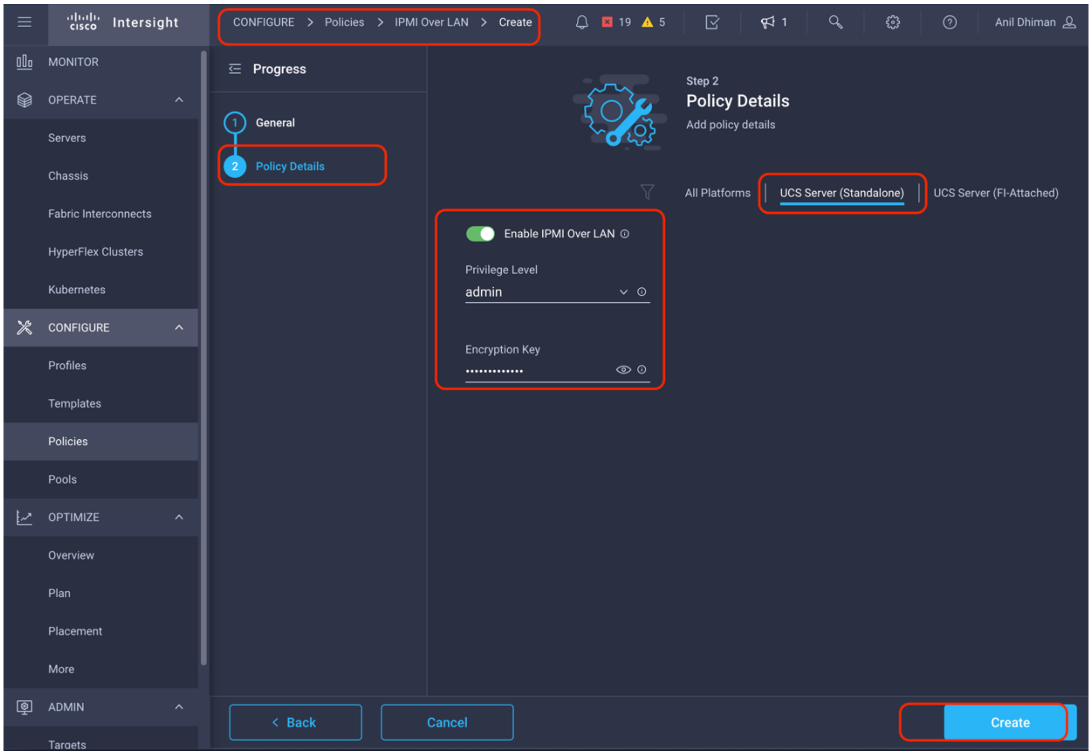
Name * coh-ipmi-over-lan

Set Tags

Description

<= 1024

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.



Step 2
Policy Details
Add policy details

Enable IPMI Over LAN

Privilege Level
admin

Encryption Key
•••••••••••••

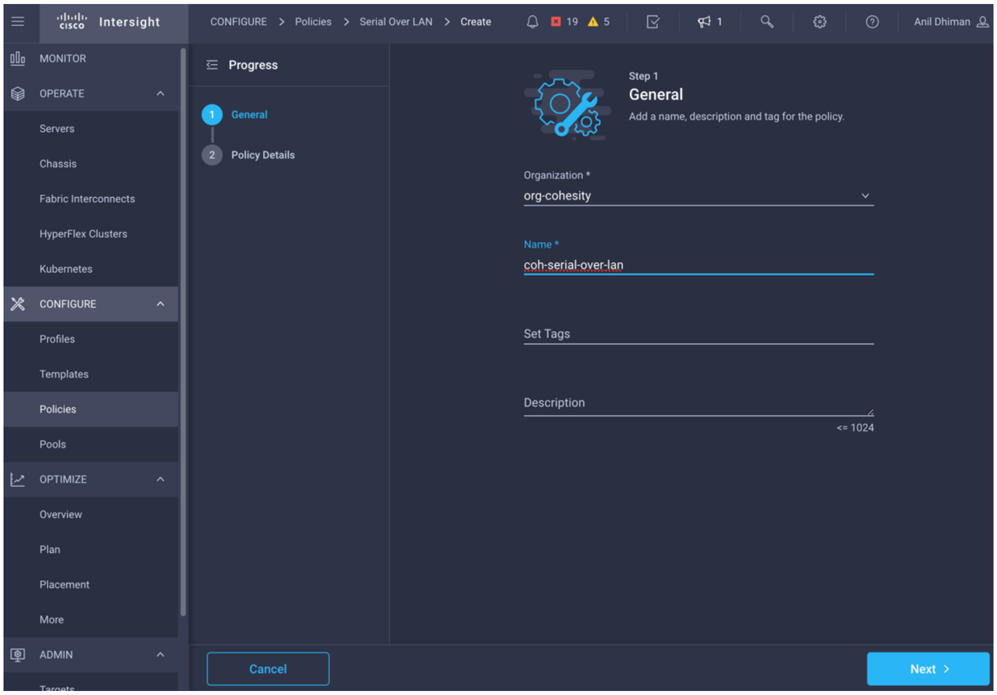
6. Verify that the IPMI-over-LAN policy was created successfully.

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.



Step 1
General
Add a name, description and tag for the policy.

Organization *
org-cohesity

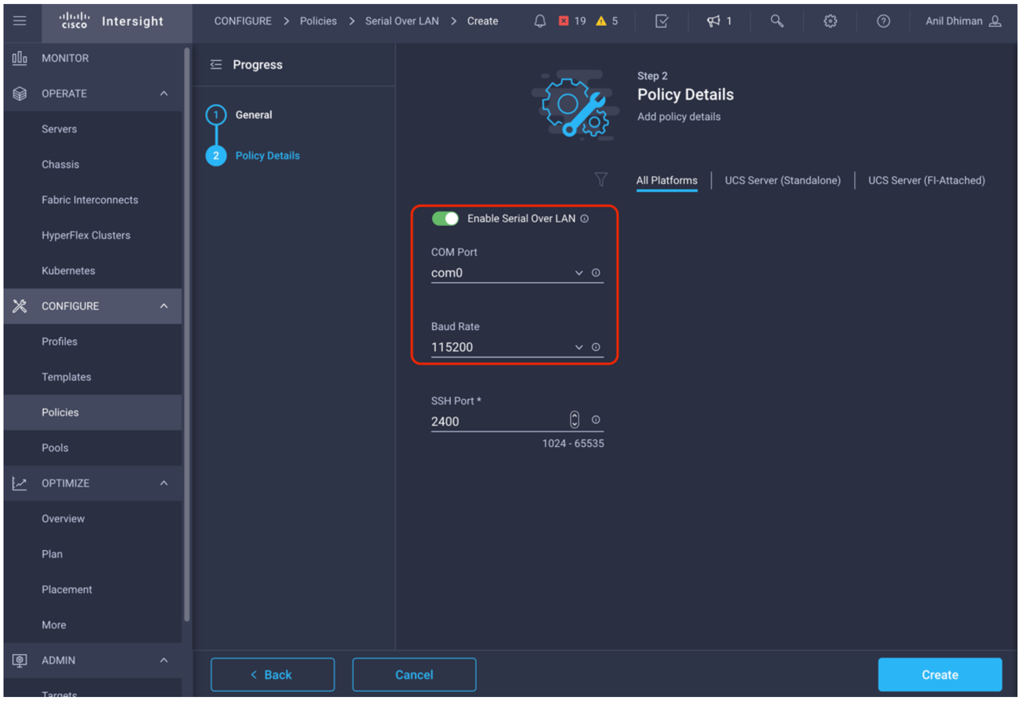
Name *
coh-serial-over-lan

Set Tags

Description
<= 1024

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.



Step 2
Policy Details
Add policy details

Enable Serial Over LAN

COM Port
com0

Baud Rate
115200

SSH Port *
2400
1024 - 65535

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

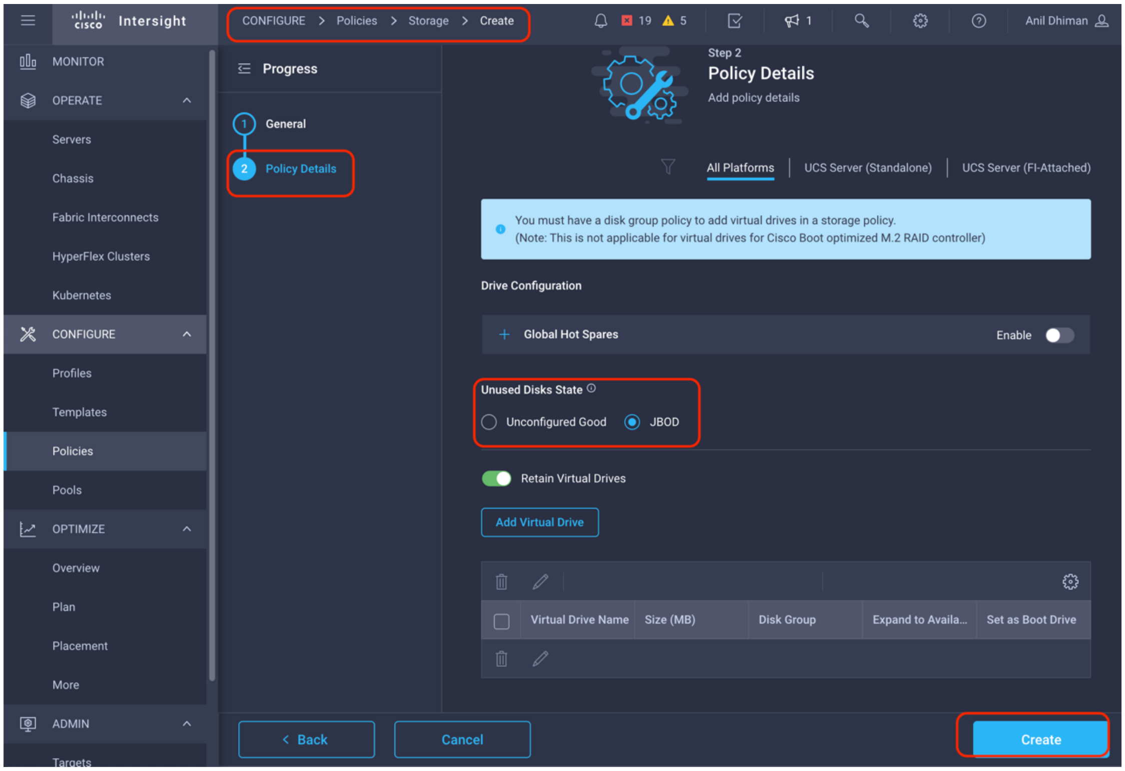
Create storage configuration policy

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.



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)

Drive Configuration

Global Hot Spares — Enable: off

Unused Disks State: ○ Unconfigured Good ● JBOD

Retain Virtual Drives: on

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

Create boot-order policy

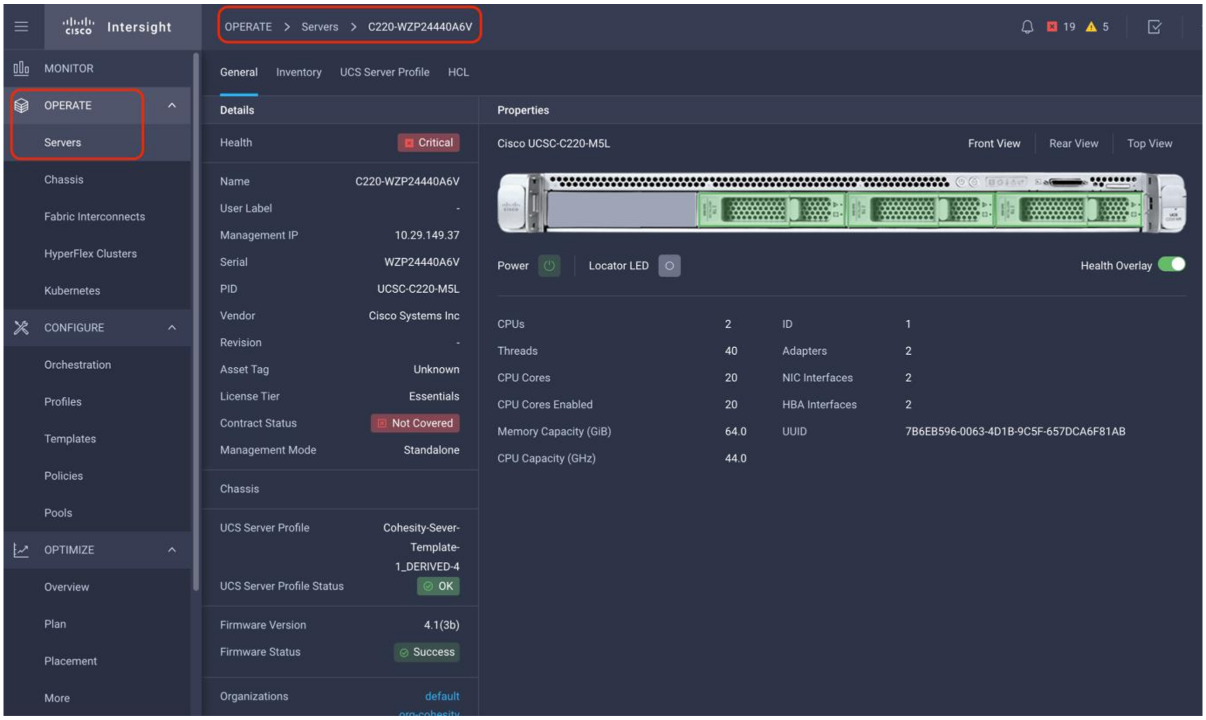
Boot-order policy configures the linear ordering of devices and enables you to change the boot order and boot mode. You can also add multiple devices under various device types, rearrange the boot order, and set parameters for each boot device type.

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.



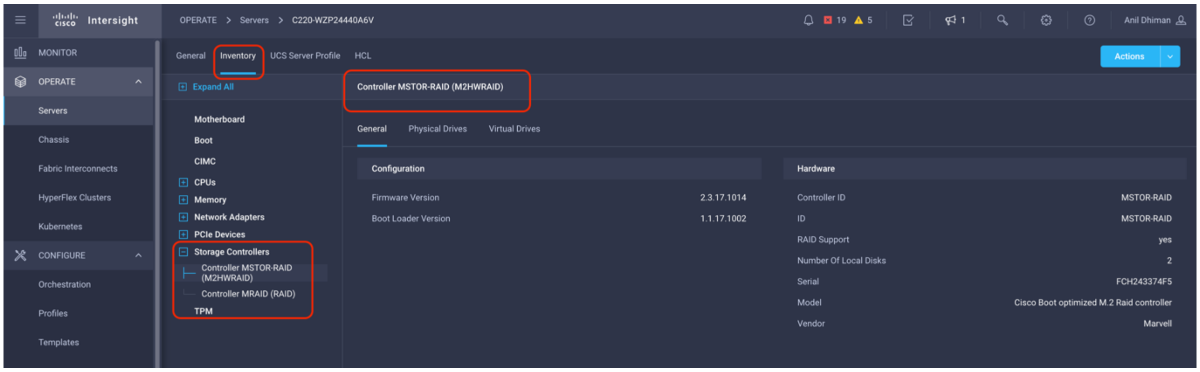
Details	
Health	Critical
Name	C220-WZP24440A6V
User Label	-
Management IP	10.29.149.37
Serial	WZP24440A6V
PID	UCSC-C220-M5L
Vendor	Cisco Systems Inc
Revision	-
Asset Tag	Unknown
License Tier	Essentials
Contract Status	Not Covered
Management Mode	Standalone
Chassis	
UCS Server Profile	Cohesity-Sever-Template-1_DERIVED-4
UCS Server Profile Status	OK
Firmware Version	4.1(3b)
Firmware Status	Success
Organizations	default org-cohesity

Properties

Cisco UCSC-C220-M5L

CPUs	2	ID	1
Threads	40	Adapters	2
CPU Cores	20	NIC Interfaces	2
CPU Cores Enabled	20	HBA Interfaces	2
Memory Capacity (GiB)	64.0	UUID	7B6EB596-0063-4D1B-9C5F-657DCA6F81AB
CPU Capacity (GHz)	44.0		

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



Controller MSTOR-RAID (M2HWRAID)

Configuration	
Firmware Version	2.3.17.1014
Boot Loader Version	1.1.17.1002

Hardware	
Controller ID	MSTOR-RAID
ID	MSTOR-RAID
RAID Support	yes
Number Of Local Disks	2
Serial	FCH243374F5
Model	Cisco Boot optimized M.2 Raid controller
Vendor	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.

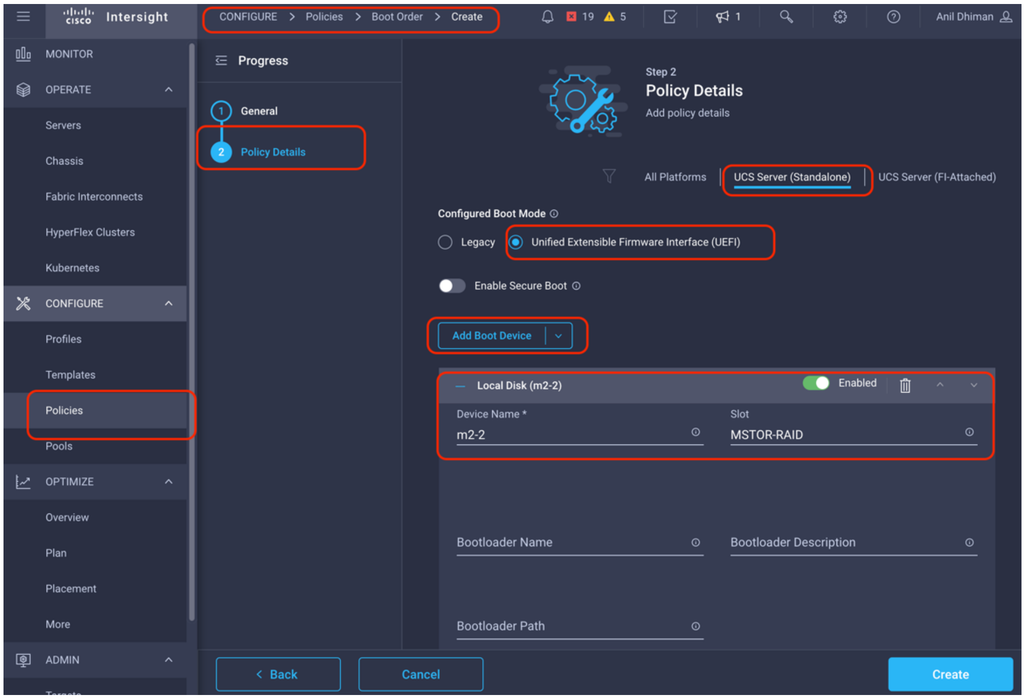
Note: UEFI boot mode for Cisco UCS C240 M5 Rack Servers with Cohesity DataPlatform is supported only by Cohesity Release 6.6.0a and later.

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.



Configured Boot Mode

○ Legacy ● Unified Extensible Firmware Interface (UEFI)

Enable Secure Boot

Local Disk (m2-2) Enabled

Device Name * m2-2

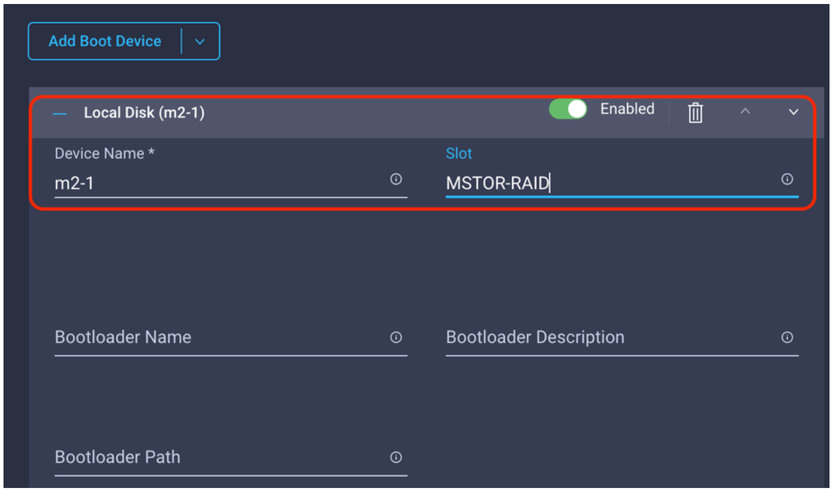
Slot MSTOR-RAID

Bootloader Name

Bootloader Description

Bootloader Path

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.



Local Disk (m2-1) Enabled

Device Name * m2-1

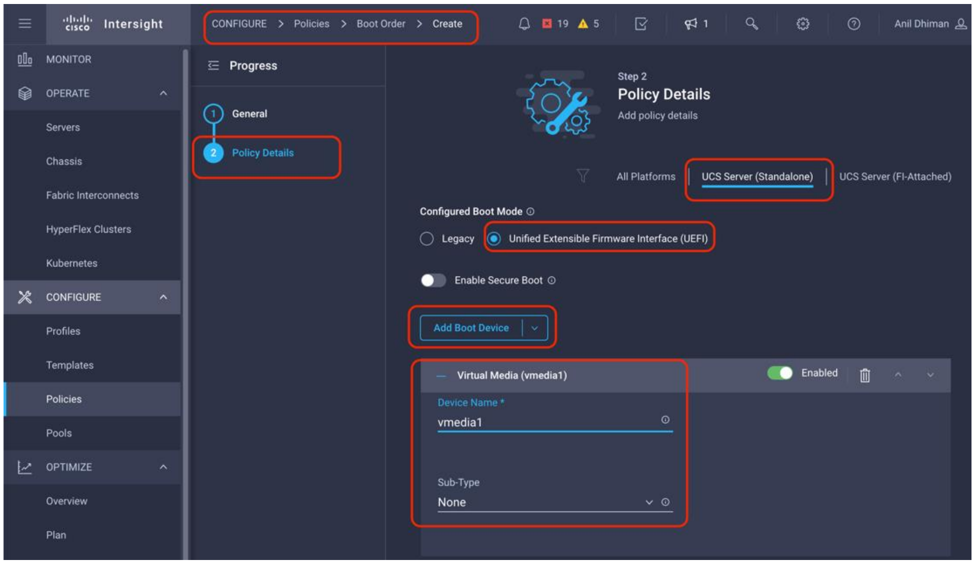
Slot MSTOR-RAID

Bootloader Name

Bootloader Description

Bootloader Path

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



Configured Boot Mode

○ Legacy ● Unified Extensible Firmware Interface (UEFI)

Enable Secure Boot

Virtual Media (vmedia1)

Device Name * vmedia1

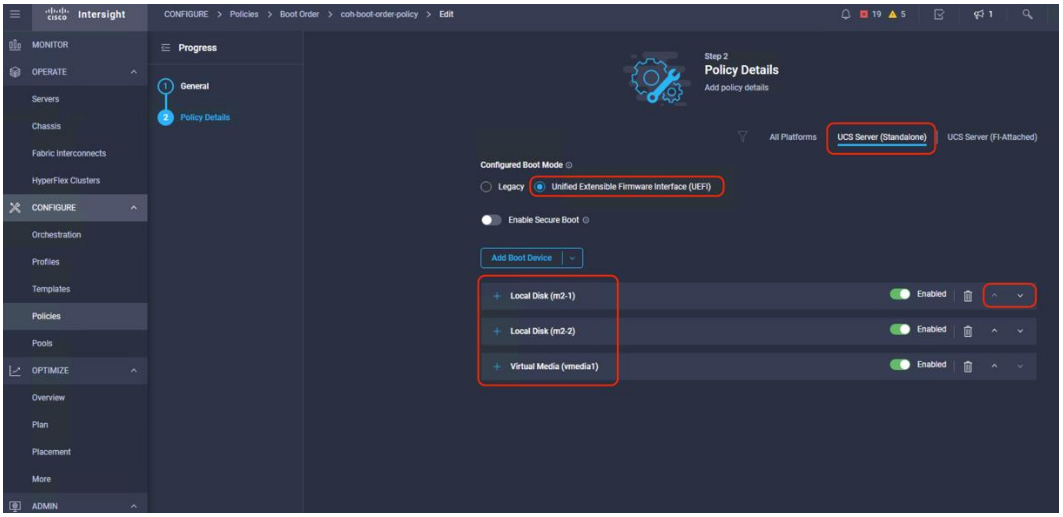
Sub-Type None

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.



Configured Boot Mode

○ Legacy ● Unified Extensible Firmware Interface (UEFI)

Enable Secure Boot

Local Disk (m2-1) Enabled

Local Disk (m2-2) Enabled

Virtual Media (vmedia1) Enabled

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.

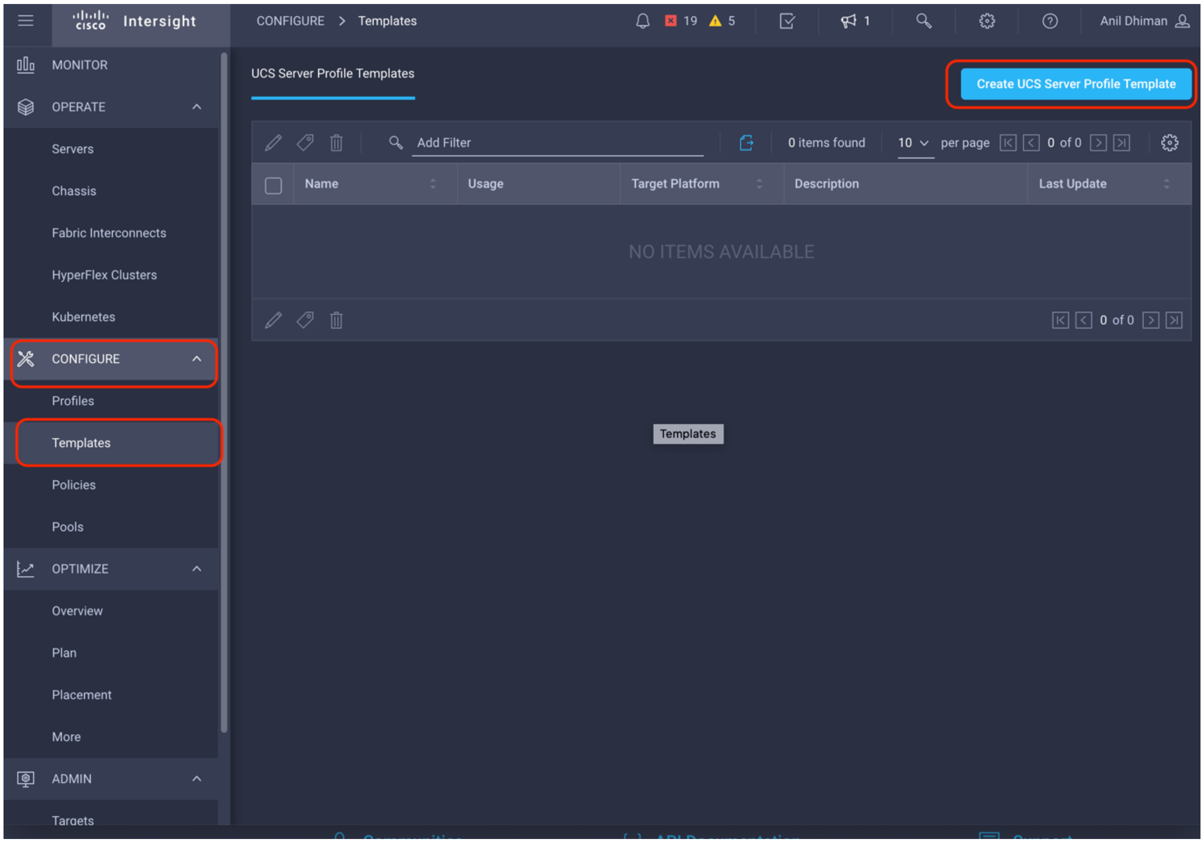
In Cisco Intersight, server profile templates enable the user to define a template from which multiple server profiles can be derived and deployed. Any property modification made in the template is synchronized in all the derived profiles. You can deploy these modified profiles individually. This feature 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.

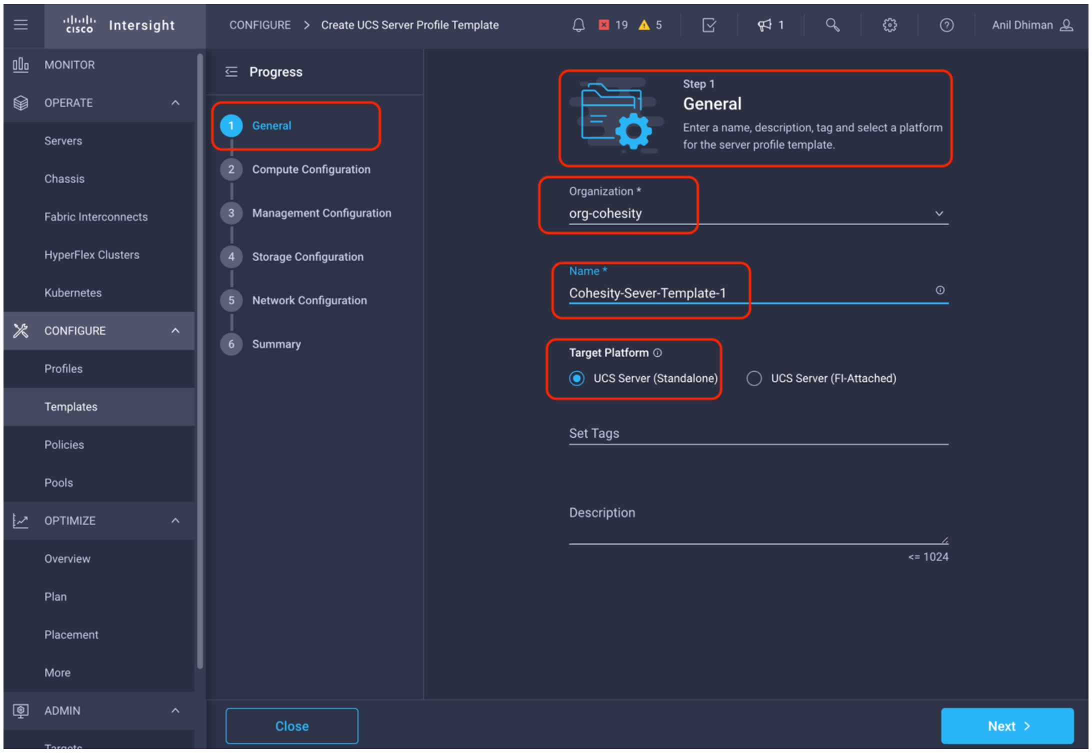
Note: Creation of a server profile template for Cohesity nodes is a one-time process generally performed during infrastructure provisioning. After a template has been created, you can instantiate server profiles and deploy them to the Cohesity nodes on Cisco UCS C220 and C240 Rack Servers, hence provisioning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

To create a server profile template, follow these steps:

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



Step 1

General

Enter a name, description, tag and select a platform for the server profile template.

Organization *: org-cohesity

Name *: Cohesity-Sever-Template-1

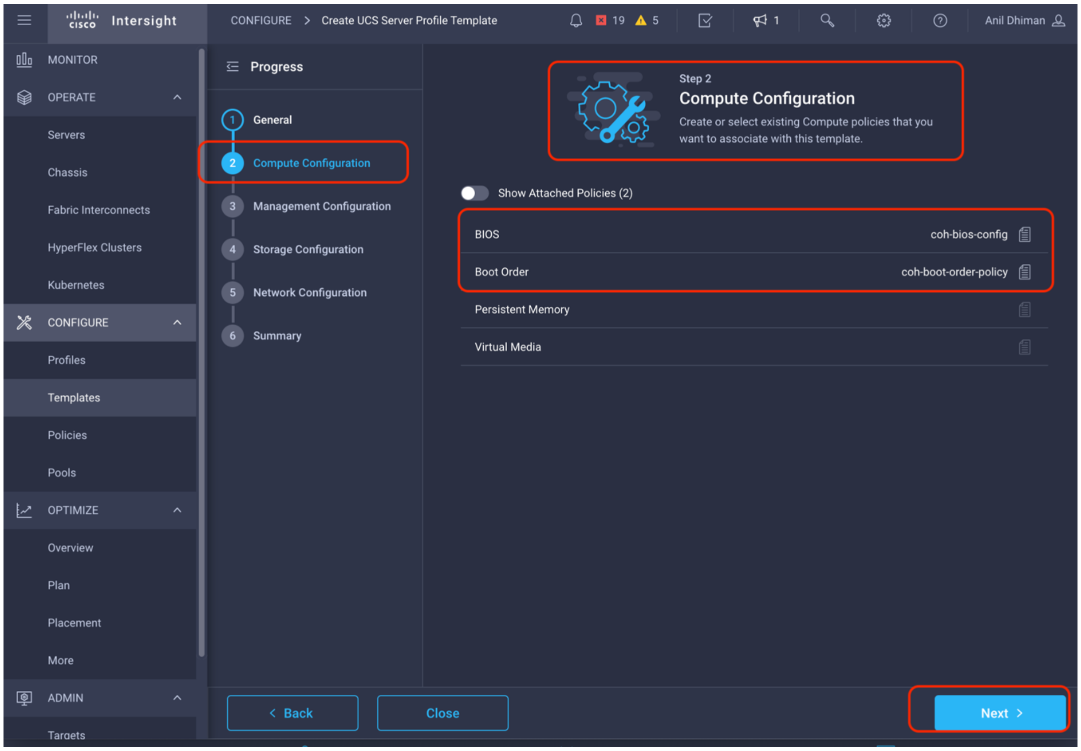
Target Platform: ● UCS Server (Standalone) ○ UCS Server (FI-Attached)

Set Tags

Description

<= 1024

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.



Step 2

Compute Configuration

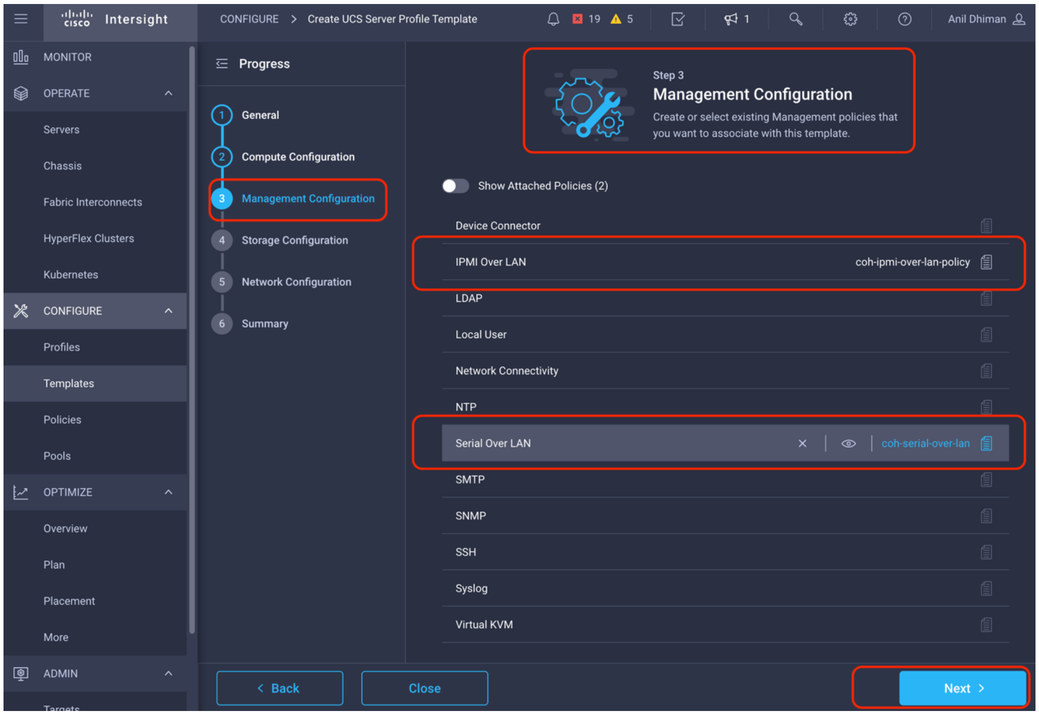
Create or select existing Compute policies that you want to associate with this template.

Show Attached Policies (2)

BIOS	coh-bios-config
Boot Order	coh-boot-order-policy
Persistent Memory	
Virtual Media	

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.



Step 3

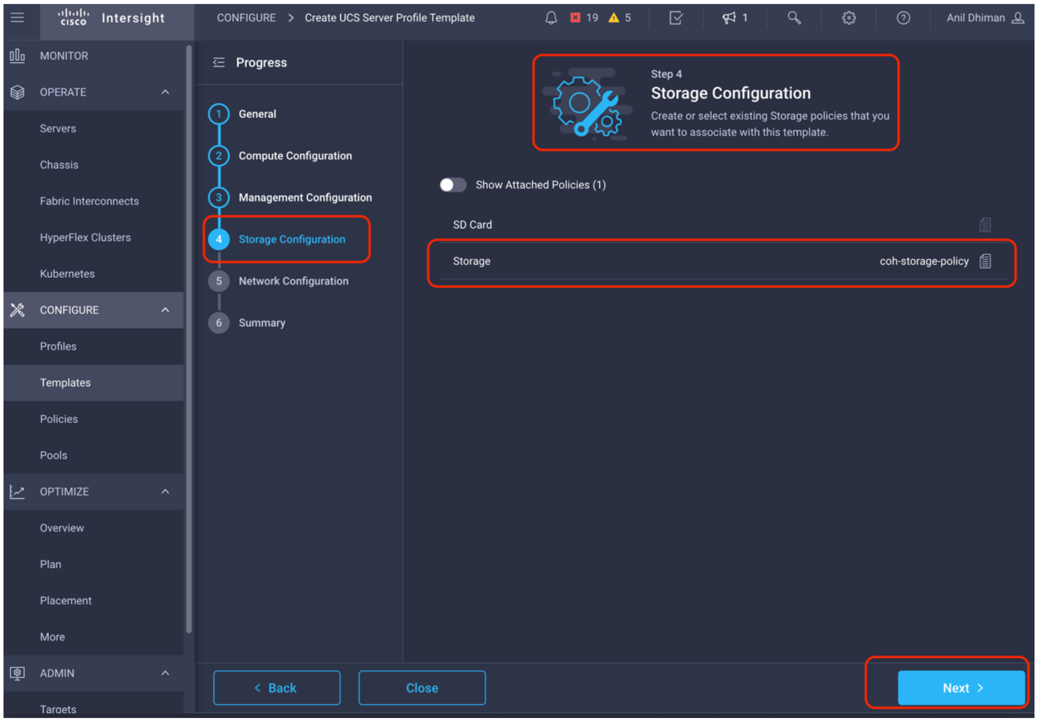
Management Configuration

Create or select existing Management policies that you want to associate with this template.

Show Attached Policies (2)

Device Connector	
IPMI Over LAN	coh-ipmi-over-lan-policy
LDAP	
Local User	
Network Connectivity	
NTP	
Serial Over LAN	coh-serial-over-lan
SMTP	
SNMP	
SSH	
Syslog	
Virtual KVM	

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



Step 4

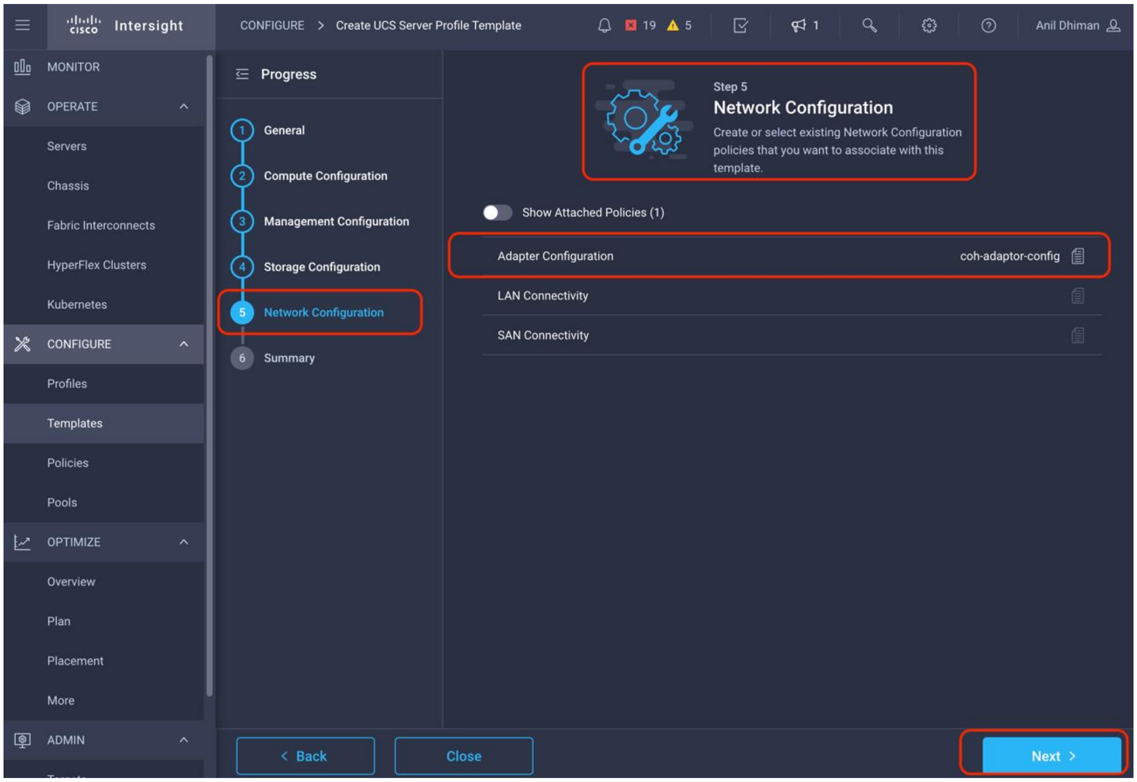
Storage Configuration

Create or select existing Storage policies that you want to associate with this template.

Show Attached Policies (1)

SD Card	
Storage	coh-storage-policy

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



Step 5

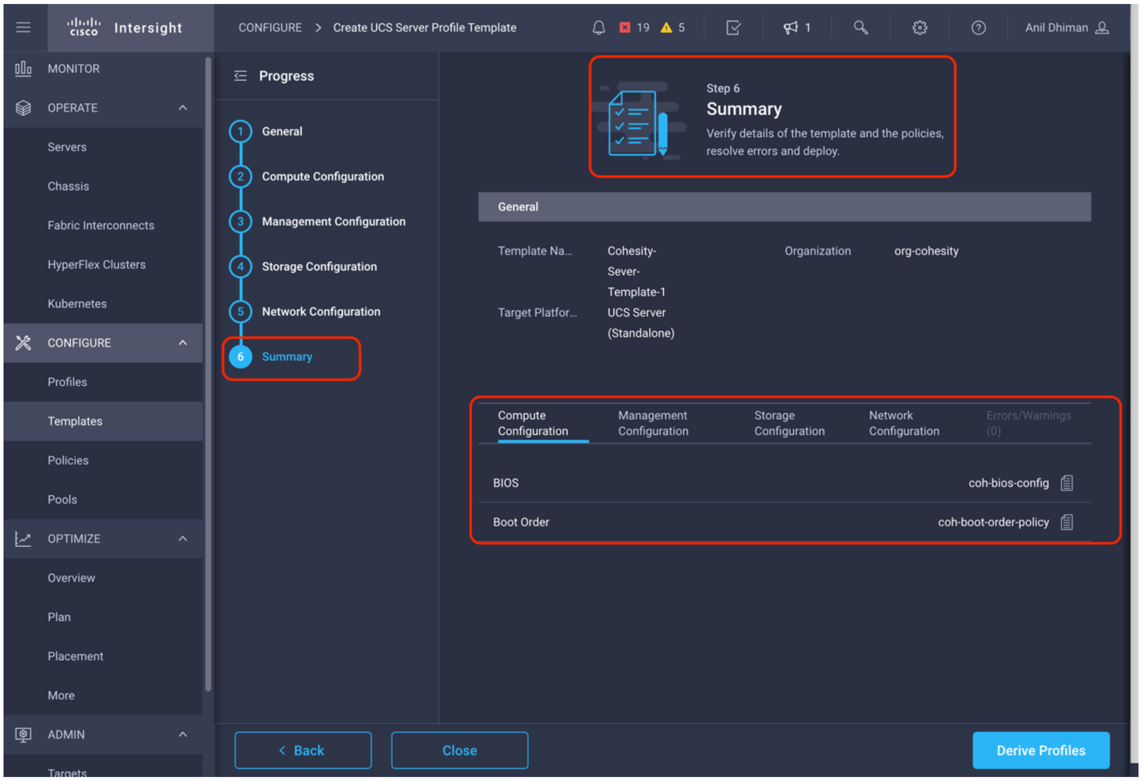
Network Configuration

Create or select existing Network Configuration policies that you want to associate with this template.

Show Attached Policies (1)

Adapter Configuration	coh-adaptor-config
LAN Connectivity	
SAN Connectivity	

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



Step 6

Summary

Verify details of the template and the policies, resolve errors and deploy.

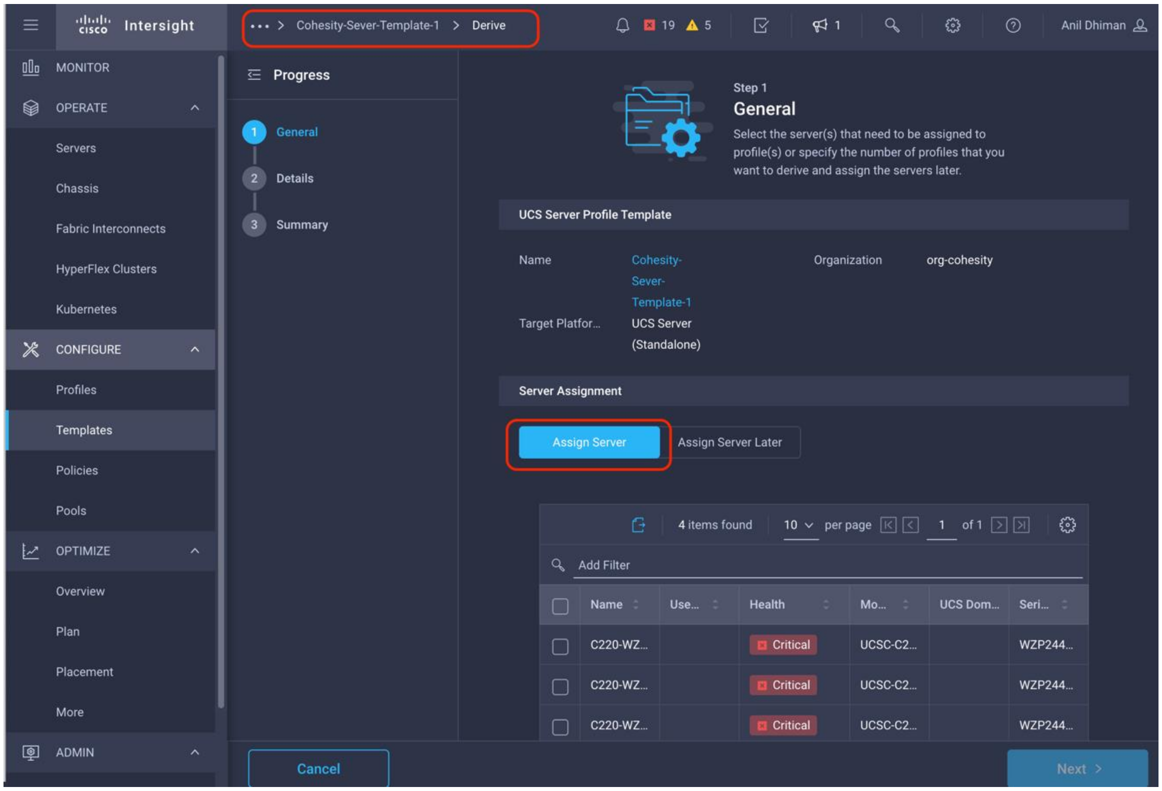
General

Template Na...	Cohesity-Sever-Template-1	Organization	org-cohesity
Target Platfor...	UCS Server (Standalone)		

Compute Configuration | Management Configuration | Storage Configuration | Network Configuration | Errors/Warnings (0)

BIOS	coh-bios-config
Boot Order	coh-boot-order-policy

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.



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.

UCS Server Profile Template

Name: Cohesity-Sever-Template-1 | Organization: org-cohesity

Target Platfor...: UCS Server (Standalone)

Server Assignment

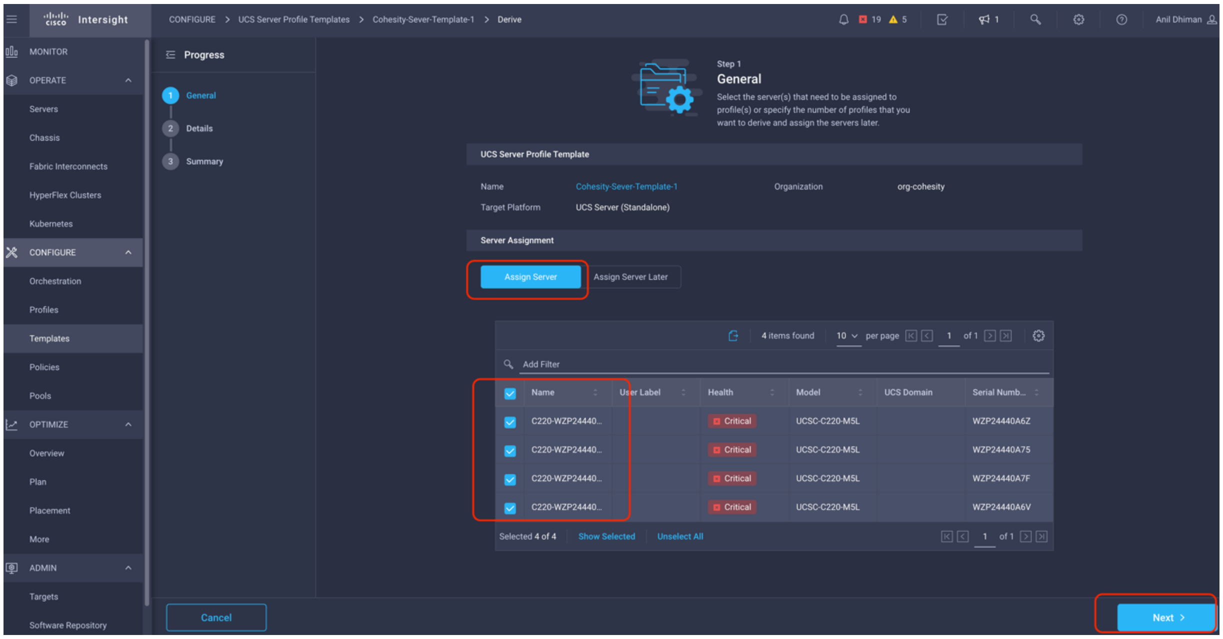
Assign Server | Assign Server Later

4 items found | 10 per page | 1 of 1

Add Filter

□	Name	Use...	Health	Mo...	UCS Dom...	Seri...
□	C220-WZ...		Critical	UCSC-C2...		WZP244...
□	C220-WZ...		Critical	UCSC-C2...		WZP244...
□	C220-WZ...		Critical	UCSC-C2...		WZP244...

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



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.

UCS Server Profile Template

Name: Cohesity-Sever-Template-1 | Organization: org-cohesity

Target Platform: UCS Server (Standalone)

Server Assignment

Assign Server | Assign Server Later

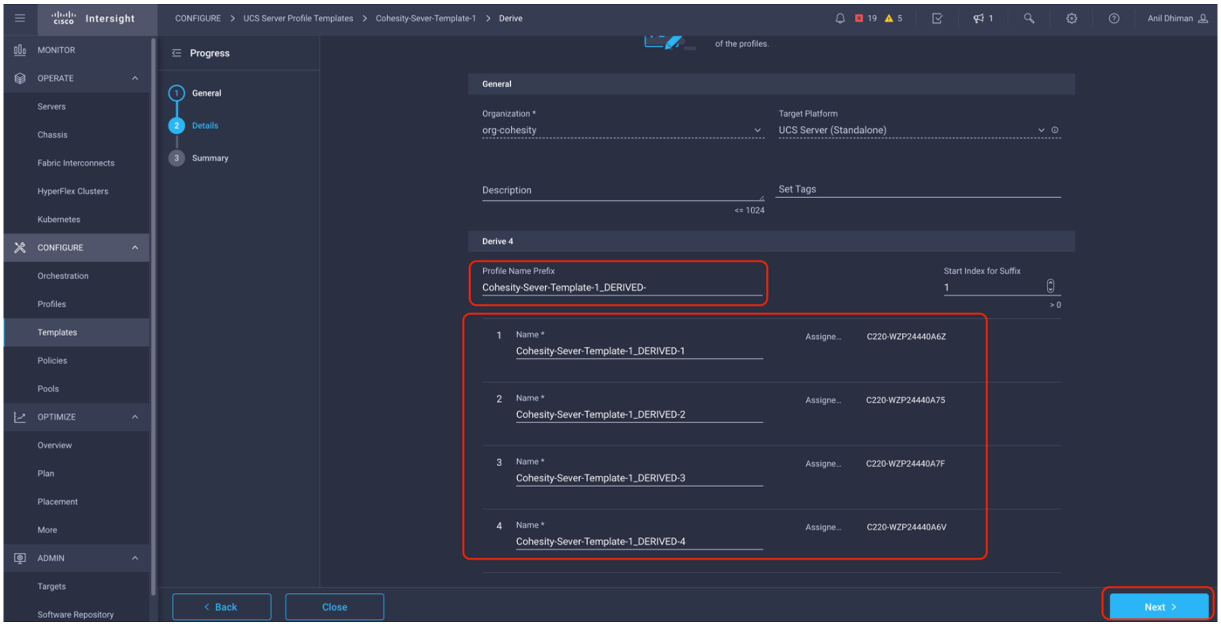
4 items found | 10 per page | 1 of 1

Add Filter

☑	Name	User Label	Health	Model	UCS Domain	Serial Numb...
☑	C220-WZP24440...		Critical	UCSC-C220-M5L		WZP24440A6Z
☑	C220-WZP24440...		Critical	UCSC-C220-M5L		WZP24440A75
☑	C220-WZP24440...		Critical	UCSC-C220-M5L		WZP24440A7F
☑	C220-WZP24440...		Critical	UCSC-C220-M5L		WZP24440A6V

Selected 4 of 4 | Show Selected | Unselect All | 1 of 1

11. Edit the profile name prefix and click Next.



General

Organization * org-cohesity

Target Platform UCS Server (Standalone)

Description

<= 1024

Set Tags

Derive 4

Profile Name Prefix Cohesity-Sever-Template-1_DERIVED-

Start Index for Suffix 1

> 0

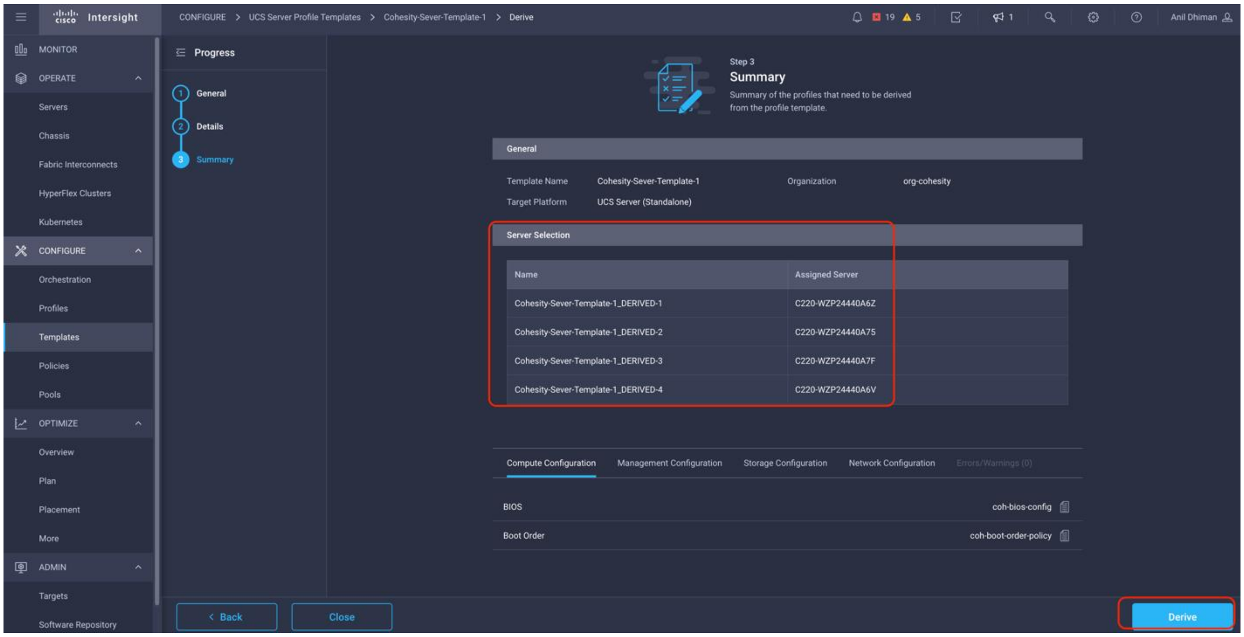
1 Name * Cohesity-Sever-Template-1_DERIVED-1 Assigne... C220-WZP24440A6Z

2 Name * Cohesity-Sever-Template-1_DERIVED-2 Assigne... C220-WZP24440A75

3 Name * Cohesity-Sever-Template-1_DERIVED-3 Assigne... C220-WZP24440A7F

4 Name * Cohesity-Sever-Template-1_DERIVED-4 Assigne... C220-WZP24440A6V

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



Step 3

Summary

Summary of the profiles that need to be derived from the profile template.

General

Template Name Cohesity-Sever-Template-1

Organization org-cohesity

Target Platform UCS Server (Standalone)

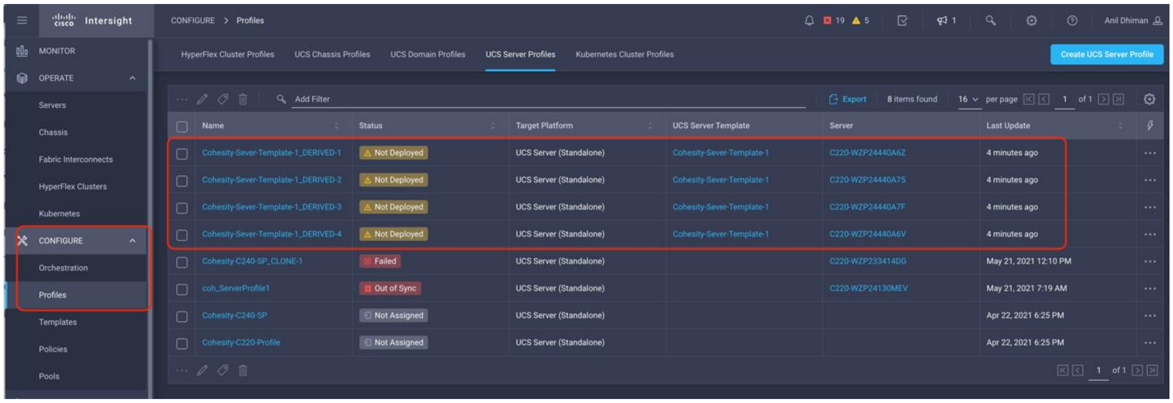
Server Selection

Name	Assigned Server
Cohesity-Sever-Template-1_DERIVED-1	C220-WZP24440A6Z
Cohesity-Sever-Template-1_DERIVED-2	C220-WZP24440A75
Cohesity-Sever-Template-1_DERIVED-3	C220-WZP24440A7F
Cohesity-Sever-Template-1_DERIVED-4	C220-WZP24440A6V

BIOS coh-bios-config

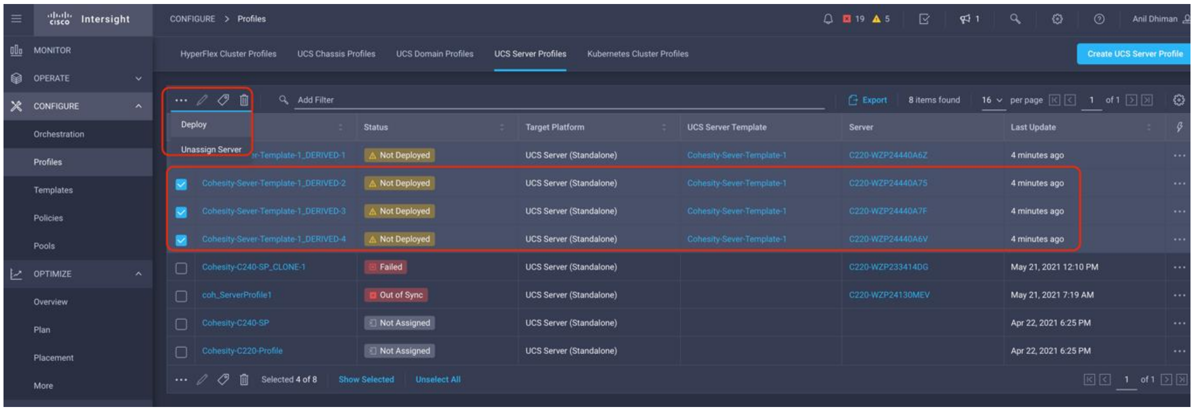
Boot Order coh-boot-order-policy

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



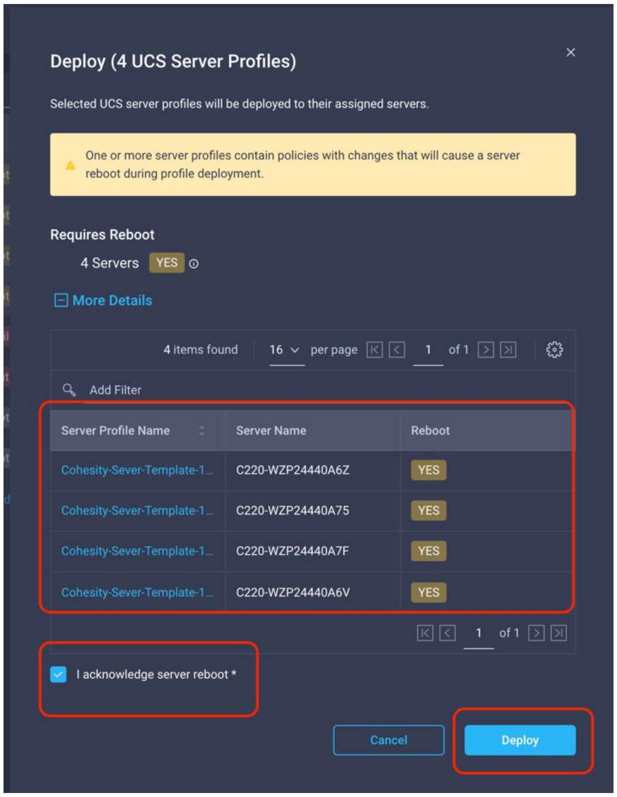
☐	Name	Status	Target Platform	UCS Server Template	Server	Last Update
☐	Cohesity-Sever-Template-1_DERIVED-1	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	4 minutes ago
☐	Cohesity-Sever-Template-1_DERIVED-2	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	4 minutes ago
☐	Cohesity-Sever-Template-1_DERIVED-3	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	4 minutes ago
☐	Cohesity-Sever-Template-1_DERIVED-4	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	4 minutes ago
☐	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
☐	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
☐	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
☐	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

14. Select the Cohesity profiles and click Deploy.



☐	Name	Status	Target Platform	UCS Server Template	Server	Last Update
	r-Template-1_DERIVED-1	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	4 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-2	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	4 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-3	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	4 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-4	⚠ Not Deployed	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	4 minutes ago
☐	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
☐	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
☐	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
☐	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

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


Deploy (4 UCS Server Profiles)

Selected UCS server profiles will be deployed to their assigned servers.

⚠ One or more server profiles contain policies with changes that will cause a server reboot during profile deployment.

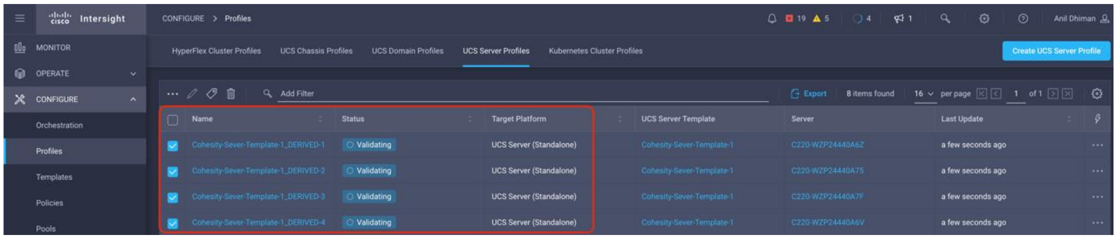
Requires Reboot

4 Servers YES

Server Profile Name	Server Name	Reboot
Cohesity-Sever-Template-1...	C220-WZP24440A6Z	YES
Cohesity-Sever-Template-1...	C220-WZP24440A75	YES
Cohesity-Sever-Template-1...	C220-WZP24440A7F	YES
Cohesity-Sever-Template-1...	C220-WZP24440A6V	YES

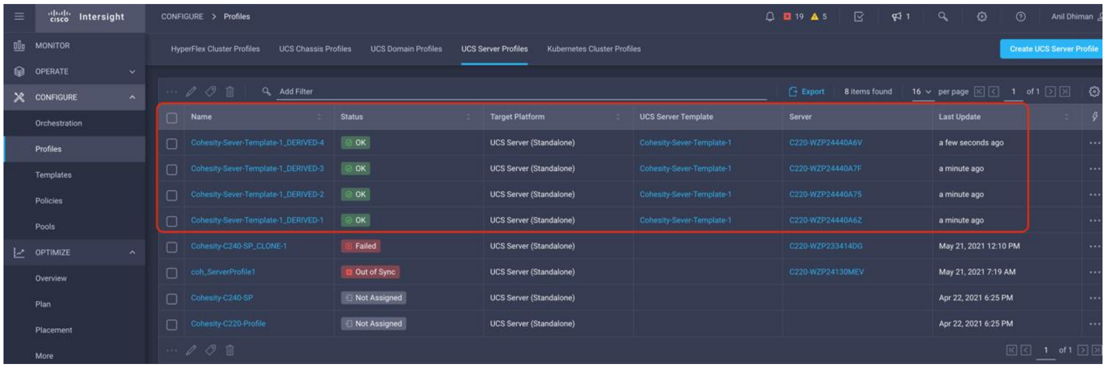
☑ I acknowledge server reboot *

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



	Name	Status	Target Platform	UCS Server Template	Server	Last Update
☑	Cohesity-Sever-Template-1_DERIVED-1	Validating	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-2	Validating	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-3	Validating	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-4	Validating	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	a few seconds ago

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.



	Name	Status	Target Platform	UCS Server Template	Server	Last Update
□	Cohesity-Sever-Template-1_DERIVED-4	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	a few seconds ago
□	Cohesity-Sever-Template-1_DERIVED-3	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	a minute ago
□	Cohesity-Sever-Template-1_DERIVED-2	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	a minute ago
□	Cohesity-Sever-Template-1_DERIVED-1	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	a minute ago
□	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
□	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
□	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
□	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

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 Cohesity 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

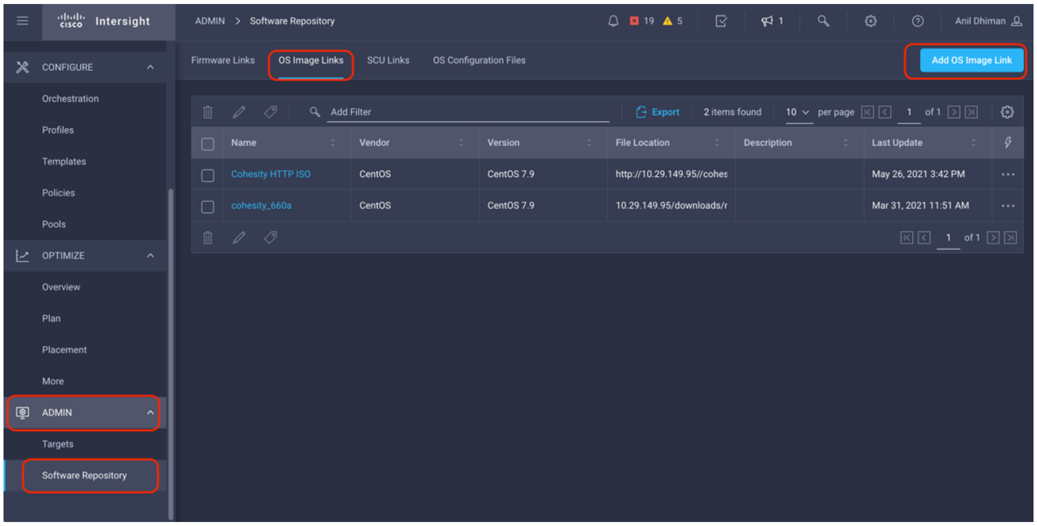
The Cisco Intersight platform introduces the capability to install vMedia-based operating systems on the managed servers in your data center. With this capability, you can perform an unattended OS installation on one or more Cisco UCS C-Series standalone servers from your central data center through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

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 Operating System Installation Guide.

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.

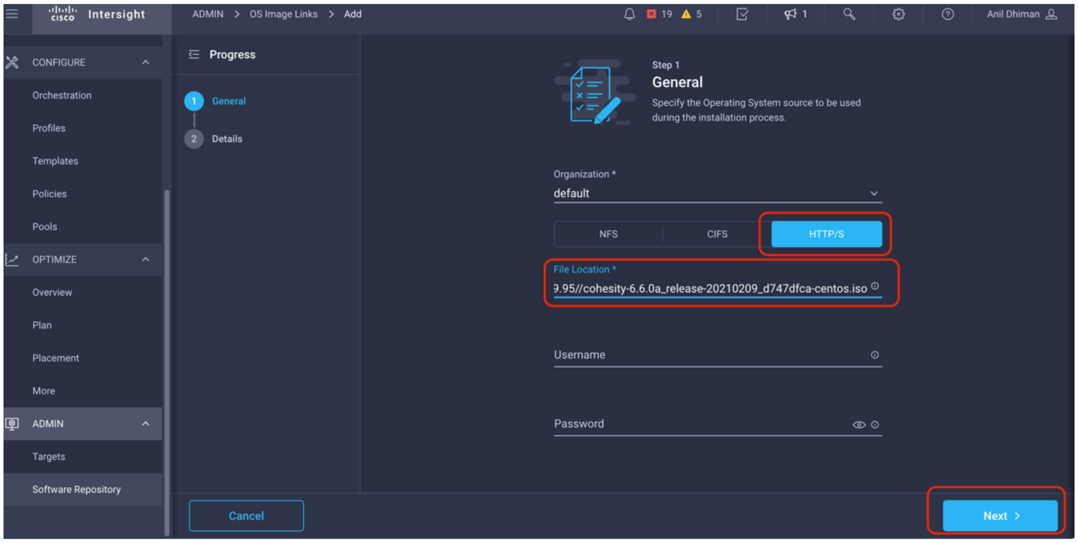
Follow the high-level procedure presented here to install a Cohesity ISO file on Cisco UCS C220 and C240 Rack Servers:

1. Add the OS Image Link option in the Cisco Intersight Software Repository:
    - Log in to the Cisco Intersight platform at [https://intersight.com/.](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.



Name	Vendor	Version	File Location	Description	Last Update
Cohesity HTTP ISO	CentOS	CentOS 7.9	http://10.29.149.95//cohes		May 26, 2021 3:42 PM
cohesity_660a	CentOS	CentOS 7.9	10.29.149.95/downloads/r		Mar 31, 2021 11:51 AM

    - 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.



Step 1

General

Specify the Operating System source to be used during the installation process.

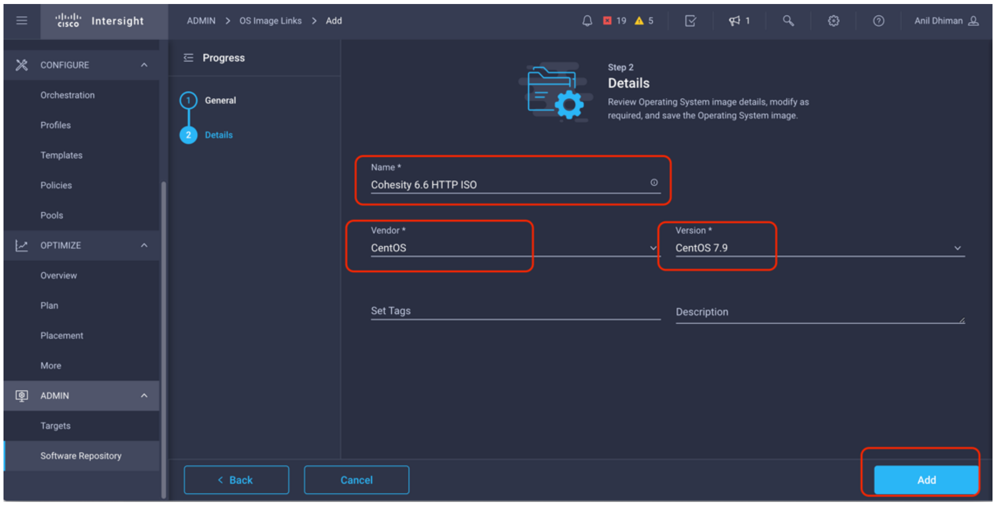
Organization * default

File Location * 9.95//cohesity-6.6.0a_release-20210209_d747dfca-centos.iso

Username

Password

    - 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.



Step 2
Details
Review Operating System image details, modify as required, and save the Operating System image.

Name * Cohesity 6.6 HTTP ISO

Vendor * CentOS

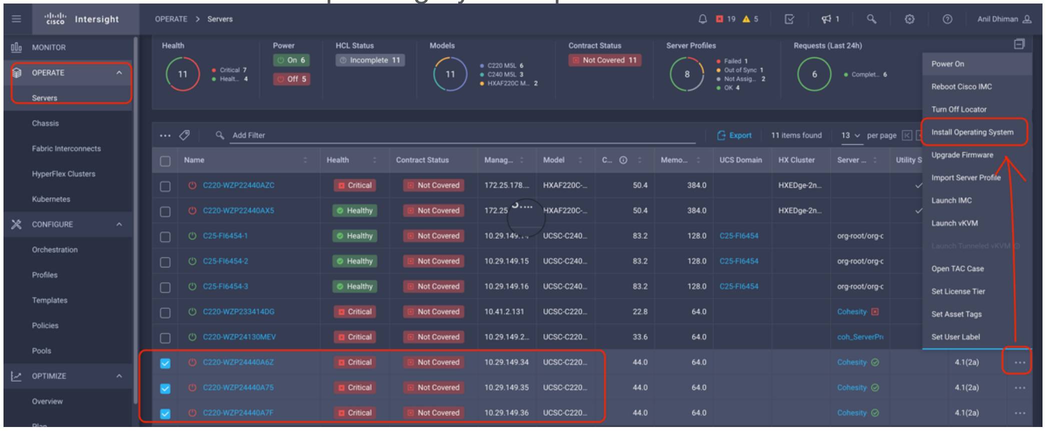
Version * CentOS 7.9

Set Tags

Description

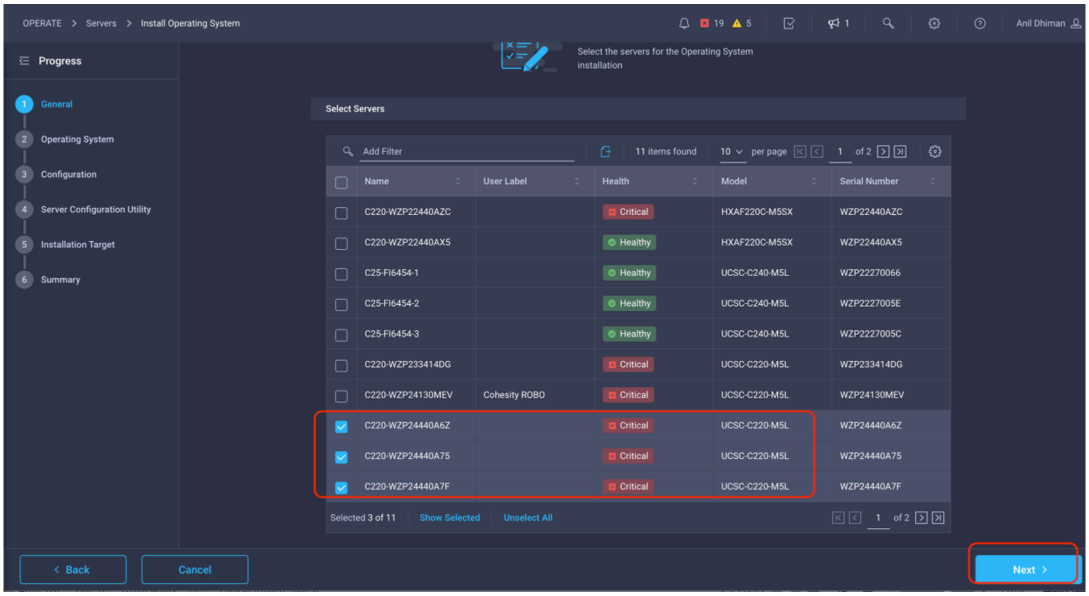
2. Install the Cohesity operating system. Verify that the Cisco Intersight license tier is set to at least the Advantage tier.

- 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.



☐	Name	Health	Contract Status	Manag...	Model	C...	Memo...	UCS Domain	HX Cluster	Server ...	Utility S		
☐	C220-WZP22440AZC	Critical	Not Covered	172.25.178....	HXAF220C-...	50.4	384.0		HXEDge-2n...		✓		
☐	C220-WZP22440AX5	Healthy	Not Covered	172.25...	HXAF220C-...	50.4	384.0		HXEDge-2n...		✓		
☐	C25-FI6454-1	Healthy	Not Covered	10.29.149....	UCSC-C240...	83.2	128.0	C25-FI6454		org-root/org-c			
☐	C25-FI6454-2	Healthy	Not Covered	10.29.149.15	UCSC-C240...	83.2	128.0	C25-FI6454		org-root/org-c			
☐	C25-FI6454-3	Healthy	Not Covered	10.29.149.16	UCSC-C240...	83.2	128.0	C25-FI6454		org-root/org-c			
☐	C220-WZP233414DG	Critical	Not Covered	10.41.2.131	UCSC-C220...	22.8	64.0			Cohesity ☒			
☐	C220-WZP24130MEV	Critical	Not Covered	10.29.149.2...	UCSC-C220...	33.6	64.0			coh_ServerPr			
☑	C220-WZP24440A6Z	Critical	Not Covered	10.29.149.34	UCSC-C220...	44.0	64.0			Cohesity ✓		4.1(2a)	...
☑	C220-WZP24440A75	Critical	Not Covered	10.29.149.35	UCSC-C220...	44.0	64.0			Cohesity ✓		4.1(2a)	...
☑	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.



Select the servers for the Operating System installation

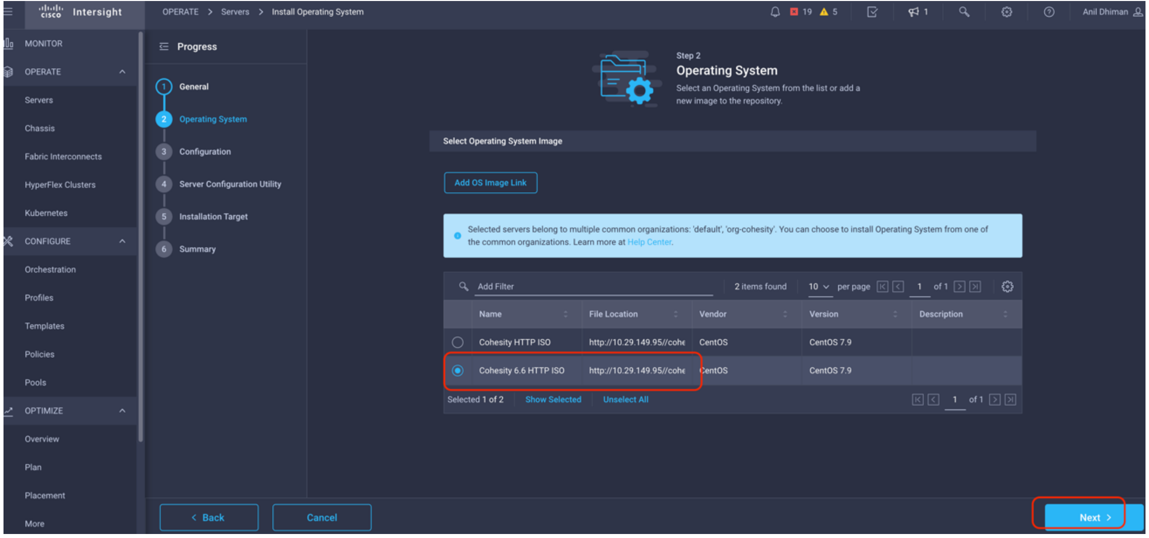
Select Servers

Add Filter · 11 items found · 10 per page · 1 of 2

	Name	User Label	Health	Model	Serial Number
□	C220-WZP22440AZC		Critical	HXAF220C-M5SX	WZP22440AZC
□	C220-WZP22440AX5		Healthy	HXAF220C-M5SX	WZP22440AX5
□	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		Critical	UCSC-C220-M5L	WZP233414DG
□	C220-WZP24130MEV	Cohesity ROBO	Critical	UCSC-C220-M5L	WZP24130MEV
☑	C220-WZP24440A6Z		Critical	UCSC-C220-M5L	WZP24440A6Z
☑	C220-WZP24440A75		Critical	UCSC-C220-M5L	WZP24440A75
☑	C220-WZP24440A7F		Critical	UCSC-C220-M5L	WZP24440A7F

Selected 3 of 11 · Show Selected · Unselect All · 1 of 2

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



Step 2

Operating System

Select an Operating System from the list or add a new image to the repository.

Select Operating System Image

Add OS Image Link

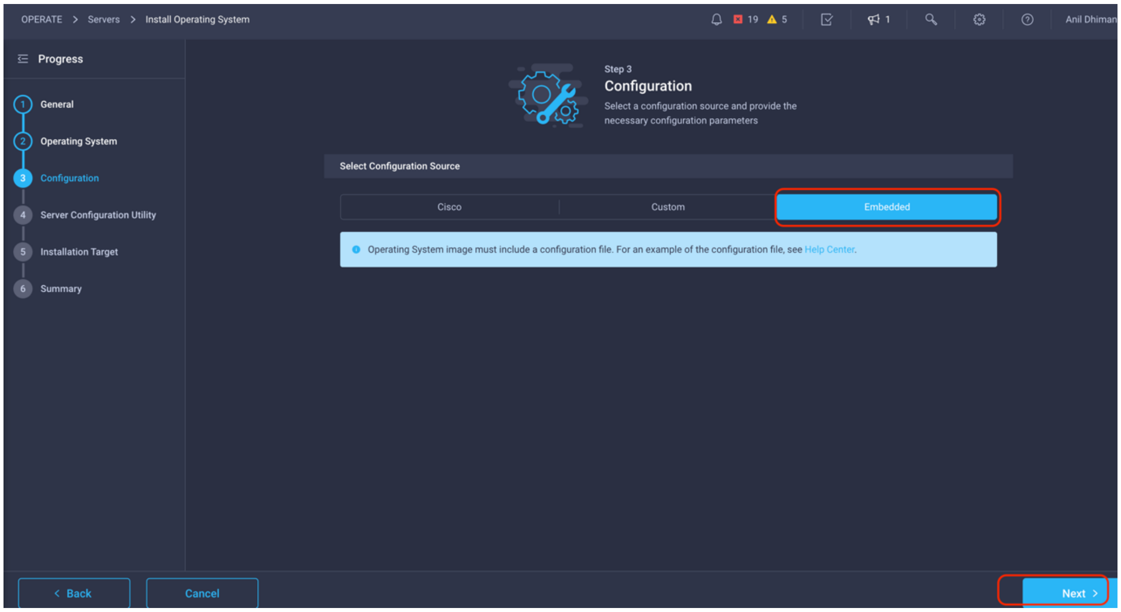
Selected servers belong to multiple common organizations: 'default', 'org-cohesity'. You can choose to install Operating System from one of the common organizations. Learn more at Help Center.

Add Filter · 2 items found · 10 per page · 1 of 1

	Name	File Location	Vendor	Version	Description
○	Cohesity HTTP ISO	http://10.29.149.95//cohe	CentOS	CentOS 7.9	
●	Cohesity 6.6 HTTP ISO	http://10.29.149.95//cohe	CentOS	CentOS 7.9	

Selected 1 of 2 · Show Selected · Unselect All · 1 of 1

- Select the Embedded tab and click Next.



Step 3

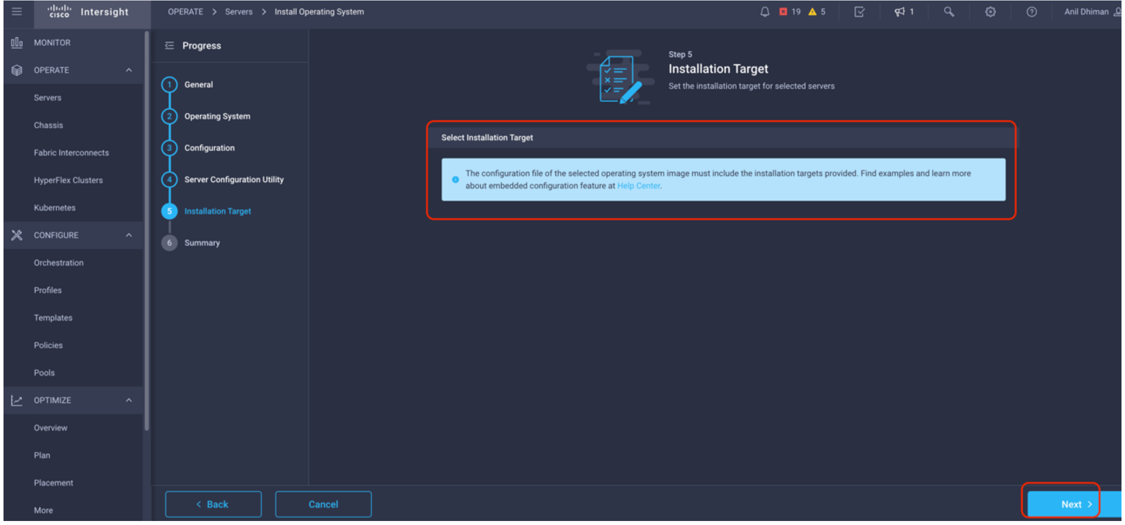
Configuration

Select a configuration source and provide the necessary configuration parameters

Select Configuration Source

Operating System image must include a configuration file. For an example of the configuration file, see Help Center.

- 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.



Step 5

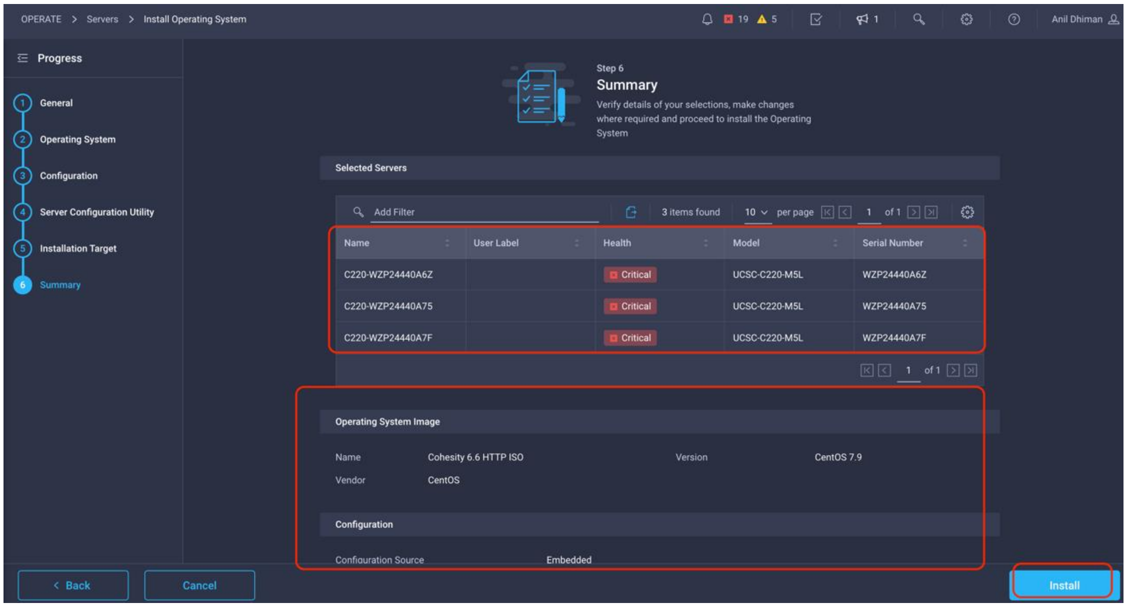
Installation Target

Set the installation target for selected servers

Select Installation Target

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.

- 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

Progress

1. General
2. Operating System
3. Configuration
4. Server Configuration Utility
5. Installation Target
6. Summary

Step 6

Summary

Verify details of your selections, make changes where required and proceed to install the Operating System

Selected Servers

3 items found · 10 per page · 1 of 1

Name	User Label	Health	Model	Serial Number
C220-WZP24440A6Z		Critical	UCSC-C220-M5L	WZP24440A6Z
C220-WZP24440A75		Critical	UCSC-C220-M5L	WZP24440A75
C220-WZP24440A7F		Critical	UCSC-C220-M5L	WZP24440A7F

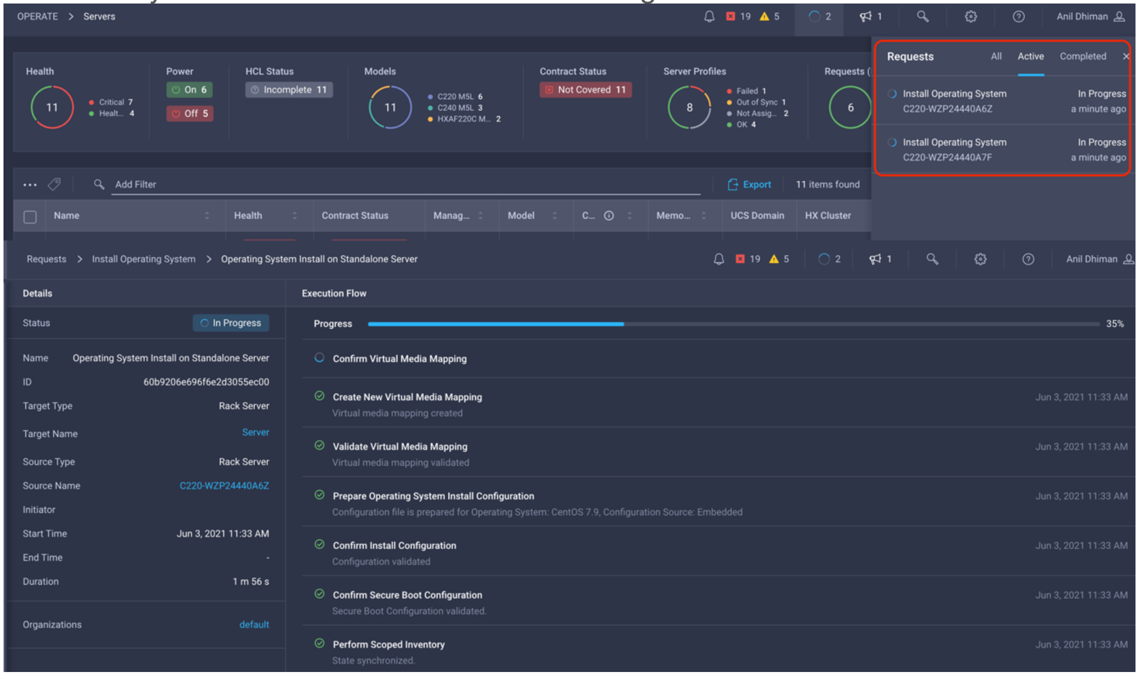
Operating System Image

Name	Cohesity 6.6 HTTP ISO	Version	CentOS 7.9
Vendor	CentOS		

Configuration

Configuration Source: Embedded

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



OPERATE > Servers

Health 11 (Critical 7, Healt... 4) · Power: On 6, Off 5 · HCL Status: Incomplete 11 · Models 11 (C220 M5L 6, C240 M5L 3, HXAF220C M... 2) · Contract Status: Not Covered 11 · Server Profiles 8 (Failed 1, Out of Sync 1, Not Assig... 2, OK 4) · Requests 6

Requests — All | Active | Completed

Install Operating System C220-WZP24440A6Z	In Progress a minute ago
Install Operating System C220-WZP24440A7F	In Progress a minute ago

Add Filter · Export · 11 items found

Name	Health	Contract Status	Manag...	Model	C...	Memo...	UCS Domain	HX Cluster

Requests > Install Operating System > Operating System Install on Standalone Server

Details

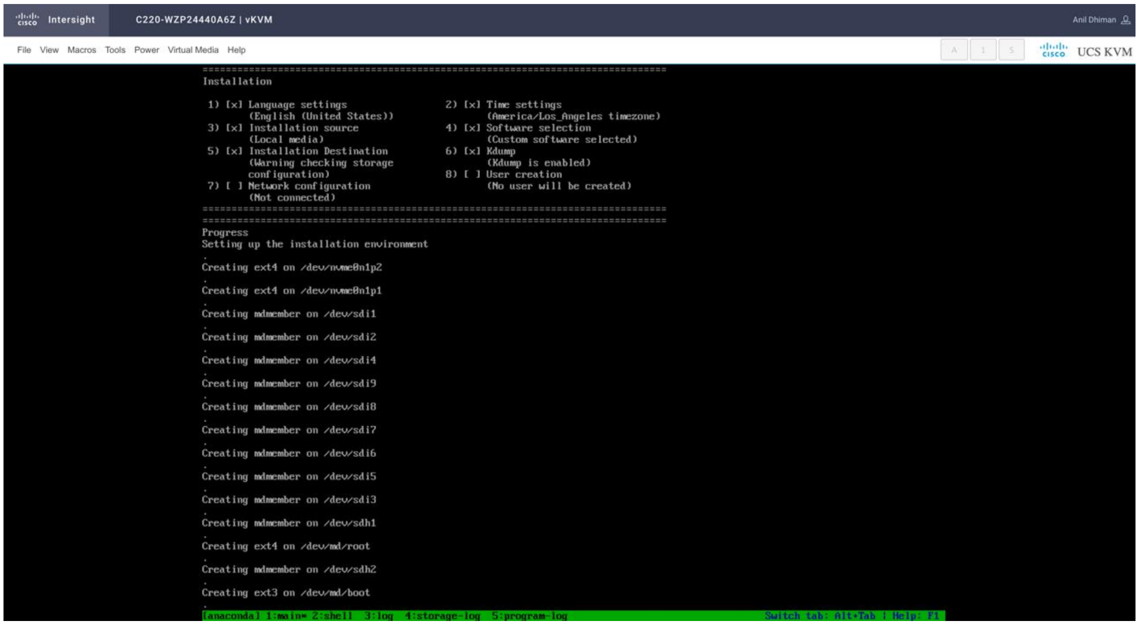
Status	In Progress
Name	Operating System Install on Standalone Server
ID	60b9206e696f6e2d3055ec00
Target Type	Rack Server
Target Name	Server
Source Type	Rack Server
Source Name	C220-WZP24440A6Z
Initiator	
Start Time	Jun 3, 2021 11:33 AM
End Time	-
Duration	1 m 56 s
Organizations	default

Execution Flow

Progress 35%

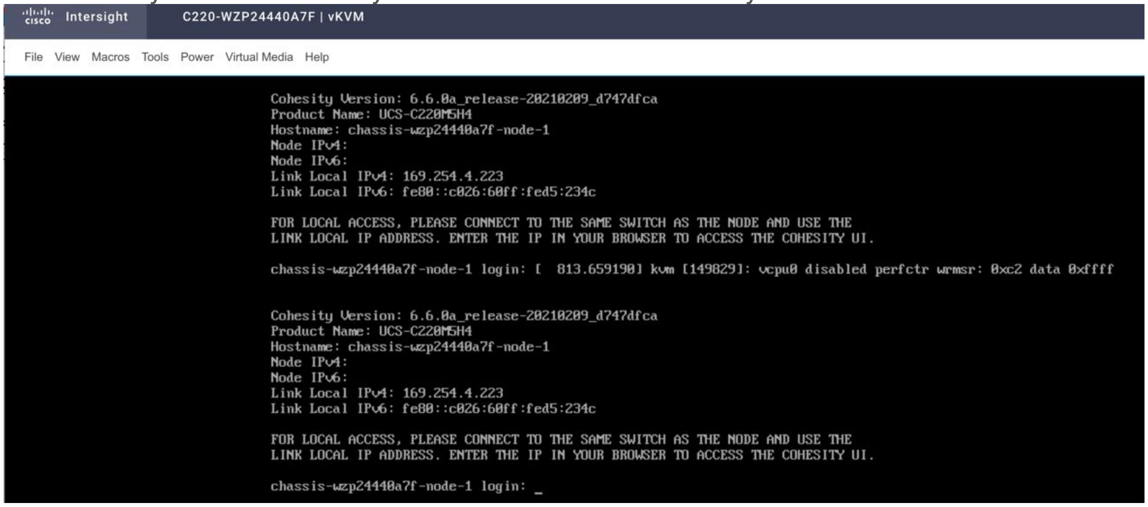
- Confirm Virtual Media Mapping
- Create New Virtual Media Mapping — Virtual media mapping created — Jun 3, 2021 11:33 AM
- Validate Virtual Media Mapping — Virtual media mapping validated — Jun 3, 2021 11:33 AM
- Prepare Operating System Install Configuration — Configuration file is prepared for Operating System: CentOS 7.9, Configuration Source: Embedded — Jun 3, 2021 11:33 AM
- Confirm Install Configuration — Configuration validated — Jun 3, 2021 11:33 AM
- Confirm Secure Boot Configuration — Secure Boot Configuration validated. — Jun 3, 2021 11:33 AM
- Perform Scoped Inventory — State synchronized. — Jun 3, 2021 11:33 AM

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



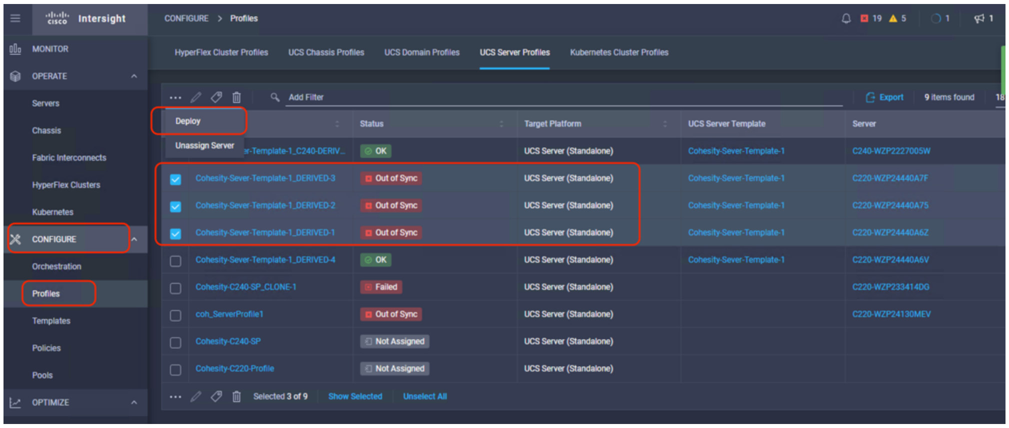
```
================================================================================
Installation

 1) [x] Language settings                 2) [x] Time settings
        (English (United States))                (America/Los_Angeles timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            (Custom software selected)
 5) [x] Installation Destination          6) [x] Kdump
        (Warning checking storage                (Kdump is enabled)
        configuration)                    8) [ ] User creation
 7) [ ] Network configuration                    (No user will be created)
        (Not connected)
================================================================================
================================================================================
Progress
Setting up the installation environment
.
Creating ext4 on /dev/nvme0n1p2
.
Creating ext4 on /dev/nvme0n1p1
.
Creating mdmember on /dev/sdi1
.
Creating mdmember on /dev/sdi2
.
Creating mdmember on /dev/sdi4
.
Creating mdmember on /dev/sdi9
.
Creating mdmember on /dev/sdi8
.
Creating mdmember on /dev/sdi7
.
Creating mdmember on /dev/sdi6
.
Creating mdmember on /dev/sdi5
.
Creating mdmember on /dev/sdi3
.
Creating mdmember on /dev/sdh1
.
Creating ext4 on /dev/md/root
.
Creating mdmember on /dev/sdh2
.
Creating ext3 on /dev/md/boot
.
[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log              Switch tab: Alt+Tab | Help: F1
```

- Verify that the Cohesity OS was installed successfully.



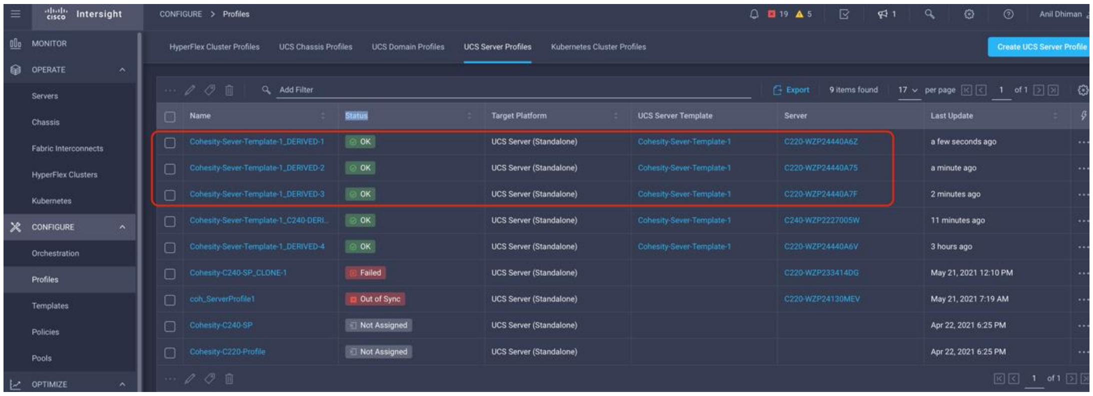
```
Cohesity Version: 6.6.0a_release-20210209_d747dfca
Product Name: UCS-C220M5H4
Hostname: chassis-wzp24440a7f-node-1
Node IPv4:
Node IPv6:
Link Local IPv4: 169.254.4.223
Link Local IPv6: fe80::c026:60ff:fed5:234c

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: 6.6.0a_release-20210209_d747dfca
Product Name: UCS-C220M5H4
Hostname: chassis-wzp24440a7f-node-1
Node IPv4:
Node IPv6:
Link Local IPv4: 169.254.4.223
Link Local IPv6: fe80::c026:60ff: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: _
```

- 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.



	Name	Status	Target Platform	UCS Server Template	Server
	…r-Template-1_C240-DERIV…	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C240-WZP2227005W
☑	Cohesity-Sever-Template-1_DERIVED-3	Out of Sync	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F
☑	Cohesity-Sever-Template-1_DERIVED-2	Out of Sync	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75
☑	Cohesity-Sever-Template-1_DERIVED-1	Out of Sync	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z
□	Cohesity-Sever-Template-1_DERIVED-4	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V
□	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG
□	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV
□	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)		
□	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)		

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



	Name	Status	Target Platform	UCS Server Template	Server	Last Update
□	Cohesity-Sever-Template-1_DERIVED-1	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	a few seconds ago
□	Cohesity-Sever-Template-1_DERIVED-2	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	a minute ago
□	Cohesity-Sever-Template-1_DERIVED-3	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	2 minutes ago
□	Cohesity-Sever-Template-1_C240-DERI…	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C240-WZP2227005W	11 minutes ago
□	Cohesity-Sever-Template-1_DERIVED-4	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	3 hours ago
□	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
□	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
□	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
□	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

- 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.

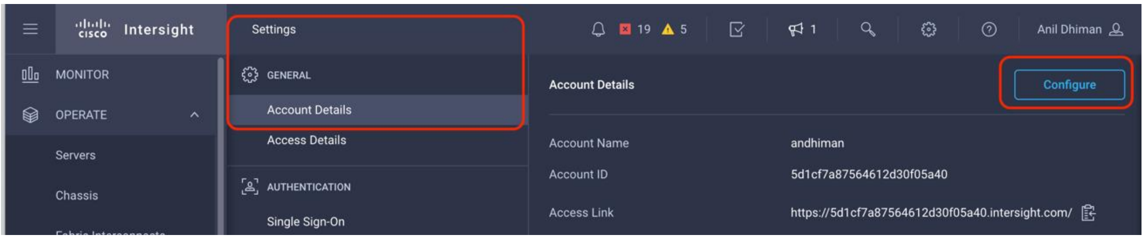
Extending vKVM timeout

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/.](https://intersight.com/)

2. Click the gear icon in the top-right corner and select Settings.

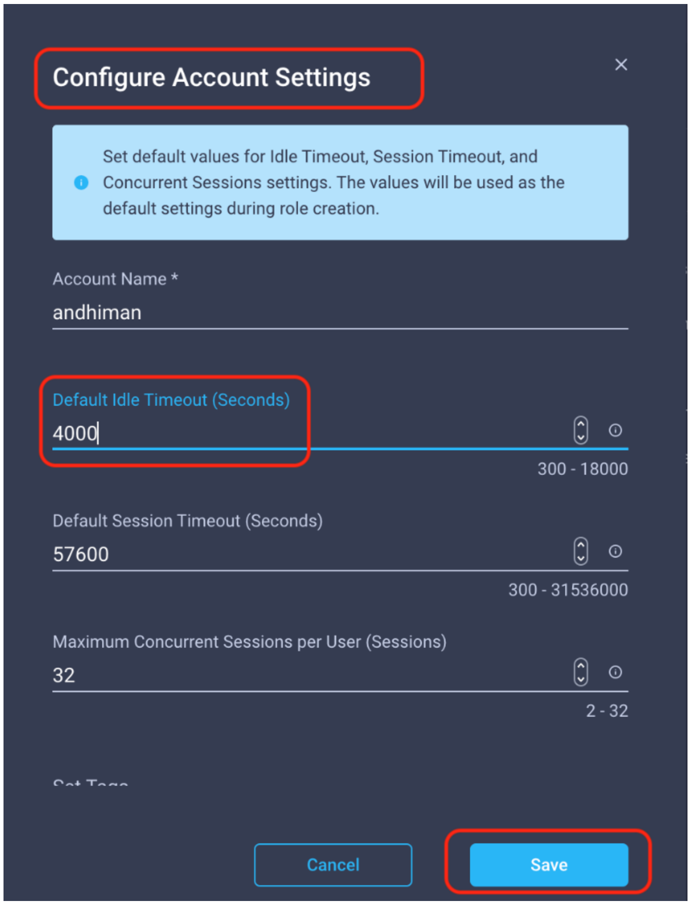
3. In the Account Details section, click Configure.



Account Details

Account Name andhiman
Account ID 5d1cf7a87564612d30f05a40
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.



Configure Account Settings

Set default values for Idle Timeout, Session Timeout, and Concurrent Sessions settings. The values will be used as the default settings during role creation.

Account Name *
andhiman

Default Idle Timeout (Seconds)
4000
300 - 18000

Default Session Timeout (Seconds)
57600
300 - 31536000

Maximum Concurrent Sessions per User (Sessions)
32
2 - 32

Set Tags

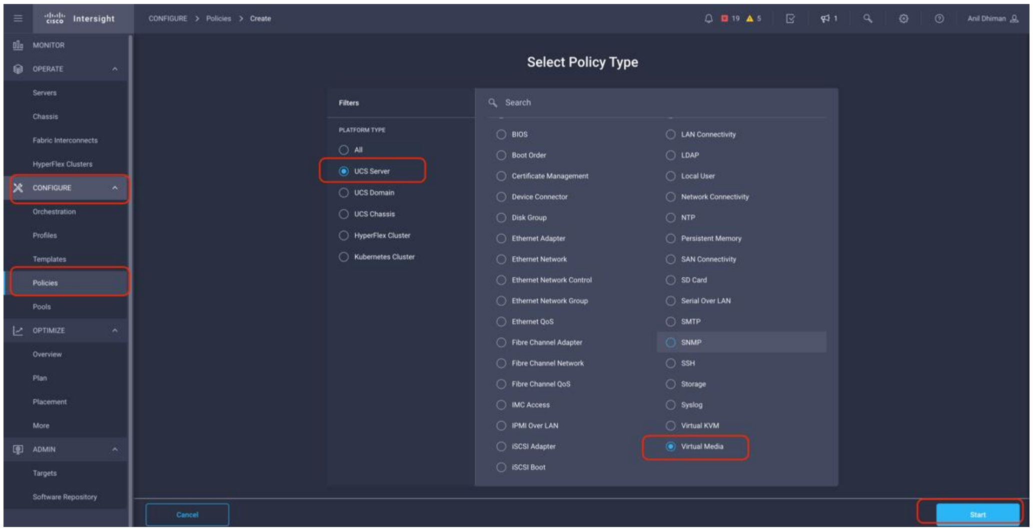
Creating and attaching a new vMedia policy to the server profile template

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

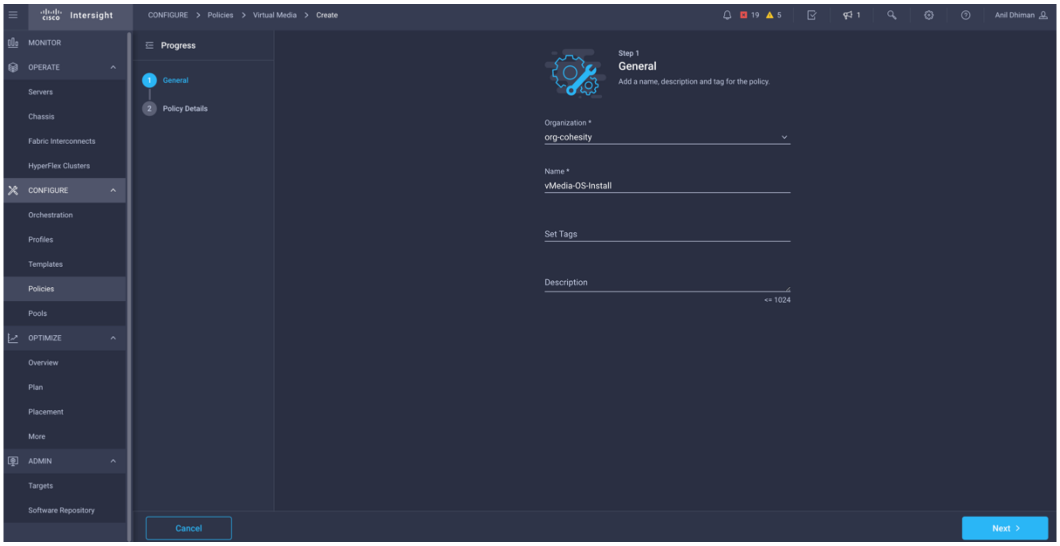
1. Log in to the Cisco Intersight platform at [https://intersight.com/.](https://intersight.com/)

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.



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

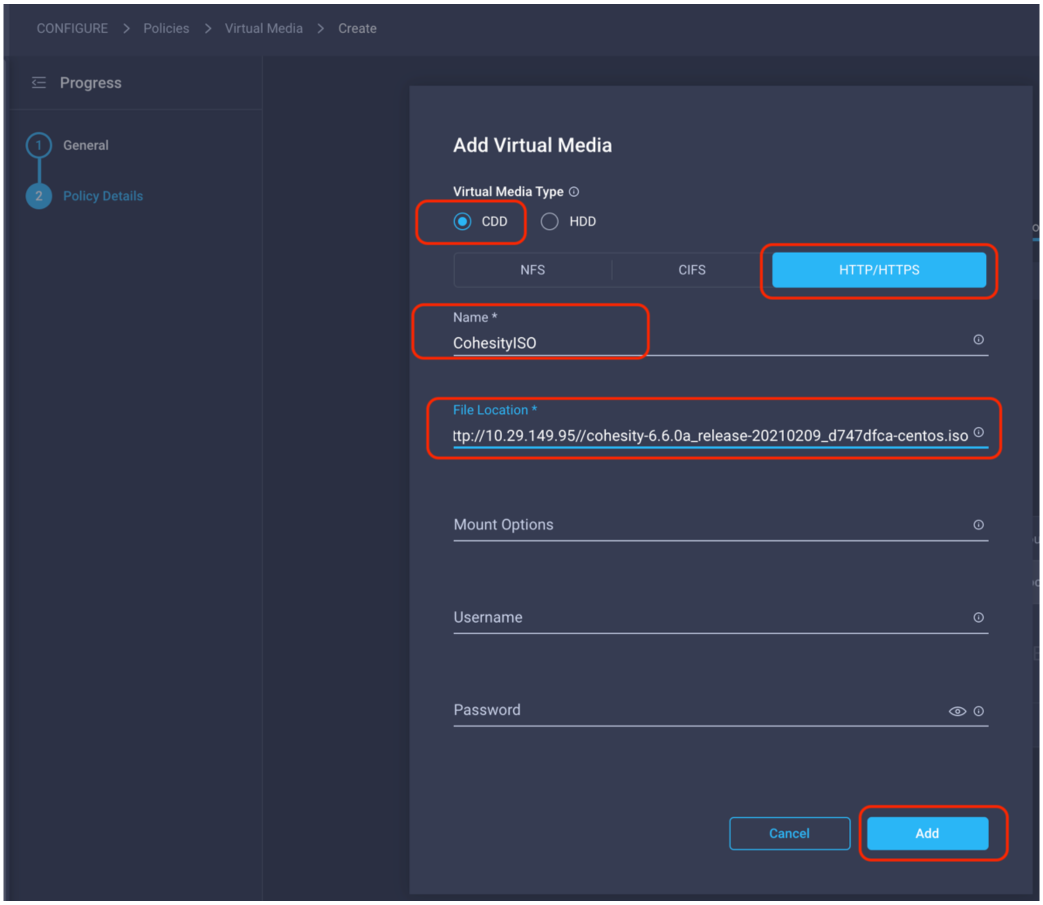


Organization * org-cohesity

Name * vMedia-OS-Install

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.



Add Virtual Media

Virtual Media Type: ● CDD ○ HDD

Name *: CohesityISO

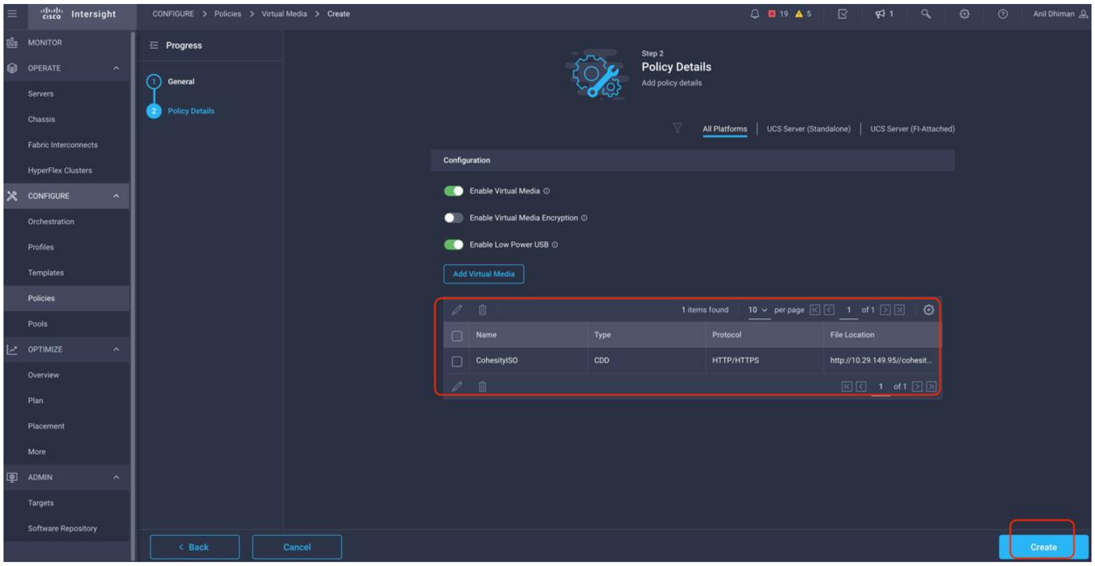
File Location *: ttp://10.29.149.95//cohesity-6.6.0a_release-20210209_d747dfca-centos.iso

Mount Options

Username

Password

7. Click Create to create the new vMedia policy.



Enable Virtual Media: on

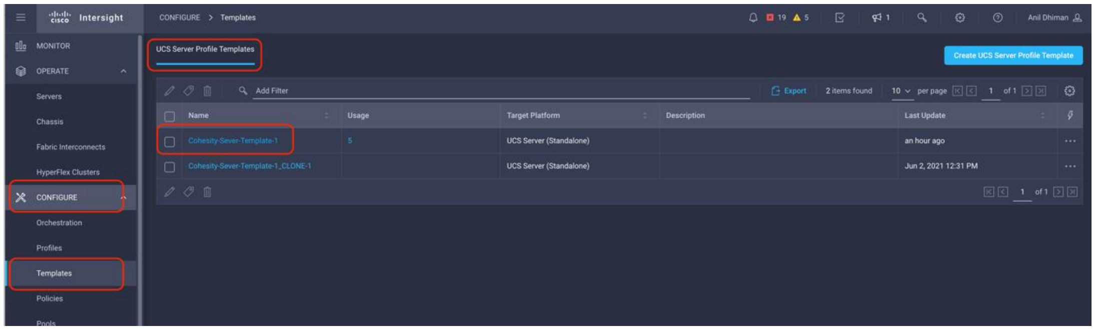
Enable Virtual Media Encryption: off

Enable Low Power USB: on

Name	Type	Protocol	File Location
CohesityISO	CDD	HTTP/HTTPS	http://10.29.149.95//cohesit...

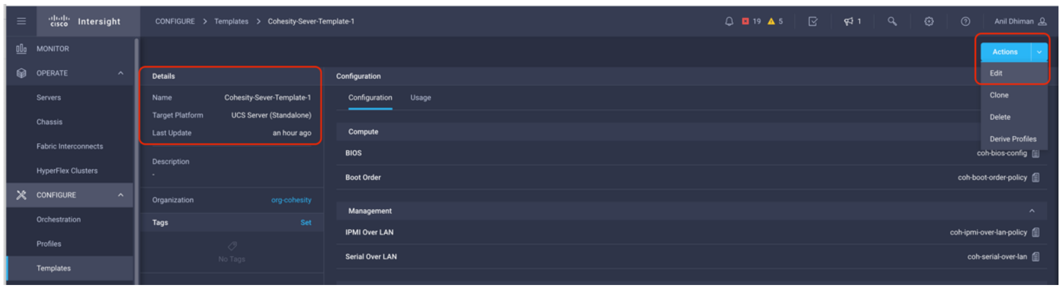
8. After the vMedia policy has been created, edit the server profile template to add the new vMedia policy.

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.



Name	Usage	Target Platform	Description	Last Update
Cohesity-Sever-Template-1	5	UCS Server (Standalone)		an hour ago
Cohesity-Sever-Template-1_CLONE-1		UCS Server (Standalone)		Jun 2, 2021 12:31 PM

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



Details

Name: Cohesity-Sever-Template-1
Target Platform: UCS Server (Standalone)
Last Update: an hour ago
Description: -
Organization: org-cohesity

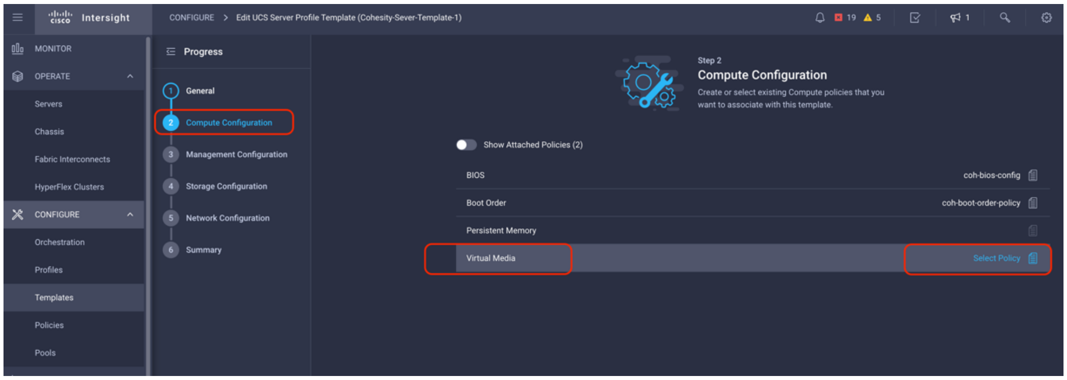
Compute

BIOS: coh-bios-config
Boot Order: coh-boot-order-policy

Management

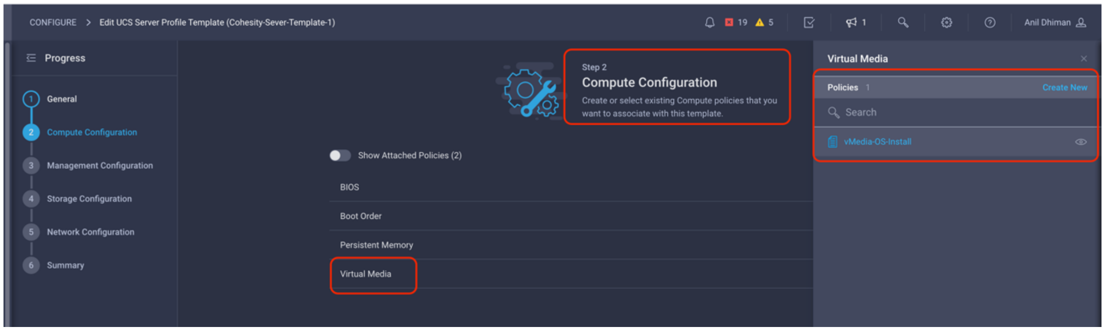
IPMI Over LAN: coh-ipmi-over-lan-policy
Serial Over LAN: coh-serial-over-lan

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

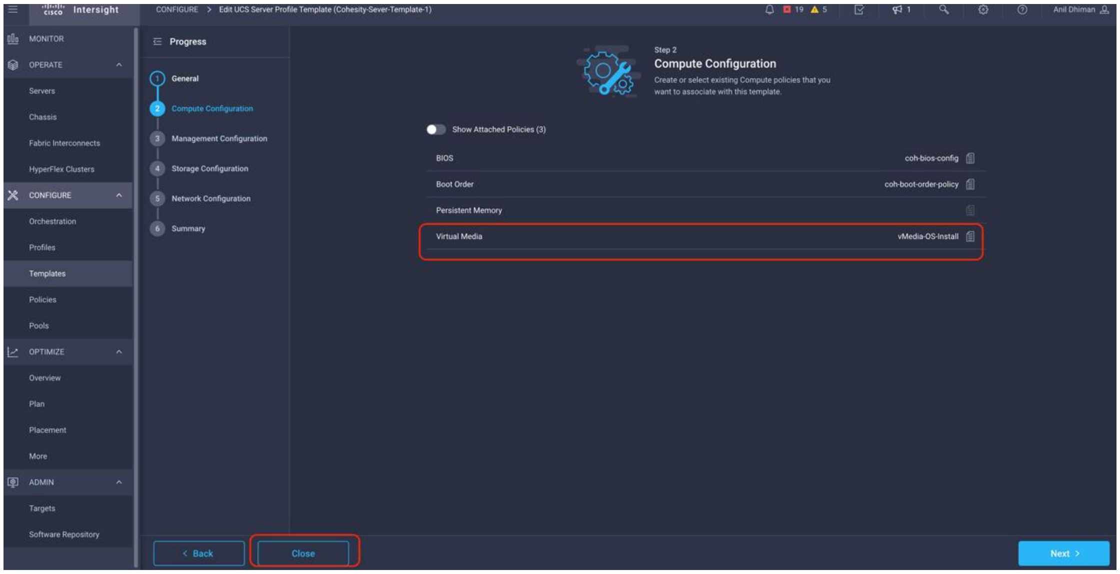


BIOS: coh-bios-config
Boot Order: coh-boot-order-policy
Persistent Memory
Virtual Media

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



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



Step 2

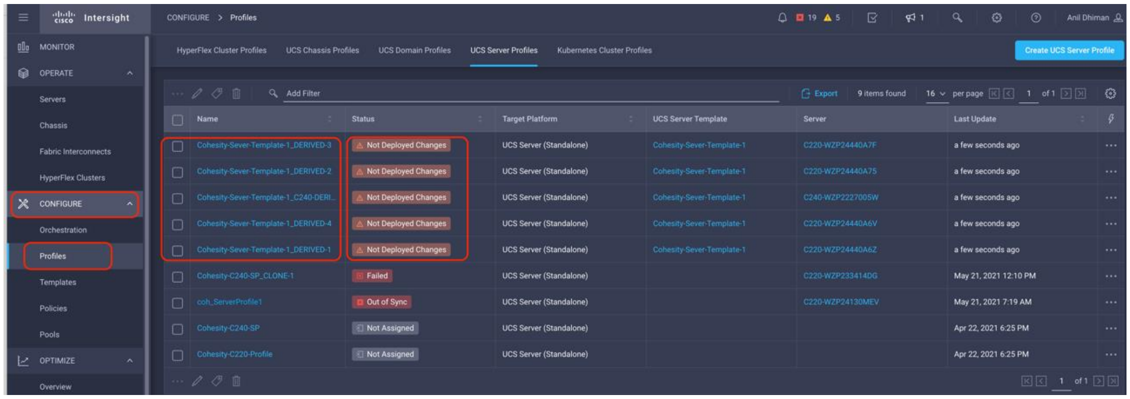
Compute Configuration

Create or select existing Compute policies that you want to associate with this template.

Show Attached Policies (3)

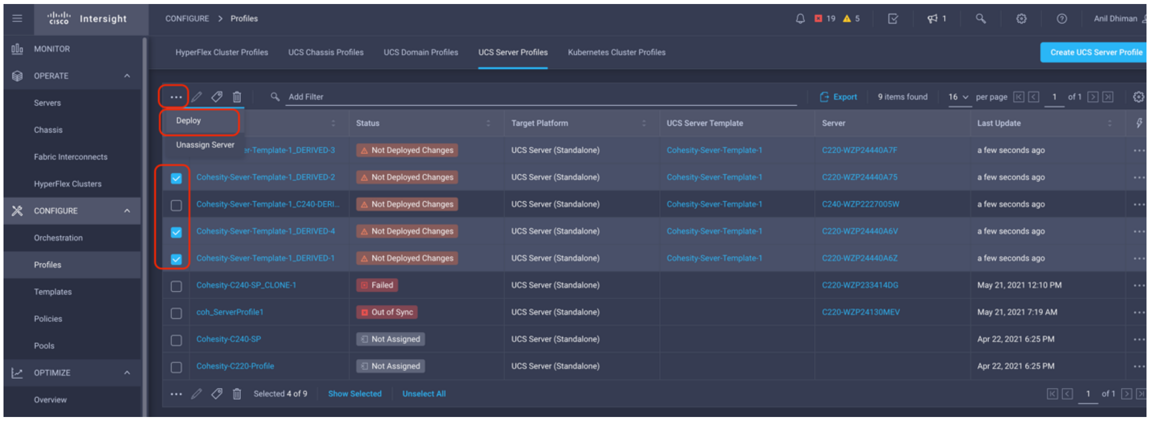
BIOS	coh-bios-config
Boot Order	coh-boot-order-policy
Persistent Memory	
Virtual Media	vMedia-OS-Install

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



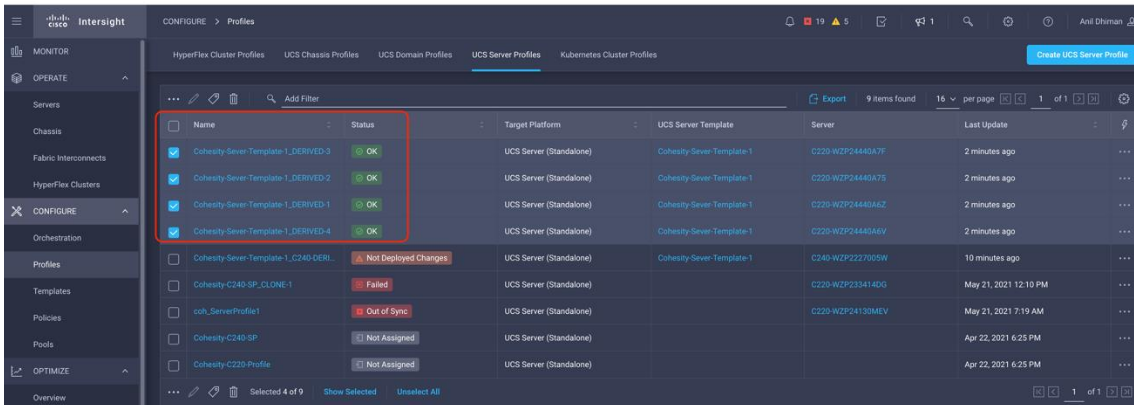
	Name	Status	Target Platform	UCS Server Template	Server	Last Update
□	Cohesity-Sever-Template-1_DERIVED-3	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	a few seconds ago
□	Cohesity-Sever-Template-1_DERIVED-2	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	a few seconds ago
□	Cohesity-Sever-Template-1_C240-DERI...	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C240-WZP2227005W	a few seconds ago
□	Cohesity-Sever-Template-1_DERIVED-4	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	a few seconds ago
□	Cohesity-Sever-Template-1_DERIVED-1	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	a few seconds ago
□	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
□	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
□	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
□	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

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.



	Name	Status	Target Platform	UCS Server Template	Server	Last Update
	...r-Template-1_DERIVED-3	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-2	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	a few seconds ago
□	Cohesity-Sever-Template-1_C240-DERI...	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C240-WZP2227005W	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-4	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	a few seconds ago
☑	Cohesity-Sever-Template-1_DERIVED-1	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	a few seconds ago
□	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
□	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
□	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
□	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

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.



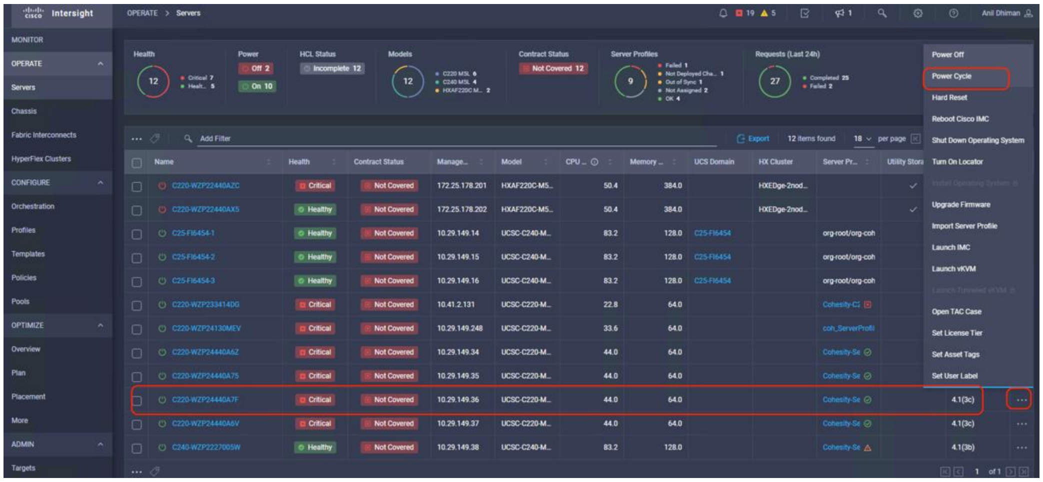
☐	Name	Status	Target Platform	UCS Server Template	Server	Last Update
☑	Cohesity-Sever-Template-1_DERIVED-3	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A7F	2 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-2	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A75	2 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-1	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6Z	2 minutes ago
☑	Cohesity-Sever-Template-1_DERIVED-4	OK	UCS Server (Standalone)	Cohesity-Sever-Template-1	C220-WZP24440A6V	2 minutes ago
☐	Cohesity-Sever-Template-1_C240-DERI...	Not Deployed Changes	UCS Server (Standalone)	Cohesity-Sever-Template-1	C240-WZP2227005W	10 minutes ago
☐	Cohesity-C240-SP_CLONE-1	Failed	UCS Server (Standalone)		C220-WZP233414DG	May 21, 2021 12:10 PM
☐	coh_ServerProfile1	Out of Sync	UCS Server (Standalone)		C220-WZP24130MEV	May 21, 2021 7:19 AM
☐	Cohesity-C240-SP	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM
☐	Cohesity-C220-Profile	Not Assigned	UCS Server (Standalone)			Apr 22, 2021 6:25 PM

Selected 4 of 9 Show Selected Unselect All

Installing the Cohesity OS through one-time boot device

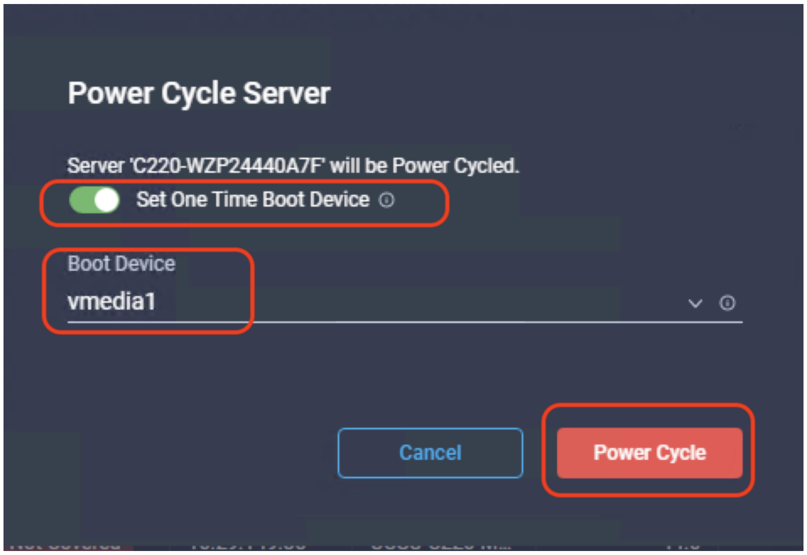
Follow these steps to install the Cohesity operating system through the one-time boot device feature:

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.



☐	Name	Health	Contract Status	Manage...	Model	CPU ...	Memory ...	UCS Domain	HX Cluster	Server Pr...	Utility Stora	
☐	C220-WZP22440AZC	Critical	Not Covered	172.25.178.201	HXAF220C-M5...	50.4	384.0		HXEDge-2nod...		✓	
☐	C220-WZP22440AX5	Healthy	Not Covered	172.25.178.202	HXAF220C-M5...	50.4	384.0		HXEDge-2nod...		✓	
☐	C25-FI6454-1	Healthy	Not Covered	10.29.149.14	UCSC-C240-M...	83.2	128.0	C25-FI6454		org-root/org-coh		
☐	C25-FI6454-2	Healthy	Not Covered	10.29.149.15	UCSC-C240-M...	83.2	128.0	C25-FI6454		org-root/org-coh		
☐	C25-FI6454-3	Healthy	Not Covered	10.29.149.16	UCSC-C240-M...	83.2	128.0	C25-FI6454		org-root/org-coh		
☐	C220-WZP233414DG	Critical	Not Covered	10.41.2.131	UCSC-C220-M...	22.8	64.0			Cohesity-C2		
☐	C220-WZP24130MEV	Critical	Not Covered	10.29.149.248	UCSC-C220-M...	33.6	64.0			coh_ServerProfil		
☐	C220-WZP24440A6Z	Critical	Not Covered	10.29.149.34	UCSC-C220-M...	44.0	64.0			Cohesity-Se		
☐	C220-WZP24440A75	Critical	Not Covered	10.29.149.35	UCSC-C220-M...	44.0	64.0			Cohesity-Se		
☐	C220-WZP24440A7F	Critical	Not Covered	10.29.149.36	UCSC-C220-M...	44.0	64.0			Cohesity-Se		4.1(3c)
☐	C220-WZP24440A6V	Critical	Not Covered	10.29.149.37	UCSC-C220-M...	44.0	64.0			Cohesity-Se		4.1(3c)
☐	C240-WZP2227005W	Healthy	Not Covered	10.29.149.38	UCSC-C240-M...	83.2	128.0			Cohesity-Se		4.1(3b)

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



Power Cycle Server

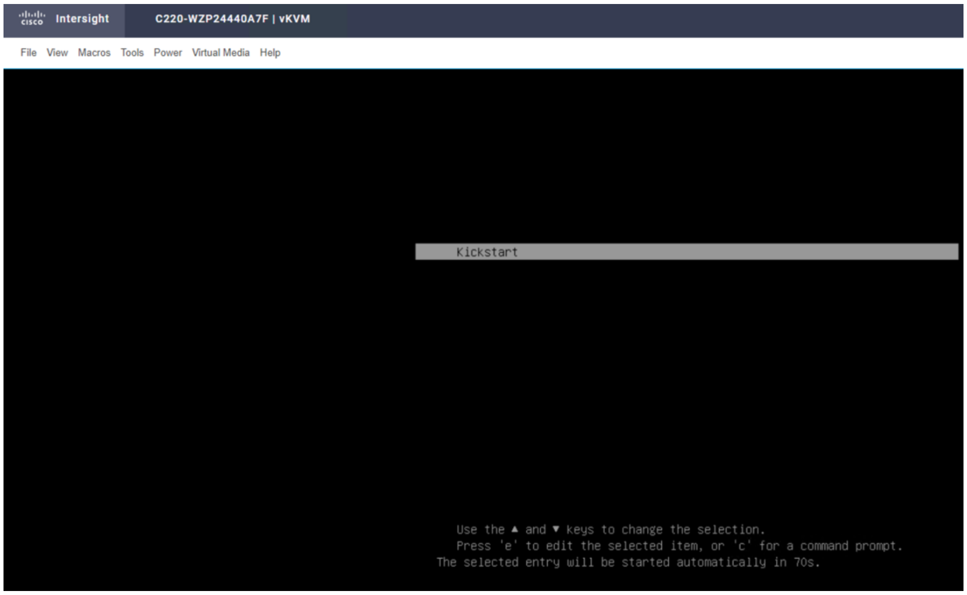
Server 'C220-WZP24440A7F' will be Power Cycled.

Set One Time Boot Device: on

Boot Device: vmedia1

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.



```
Kickstart

  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.

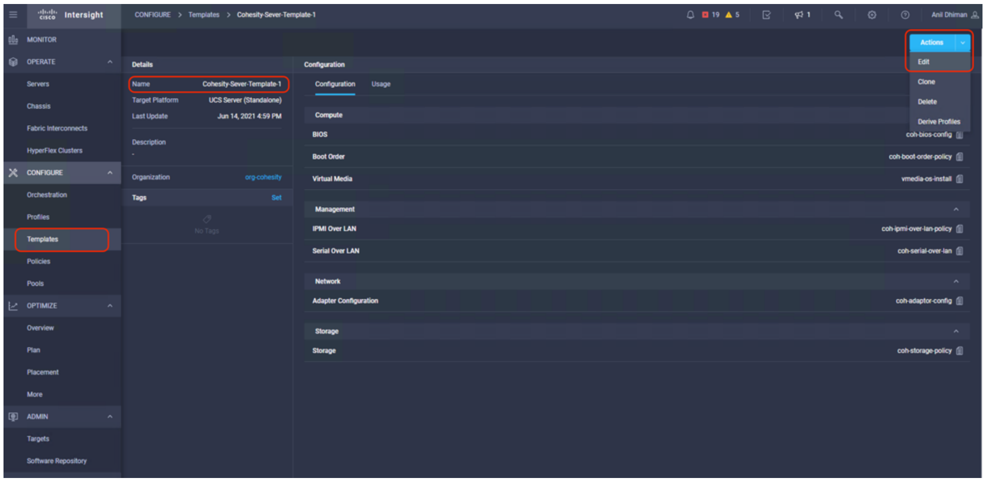
Remove the vMedia configuration from the server profile template

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/.](https://intersight.com/)

2. 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.



Details

Name Cohesity-Sever-Template-1

Target Platform UCS Server (Standalone)

Last Update Jun 14, 2021 4:59 PM

Description -

Organization org-cohesity

Tags Set

Configuration

Configuration Usage

Compute

BIOS coh-bios-config

Boot Order coh-boot-order-policy

Virtual Media vmedia-os-install

Management

IPMI Over LAN coh-ipmi-over-lan-policy

Serial Over LAN coh-serial-over-lan

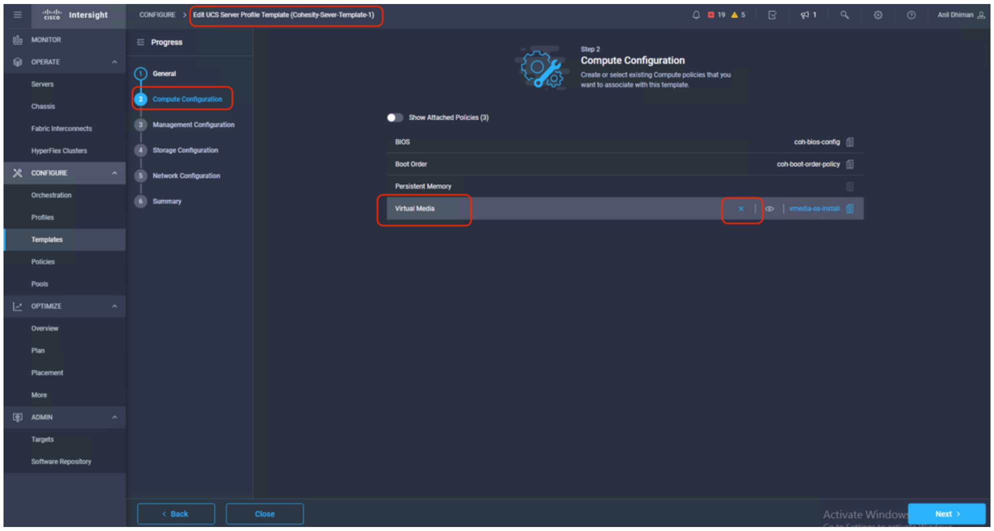
Network

Adapter Configuration coh-adaptor-config

Storage

Storage coh-storage-policy

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



Step 2

Compute Configuration

Create or select existing Compute policies that you want to associate with this template.

Show Attached Policies (3)

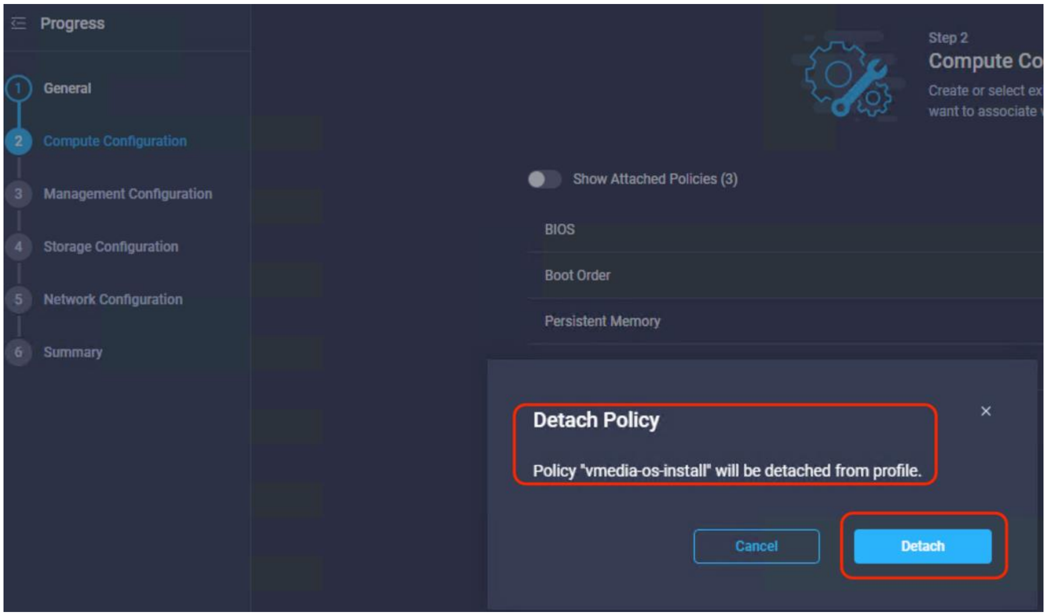
BIOS coh-bios-config

Boot Order coh-boot-order-policy

Persistent Memory

Virtual Media × vmedia-os-install

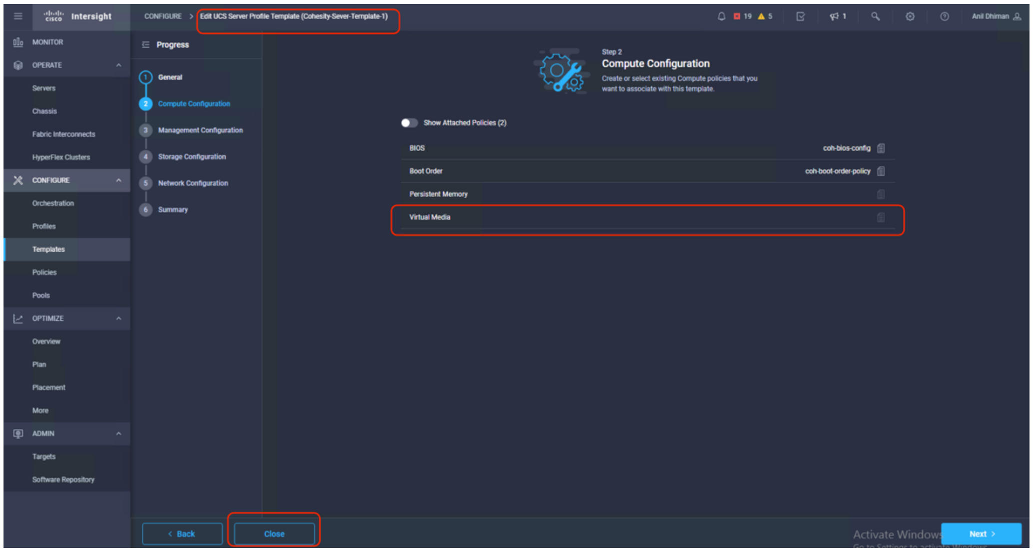
5. Confirm that you want to detach the vMedia server policy from the Cohesity server profile template.



Detach Policy

Policy "vmedia-os-install" will be detached from profile.

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



Edit UCS Server Profile Template (Cohesity-Sever-Template-1)

Step 2
Compute Configuration
Create or select existing Compute policies that you want to associate with this template.

BIOS	coh-bios-config
Boot Order	coh-boot-order-policy
Persistent Memory	
Virtual Media	

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 Firmware Management in Intersight and Upgrading UCS C-Series Standalone Servers Firmware.

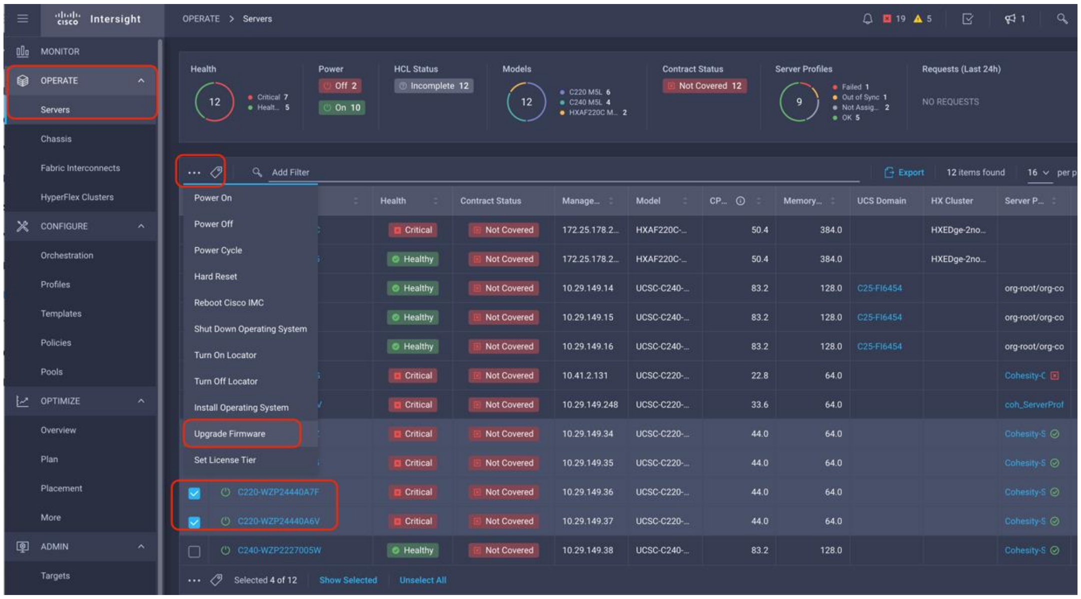
Firmware for Cisco UCS C-Series servers deployed with Cohesity DataPlatform can be upgraded as described here for the two main use cases:

- 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.

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

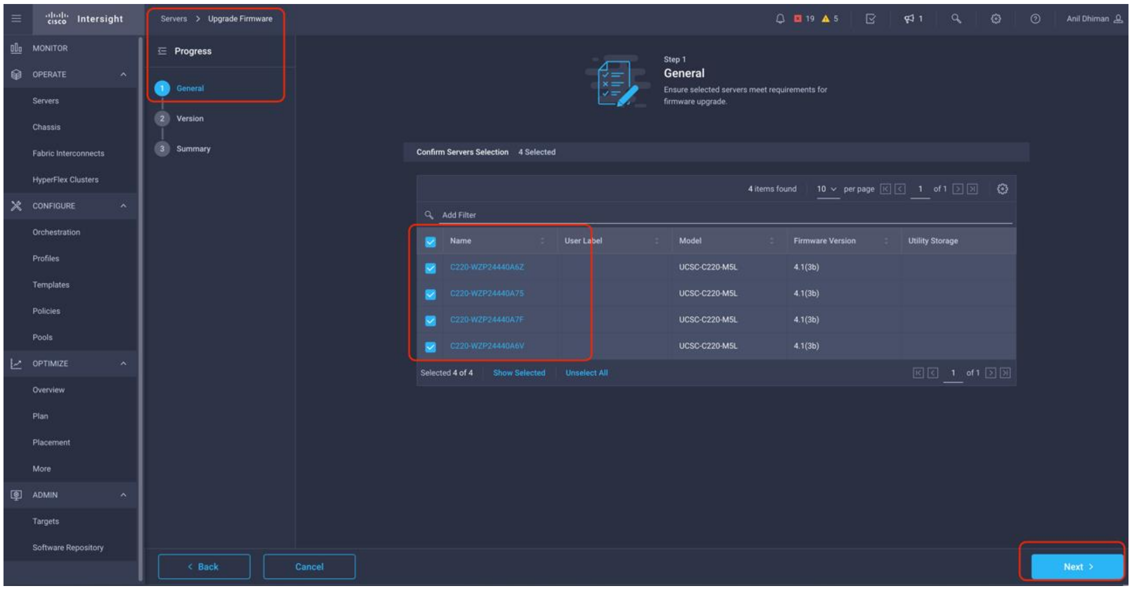


		Health	Contract Status	Manage...	Model	CP...	Memory...	UCS Domain	HX Cluster	Server P...
		Critical	Not Covered	172.25.178.2...	HXAF220C-...	50.4	384.0		HXEDge-2no...	
		Healthy	Not Covered	172.25.178.2...	HXAF220C-...	50.4	384.0		HXEDge-2no...	
		Healthy	Not Covered	10.29.149.14	UCSC-C240-...	83.2	128.0	C25-FI6454		org-root/org-co
		Healthy	Not Covered	10.29.149.15	UCSC-C240-...	83.2	128.0	C25-FI6454		org-root/org-co
		Healthy	Not Covered	10.29.149.16	UCSC-C240-...	83.2	128.0	C25-FI6454		org-root/org-co
		Critical	Not Covered	10.41.2.131	UCSC-C220-...	22.8	64.0			Cohesity-C
		Critical	Not Covered	10.29.149.248	UCSC-C220-...	33.6	64.0			coh_ServerProf
		Critical	Not Covered	10.29.149.34	UCSC-C220-...	44.0	64.0			Cohesity-S
		Critical	Not Covered	10.29.149.35	UCSC-C220-...	44.0	64.0			Cohesity-S
☑	C220-WZP24440A7F	Critical	Not Covered	10.29.149.36	UCSC-C220-...	44.0	64.0			Cohesity-S
☑	C220-WZP24440A6V	Critical	Not Covered	10.29.149.37	UCSC-C220-...	44.0	64.0			Cohesity-S
□	C240-WZP2227005W	Healthy	Not Covered	10.29.149.38	UCSC-C240-...	83.2	128.0			Cohesity-S

Selected 4 of 12 Show Selected Unselect All

4. On the Upgrade Firmware screen, click Start.

5. Verify that the correct nodes are selected for the firmware upgrade and click Next.



Ensure selected servers meet requirements for firmware upgrade.

Confirm Servers Selection 4 Selected

4 items found

☑	Name	User Label	Model	Firmware Version	Utility Storage
☑	C220-WZP24440A6Z		UCSC-C220-M5L	4.1(3b)	
☑	C220-WZP24440A75		UCSC-C220-M5L	4.1(3b)	
☑	C220-WZP24440A7F		UCSC-C220-M5L	4.1(3b)	
☑	C220-WZP24440A6V		UCSC-C220-M5L	4.1(3b)	

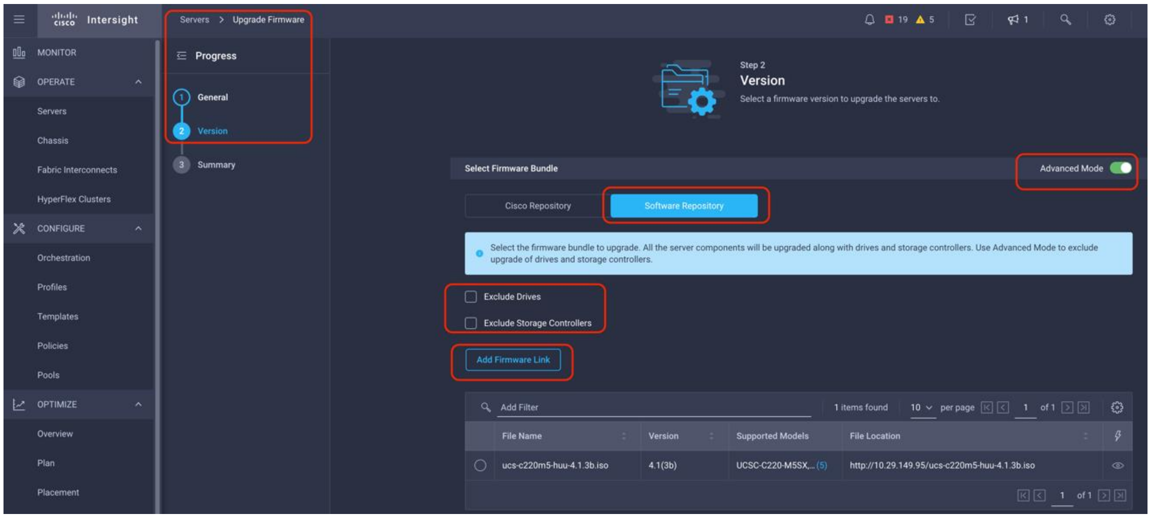
Selected 4 of 4 Show Selected Unselect All

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.

9. 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.



Step 2

Version

Select a firmware version to upgrade the servers to.

Select Firmware Bundle

Advanced Mode

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

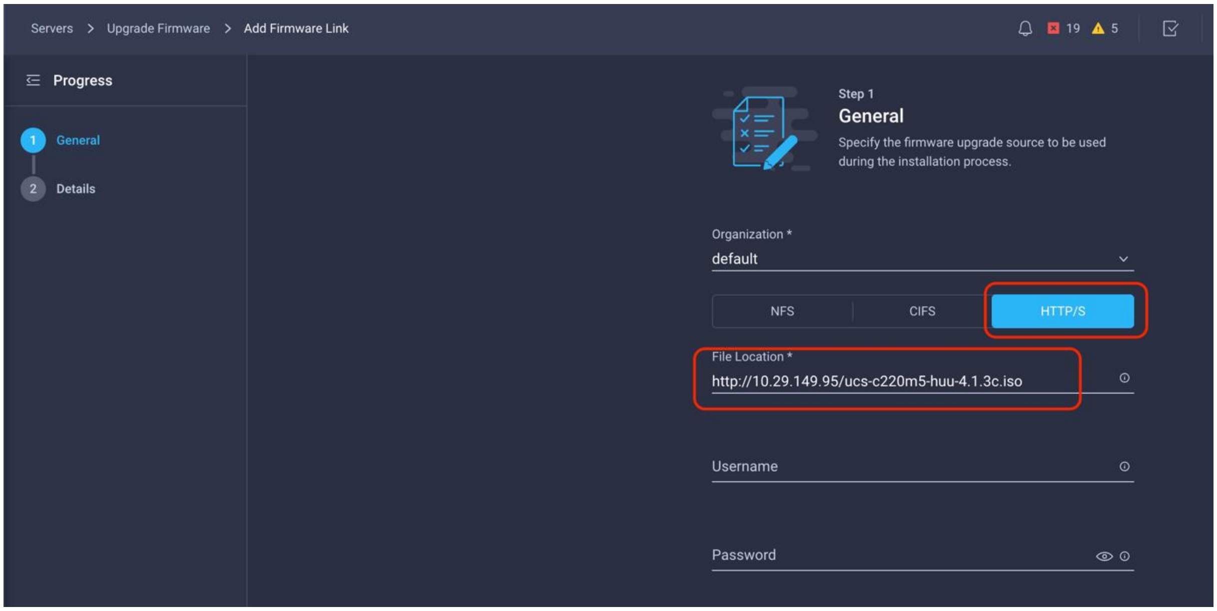
□ Exclude Storage Controllers

1 items found 10 per page 1 of 1

	File Name	Version	Supported Models	File Location
○	ucs-c220m5-huu-4.1.3b.iso	4.1(3b)	UCSC-C220-M5SX,... (5)	http://10.29.149.95/ucs-c220m5-huu-4.1.3b.iso

1 of 1

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



Step 1

General

Specify the firmware upgrade source to be used during the installation process.

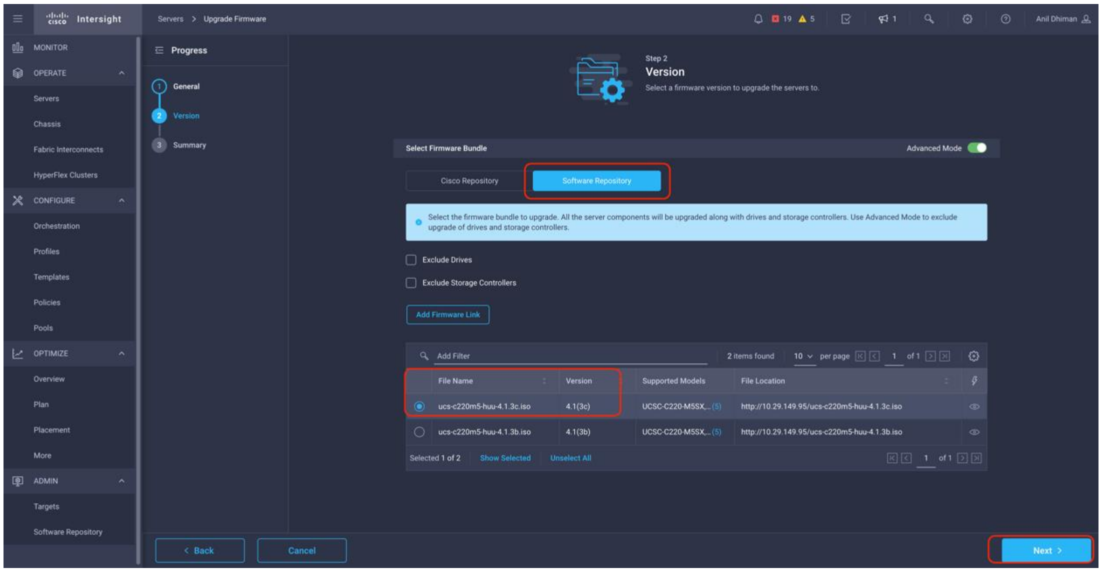
Organization *
default

File Location *
http://10.29.149.95/ucs-c220m5-huu-4.1.3c.iso

Username

Password

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



Step 2

Version

Select a firmware version to upgrade the servers to.

Select Firmware Bundle — Advanced Mode

Cisco Repository | Software Repository

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

☐ Exclude Storage Controllers

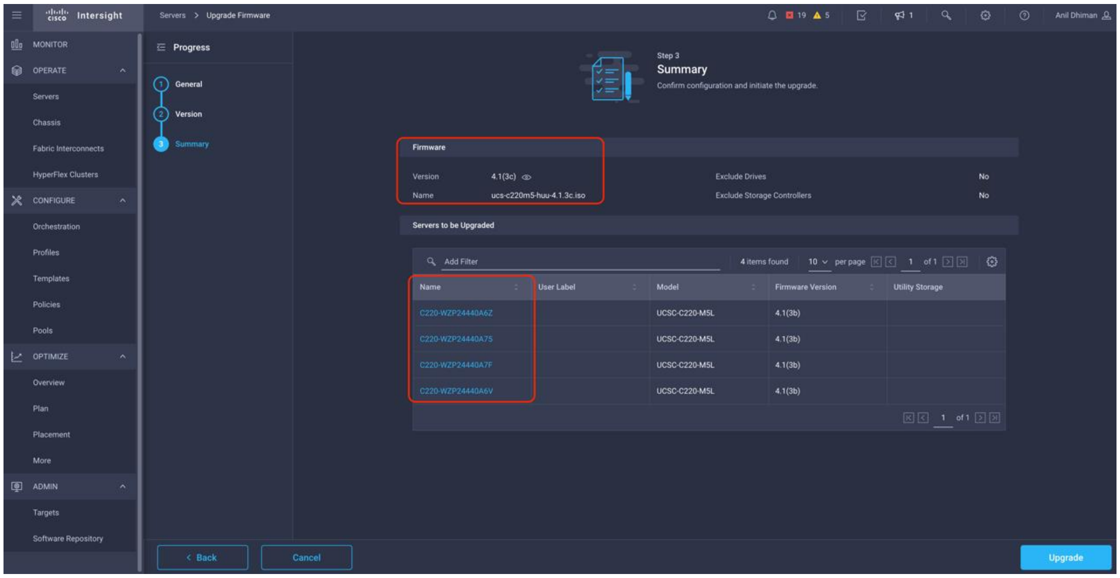
Add Firmware Link

Add Filter — 2 items found — 10 per page — 1 of 1

	File Name	Version	Supported Models	File Location
●	ucs-c220m5-huu-4.1.3c.iso	4.1(3c)	UCSC-C220-M5SX,... (5)	http://10.29.149.95/ucs-c220m5-huu-4.1.3c.iso
○	ucs-c220m5-huu-4.1.3b.iso	4.1(3b)	UCSC-C220-M5SX,... (5)	http://10.29.149.95/ucs-c220m5-huu-4.1.3b.iso

Selected 1 of 2 — Show Selected — Unselect All — 1 of 1

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



Step 3

Summary

Confirm configuration and initiate the upgrade.

Firmware

Version	4.1(3c)	Exclude Drives	No
Name	ucs-c220m5-huu-4.1.3c.iso	Exclude Storage Controllers	No

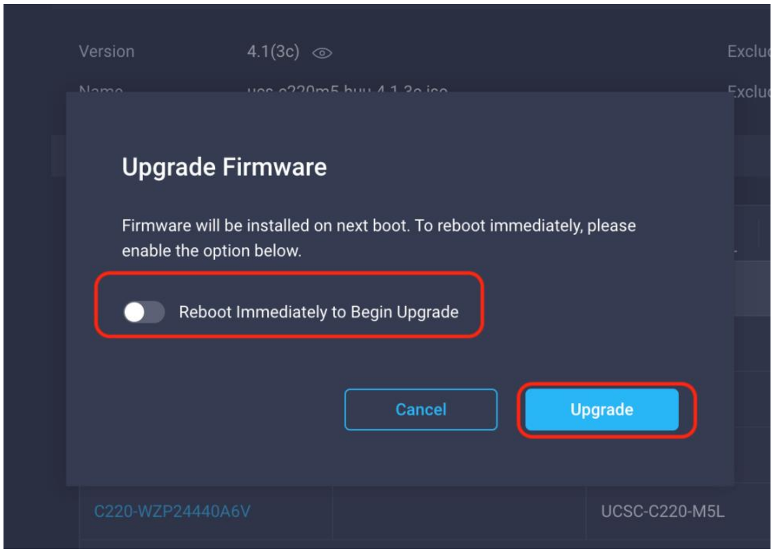
Servers to be Upgraded

Add Filter — 4 items found — 10 per page — 1 of 1

Name	User Label	Model	Firmware Version	Utility Storage
C220-WZP24440A6Z		UCSC-C220-M5L	4.1(3b)	
C220-WZP24440A75		UCSC-C220-M5L	4.1(3b)	
C220-WZP24440A7F		UCSC-C220-M5L	4.1(3b)	
C220-WZP24440A6V		UCSC-C220-M5L	4.1(3b)	

1 of 1

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



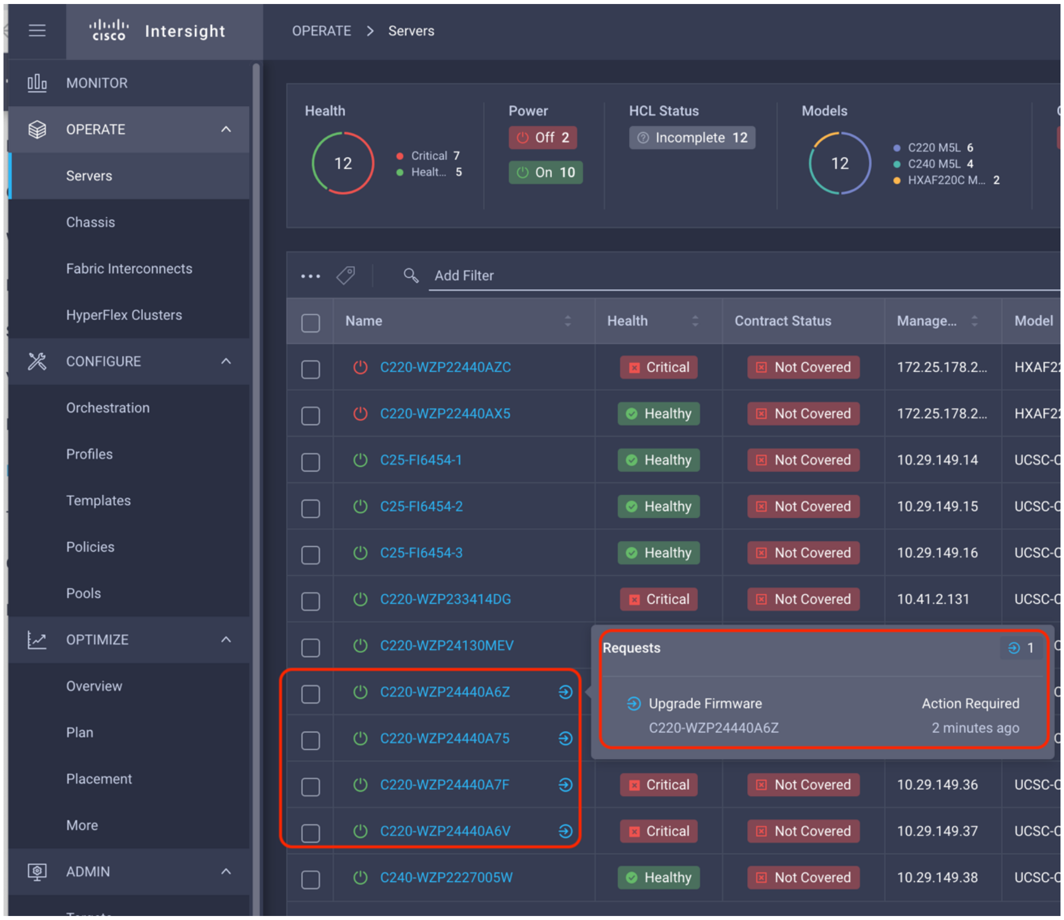
Version 4.1(3c)

Upgrade Firmware

Firmware will be installed on next boot. To reboot immediately, please enable the option below.

○ Reboot Immediately to Begin Upgrade

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



Health: 12 — Critical 7, Healt... 5

Power: Off 2, On 10

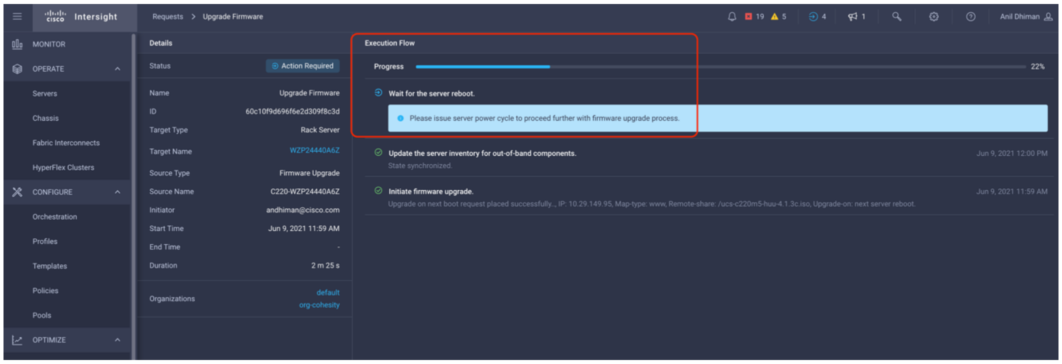
HCL Status: Incomplete 12

Models: 12 — C220 M5L 6, C240 M5L 4, HXAF220C M... 2

Name	Health	Contract Status	Manage...	Model
C220-WZP22440AZC	Critical	Not Covered	172.25.178.2...	HXAF2
C220-WZP22440AX5	Healthy	Not Covered	172.25.178.2...	HXAF2
C25-FI6454-1	Healthy	Not Covered	10.29.149.14	UCSC-C
C25-FI6454-2	Healthy	Not Covered	10.29.149.15	UCSC-C
C25-FI6454-3	Healthy	Not Covered	10.29.149.16	UCSC-C
C220-WZP233414DG	Critical	Not Covered	10.41.2.131	UCSC-C
C220-WZP24130MEV				
C220-WZP24440A6Z				
C220-WZP24440A75				
C220-WZP24440A7F	Critical	Not Covered	10.29.149.36	UCSC-C
C220-WZP24440A6V	Critical	Not Covered	10.29.149.37	UCSC-C
C240-WZP2227005W	Healthy	Not Covered	10.29.149.38	UCSC-C

Requests 1

Upgrade Firmware — Action Required
C220-WZP24440A6Z — 2 minutes ago



Details

Status	Action Required
Name	Upgrade Firmware
ID	60c10f9d696f6e2d309f8c3d
Target Type	Rack Server
Target Name	WZP24440A6Z
Source Type	Firmware Upgrade
Source Name	C220-WZP24440A6Z
Initiator	andhiman@cisco.com
Start Time	Jun 9, 2021 11:59 AM
End Time	-
Duration	2 m 25 s
Organizations	default org-cohesity

Execution Flow

Progress 22%

Wait for the server reboot.

Please issue server power cycle to proceed further with firmware upgrade process.

Update the server inventory for out-of-band components. Jun 9, 2021 12:00 PM
State synchronized.

Initiate firmware upgrade. Jun 9, 2021 11:59 AM
Upgrade on next boot request placed successfully.., IP: 10.29.149.95, Map-type: www, Remote-share: /ucs-c220m5-huu-4.1.3c.iso, Upgrade-on: next server reboot.

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:
  https://www.intersight.com
- Cisco Unified Computing System:
  http://www.cisco.com/en/US/products/ps10265/index.html
- Cisco UCS adapters:
  http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html
- Cohesity on Cisco UCS:
  https://www.cisco.com/go/cohesity

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

Configuration guides

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

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**.

Printed in USA 221181.1 07/21