White Paper
Public

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

© 2021 Cisco and/or its affiliates. All rights reserved.

Contents

Executive summary 3

Cisco Intersight platform 3

Cisco Intersight Virtual Appliance and Private Virtual Appliance 4

Solution design and deployment 5

Deployment hardware and software 5

Licensing requirements 6

Configuration constructs for Cisco Intersight mode 7

Configure Cisco IMC network 7

Claim Cisco UCS C220 or C240 node in Cisco Intersight platform 8

Claim device in Cisco Intersight platform 9

Configure server policies 11

Create organization policy 12

Create adaptor configuration policy 14

Create BIOS profile policy 17

Create IPMI-over-LAN policy 19

Create serial-over-LAN policy 21

Create storage configuration policy 23

Create boot-order policy 24

Configure and deploy server profile for Cohesity nodes 27

Install the Cohesity operating system 35

Install the OS through the Cisco Intersight platform 35

Install the OS through vMedia and one-time boot device 42

Firmware upgrades 51

Conclusion 56

For more information 57

Products and solutions 57

Configuration guides 57

© 2021 Cisco and/or its affiliates. All rights reserved.

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

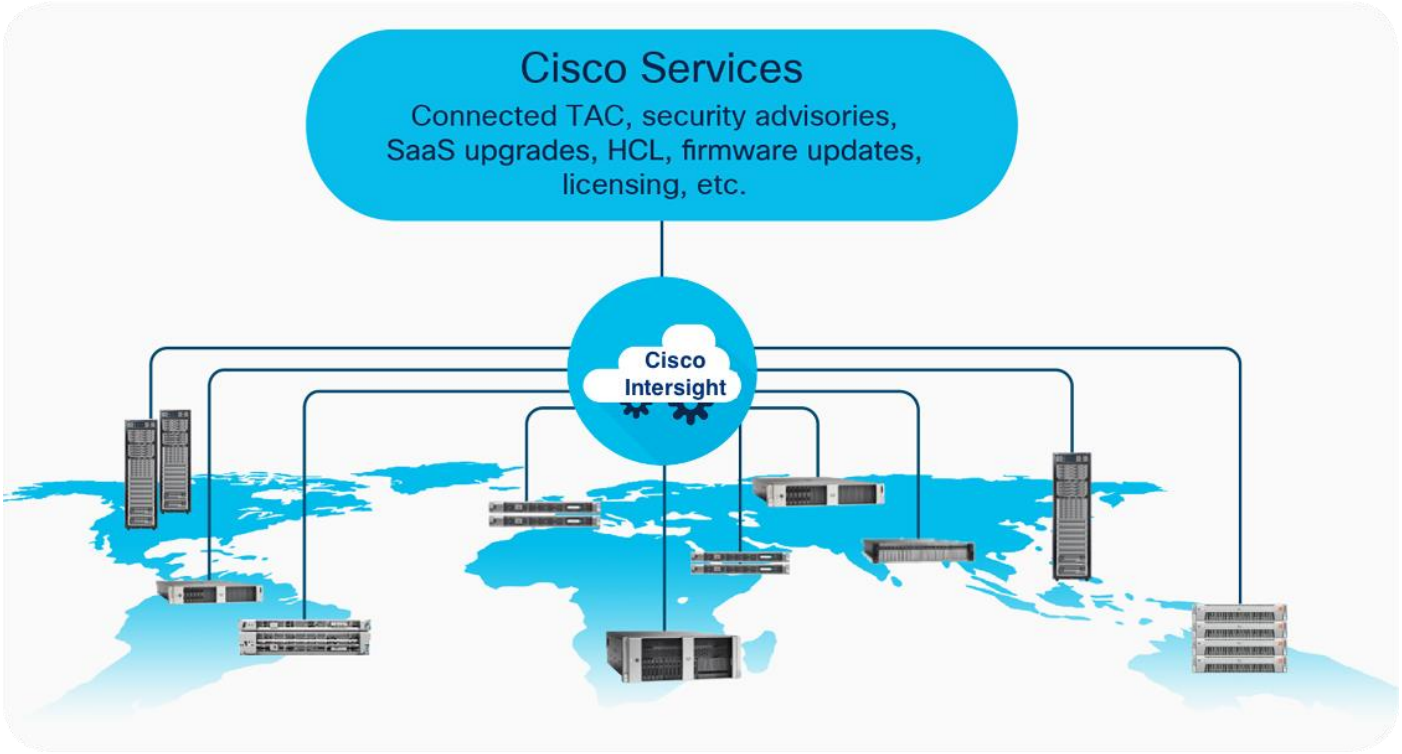


Figure 1.
Cisco Intersight overview

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

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.

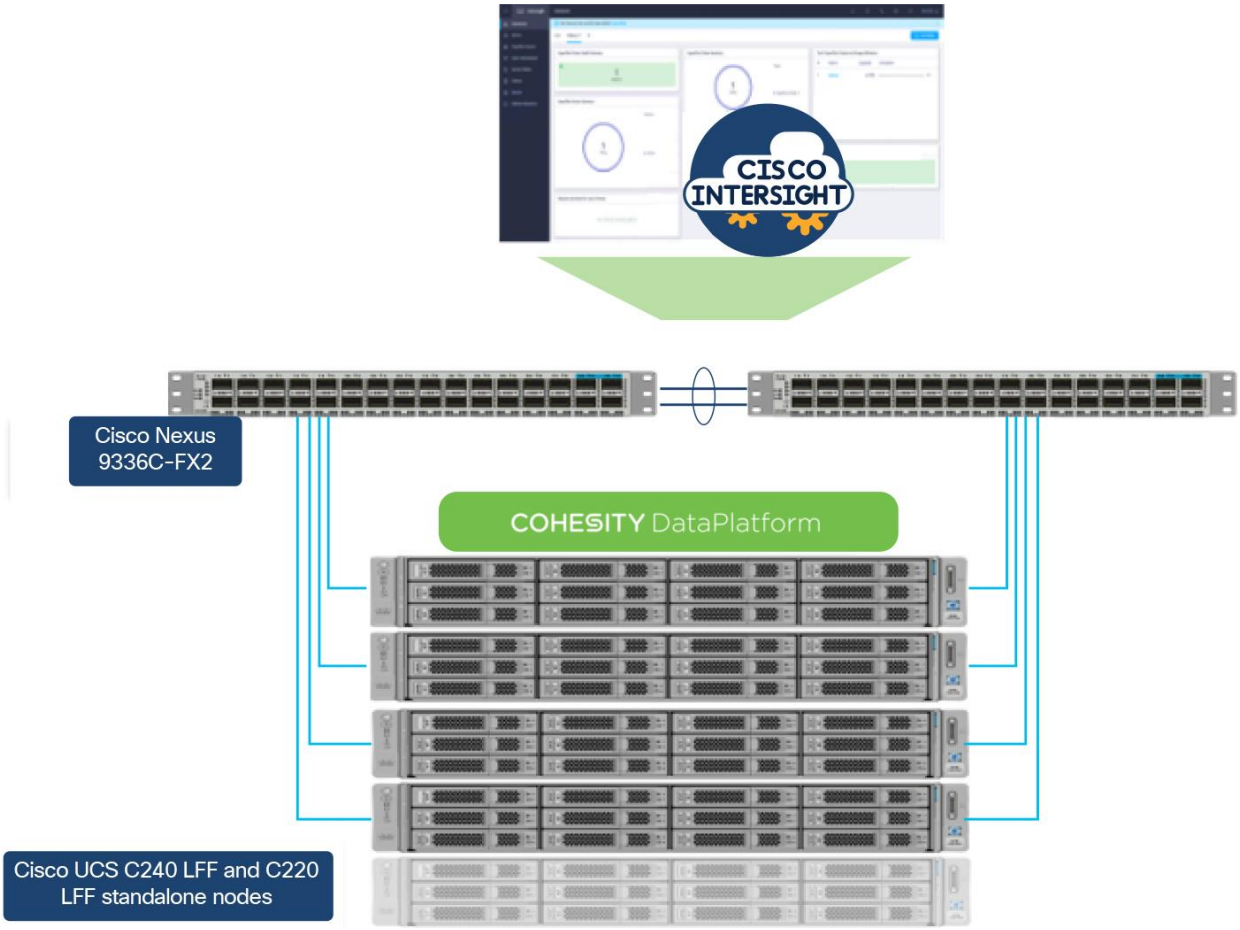


Figure 2.
Cohesity on Cisco UCS server nodes

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

© 2021 Cisco and/or its affiliates. All rights reserved.

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

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.

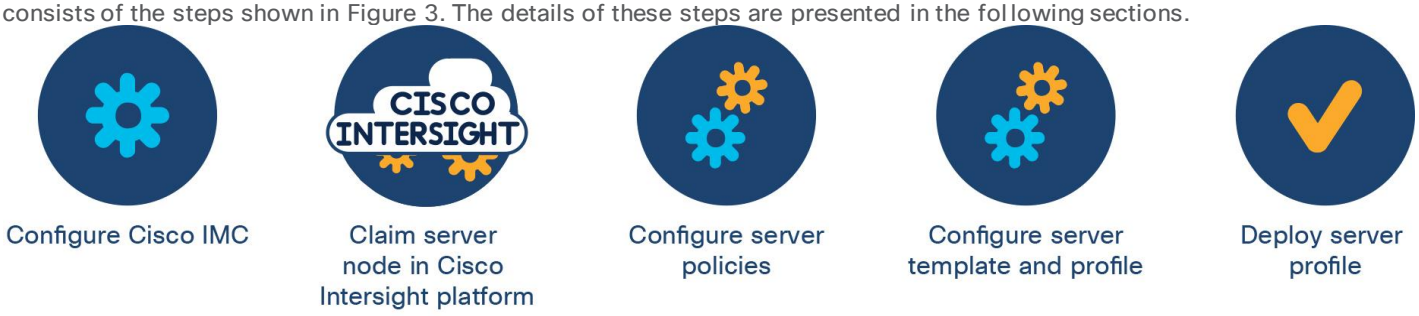


Figure 3.
Steps to configure Cisco UCS server nodes using the Cisco Intersight platform

Configure Cisco IMC network

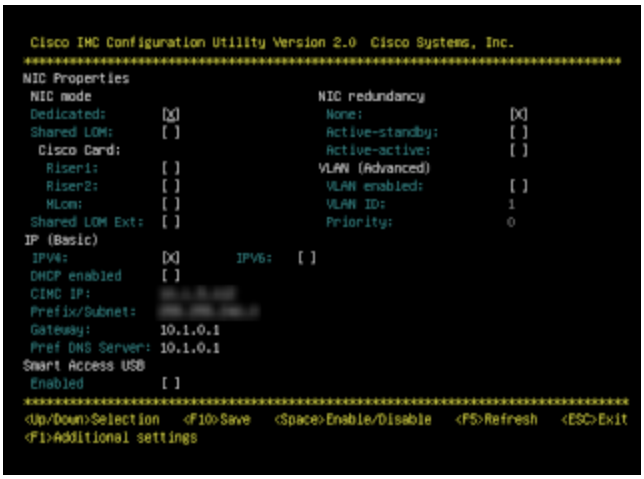
To configure the Cisco IMC network, follow these steps:

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.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.

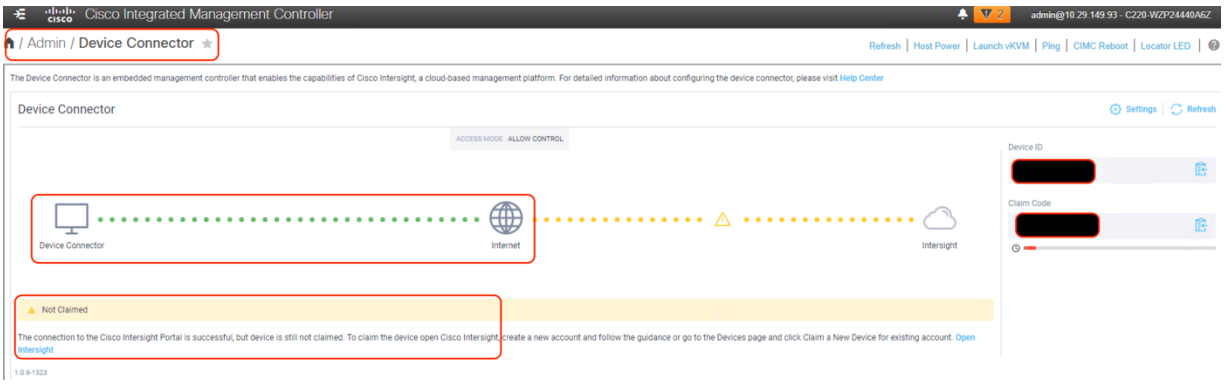
Note: This document assumes that customers already have a Cisco Intersight account. If you need to create a new account, refer to Intersight Overview.

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

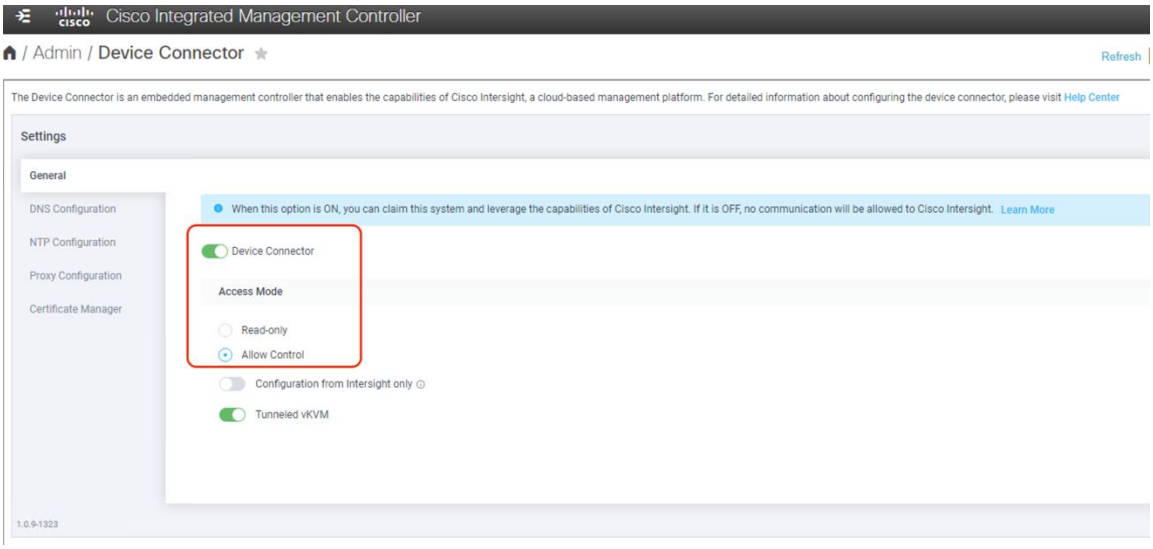
Follow these steps to prepare the device that you want to claim in the Cisco Intersight platform:

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.

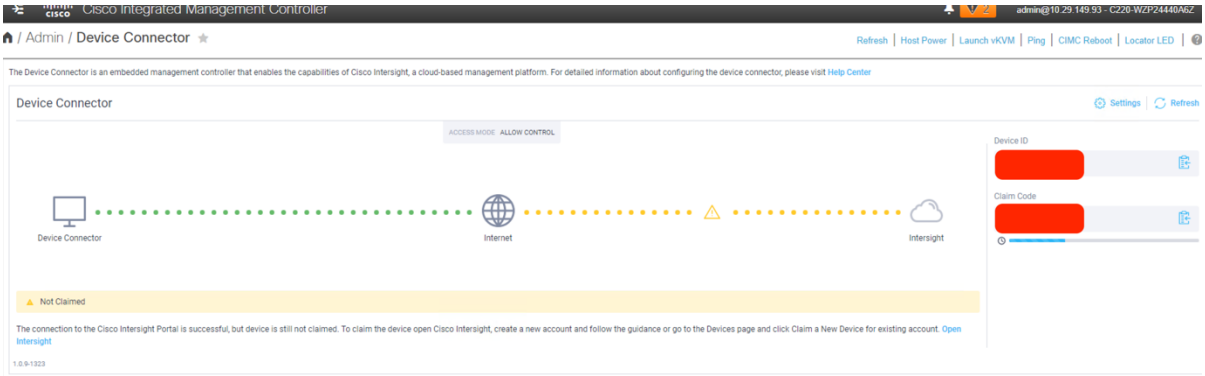


© 2021 Cisco and/or its affiliates. All rights reserved.

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.



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).



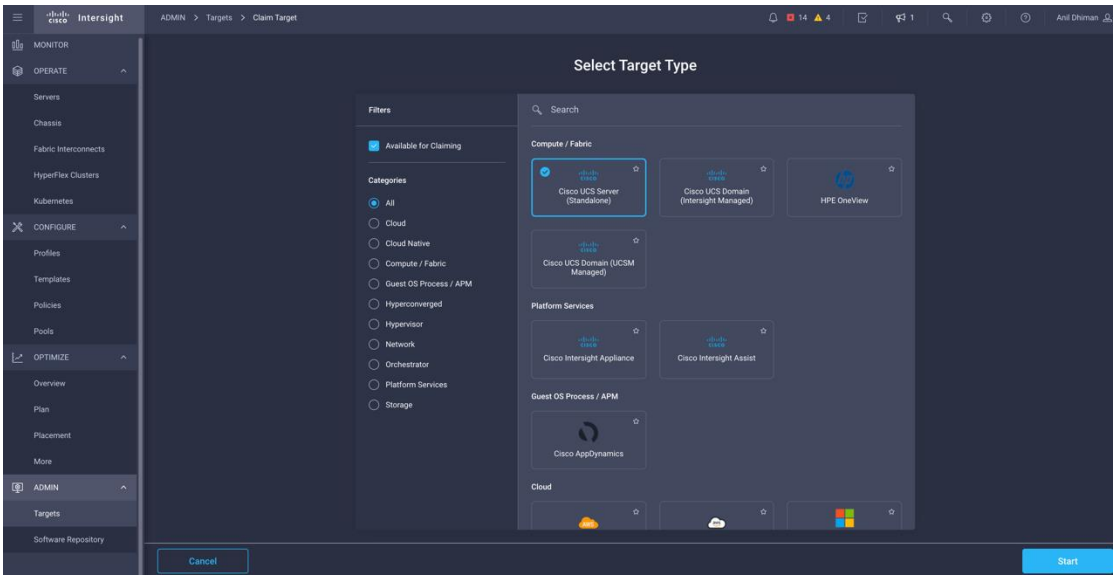
8. Repeat steps 1 through 7 for all the nodes deployed in the Cohesity DataPlatform cluster.

Claim device in Cisco Intersight platform

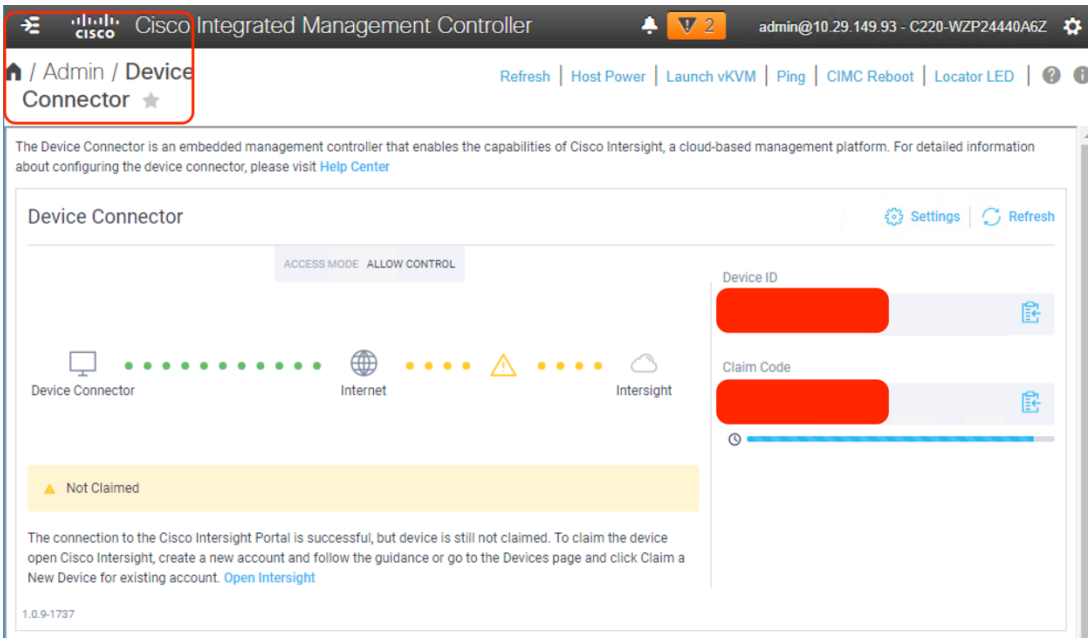
This section describes the process for claiming devices in the Cisco Intersight platform.

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

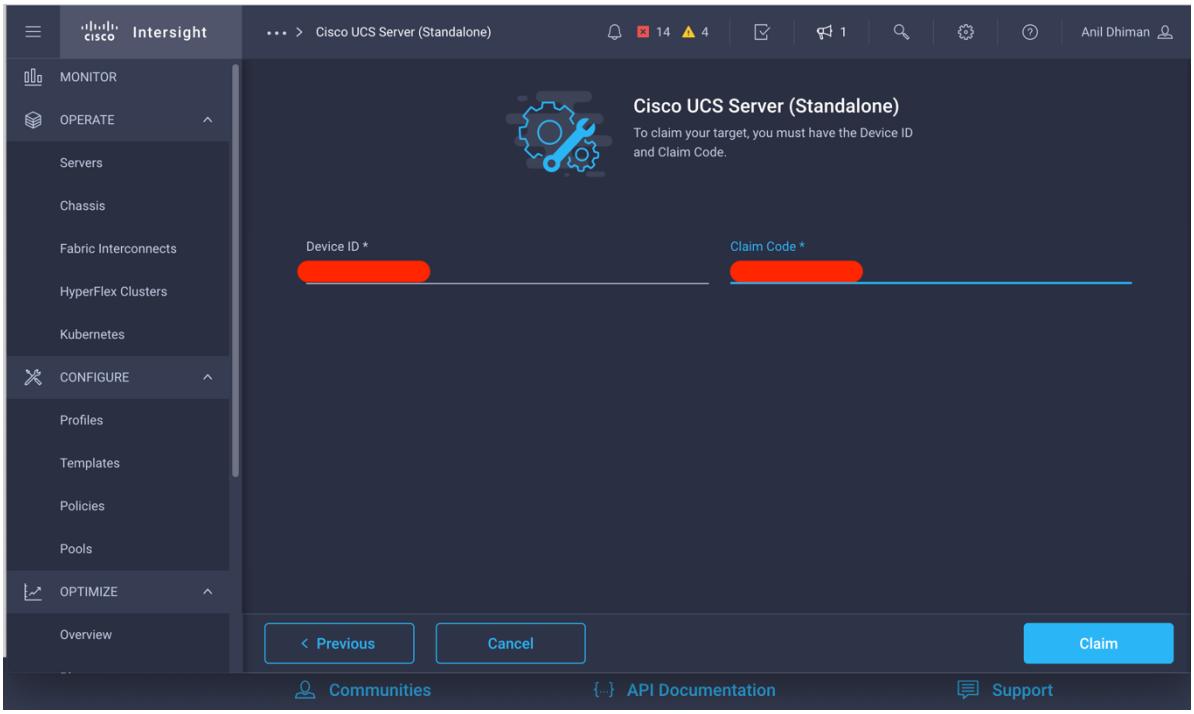


4. Enter the device ID and claim code details from the Cisco IMC (Admin > Device Connector) of each Cisco UCS C-Series node, marked here in red.

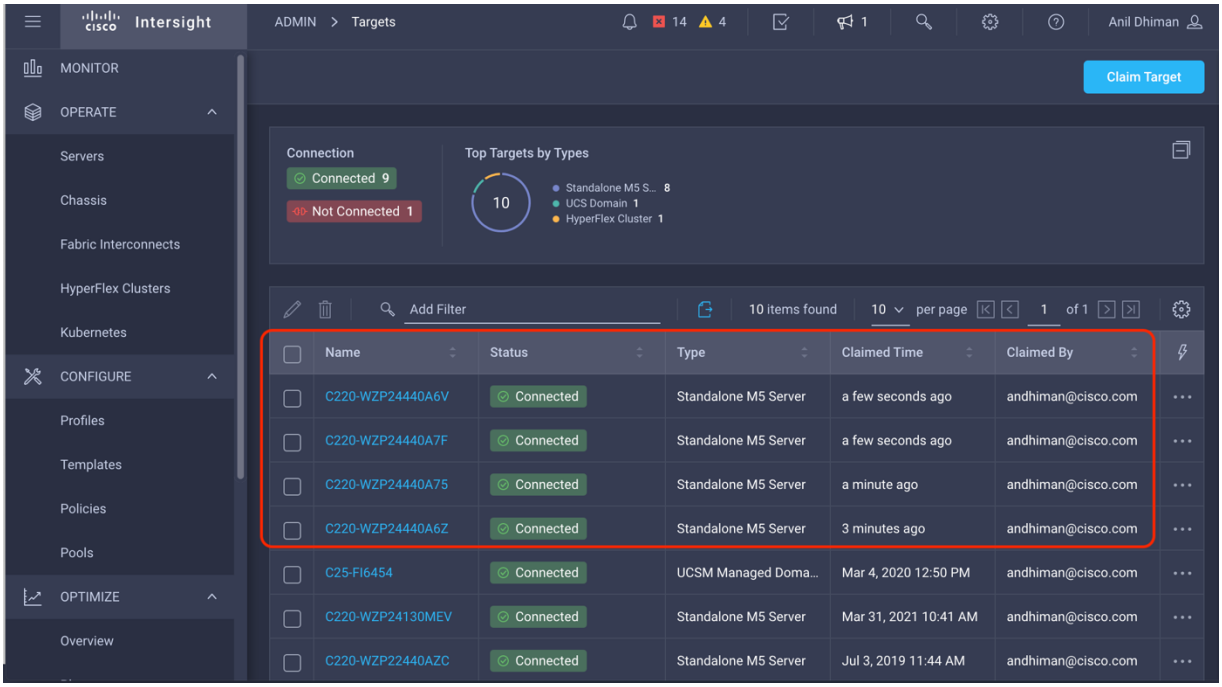


5. Click Claim.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



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.

© 2021 Cisco and/or its affiliates. All rights reserved.

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

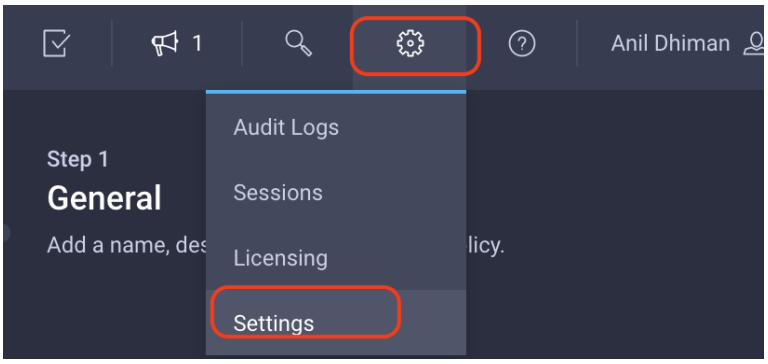
The following sections describe the server policies created to deploy Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform.

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.

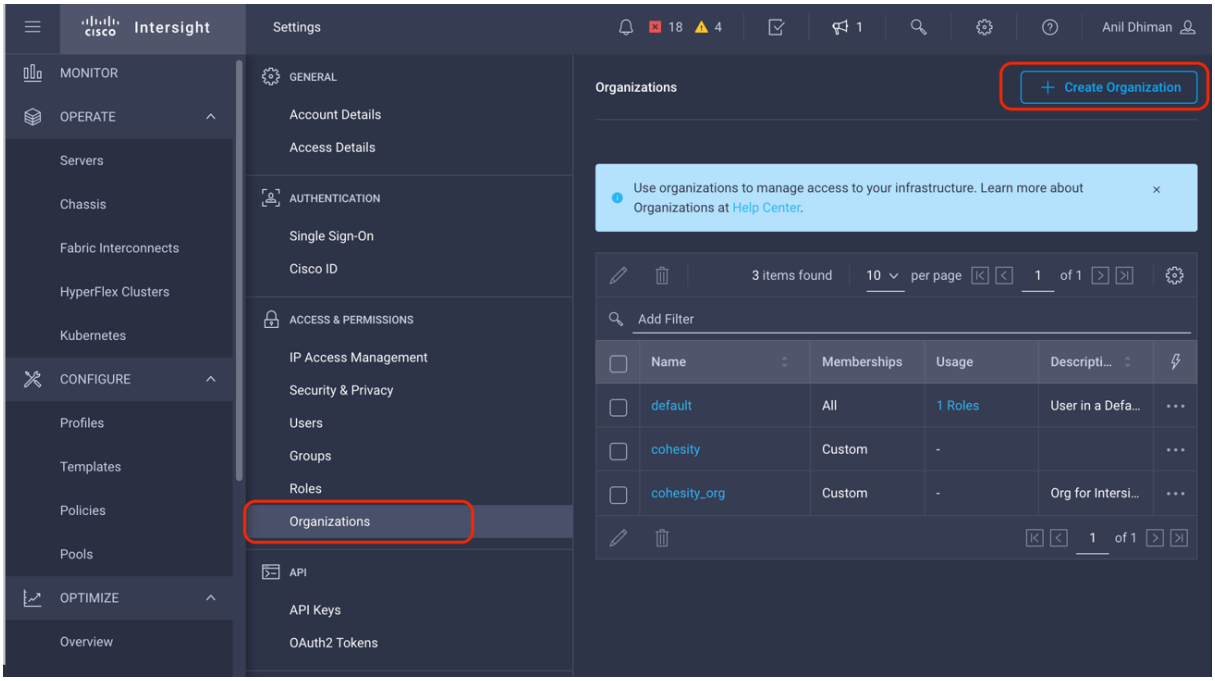
Follow these steps to create an organization:

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

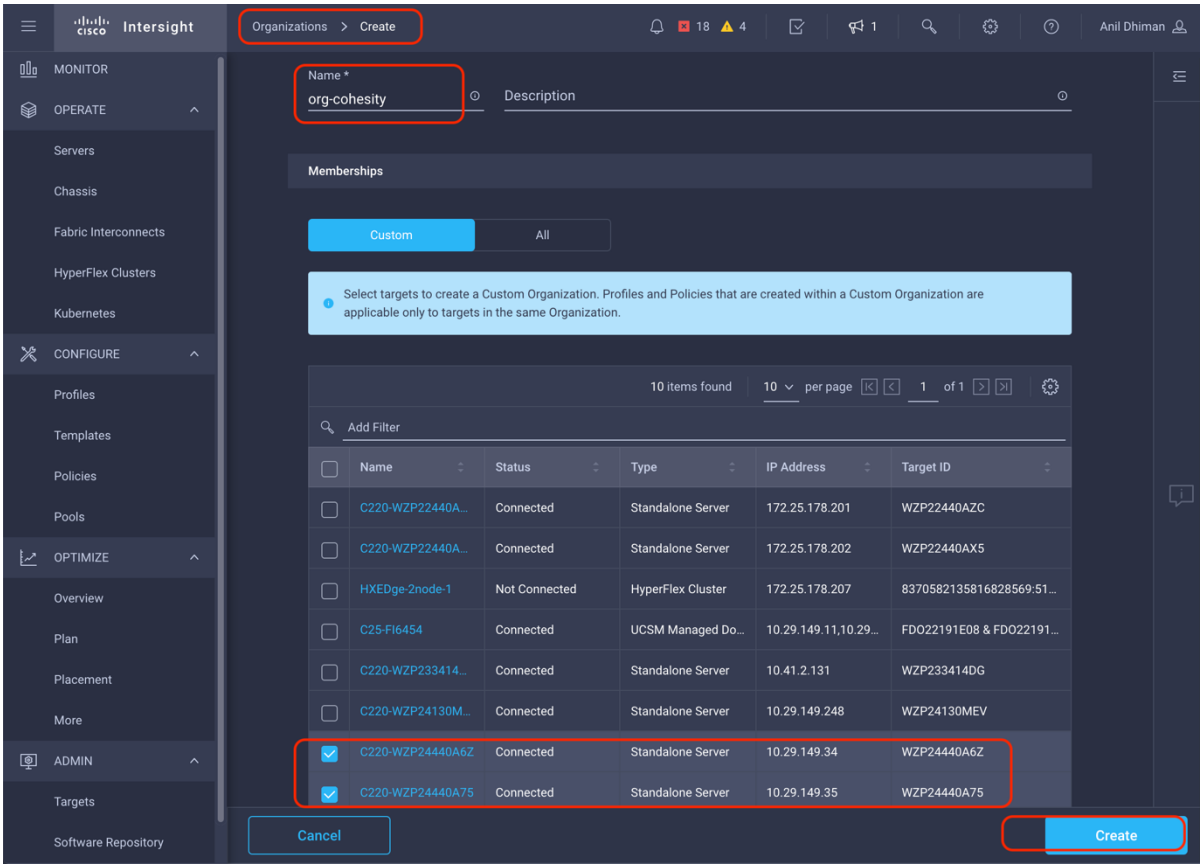


3. Click Organizations and click the Create Organization tab in the top-left corner.

© 2021 Cisco and/or its affiliates. All rights reserved.



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



5. Verify that the organization was created successfully.

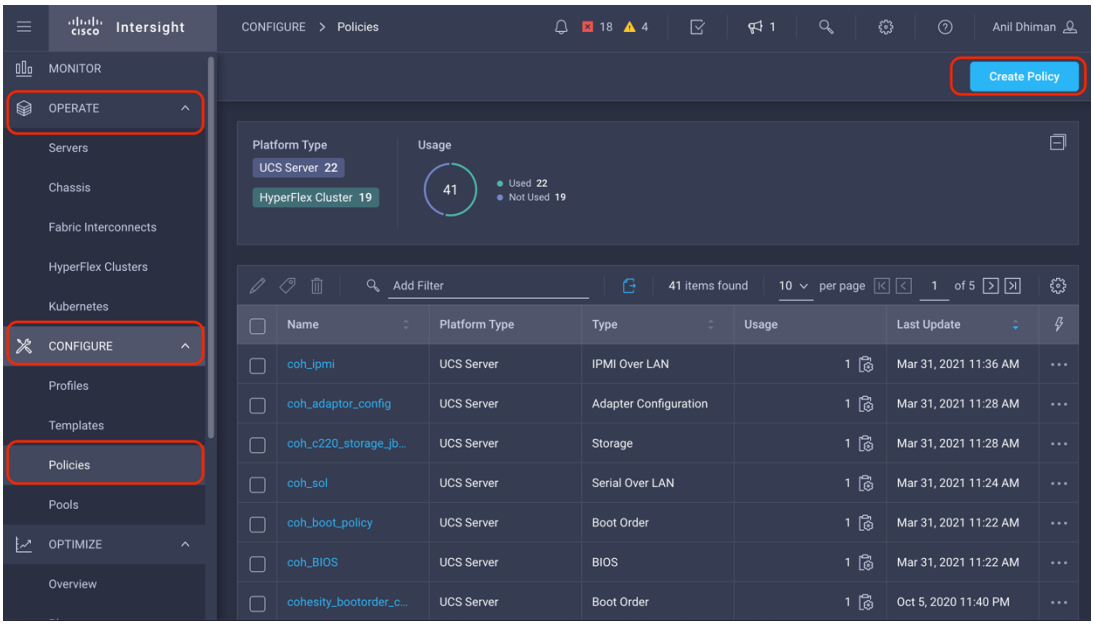
© 2021 Cisco and/or its affiliates. All rights reserved.

Create adaptor configuration policy

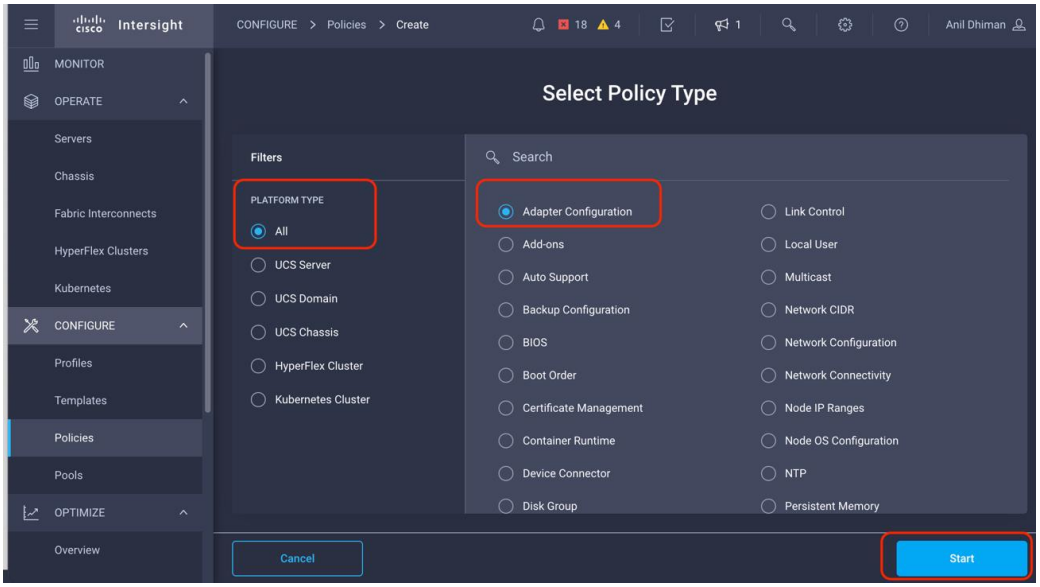
Adapter configuration policy configures the Ethernet and Fibre Channel settings for the VIC adapter.

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

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

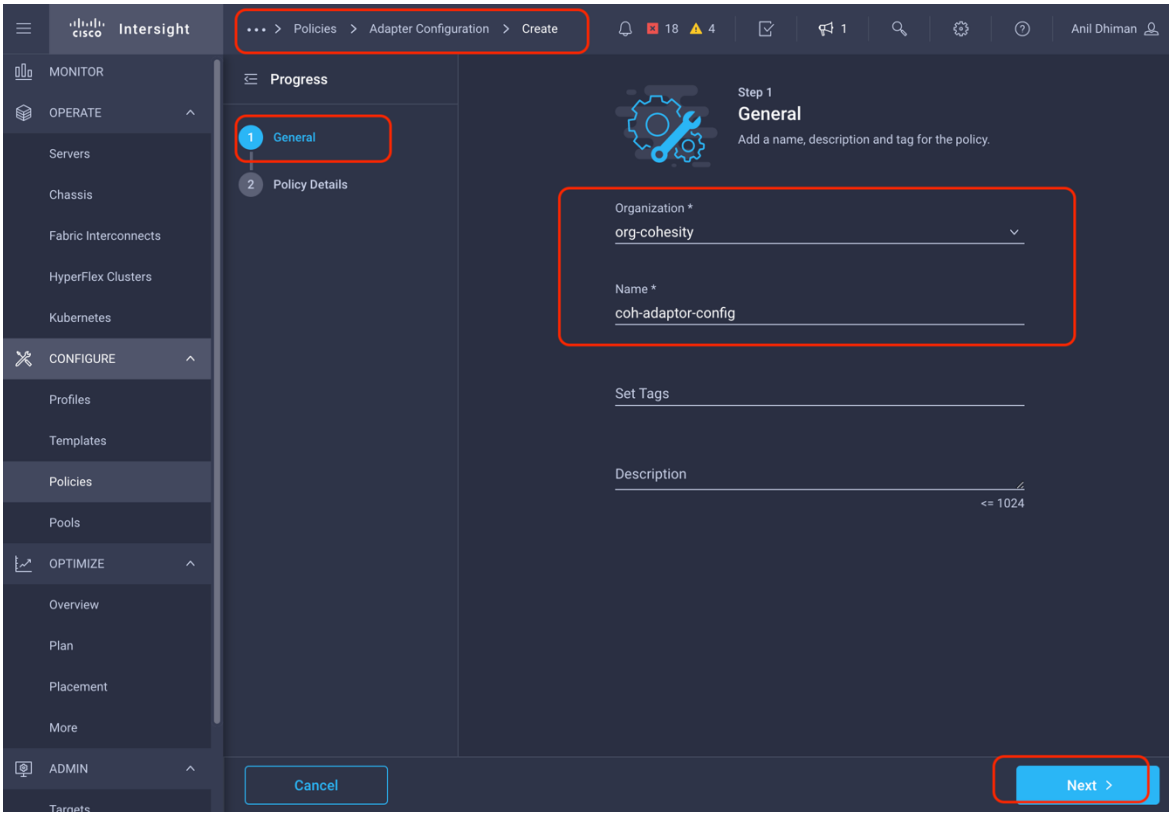


3. For Platform Type, select All. Select Adaptor Configuration and click Start.

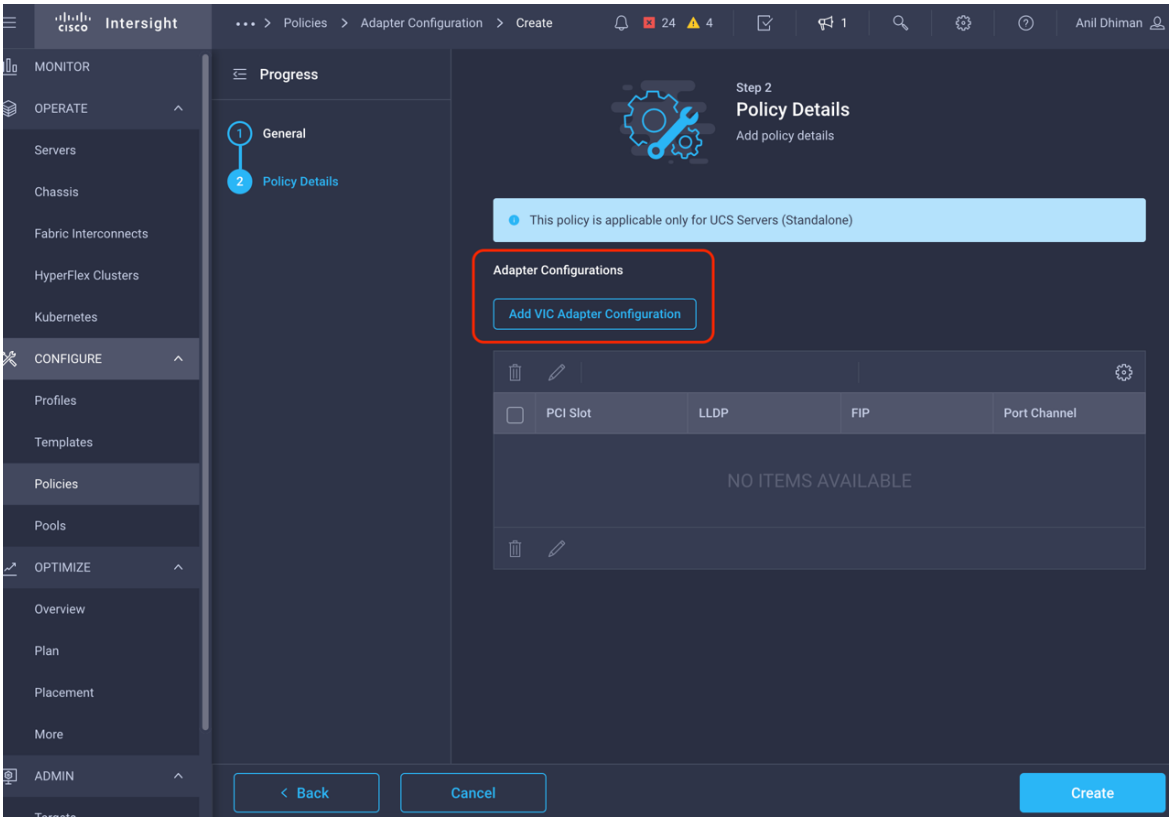


4. On the adaptor configuration Create page, do the following:
   - For Organization, select org-cohesity, created in the previous section.
   - For Name, enter coh-adaptor-config.
   - Click Next.

© 2021 Cisco and/or its affiliates. All rights reserved.



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



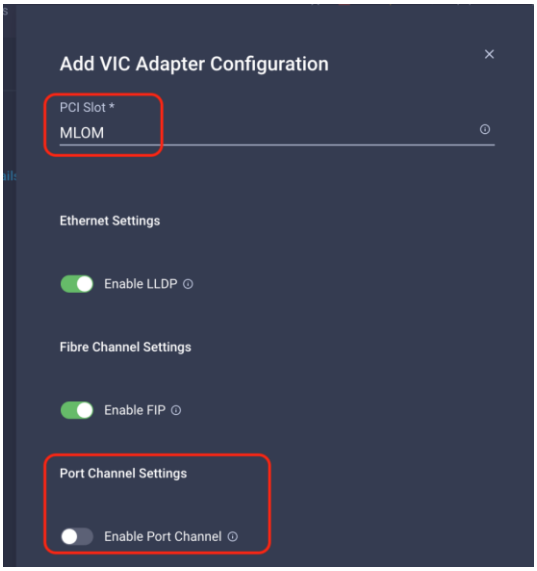
6. Enter the following details for the VIC configuration:
    - For PCIe Slot, specify MLOM.

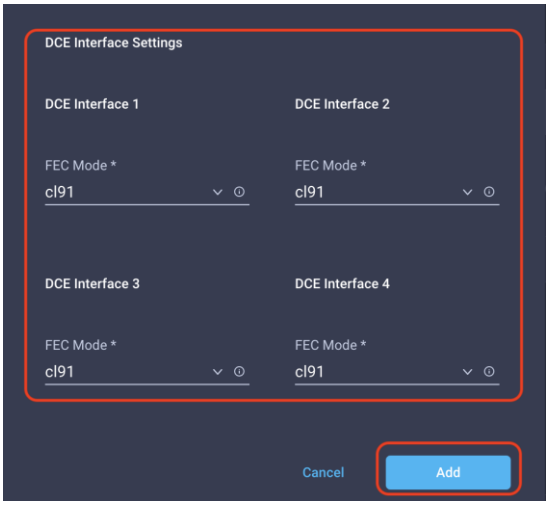
© 2021 Cisco and/or its affiliates. All rights reserved.

- 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.

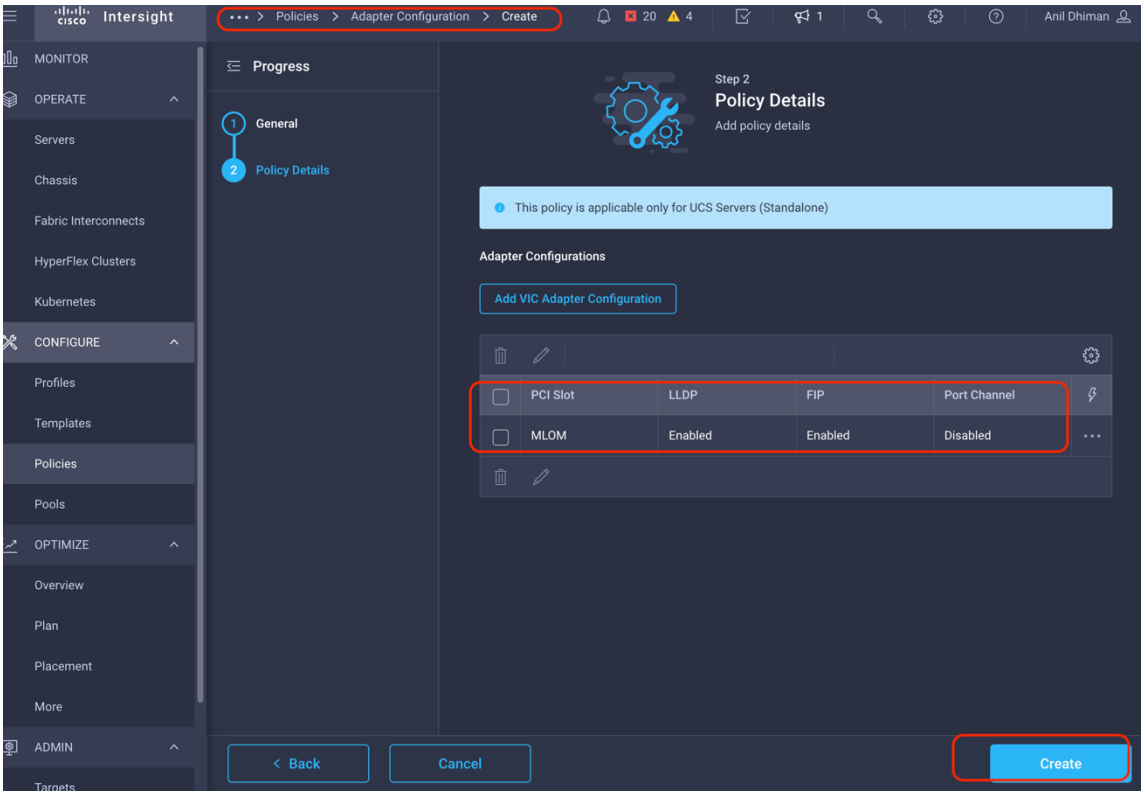
- Click the Add button.





© 2021 Cisco and/or its affiliates. All rights reserved.

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



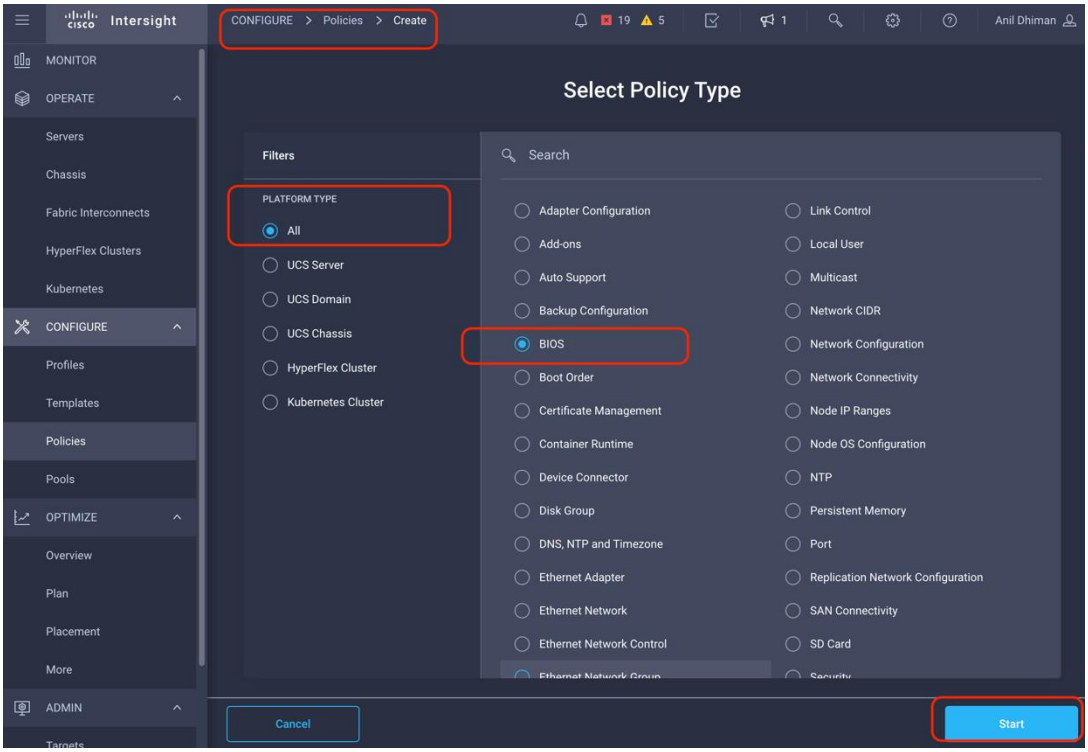
Create BIOS profile policy

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.

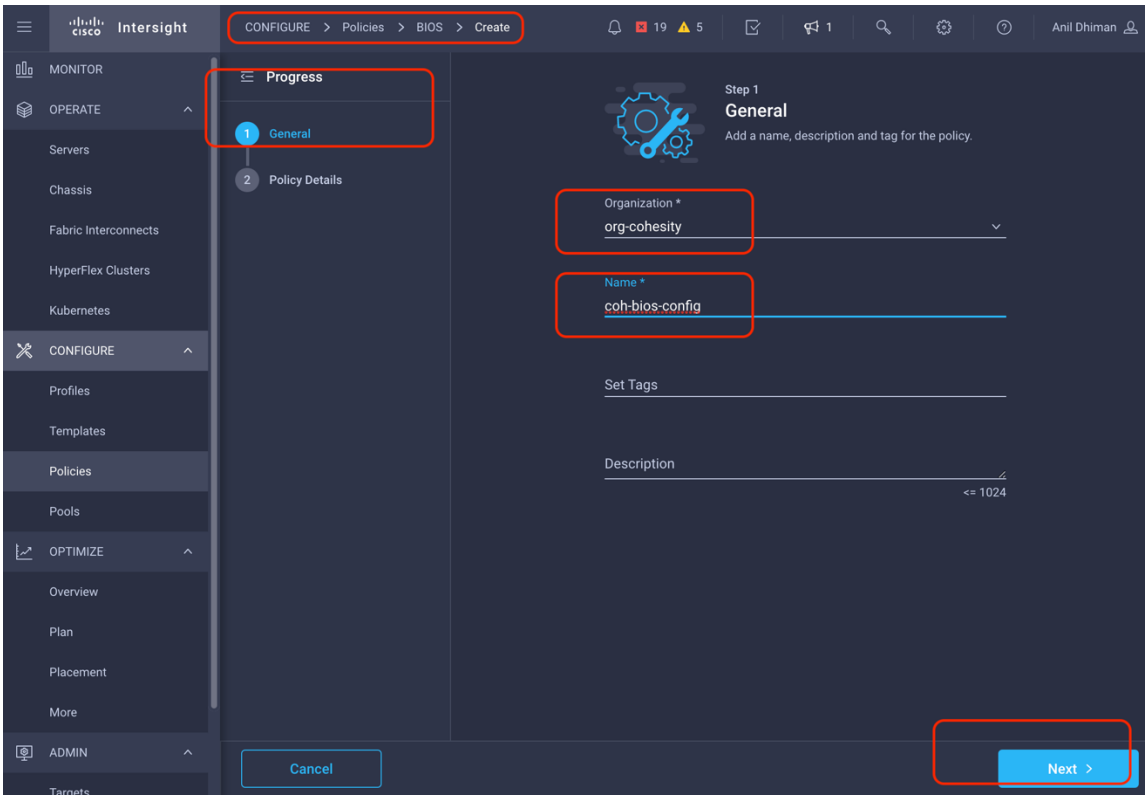
Follow these steps to configure BIOS policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

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.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



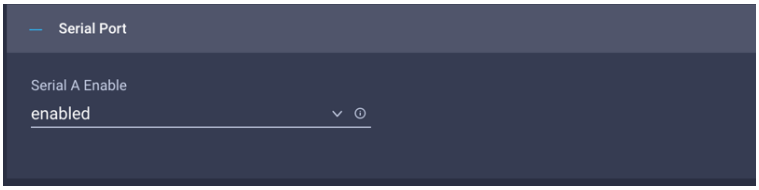
© 2021 Cisco and/or its affiliates. All rights reserved.

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



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



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

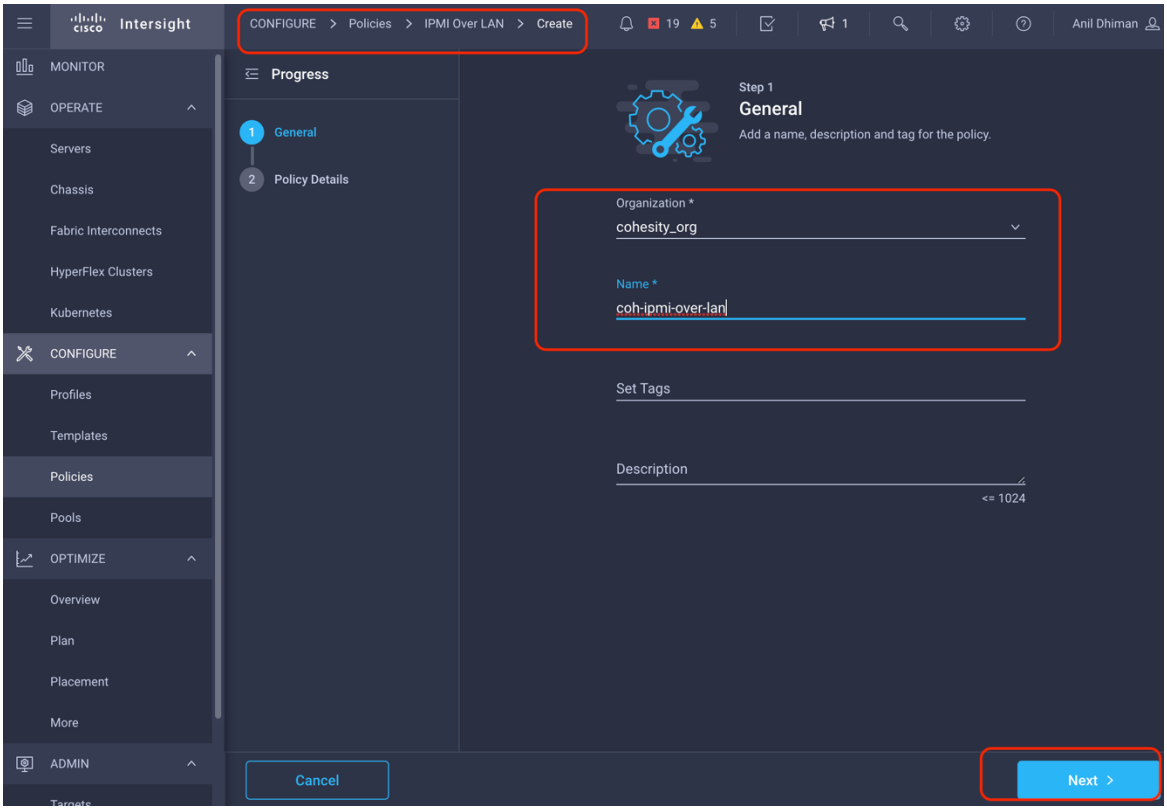
Create IPMI-over-LAN policy

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

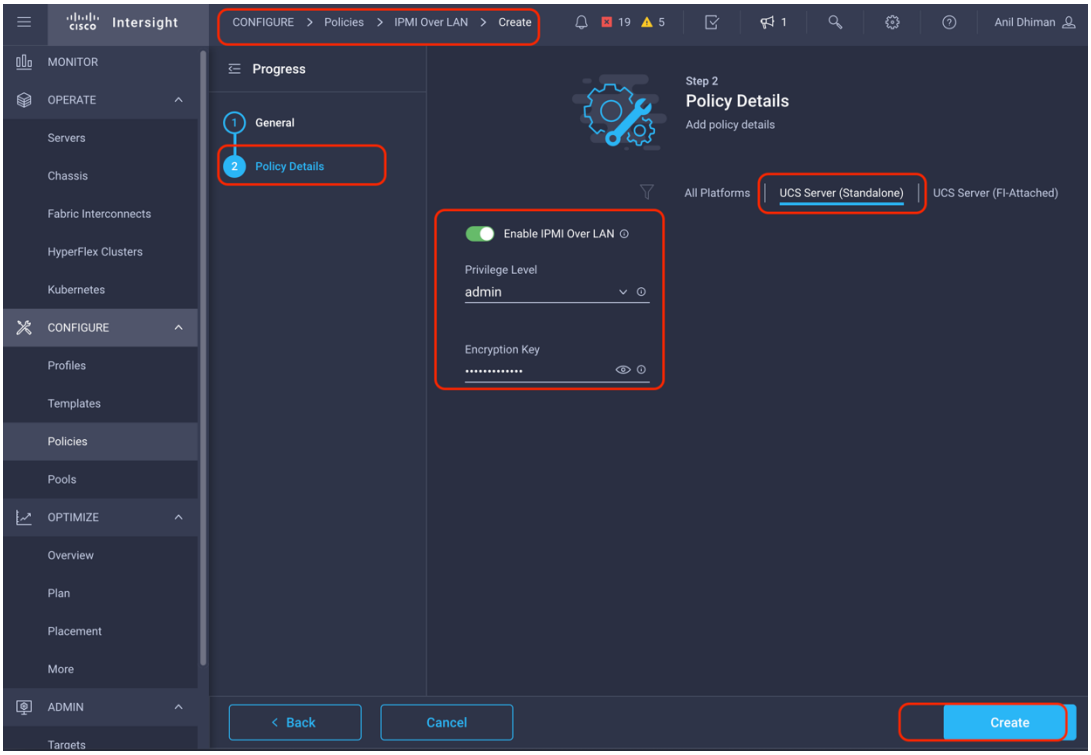
Follow these steps to create IPMI-over-LAN policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

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.



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.

© 2021 Cisco and/or its affiliates. All rights reserved.



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

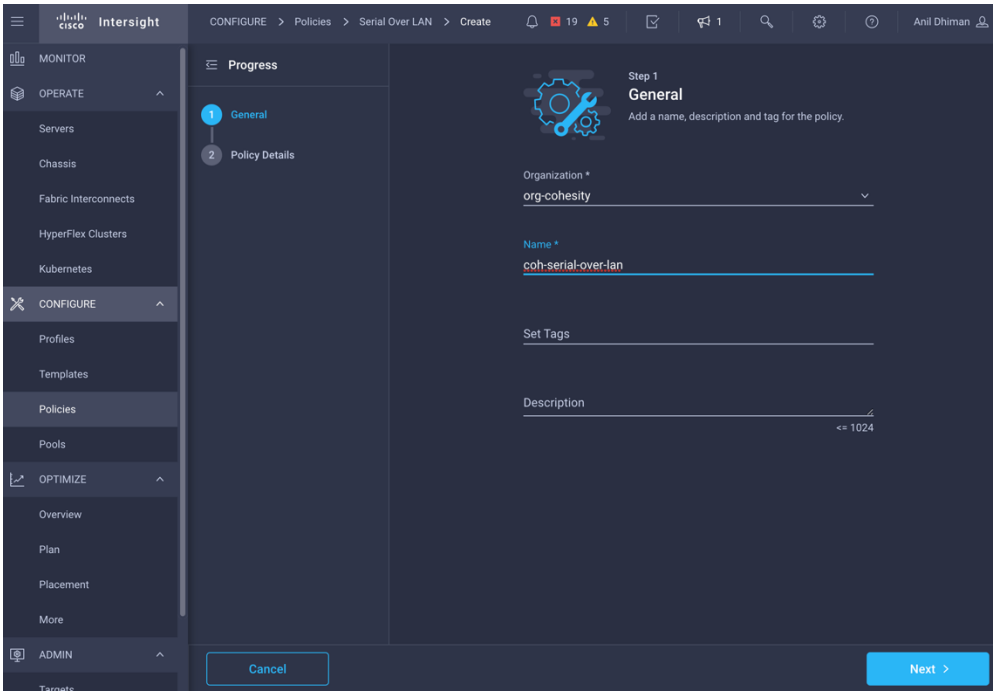
Create serial-over-LAN policy

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.

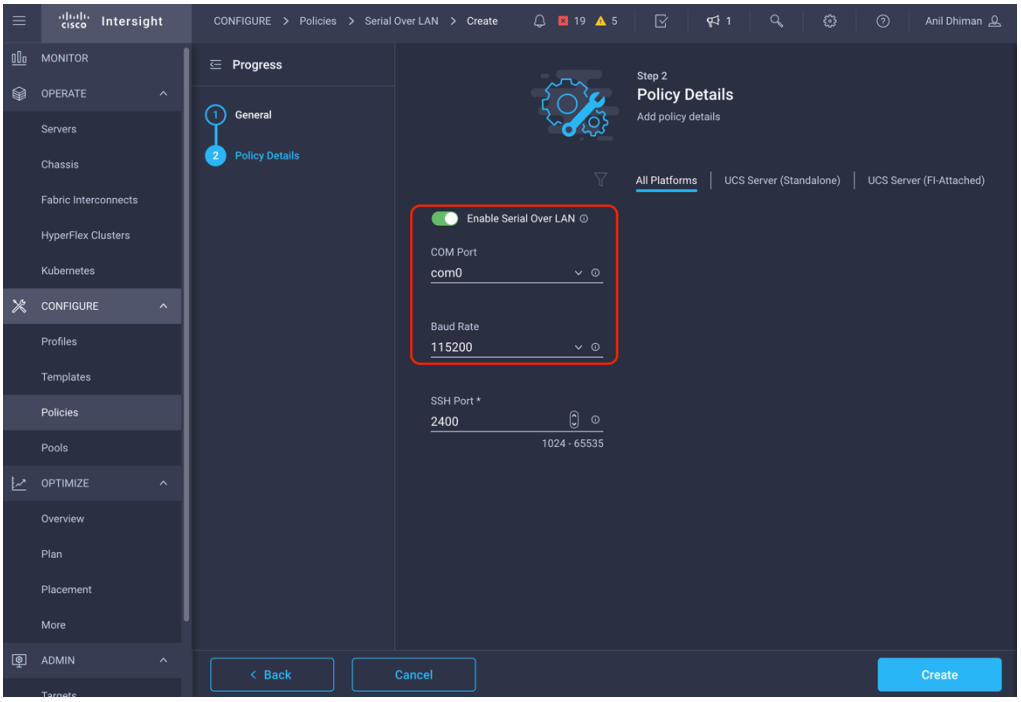
Follow these steps to create serial-over-LAN policy for Cisco UCS C220 and C240 standalone nodes specific to Cohesity DataPlatform:

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.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



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

© 2021 Cisco and/or its affiliates. All rights reserved.

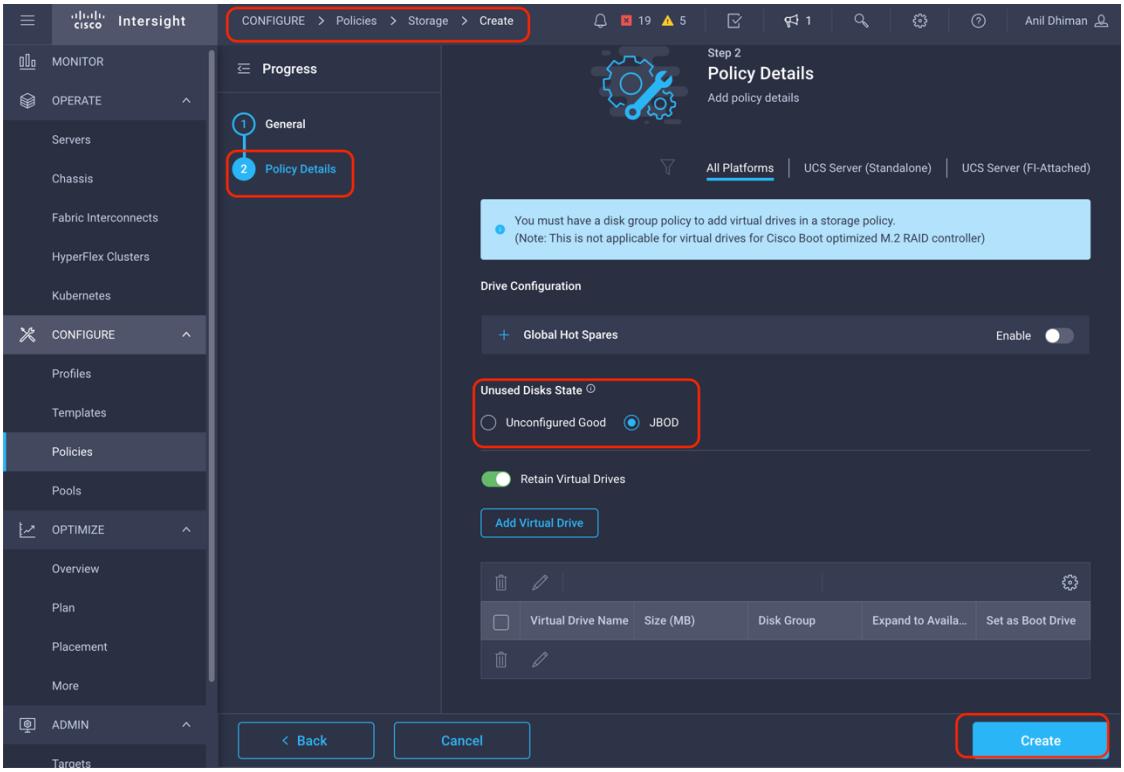
Create storage configuration policy

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.



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

© 2021 Cisco and/or its affiliates. All rights reserved.

Create boot-order policy

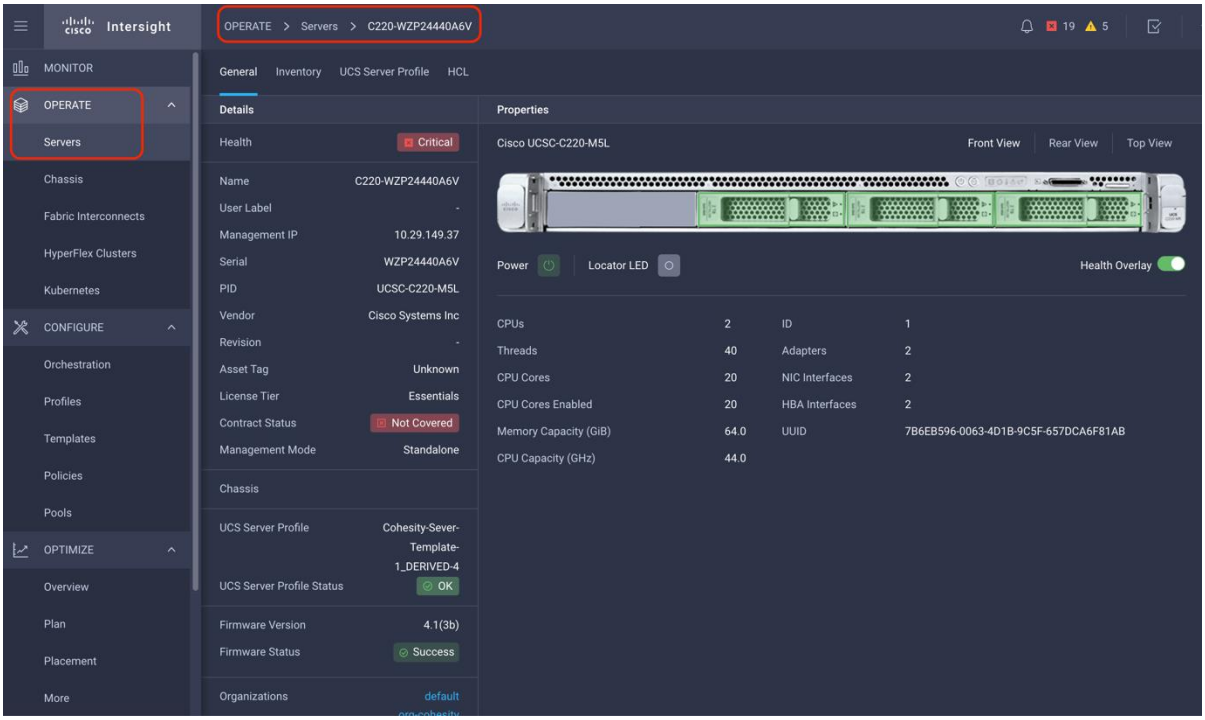
Boot-order policy configures the linear ordering of devices and enables you to change the boot order and boot mode. You can also add multiple devices under various device types, rearrange the boot order, and set parameters for each boot device type.

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).

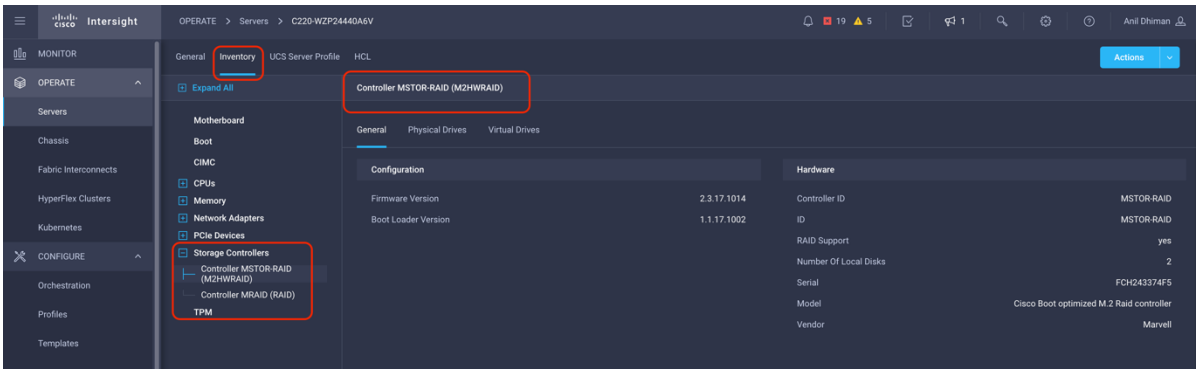
Confirming the server RAID controller

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.



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



© 2021 Cisco and/or its affiliates. All rights reserved.

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.

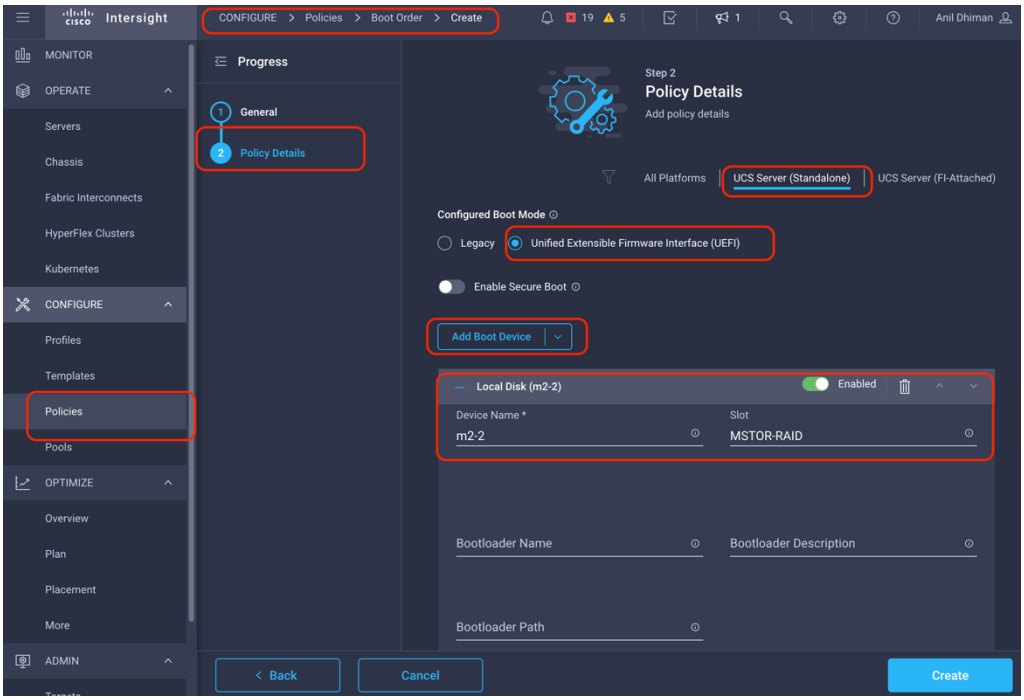
Note: UEFI boot mode for Cisco UCS C220 M5 Rack Servers with Cohesity DataPlatform is supported by all Cohesity releases.

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).

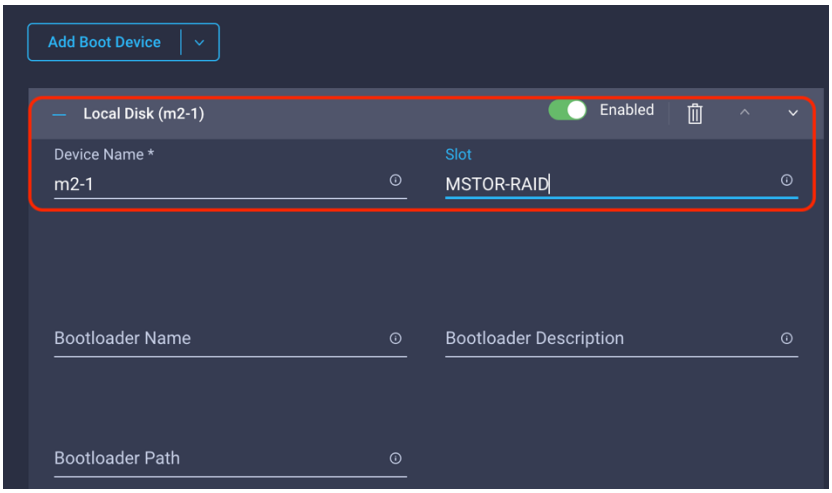
Note: Be sure that the slot is named as MSTOR-RAID.

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

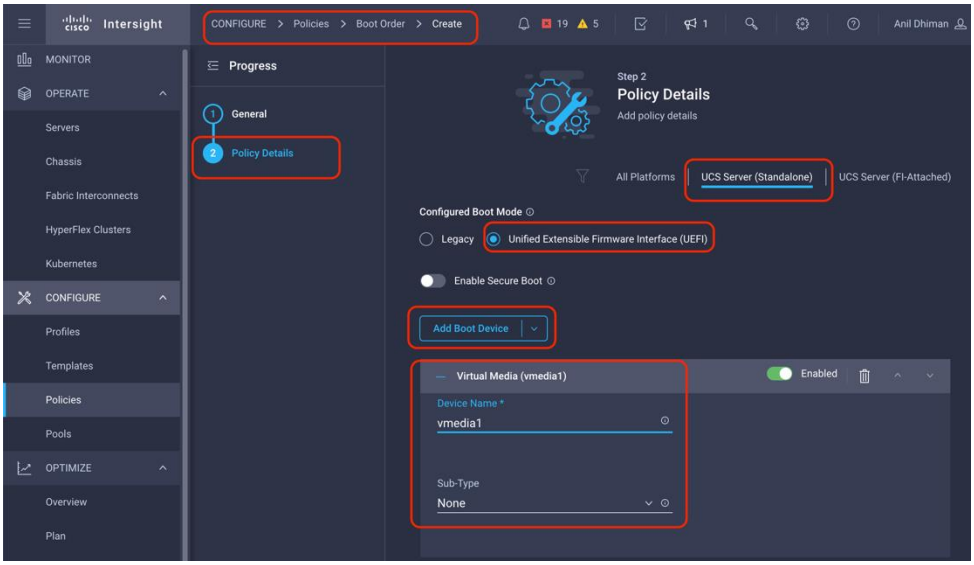


4. Again click Add Boot Device and select Local Disk.
5. Name the device **m2-1**. (This name can be any name defined by the user.)
6. Verify that the slot is named MSTOR-RAID. This name is fixed and must be the name used.

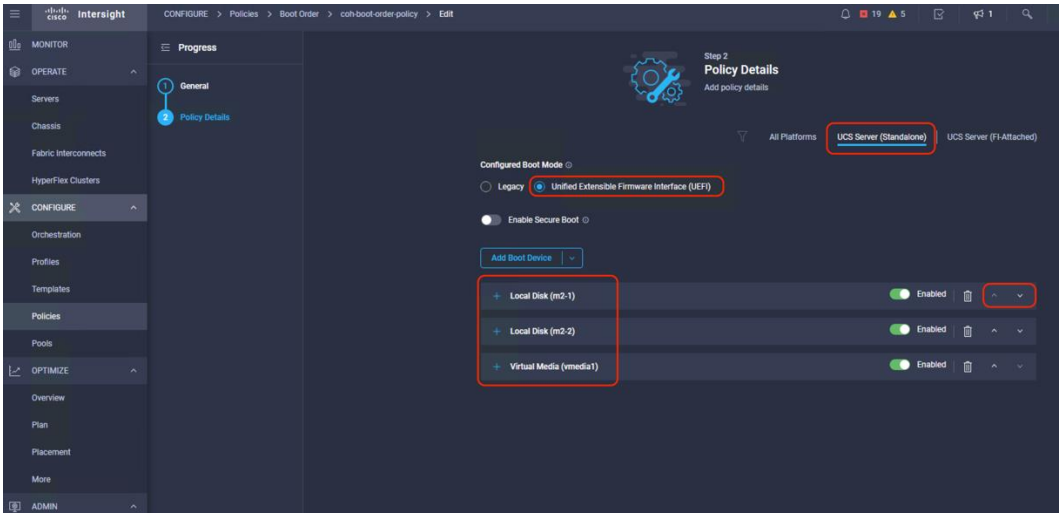


7. Again click Add Boot Device. Select Virtual Media.
8. Name the device **vmedia1**.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



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.

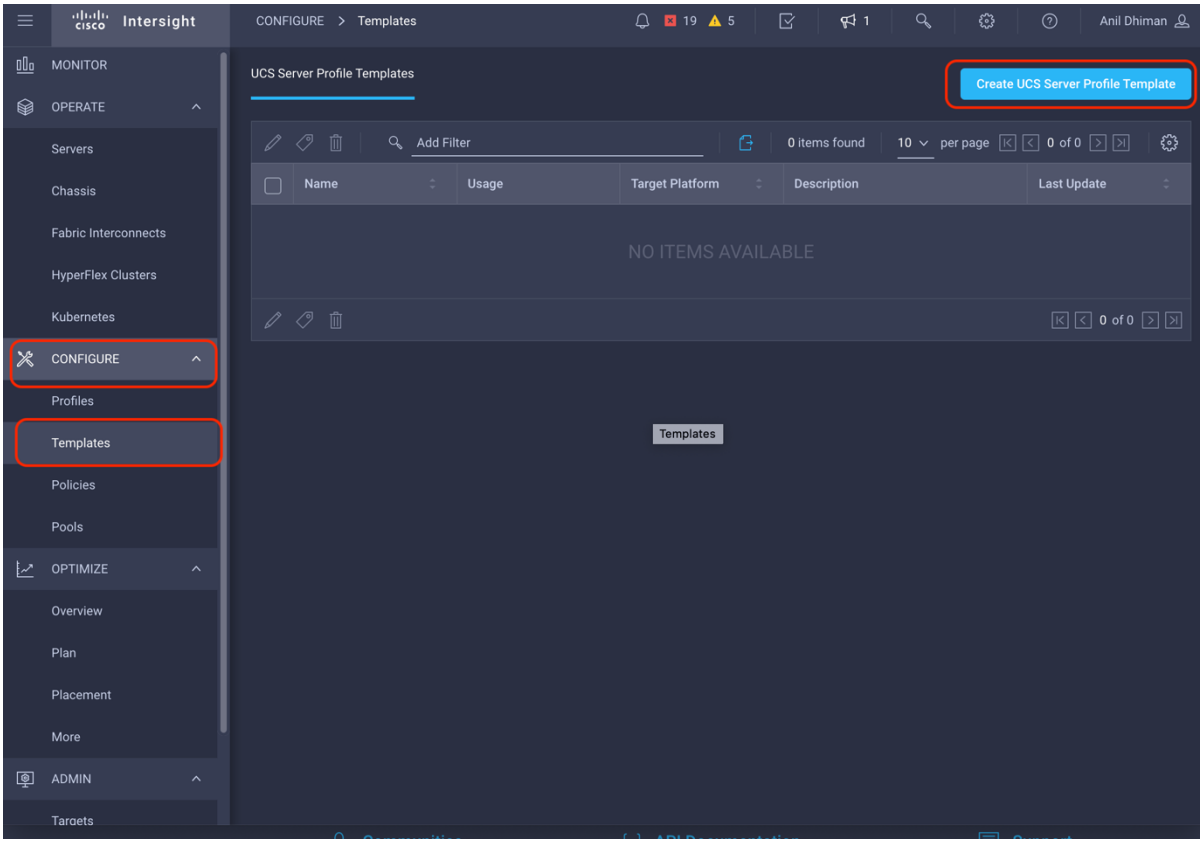
© 2021 Cisco and/or its affiliates. All rights reserved.

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

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

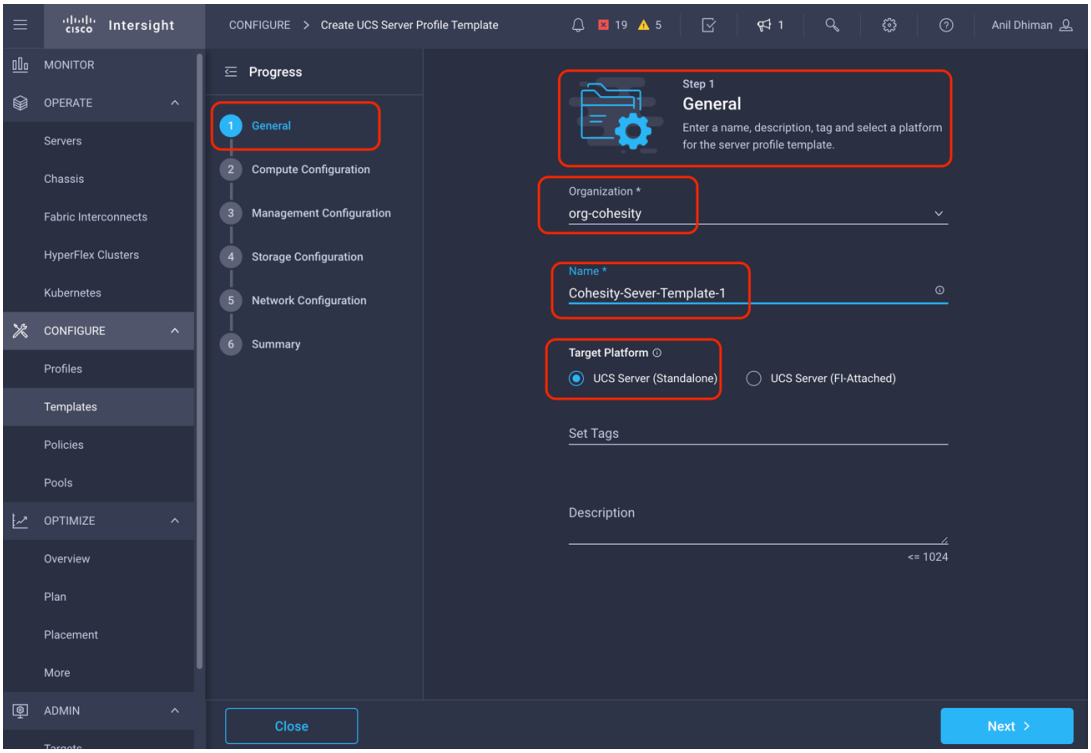
To create a server profile template, follow these steps:

1. Log in to the Cisco Intersight platform at https://intersight.com/.
2. Navigate to Operate > Configure > Templates. Click Create UCS Server Profile Template.

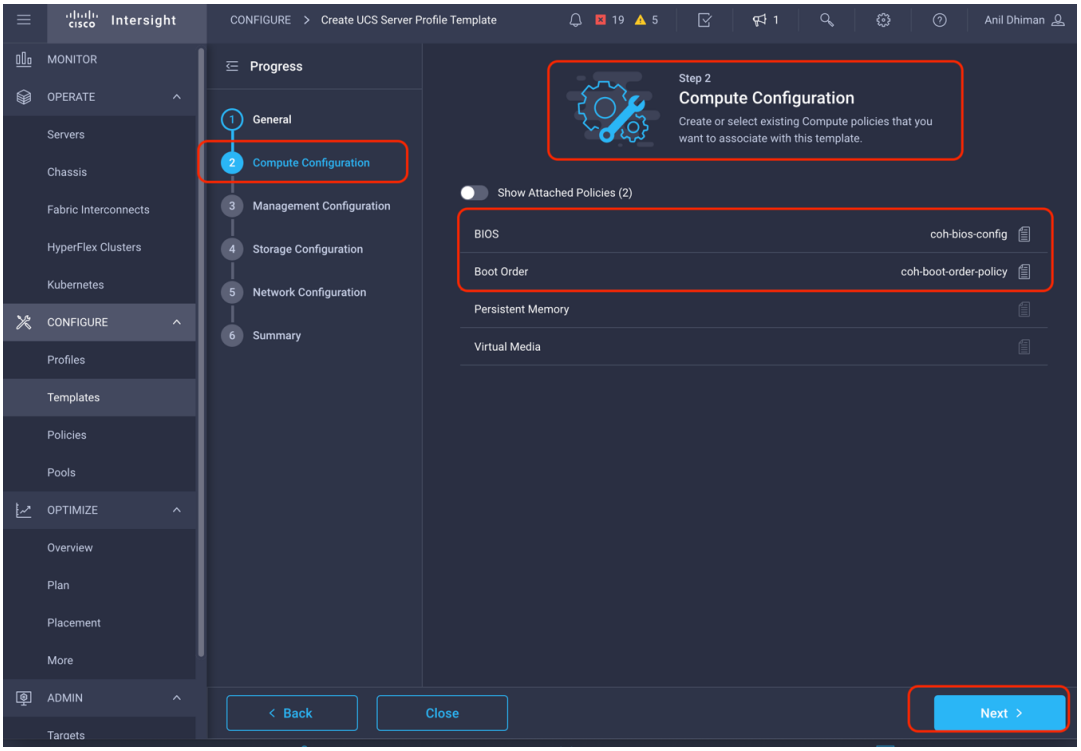


3. On the General page, do the following:
   - For Organization, choose org-cohesity (created in the previous section).
   - Name the template **Cohesity-Server-Template1**. (This name can be any name defined by user.)
   - For Target Platform, select UCS Server (Standalone).
   - Click Next.

© 2021 Cisco and/or its affiliates. All rights reserved.



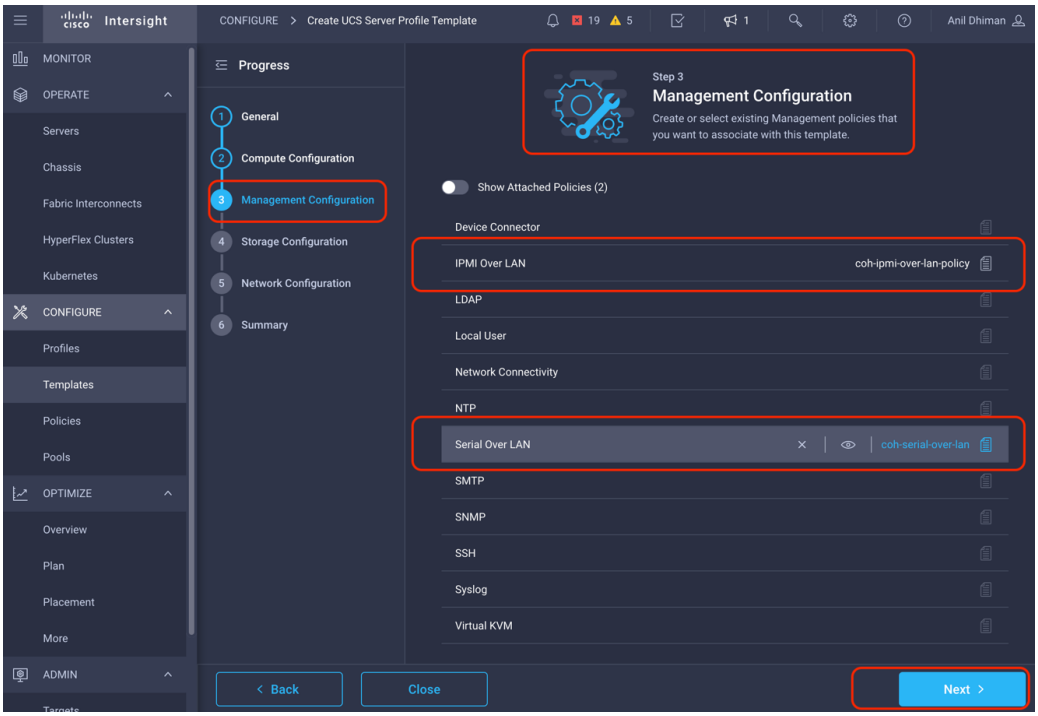
4. On the Compute Configuration page, select the server policies created earlier.
    - For BIOS, select coh-bios-policy.
    - For Boot Order, select coh-boot-order-policy.
    - Click Next.



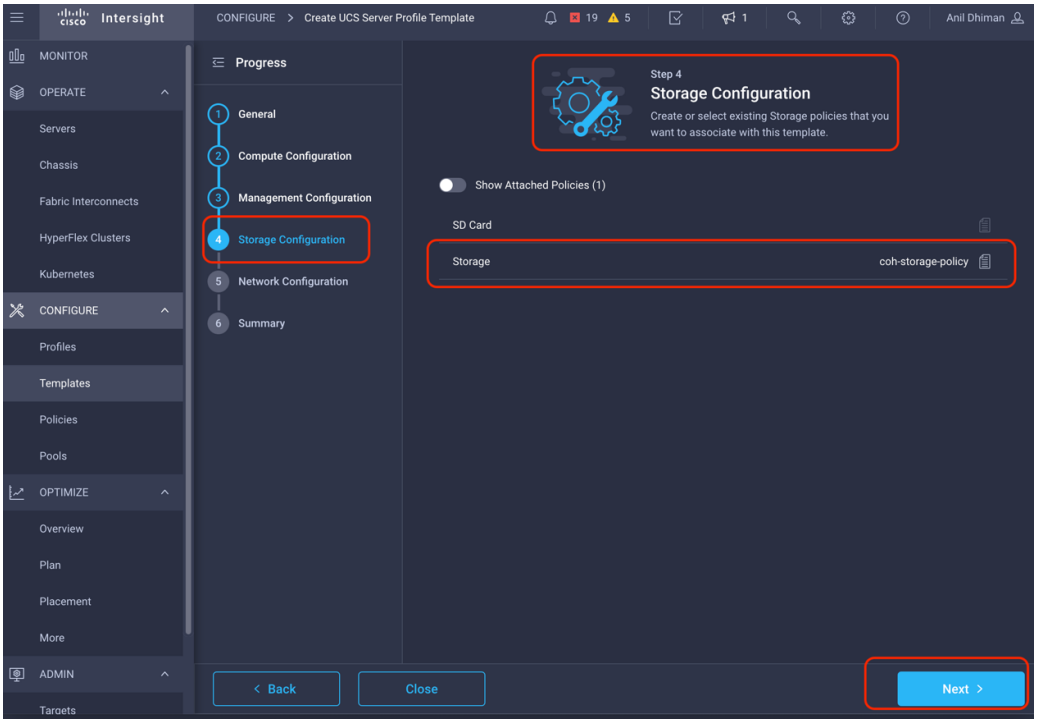
5. On the Managed Configuration page, select the appropriate policies.

© 2021 Cisco and/or its affiliates. All rights reserved.

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

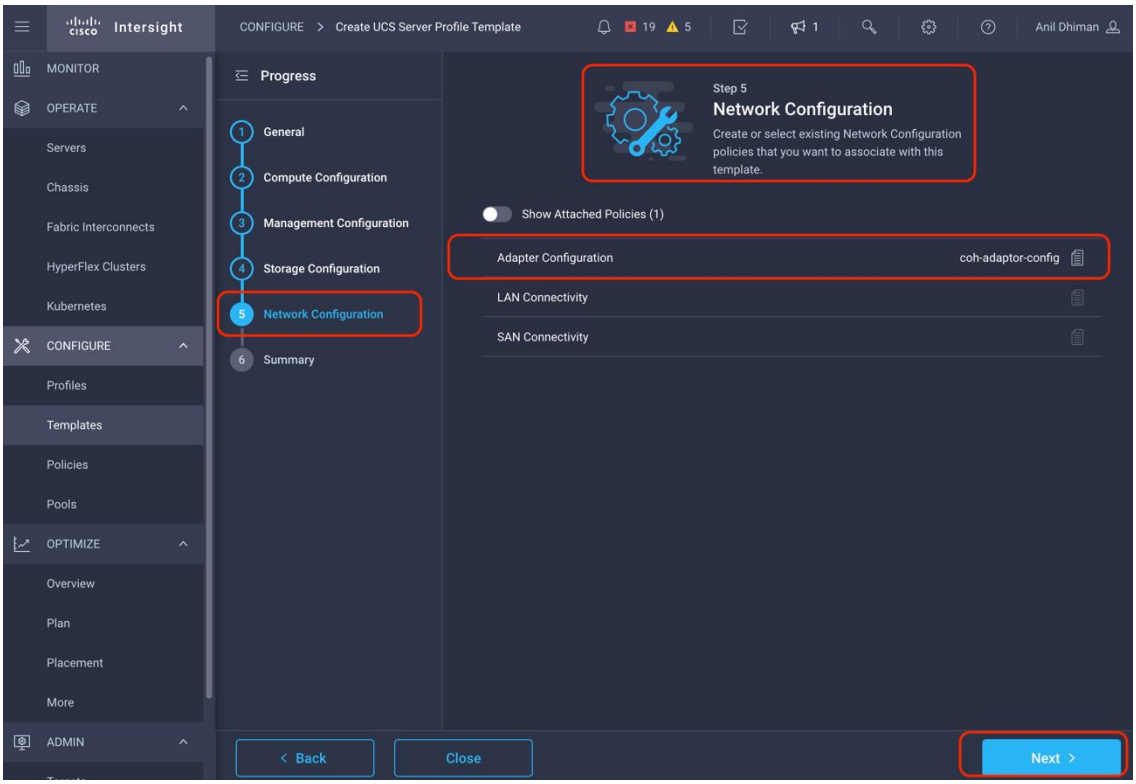


6. On the Storage Configuration page, do the following:
   - For Storage, select coh-storage-policy.
   - Click Next.

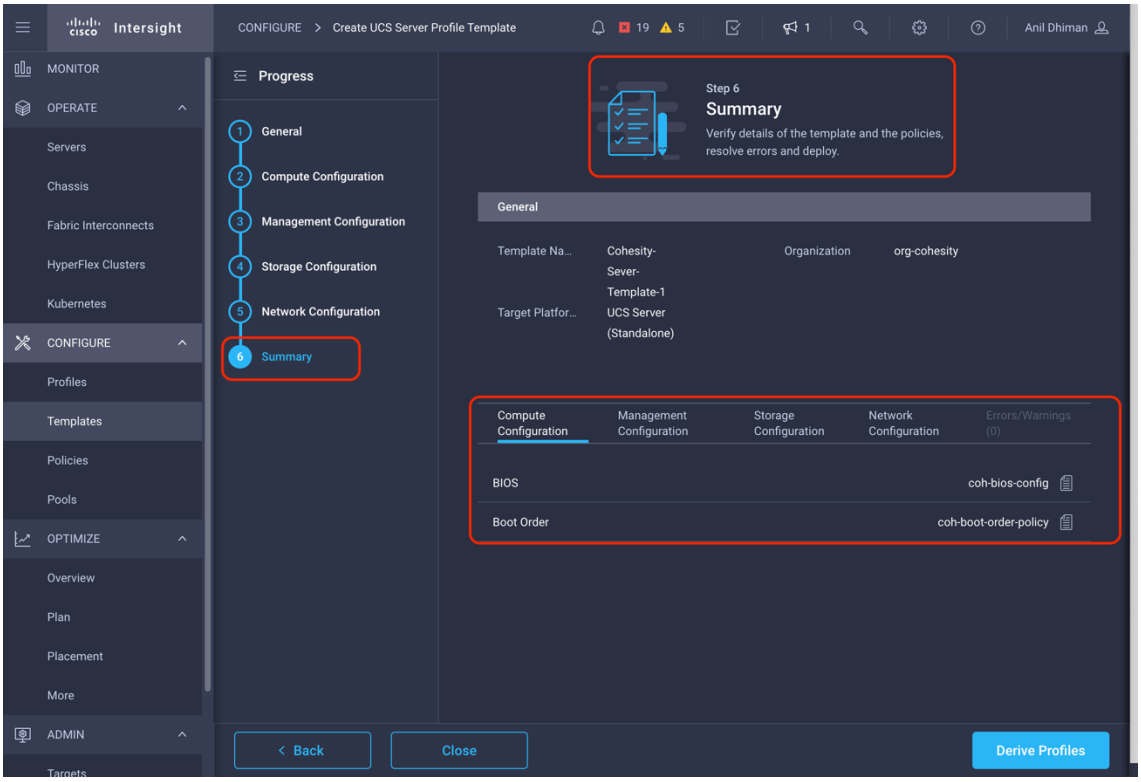


© 2021 Cisco and/or its affiliates. All rights reserved.

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

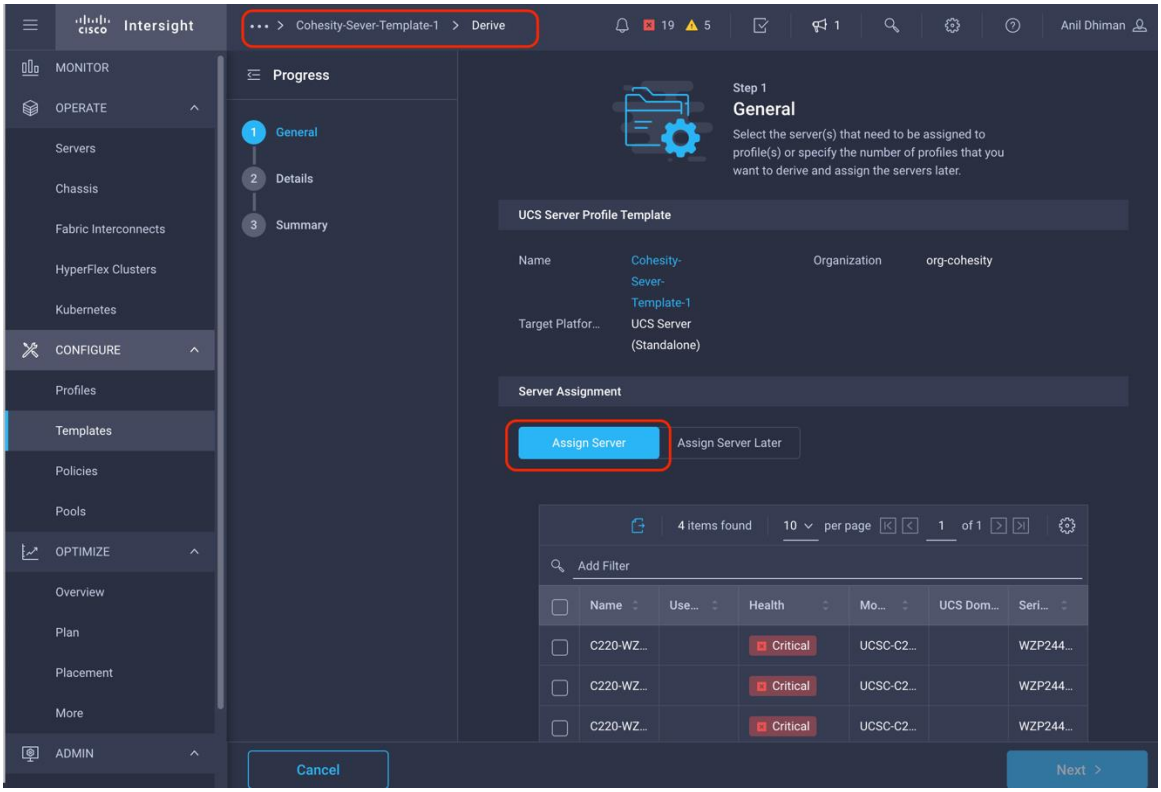


8. Review the summary on the Summary page and verify the settings. Then click Derive Profiles.

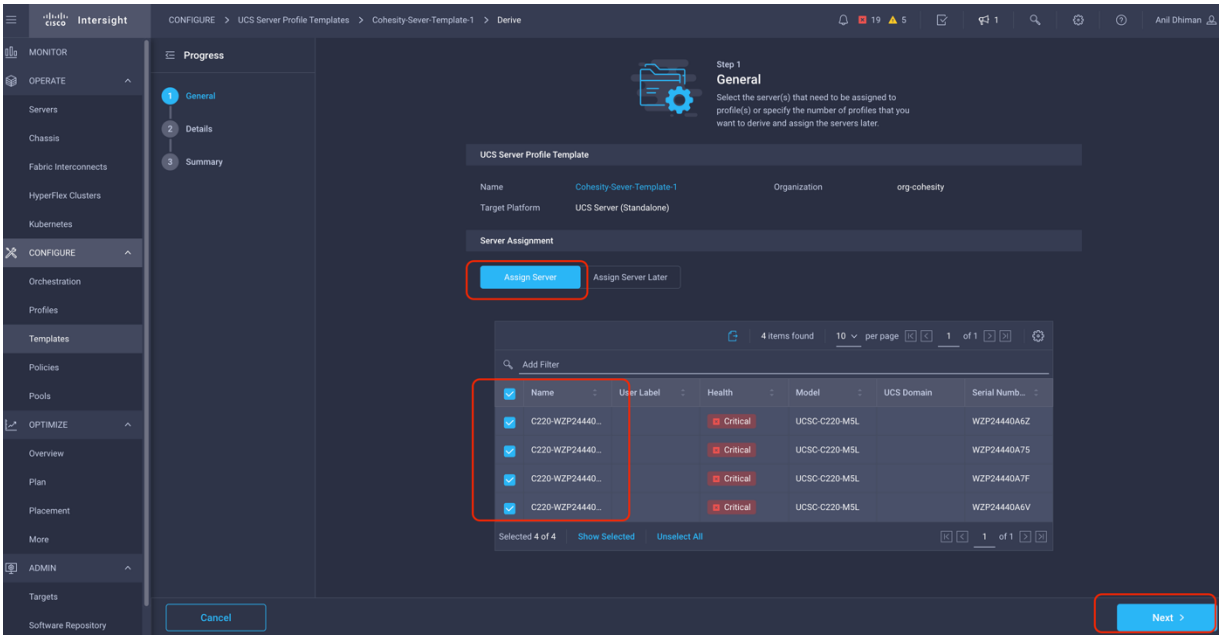


© 2021 Cisco and/or its affiliates. All rights reserved.

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.

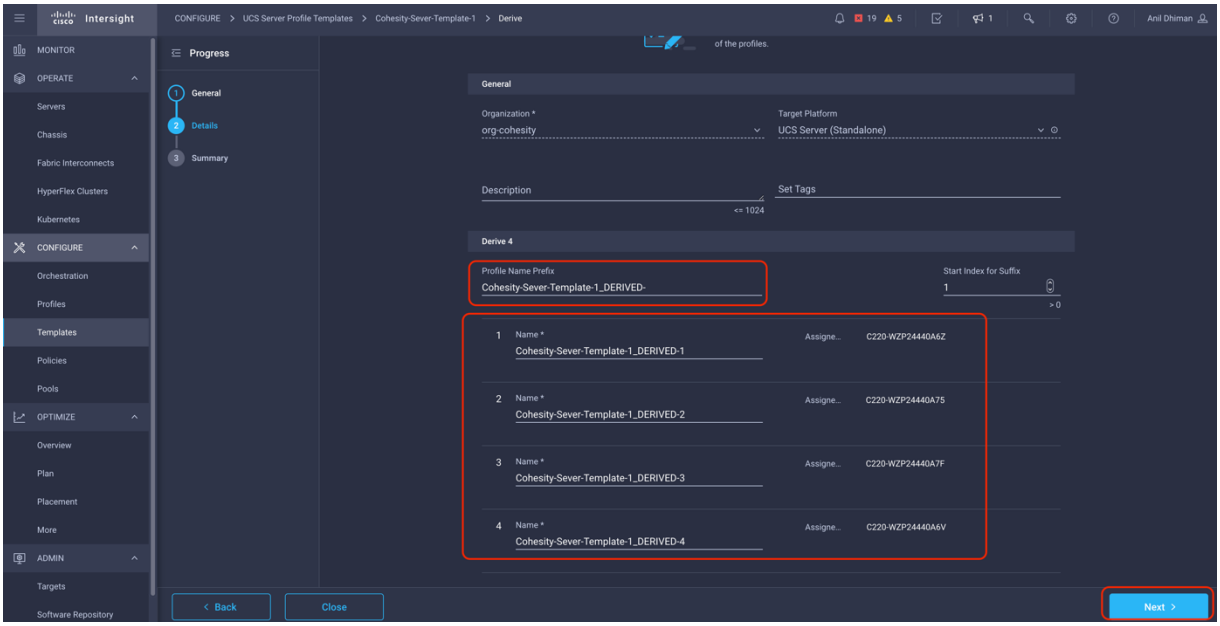


10. Select Assign Server and select all the nodes claimed in Cisco Intersight for Cohesity cluster deployment. Click Next.

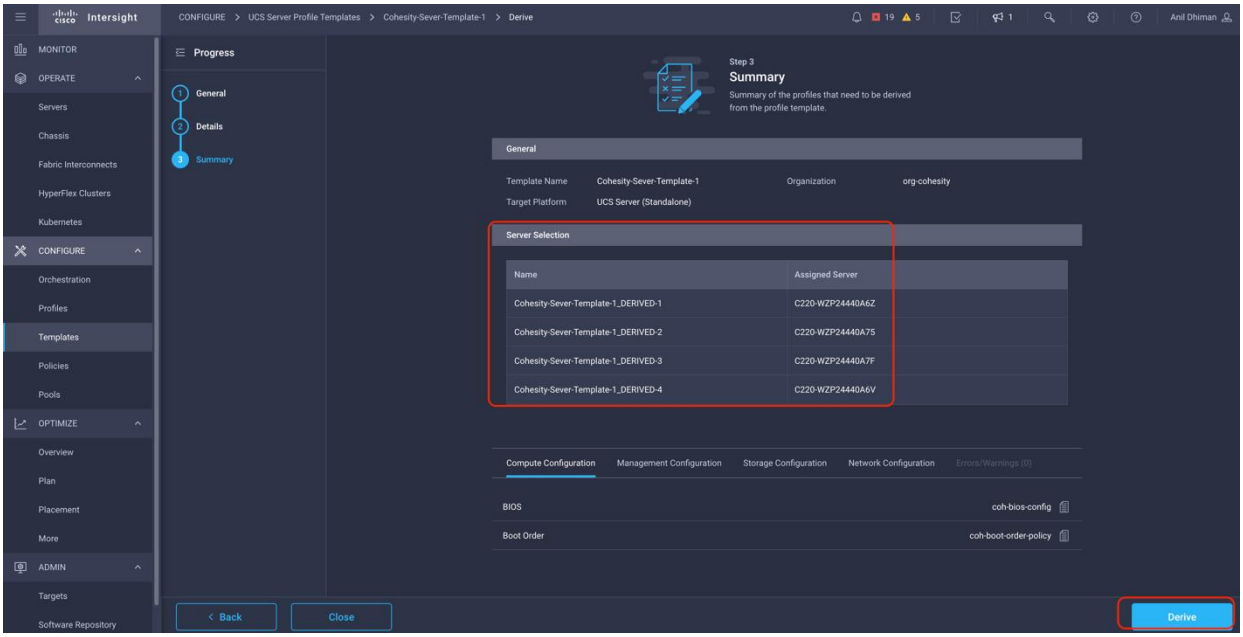


© 2021 Cisco and/or its affiliates. All rights reserved.

11. Edit the profile name prefix and click Next.

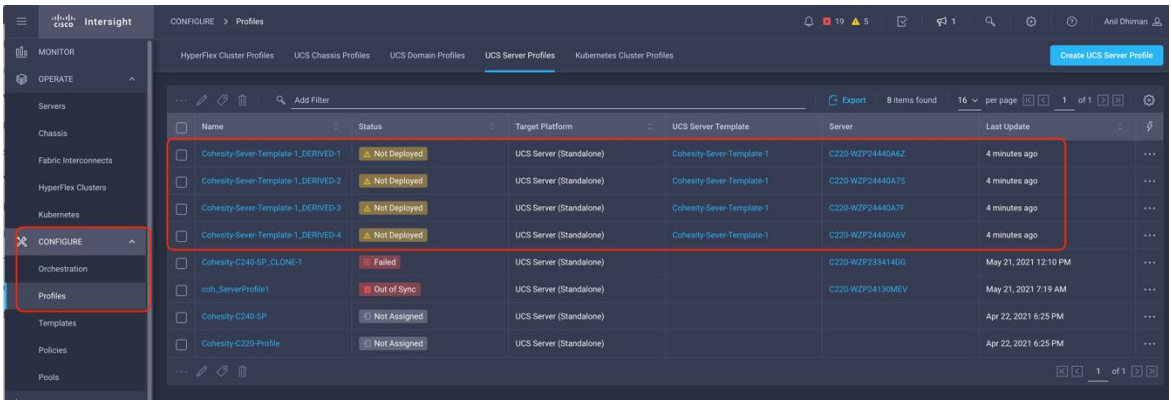


12. Review the Summary page and confirm the settings. Then click Derive.

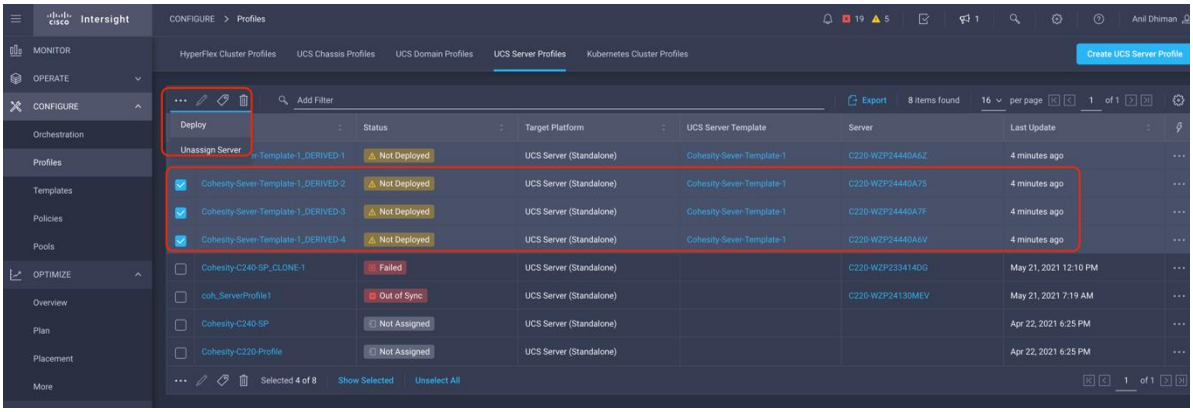


13. Navigate to Configure > Profiles and verify that the server profiles assigned to server nodes are in the Not Deployed state.

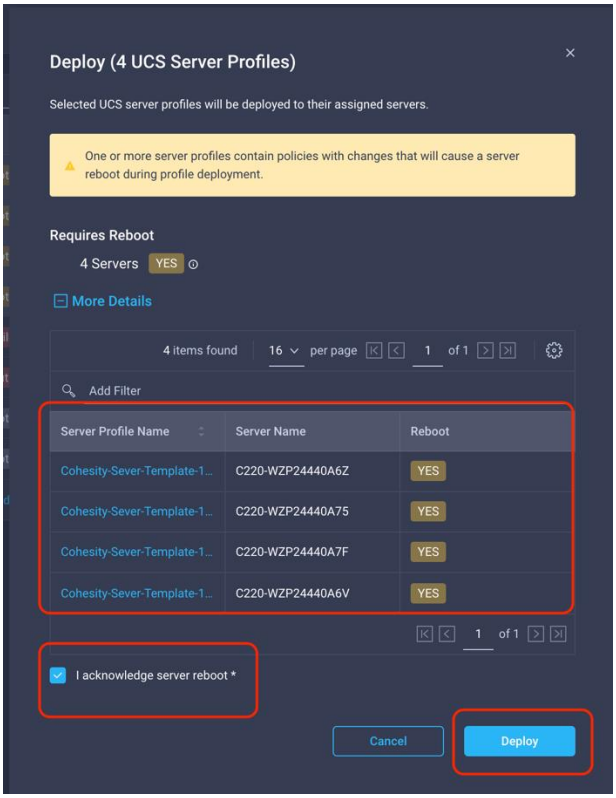
© 2021 Cisco and/or its affiliates. All rights reserved.



14. Select the Cohesity profiles and click Deploy.

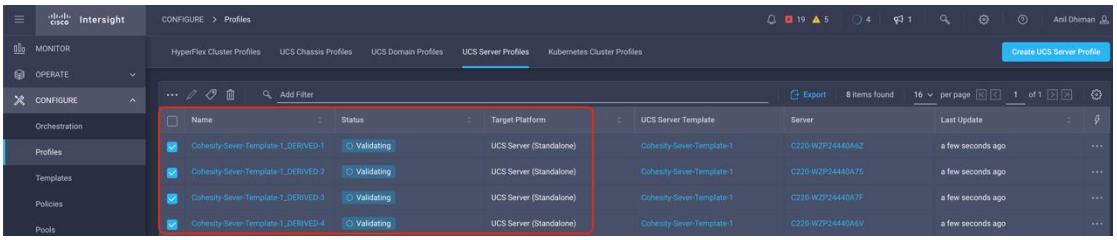


15. A new window opens. Acknowledge the server reboot and click Deploy.

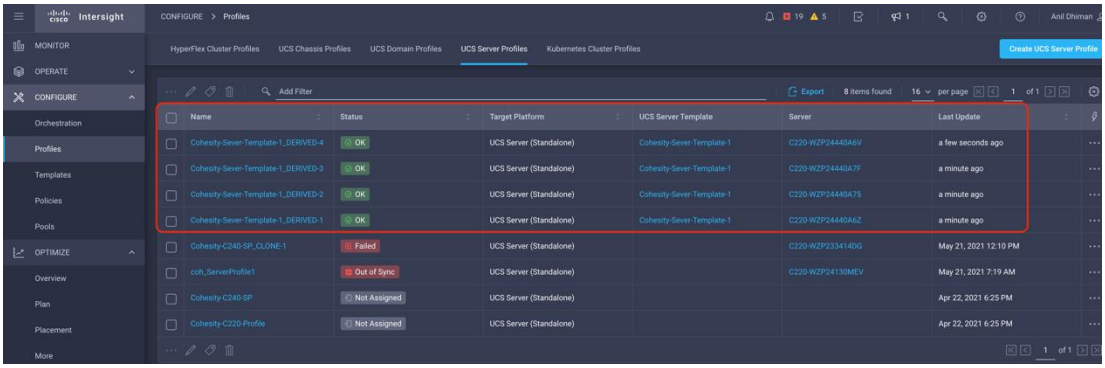


16. Monitor the deployment process. The state will transition from Validating to Configuring to OK.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



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.

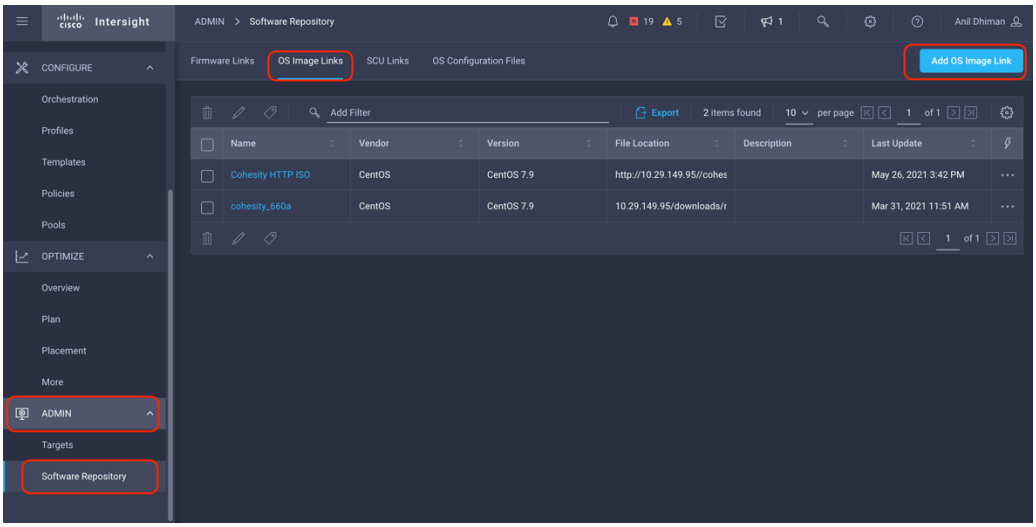
The following section presents the main requirements and supported process for successfully installing the Cohesity ISO file through the Cisco Intersight Install Operating System feature. Cisco Intersight provides several options for installing the OS. For more information, refer to Operating System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

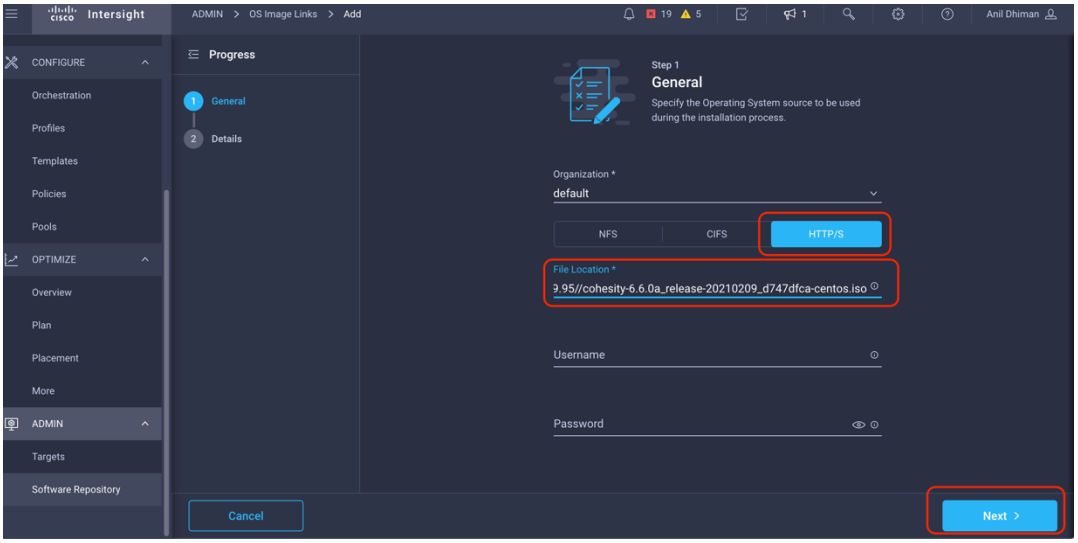
© 2021 Cisco and/or its affiliates. All rights reserved.

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

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

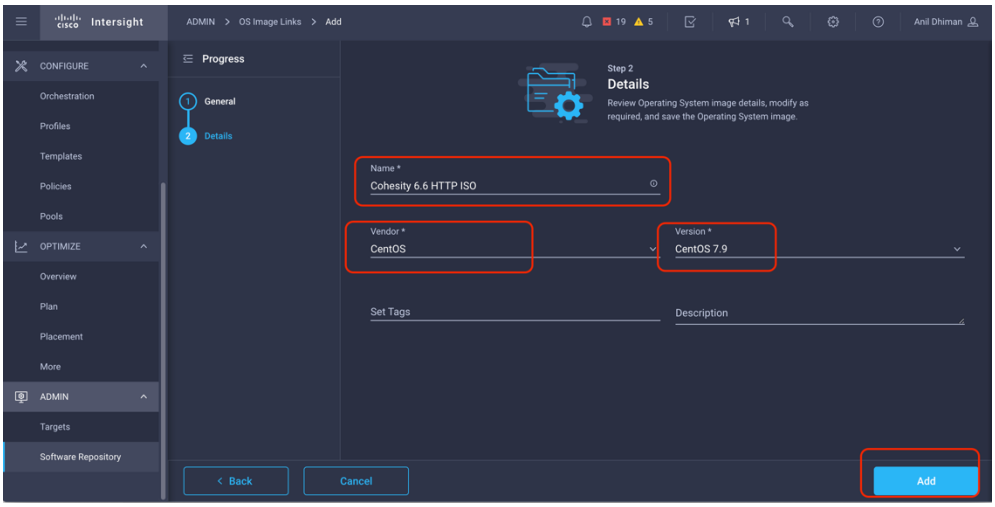


    - You can select Network File System (NFS), HTTP/S, or Common Internet File System (CIFS) to use to provide the location of the Cohesity ISO file to the Cisco Intersight Software Repository. This location will be accessed during OS installation. Click Next.



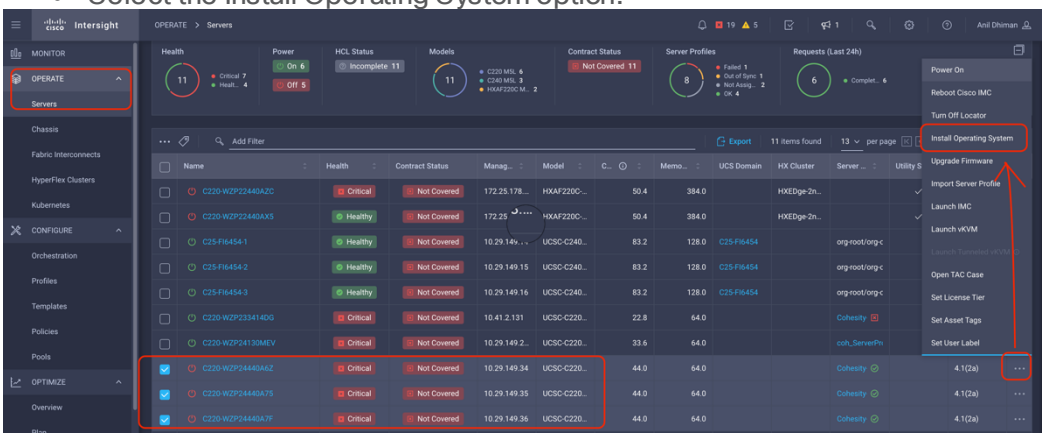
    - Add a name and specify CentOS as the vendor and Version 7.9. Click Add. This step will allow access to the Cohesity ISO file during OS installation.

© 2021 Cisco and/or its affiliates. All rights reserved.



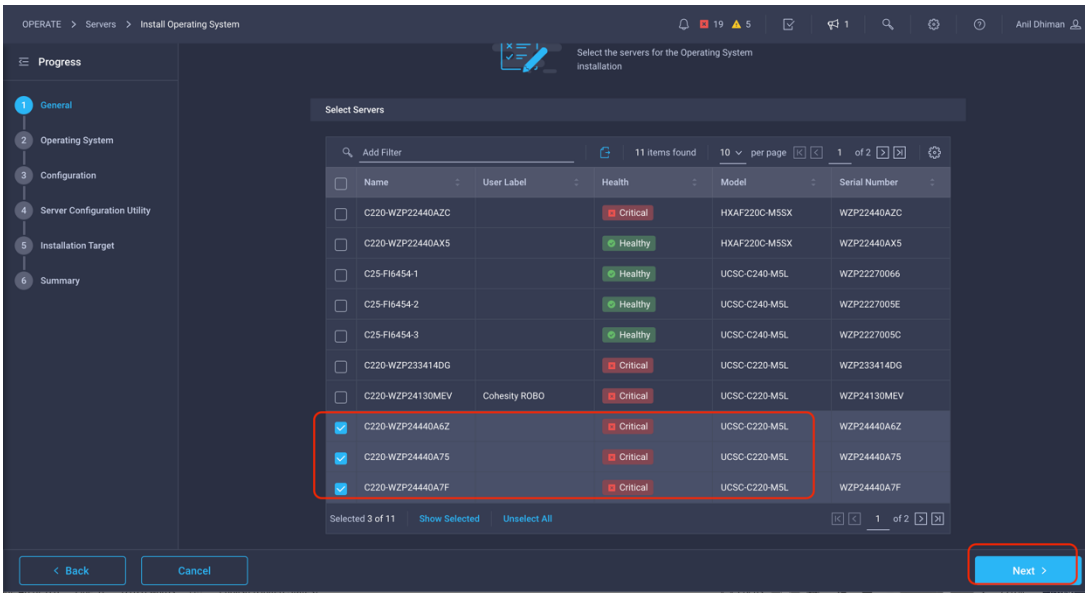
2. Install the Cohesity operating system. Verify that the Cisco Intersight license tier is set to at least the Advantage tier.

- Log in to the Cisco Intersight platform at [https://intersight.com/.](https://intersight.com/)
- Navigate to Operate > Servers and select the Cohesity nodes.
- Select the Install Operating System option.

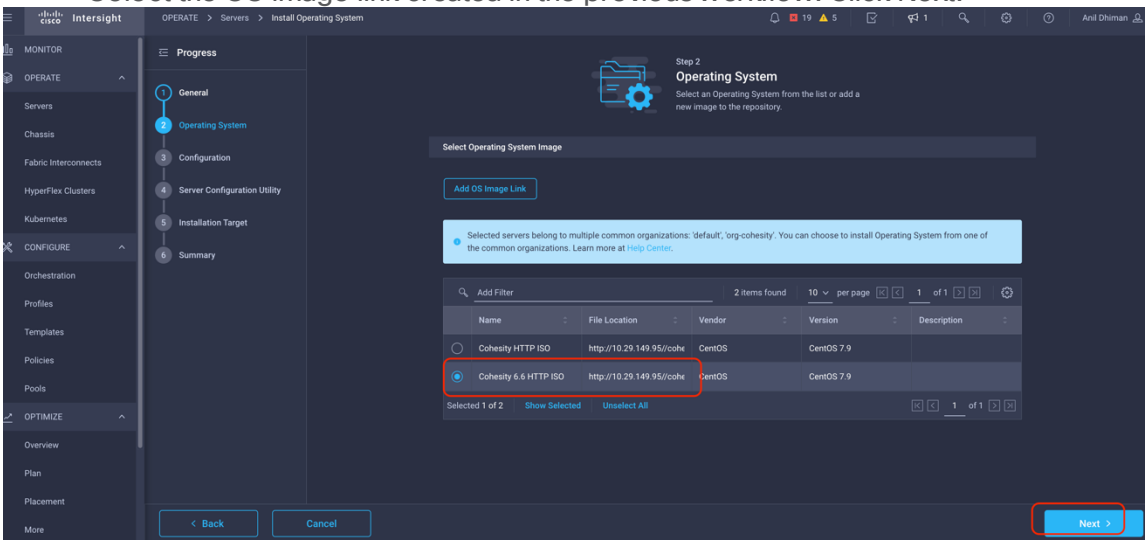


- Verify that all the nodes are selected. Click Next.

© 2021 Cisco and/or its affiliates. All rights reserved.

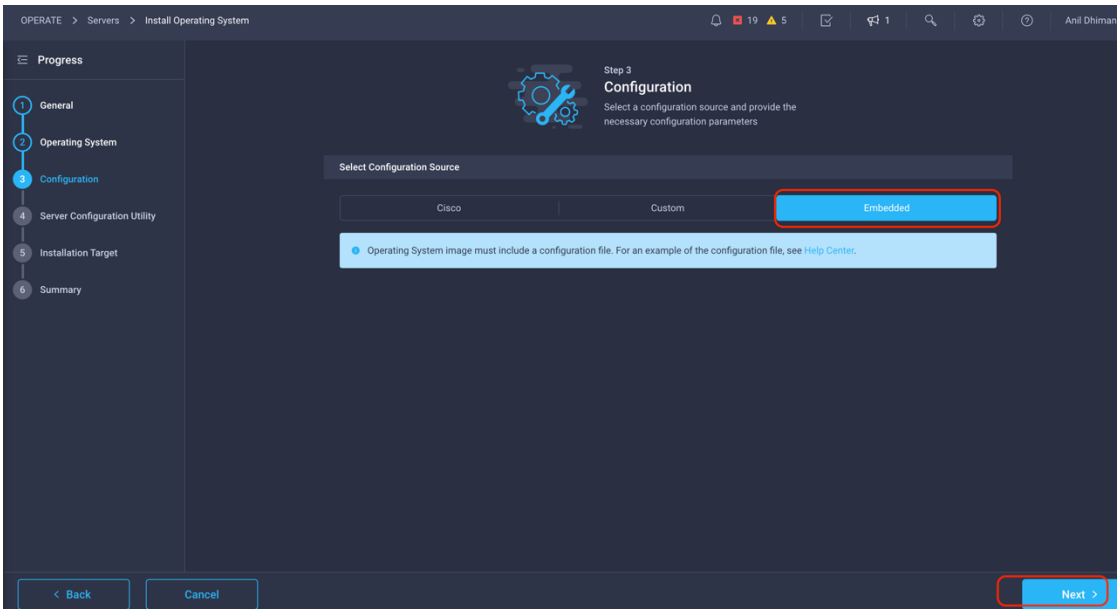


- Select the OS image link created in the previous workflow. Click Next.

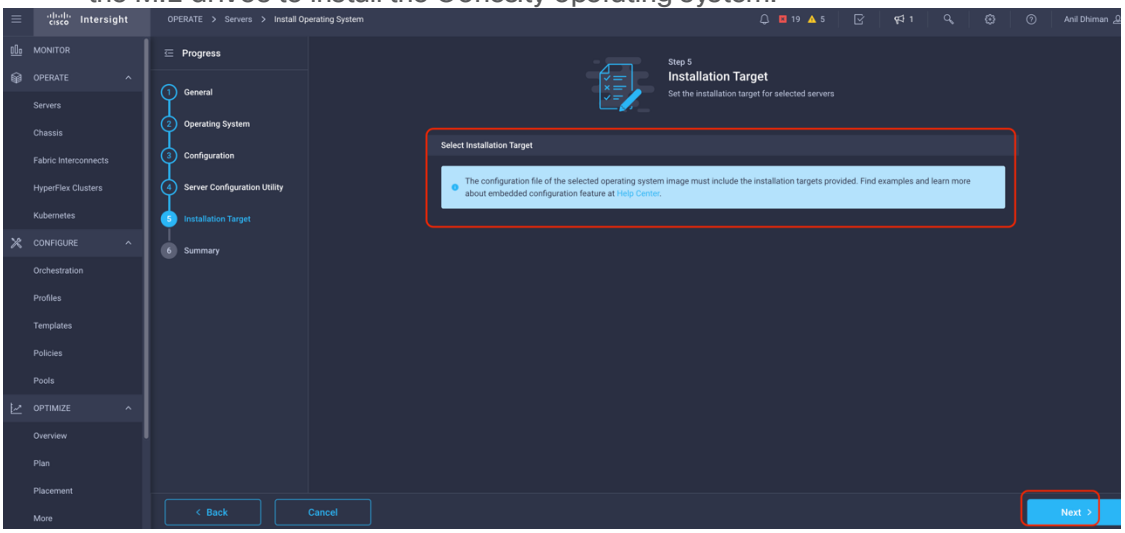


- Select the Embedded tab and click Next.

© 2021 Cisco and/or its affiliates. All rights reserved.

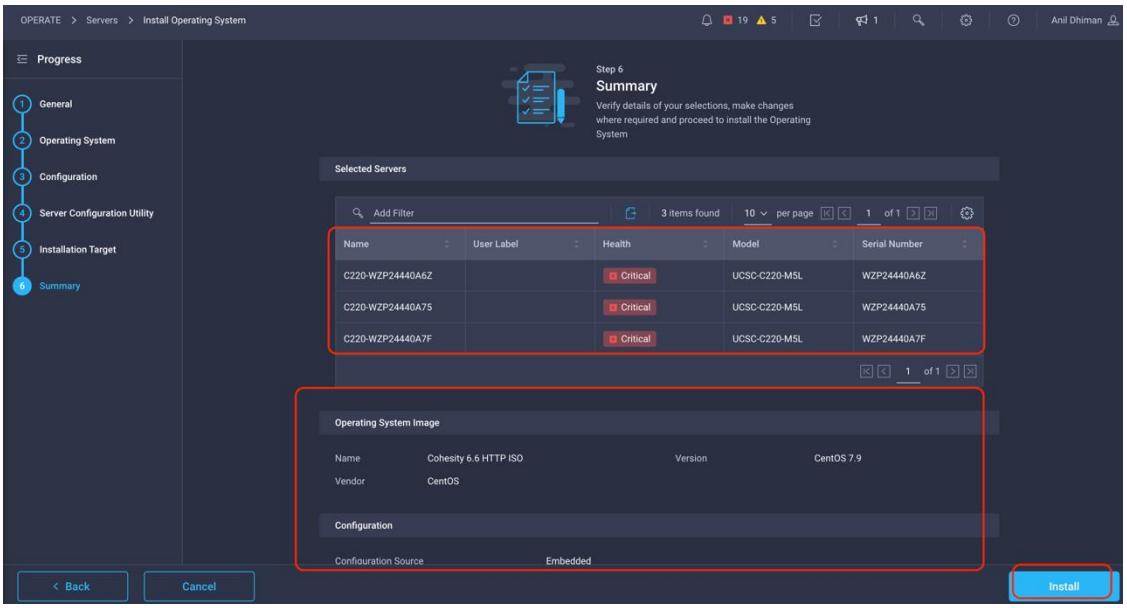


- On the Server Configuration Utility screen, click Next.
- On the Select Installation Target screen, click Next. The Cohesity ISO file will automatically identify the M.2 drives to install the Cohesity operating system.

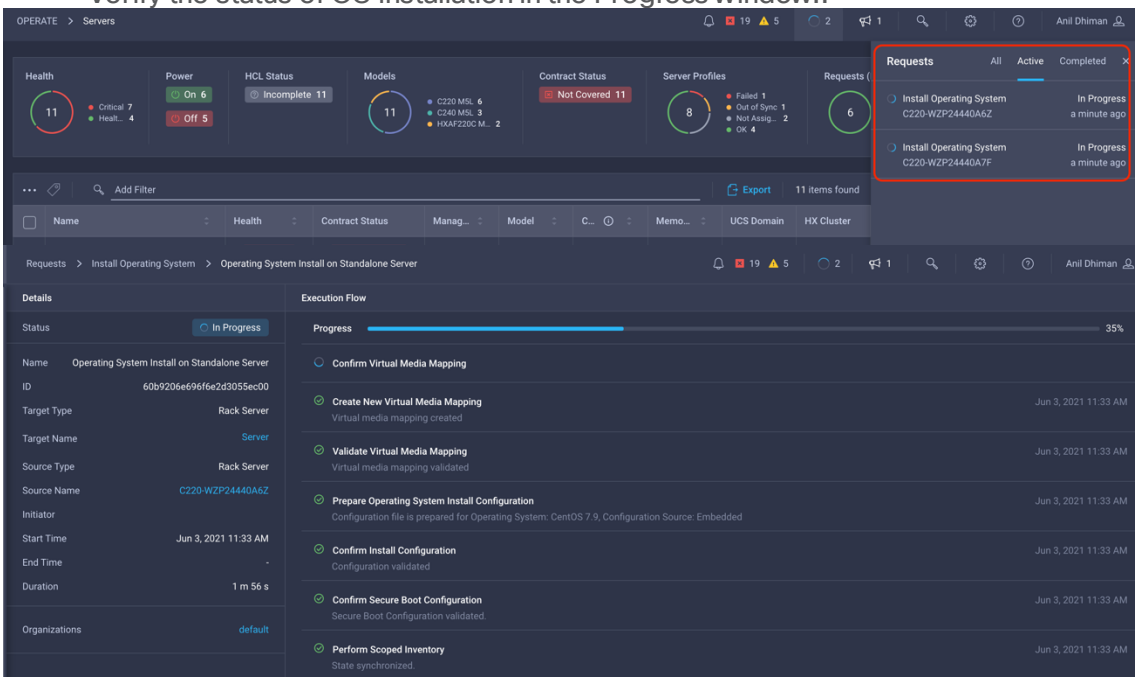


- Verify the Cohesity nodes and Cohesity ISO target repository and click Install. Confirm the process in the warning window and click Install.

© 2021 Cisco and/or its affiliates. All rights reserved.

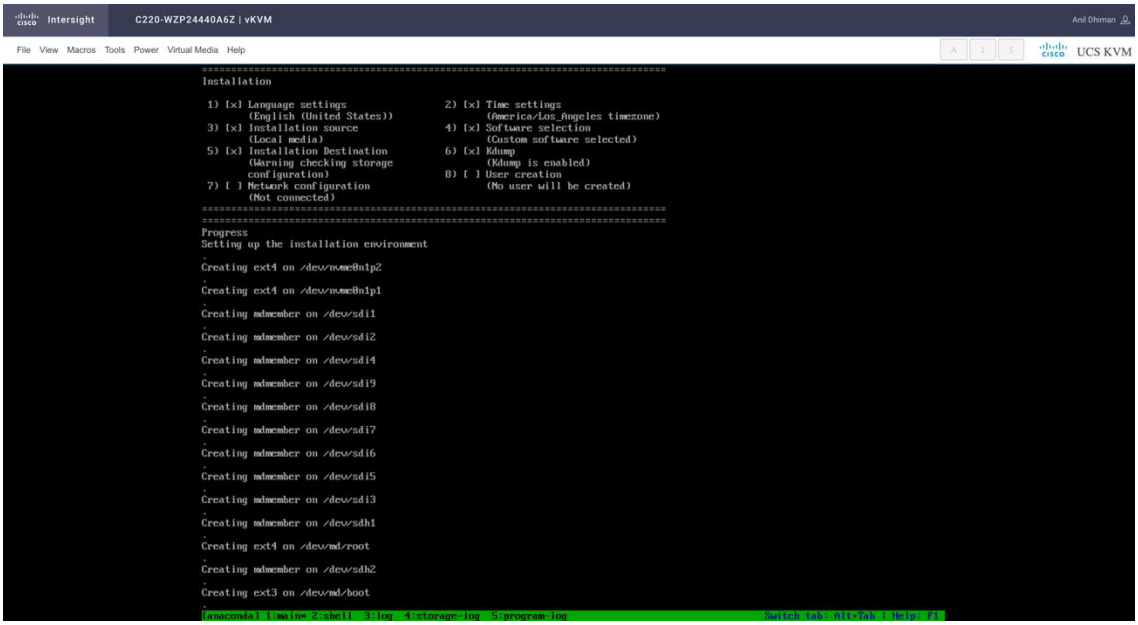


- Verify the status of OS installation in the Progress window..

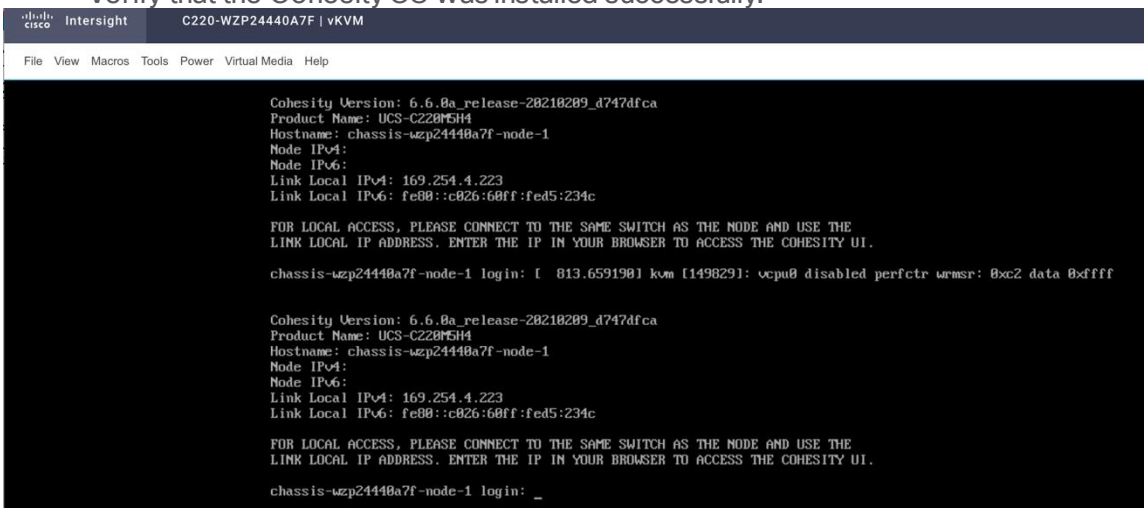


- Monitor the progress of the Cohesity ISO file installation through a virtual KVM (vKVM) session.

© 2021 Cisco and/or its affiliates. All rights reserved.

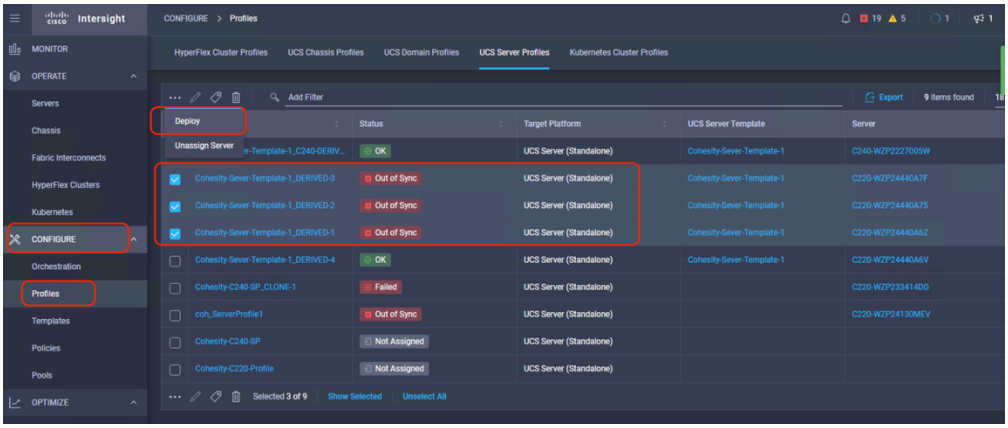


- Verify that the Cohesity OS was installed successfully.

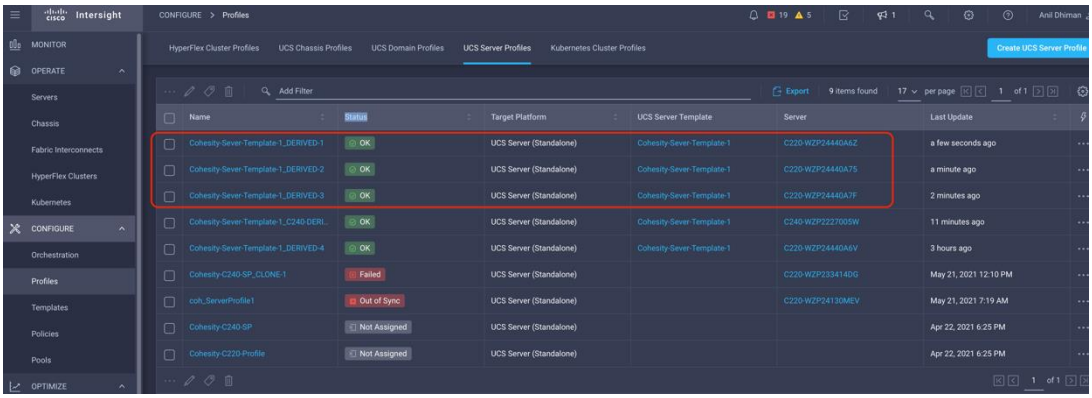


- After Cohesity OS installation through the Cisco Intersight platform, the server profiles become out of sync. This loss of synchronization occurs because of the configuration of the one-time boot order to install the operating system.
  - Go to Configure > Profiles.
  - Select the out-of-sync profiles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

© 2021 Cisco and/or its affiliates. All rights reserved.



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



- 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.

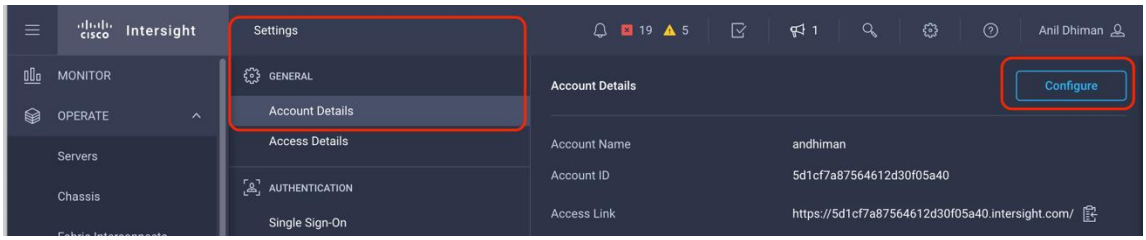
Note: Installation of the Cohesity operation system through the one-time boot device feature requires at least a Cisco Intersight Essential license.

© 2021 Cisco and/or its affiliates. All rights reserved.

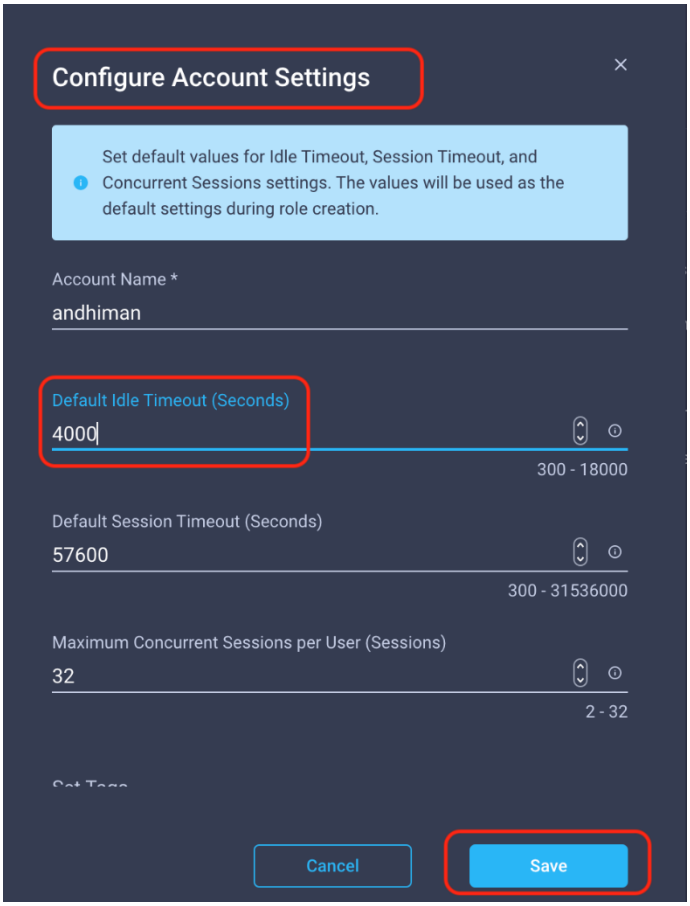
Extending vKVM timeout

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

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



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

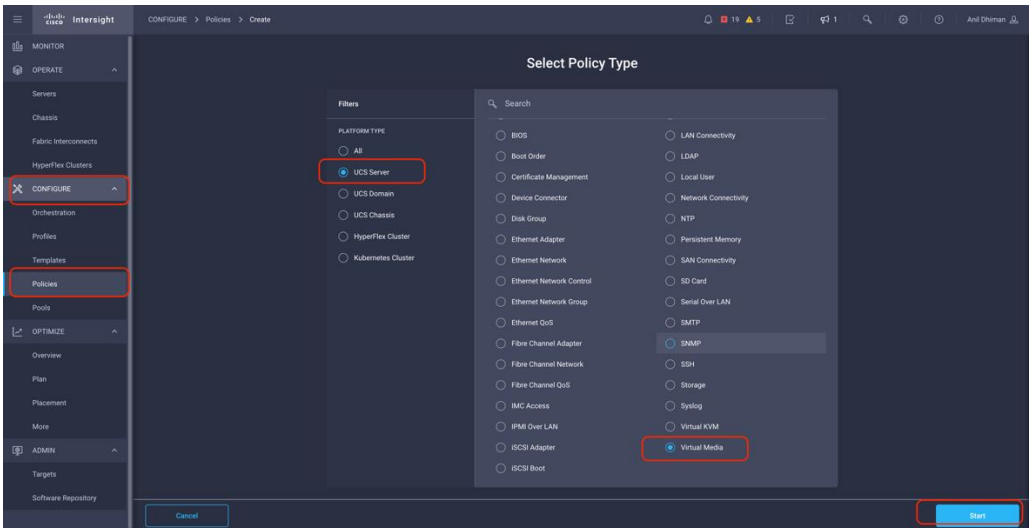


Creating and attaching a new vMedia policy to the server profile template

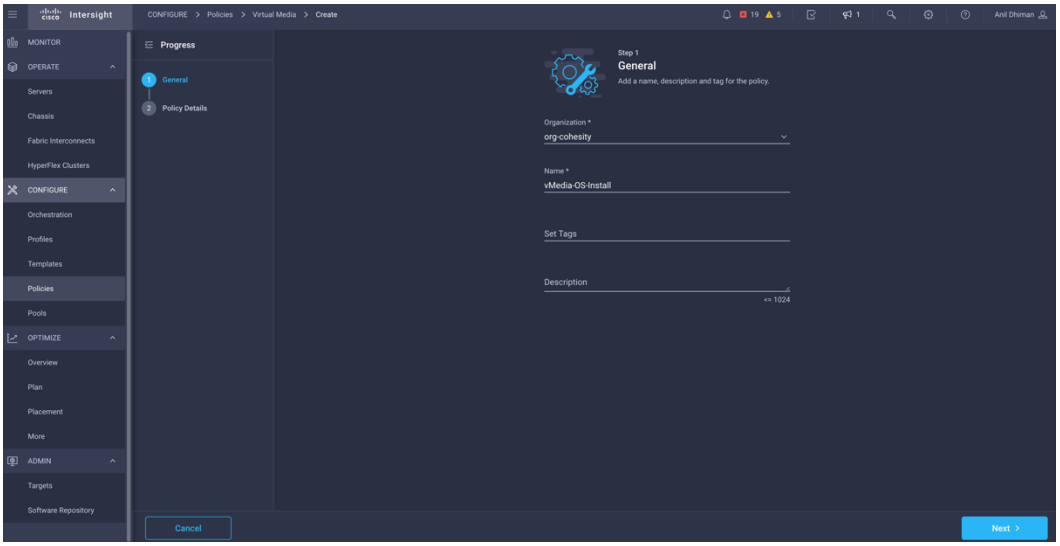
Follow these steps to create and attach a new vMedia policy to the server profile template:

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

© 2021 Cisco and/or its affiliates. All rights reserved.

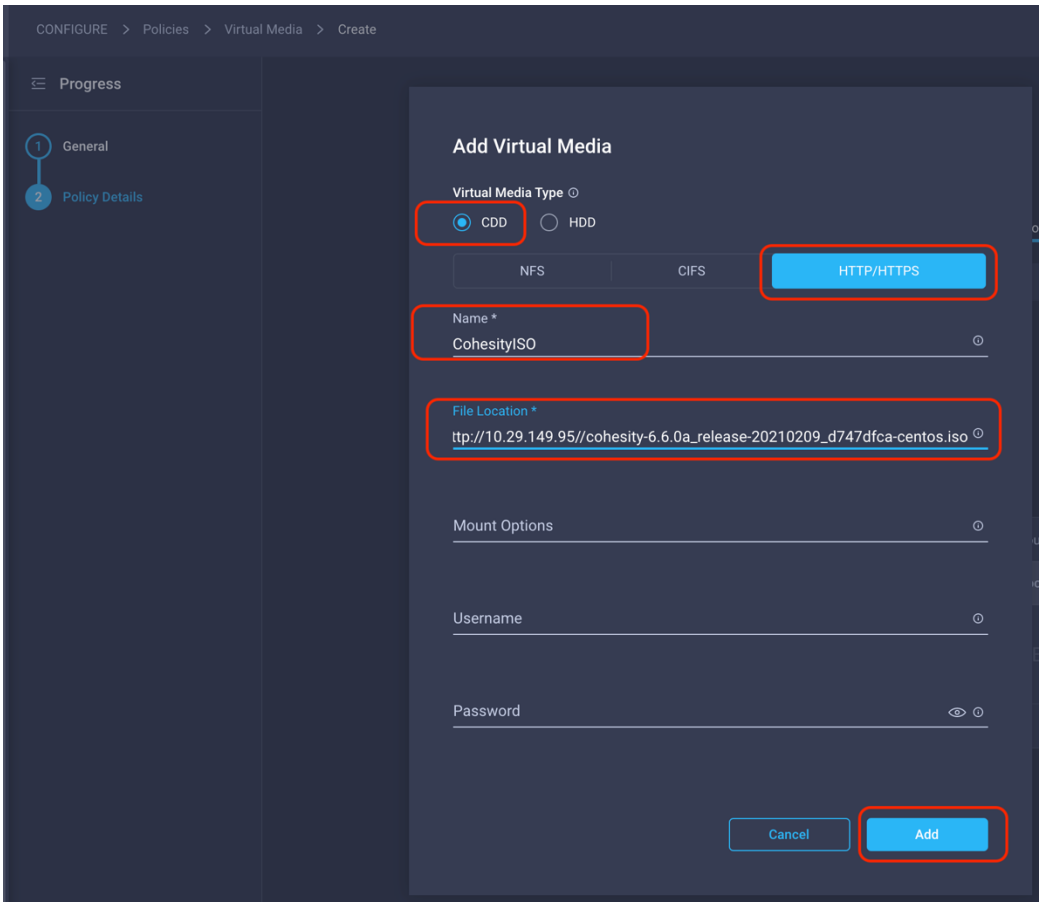


4. For Organization, select org-cohesity, and for the policy name, enter **vMedia-OS-Install**. Then click Next.

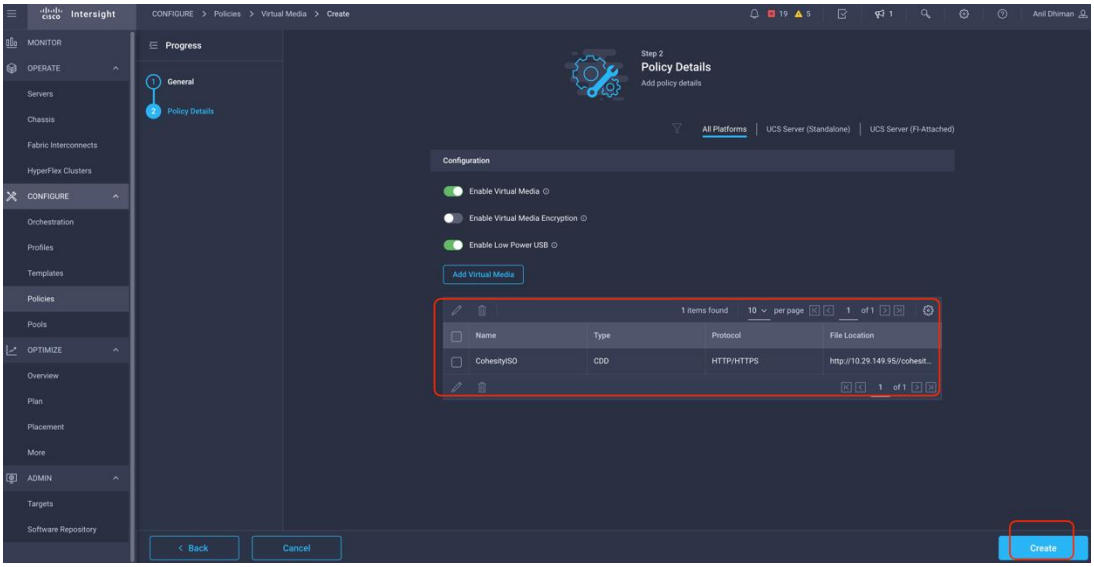


5. Leave the configuration at the default settings and click Add Virtual Media.
6. On the Add Virtual Media screen, add the mount points of the Cohesity ISO file on the NFS, HTTP/HTTPS, or CIFS server. Click Add.

© 2021 Cisco and/or its affiliates. All rights reserved.



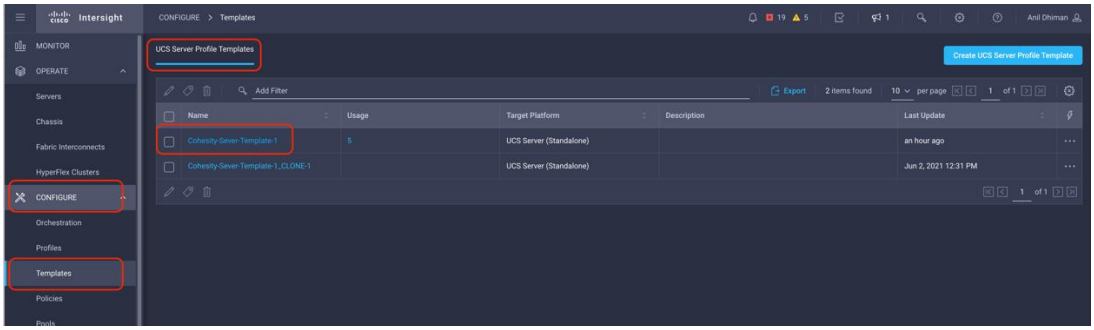
7. Click Create to create the new vMedia policy.



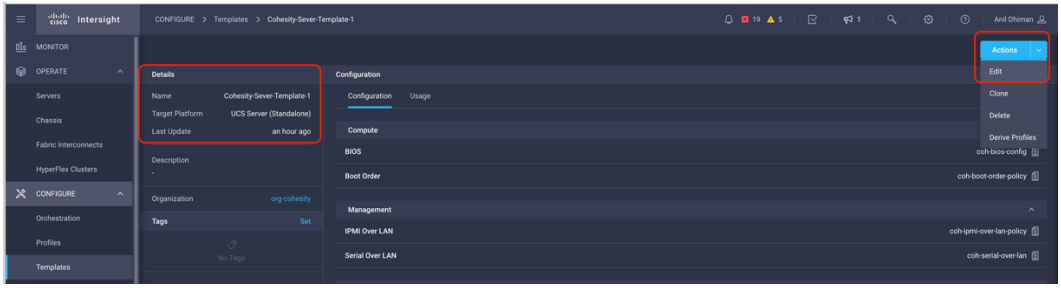
8. After the vMedia policy has been created, edit the server profile template to add the new vMedia policy.

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.

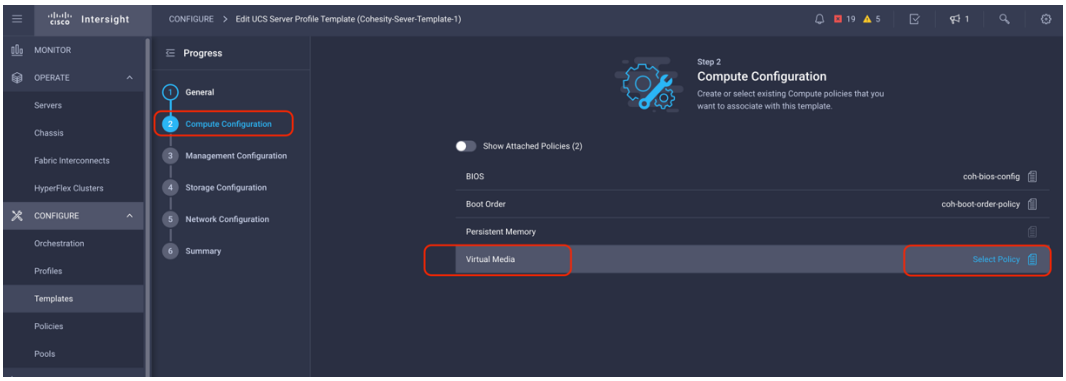
© 2021 Cisco and/or its affiliates. All rights reserved.



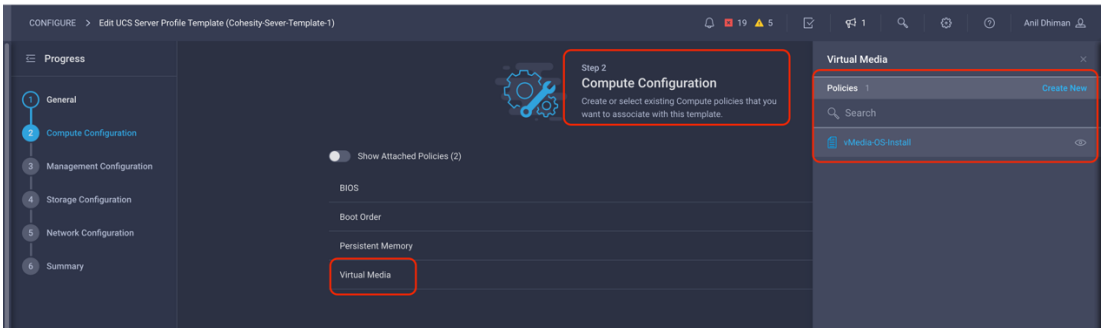
10. From Actions in the top-right corner, select Edit.



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

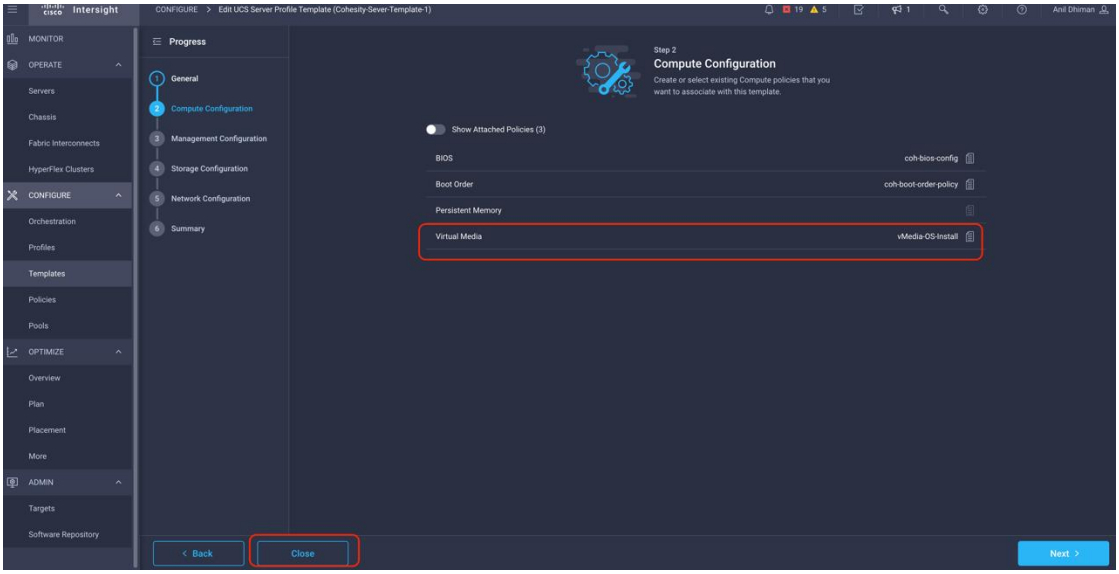


12. Select the vMedia-OS-Install policy created in the previous section.

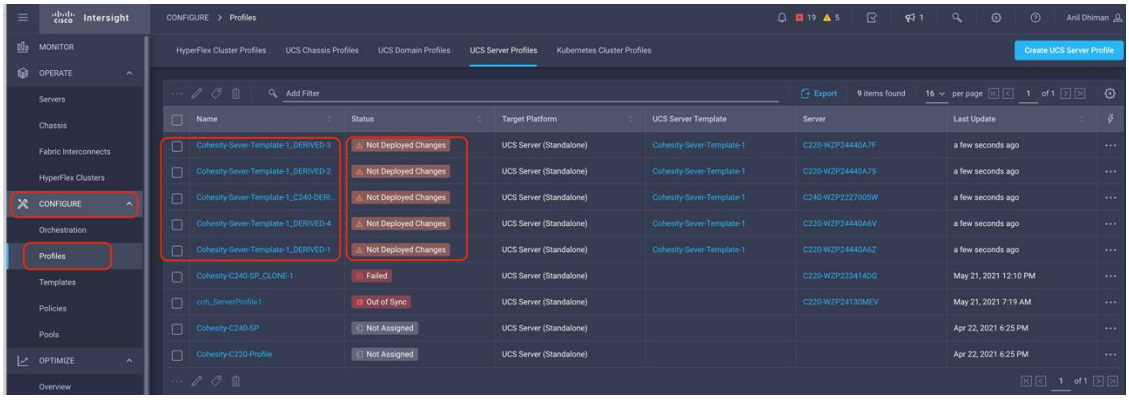


13. Click Close. The server profile template will be configured with the vMedia policy.

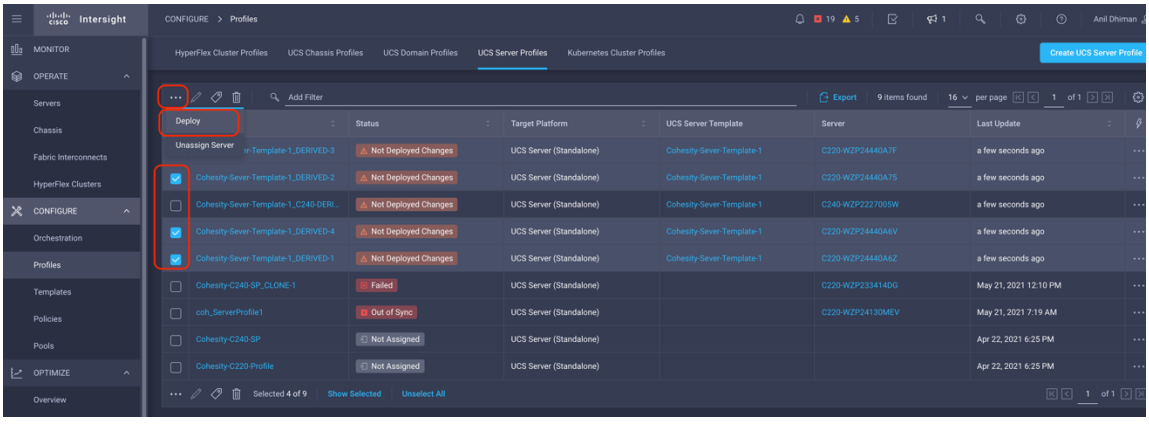
© 2021 Cisco and/or its affiliates. All rights reserved.



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

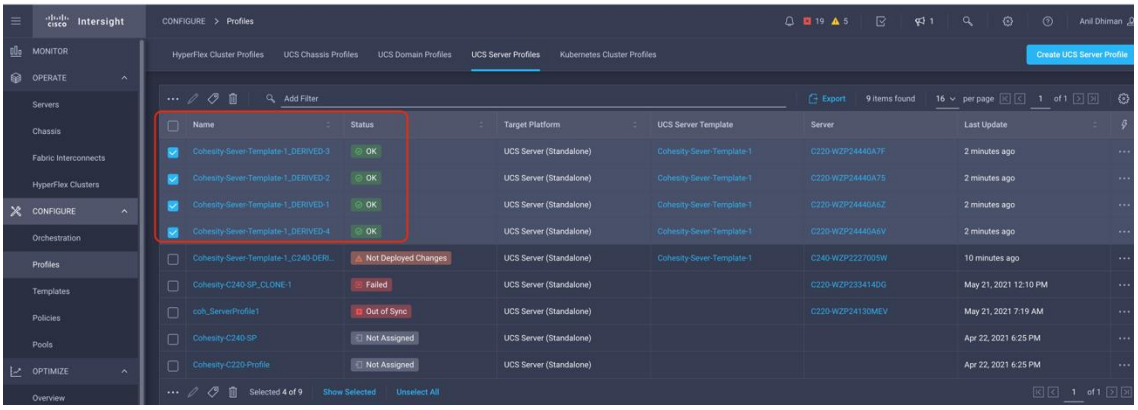


15. Select the Cohesity server profiles, Click the Options icon (...) and select Deploy. This action will deploy the vMedia changes to the Cohesity server profiles.



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.

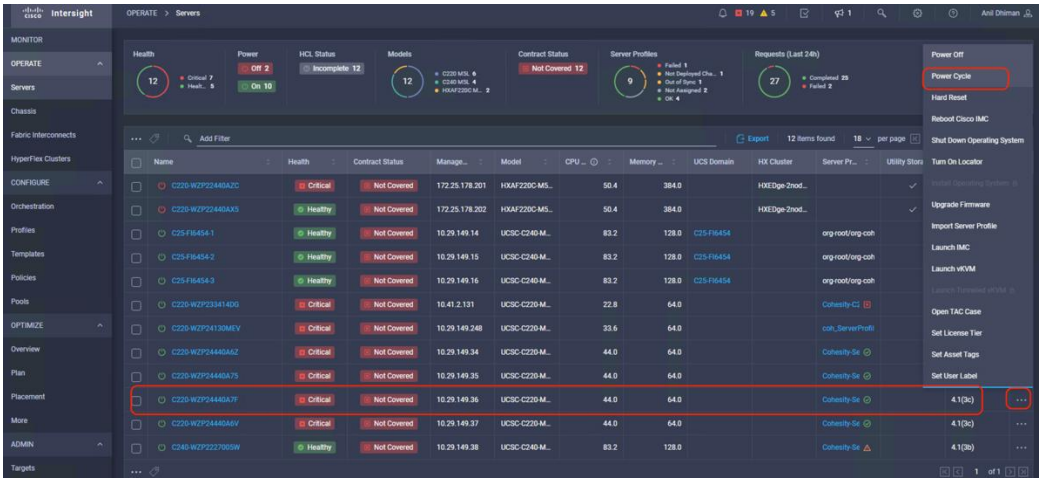
© 2021 Cisco and/or its affiliates. All rights reserved.



Installing the Cohesity OS through one-time boot device

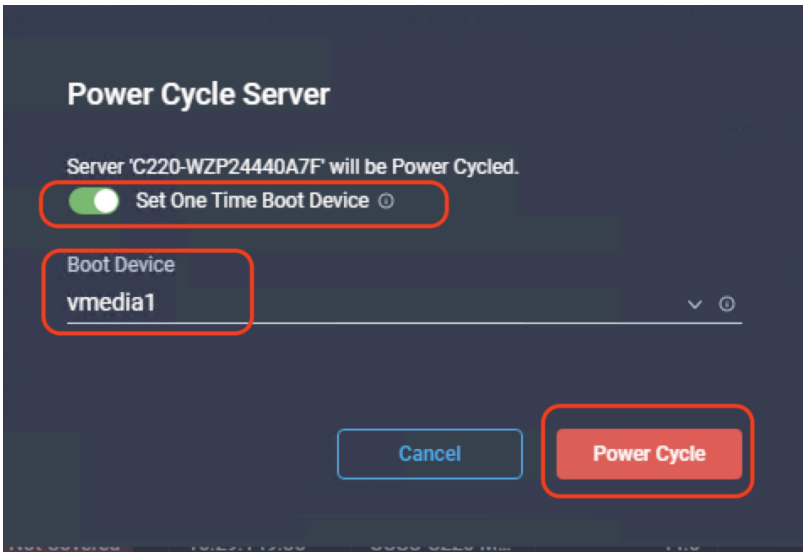
Follow these steps to install the Cohesity operating system through the one-time boot device feature:

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.

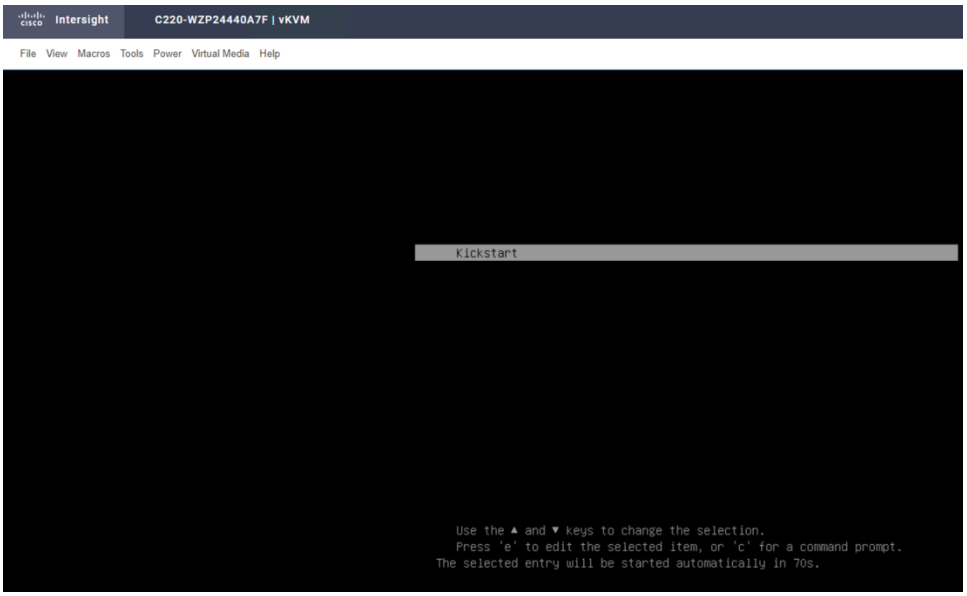


4. On the Power Cycle Server screen, enable One Time Boot Device and select vmedia1 as the boot device.

© 2021 Cisco and/or its affiliates. All rights reserved.



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.



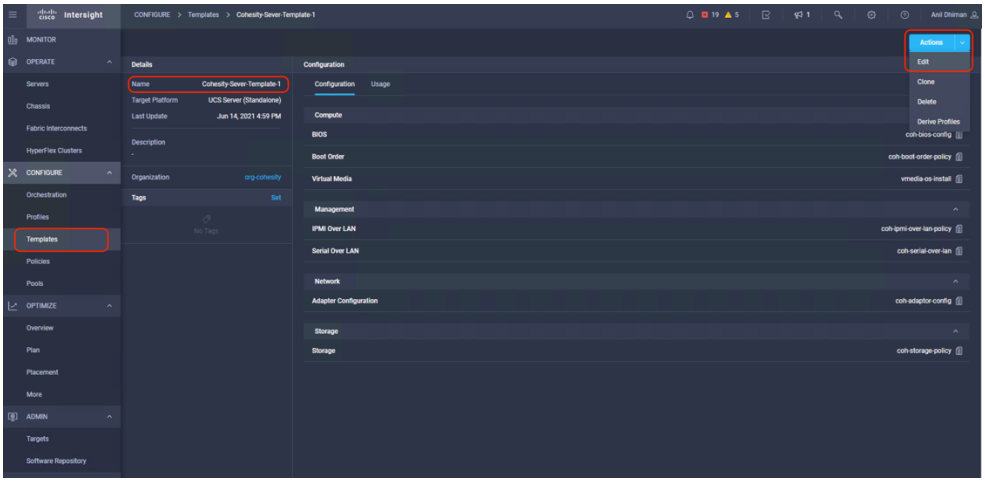
7. Repeat steps 1 through 6 to install the Cohesity OS on other nodes.

Remove the vMedia configuration from the server profile template

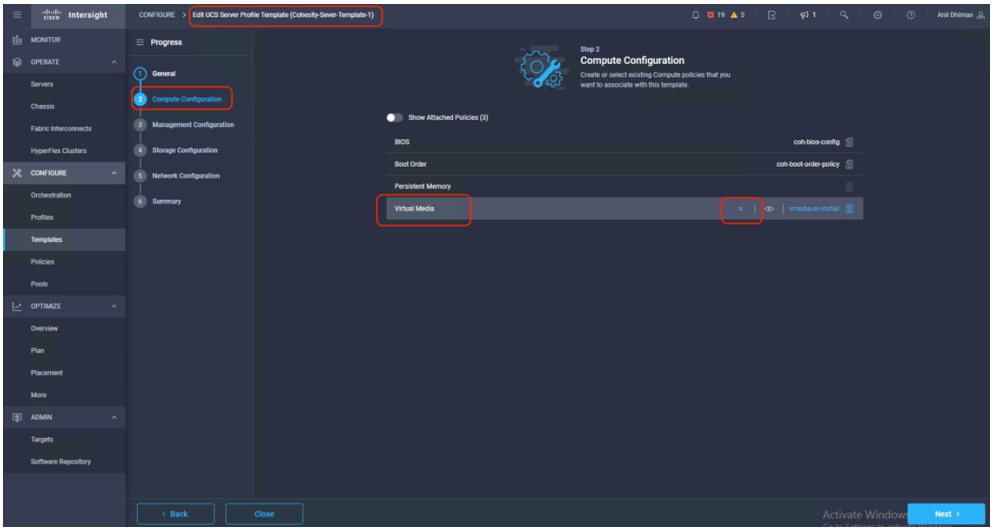
After the operating system is installed, you should remove the vMedia policy from the server profile template. Follow these steps to remove the vMedia policy:

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

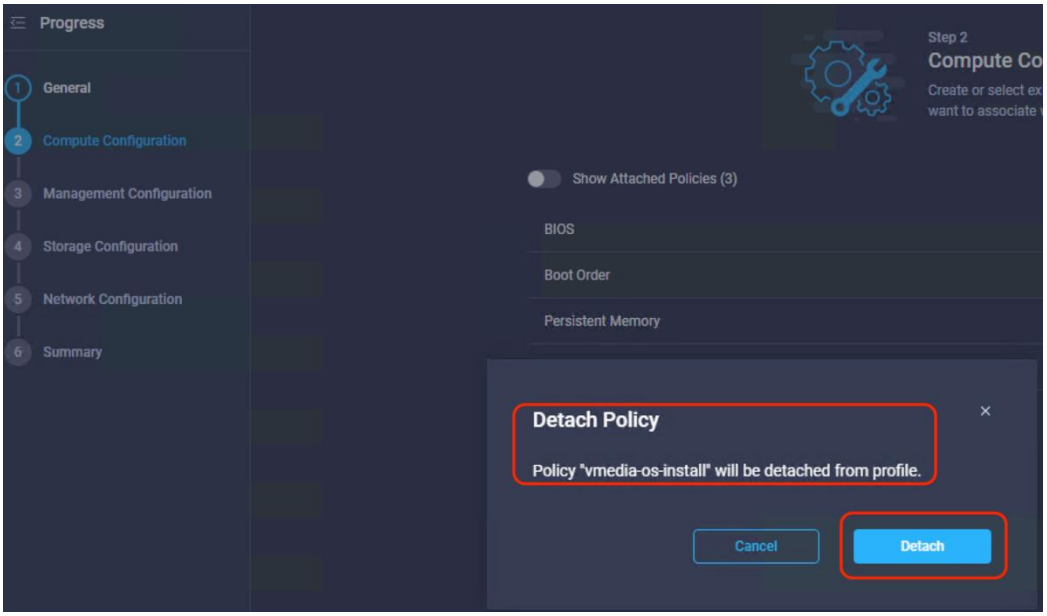
© 2021 Cisco and/or its affiliates. All rights reserved.



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

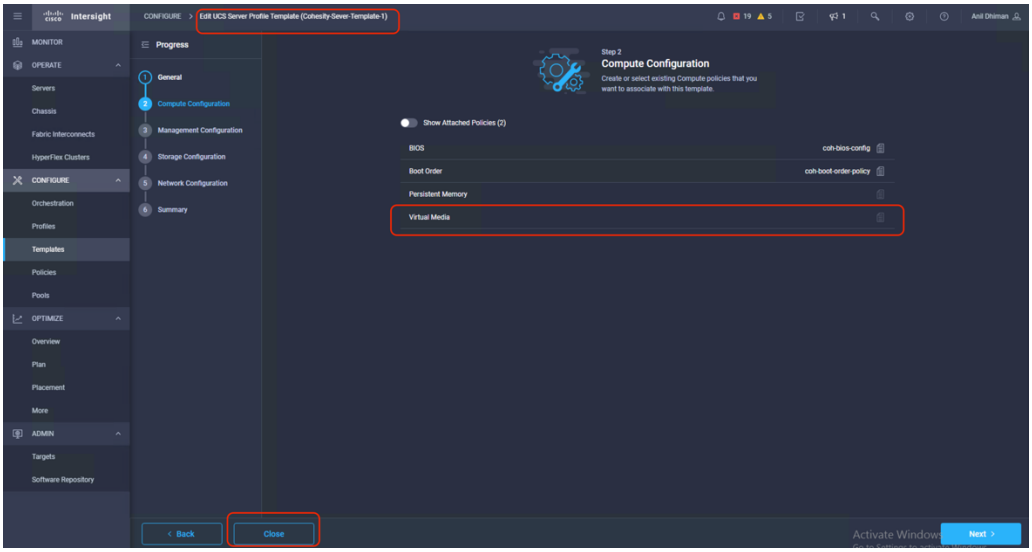


5. Confirm that you want to detach the vMedia server policy from the Cohesity server profile template.



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

© 2021 Cisco and/or its affiliates. All rights reserved.



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:

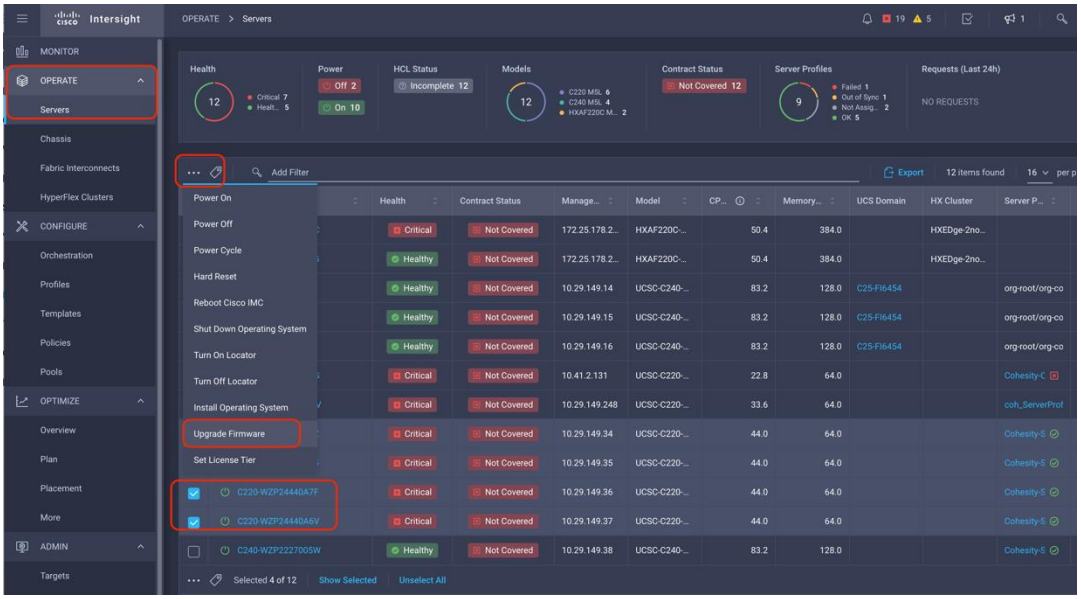
- Upgrade Cisco UCS C-Series firmware in combination with software upgrades of Cohesity DataPlatform. Cohesity nondistributive upgrades manage the sequential server reboot, allowing upgrades of Cisco UCS C-Series firmware during a Cohesity software upgrade. Because each node is upgrading sequentially, 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.

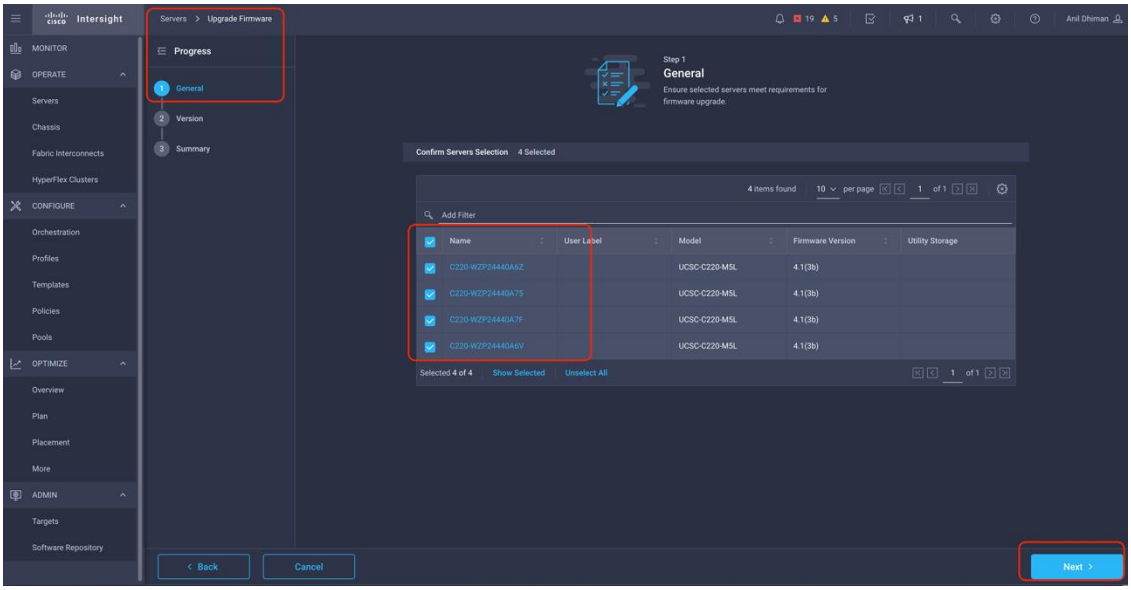
© 2021 Cisco and/or its affiliates. All rights reserved.

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



4. On the Upgrade Firmware screen, click Start.

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



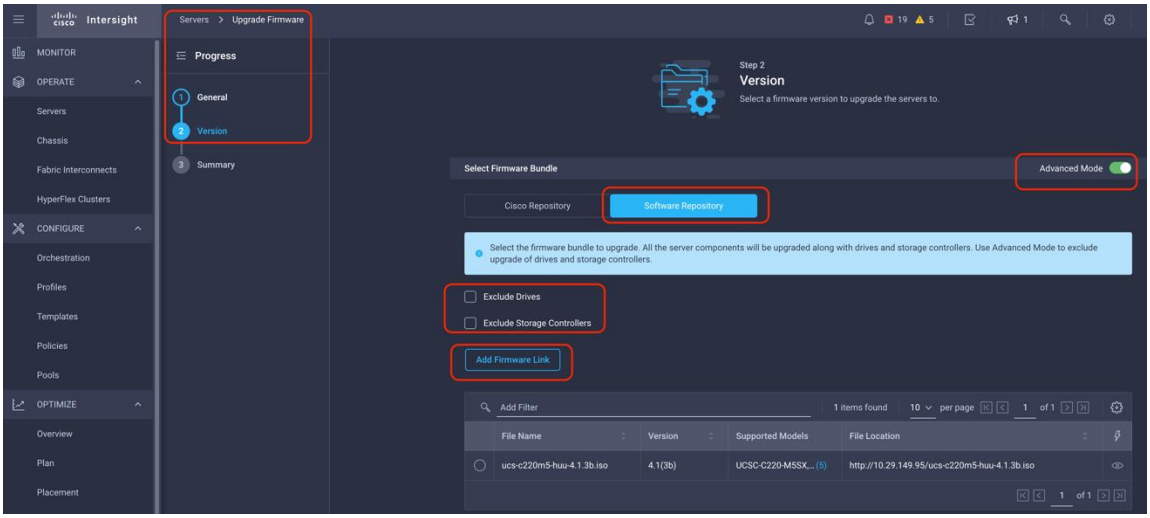
6. Select either Cisco Repository or Software Repository for the firmware image.

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.

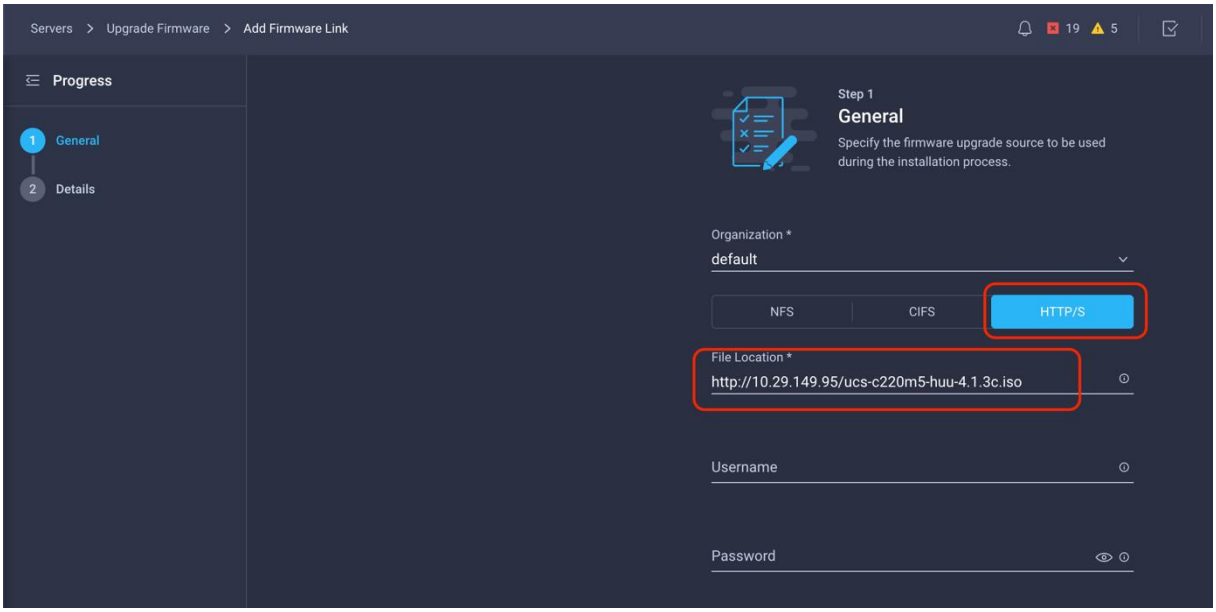
8. In the Software Repository, you can add images from NFS-, CIFS-, and HTTP/HTTPS-based network share repositories.

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.

© 2021 Cisco and/or its affiliates. All rights reserved.

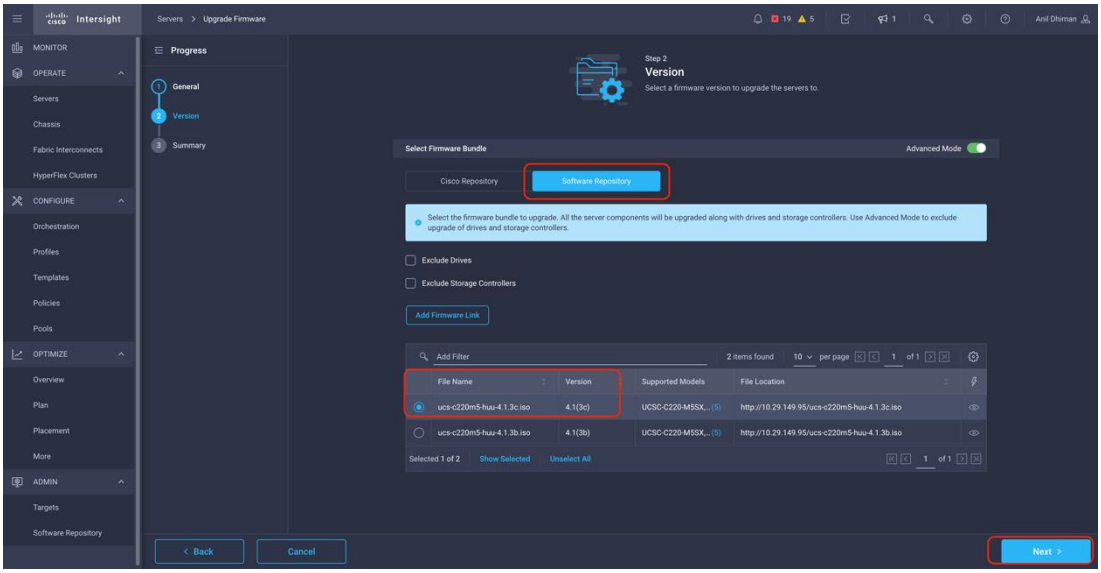


10. Add the location of the Cisco UCS C-Series Host Upgrade Utility (HUU). Click Next and then click Add.

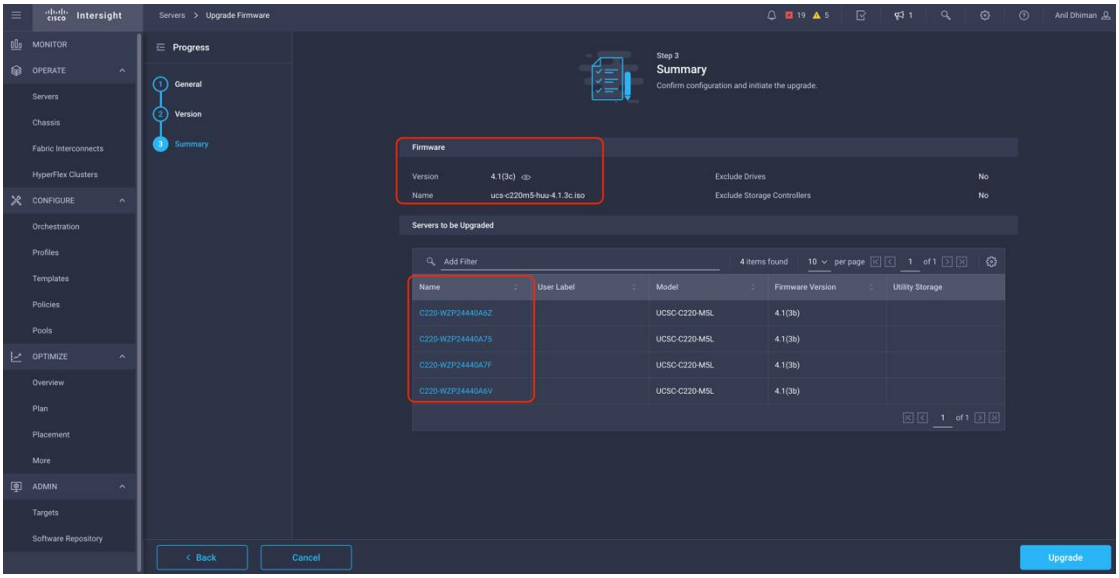


11. On the Select Firmware Link screen, select the appropriate firmware for upgrade and click Next.

© 2021 Cisco and/or its affiliates. All rights reserved.

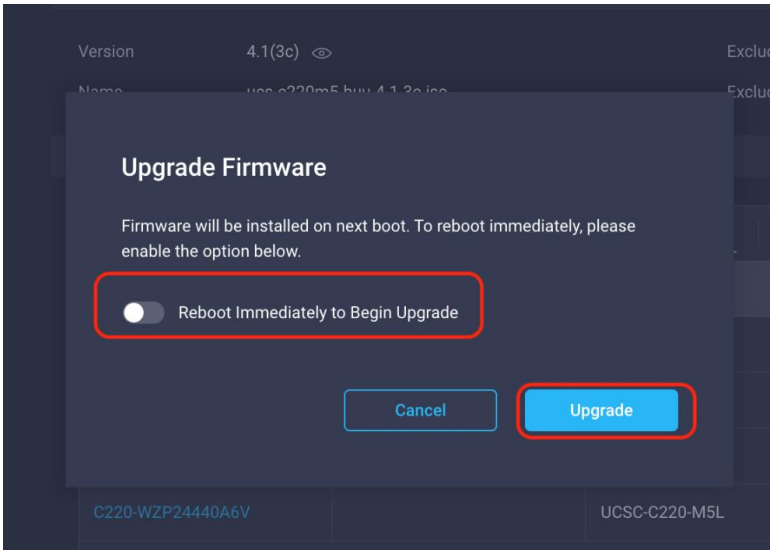


12. Confirm the firmware to be upgraded and click Upgrade.

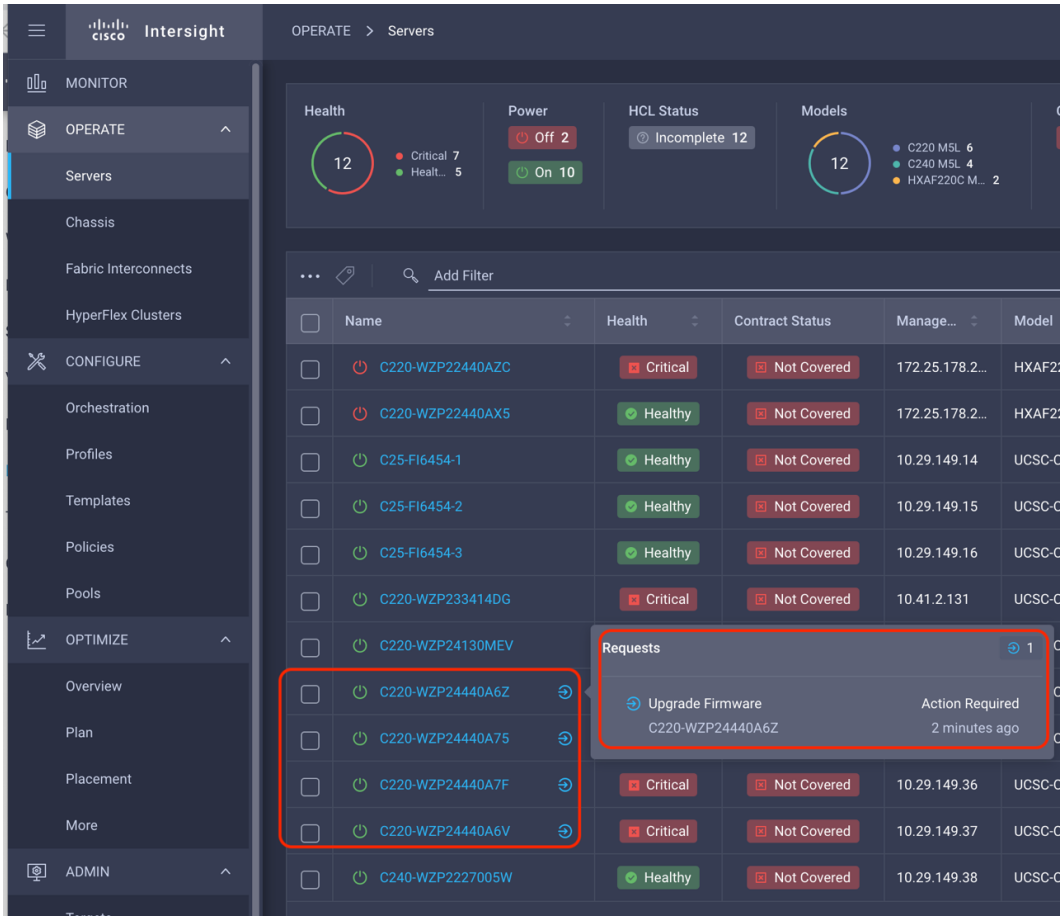


13. On the Upgrade Firmware screen that appears, **do not** enable the Reboot Immediately to Begin Upgrade option. Click Upgrade.

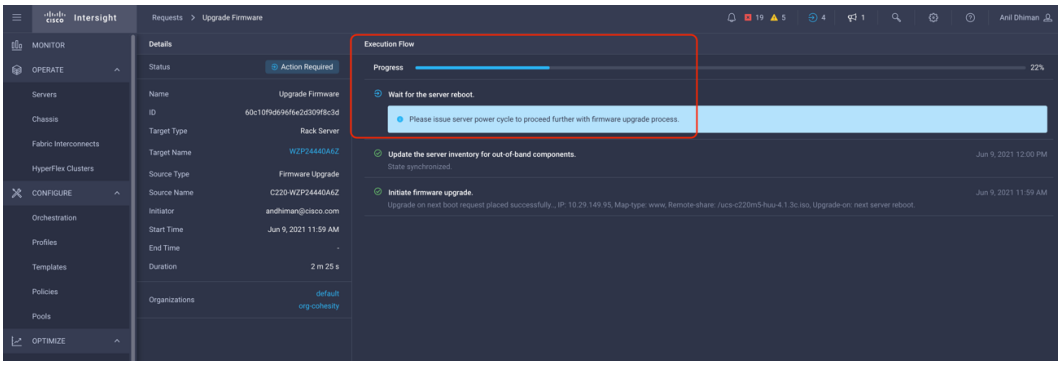
© 2021 Cisco and/or its affiliates. All rights reserved.



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



© 2021 Cisco and/or its affiliates. All rights reserved.



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.

© 2021 Cisco and/or its affiliates. All rights reserved.

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**.

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

Printed in USA 221181.1 07/21

© 2021 Cisco and/or its affiliates. All rights reserved.