VAST on Cisco UCS C225 M8 (EBox)

Install Guide

Published: December 2024

In partnership with:

Contents

Summary

The Install Guide provides a guidance for the design, setup and configuration of VAST on Cisco EBox nodes (UCS C225 M8). The Cisco UCS C225 M8 nodes is managed through Cisco Intersight in Intersight Standalone Mode (ISM).

Some of the key guidelines detailed in this document are

- Validated and Certified configuration for EBox nodes
- Networking recommendations VAST EBox cluster
- Cabling guidelines
- Step-by-Step procedures to configure UCS C225 M8 servers with Cisco Intersight
- Firmware upgrades and OS installation guidelines
- Known deployment Issues and workaround

Solution Design

This chapter contains the following:

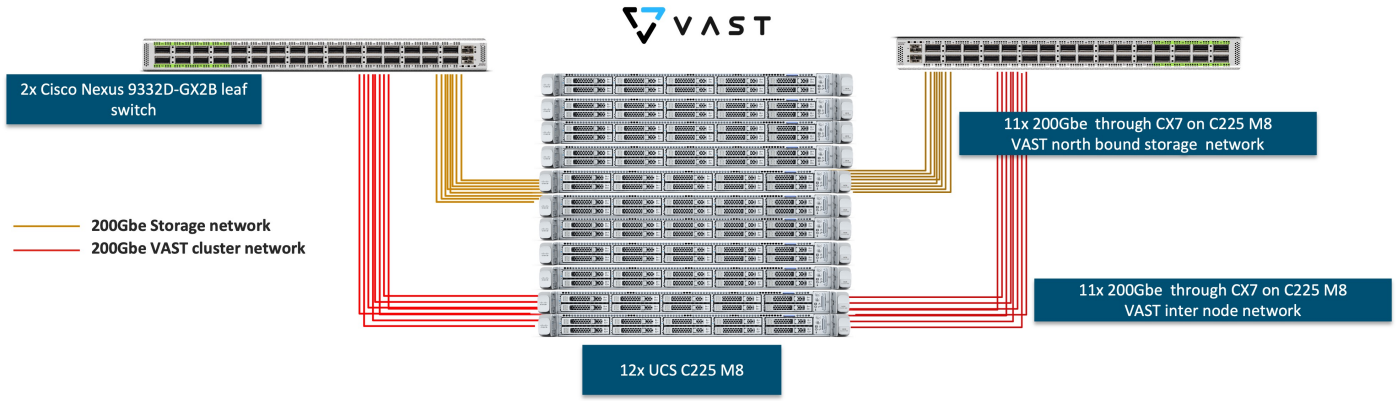
Solution Overview

VAST Data on Cisco UCS C225 M8 server is configured in Intersight Standalone mode with a minimum of twelve (12) nodes for VAST cluster.

Note: Please contact Cisco and VAST Tiger Team for cluster size of less than 12 nodes.

Figure below details a high level deployment of VAST on Cisco UCS C225 M8 (EBox) nodes

Figure 1. VAST Data on Cisco UCS C225 M8 server



The deployment includes

- 12 x Cisco UCS C225 M8 servers (EBox) certified for VAST
- 2/4 x Cisco Nexus 9332D-GX2B or Nexus 9364D-GX2A
- Optics (passive cables)
    - 24x *QDD-2Q200-CU3M (*400G QSFP56-DD to 2x200G QSFP56 Copper Breakout Cable, 3m)
    - 4x QDD-400-CU3M **(**400G Passive Cable, 3m)
- Optics (Active cables)
    - on 400G switch side , 24x QDD-400G-SR8-S (400G QSFP-DD Transceiver, MPO-16 APC, 100m OM4 MMF),
    - on CX7 side , 48x QSFP-200G-SR4-S (200GBASE SR4 QSFP56 Transceiver, MPO, 100m over OM4 MMF)
    - MPO breakout cable

EBox Specifications

This section details the hardware component specification of Cisco UCS C225 M8 server configured as VAST EBox node.

Note: Deployment administrators should adhere to the below mentioned specifications, any deviation will lead to failure of installation

Figure below details the front and rear of UCS C225 M8 server (EBox) certified for VAST. Each of the critical components are marked as per the table below

Note: Figure below is applicable for VAST EBox 15.3TB and 30TB SSD configuration. The 60TB SSD configuration has 7x SSDs and 3x SCM drives on drive Slot1, Slot6 and Slot7

Figure 2. UCS C225 M8 for VAST EBox (Front)

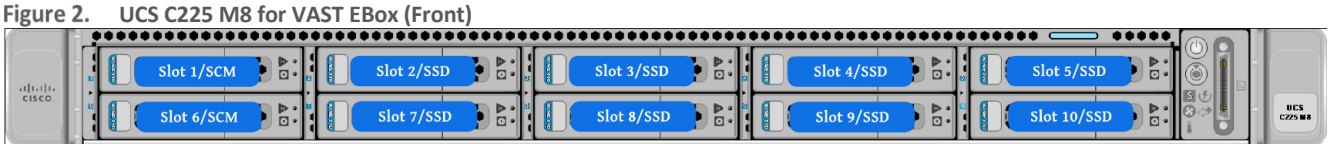


Figure 3. UCS C225 M8 for VAST EBox (Rear)

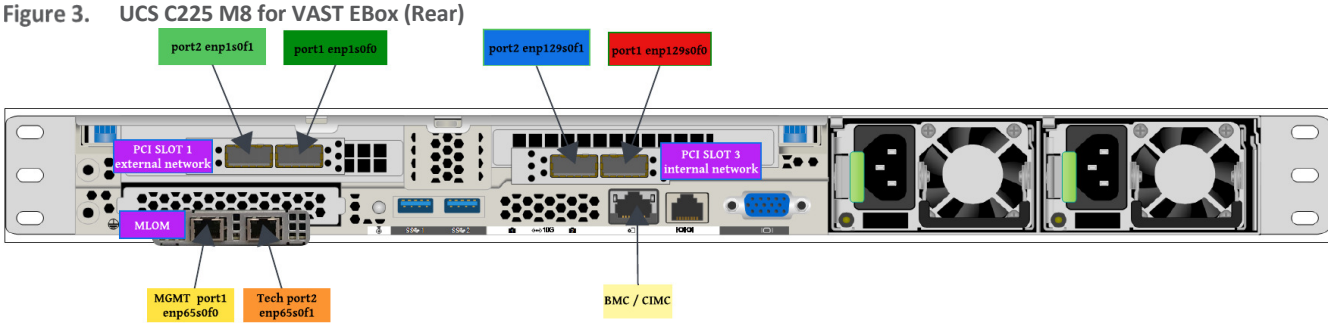


Table below elaborates on each of the critical hardware component for UCS C225 M8 server certified as VAST EBox node. Each table details the hardware specifications for UCS C225 M8 EBox configuration with 15.3TB, 30TB and 60TB SSDs

Table 1. Hardware components of EBox/ Cisco UCS C225 M8 server with 15 .3TB SSDs

Processor	1x AMD 9454P 2.75GHz 290W 48C/256MB Cache DDR5 4800MT/s
Memory	384GB DDR Memory (12 x 2GB DDR5-5600 RDIMM 1Rx4 (16Gb)
Boot Drive	2x 960GB M.2 cards with M.2 H/w RAID (RAID1)
SCM Drive	2x 960GB 2.5in U.3 Micron XTR NVMe (SCM Drives). These drives must be in drive Slot 1 and drive Slot 6 of each UCS C225 node
SSD	8x 15.3TB 2.5in U.2 P5316 (Intel/Solidigm)

BMC/CIMC, IPMI over LAN	1GBE dedicated Ethernet management port (BMC/CIMC)
MLOM	1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM) • Port 1 (enp65s0f0) configured VAST management • Port 2 (enp65s0f1) configured as VAST tech support port. It has a static IP (192.168.2.2/24)
RISER 1 / external RDMA Network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1 • Port 1 (enp1s0f0) configured for external or customer network • Port 2 (enp1s0f1) configured for external or customer network • Used for VAST external or customer network
RISER 3 / internal RDMA network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3 • Port 1 (enp129s0f0) configured for VAST internal/southbound network • Port 2 (enp129s0f1) configured for VAST internal/southbound network • Used for VAST internal RDMA network

Table 2. Hardware components of EBox/ Cisco UCS C225 M8 server with 30TB SSDs

Processor	1x AMD 9454P 2.75GHz 290W 48C/256MB Cache DDR5 4800MT/s
Memory	384GB DDR Memory (12 x 2GB DDR5-5600 RDIMM 1Rx4 (16Gb)
Boot Drive	2x 960GB M.2 cards with M.2 H/w RAID (RAID1)
SCM Drive	2x 1.9TB 2.5in U.3 Micron XTR NVMe (SCM Drives). These drives must be in drive Slot 1 and drive Slot 6 of each UCS C225 node
SSD	8x 30TB 2.5in U.2 P5316 (Intel/Solidigm)

BMC/CIMC, IPMI over LAN	1GBE dedicated Ethernet management port (BMC/CIMC)
MLOM	1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM) • Port 1 (enp65s0f0) configured VAST management • Port 2 (enp65s0f1) configured as VAST tech support port. It has a static IP (192.168.2.2/24)
RISER 1 / external RDMA Network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1 • Port 1 (enp1s0f0) configured for external or customer network • Port 2 (enp1s0f1) configured for external or customer network • Used for VAST external or customer network
RISER 3 / internal RDMA network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3 • Port 1 (enp129s0f0) configured for VAST internal/southbound network • Port 2 (enp129s0f1) configured for VAST internal/southbound network • Used for VAST internal RDMA network

Table 3. Hardware components of EBox/ Cisco UCS C225 M8 server with 60TB SSDs

Processor	1x AMD 9454P 2.75GHz 290W 48C/256MB Cache DDR5 4800MT/s
Memory	384GB DDR Memory (12 x 2GB DDR5-5600 RDIMM 1Rx4 (16Gb)
Boot Drive	2x 960GB M.2 cards with M.2 H/w RAID (RAID1)
SCM Drive	3x 1.9TB 2.5in U.3 Micron XTR NVMe (SCM Drives). These drives must be in drive Slot 1 , Slot 6 and Slot7 of each UCS C225 node
SSD	7x 60TB 2.5in U.2 Micron 6550 ION

BMC/CIMC, IPMI over LAN	1GBE dedicated Ethernet management port (BMC/CIMC)
MLOM	1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM) • Port 1 (enp65s0f0) configured VAST management • Port 2 (enp65s0f1) configured as VAST tech support port. It has a static IP (192.168.2.2/24)
RISER 1 / external RDMA Network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1 • Port 1 (enp1s0f0) configured for external or customer network • Port 2 (enp1s0f1) configured for external or customer network • Used for VAST external or customer network
RISER 3 / internal RDMA network	1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3 • Port 1 (enp129s0f0) configured for VAST internal/southbound network • Port 2 (enp129s0f1) configured for VAST internal/southbound network • Used for VAST internal RDMA network

Deployment Architecture

VAST EBox cluster with Cisco UCS C225 M8 servers can be deployment with two key network deployment designs.

- Unified network
- Split network

Each of the design require a minimum of twelve (12) nodes of UCS C225M8 and differentiate on how the external/customer network ports and internal/southbound network ports connect to the Cisco Nexus switches.

Unified network Connectivity

In the deployment both the internal/southbound network ports (from network adapter in PCI Slot 3) and the external/customer network ports (from network adapter in PCI slot 1) are connected to the same pair of 400G Cisco Nexus switches.

Figure below details on connectivity of Cisco UCS C225 M8 server (EBox) with a single pair of Cisco Nexus 9332D-GX2B switches.

Note: The network design below, is an illustration of lab deployment, please contact your VAST Network SME to design a network confguration as per the customer environment

Figure 4. EBox unified network connectivity

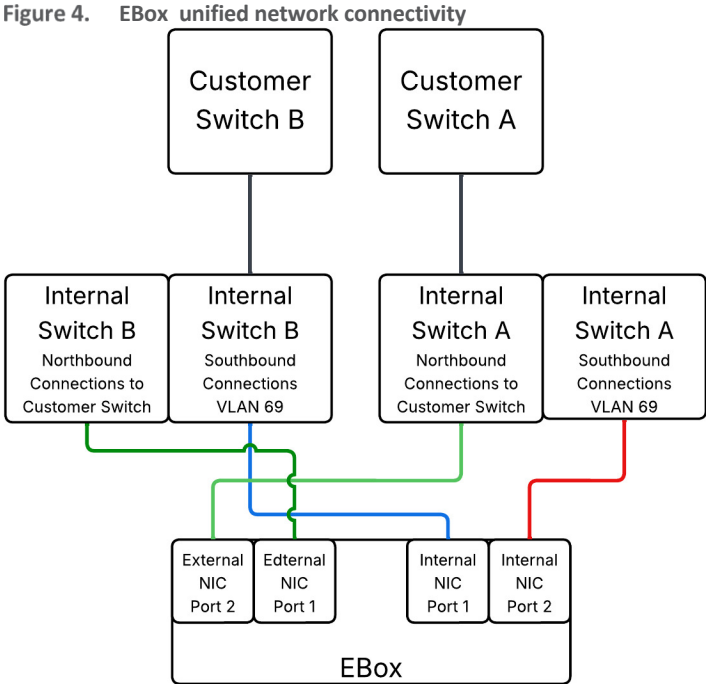
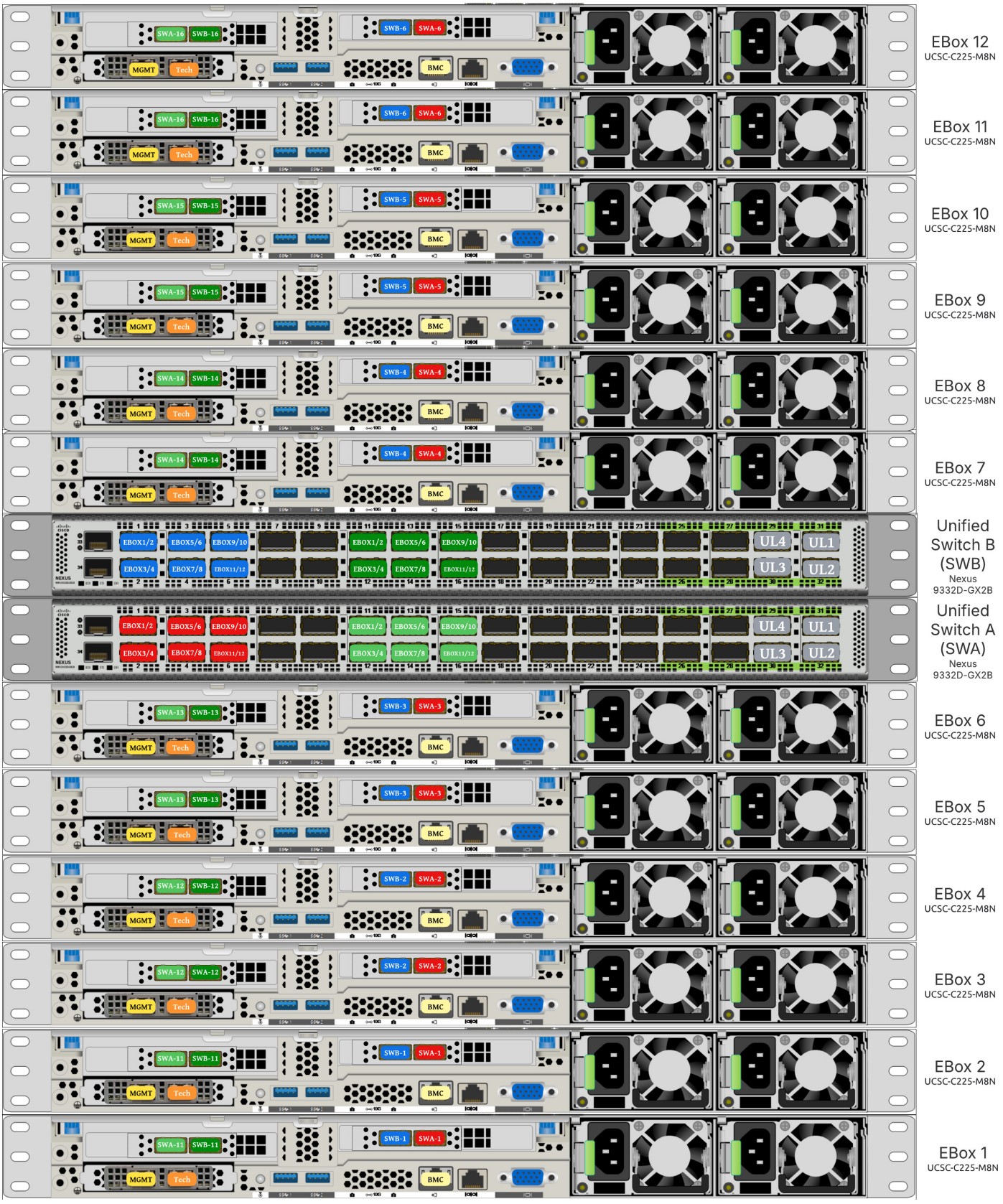


Figure 5. Unified network with 12 x UCS C225 M8N server (12x EBox)



Below are the labelling instructions for unified connectivity diagram illustrated above

- SWA is defined as switch A
- SWB is defined as switch B
- Ports marked in blue and red are used for VAST internal network
- Ports marked in light and dark green are used for connectivity to customer network or external network
- Number of uplinks or connections to spine switches is dependent on the number of EBox connected to the switch pair. In case of 12 EBox nodes,we need 4x 400G uplinks from each switch
- In the deployment, 400G to 2x 200G breakout cable (QDD-2Q200-CU3M) was used allowing connections to 400G ports on switch side and 200G ports on CX7 adapter for each EBox. For ex.
    - EBox1 and EBox2 both marked with SWA-11 connects to Port 11 of Switch A
    - EBox1 and EBox2 both marked with SWB-11 connects to Port 11 of Switch B

The key design and cabling considerations for unified connectivity are listed below

- The unified network deployment is a spine-leaf design with VXLAN BGP EVPN. Both external and internal networks of EBox nodes connects to same pair of leaf switches
- For small clusters , customers can use a L2-adjacency network design without VXLAN BGP EVPN

Note: In unified network design, VAST does not recommend connecting the clients or GPU nodes and the network ports of VAST cluster the same pair of leaf switches.

Split network Connectivity

In the deployment internal/southbound networks connects to a separate pair of 400G Nexus switches and the external/customer network connect to a different pair of leaf switches which connects to the network.

Figure below details on connectivity of Cisco UCS C225 M8 server (EBox) with a separate pair of Cisco Nexus 9332D-GX2B switches for internal/southbound network and external/customer network.

Figure 6. EBox split network connectivity

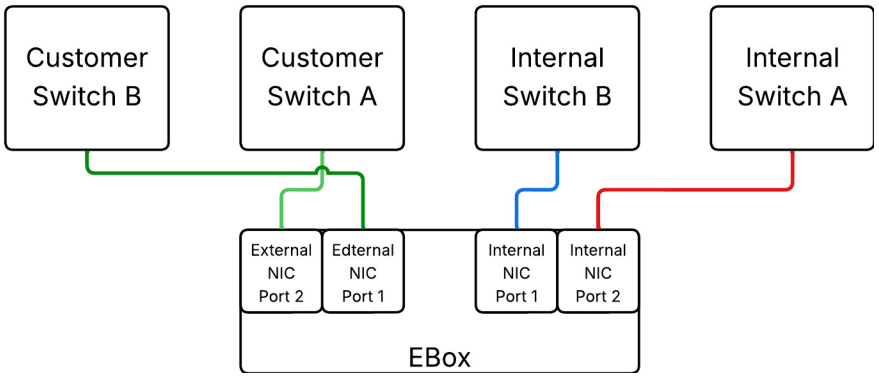
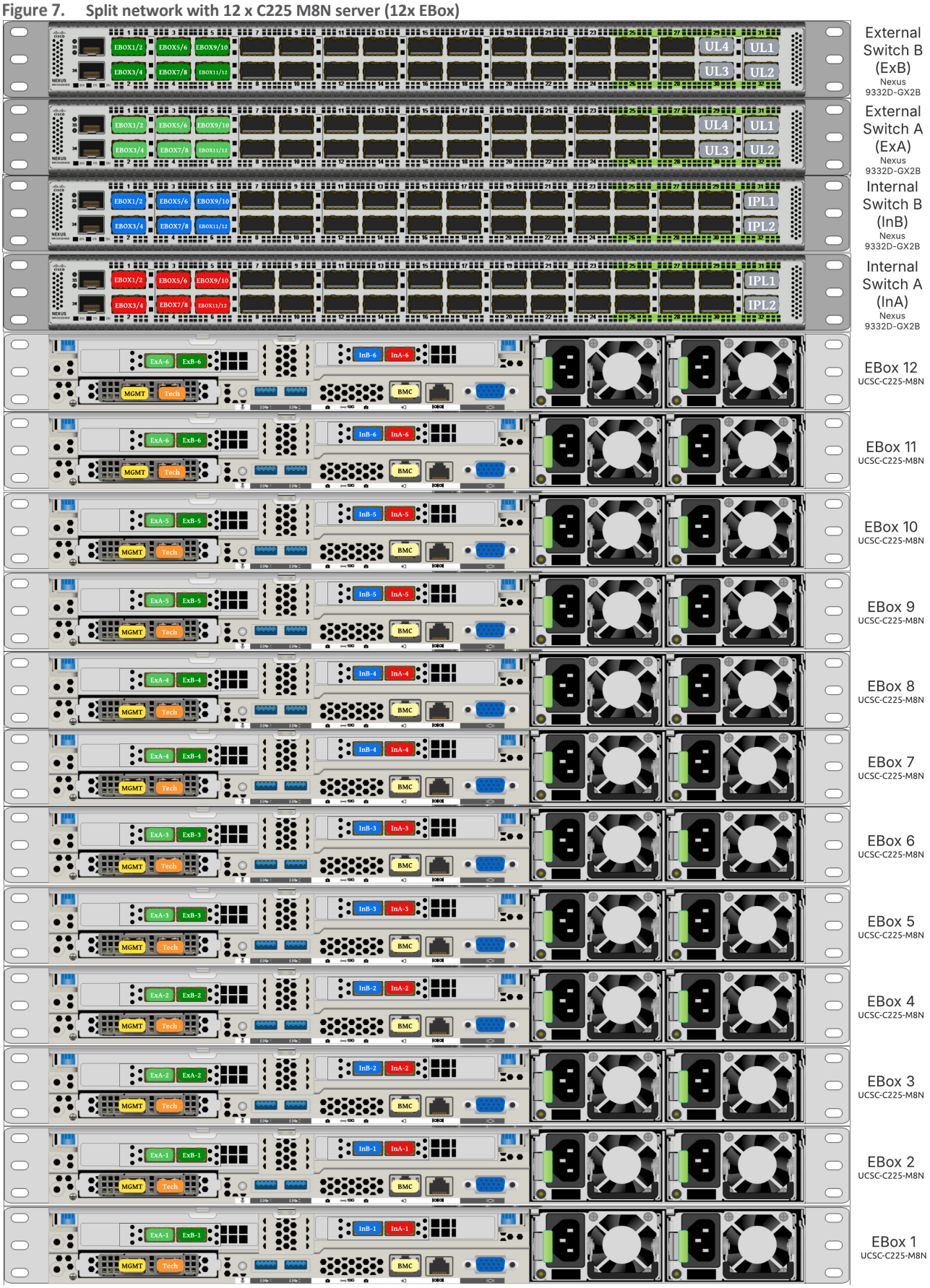


Figure 7. Split network with 12 x C225 M8N server (12x EBox)



Below are the labelling instructions for split connectivity diagram illustrated above

- InA and InB are defined as VAST Internal switch A and B. This switch pair is used for internal network of VAST cluster through network adapter (CX7) on EBox (marked with ports colors as Blue and Red)
- EXA and EXB are defined as VAST external/customer switch A and B. This switch pair is used for external/customer network of VAST cluster through network adapter (CX7) on EBox (marked with ports colors as light and dark Green). Clients can connect to this switch pair.
- Number of uplinks or connections to spine switches for exteral switch is dependent on the number of EBox connected to the switch pair. In case of 12 EBox nodes,we need 4x 400G uplinks from each switch
- 2x Inter Peer Links are required on Internal switch pair. This is leveraged for VAST management network
- In the deployment, 400G to 2x 200G breakout cable (QDD-2Q200-CU3M) was used allowing connections to 400G ports on switch side and 200G ports on CX7 adapter for each EBox.

The split network deployment allows isolation of VAST internal network with a separate pair if Cisco Nexus 400G switches. The external or customer network connects to external pair of switches and external clients can connect to these swtiches

Licensing

Cisco Intersight Licensing

Cisco Intersight uses a subscription-based license with multiple tiers. Each Cisco automatically includes a Cisco Intersight Essential trial license when you access the Cisco Intersight portal and claim a device. The Essential Tier allows configuration of Server Profiles for VAST on Cisco UCS C-Series Rack Servers.

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

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

- Tunneled KVM access, allowing remote KVM access to Cisco UCS C225 M8 nodes
- Intersight operating system install feature

VAST Licensing

In order to license VAST, customers should properly size their deployment. Please take assistance of VAST SE or Cisco VAST Tiger Team to correctly size the deployment. VAST sizer generates storage (PB) and core licenses which needs to be added to CCW. This will generate the right sized BoM with both EBox hardware and VAST licenses.

Software and Firmware versions

Table below, lists the software and Firmware versions for configuration of Cisco UCS C225 M8 nodes with VAST

Note: These versions are subjected to change , please verify with your VAST support or install team for the correct software and firmware versions

Table 4. Software and Firmware versions

Component	Version	Notes
CIMC Firmware Version	4.3(5.250030)	
BIOS Firmware Version	C225M8.4.3.5d.0.0206250854.	

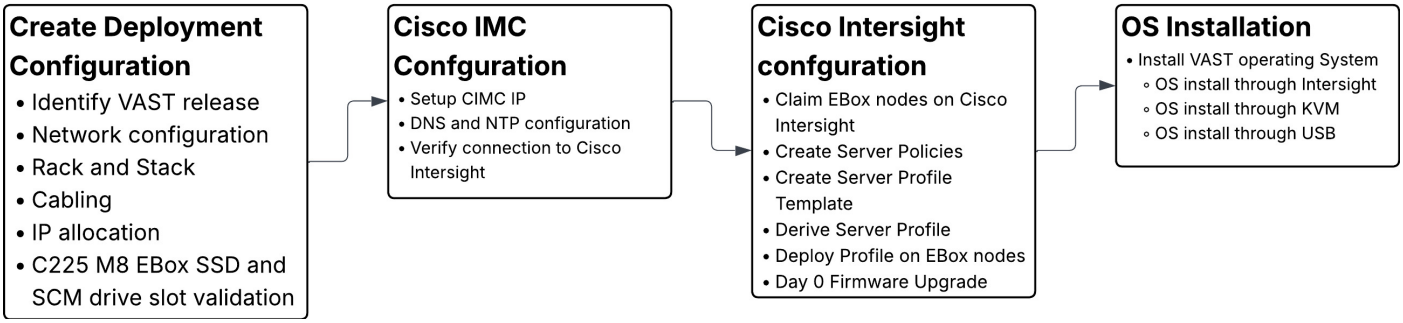
Component	Version	Notes
SCM drive , 960GB Micron XTR	E2XC000	
15.3 TB , Intel/Solidigm 5316 QLC drive	ACV1V204	Updated through VAST VMS bootstrap
M.2 HW RAID controller	2.3.17.1014	
960 GB M.2 Boot drive	D4CS000	
MLOM / Cisco(R) X710T2LG 2x10 GbE RJ45 OCP 3.0 NI	0x8000F961-1.836.0-9.5	
Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe	28.39.1002	Currently not getting updated through VAST VMS bootstrap. Remains at version 28.41.1000
VAST OS	vast-os-12.14.17-1818066	
VAST VMS	release-5.3.0-sp8-hf6-1872389	

VAST EBOX node configuration

This chapter describes the step-by-step procedures to configure Cisco EBOX nodes on Cisco UCS C225 M8 platform. The Cisco UCS C-Series Rack Servers are configured in Intersight Standalone Mode (ISM)

The process flow below elaborates on the high level steps to configure Cisco UCS C225 M8 server and install operating system.

Note: Installation of VAST cluster is outside the scope of this document; VAST support should be involved to install VAST Cluster on Cisco UCS C225 M8 servers (EBox)



- CIMC IP configuration
- Claim EBOX Nodes on Cisco Intersight
- Create Server Policies
- Create Server Profile Template
- Derive and Deploy UCS Server Profile
- Day 0 EBOX firmware upgrade
- VAST OS Installation

CIMC IP configuration

Note: CIMC IP configuration requires local access to the server nodes.

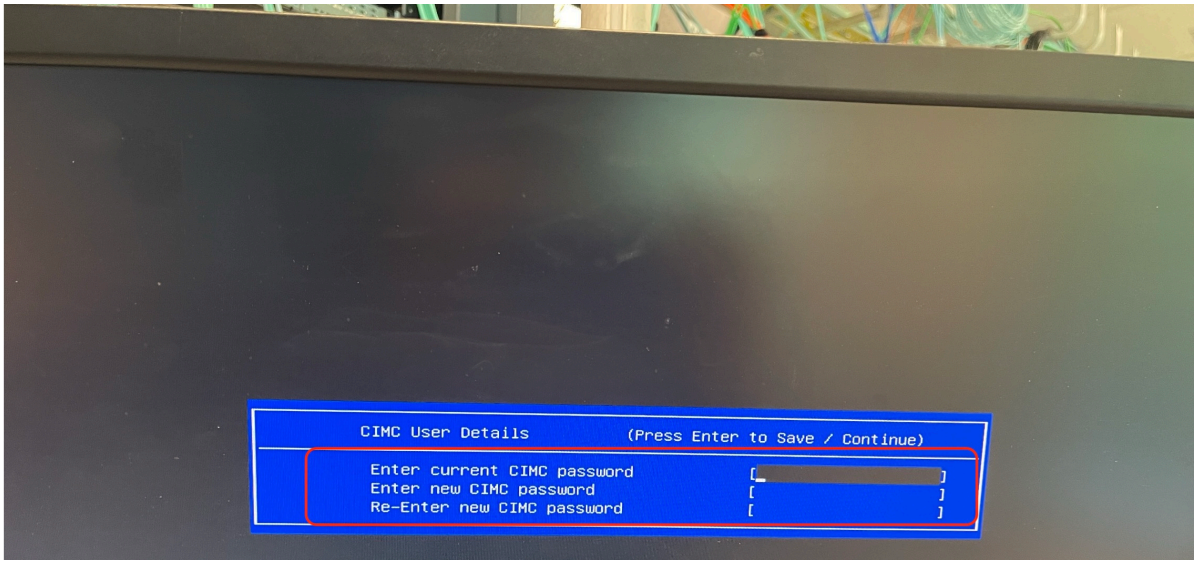
Step 1. Connect a USB keyboard and VGA monitor to the server using one of the following methods:

- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel. Connect your USB keyboard and VGA monitor to the KVM cable. (OR)
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel.

Step 2. Power On the Server

Step 3. During bootup, press F8 when prompted to open the Cisco IMC Configuration Utility.

Step 4. The first time that you enter the Cisco IMC Configuration Utility, you are prompted to change the default password. The default password is ***password***. The Strong Password feature is enabled. Setup the password and press Enter.

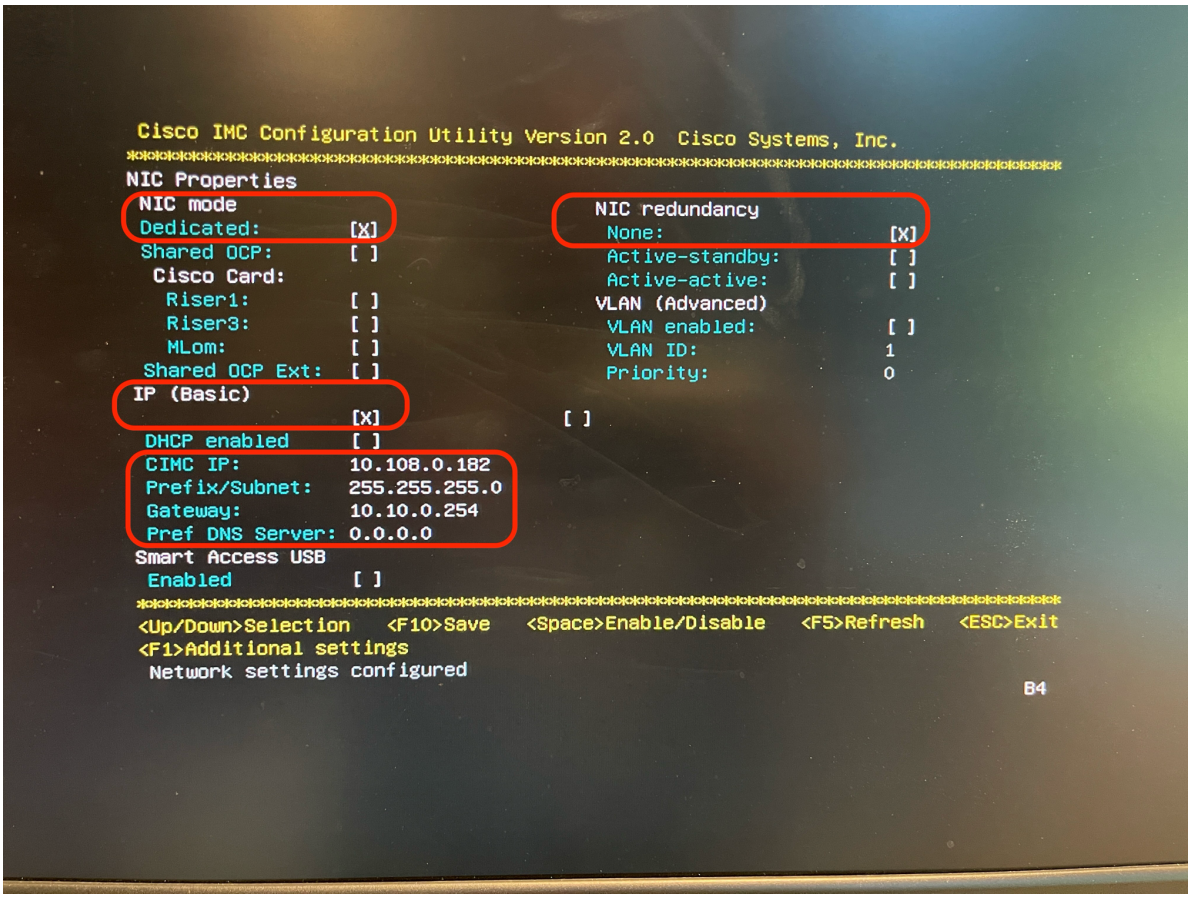


Step 5. On the Cisco IMC Configuration utility ,Edit the below mentioned details. The details are also displayed the screenshot below with edits marked in ‘red’

- NIC mode to ‘dedicated’
- Select IP (Basic) configuration.

Note: This CIMC IP should be taken from IP configuration table created in Cabling and IP configuration sheet

- Enter CIMC IP, prefix, gateway and Preferred DNS Server
- Select NIC redundancy to ‘none’



Step 6. Press ‘F10’ to save the configuration and exist During bootup, press F8 when prompted to open the Cisco IMC Configuration Utility.

Step 7. Once configuration is saved, press ‘ESC’ to exit the screen.

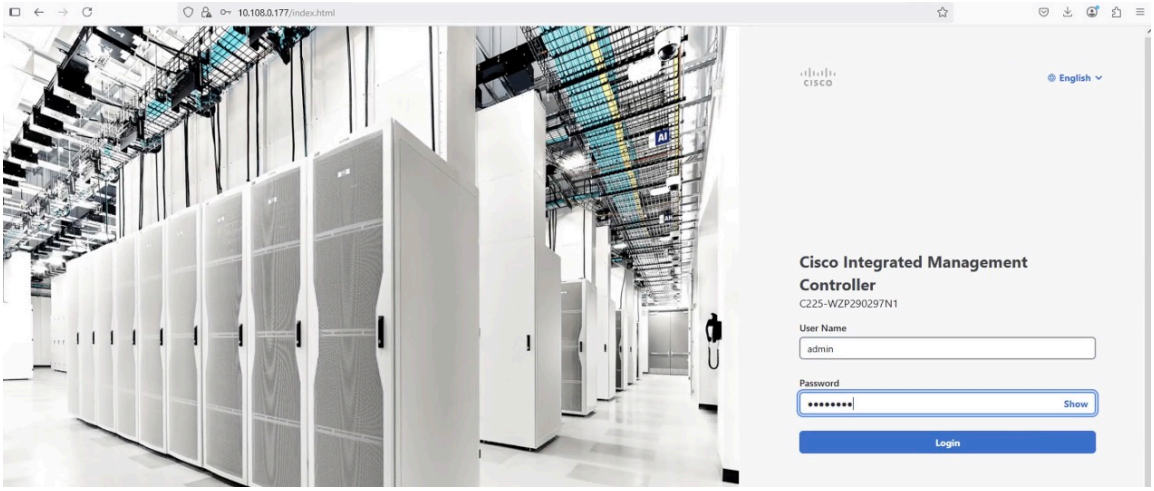
Claim EBOX Nodes on Cisco Intersight

The steps below elaborate on the procedure to claim Cisco UCS C225 M8 nodes on Cisco Intersight.

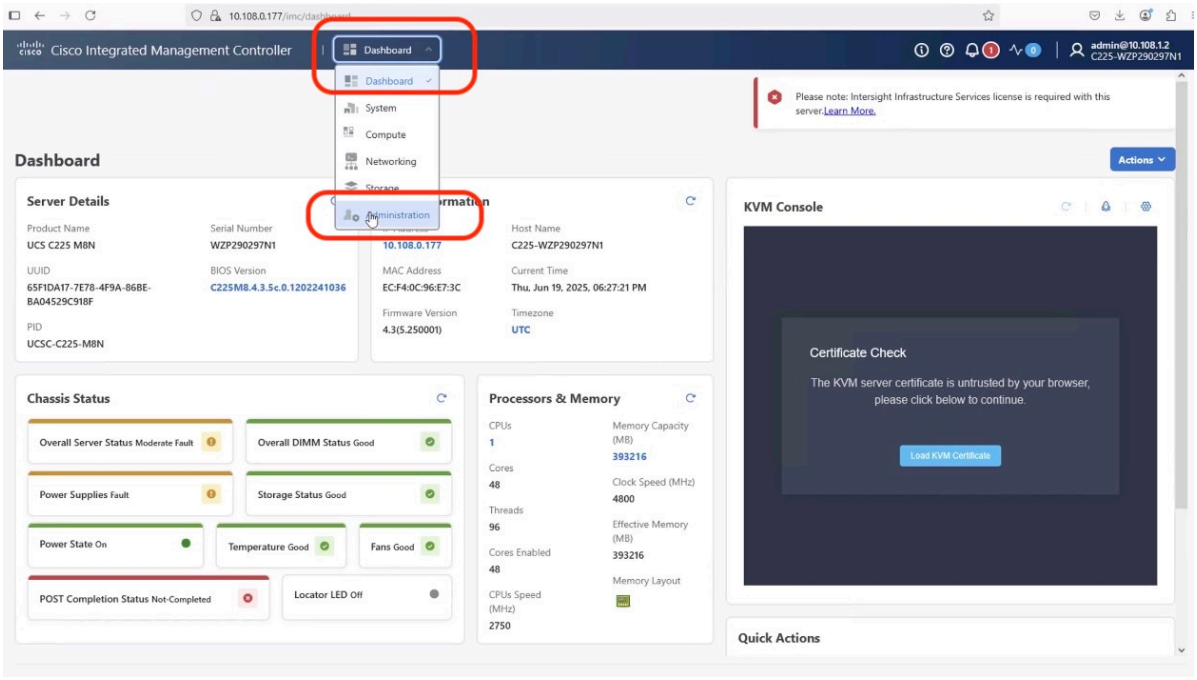
The below access require local access to the server nodes.

Step 1. Login to Cisco Intersight account. If this is the first time, pls create Cisco Intersight Account. For detailed steps please refer to Cisco Intersight Account Creation

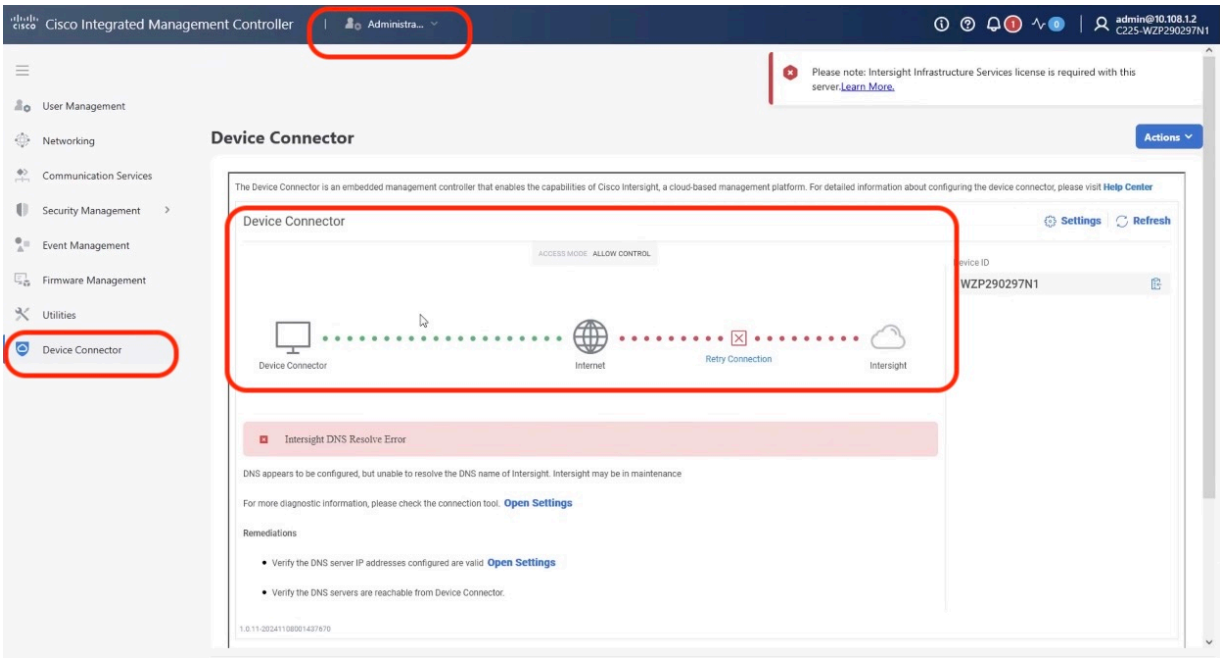
Step 2. Open a web browser and enter Cisco IMC IP, login with the username: admin and the password as configured during CIMC configuration process.



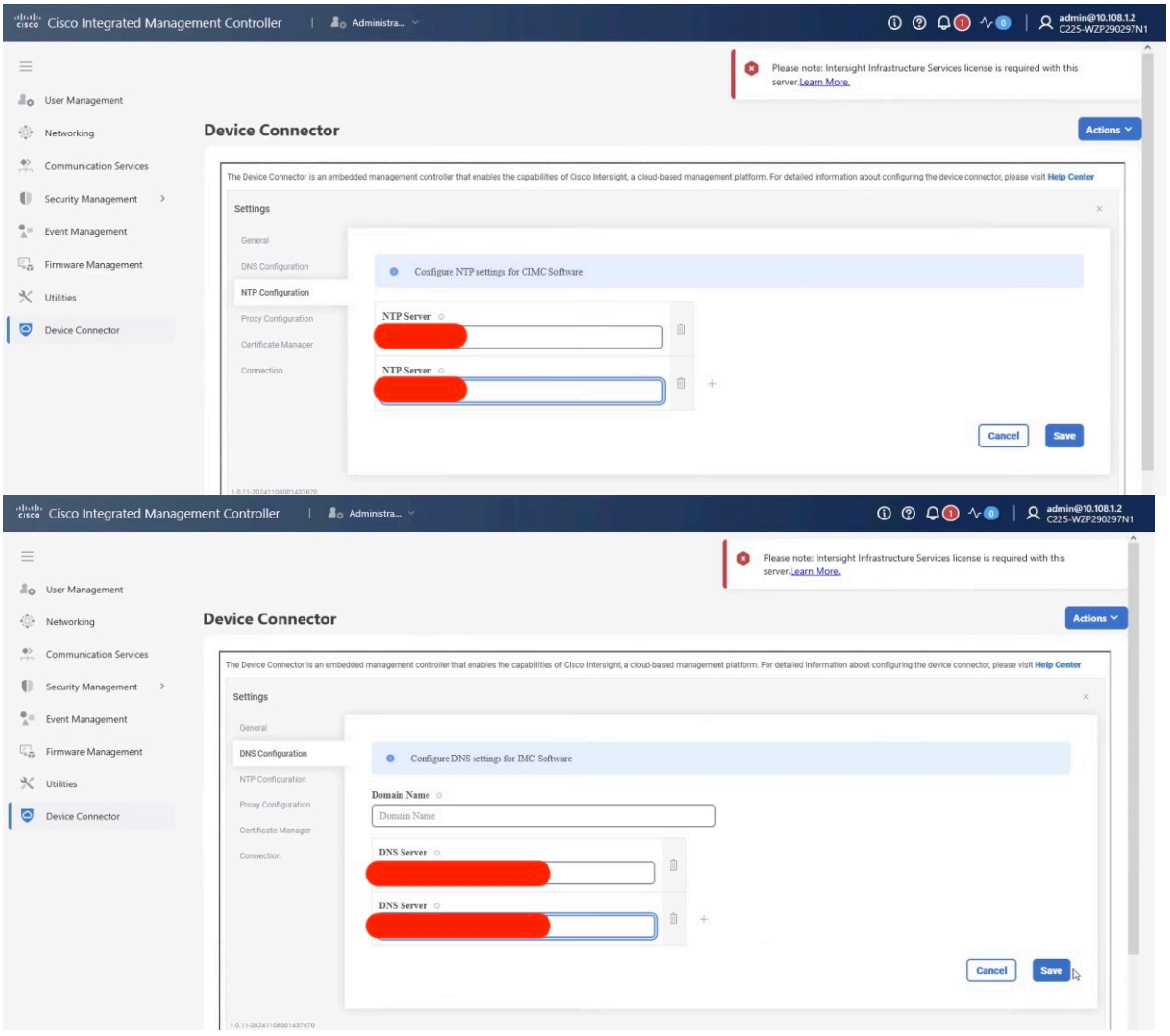
Step 3. From the top navigation drop down, select Dashboard -> Administration



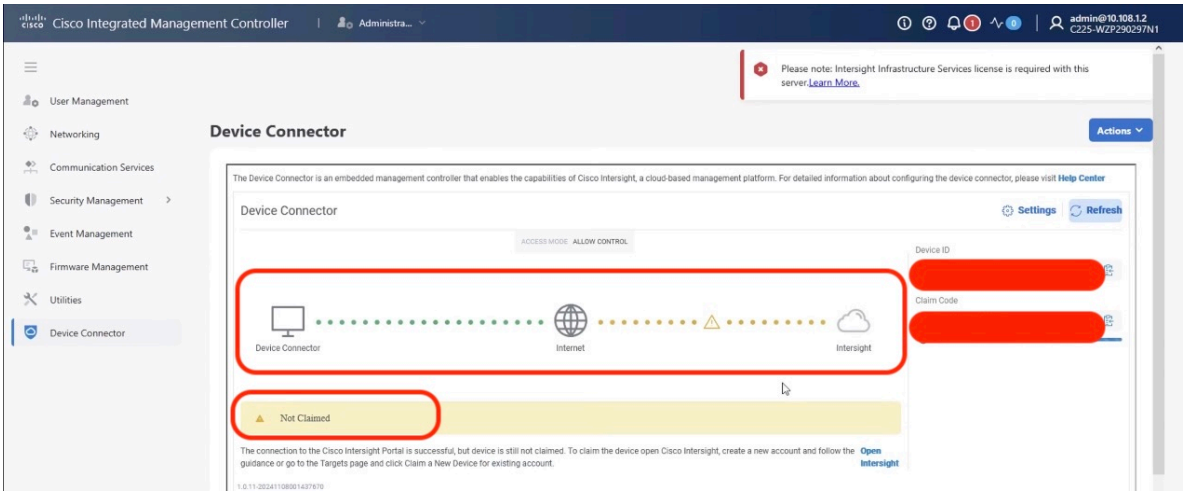
Step 4. From the left Navigation pane, click on Device Connector and verify the connection of node to Cisco Intersight. As shown below, we need to update DNS and NTP configuration to successfully resolve Intersight domain name.



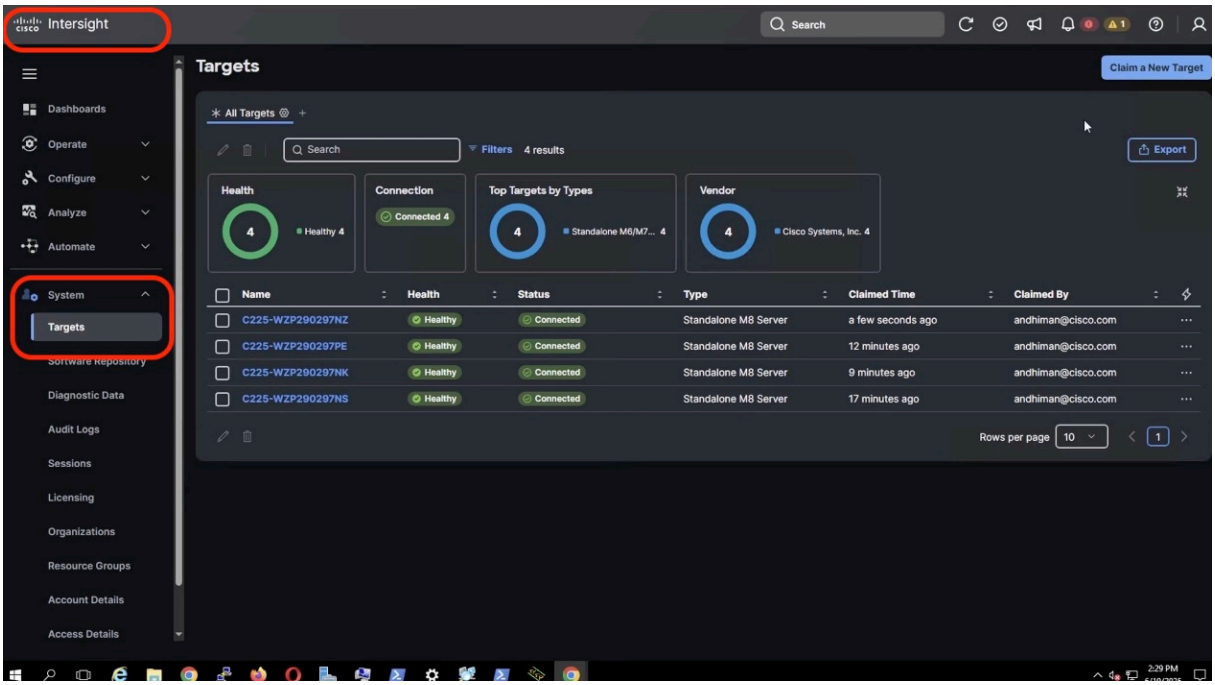
Step 5. Click on ‘open settings” and update NTP and DNS servers.



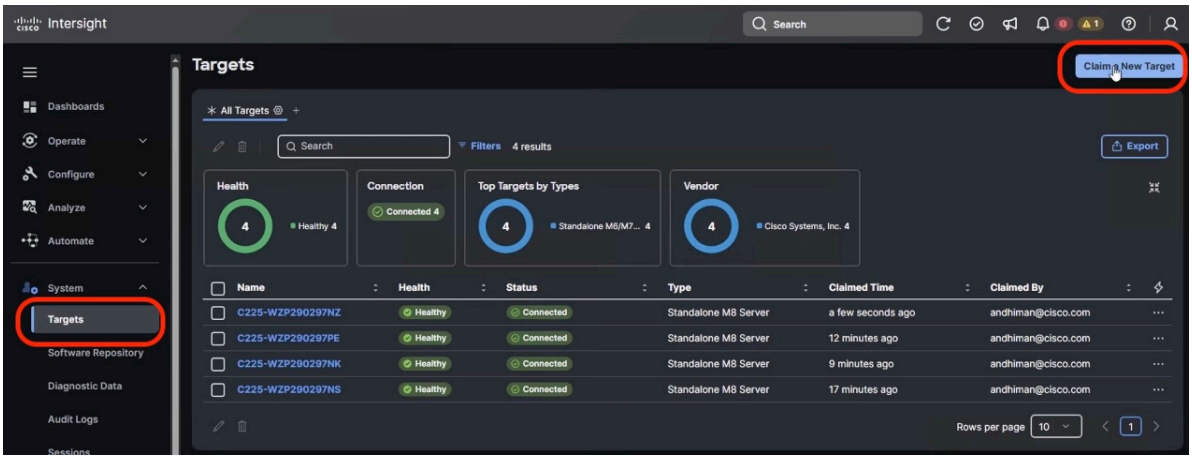
Step 6. Ensure the server is not already claimed, copy the Device ID and Claim Code which would be used to claim server on Cisco Intersight



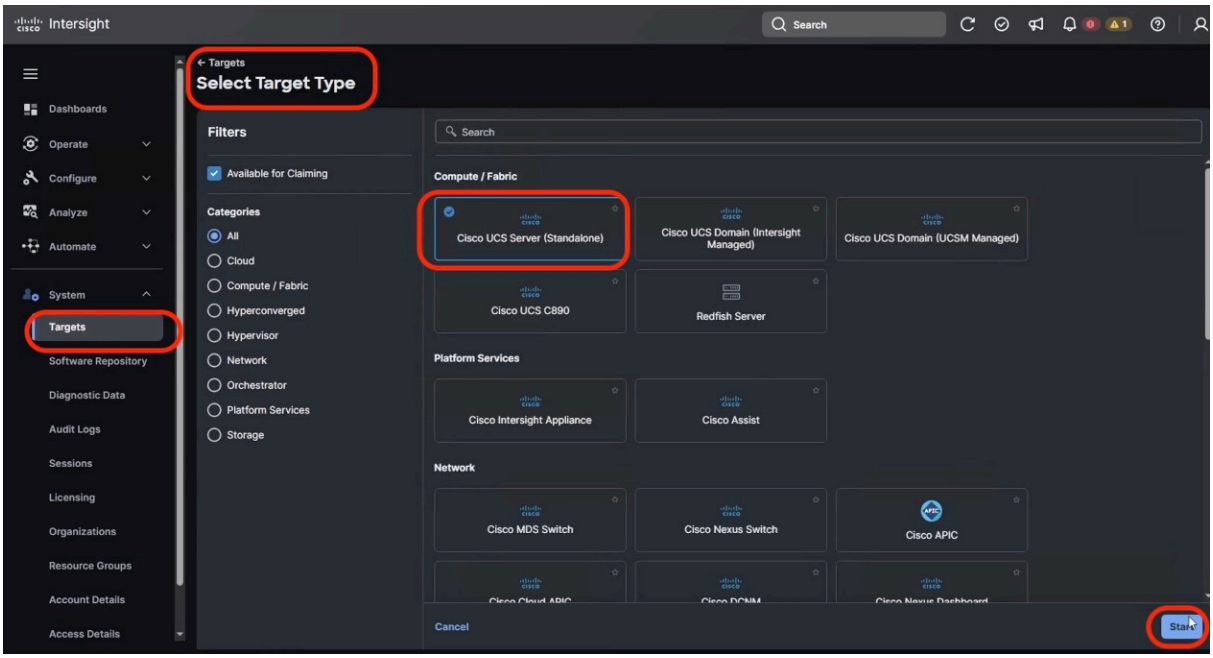
Step 7. Login to Cisco Intersight, navigate to System → Targets



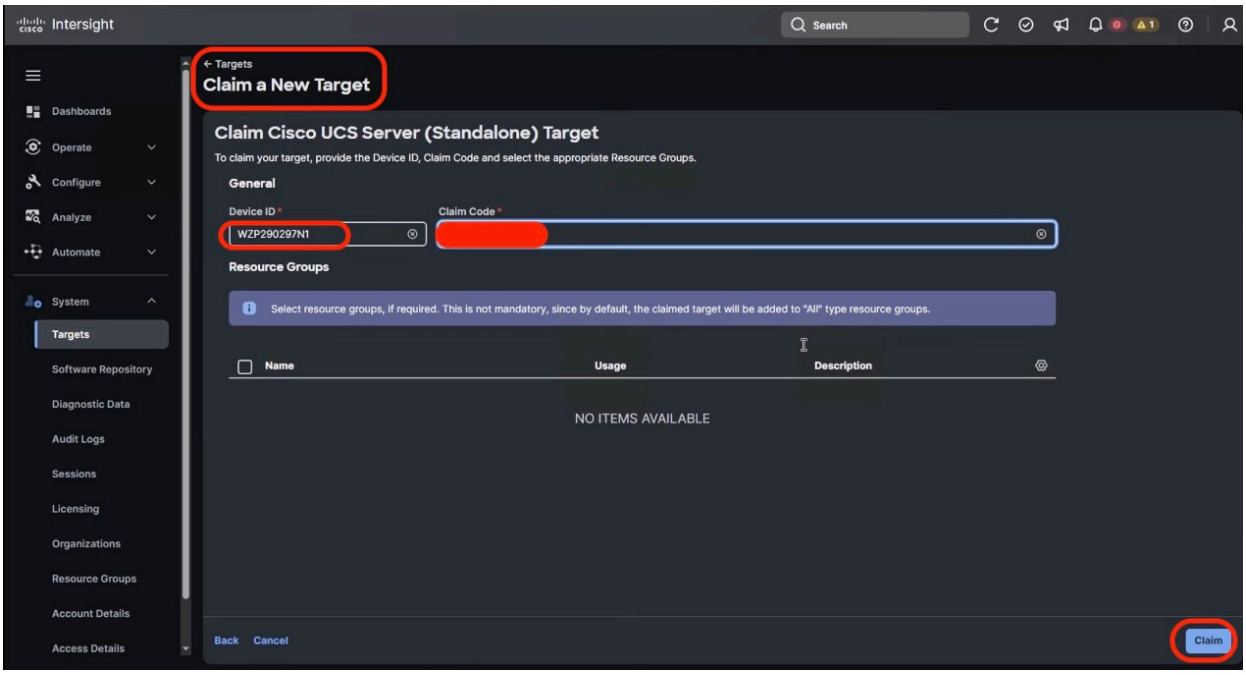
Step 8. On the top left corner, click on ‘Clain New Target’



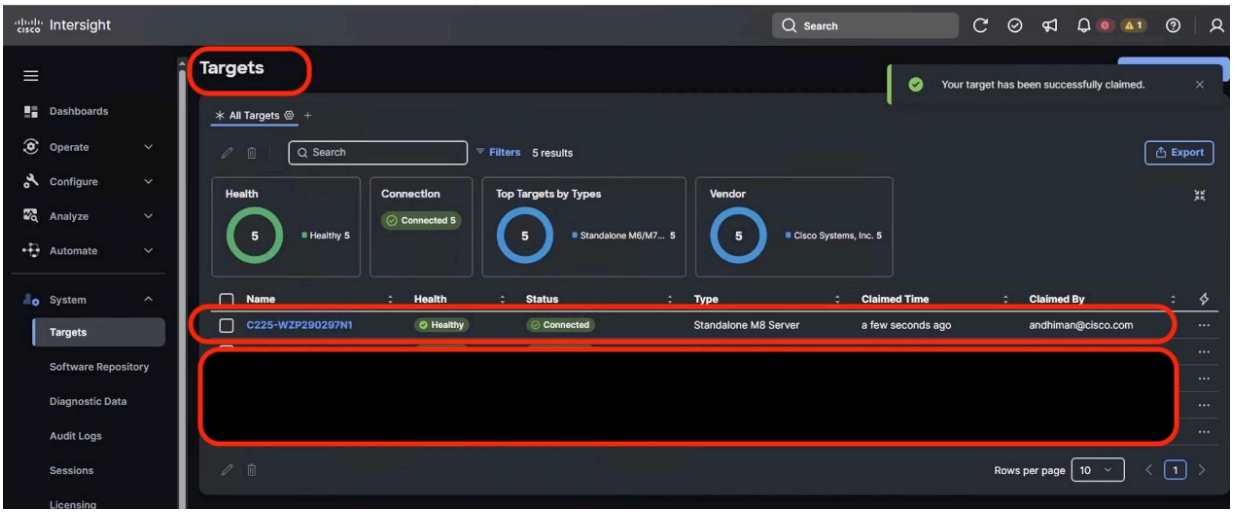
Step 9. On the 'Select Target Type" Screen, select 'Cisco UCS Server (Standalone) and click start button



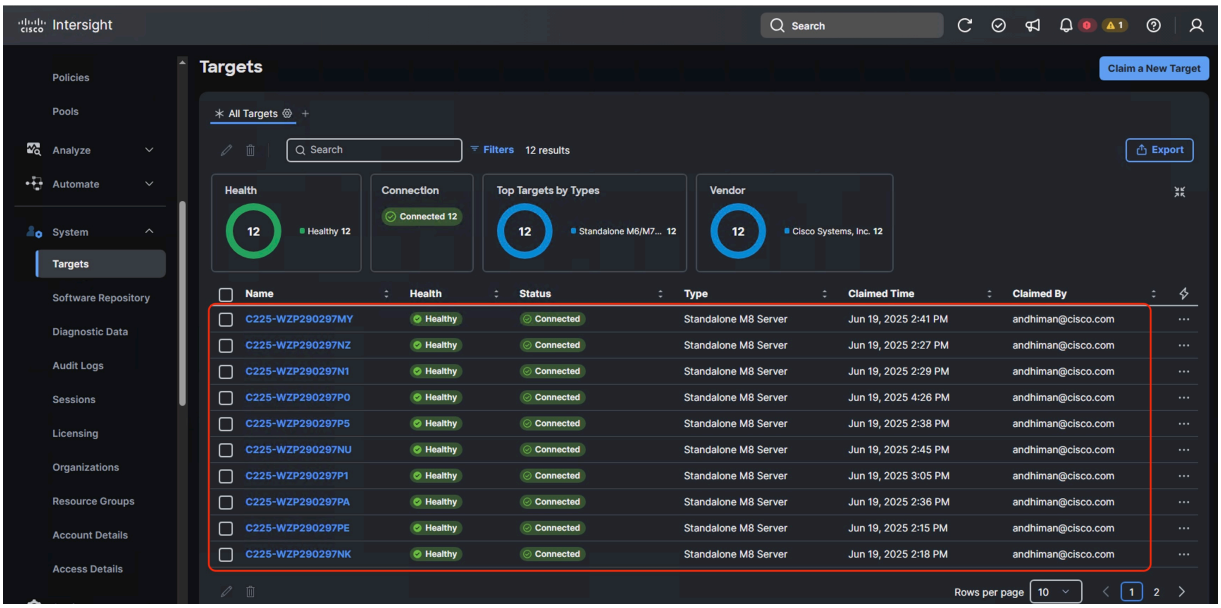
Step 10. On the 'claim a new Target' screen, Enter the Device ID and Claim Code from Cisco IMC as detailed in Step6. Click on 'Claim' button on the bottom right corner of the screen



Step 11. Cisco Intersight start the claim process of Cisco UCS C225 M8 node. Ensure the server serial number is listed in the Target screen



Step 12. Repeat the Step1 -11 to claim all the servers on Cisco Intersight.



Create Server Policies

Cisco Intersight server policies are used to define and manage the configuration of Cisco UCS servers, both in Intersight Managed Mode (IMM) and Intersight Standalone Mode (ISM). These policies cover various aspects like BIOS settings, local disk configurations, boot security, and maintenance windows. They ensure consistency, efficiency, and flexibility in server management by allowing administrators to apply predefined configurations across multiple servers.

Below are the list of Server Policies to enable VAST Data cluster on Cisco UCS C225 M8 node

- **Compute policies:**
    - Basic input/output system (BIOS)
    - Boot Order
    - Power
- **Storage policy** to define the RAID1 configuration on M.2 Boot SSD
- **Management Policies:**
    - IPMI over LAN
    - Serial over LAN
    - Local User – enables IPMI username password. Once configured , same username password would be used to access KVM and local Cisco IMC Dashboard
    - Virtual KVM – enables tunned/remote access to KVM of each VAST cluster node

Procedure 1. Create BIOS Policy

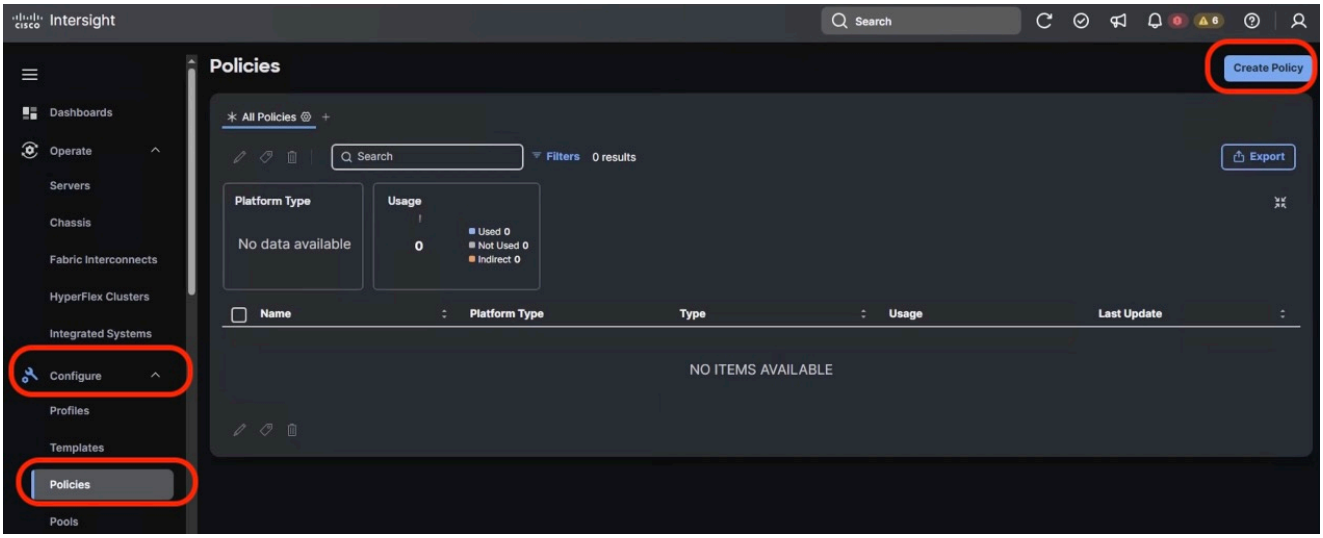
Table below, lists the required configuration for the BIOS policy.

Table 5. BIOS settings for VAST Data on Cisco UCS C225 M8 nodes

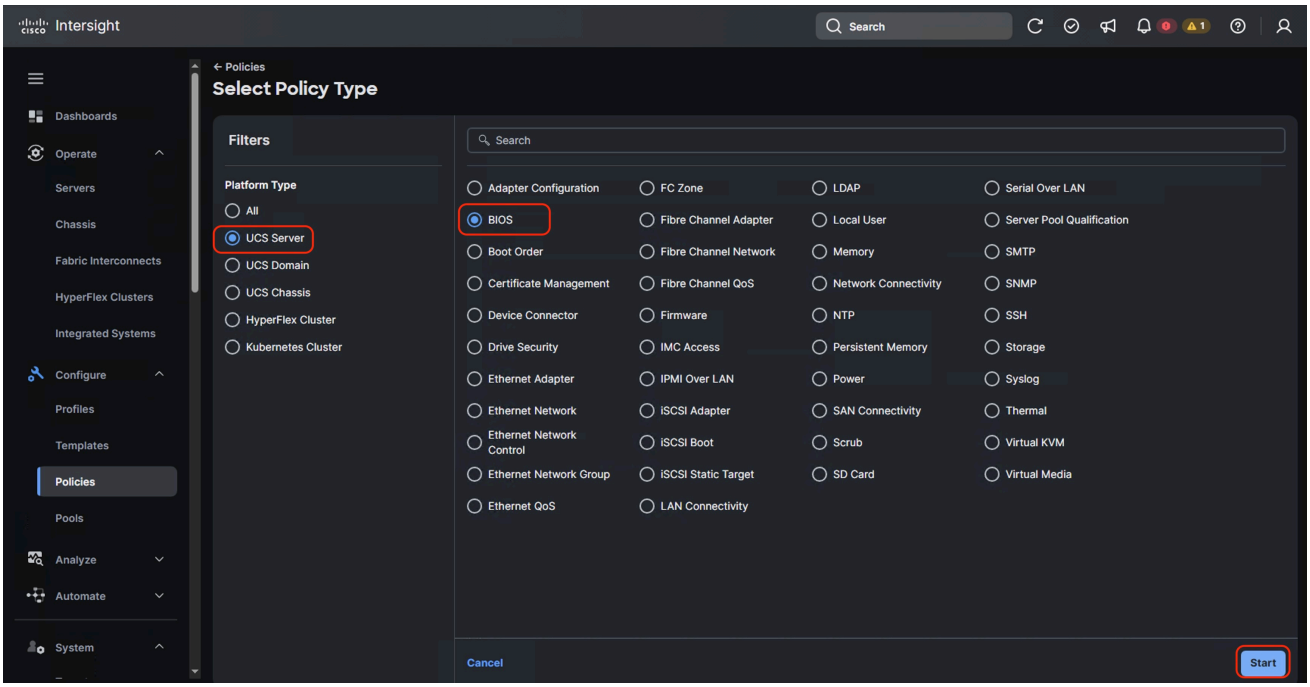
	Option	Settings
Boot Options	IPV4 HTTP Support	disabled
	IPv4 PXE Support	disabled

	Option	Settings
	IPV6 HTTP Support	disabled
	IPV6 PXE Support	disabled
Processor	Local APIC Mode	X2APIC
PCI	SR-IOV Support	enabled
Server Management	Console Redirection	COM0

Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

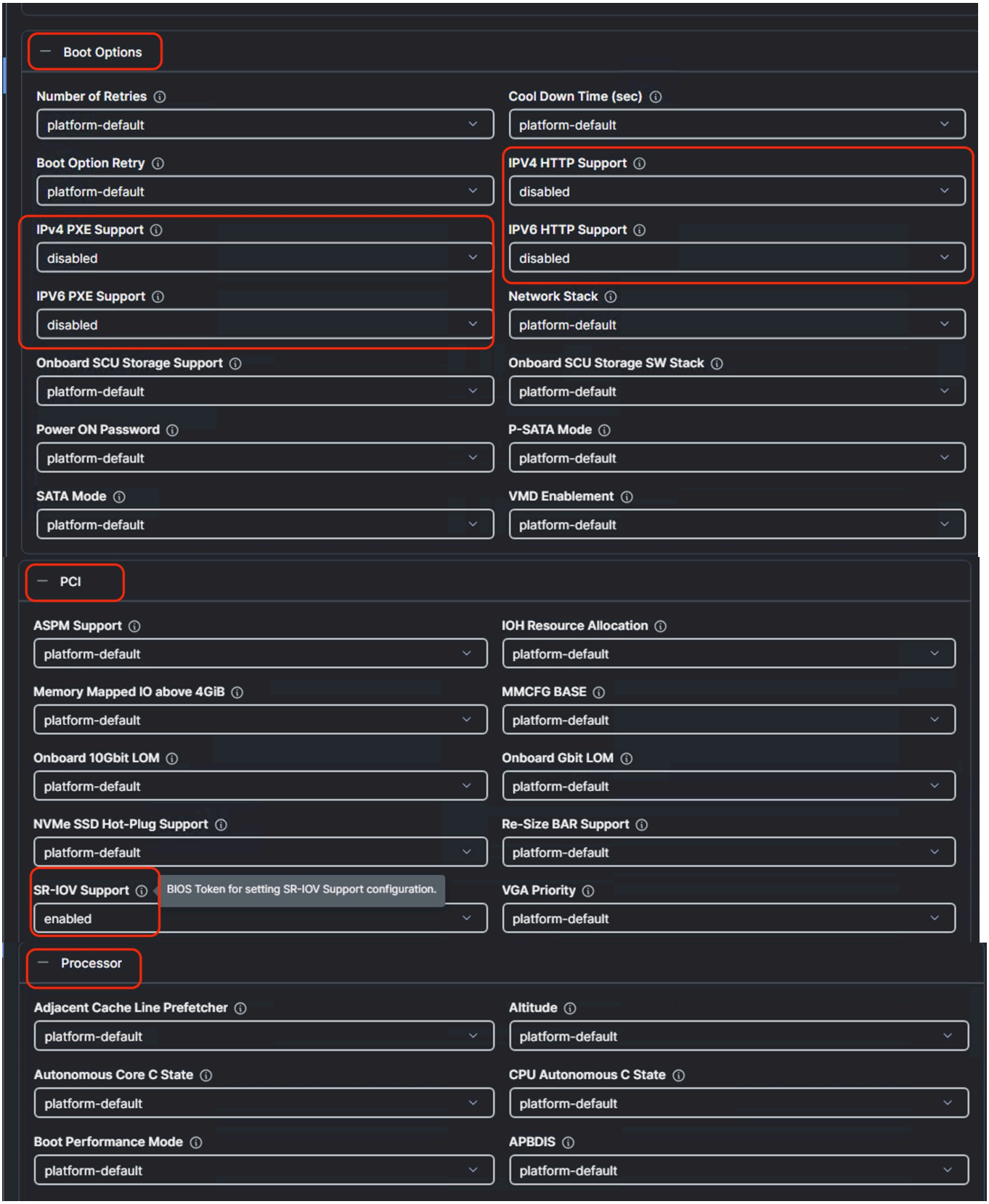


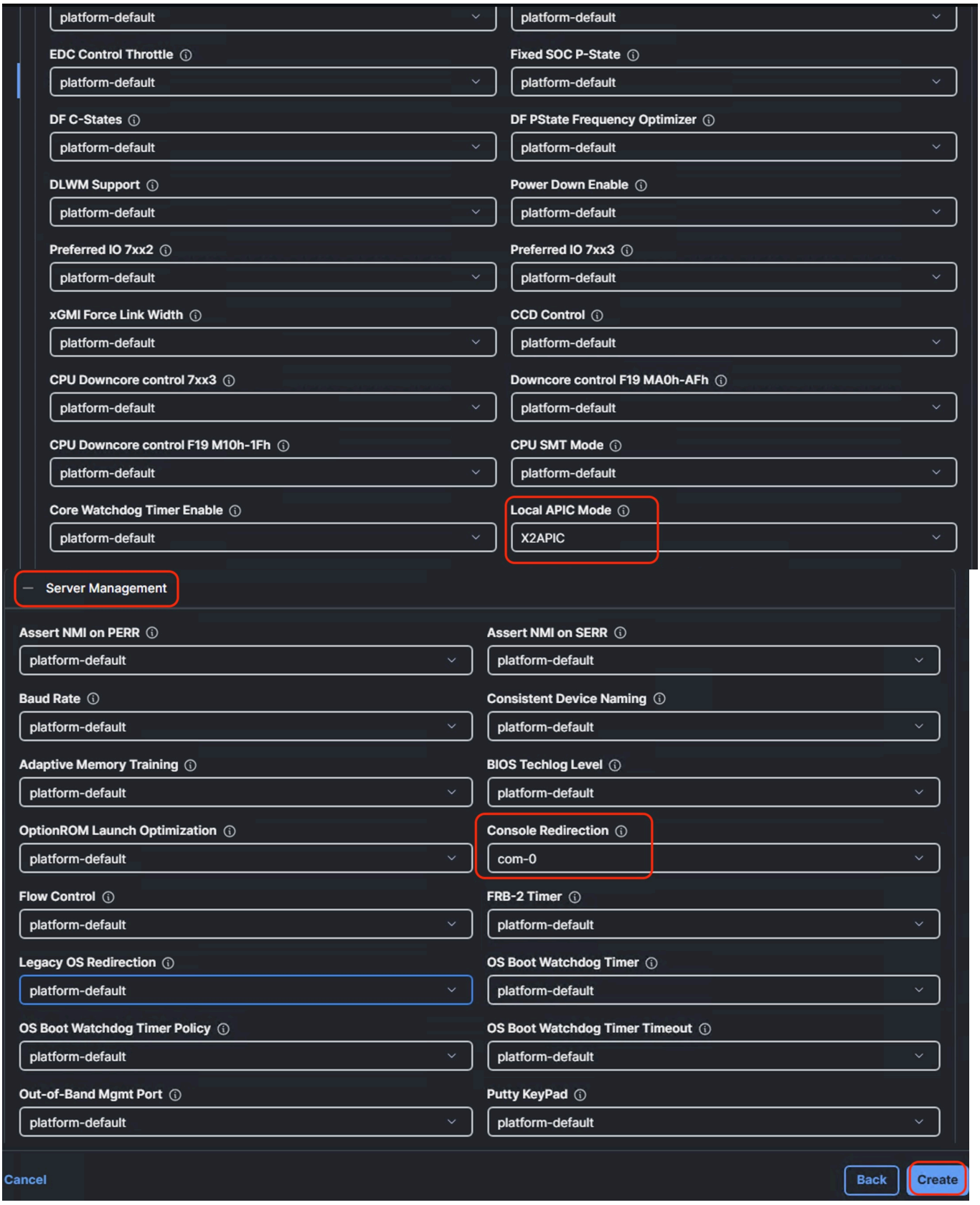
Step 2. On the 'Select Policy Type" screen , Select UCS Server and BIOS. Click on Start button



Step 3. Enter name of the Policy and click Next

Step 4. On Policy detail screen, select UCS Server (Standalone) tab. Select BIOS options as given in above table. The BIOS policy attribute selection are detailed in figure below and click ‘Create’





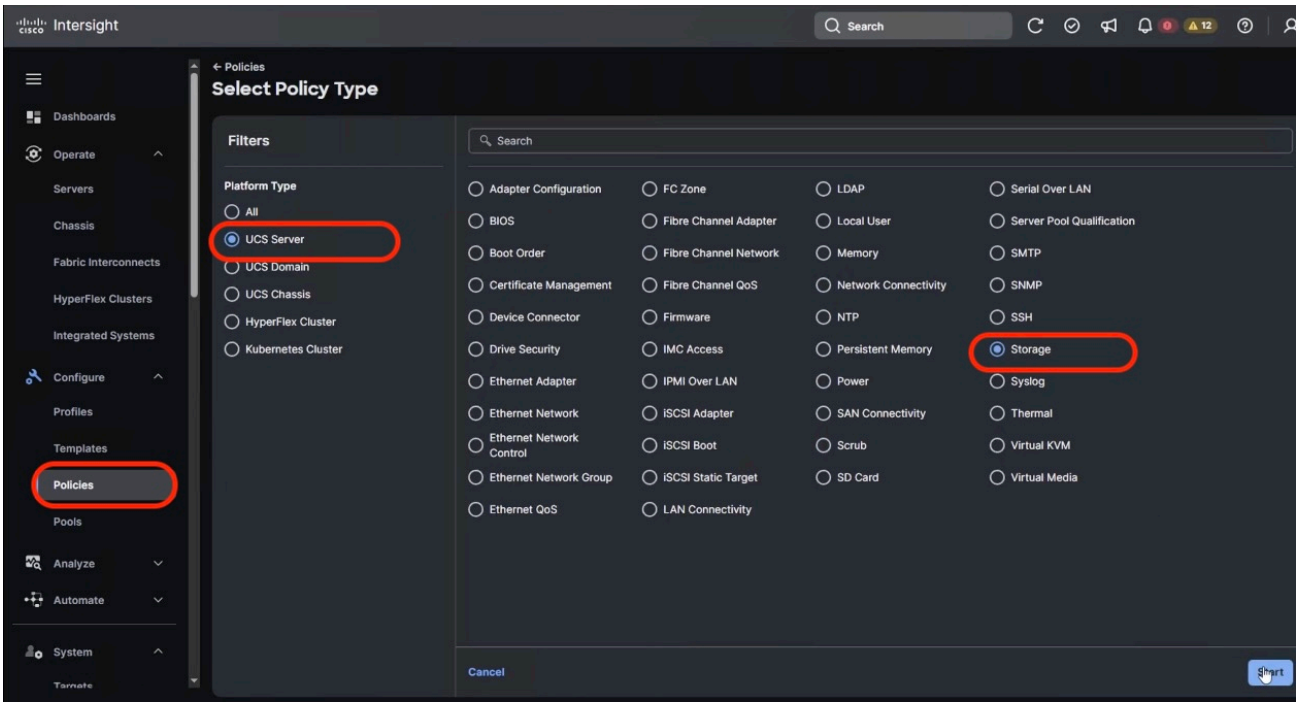
○

Procedure 2. Create Storage Policy

Storage Policy enables RAID1 across 2x M.2 Boot drives

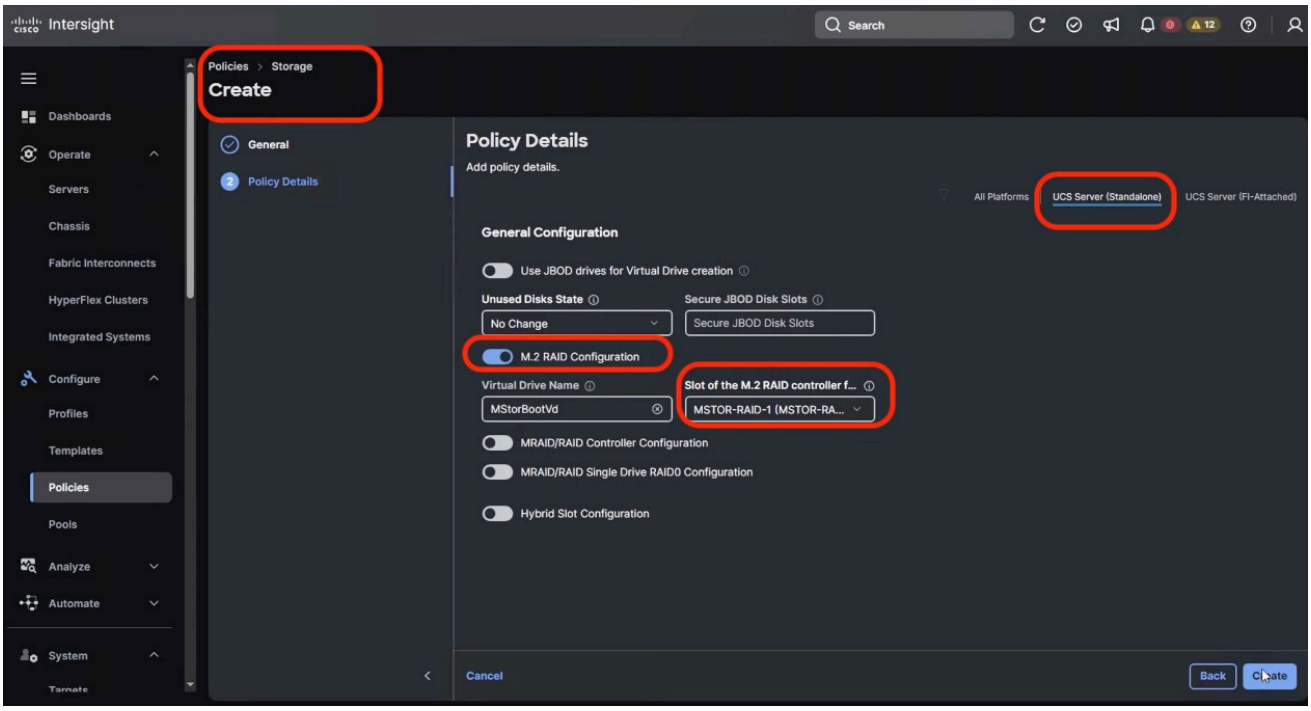
Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → Storage option and click Start



Step 3. Add a name to the Storage Policy and click Next

Step 4. Select UCS Server (Standalone), Enable M.1 RAID Configuration. MSTOR-RAID is selected by default for 'Slot of the M.2 RAID controller'. Click 'Create'

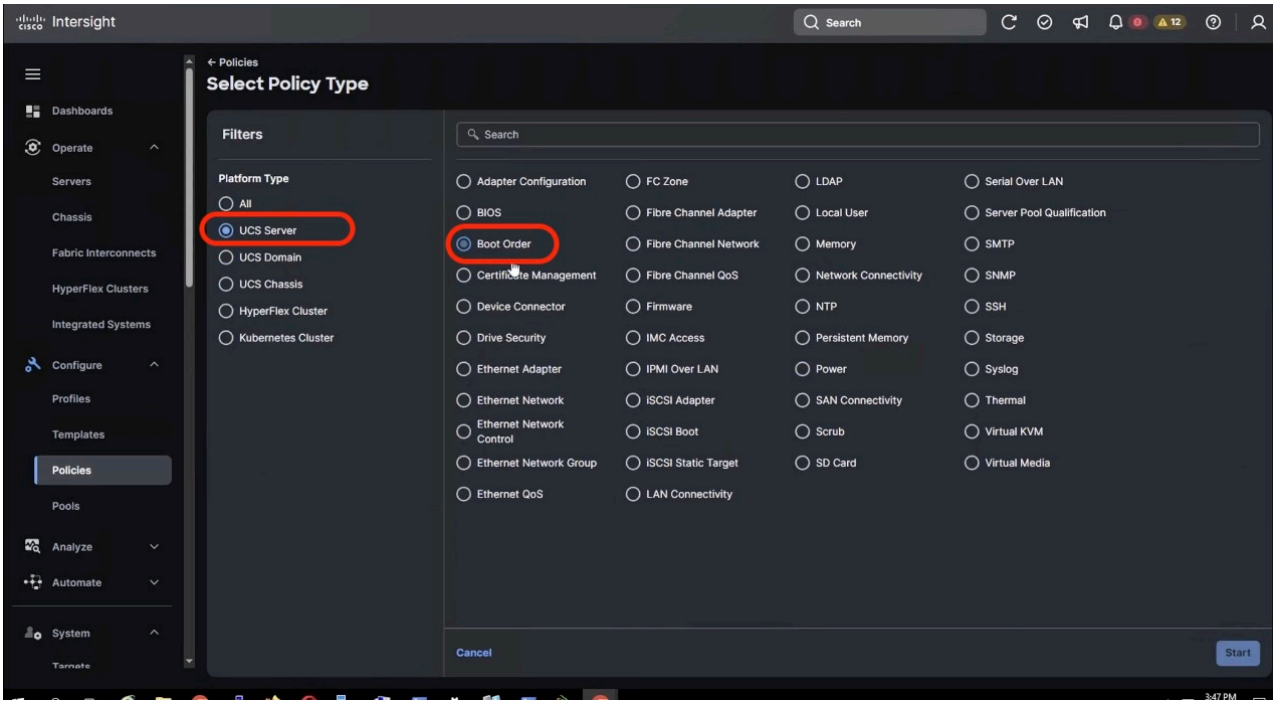


Procedure 3. Create Boot Order Policy

Boot Order Policy enable boot for RAID1 virtual drive created on 2x M.2 cards and virtual media mount point

Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

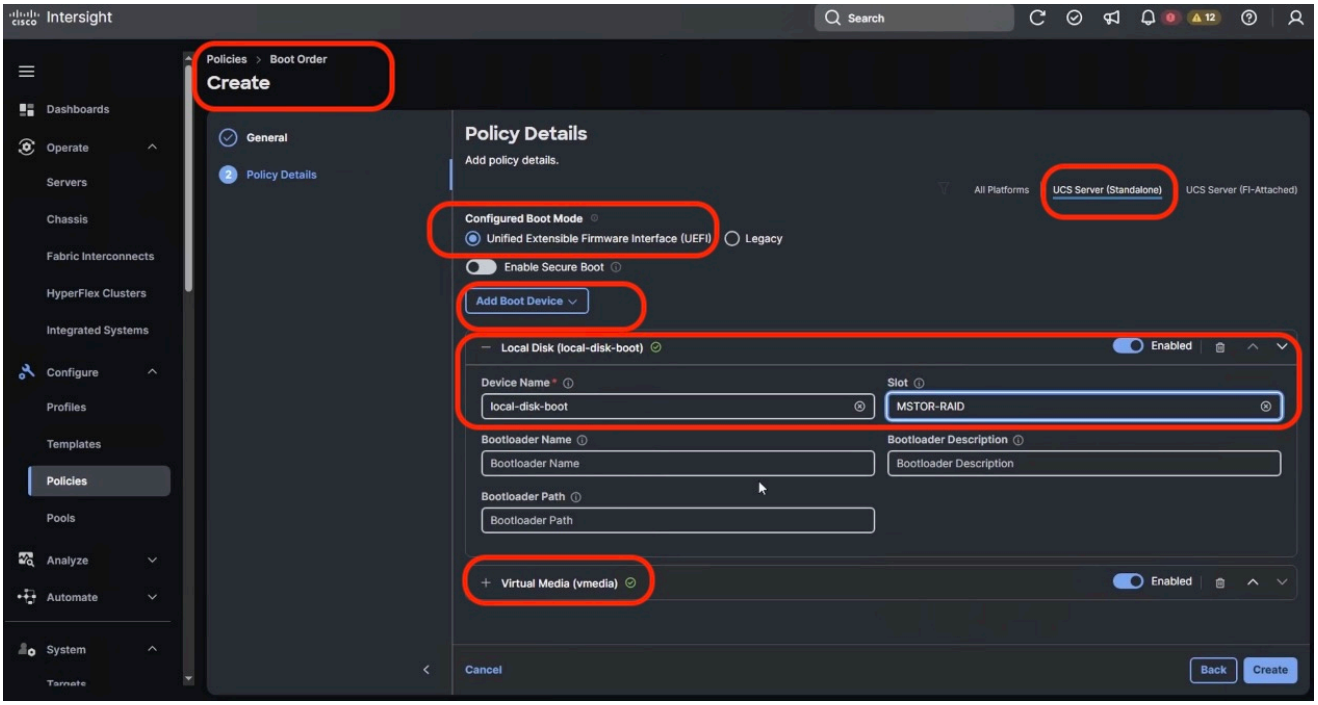
Step 2. Select UCS Server → Boot Order option and click Start



Step 3. Add a name to Boot Order Policy and click ‘Next’

Step 4. Under Policy details ,

- Select UCS Server (Standalone) option
- Add **virtual media (vmedia)** as boot device and name the device as ‘vmedia1’ or any name as per your naming convention
- Add another boot target as ‘**local disk’.** Name the boto target device as **‘local-disk-boot’ or** any name as per your naming convention. In the Slot field, enter ‘**MSTOR-RAID’** as shown in screenshot below.



Step 5. Ensure the first boto target is Local Disk and the Slot for Local Disk is ‘MSTOR-RAID’

Step 6. Click create

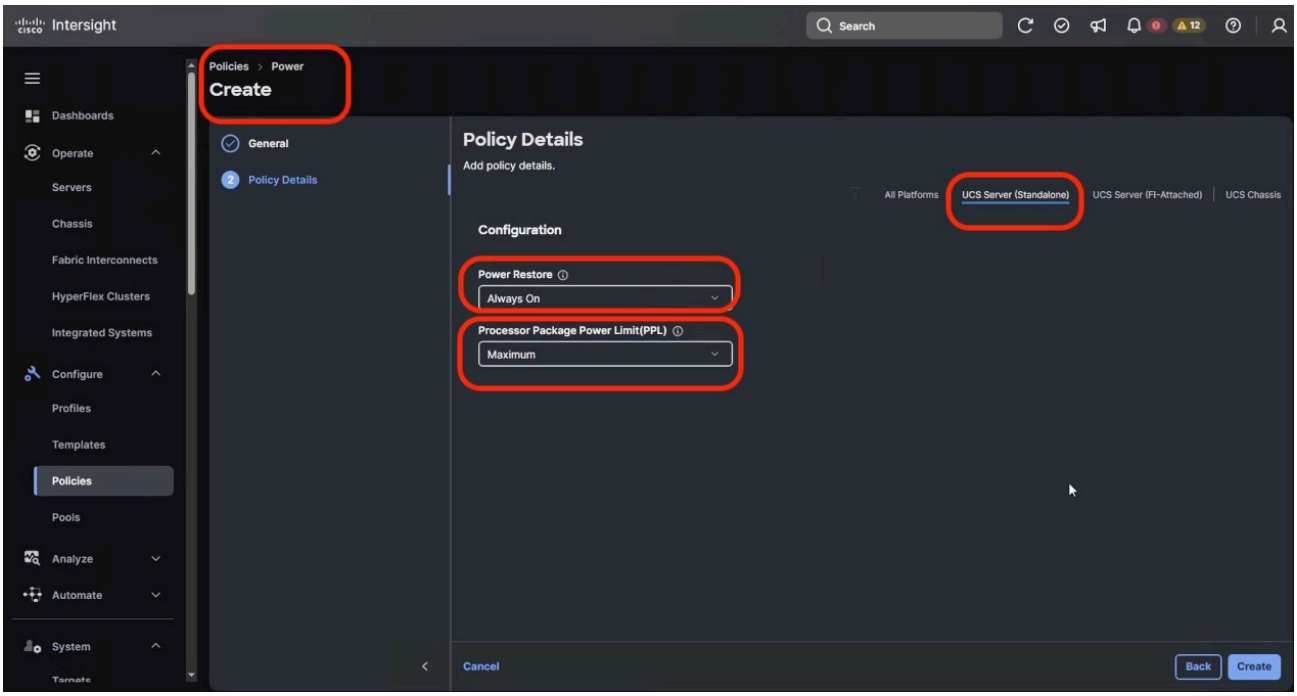
Procedure 4. Create Power Policy

Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → Power option and click Start

Step 3. Add a name to the Power Policy and click Next

Step 4. On the Policy detail screen, **Select UCS Server (Standalone)** , **Power Restore Policy** as Always On **and Processor Package Power Limit (PPL)** as Maximum . Selections are details in screenshot Below



Step 5. Click create

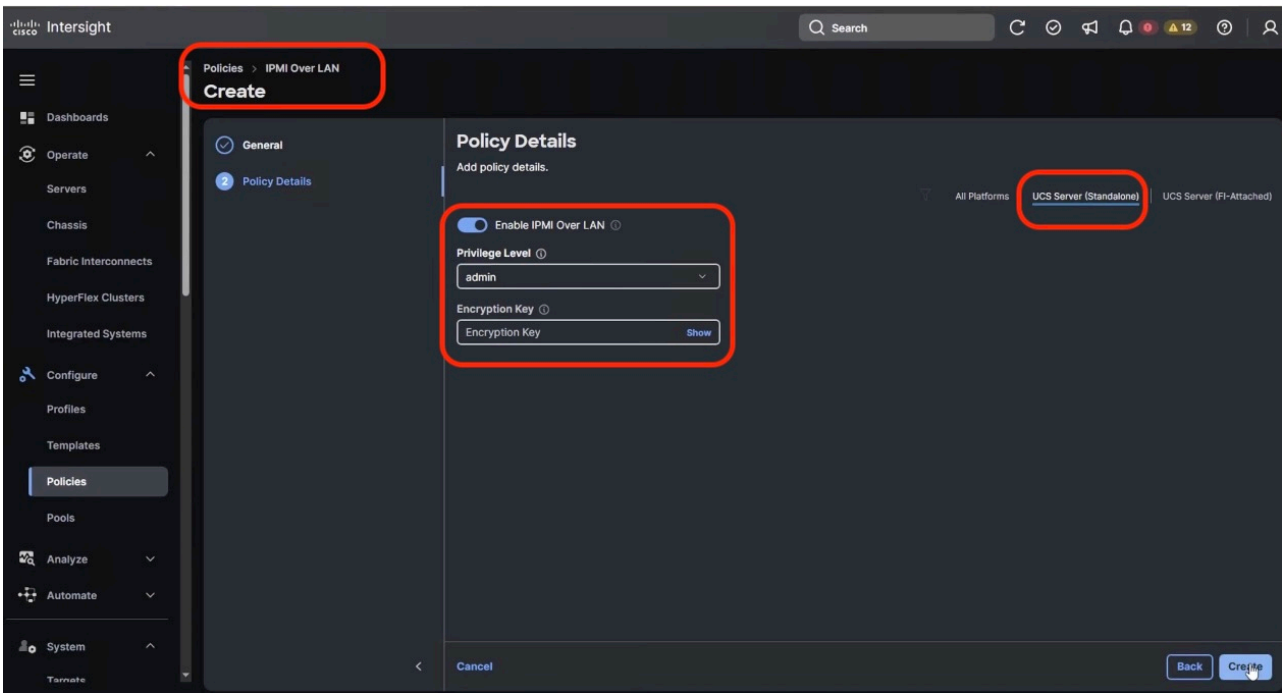
Procedure 5. Create IPMI over LAN Policy

Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → IPMI over LAN option and click Start

Step 3. Add a name to the Policy and click Next

Step 4. On the Policy detail screen, Select UCS Server (Standalone) , Ensure **Privilege Level** is admin and click create



Step 5. Click create

Procedure 6. Create Local User Policy

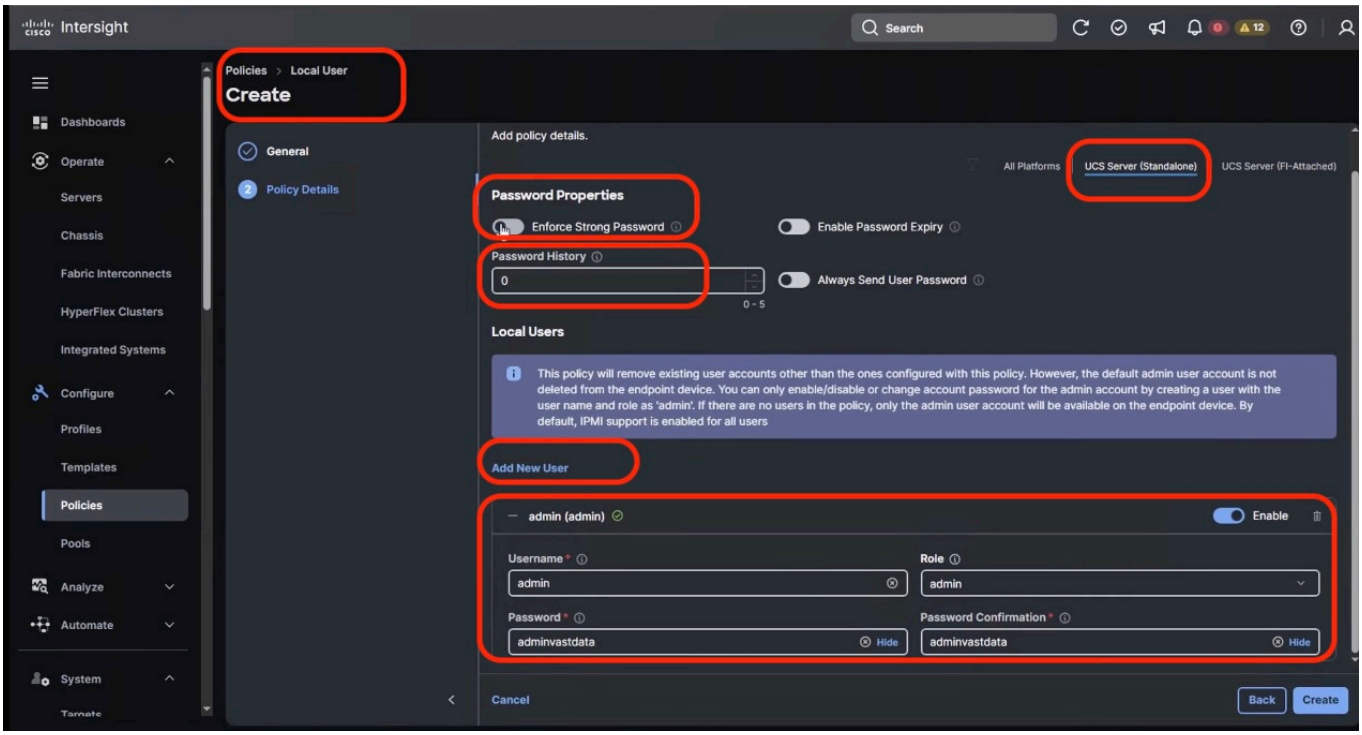
Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → Local User option and click Start

Step 3. Add a name to the Policy and click Next

Step 4. On the Policy detail screen, Select UCS Server (Standalone) ,

- Disable “Enforce Strong Password’
- Change the Password History to 0 (password never expires)
- Add a New user with username admin , Role admin and password as ‘adminvastdata’



Step 5. Click create

Note: During initial deployment , password should be kept as adminvastdata with Role admin. User can change access the KVM and CIMC local dashboard through this username and password

Note: Same username password is used for VAST IPMI access of nodes. In the event user change the IPMI password through VAST cluster , they should ensure to change the admin password for local user through the User Policy

Procedure 7. Create Serial Over LAN Policy

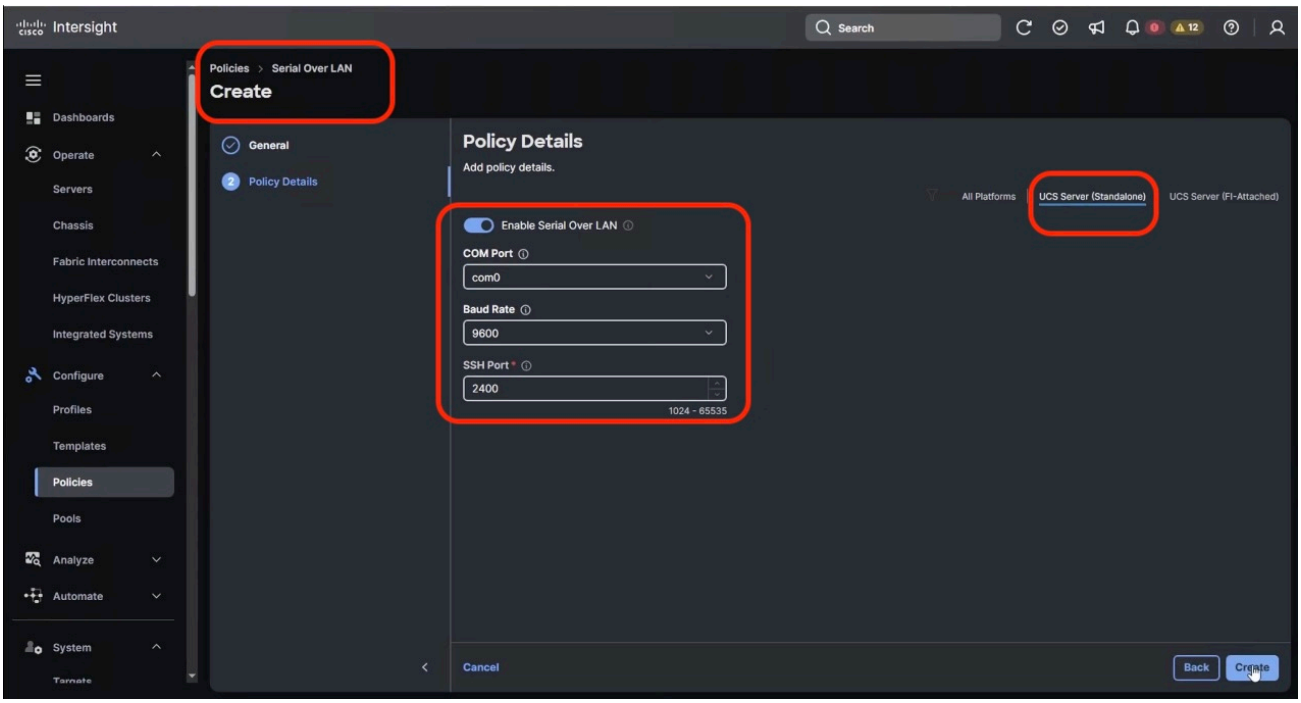
Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → Serial Over LAN option and click Start

Step 3. Add a name to the Policy and click Next

Step 4. On the Policy detail screen, Select UCS Server (Standalone) , and ensure default selected are as below

- COM Port as com0
- Baud Rate as 9600
- SSH Port as 2400



Step 5. Click create

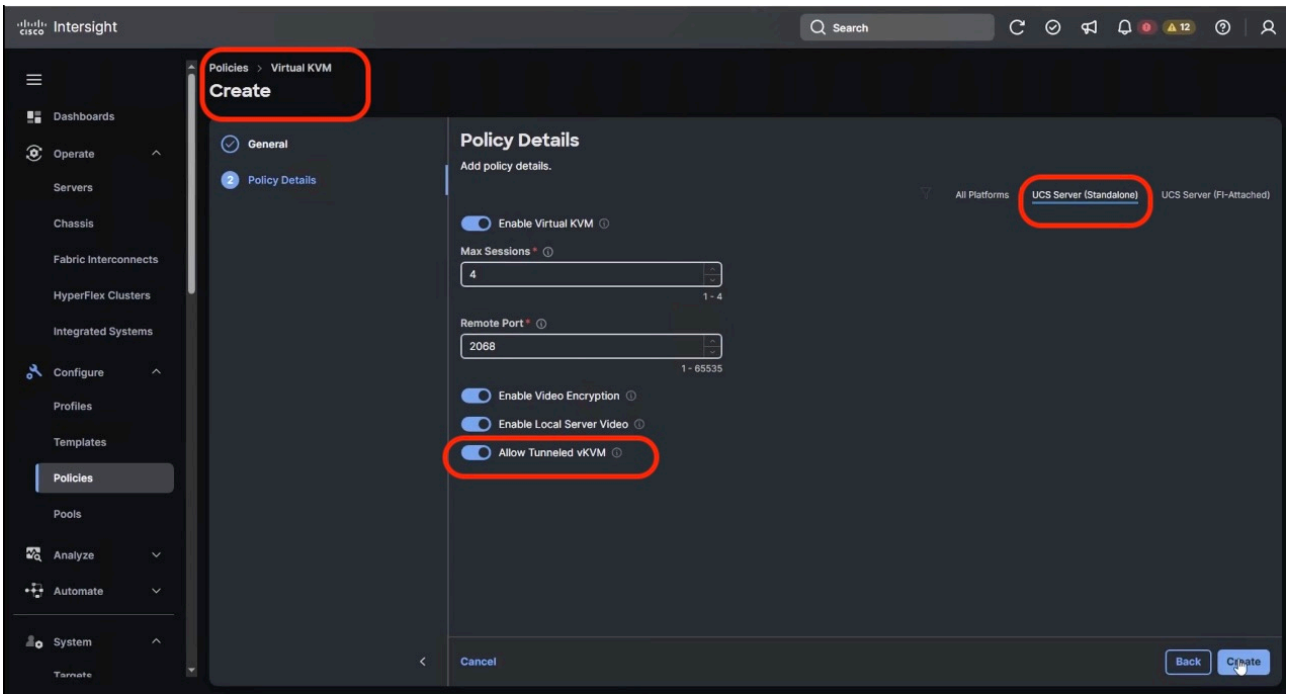
Procedure 8. Create Virtual KVM Policy

Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

Step 2. Select UCS Server → Virtual KVM and click Start

Step 3. Add a name to the Policy and click Next

Step 4. On the Policy detail screen, Select UCS Server (Standalone) , and **enable Allow Tunneled vKVM**



Step 5. Click create

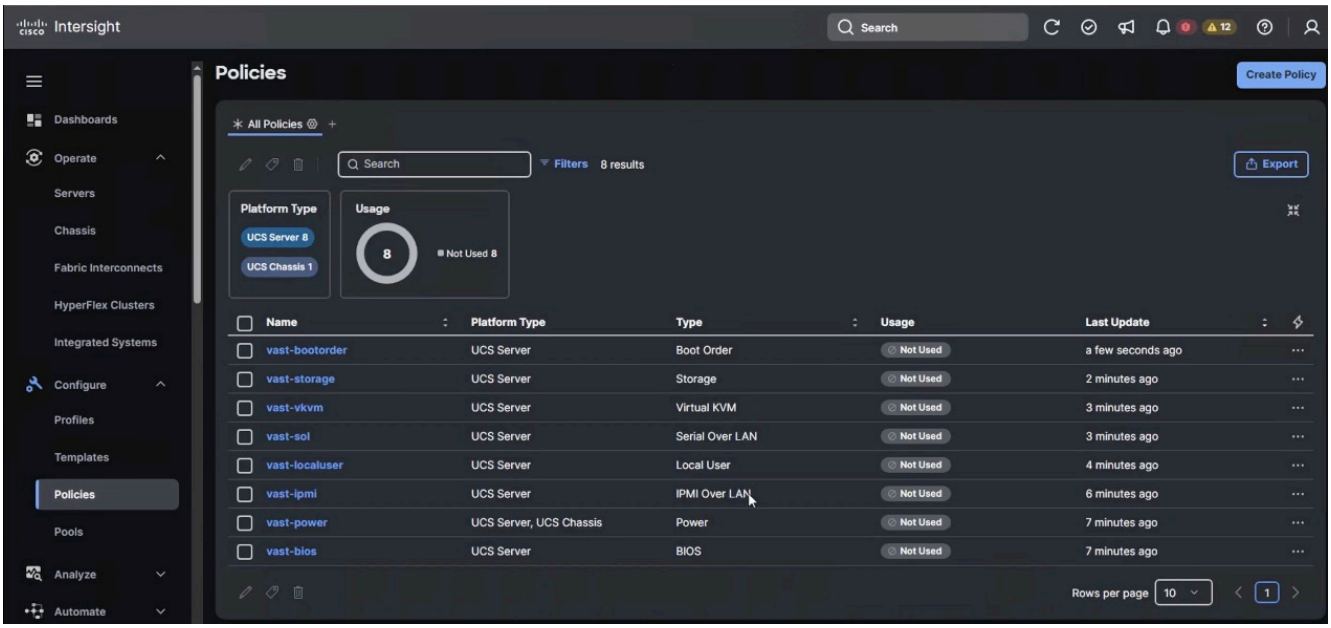
Create UCS Server Profile Template

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

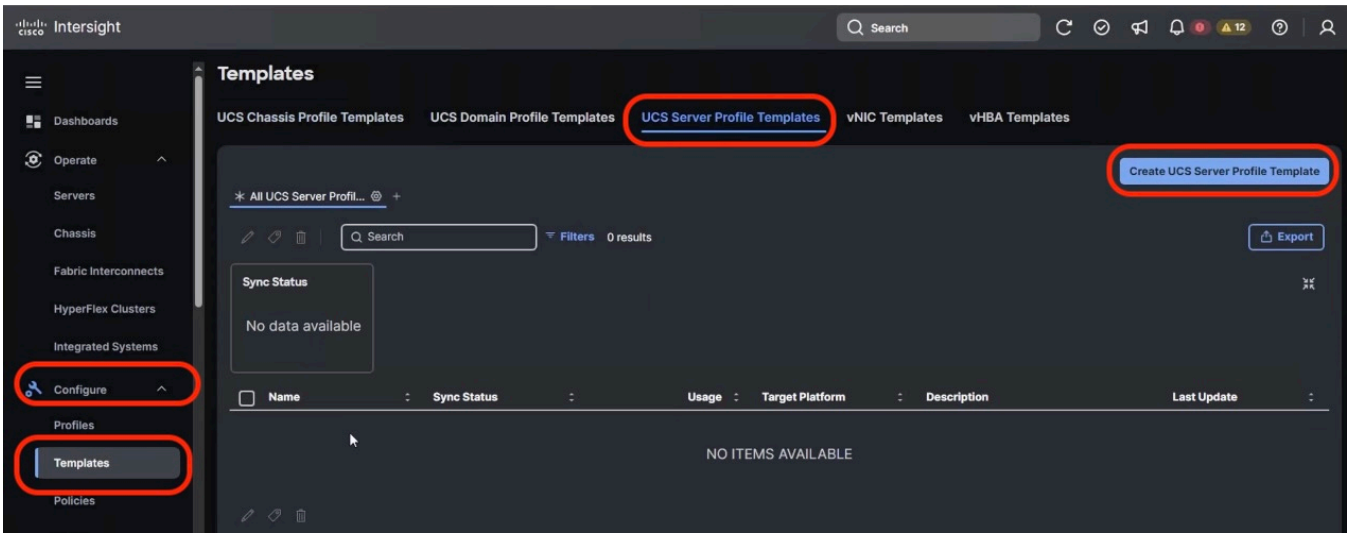
Table 6. Policies required for Server profile template

Compute Policies	Storage Policies	Management Policies
BIOS Policy	RAID1 for 2x M.2 Boot card	IPMI Over LAN Policy
Boot Order Policy		Local User Policy
Power Policy		Serial Over LAN Policy
		Virtual KVM Policy

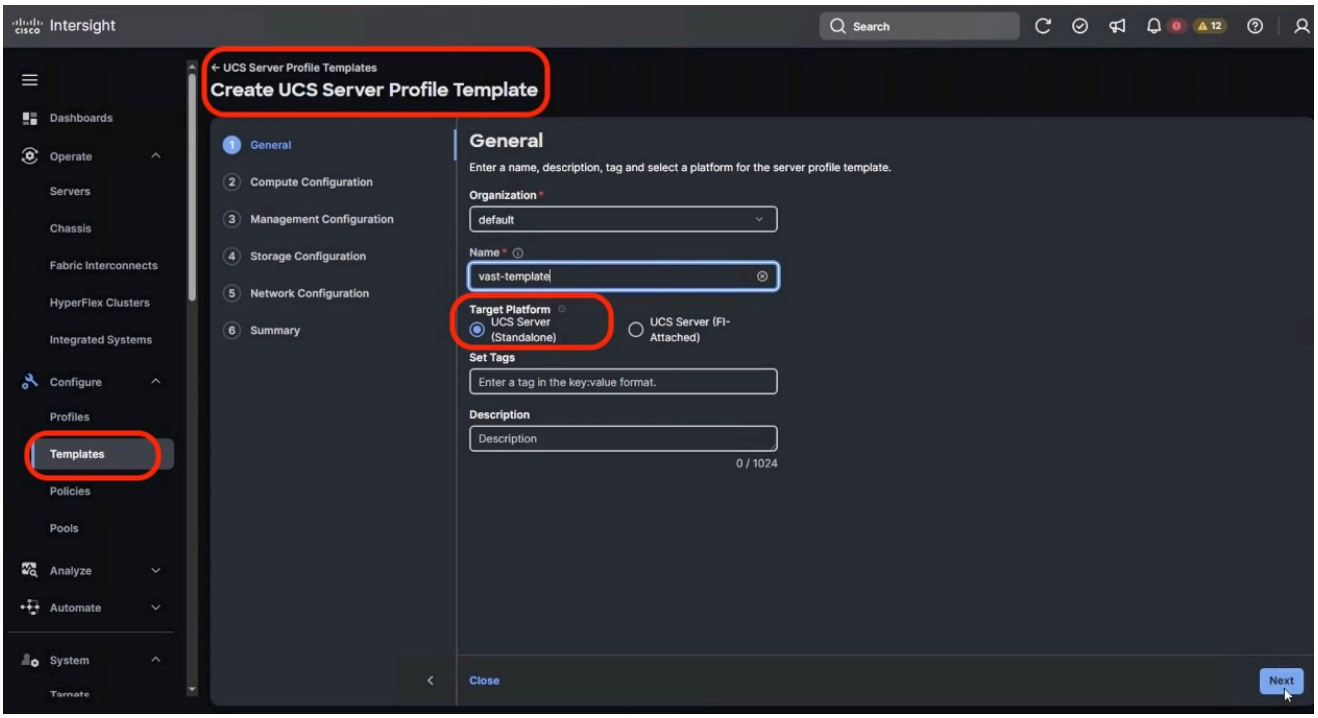
The screenshot below displays all the seven Sever Policies created to create Server Profile Template for VAST Data nodes



Step 1. From left navigation pane, Select Configure, select Templates, select UCS Server Profile Template and click Create UCS Server Profile Template.

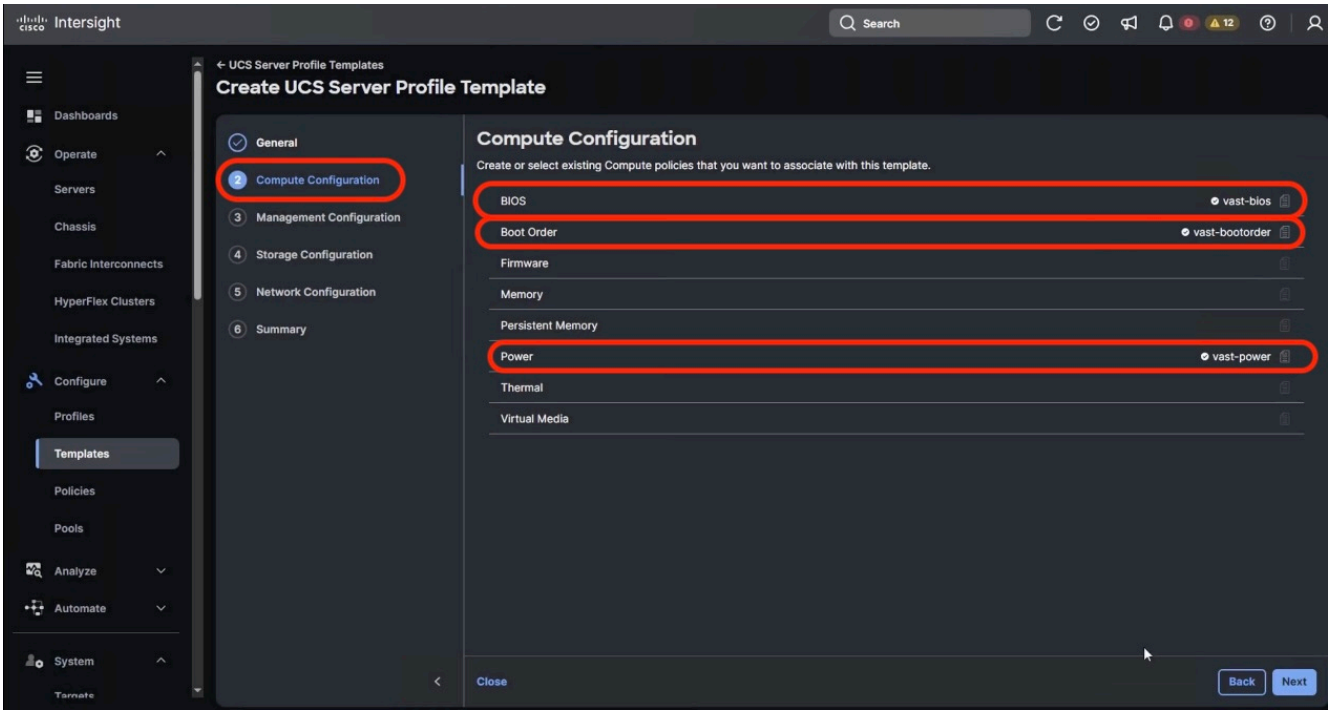


Step 2. Name the Server Profile Template, select Target Platform as UCS Server (Standalone) and click Next.



Step 3. On the Compute Configuration section, select the previously created policies as detailed below. Click Next

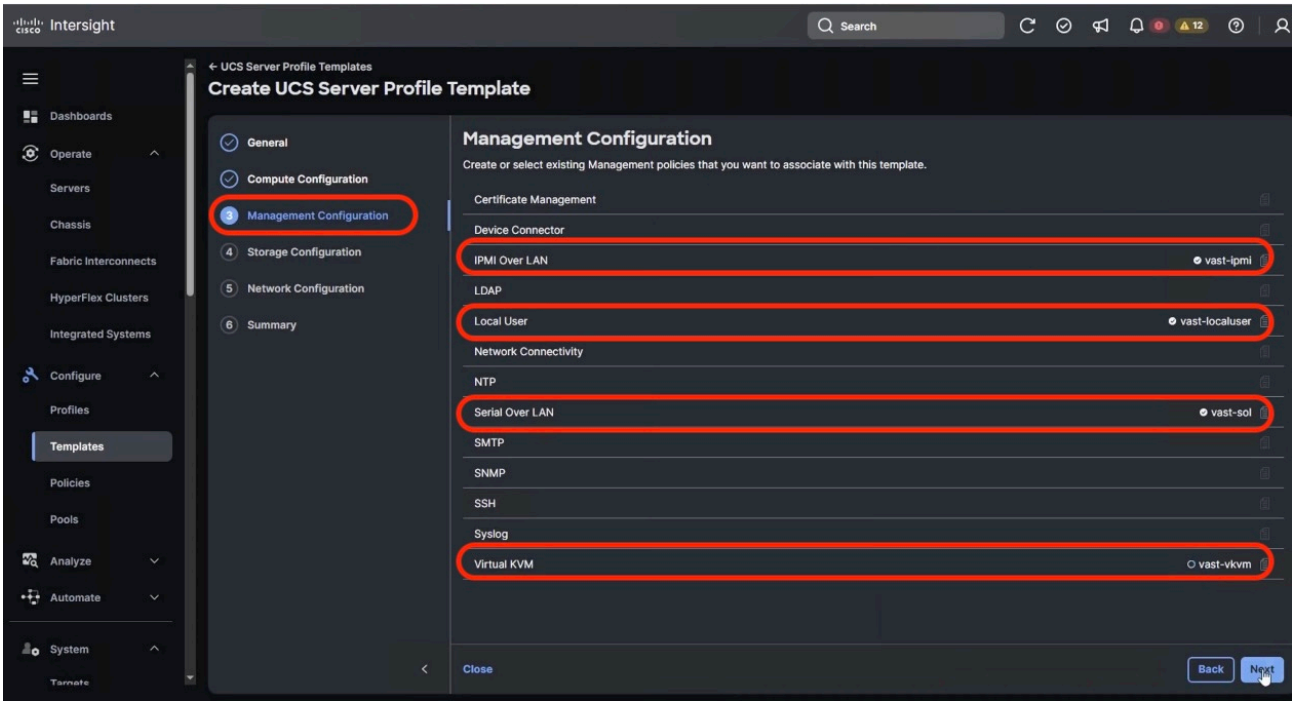
- BIOS Policy
- Boot Order Policy
- Power Policy



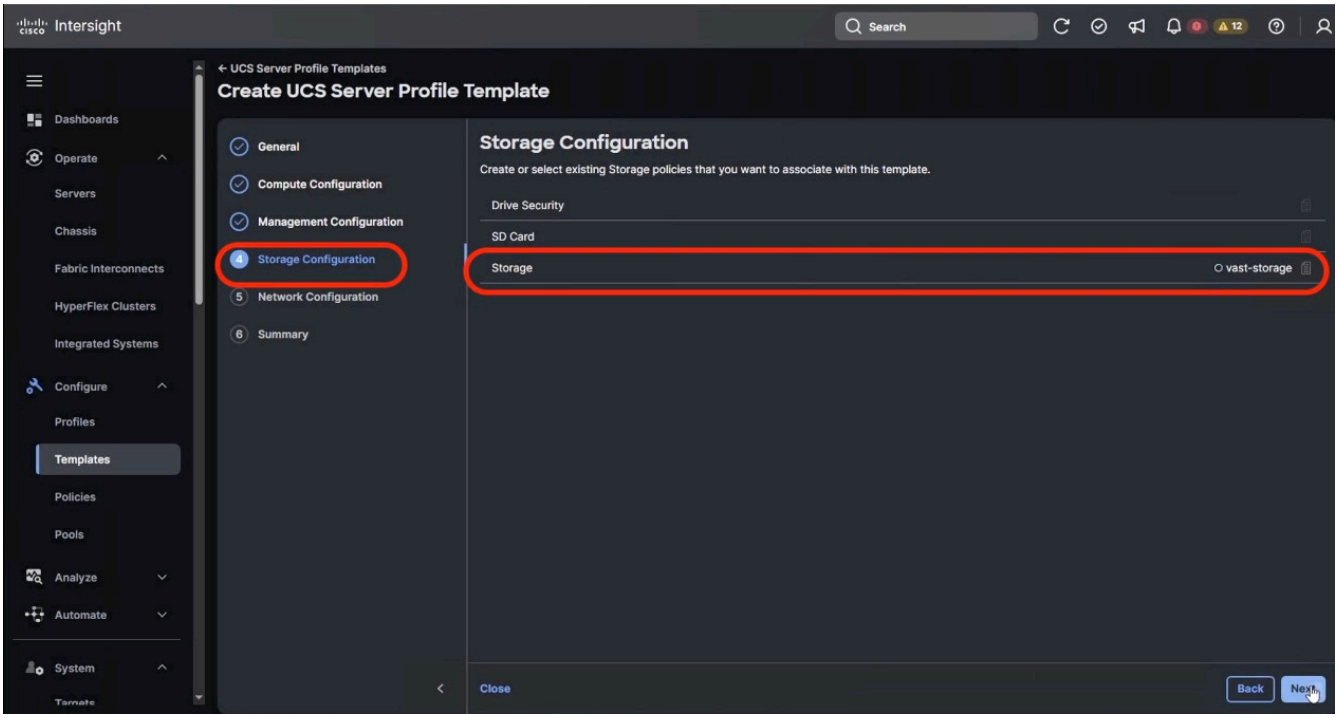
Step 4. On the Management Configuration section, select the previously created policies as detailed below. Click Next

- IPMI Over LAN Policy

- Local User Policy
- Serial Over LAN Policy
- Virtual KVM Policy

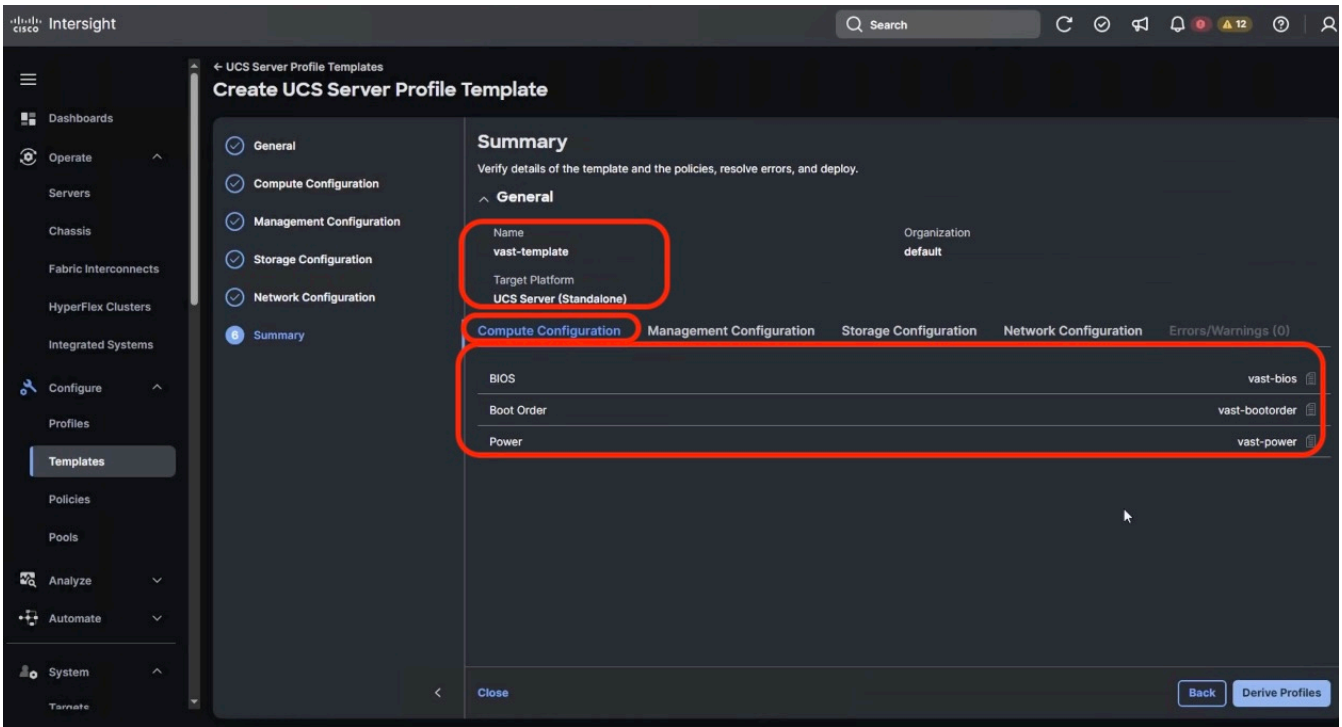


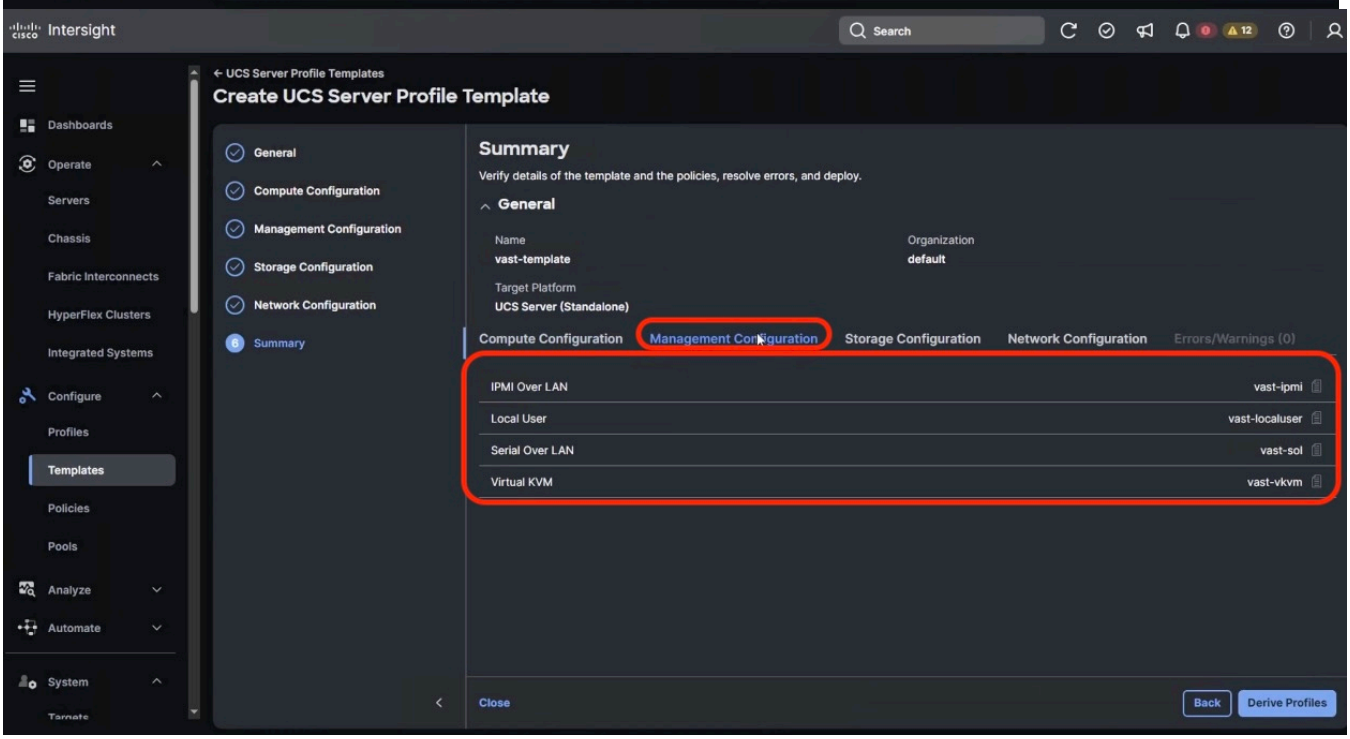
Step 5. On the Storage Configuration section, select the previously created Storage Policy as detailed below. Click Next

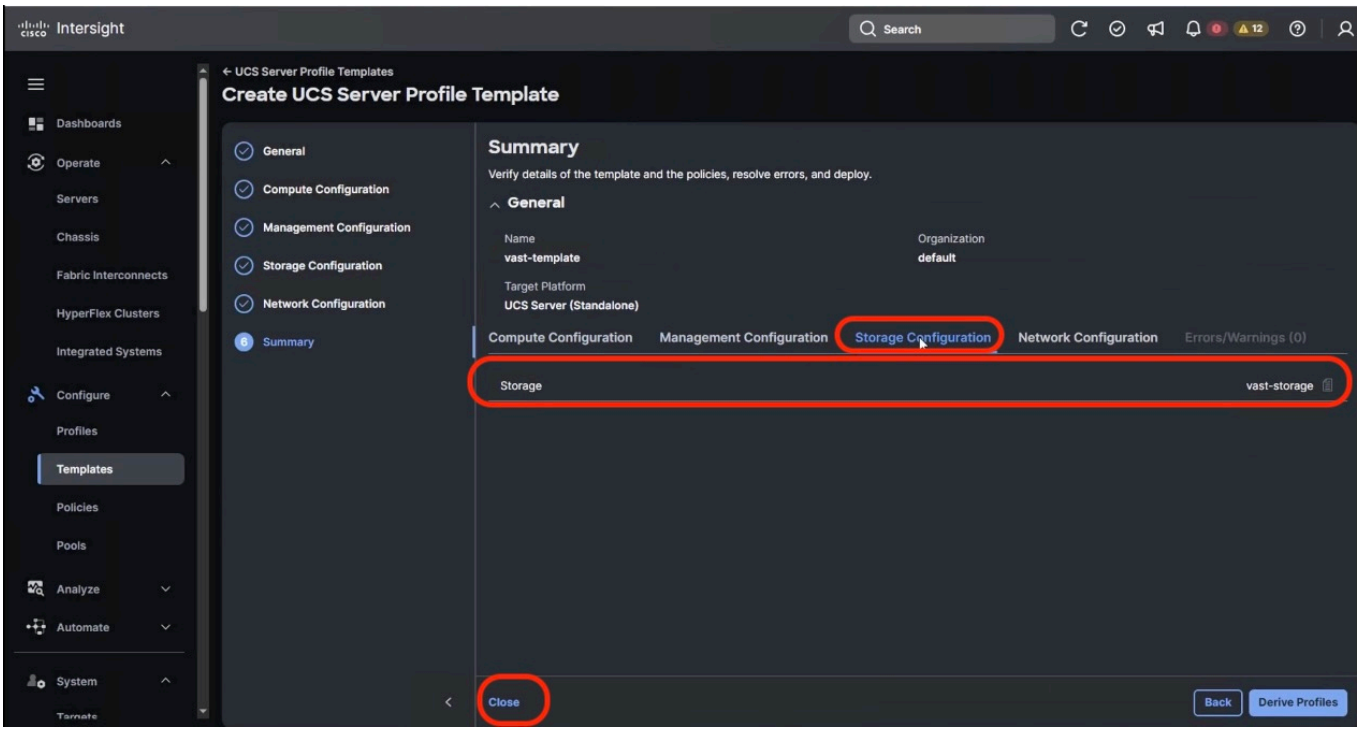


Step 6. No Server Policies are selected in Network Configuration section. Click Next

Step 7. Verify the Server Profile Template Summary (Compute , Management and Storage Configuration), click Close





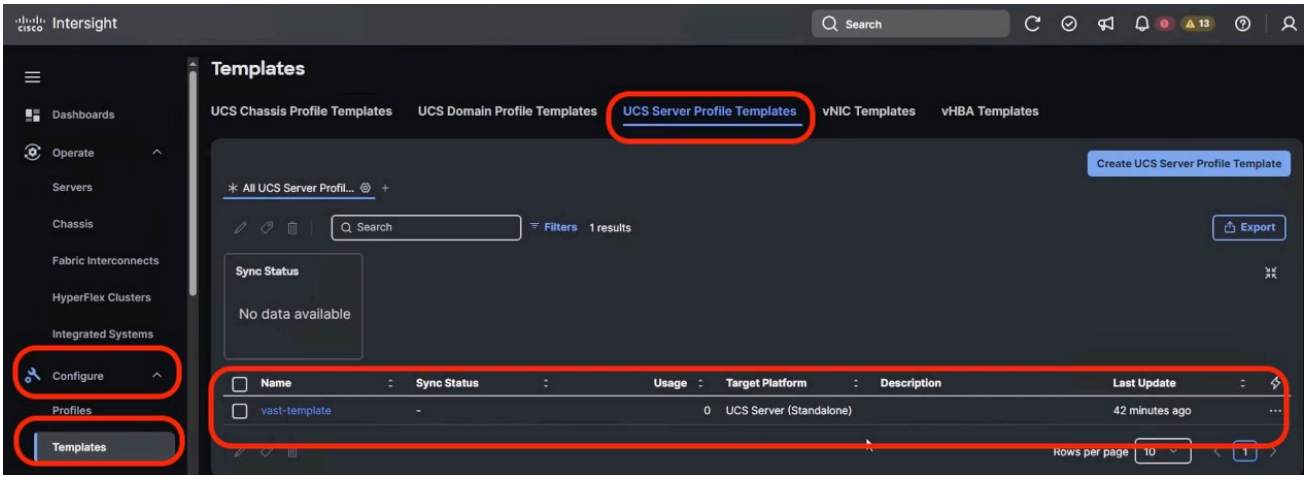


Derive and Deploy UCS Server Profile

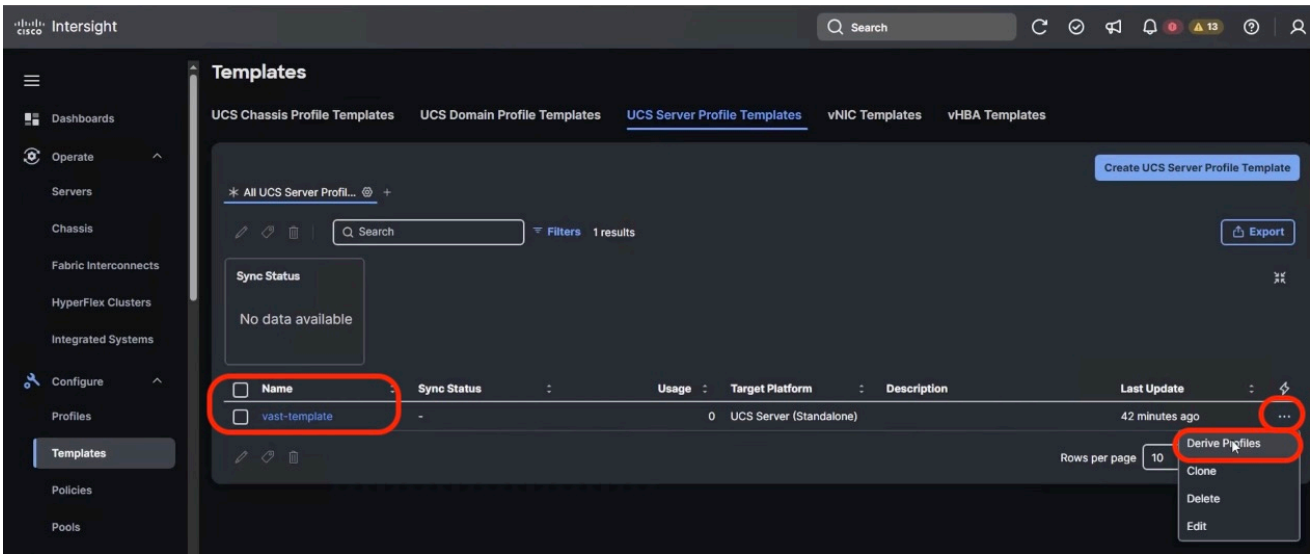
In this procedure, Server Profiles are derived from Server Profile Template and deployed on Cisco UCS C-Series nodes certified for the VAST Data

Note: The Server Profile Template specific to the VAST Cluster was configured in the previous section.

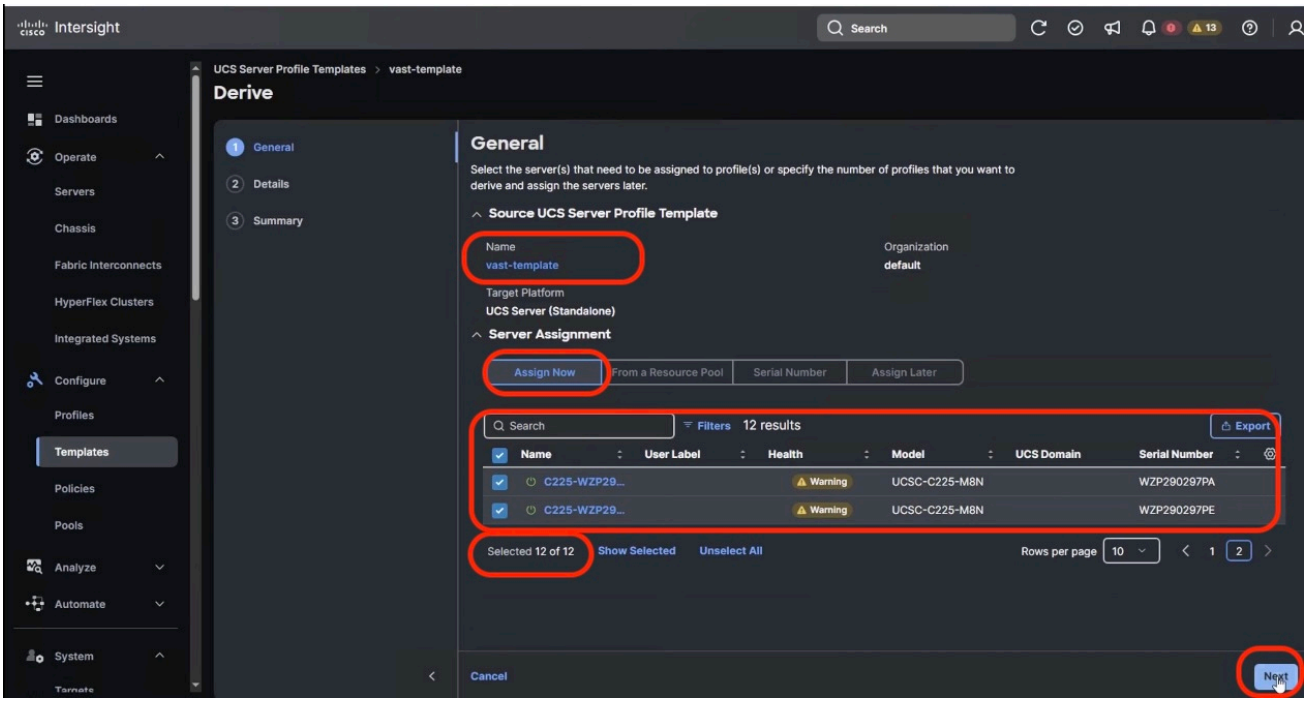
Step 1. Select Configure → UCS Server Profile Template and identify the VAST Server Profile Template created.



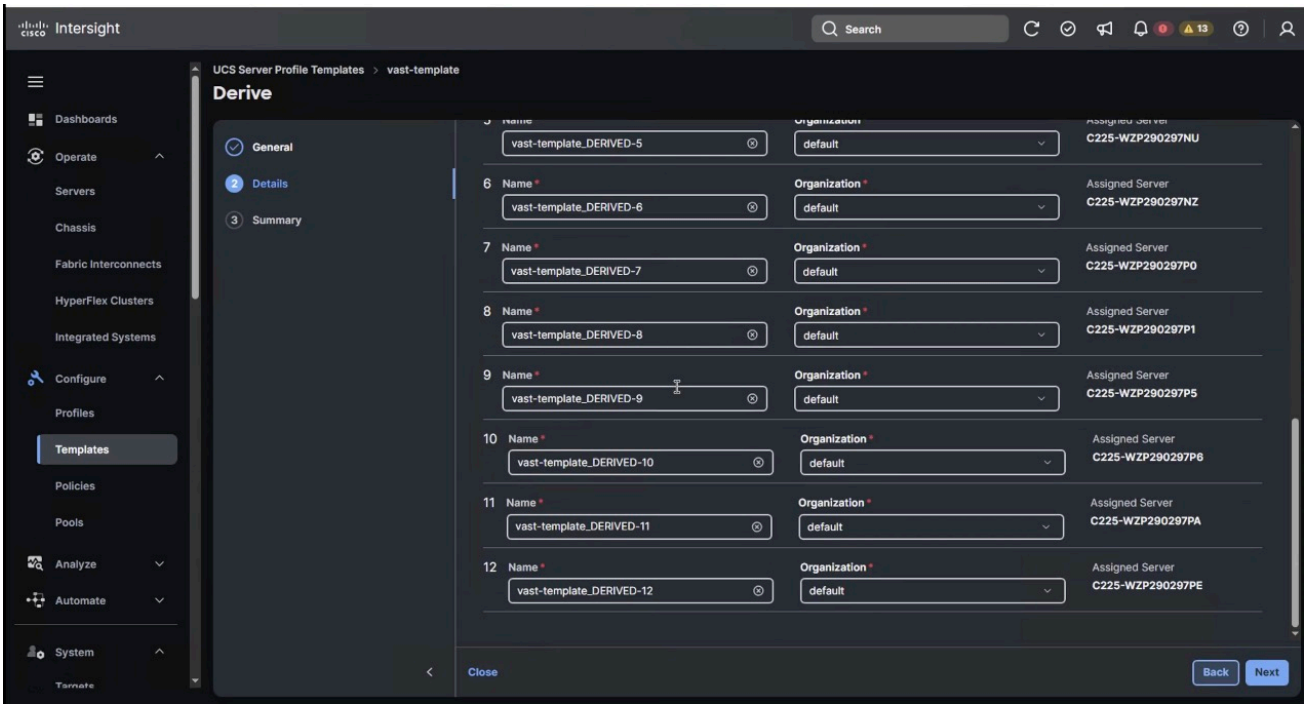
Step 2. Click the … icon and select Derive Profiles.



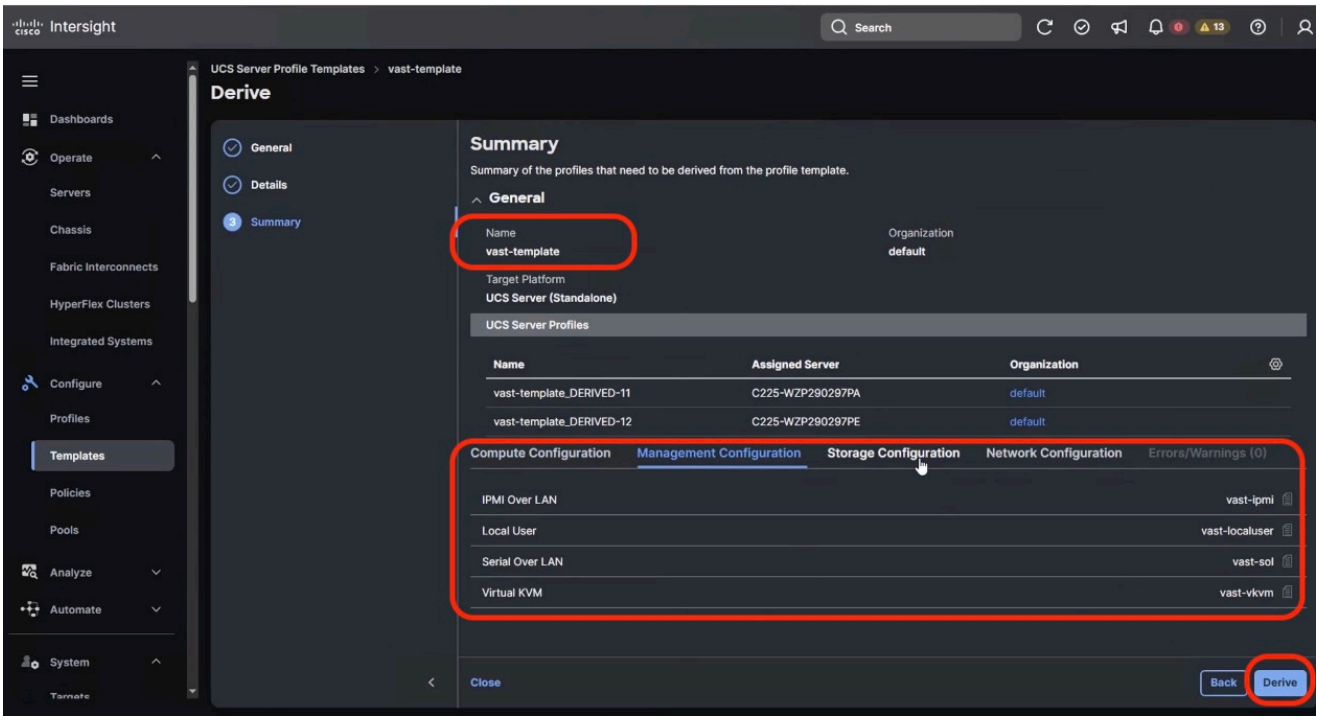
Step 3. Select all the Cisco UCS C225 M8 nodes which are claimed to create VAST cluster. Ensure 'Assign Now' option is selected by default. Click Next



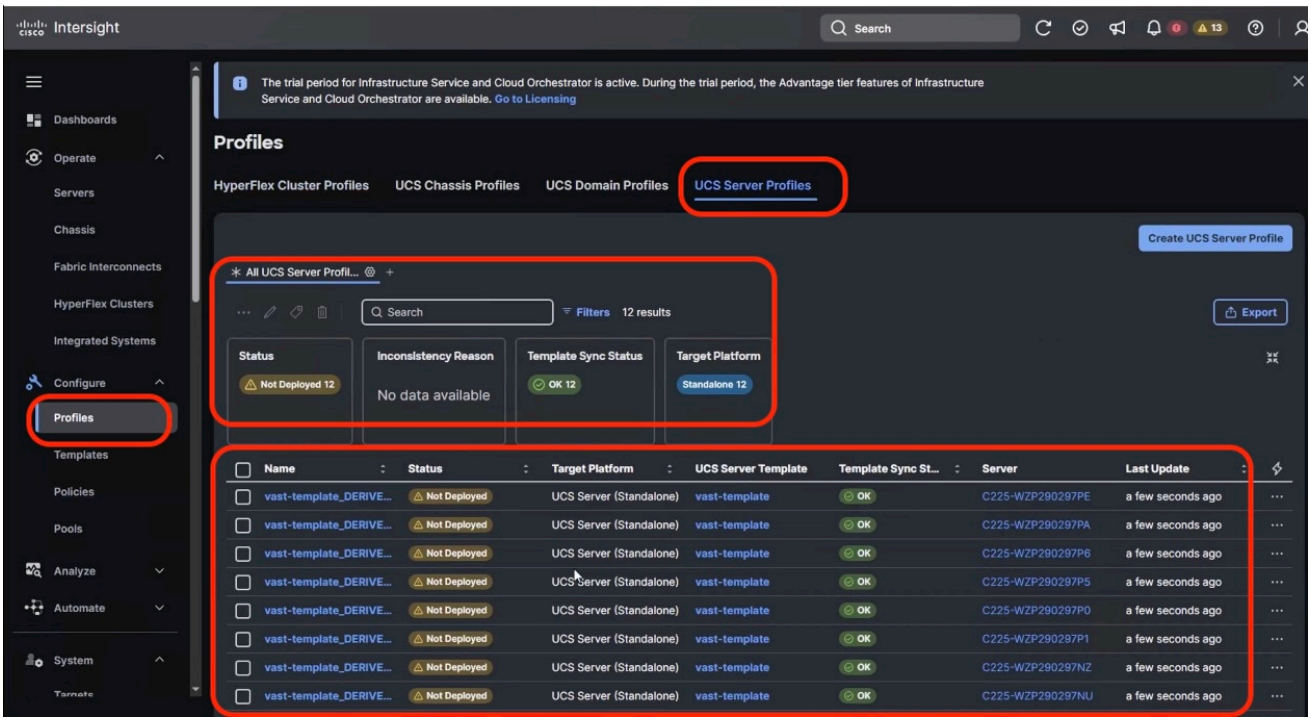
Step 4. Edit the Server Profile Name prefix and click Next



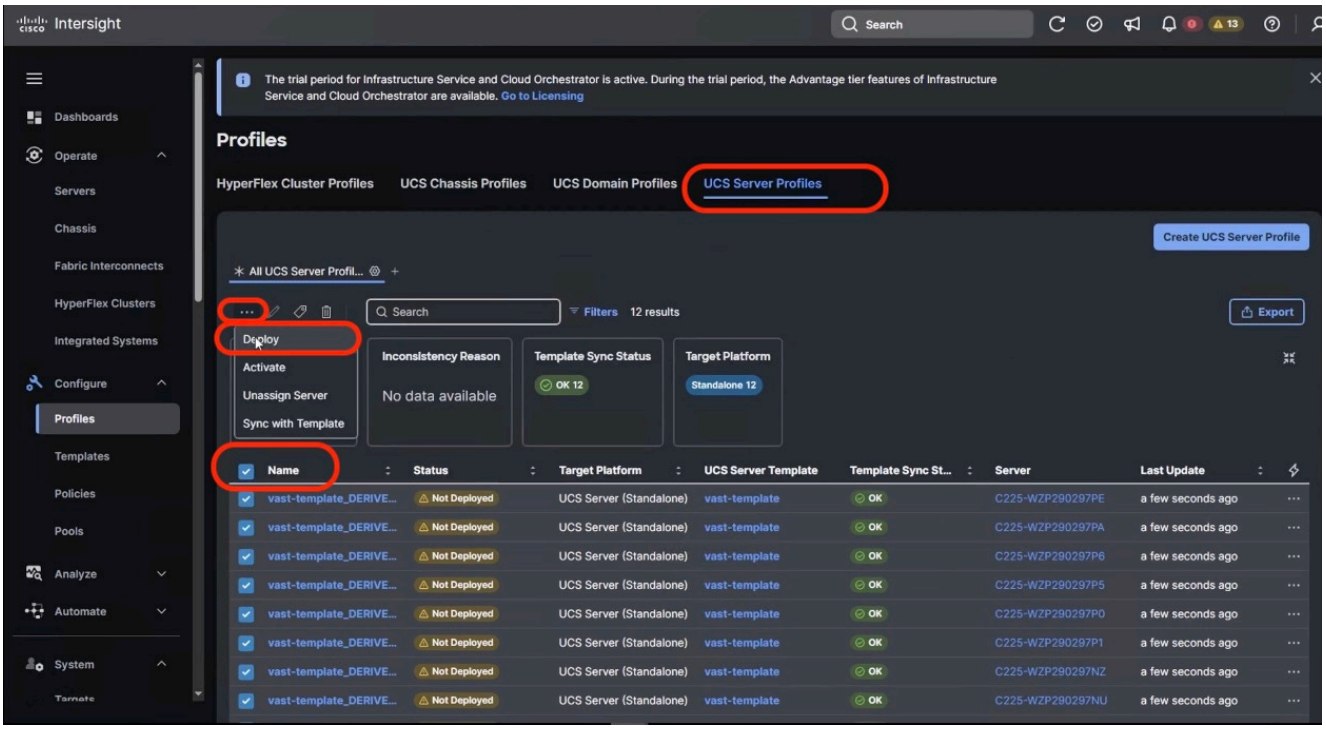
Step 5. In the summary section, ensure all the Server Policies are part of the template and click Derive



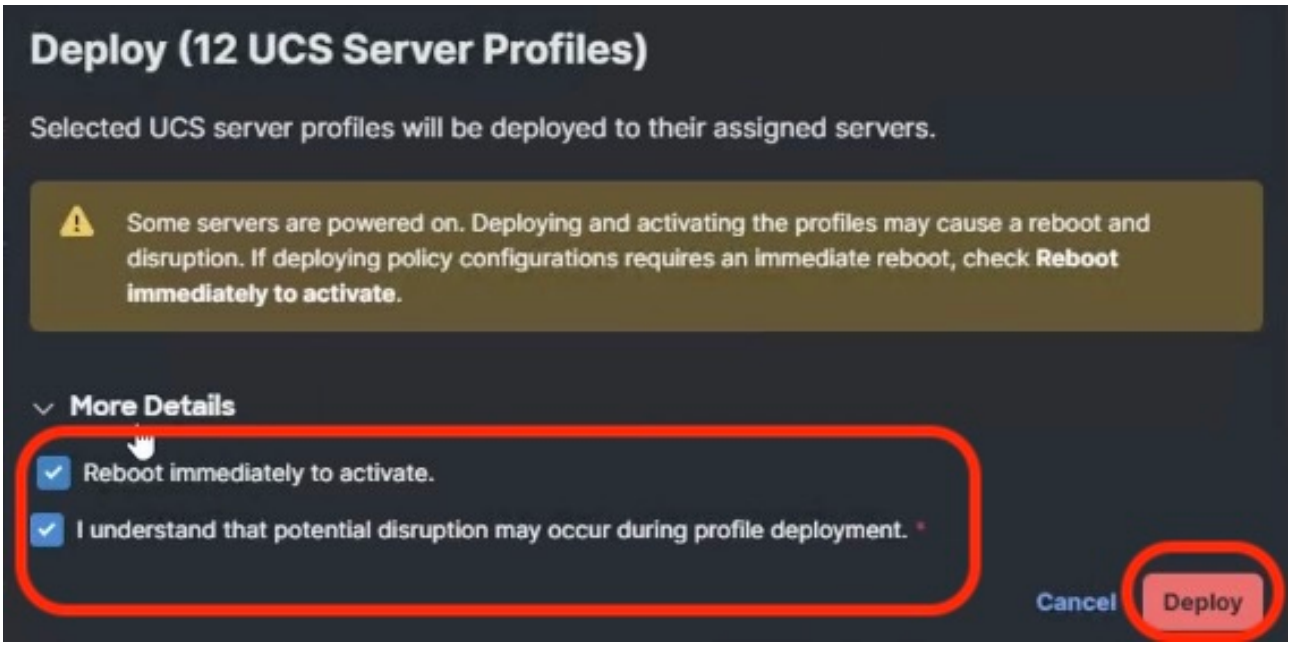
Step 6. From the left navigation pane, Navigate to Profiles → UCS Server Profiles. Ensure Profiles are attached to UCS C225 M8 server nodes and are in '**Not Deployed**' state



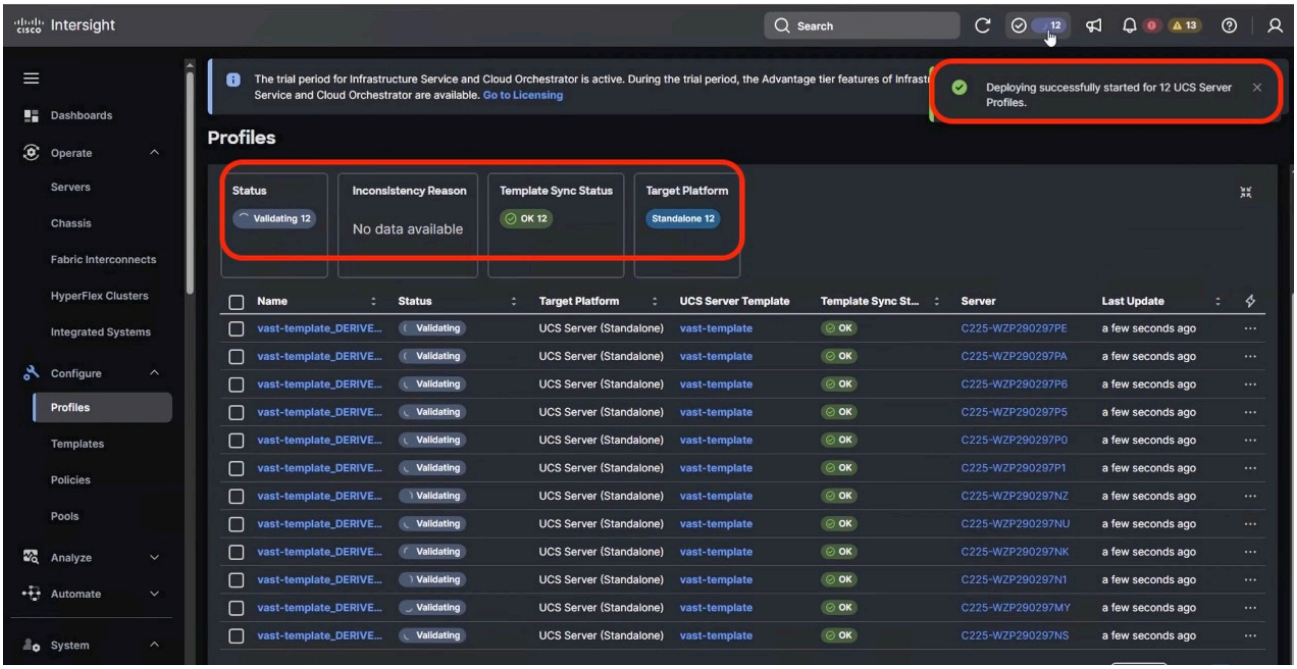
Step 7. To select all profiles , Select the Name check box, click on '…' icon and select 'Deploy'.



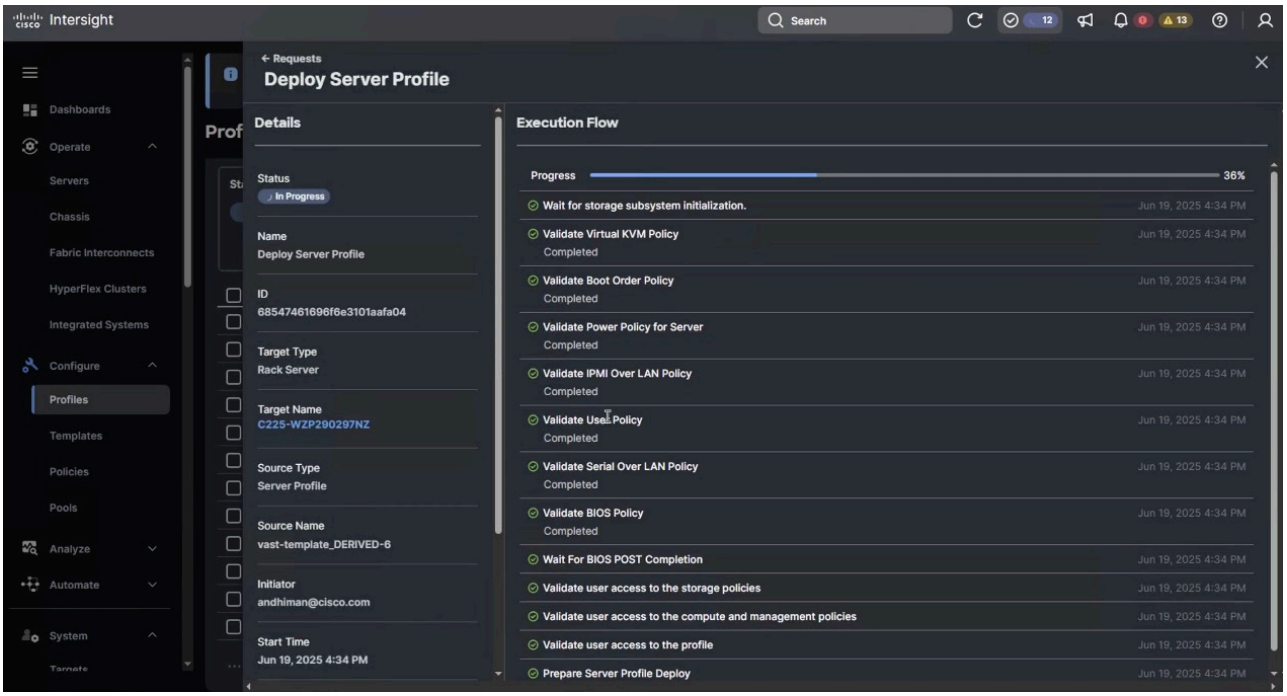
Step 8. Select the Reboot immediately and warning for potential disruption and select Deploy Click the … icon and select Derive Profiles. The Server Profiles will deploy on each of UCS C225 node with policy driven state applicable for VAST nodes on UCS C225 M8 servers.



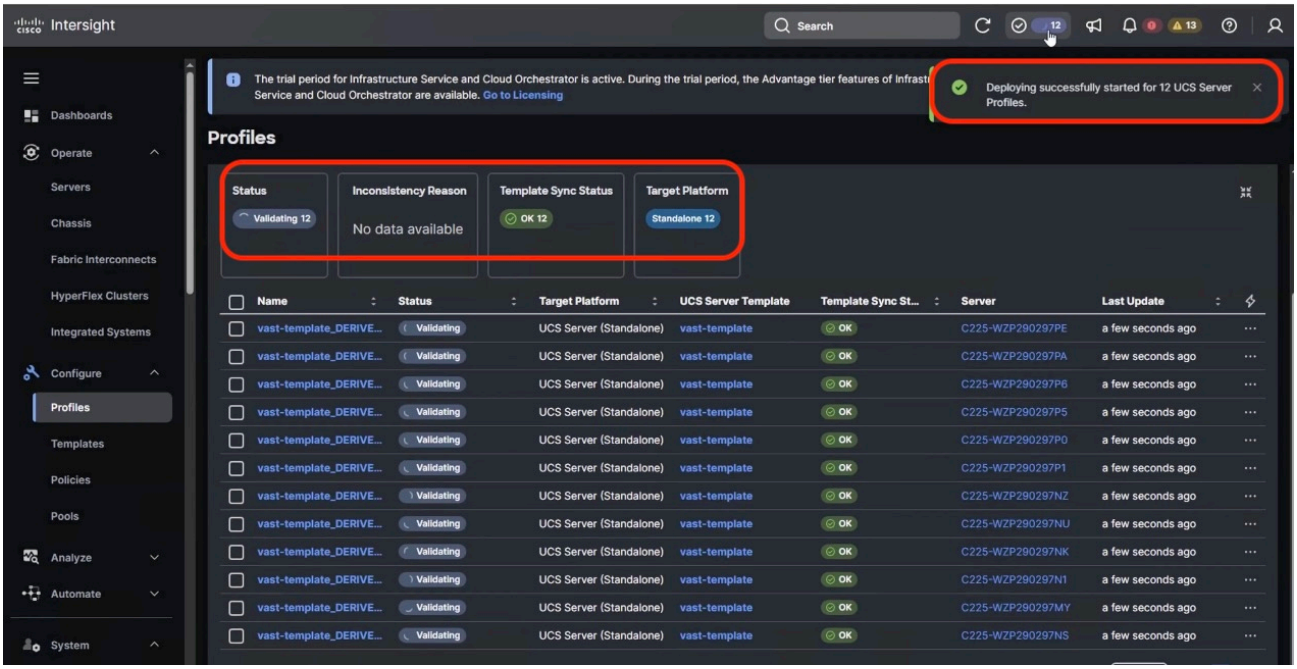
Step 9. The process would enable validation, deployment and activation of Server Profiles on each UCS C225 M8 node. Each node would be rebooted. This process may take around 15 to 20 minutes



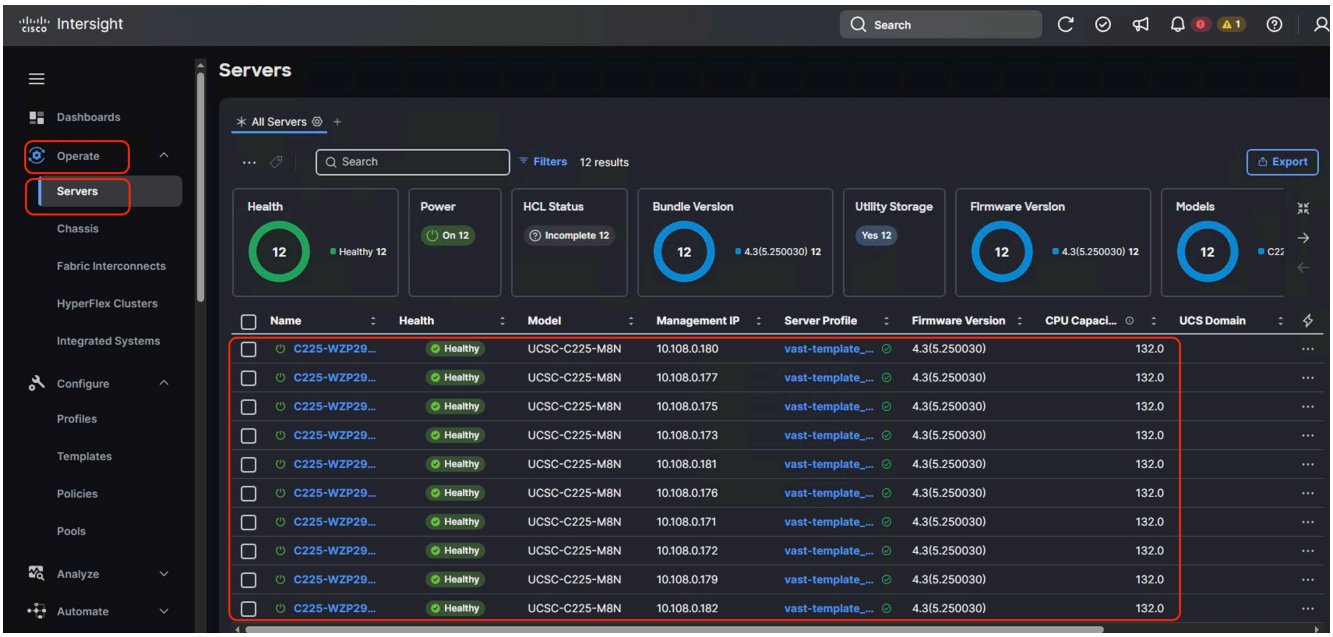
Step 10. You can also monitor the execution flow and progress of Server Profile deployment



Step 11. The process would enable validation, deployment and activation of Server Profiles on each UCS C225 M8 node. Each node would be rebooted. This process may take around 15 to 20 minutes



Step 12. Navigate to Operate → Servers and ensure Server Profile is deployed successfully



Day 0 EBOX firmware upgrade

Prior to installing VAST software, it is highly recommended to upgrade the Cisco UCS C225 M8 server firmware to the recommended Cisco UCS C-Series Firmware release.

Day 0 node firmware upgrade can be executed parallelly across all the server nodes. Intersight firmware upgrades for servers in Standalone mode or for servers deployed for VAST are streamlined through the Intersight platform. This process involves selecting the device, choosing the target firmware, and initiating the upgrade.

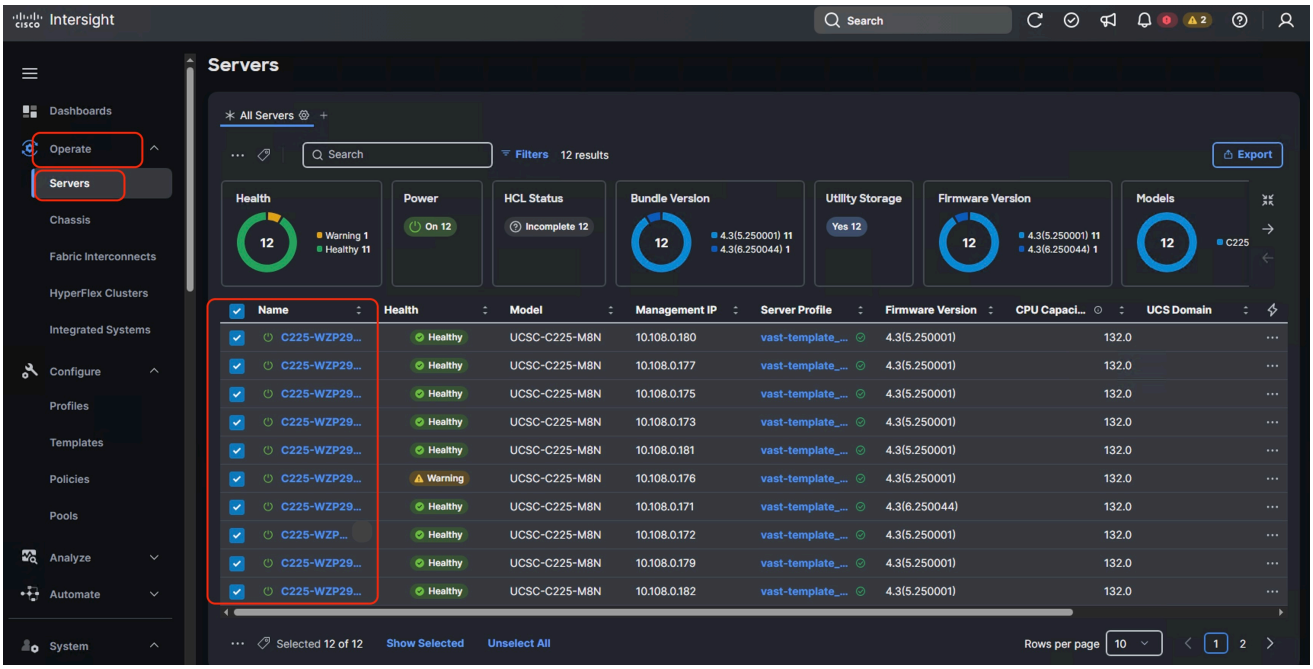
Note: This procedure should only be initiated during first time node configuration. It could be also used for cluster expansion or during replacement of cluster node

Note: User should identify the correct firmware version either through Installation team or through VAST support

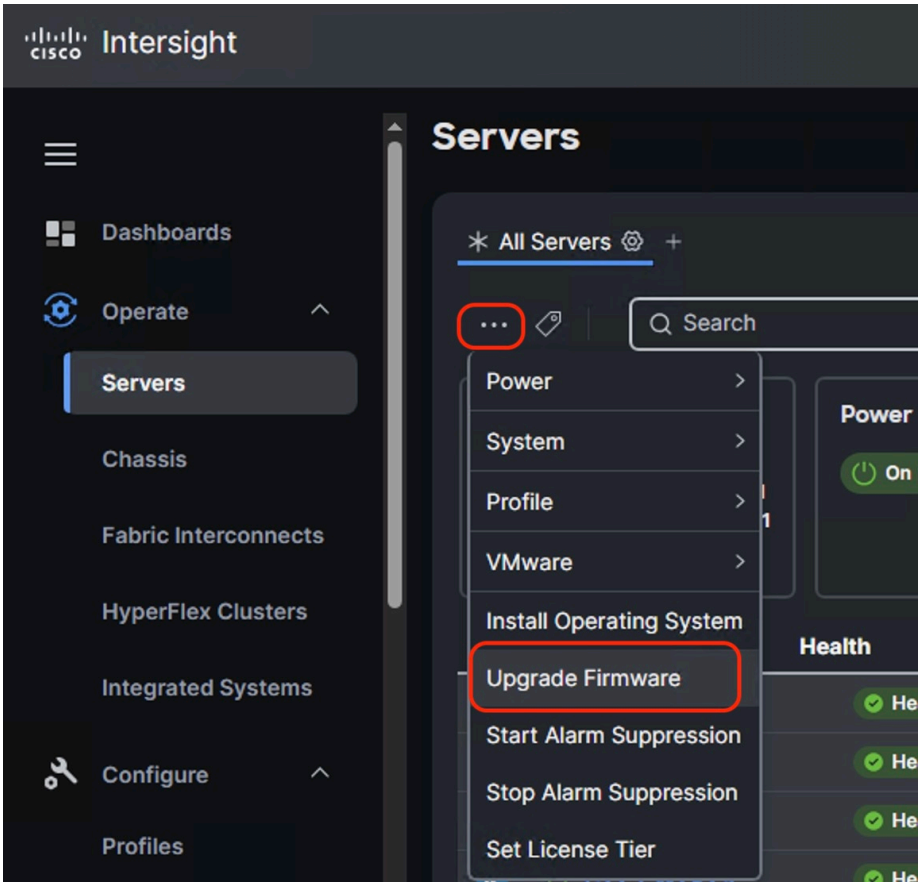
Step 1. Identify the Cisco C225 M8 firmware validated for VAST. At the time of writing this install guide the validated firmware Version was **4.3(5.250030)**

Step 2. From the left navigation pane, navigate to Operate → Servers. Select the servers which are either part of new cluster or which are being added to an existing cluster.

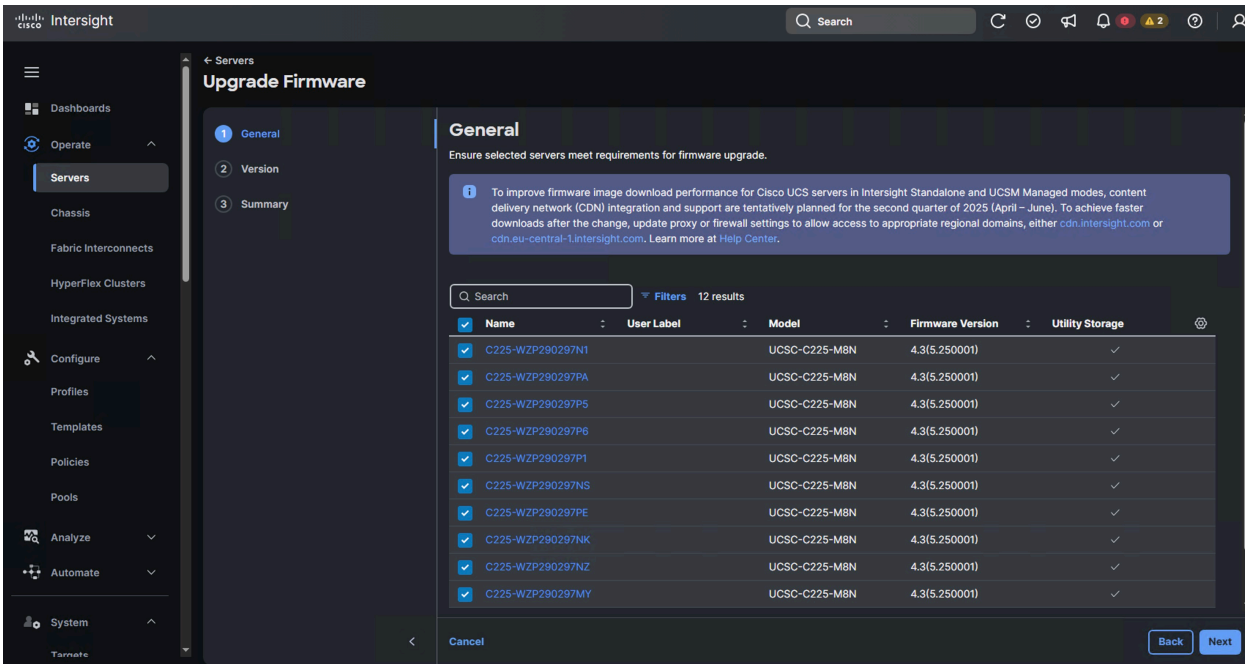
Step 3. Select the Servers check box



Step 4. click on '…' icon and select 'Upgrade Firmware' option.

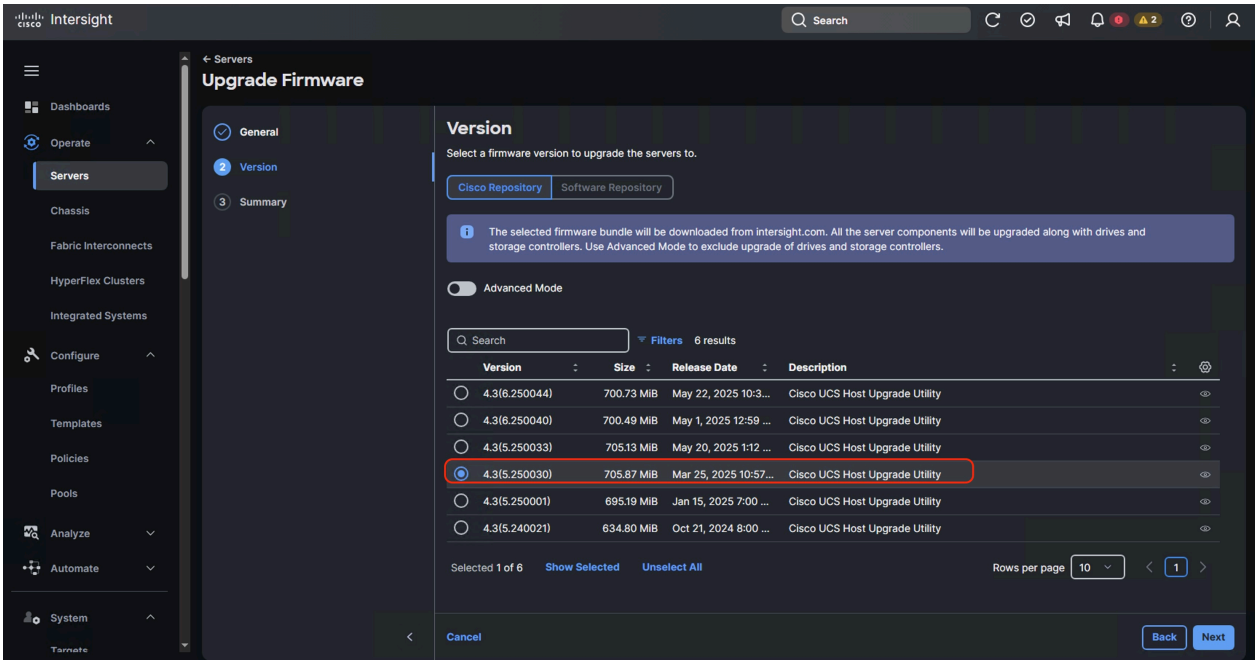


Step 5. Select start and click Next, In the General options, ensure UCS C225 M8 nodes are selected

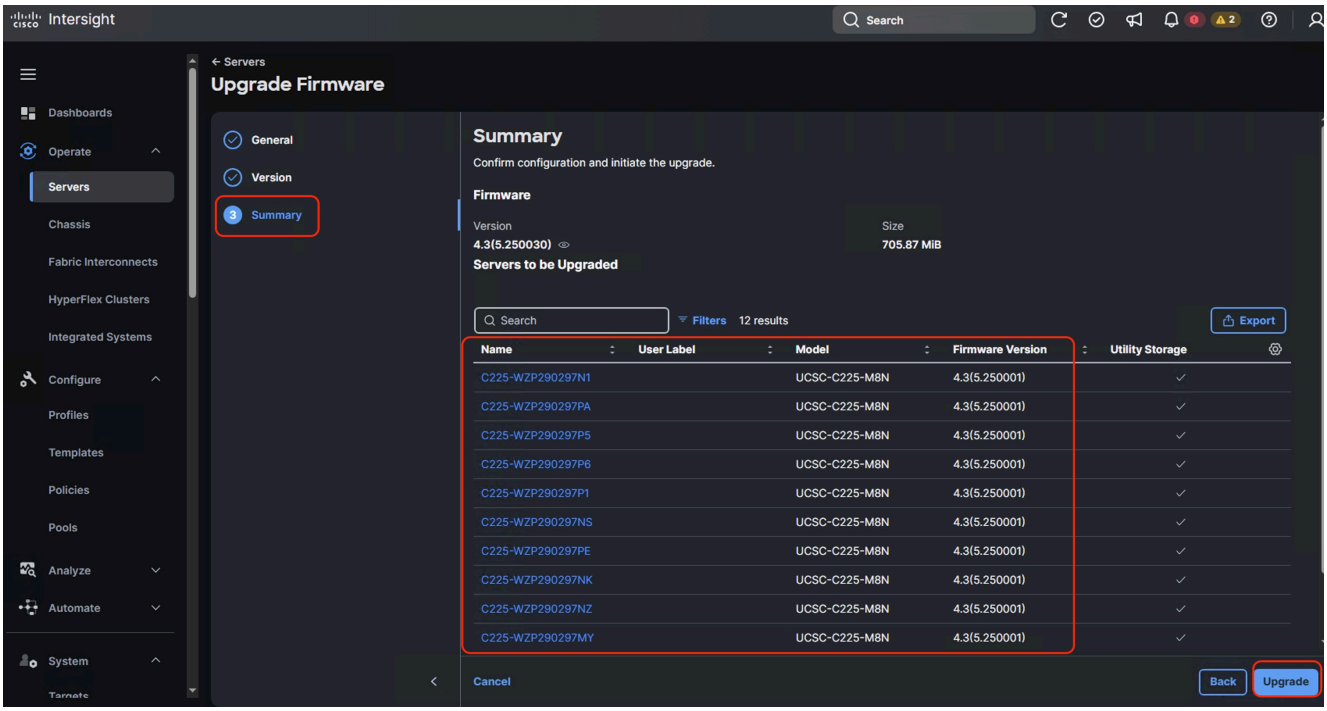


Step 6. Select the firmware version for the group of UCS C225 M8 nodes.

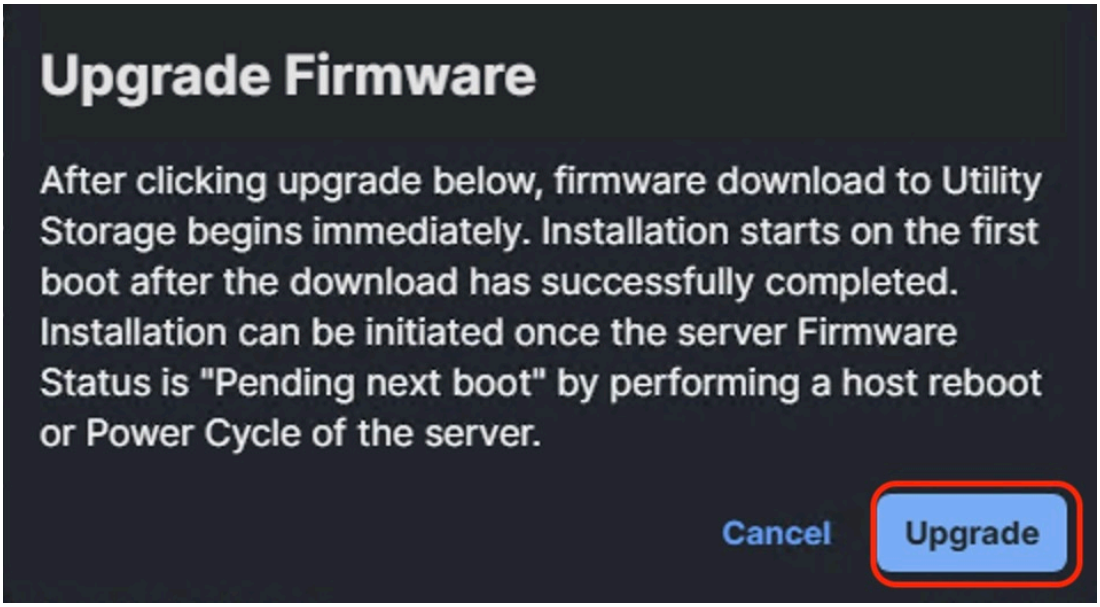
Note: By default, the storage controller and drive firmware is upgraded The Advanced Mode enabled users to de-select firmware upgrade for storage controller and drive firmware



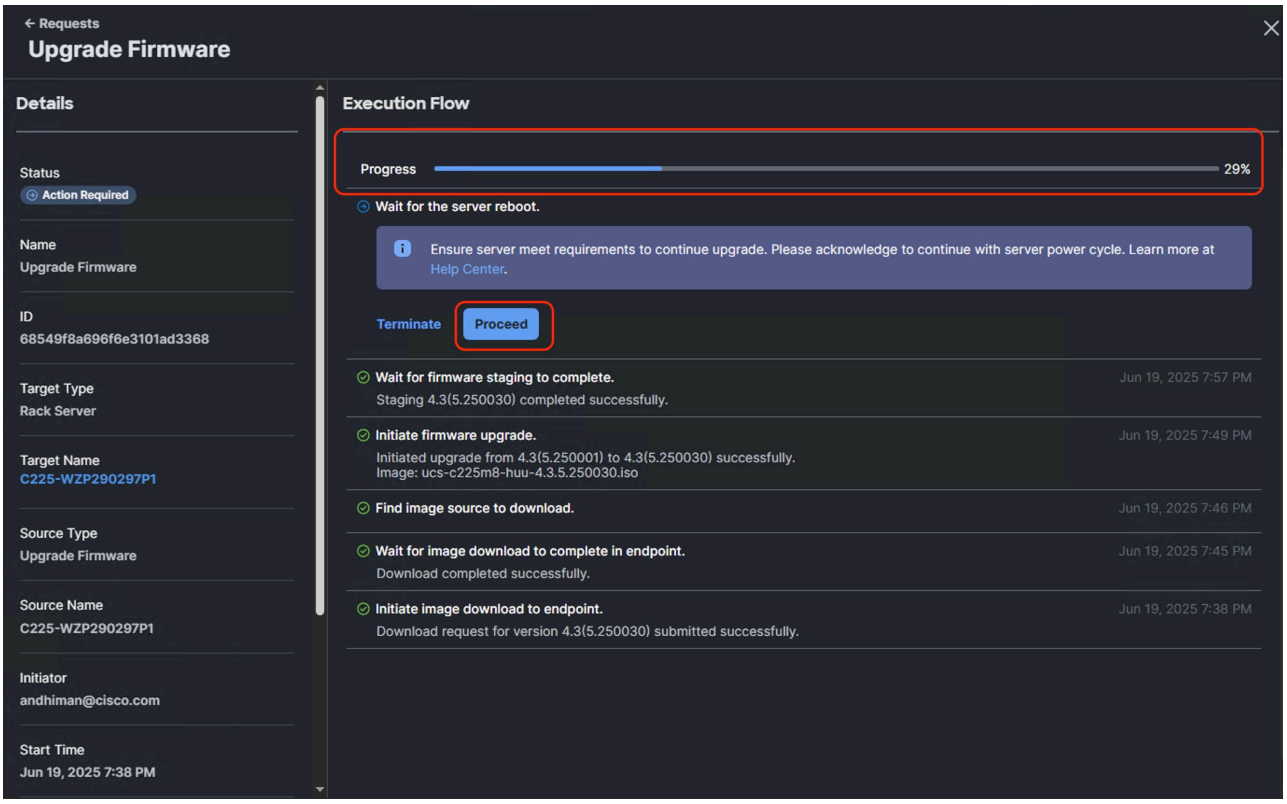
Step 7. Verify the Firmware upgrade summary. The selected firmware will be downloaded on local utility storage of each of the server end points. Once the download complete the firmware upgrade workflow will be executed. Click upgrade



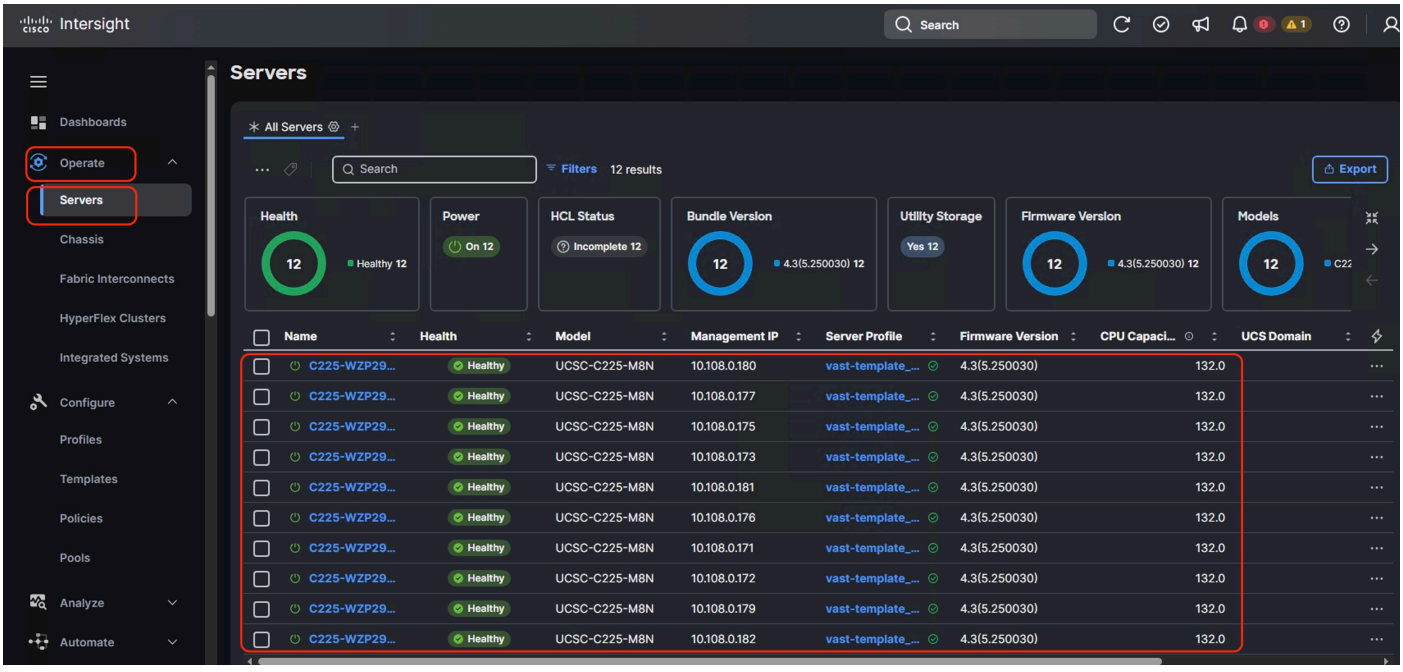
Step 8. On the Upgrade Firmware popup , confirm firmware upgrade



Step 9. Once the firmware is downloaded and staged locally to utility storage of each server end point. Acknowledge server reboot and wait for Server Firmware to upgrade successfully .



Step 10. Verify successful Server Firmware upgrade to 4.2(5.250030) across all the nodes



Note: User should identify the correct firmware version either through Installation team or through VAST support

VAST OS Installation

The base OS installation before VAST cluster bootstrap process can be executed through three different ways

1. OS installation through Cisco Intersight
2. OS installation through KVM
3. OS installation through USB drive

This document illustrates step-by-step procedure to install base OS through Cisco Intersight and KVM. Both the procedures require a local copy of VAST operating System

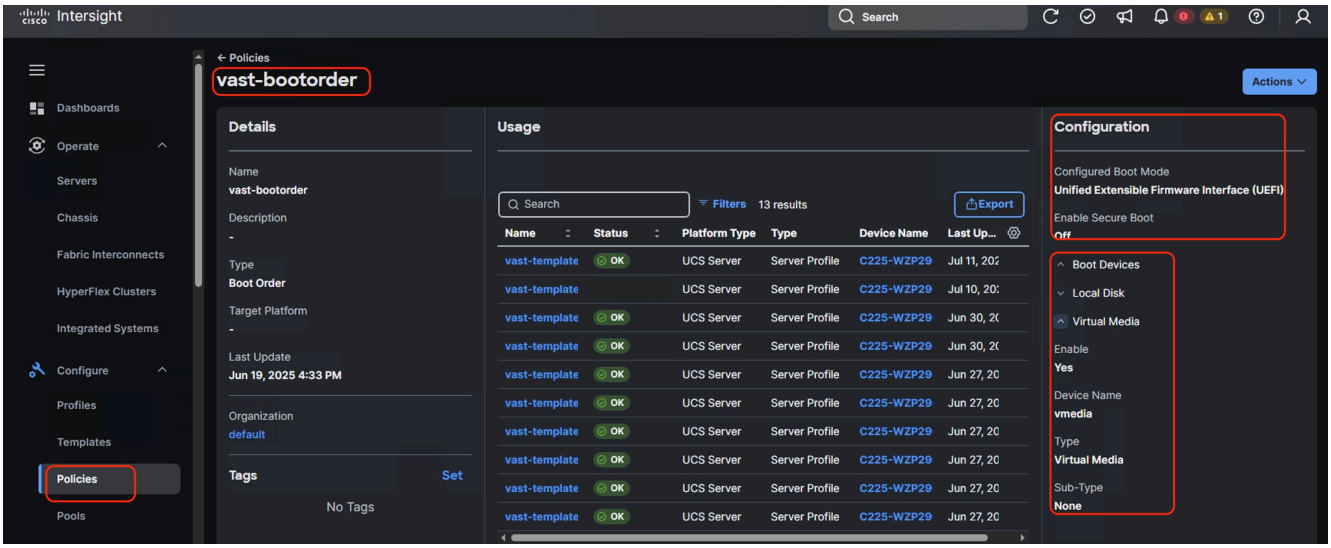
Note: Please identify the correct base operating system version to be installed on UCS C225 M8 servers for VAST. At the time of creating this install guide , the available VAST OS version was vast-os-12.14.17-1818066.

Note: This procedure can be executed either only on UCS C225 M8 nodes during new VAST cluster setup or for additional nodes for expansion of an existing cluster.

Procedure 1. Install VAST OS through Cisco Intersight OS Installation feature

This procedure expands on the process to install the VAST operating system through the Cisco Intersight OS installation feature.

Note: Before proceeding to installing VAST OS through Intersight Install feature, please ensure virtual media (vmedia) has the lowest priority in the Boot Order policy. This is displayed in screenshot below:



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

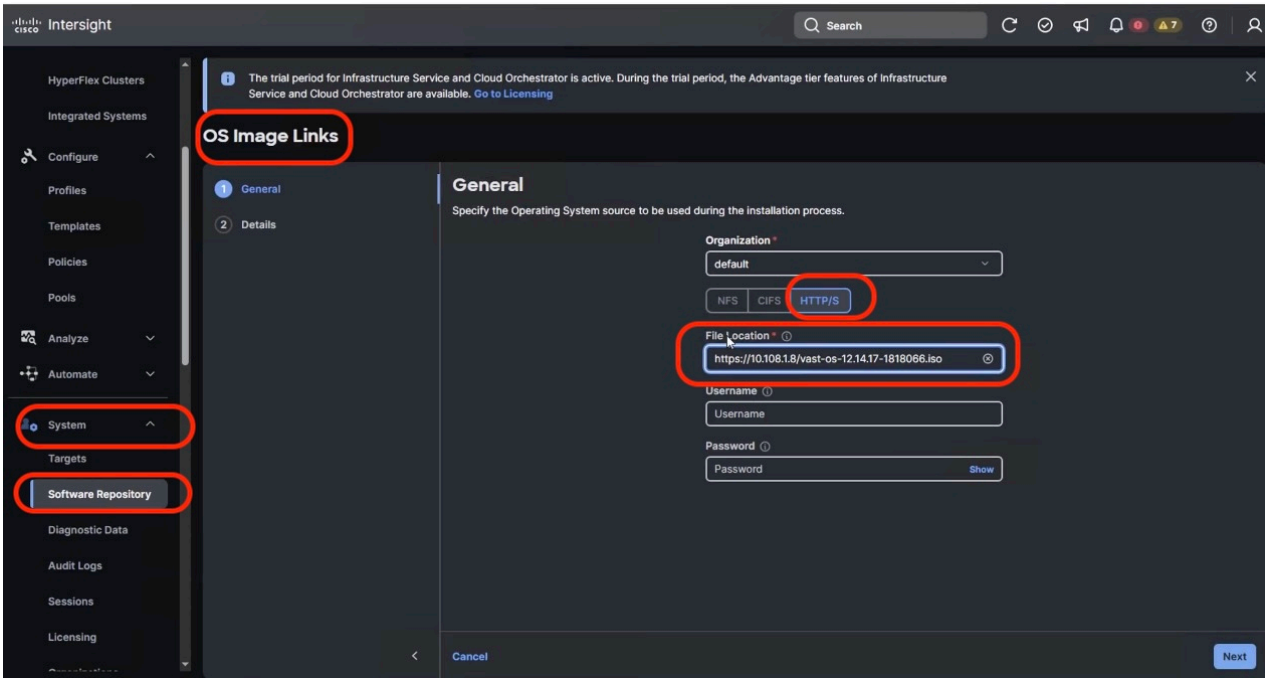
Note: Make sure the VAST operating system ISO is available from a local repository, for example an HTTPS/NFS/CIFS server. This is a one-time process for each version of the VAST OS ISO.

Step 1. Login to Cisco Intersight and click System.

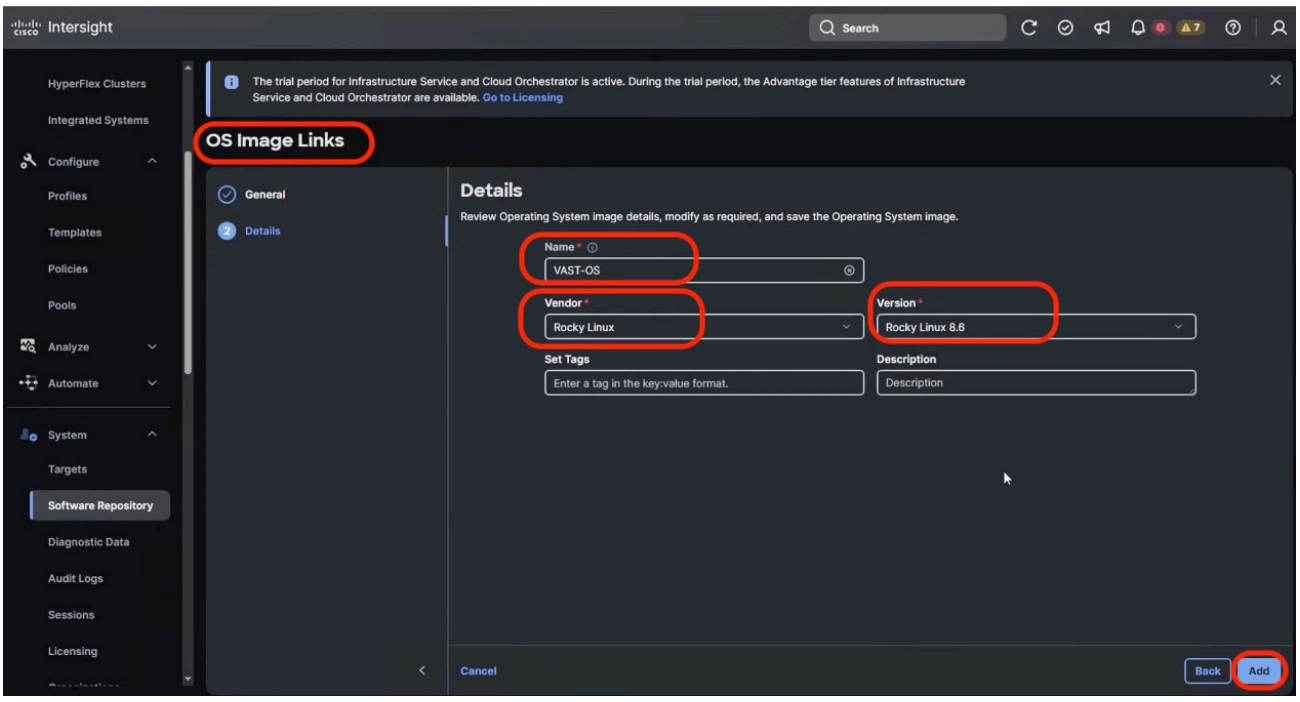
Step 2. Click Software Repository and click the OS Image Links tab.

Step 3. Click Add OS Image Link.

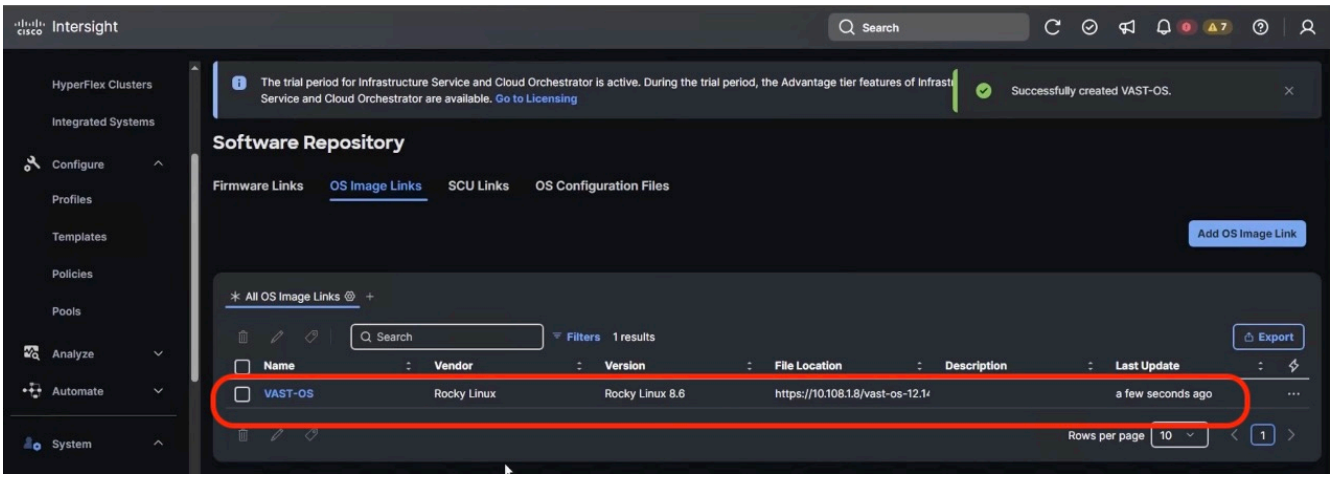
Step 4. Add the location of VAST operating system ISO (NFS/CIFS or HTTPS server) and click Next.



Step 5. Enter a name for the Repository, for the Vendor enter Rocky Linux, and for the Version enter Rocky Linux 8.6. Click Add.

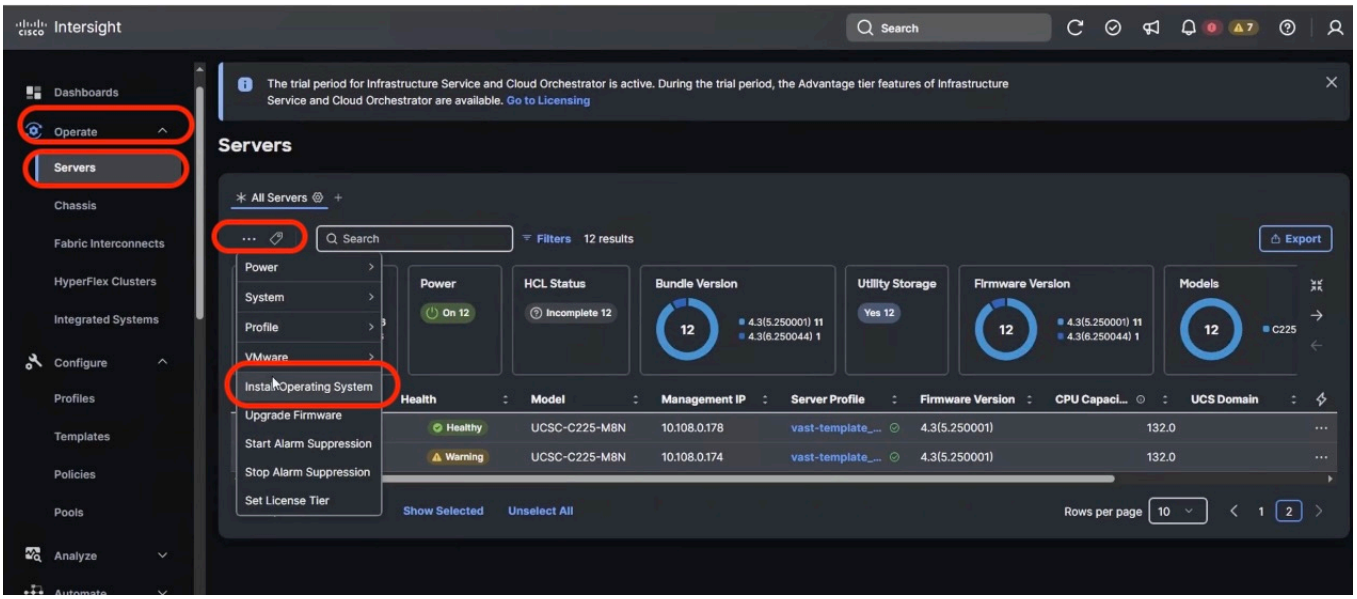


Step 6. Verify that the OS Repository is successfully created in Cisco Intersight.

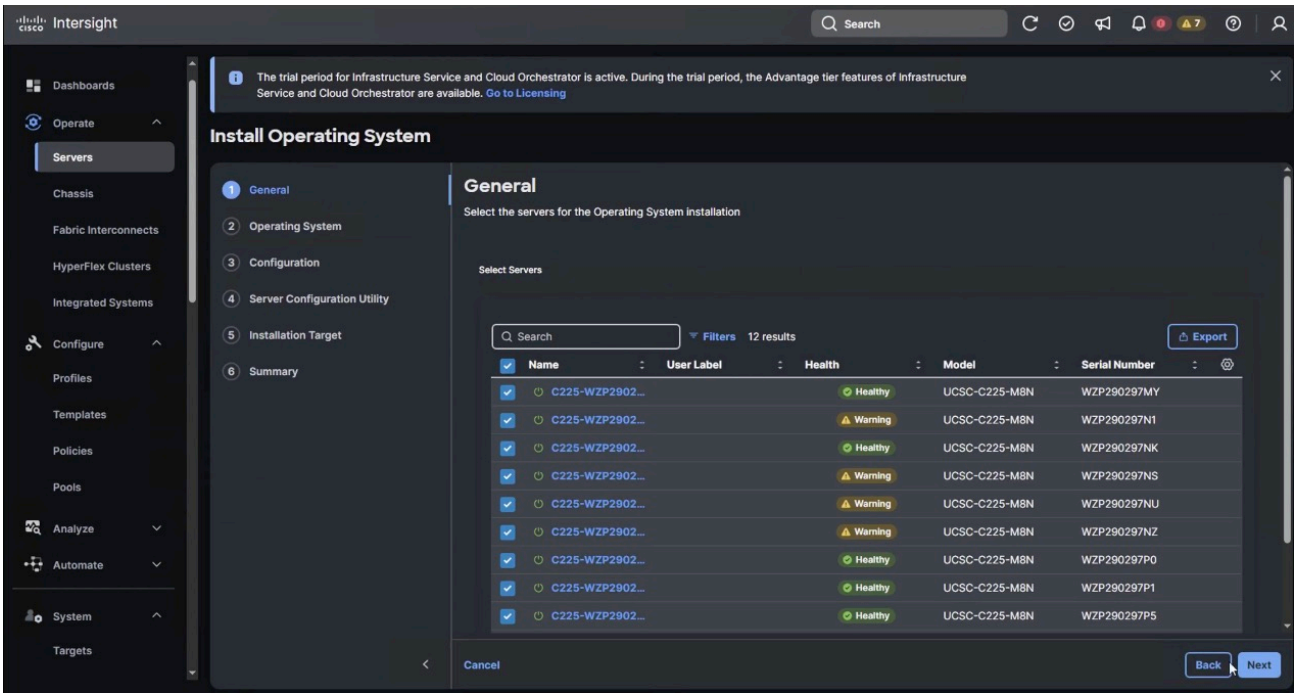


Step 7. From the left navigation pane, click on Operate→Servers, and select the Cisco UCS C-Series nodes ready for the OS deployment.

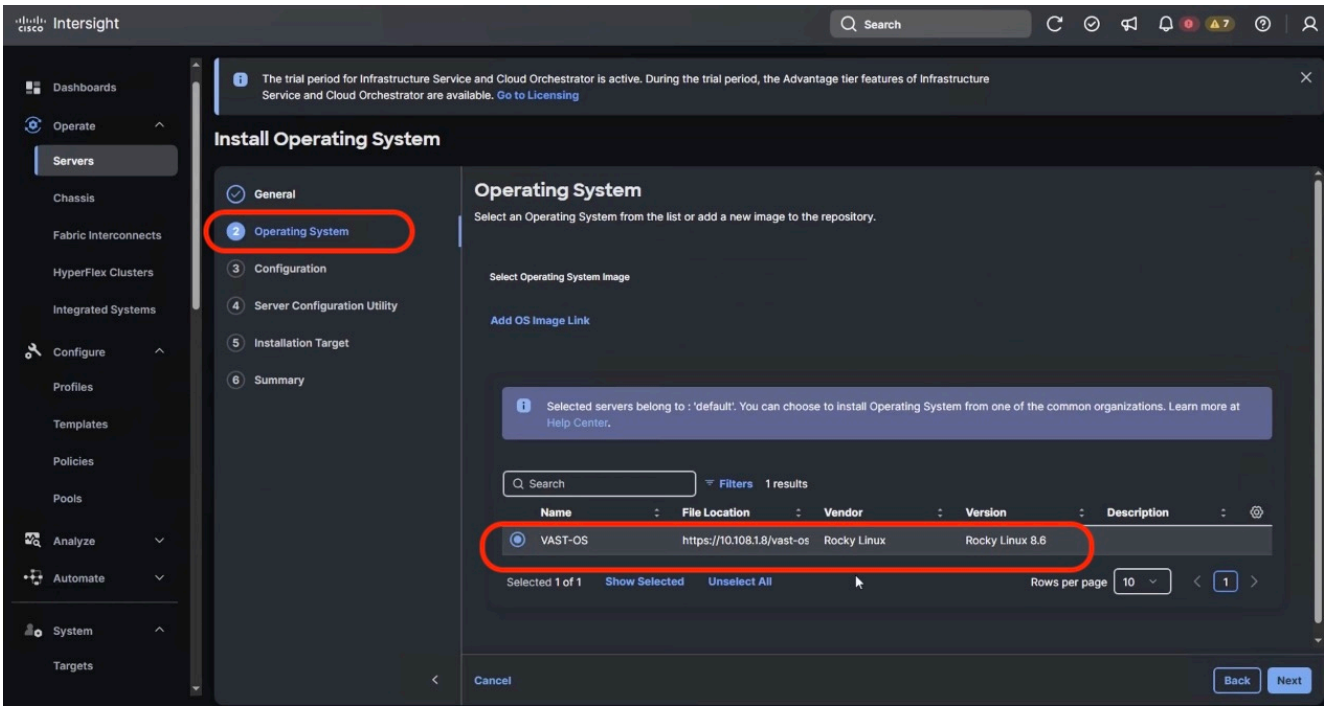
Step 8. Click the … and select Install Operating System.



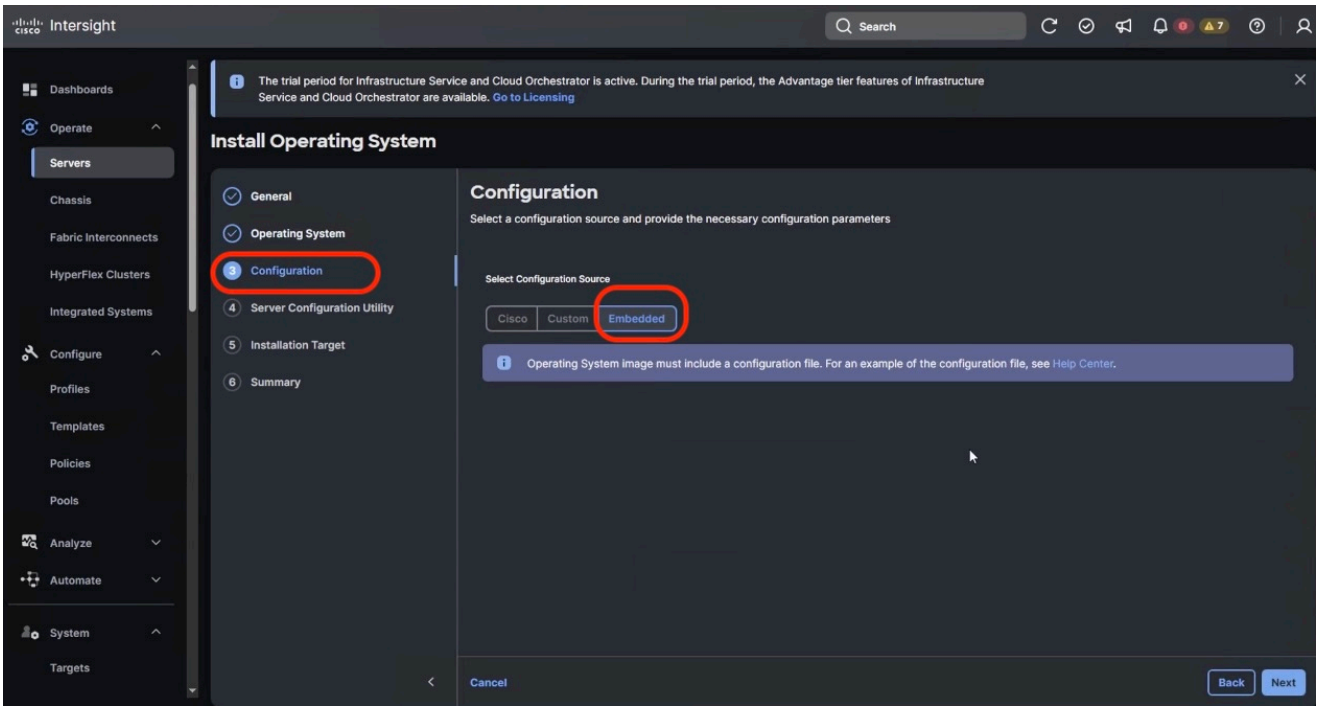
Step 9. Make sure the servers are already selected and click Next.



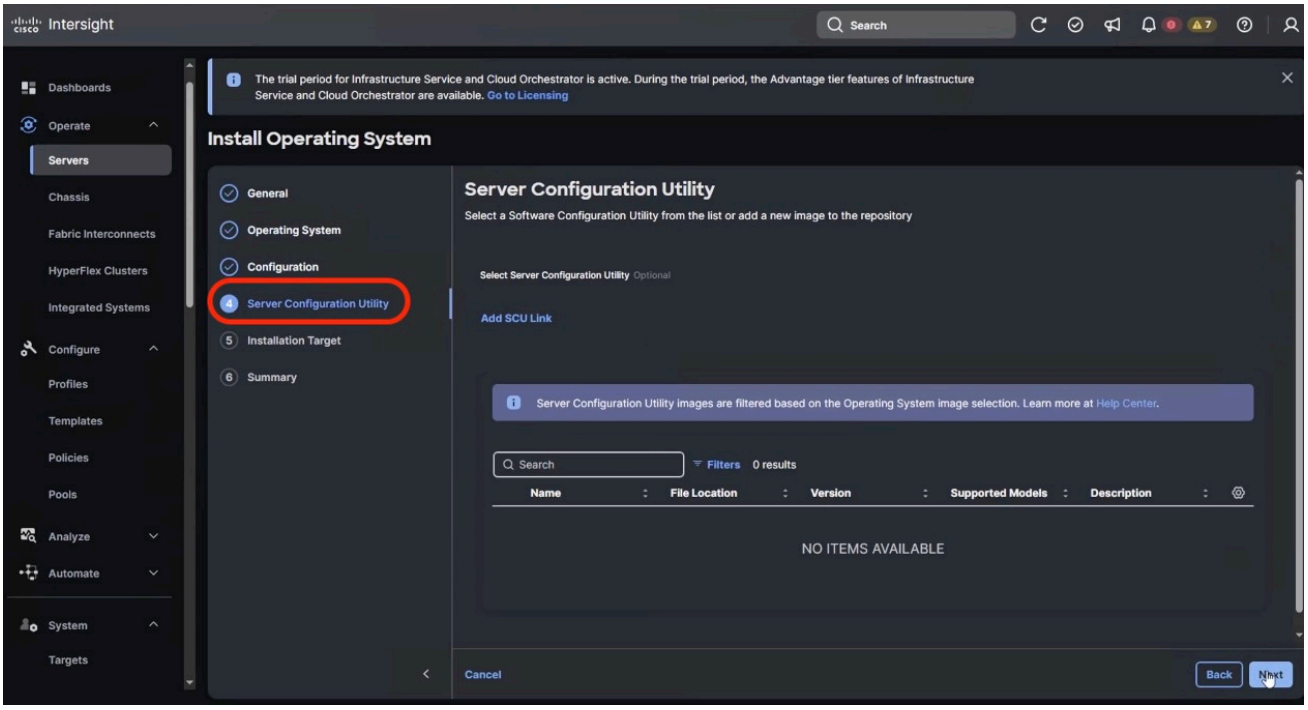
Step 10. Select the Operating System repository which was previously created with the VAST operating system ISO and click Next.



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

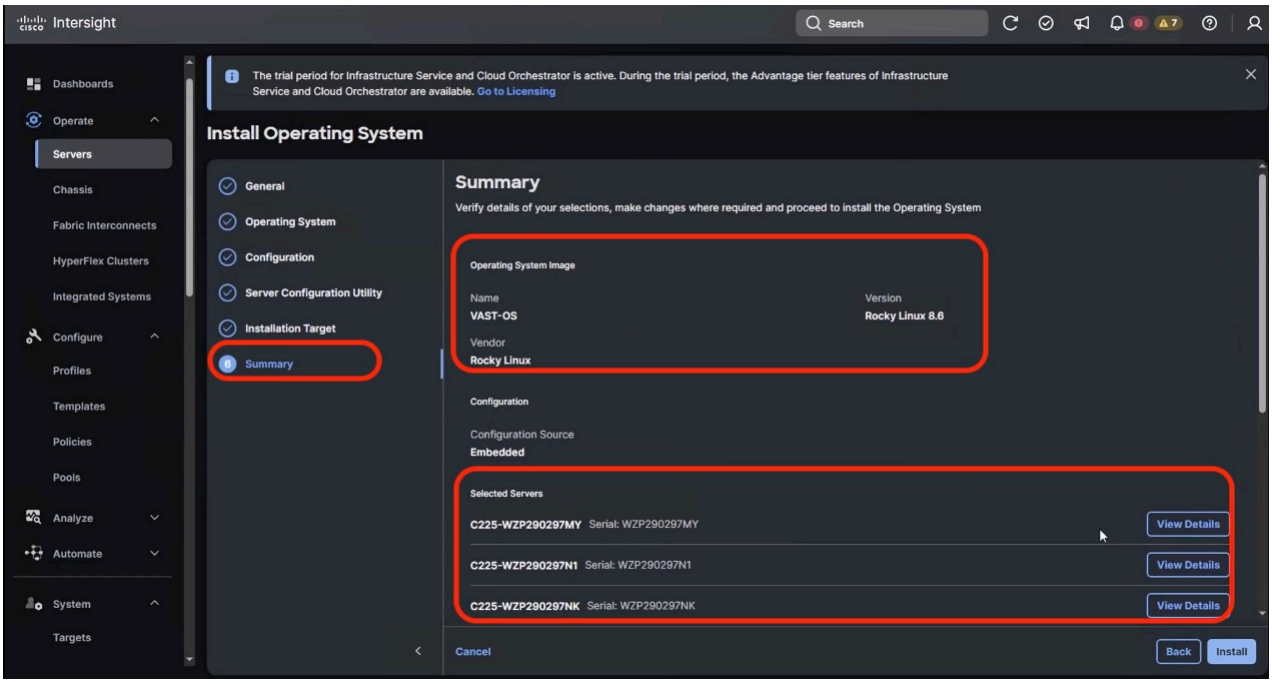


Step 12. Click Next. No SCU Link is required.

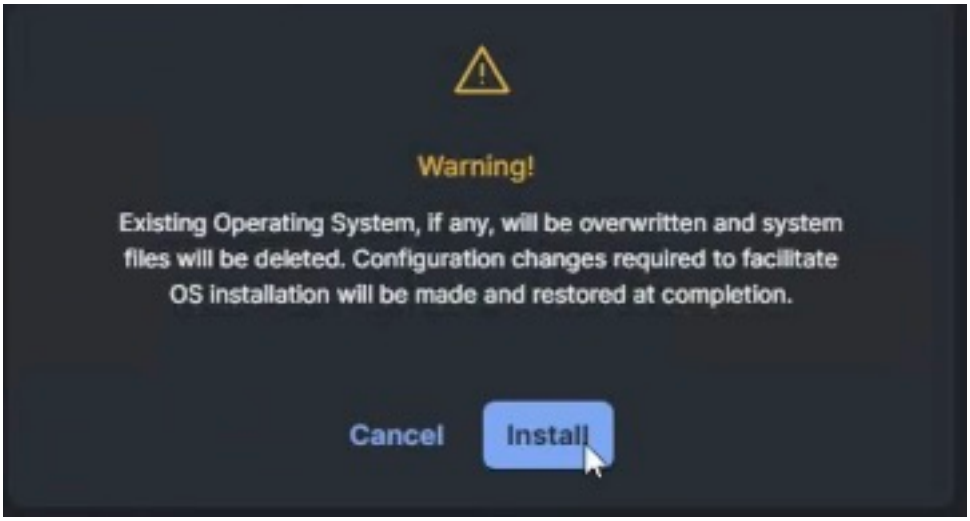


Step 13. Click Next. In the Installation target screen. VAST ISO automatically identifies the Installation target as the RAID1 virtual drive on 2x M.2 internal drives configured in the Boot Order Server Policy.

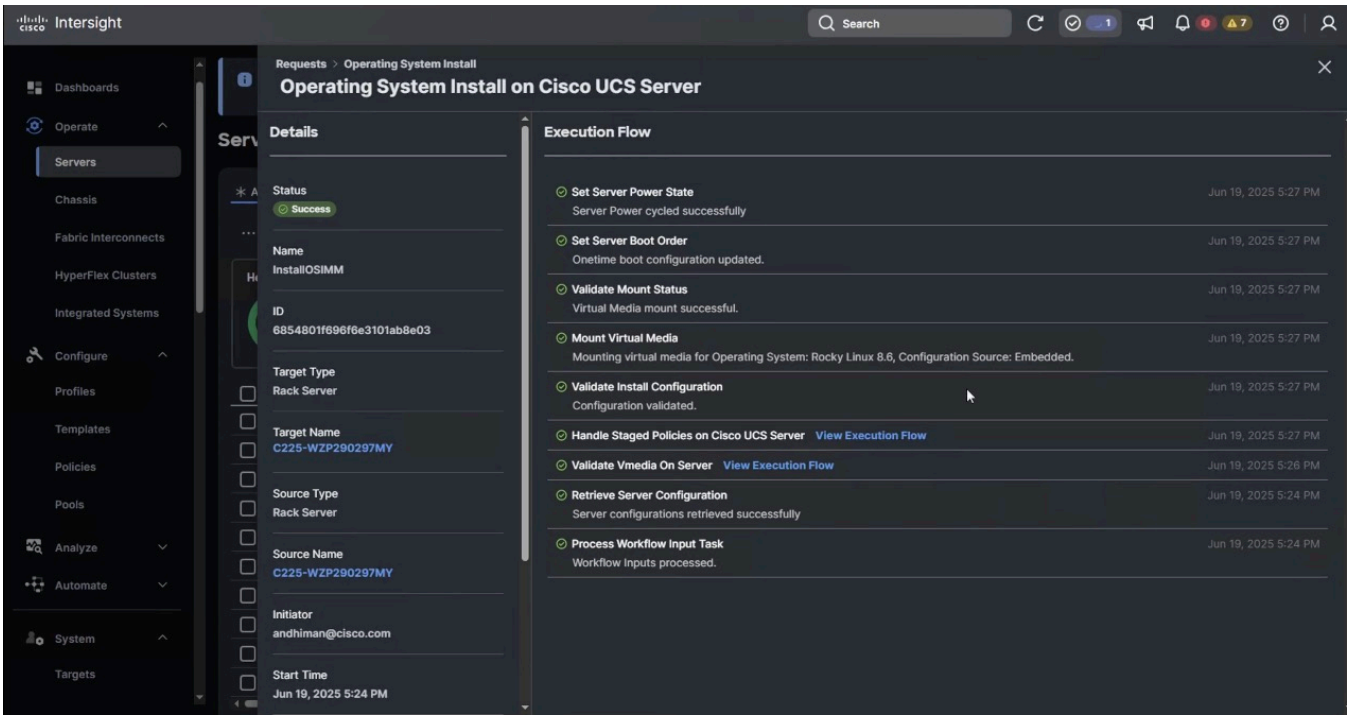
Step 14. Verify the summary and click Install.



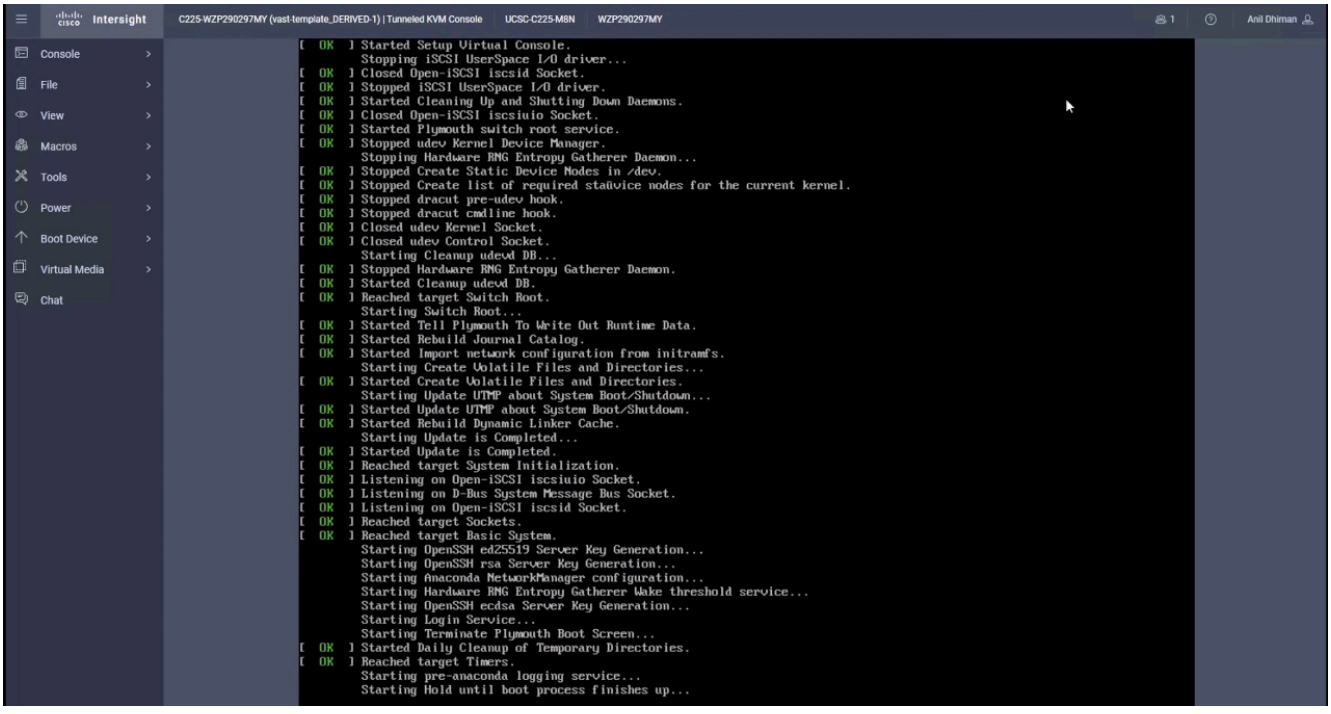
Step 15. Accept the warning for overwriting the existing OS image on the node and click Install.



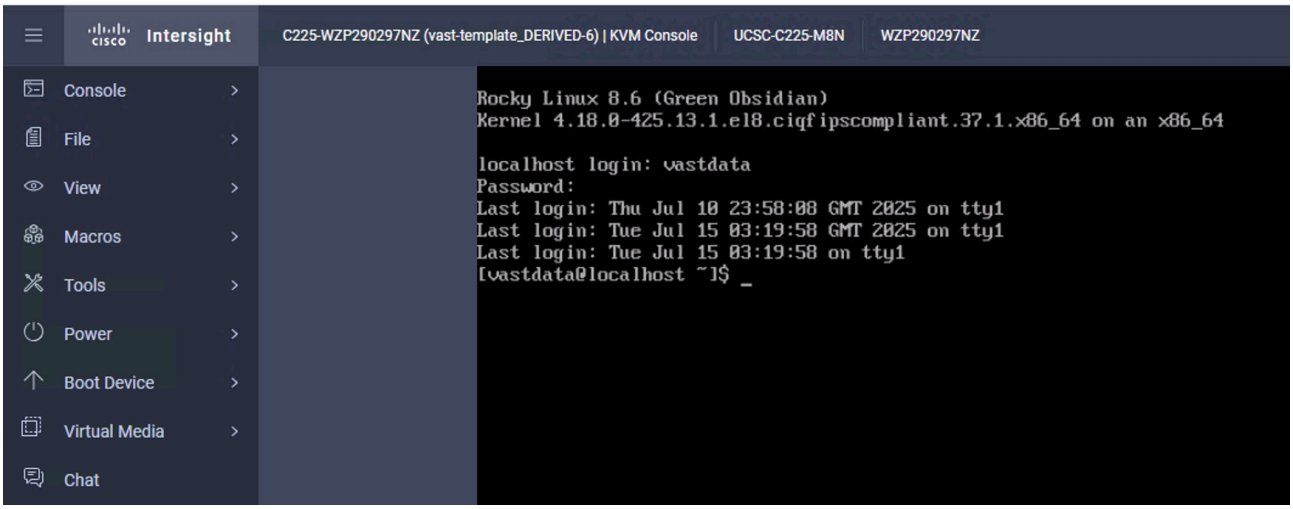
Step 16. Monitor the OS installation progress and wait for completion. Depending on the network bandwidth between the node management network and the repository network, it can take up to 20 to 30 minutes for the OS installation to complete.



Step 17. Since this is an embedded installation without the Cisco Server Configuration utility, Cisco Intersight displays the OS installation completion in about five minutes. Open a virtual KVM session and monitor the OS install progress. Since this is an automated install, you are not required to provide any inputs on the virtual KVM screen. The OS installation progress is shown below:



Step 18. Ensure OS is successfully installed on Cisco UCS C-Series nodes. Login with vastdata/vastdata to verify successful OS installation

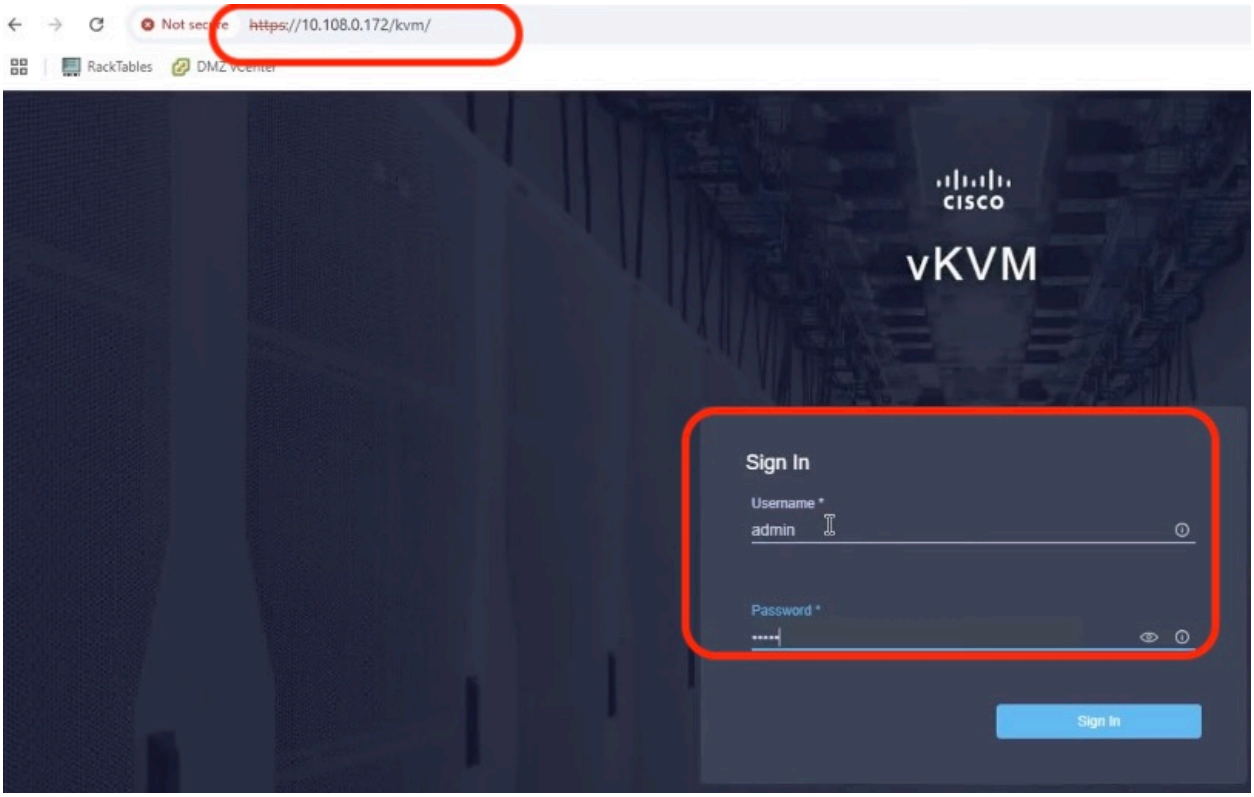


Procedure 2. Install the VAST OS through virtual media

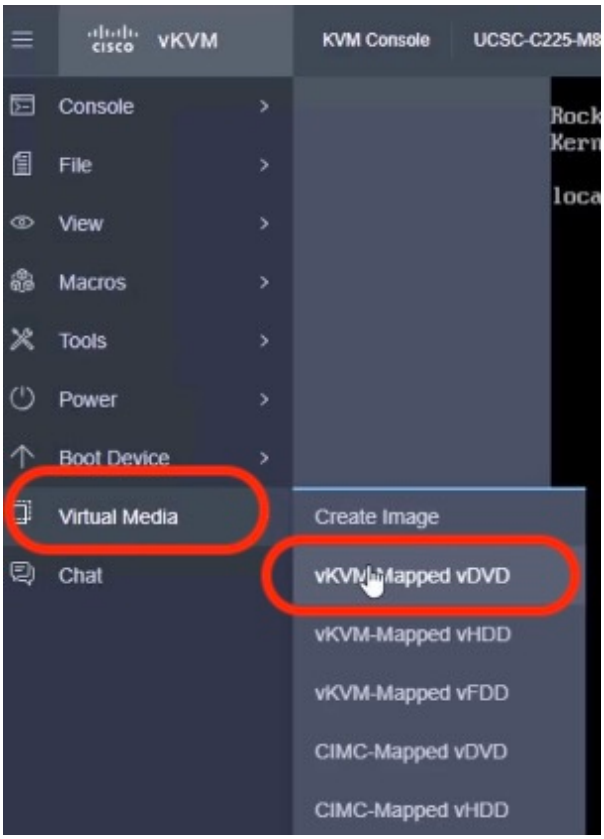
This procedure expands on the process to install the operating system through virtual media. You need to open a virtual KVM session for each node. Virtual KVM session can be accessed through Cisco Intersight or logging into node CIMC IP. During the OS installation, it is recommended to open vKVM through node CIMC IP. Access the vKVM through the user created in Local User policy (admin/<<password>>)

Step 1. Login to Intersight, Navigate to Infrastructure Service → Operate → Servers and identify the node management IP

Step 2. Login to vKVM with the username/password as defined in the user access policy. (https://CIMC-IP/kvm

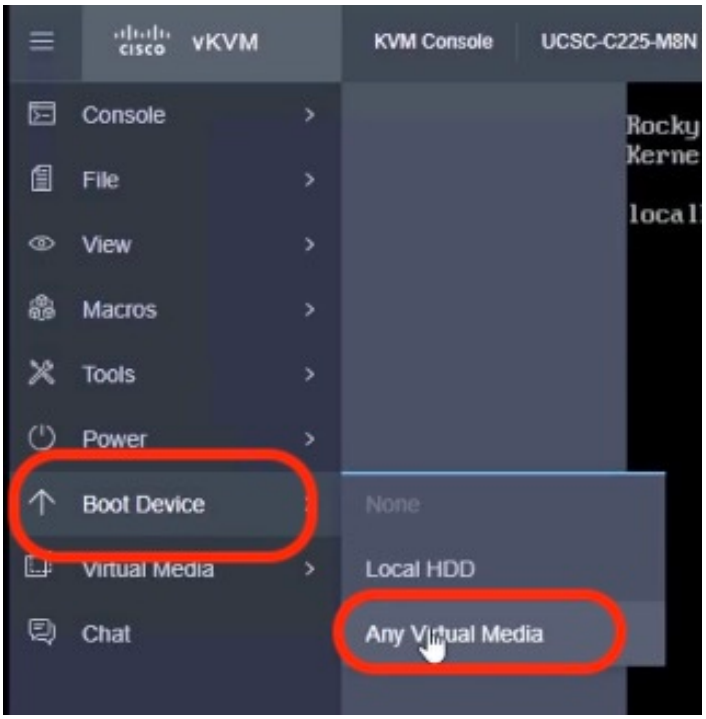


Step 3. On KVM screen, navigate to Virtual Media → vKVM Mapped vDVD

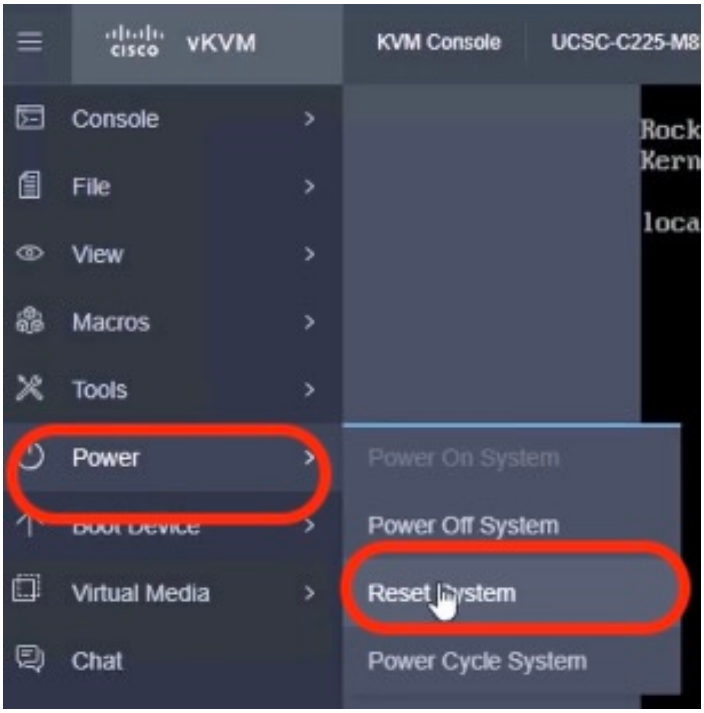


Step 4. Select the VAST operating system ISO from your local file system and click Map Drive.

Step 5. Modify the Boot Device to Any Virtual Media , this will implement a one time boot through virtual media and override the default Boot Order Policy. Selected one time boto media avoids manually selecting virtual media mapped ISO on node bootloader prompt



Step 6. Click Power and then click Reset System to reset the power cycle on the node. The ISO automatically loads (with virtual Media having highest priority in Boot Order Server Policy).



Step 7. The ISO automatically identifies the drives to install the VAST operating system ISO; the OS installation completes in about 15 to 20 minutes.

Step 8. Repeat this procedure for all the other UCS C225 M8 nodes to be configured for the VAST cluster.

Appendix

This appendix is organized into the following sections:

Appendix A – Bill of Materials

Table below, provides an example the Bill of Materials used for twelve (12) EBOX VAST cluster

Table 7. EBOX (12 nodes) on Cisco UCS BC225M8 Bill of Materials

Line Number	Part Number	Description	Qty
1.0	**VAST-DATA-MLB**	VAST Software and Hardware MLB	1
1.1	DC-MGT-SAAS	Cisco Intersight SaaS	1
1.1.1	SAAS-AI	Artificial Intelligence Use Case	1
1.1.2	DC-MGT-IS-SAAS-AD	Infrastructure Services SaaS/CVA - Advantage	12
1.1.3	SVS-DCM-SUPT-BAS	Basic Support for DCM	1
1.1.4	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License	12
1.1.5	DC-MGT-ADOPT-BAS	Intersight - 3 virtual adopt session http://cs.co/requestCSS	1
1.2	UCSC-C225M8N-EBOX	UCS C225 M8 1U Rack Server for VAST with 15.3 TB Drives	12
1.2.0.1	CON-L1NCO-UCSC2M8X	CX LEVEL 1 8X7XNCDOS UCS C225 M8 1U Rack Server for VAST wit	12
1.2.1	ISM-MANAGED	Deployment mode for C Series Servers in Standalone mode	12
1.2.2	UCS-CPU-A9454P	AMD 9454P 2.75GHz 290W 48C/256MB Cache DDR5 4800MT/s	12
1.2.3	UCS-MRX32G1RE3	32GB DDR5-5600 RDIMM 1Rx4 (16Gb)	144
1.2.4	UCSC-RIS1C-225M8	C225 M8 1U Riser 1C PCIe Gen5 x16 FH	12
1.2.5	UCSC-RIS3C-225M8	C225 M81U Riser 3C PCIe Gen5 x16 FH	12
1.2.6	UCSC-O-ID10GC-D	Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC	12
1.2.7	UCS-NVB15T3O1L	15.3TB 2.5in U.2 15mm SolidigmP5316 HgPerf LowEnd <0.5X NVMe	96
1.2.8	UCS-NVB960M1H	960GB 2.5in U.3 15mm Micron XTR Hg Perf Ext End 60X NVMe	24
1.2.9	UCSC-P-N7D200GF	MCX755106AS-HEAT:CX-7 2x200GbE QSFP112 PCIe Gen5x16, VPI NIC	12
1.2.10	UCSC-P-N7D200GF	MCX755106AS-HEAT:CX-7 2x200GbE QSFP112 PCIe Gen5x16, VPI NIC	12
1.2.11	UCS-M2-960G-D	960GB M.2 SATA Micron G2 SSD	24

1.2.12	UCS-M2-HWRAID-D	Cisco Boot optimized M.2 Raid controller	12
1.2.13	UCSC-PSU1-1200W-D	1200w AC Titanium Power Supply for C-series Rack Servers	24
1.2.14	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	24
1.2.15	CIMC-LATEST-D	IMC SW (Recommended) latest release for C-Series Servers.	12
1.2.16	UCSC-RAIL-D	Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers	12
1.2.17	UCS-TPM2-002D-D	TPM 2.0 FIPS 140-2 MSW2022 compliant AMD M8 servers	12
1.2.18	UCSC-HSLP-C225M8	UCS C225 M8 Heatsink	12
1.2.19	UCSC-OCP3-KIT-D	C2XX OCP 3.0 Interposer W/Mech Assy	12

Appendix B – References Used in Guide

Cisco UCS C-Series

Product Installation and Service Guide:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/c225m8/install/b-cisco-ucs-c225-m8/m_maintaining-the-server.html

Cisco UCS C225 M8 specification sheet

https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-c220-m8-sff-rack-server.pdf

Cisco Intersight Help Center

https://intersight.com/help/saas

VAST

Appendix C – Known Issues and Workarounds

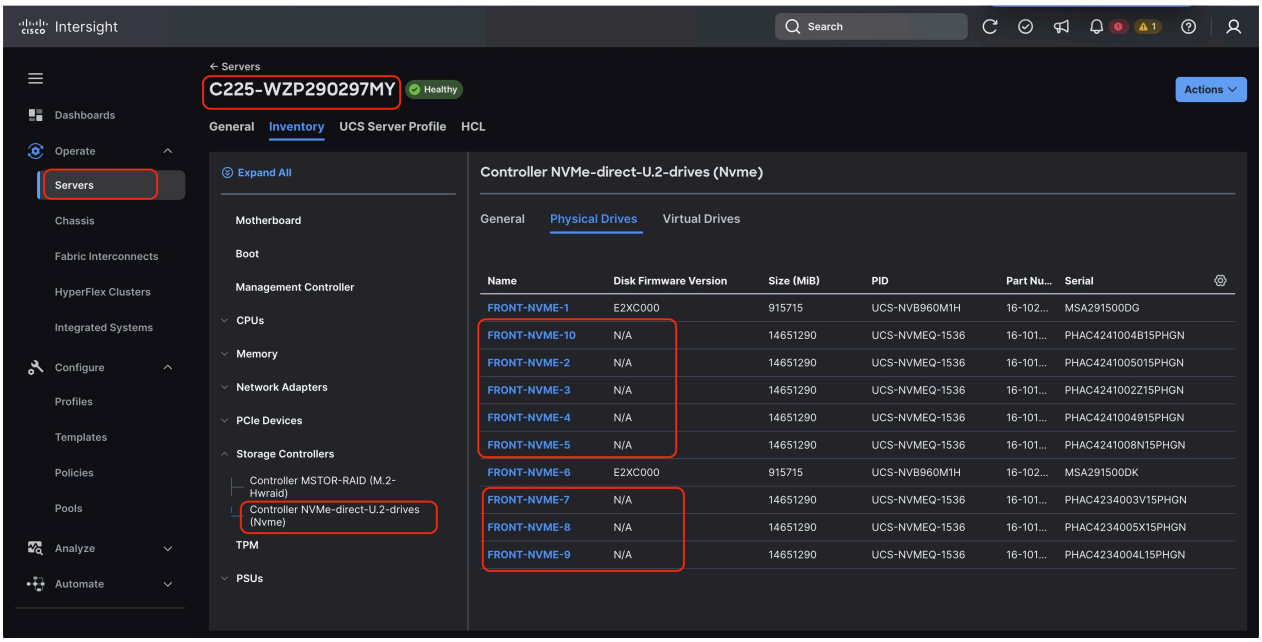
Boot device missing warning

Once the cluster is installed , VAST dashboard displays below warning for all nodes in the cluster

dnode-128-9-4100 (172.16.128.9) [] one or more boot-devices are missing

SSD firmware version on Cisco Intersight dashboard

Once the cluster is installed on Cisco UCS C225 M8 nodes (EBox), the firmware version of 1.5 TB SSDs on Cisco Intersight dashboard is displayed as ‘n/a’.



Appendix D – Sample Network configuration for split network deployment

Nexus 9332D-GX2B - Customer or External Switch configuration

```
feature nxapi
 feature lldp
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp

interface breakout module 1 port 1-6 map 200g-2x

vlan 1080
  name oob-mgmt
vlan 1081
  name inband-network
vlan 1082
  name inband-network-2

class-map type network-qos ROCE_NETWORK_CLASS
  match qos-group 3
policy-map type network-qos ROCE_NETWORK_POLICY
  class type network-qos ROCE_NETWORK_CLASS
    mtu 9216
    pause pfc-cos 3
!
class-map type qos match-all ROCE_CLASS
  match cos 3
  match dscp 26
policy-map type qos ROCE_POLICY
  class ROCE_CLASS
    set qos-group 3
policy-map type queuing ROCE_QUEUING_OUT
  class type queuing c-out-8q-q3
    bandwidth remaining percent 50
    random-detect minimum-threshold 150 kbytes maximum-threshold 3000 kbytes drop-probability 7
weight 0 ecn
```

```
  class type queuing c-out-8q-q2
    bandwidth remaining percent 0
  class type queuing c-out-8q-q1
    bandwidth remaining percent 0
  class type queuing c-out-8q-q-default
    bandwidth remaining percent 50
!
system qos
  service-policy type network-qos ROCE_NETWORK_POLICY
  service-policy type queuing output ROCE_QUEUING_OUT
!

vpc domain 16
  peer-switch
  role priority 10
  peer-keepalive destination 10.108.0.11 source 10.108.0.12
  delay restore 150
  peer-gateway
  auto-recovery
!

interface port-channel16
  description vPC peer-link
  switchport mode trunk
  spanning-tree port type network
service-policy type qos input ROCE_POLICY
  vpc peer-link
!

interface Ethernet1/29-32
  description vpc peer-link
  switchport mode trunk
  channel-group 16 mode active
!

interface Ethernet 1/1/1, Ethernet1/1/2, Ethernet 1/2/1, Ethernet 1/2/2, Ethernet 1/3/1,
Ethernet 1/3/2, Ethernet 1/4/1, Ethernet 1/4/2, Ethernet 1/5/1, Ethernet 1/5/2, Ethernet 1/6/1,
Ethernet 1/6/2
  switchport
  switchport mode trunk
  mtu 9216
  service-policy type qos input ROCE_POLICY no-stats
  no shutdown
!
```

Nexus 9332D-GX2B - Southbound or Internal Switch configuration

```
feature nxapi
 feature lldp
interface breakout module 1 port 1-6 map 200g-2x

vlan 69
  name storage-vlan69


class-map type network-qos ROCE_NETWORK_CLASS
  match qos-group 3
policy-map type network-qos ROCE_NETWORK_POLICY
  class type network-qos ROCE_NETWORK_CLASS
    mtu 9216
    pause pfc-cos 3
!
class-map type qos match-all ROCE_CLASS
  match cos 3
```

```
  match dscp 26
policy-map type qos ROCE_POLICY
  class ROCE_CLASS
    set qos-group 3
policy-map type queuing ROCE_QUEUING_OUT
  class type queuing c-out-8q-q3
    bandwidth remaining percent 50
    random-detect minimum-threshold 150 kbytes maximum-threshold 3000 kbytes drop-probability 7 weight 0 ecn
  class type queuing c-out-8q-q2
    bandwidth remaining percent 0
  class type queuing c-out-8q-q1
    bandwidth remaining percent 0
  class type queuing c-out-8q-q-default
    bandwidth remaining percent 50
!
system qos
  service-policy type network-qos ROCE_NETWORK_POLICY
  service-policy type queuing output ROCE_QUEUING_OUT
!
interface port-channel1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,69
  mtu 9216
  service-policy type qos input ROCE_POLICY
!

interface Ethernet1/27 - 32
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,69
  mtu 9216
  channel-group 1
  no shutdown
!

interface Ethernet 1/1/1, Ethernet1/1/2, Ethernet 1/2/1, Ethernet 1/2/2, Ethernet 1/3/1, Ethernet 1/3/2,
Ethernet 1/4/1, Ethernet 1/4/2, Ethernet 1/5/1, Ethernet 1/5/2, Ethernet 1/6/1, Ethernet 1/6/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,69
  mtu 9216
  service-policy type qos input ROCE_POLICY no-stats
  no shutdown
!
```