



VAST on Cisco UCS C225 M8 (EBox)

Install Guide

Published: December 2024

In partnership with:



Contents

Summary	3
Solution Design	4
Solution Overview	4
EBox Specifications	5
Deployment Architecture	8
Unified network Connectivity	8
Split network Connectivity	11
Licensing	13
Cisco Intersight Licensing	13
VAST Licensing	13
Software and Firmware versions	13
VAST EBOX node configuration	15
CIMC IP configuration	15
Claim EBOX Nodes on Cisco Intersight	17
Create Server Policies	23
Create UCS Server Profile Template	34
Derive and Deploy UCS Server Profile	39
Day 0 EBOX firmware upgrade	45
VAST OS Installation	50
Appendix	60
Appendix A – Bill of Materials	60
Appendix B – References Used in Guide	61
Cisco UCS C-Series	61
Appendix C – Known Issues and Workarounds	61
Boot device missing warning	61
SSD firmware version on Cisco Intersight dashboard	61
Appendix D – Sample Network configuration for split network deployment	62
Nexus 9332D-GX2B - Customer or External Switch configuration	62
Nexus 9332D-GX2B - Southbound or Internal Switch configuration	63

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](#)
- [EBox specifications](#)
- [Deployment Architecture](#)
- [Licensing](#)
- [Software and Firmware versions](#)

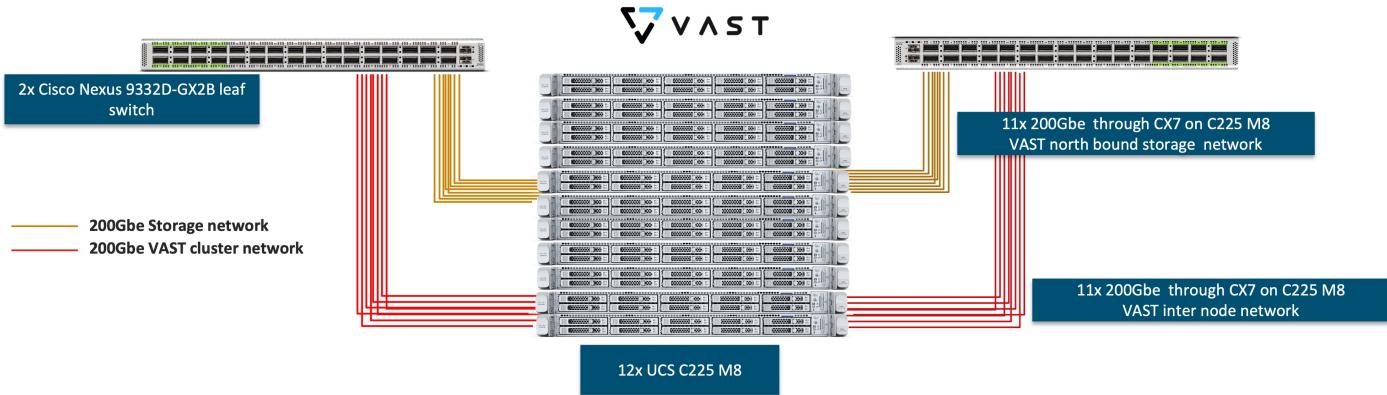
Solution Overview

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)

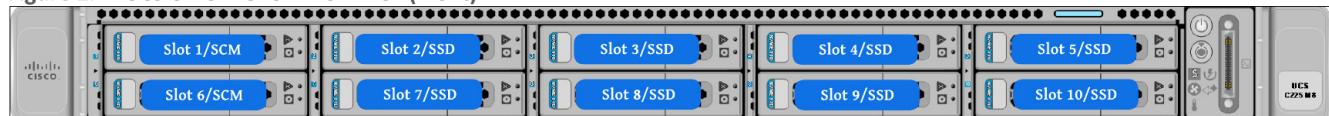


Figure 3. UCS C225 M8 for VAST EBox (Rear)

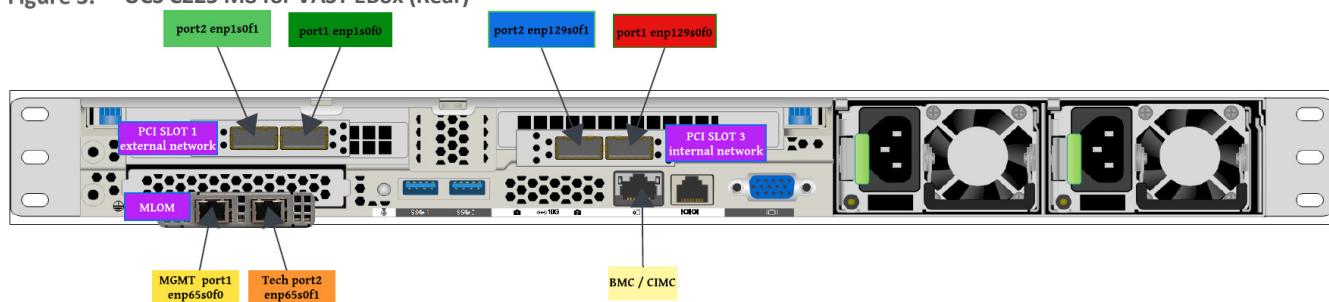


Table below elaborates on each of the critical hardware component for UCS C225 M8 server certified as VAST EBox node. Each table details the hardware specifications for UCS C225 M8 EBox configuration with 15.3TB, 30TB and 60TB SSDs

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

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	<p>1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM)</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM)</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC (MLOM)</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 1</p> <ul style="list-style-type: none"> • 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	<p>1x Cisco-NVDA MCX755106AS-HEAT 2x200GbE QSFP112 Gen5 x16 PCIe NIC on PCI Slot 3</p> <ul style="list-style-type: none"> • 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 configuration as per the customer environment

Figure 4. EBox unified network connectivity

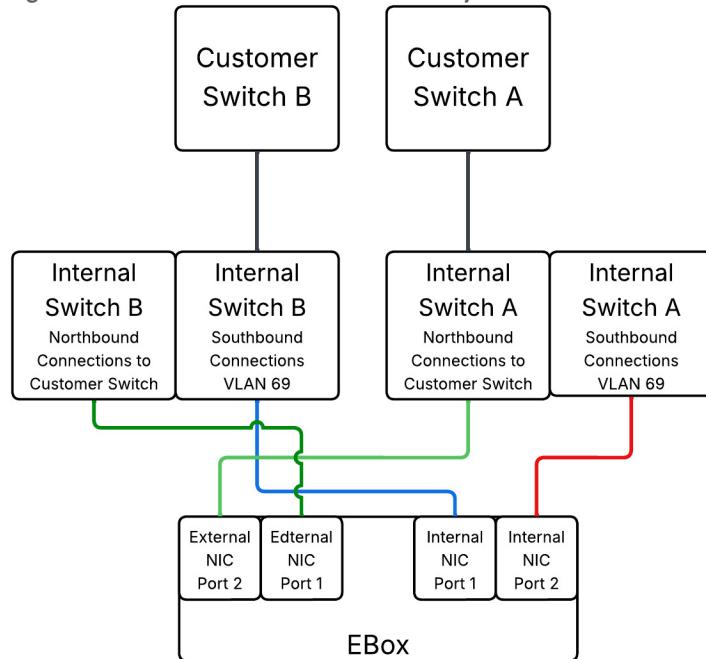
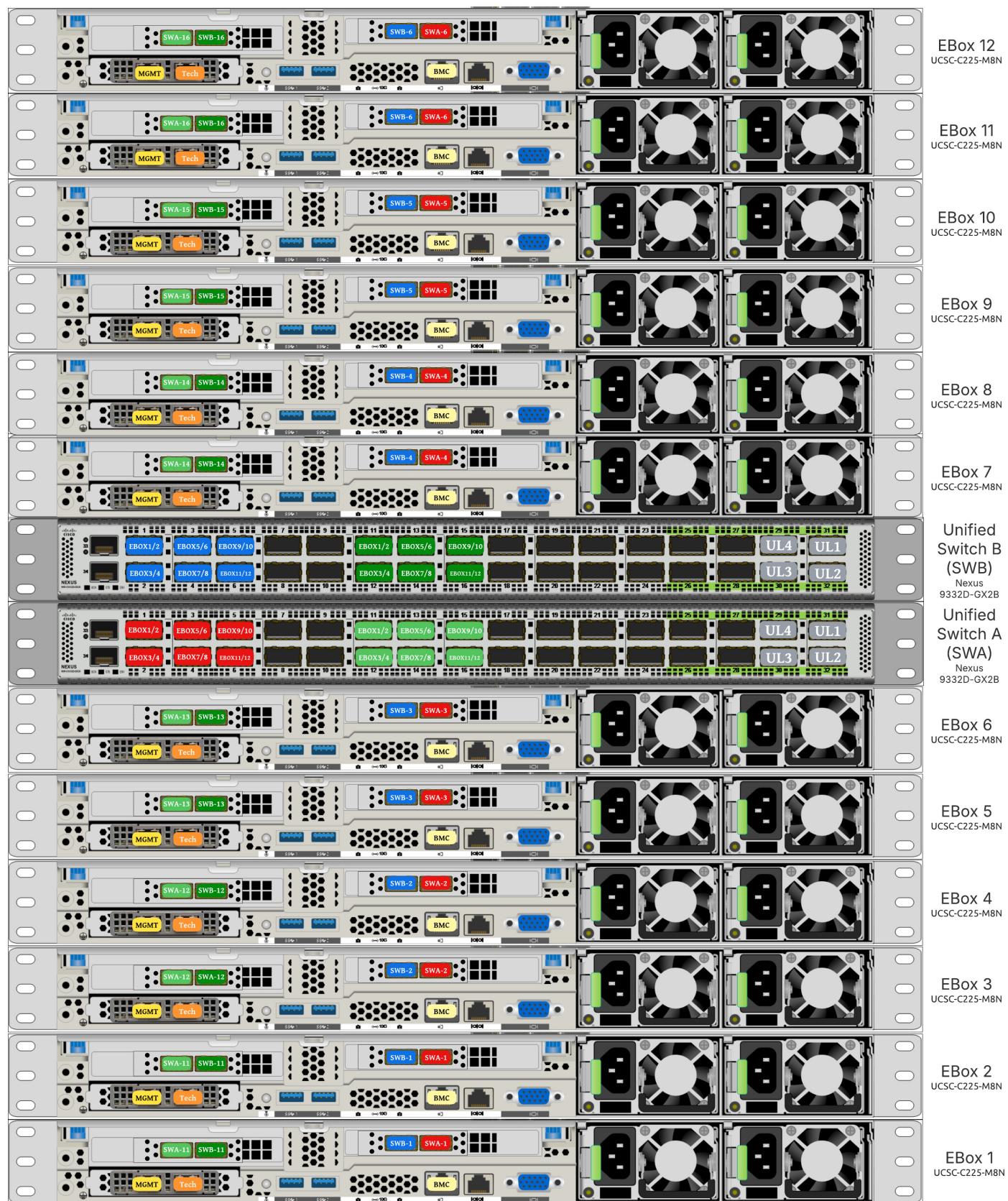


Figure 5. Unified network with 12 x UCS C225 M8N server (12x EBox)



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 connect 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

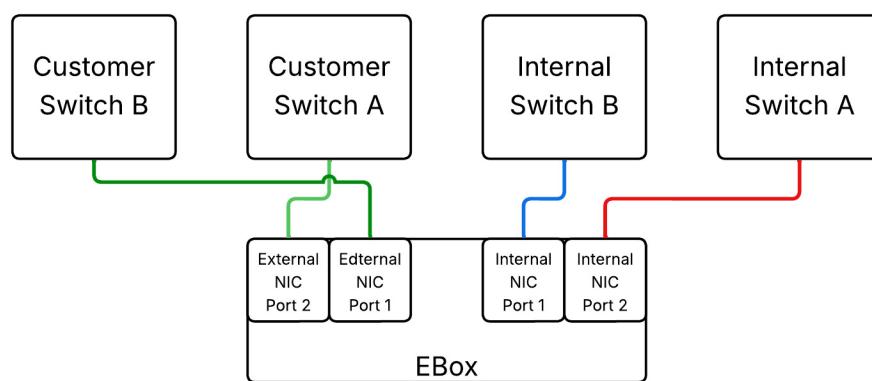
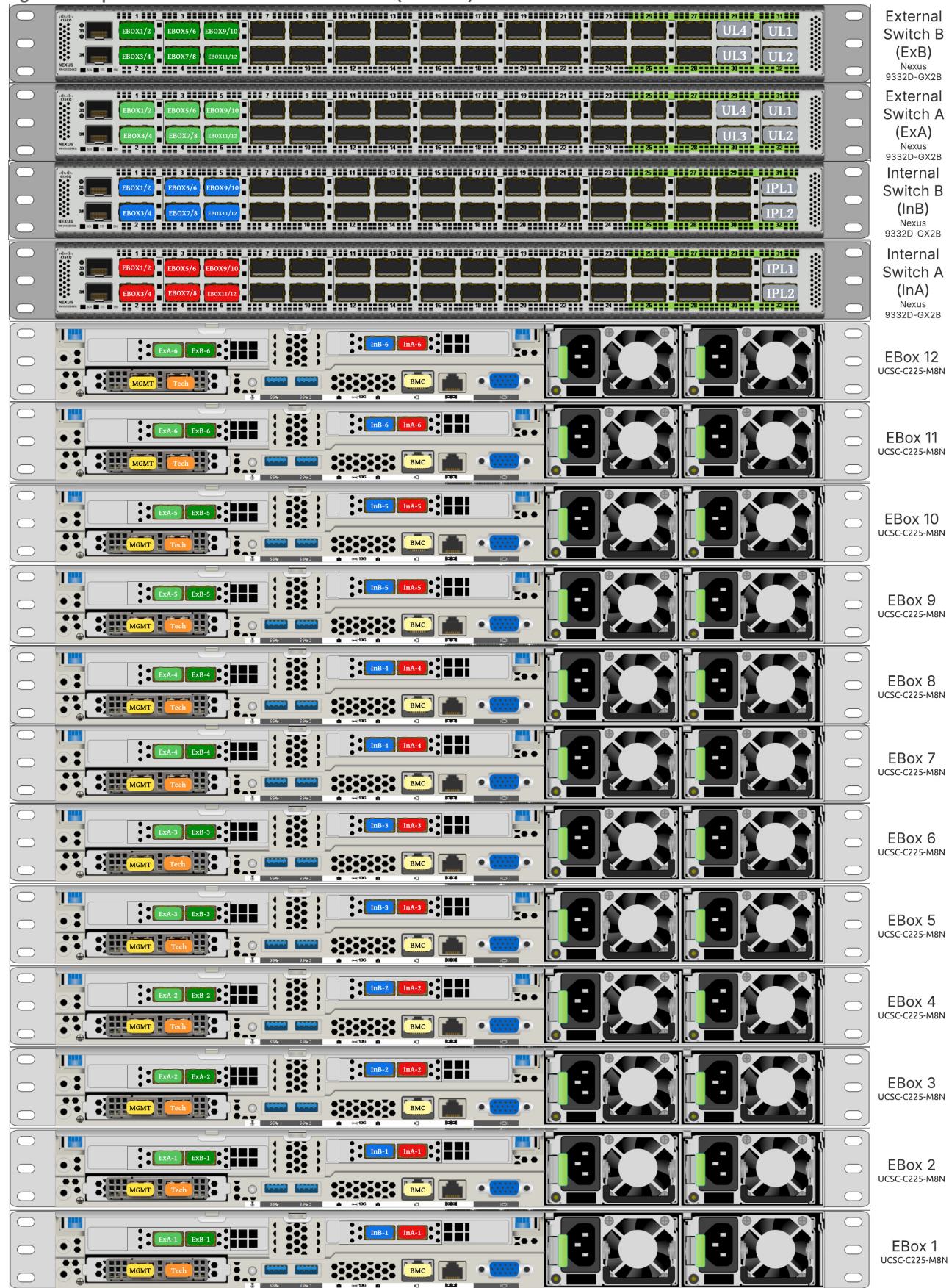


Figure 7. Split network with 12 x C225 M8N server (12x EBox)



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 external 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 of Cisco Nexus 400G switches. The external or customer network connects to external pair of switches and external clients can connect to these switches

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.	

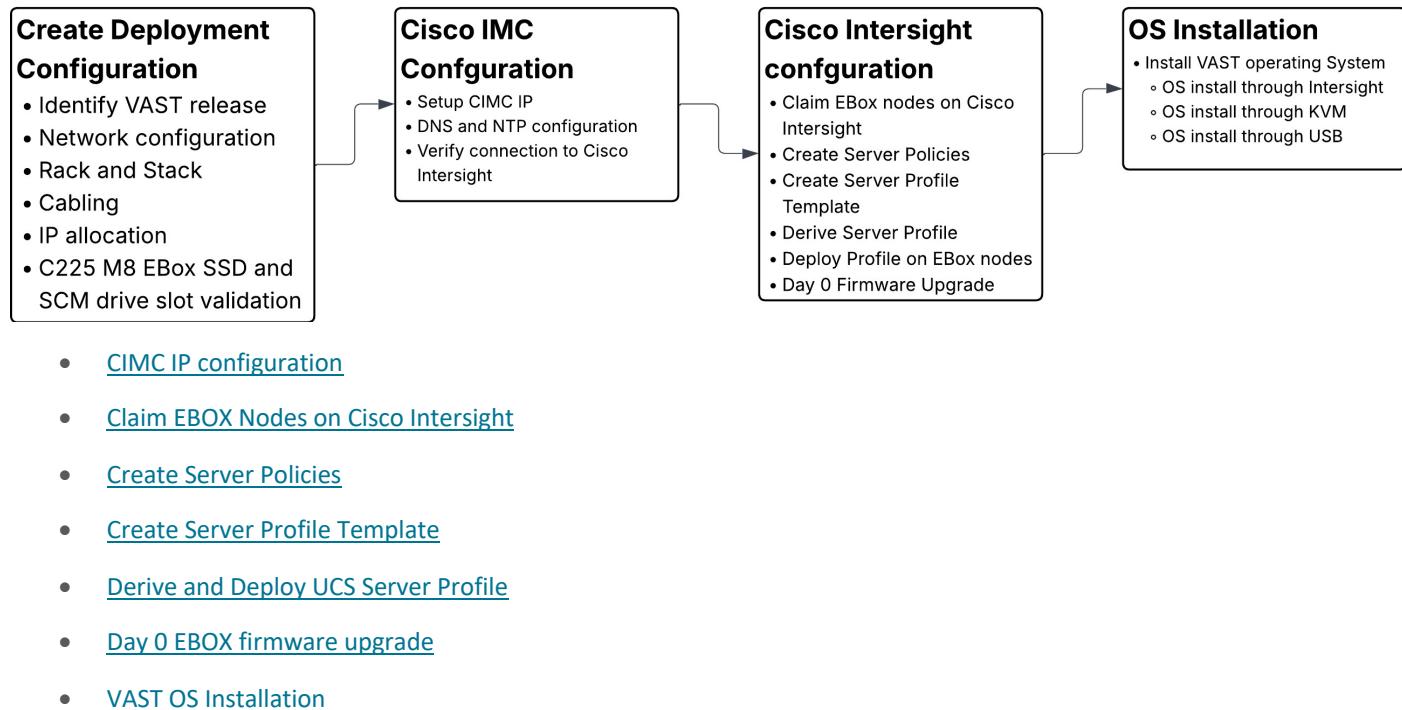
Component	Version	Notes
SCM drive , 960GB Micron XTR	E2XC000	
15.3 TB , Intel/Solidigm 5316 QLC drive	ACV1V204	Updated through VAST VMS bootstrap
M.2 HW RAID controller	2.3.17.1014	
960 GB M.2 Boot drive	D4CS000	
MLOM / Cisco(R) X710T2LG 2x10 GbE RJ45 OCP 3.0 NI	0x8000F961-1.836.0-9.5	
Cisco-NVDA MCX755106AS-HEAT 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

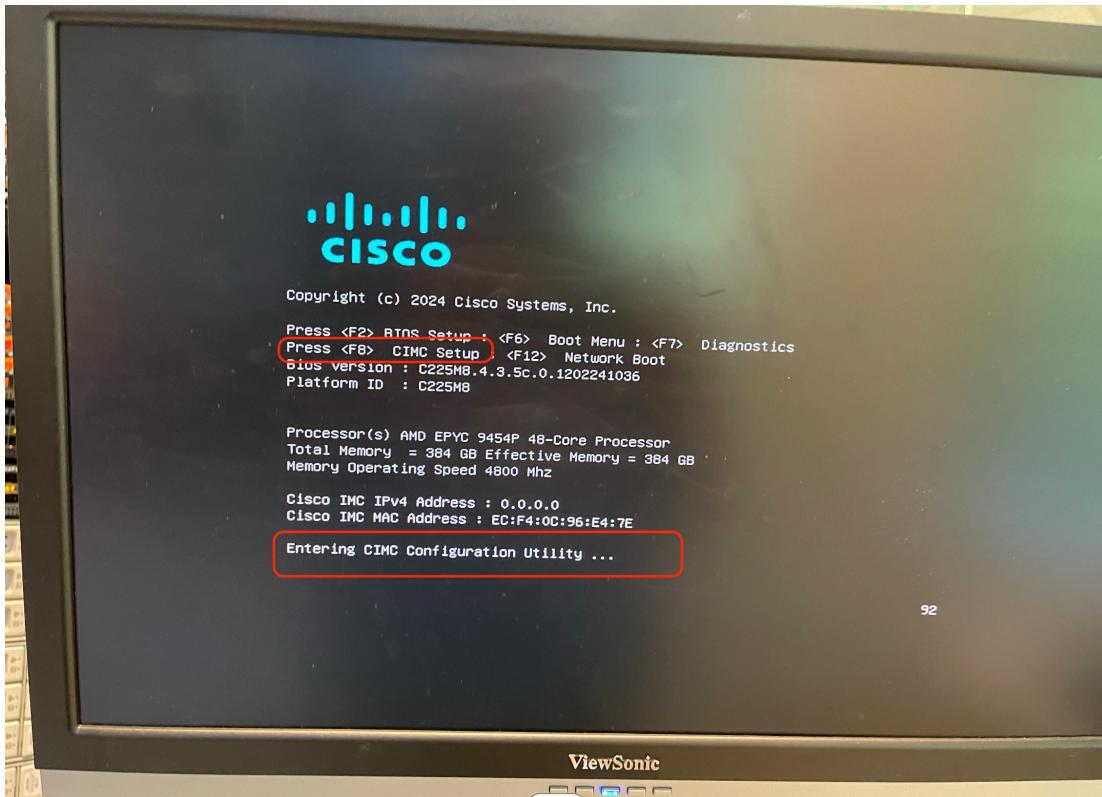
Note: CIMC IP configuration requires local access to the server nodes.

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

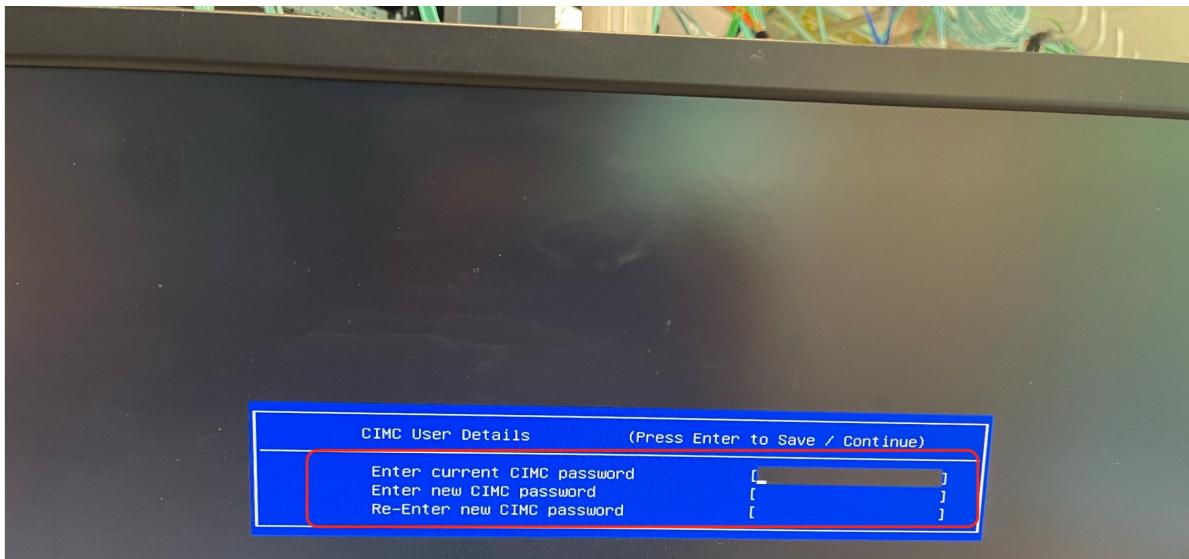
- Connect an optional KVM cable (Cisco PID N20-BKVM) to the KVM connector on the front panel. Connect your USB keyboard and VGA monitor to the KVM cable. (OR)
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel.

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.

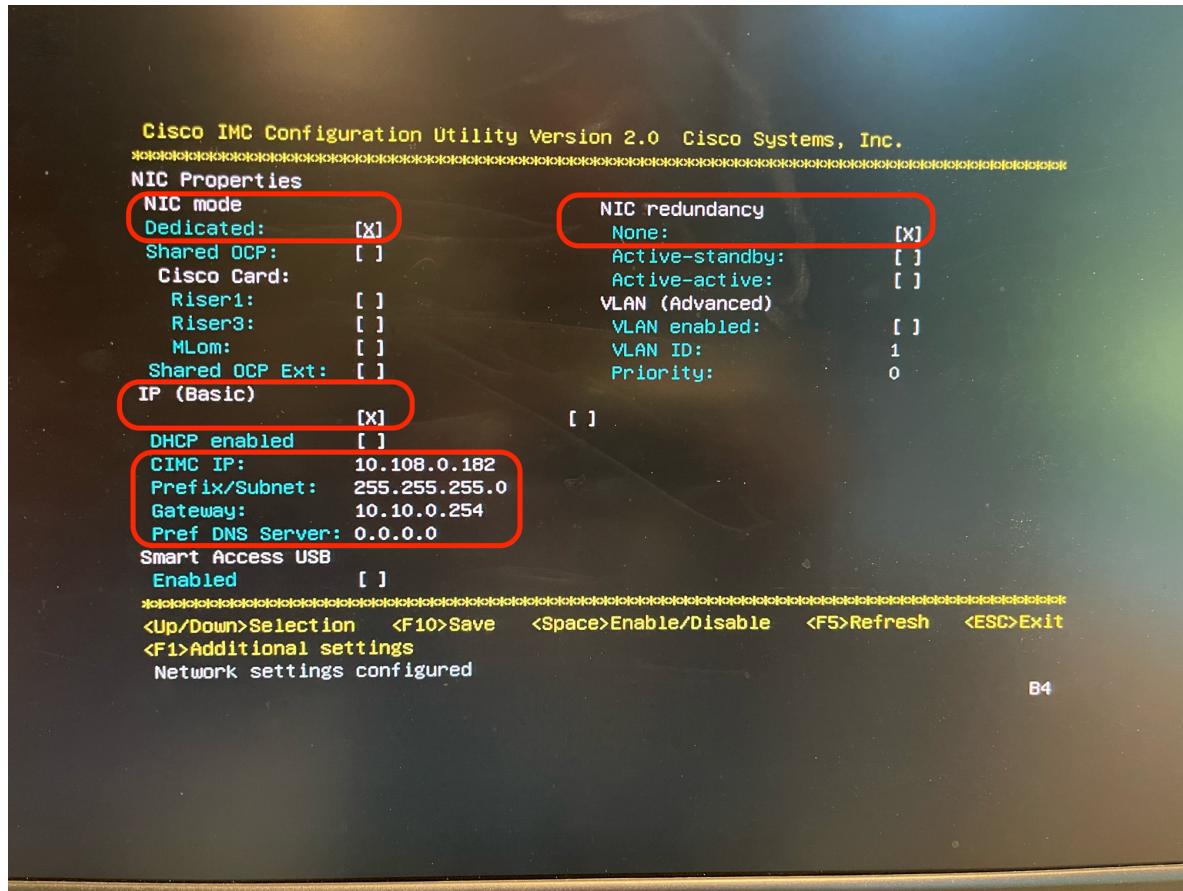


Step 5. On the Cisco IMC Configuration utility ,Edit the below mentioned details. The details are also displayed the screenshot below with edits marked in 'red'

- 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.

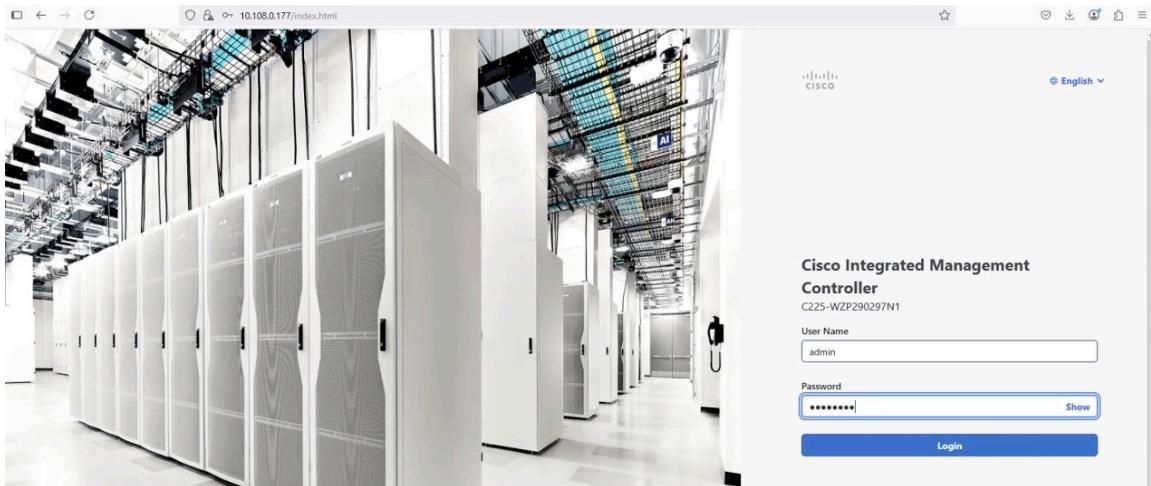
Claim EBOX Nodes on Cisco Intersight

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

Product Name UCS C225 M8N	Serial Number WZP290297N1	Host Name C225-WZP290297N1
ULID 65F1DA17-7E78-4F9A-86BE- BA04529C918F	BIOS Version C225M8.4.3.c.0.1202241036	Current Time Thu, Jun 19, 2025, 06:27:21 PM
PID UCSC-C225-M8N	MAC Address ECF4:0C:96:E7:3C	Timezone UTC
	Firmware Version 4.3(5.25000)	

Overall Server Status Moderate Fault	Overall DIMM Status Good
Power Supplies Fault	Storage Status Good
Power State On	Temperature Good
POST Completion Status Not-Completed	Fans Good

CPUUs 1	Memory Capacity (MB) 393216
Cores 48	Clock Speed (MHz) 4800
Threads 96	Effective Memory (MB) 393216
Cores Enabled 48	Memory Layout
CPUUs Speed (MHz) 2750	

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.

The screenshot shows the Cisco Integrated Management Controller interface. The left sidebar has a 'Device Connector' link highlighted with a red box. The main content area displays the 'Device Connector' configuration page, which includes a network diagram and a status bar indicating an 'Intersight DNS Resolve Error'. A large red box highlights the entire configuration page.

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

The screenshots show the 'Open Settings' dialog for the Device Connector. The top screenshot shows the 'NTP Configuration' tab, and the bottom screenshot shows the 'DNS Configuration' tab. Both dialogs have 'NTP Server' and 'DNS Server' fields, which are redacted in the screenshots. The 'Save' button is visible at the bottom right of each dialog.

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

The screenshot shows the 'Device Connector' configuration page. It displays a network diagram with a 'Device Connector' icon connected to an 'Internet' icon, which is then connected to an 'Intersight' icon. Below the diagram, a yellow box indicates the device is 'Not Claimed'. At the top right, there is a note about the required license: 'Please note: Intersight Infrastructure Services license is required with this server. [Learn More](#)'. On the right side, there are fields for 'Device ID' and 'Claim Code', both of which are redacted with a red box. There are also 'Settings' and 'Refresh' buttons.

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

The screenshot shows the 'Targets' page in the Cisco Intersight interface. The left sidebar has a 'System' category with a 'Targets' link, which is highlighted with a red box. The main content area shows a summary of targets with four cards: 'Health' (4 Healthy), 'Connection' (4 Connected), 'Top Targets by Types' (4 Standalone M8/M7...), and 'Vendor' (4 Cisco Systems, Inc.). Below this is a detailed table of targets:

Name	Health	Status	Type	Claimed Time	Claimed By
C225-WZP290297NZ	Healthy	Connected	Standalone M8 Server	a few seconds ago	andhiman@cisco.com
C225-WZP290297PE	Healthy	Connected	Standalone M8 Server	12 minutes ago	andhiman@cisco.com
C225-WZP290297NK	Healthy	Connected	Standalone M8 Server	9 minutes ago	andhiman@cisco.com
C225-WZP290297NS	Healthy	Connected	Standalone M8 Server	17 minutes ago	andhiman@cisco.com

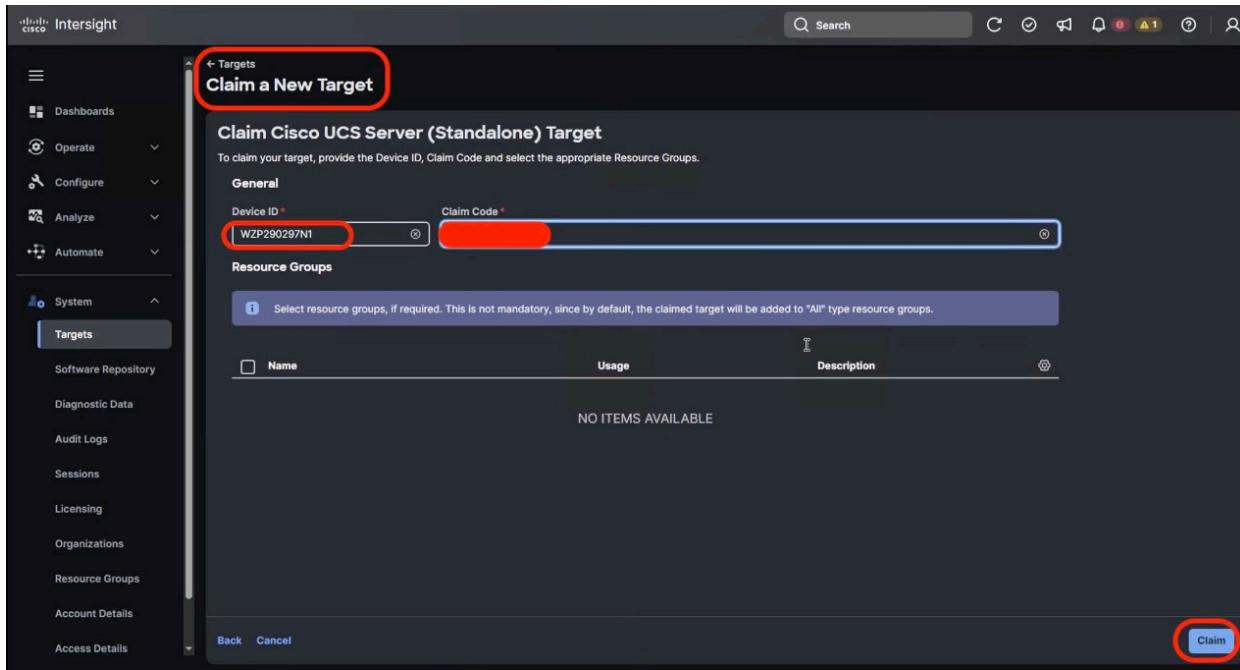
Step 8. On the top left corner, click on 'Claim New Target'

The screenshot shows the Cisco Intersight interface. On the left, there's a navigation sidebar with various options like Dashboards, Operate, Configure, Analyze, Automate, System, and Targets. The Targets option is highlighted with a red box. The main area is titled 'Targets' and displays a summary with four cards: Health (4 healthy), Connection (4 connected), Top Targets by Types (4 Standalone M8/M7...), and Vendor (4 Cisco Systems, Inc.). Below this is a table listing four targets, each with columns for Name, Health, Status, Type, Claimed Time, and Claimed By. A red box highlights the 'Claim a New Target' button at the top right of the page.

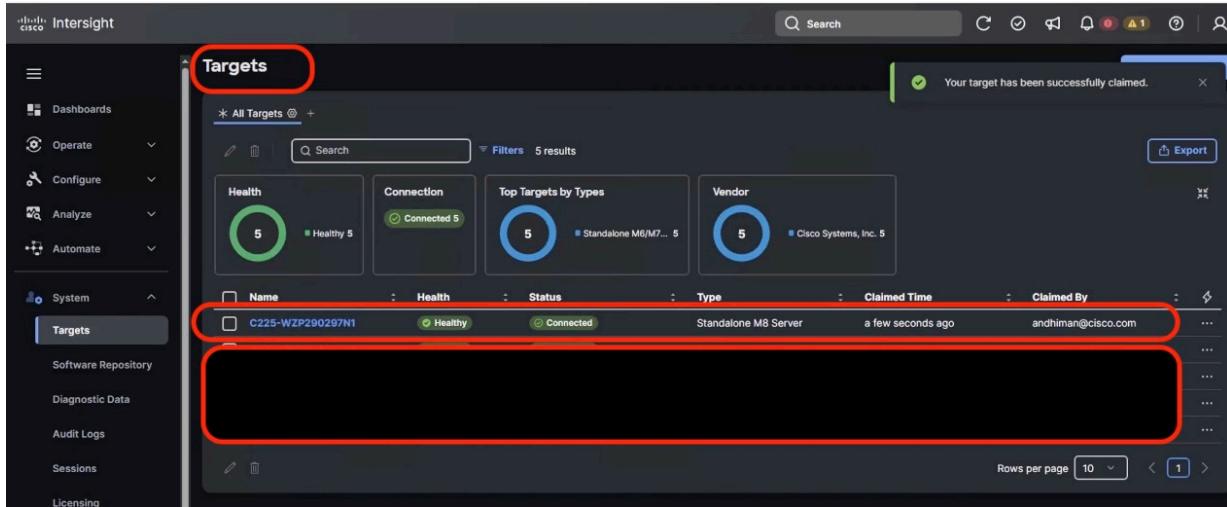
Step 9. On the ‘Select Target Type’ Screen, select ‘Cisco UCS Server (Standalone) and click start button

This screenshot shows the 'Select Target Type' screen. The left sidebar has the 'Targets' option highlighted with a red box. The main area has a title 'Select Target Type' with a red box around it. It includes a 'Filters' section with a checked 'Available for Claiming' checkbox. Below that is a 'Categories' section with 'All' selected. Under 'Compute / Fabric', there's a grid of icons. One icon for 'Cisco UCS Server (Standalone)' is highlighted with a red box. At the bottom right of the screen, there's a blue 'Start' button with a red circle around it.

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.

The screenshot shows the Cisco Intersight interface with the 'Targets' tab selected. The main area displays a summary of target health and connection status, followed by a detailed list of 12 targets. The first 10 targets in the list are highlighted with a red border. Each target entry includes columns for Name, Health, Status, Type, Claimed Time, and Claimed By. All targets listed are 'Healthy' and 'Connected' Standalone M8 servers, claimed by 'andhiman@cisco.com' on June 19, 2025.

Name	Health	Status	Type	Claimed Time	Claimed By
C225-WZP290297MY	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:41 PM	andhiman@cisco.com
C225-WZP290297NZ	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:27 PM	andhiman@cisco.com
C225-WZP290297N1	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:29 PM	andhiman@cisco.com
C225-WZP290297P0	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 4:26 PM	andhiman@cisco.com
C225-WZP290297P5	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:38 PM	andhiman@cisco.com
C225-WZP290297NU	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:45 PM	andhiman@cisco.com
C225-WZP290297P1	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 3:05 PM	andhiman@cisco.com
C225-WZP290297PA	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:36 PM	andhiman@cisco.com
C225-WZP290297PE	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:15 PM	andhiman@cisco.com
C225-WZP290297NK	Healthy	Connected	Standalone M8 Server	Jun 19, 2025 2:18 PM	andhiman@cisco.com

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’

Boot Options	
Number of Retries ⓘ	platform-default
Cool Down Time (sec) ⓘ	platform-default
Boot Option Retry ⓘ	platform-default
IPv4 PXE Support ⓘ	disabled
IPv6 PXE Support ⓘ	disabled
Onboard SCU Storage Support ⓘ	platform-default
Onboard SCU Storage SW Stack ⓘ	platform-default
Power ON Password ⓘ	platform-default
P-SATA Mode ⓘ	platform-default
SATA Mode ⓘ	platform-default
VMD Enablement ⓘ	platform-default

PCI	
ASPM Support ⓘ	platform-default
IOH Resource Allocation ⓘ	platform-default
Memory Mapped IO above 4GiB ⓘ	platform-default
MMCFG BASE ⓘ	platform-default
Onboard 10Gbit LOM ⓘ	platform-default
Onboard Gbit LOM ⓘ	platform-default
NVMe SSD Hot-Plug Support ⓘ	platform-default
Re-Size BAR Support ⓘ	platform-default
SR-IOV Support ⓘ	enabled
VGA Priority ⓘ	platform-default

Processor	
Adjacent Cache Line Prefetcher ⓘ	platform-default
Altitude ⓘ	platform-default
Autonomous Core C State ⓘ	platform-default
CPU Autonomous C State ⓘ	platform-default
Boot Performance Mode ⓘ	platform-default
APBDIS ⓘ	platform-default

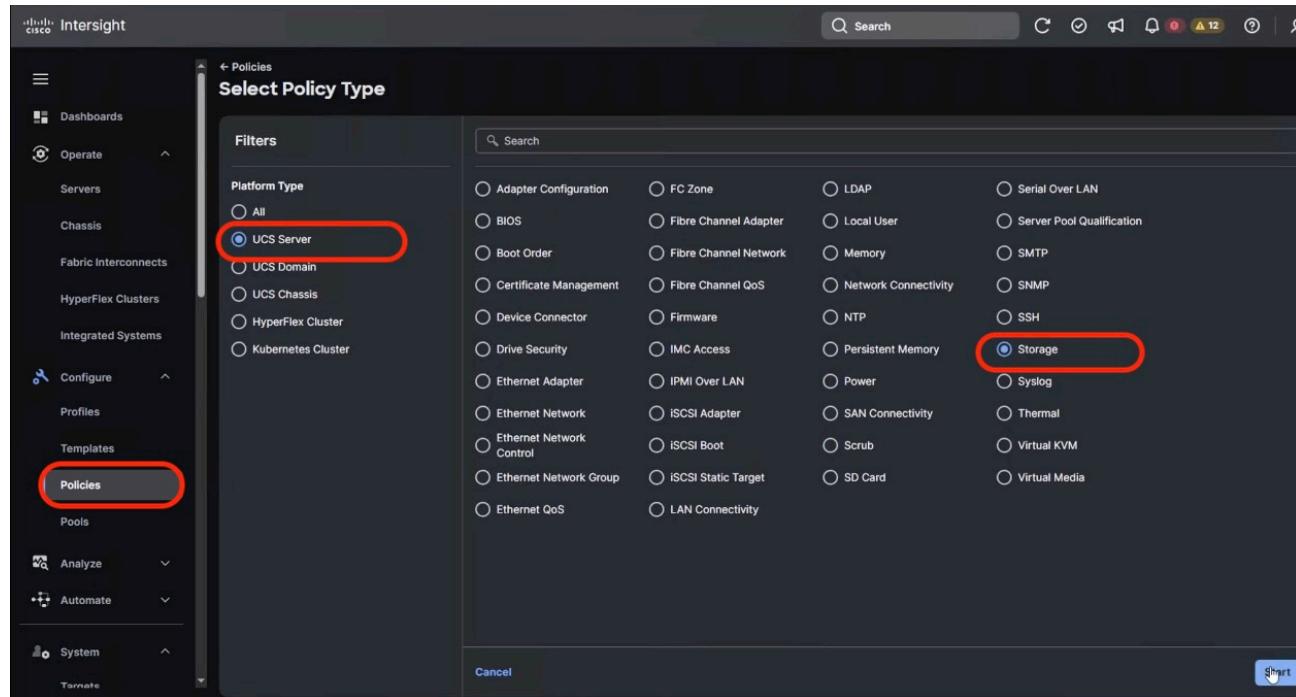
platform-default	platform-default
EDC Control Throttle ⓘ platform-default	Fixed SOC P-State ⓘ platform-default
DF C-States ⓘ platform-default	DF PState Frequency Optimizer ⓘ platform-default
DLWM Support ⓘ platform-default	Power Down Enable ⓘ platform-default
Preferred IO 7xx2 ⓘ platform-default	Preferred IO 7xx3 ⓘ platform-default
xGMI Force Link Width ⓘ platform-default	CCD Control ⓘ platform-default
CPU Downcore control 7xx3 ⓘ platform-default	Downcore control F19 MA0h-AFh ⓘ platform-default
CPU Downcore control F19 M10h-1Fh ⓘ platform-default	CPU SMT Mode ⓘ platform-default
Core Watchdog Timer Enable ⓘ platform-default	Local APIC Mode ⓘ X2APIC
– Server Management	
Assert NMI on PERR ⓘ platform-default	Assert NMI on SERR ⓘ platform-default
Baud Rate ⓘ platform-default	Consistent Device Naming ⓘ platform-default
Adaptive Memory Training ⓘ platform-default	BIOS Techlog Level ⓘ platform-default
OptionROM Launch Optimization ⓘ platform-default	Console Redirection ⓘ com-0
Flow Control ⓘ platform-default	FRB-2 Timer ⓘ platform-default
Legacy OS Redirection ⓘ platform-default	OS Boot Watchdog Timer ⓘ platform-default
OS Boot Watchdog Timer Policy ⓘ platform-default	OS Boot Watchdog Timer Timeout ⓘ platform-default
Out-of-Band Mgmt Port ⓘ platform-default	Putty KeyPad ⓘ platform-default

Cancel **Back** **Create**

Procedure 2. Create Storage Policy

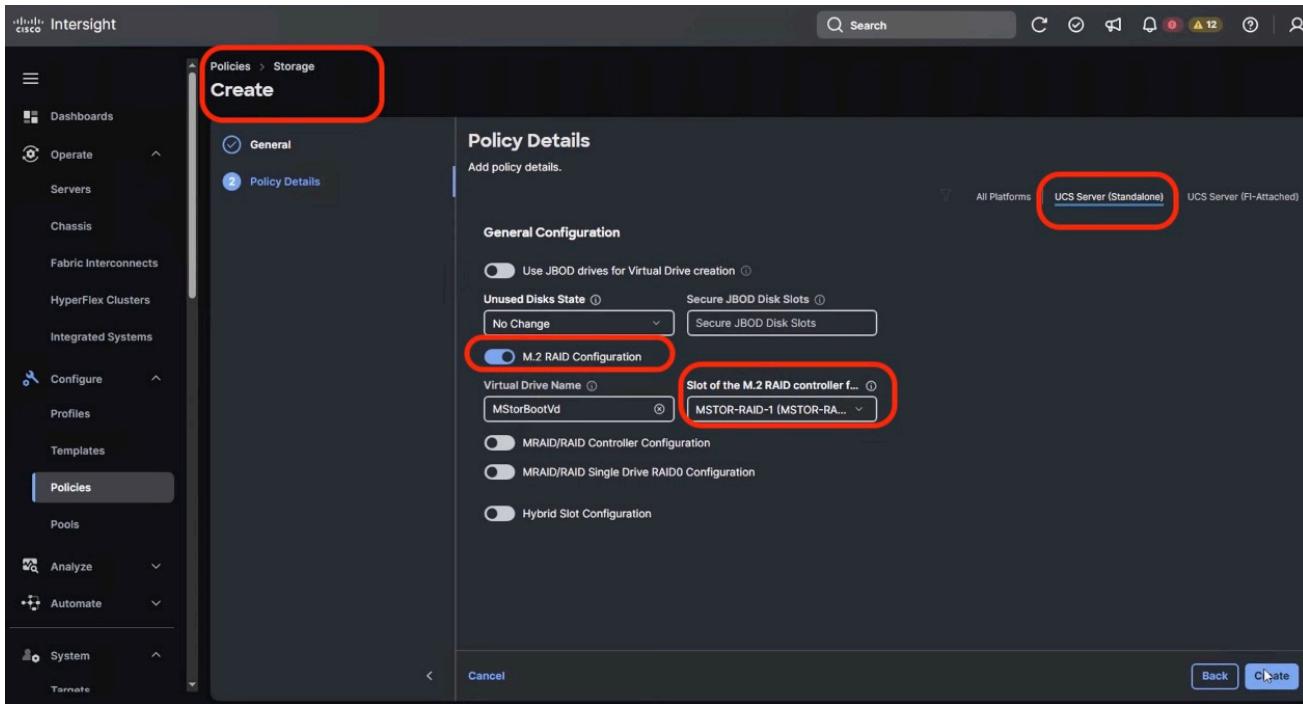
Storage Policy enables RAID1 across 2x M.2 Boot drives

- 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

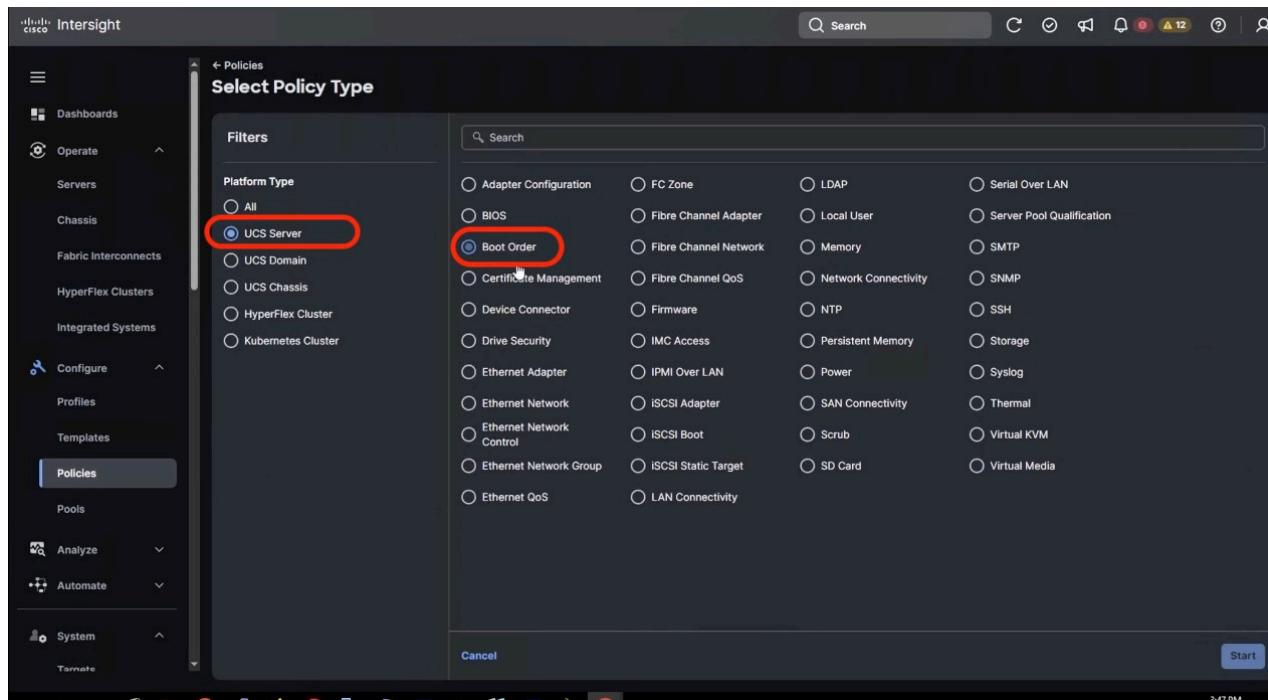
- Step 4.** Select UCS Server (Standalone), Enable M.1 RAID Configuration. MSTOR-RAID is selected by default for 'Slot of the M.2 RAID controller'. Click 'Create'



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

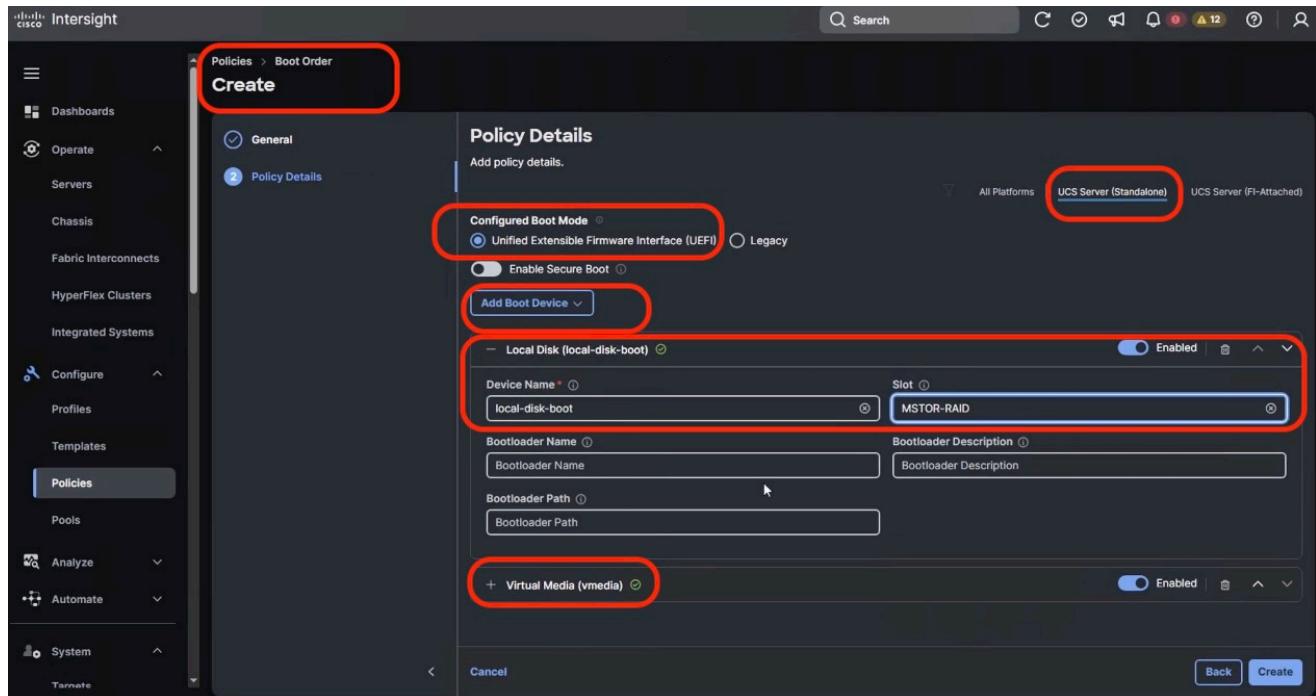
- Step 1.** Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.
- Step 2.** Select UCS Server → Boot Order option and click Start



- 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 boot 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.

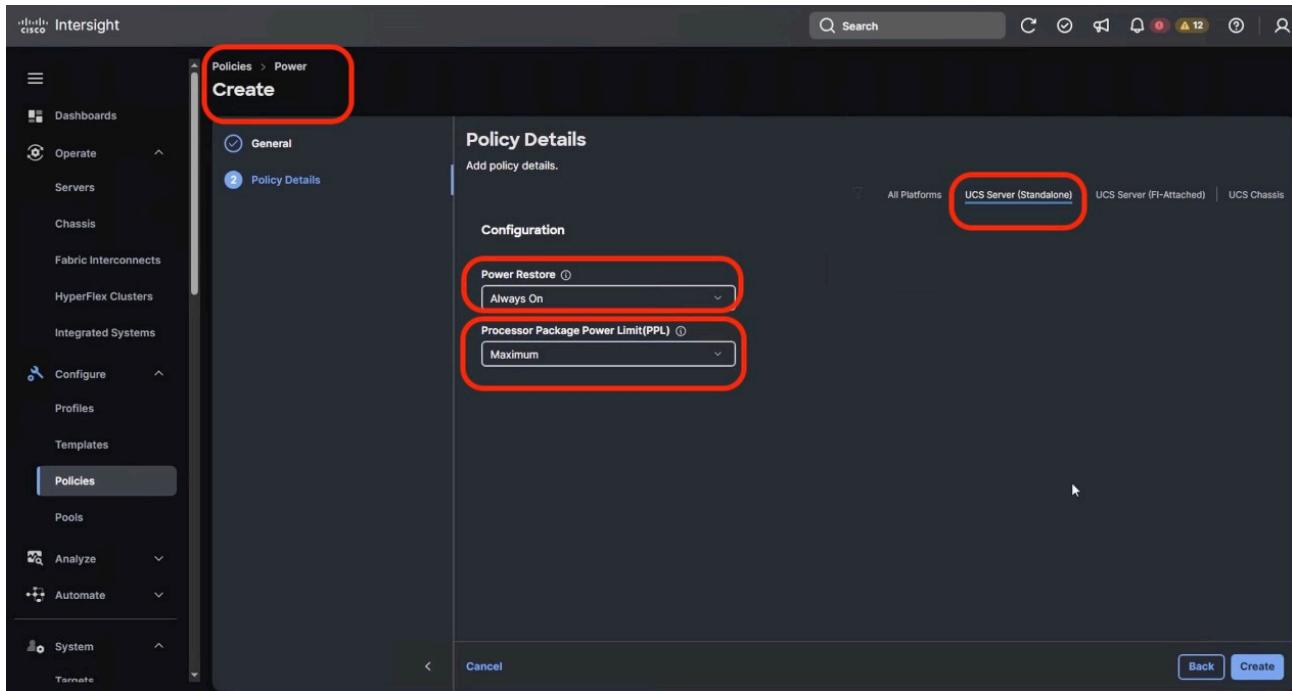


Step 5. Ensure the first boot target is Local Disk and the Slot for Local Disk is ‘MSTOR-RAID’

Step 6. Click create

Procedure 4. Create Power Policy

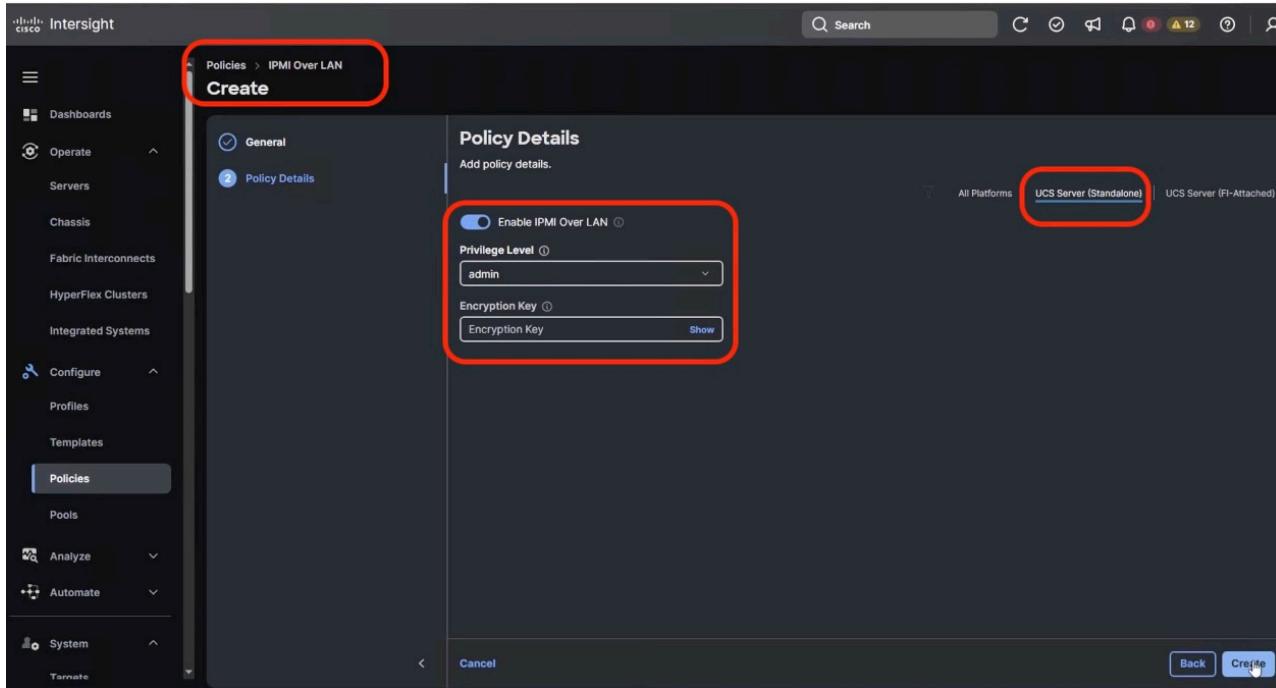
- Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.
- Step 2. Select UCS Server → Power option and click Start
- Step 3. Add a name to the Power Policy and click Next
- Step 4. On the Policy detail screen, **Select UCS 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

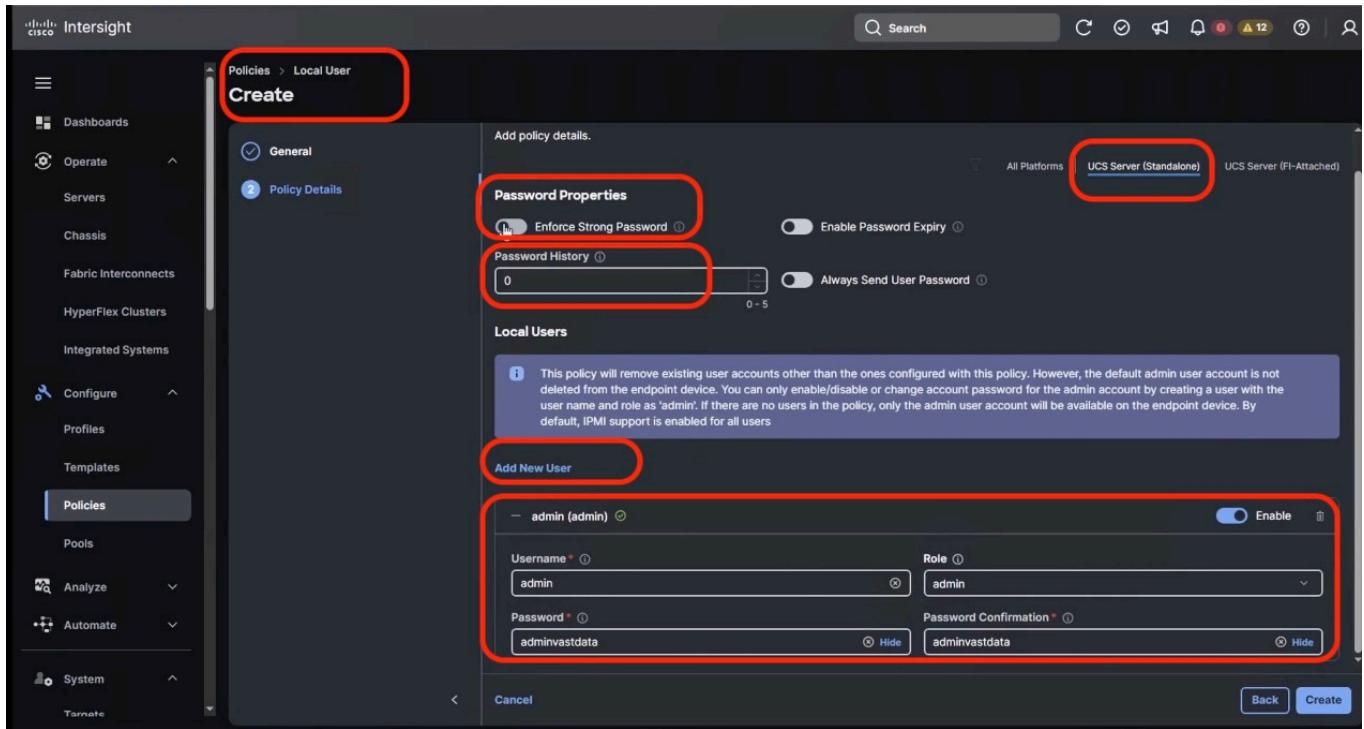
Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

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

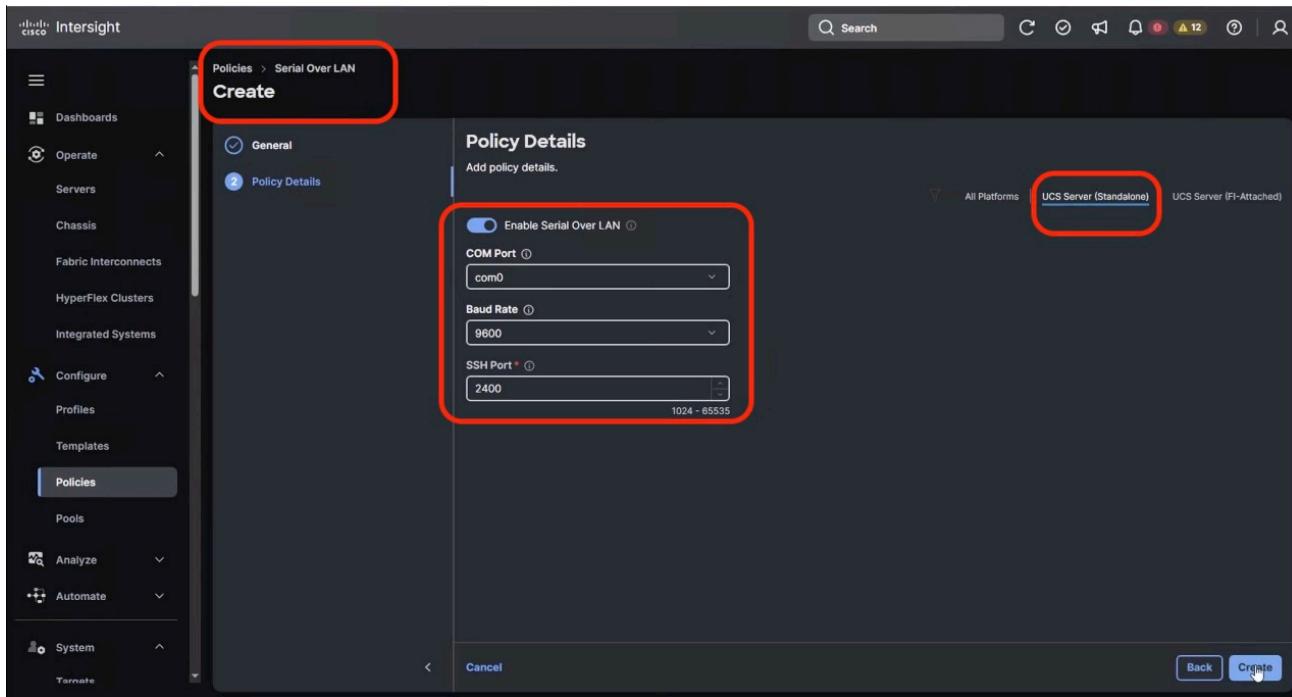
Step 1. Navigate to Cisco Intersight Dashboard, from the left navigation pane, click on Configure → Policies. Click on Create Policy.

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

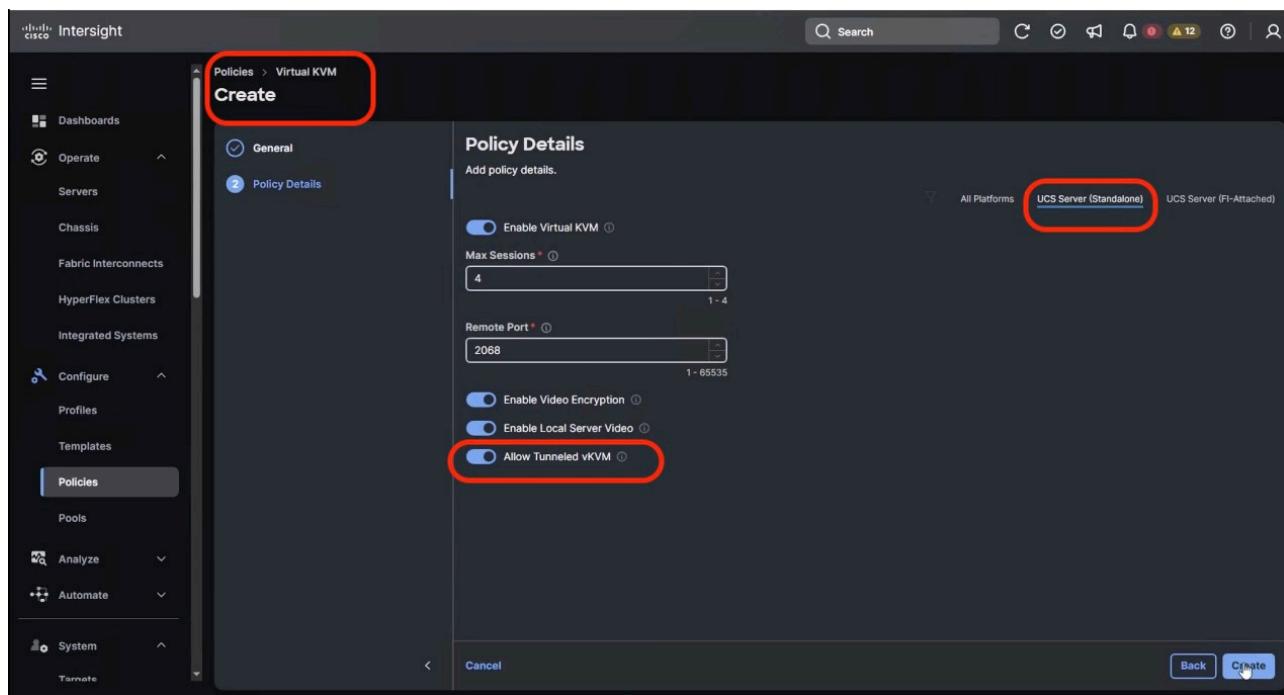
- COM Port as com0
- Baud Rate as 9600
- SSH Port as 2400



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 Tunneld 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

The screenshot shows the Cisco Intersight interface under the 'Policies' section. On the left, a navigation pane includes 'Dashboards', 'Operate', 'Servers', 'Chassis', 'Fabric Interconnects', 'HyperFlex Clusters', 'Integrated Systems', 'Configure' (with 'Profiles' and 'Templates' sub-options), 'Policies' (which is selected and highlighted in blue), 'Pools', 'Analyze', and 'Automate'. The main content area is titled 'Policies' and displays a summary card for 'Platform Type' (UCS Server 8) and 'Usage' (8 Not Used). Below this is a table listing 8 policies:

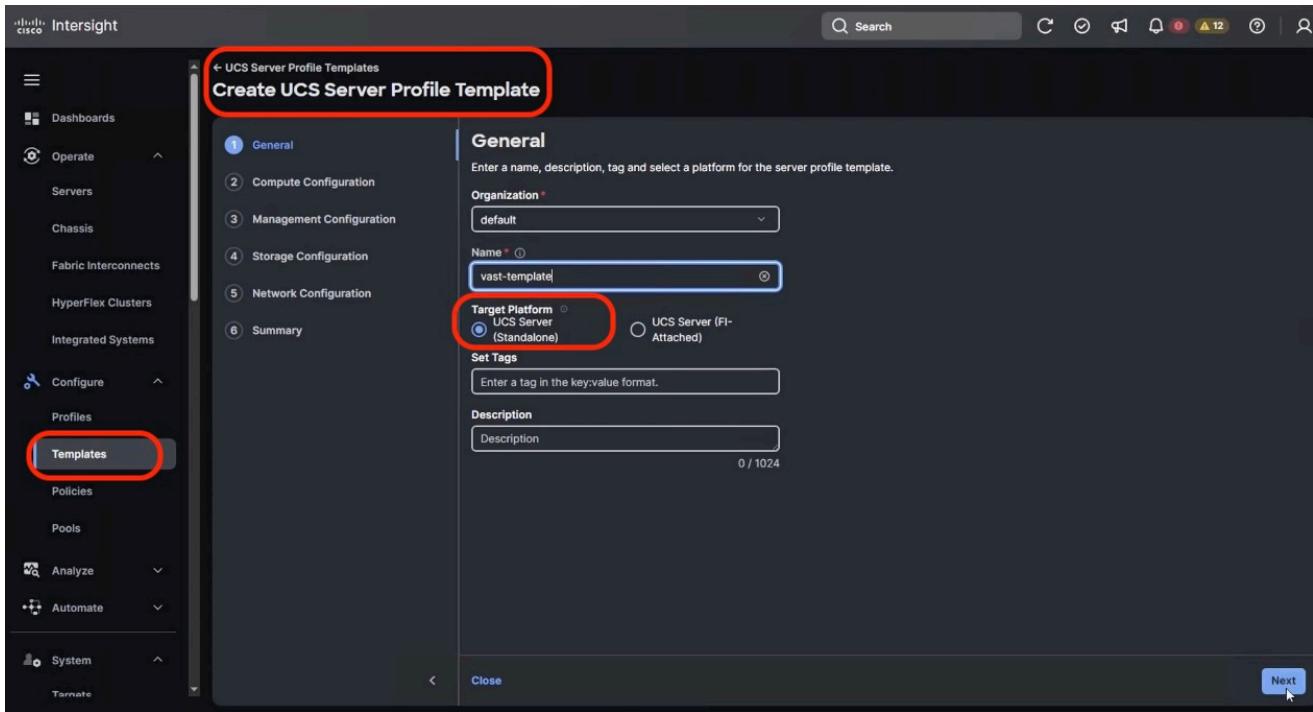
Name	Platform Type	Type	Usage	Last Update
vast-bootorder	UCS Server	Boot Order	Not Used	a few seconds ago
vast-storage	UCS Server	Storage	Not Used	2 minutes ago
vast-vkvm	UCS Server	Virtual KVM	Not Used	3 minutes ago
vast-sol	UCS Server	Serial Over LAN	Not Used	3 minutes ago
vast-localuser	UCS Server	Local User	Not Used	4 minutes ago
vast-ipmi	UCS Server	IPMI Over LAN	Not Used	6 minutes ago
vast-power	UCS Server, UCS Chassis	Power	Not Used	7 minutes ago
vast-bios	UCS Server	BIOS	Not Used	7 minutes ago

Buttons for 'Create Policy' and 'Export' are at the top right, and a 'Rows per page' dropdown is at the bottom right.

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

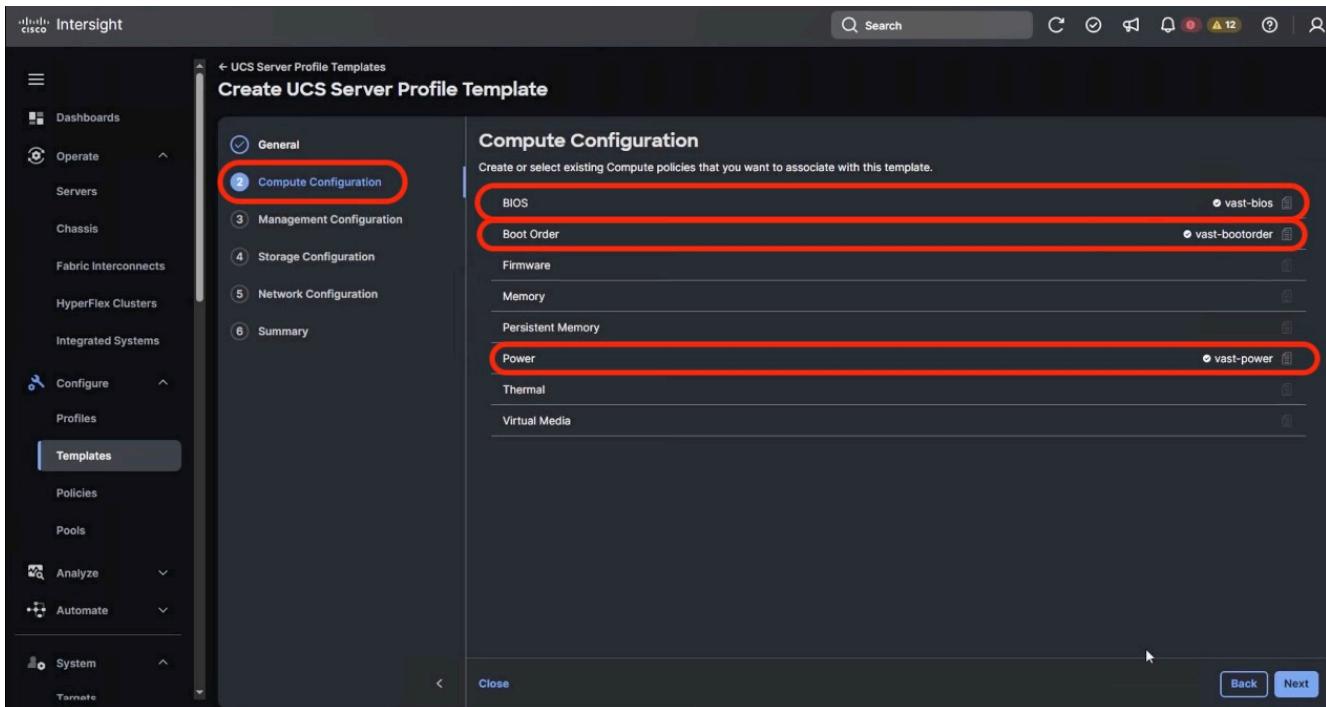
The screenshot shows the Cisco Intersight interface under the 'Templates' section. On the left, a navigation pane includes 'Dashboards', 'Operate', 'Servers', 'Chassis', 'Fabric Interconnects', 'HyperFlex Clusters', 'Integrated Systems', 'Configure' (with 'Profiles' and 'Templates' sub-options), 'Policies' (which is selected and highlighted in blue), 'Pools', 'Analyze', and 'Automate'. The main content area is titled 'Templates' and shows tabs for 'UCS Chassis Profile Templates', 'UCS Domain Profile Templates', 'UCS Server Profile Templates' (which is selected and highlighted in blue), 'vNIC Templates', and 'vHBA Templates'. A red box highlights the 'UCS Server Profile Templates' tab. Another red box highlights the 'Create UCS Server Profile Template' button at the top right. The table below shows 0 results.

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

Create UCS Server Profile Template

Management Configuration

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

Certificate Management

Device Connector

- IPMI Over LAN (vast-ipmi)
- LDAP
- Local User (vast-localuser)

Network Connectivity

NTP

- Serial Over LAN (vast-sol)
- SMTP
- SNMP
- SSH
- Syslog

Virtual KVM (vast-vkvm)

Back Next

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

Create UCS Server Profile Template

Storage Configuration

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

Drive Security

SD Card

- Storage (vast-storage)

Back 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

cisco Intersight

Create UCS Server Profile Template

UCS Server Profile Templates

General Compute Configuration Management Configuration Storage Configuration Network Configuration

Summary

Name: vast-template Organization: default

Target Platform: UCS Server (Standalone)

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

BIOS: vast-bios

Boot Order: vast-bootorder

Power: vast-power

Close Back Derive Profiles

cisco Intersight

Create UCS Server Profile Template

UCS Server Profile Templates

General Compute Configuration Management Configuration Storage Configuration Network Configuration

Summary

Name: vast-template Organization: default

Target Platform: UCS Server (Standalone)

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

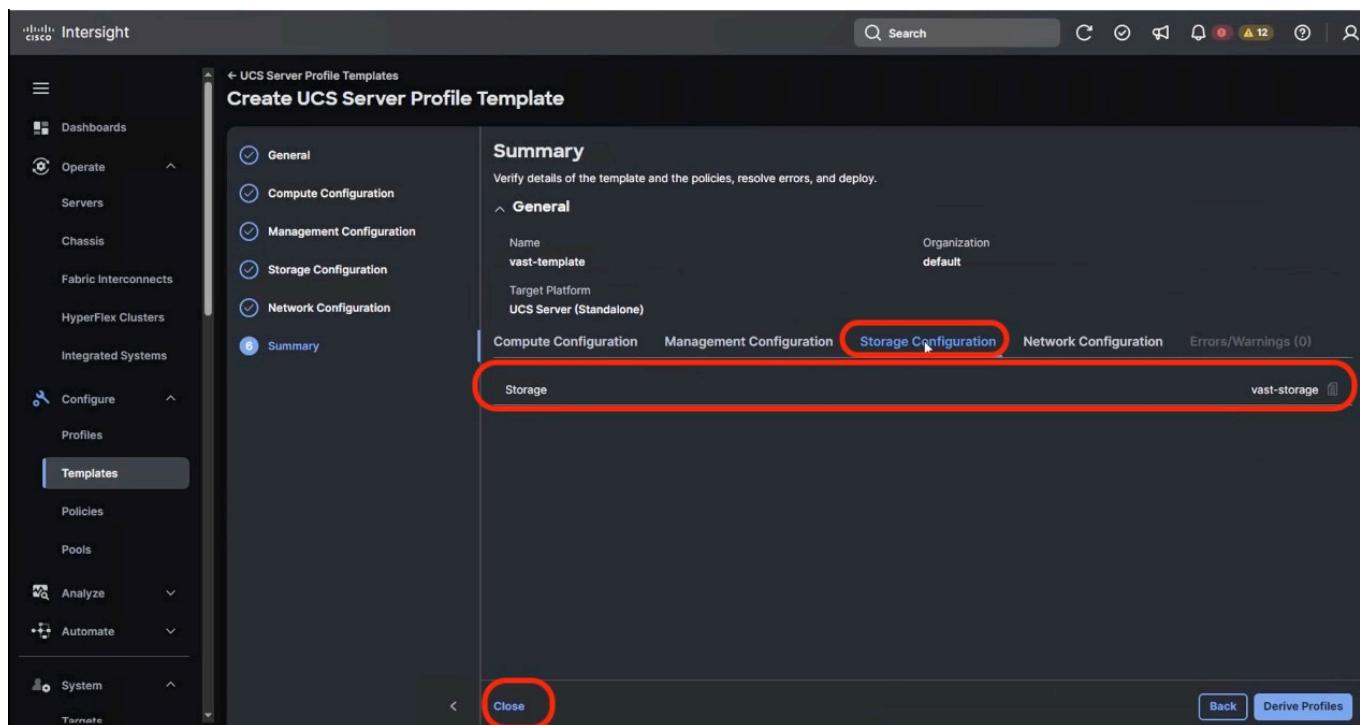
IPMI Over LAN: vast-ipmi

Local User: vast-localuser

Serial Over LAN: vast-sol

Virtual KVM: vast-vkvm

Close Back Derive Profiles



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.

Name	Sync Status	Usage	Target Platform	Description	Last Update
vast-template	-	0	UCS Server (Standalone)		42 minutes ago

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

The screenshot shows the Cisco Intersight interface. On the left, there's a navigation sidebar with sections like Dashboards, Operate, Configure, and Templates. The 'Templates' section is currently selected. In the main area, under 'UCS Server Profile Templates', there's a table with one row. The first column, 'Name', contains 'vast-template'. To the right of the table is a 'Derive Profiles' button, which is also circled in red.

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

This screenshot shows the 'Derive' configuration page for the 'vast-template' profile. The 'General' tab is active. Under 'Source UCS Server Profile Template', the name 'vast-template' is selected. In the 'Server Assignment' section, the 'Assign Now' button is highlighted with a red box. Below, a table lists 12 selected server profiles, with two entries for 'C225-WZP29...' highlighted. At the bottom right, the 'Next' button is also circled in red.

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

The screenshot shows the 'Derive' interface for UCS Server Profile Templates. On the left, there's a navigation pane with sections like Dashboards, Operate, Servers, Chassis, Fabric Interconnects, HyperFlex Clusters, Integrated Systems, Configure, Profiles (selected), Policies, Pools, Analyze, Automate, System, and Ternate. The main area is titled 'Derive' and shows a list of derived profiles. Each profile entry includes a name field (e.g., 'vast-template_DERIVED-5' through 'vast-template_DERIVED-12'), an organization dropdown set to 'default', and an assigned server field showing the server ID (e.g., 'C225-WZP290297NU'). At the bottom right of the main area are 'Close', 'Back', and 'Next' buttons.

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

This screenshot shows the 'Summary' section of the 'Derive' interface. It includes a 'General' section with the template name 'vast-template' and organization 'default', and a 'Management Configuration' section listing four policies: 'IPMI Over LAN', 'Local User', 'Serial Over LAN', and 'Virtual KVM'. The 'Management Configuration' section is highlighted with a red box. At the bottom right, there are 'Close', 'Back', and 'Derive' buttons, with the 'Derive' button also highlighted with a red box.

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

The trial period for Infrastructure Service and Cloud Orchestrator is active. During the trial period, the Advantage tier features of Infrastructure Service and Cloud Orchestrator are available. [Go to Licensing](#)

Profiles

HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles **UCS Server Profiles**

Create UCS Server Profile **Export**

All UCS Server Profil...						
Status		Inconsistency Reason	Template Sync Status	Target Platform		
! Not Deployed 12		No data available	OK 12	Standalone 12		
<input type="checkbox"/>	Name	Status	Target Platform	UCS Server Template	Template Sync St...	Server
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PE
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PA
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P6
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P5
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P0
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P1
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NZ
<input type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NU

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

The trial period for Infrastructure Service and Cloud Orchestrator is active. During the trial period, the Advantage tier features of Infrastructure Service and Cloud Orchestrator are available. [Go to Licensing](#)

Profiles

HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles **UCS Server Profiles**

Create UCS Server Profile **Export**

All UCS Server Profil...						
Deploy		Inconsistency Reason	Template Sync Status	Target Platform		
<input type="checkbox"/>	Activate	No data available	OK 12	Standalone 12		
<input checked="" type="checkbox"/>	Name	Status	Target Platform	UCS Server Template	Template Sync St...	Server
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PE
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PA
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P6
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P5
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P0
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P1
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NZ
<input checked="" type="checkbox"/>	vast-template_DERIVE...	! Not Deployed	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NU

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.

Deploy (12 UCS Server Profiles)

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



Some servers are powered on. Deploying and activating the profiles may cause a reboot and disruption. If deploying policy configurations requires an immediate reboot, check Reboot immediately to activate.

More Details

- Reboot immediately to activate.
- I understand that potential disruption may occur during profile deployment.

Cancel

Deploy

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

The screenshot shows the Cisco Intersight interface. On the left, there's a navigation sidebar with options like Dashboards, Operate, Servers, Chassis, Fabric Interconnects, HyperFlex Clusters, Integrated Systems, Configure (selected), Profiles (selected), Templates, Policies, Pools, Analyze, Automate, and System. The main area is titled 'Profiles' and contains four summary cards: Status (Validating 12), Inconsistency Reason (No data available), Template Sync Status (OK 12), and Target Platform (Standalone 12). Below these cards is a table listing 12 server profiles. Each row includes a checkbox, Name, Status (Validating), Target Platform (UCS Server (Standalone)), UCS Server Template (vast-template), Template Sync St... (OK), Server (C225-WZP290297PE, etc.), and Last Update (a few seconds ago). A red box highlights the 'Status' card. Another red box highlights the top right corner of the screen, which displays a success message: 'Deploying successfully started for 12 UCS Server Profiles.'

Name	Status	Target Platform	UCS Server Template	Template Sync St...	Server	Last Update
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PE	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PA	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297PB	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P5	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P0	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297P1	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NZ	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NU	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NK	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NI	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297MY	a few seconds ago
vast-template_DERIVE...	Validating	UCS Server (Standalone)	vast-template	OK	C225-WZP290297NS	a few seconds ago

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

The screenshot shows the 'Deploy Server Profile' page in Cisco Intersight. The left sidebar is titled 'Profiles' and lists various categories like Dashboards, Servers, Chassis, etc. The main area has tabs for 'Details' and 'Execution Flow'. In 'Details', the status is 'In Progress', name is 'Deploy Server Profile', ID is '68547461696f6e3101aafa04', target type is 'Rack Server', target name is 'C225-WZP290297NZ', source type is 'Server Profile', source name is 'vast-template_DERIVED-6', initiator is 'andhiman@cisco.com', and start time is 'Jun 19, 2025 4:34 PM'. The 'Execution Flow' tab shows a list of steps with their status and completion time, all completed successfully. A progress bar at the top indicates 36% completion.

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

The screenshot shows the 'Profiles' page in Cisco Intersight. The left sidebar is the same as the previous screenshot. The main area displays a table of profiles. The first four columns are highlighted with a red box: 'Status' (Validating 12), 'Inconsistency Reason' (No data available), 'Template Sync Status' (OK 12), and 'Target Platform' (Standalone 12). A red box also highlights a success message at the top right: 'Deploying successfully started for 12 UCS Server Profiles.' The table below lists 12 profiles, each with a status of 'Validating' and a green 'OK' icon.

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

The screenshot shows the Cisco Intersight interface. The left sidebar has 'Operate' and 'Servers' selected. The main area is titled 'Servers' and shows a summary of 12 servers. Below the summary are six cards: Health (12 healthy), Power (On 12), HCL Status (Incomplete 12), Bundle Version (12, 4.3(5.250030) 12), Utility Storage (Yes 12), Firmware Version (12, 4.3(5.250030) 12), and Models (12, C22). A red box highlights the table below, which lists 12 servers with columns: Name, Health, Model, Management IP, Server Profile, Firmware Version, CPU Capacity, and UCS Domain. All servers listed are healthy (green) and have the same model (UCSC-C225-M8N).

Name	Health	Model	Management IP	Server Profile	Firmware Version	CPU Capacity	UCS Domain
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.180	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.177	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.175	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.173	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.181	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.176	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.171	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.172	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.179	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.182	vast-template...	4.3(5.250030)	132.0	...

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

The screenshot shows the Cisco Intersight interface. The left sidebar has 'Operate' and 'Servers' selected. The main area displays a summary of 12 servers with metrics like Health (12), Power (On 12), and HCL Status (Incomplete 12). Below is a detailed table of 12 servers, each with a checkbox. The entire table row is highlighted with a red box. At the bottom, there are buttons for 'Selected 12 of 12', 'Show Selected', and 'Unselect All'. On the right, there's a 'Rows per page' dropdown set to 10, and navigation arrows.

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

The screenshot shows the Cisco Intersight interface. The left sidebar has 'Operate' and 'Servers' selected. A context menu is open over the server table, with the 'Upgrade Firmware' option highlighted by a red box. Other options in the menu include Power, System, Profile, VMware, Install Operating System, Start Alarm Suppression, Stop Alarm Suppression, and Set License Tier.

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

The screenshot shows the 'Upgrade Firmware' interface in Cisco Intersight. On the left, a sidebar menu is open under the 'Servers' section. The main panel is titled 'General' and displays a message about improving firmware download performance via CDN. Below this is a table listing 12 selected server components, all of which are checked. The columns are Name, User Label, Model, Firmware Version, and Utility Storage. The table shows various models like UCSC-C225-M8N and UCSC-C225-M8P across different part numbers.

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

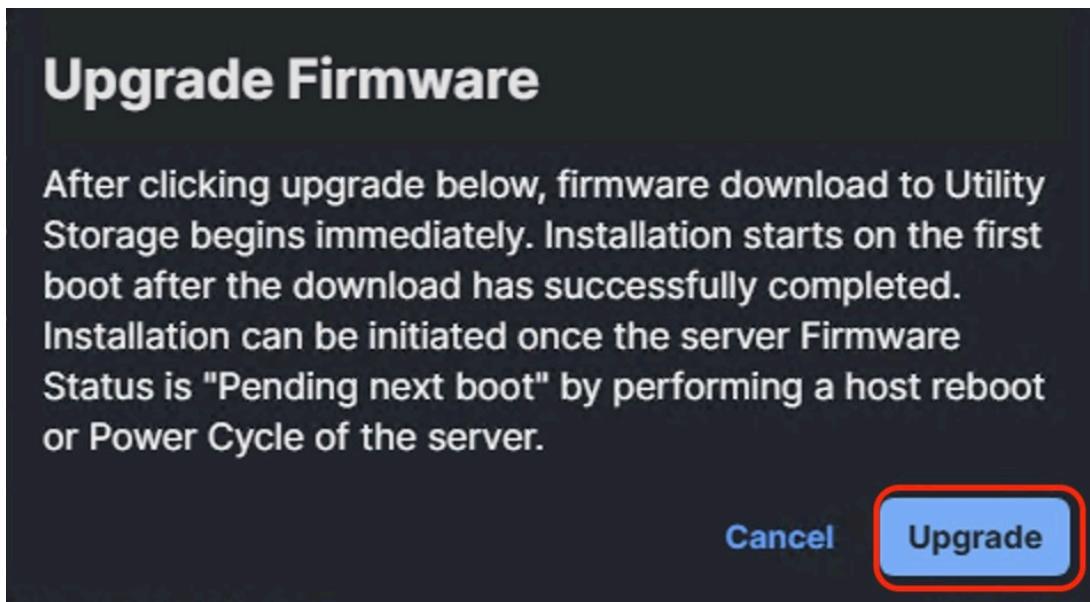
Note: By default, the storage controller and drive firmware is upgraded. The Advanced Mode enabled users to de-select firmware upgrade for storage controller and drive firmware.

The screenshot shows the 'Version' tab of the 'Upgrade Firmware' interface. It displays a list of 6 firmware versions from the Cisco Repository. One specific version, '4.3(5.250030)', is highlighted with a red border. The table includes columns for Version, Size, Release Date, and Description. The description for the highlighted version is 'Cisco UCS Host Upgrade Utility'.

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

The screenshot shows the Cisco Intersight web interface. On the left, there's a sidebar with various navigation options like Dashboards, Operate, Servers, Chassis, etc. The 'Servers' option is currently selected. In the main content area, there's a title 'Upgrade Firmware'. Below it, there are three tabs: 'General', 'Version', and 'Summary', with 'Summary' being the active tab and highlighted with a red box. The 'Summary' section contains a brief description: 'Confirm configuration and initiate the upgrade.' Below this is a 'Firmware' section showing the current version as '4.3(5.250030)' and a file size of '705.87 MB'. To the right of this is a table titled 'Servers to be Upgraded' with 12 results. The table has columns for Name, User Label, Model, Firmware Version, and Utility Storage. All entries show 'UCSC-C225-M8N' as the model and '4.3(5.250001)' as the firmware version. The 'Utility Storage' column shows a checkmark in every row. At the bottom of the table is a 'Cancel' button and an 'Upgrade' button, which is also highlighted with a red box.

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 .

Details

Status: Action Required

Name: Upgrade Firmware

ID: 68549f8a696f6e3101ad3368

Target Type: Rack Server

Target Name: C225-WZP290297P1

Source Type: Upgrade Firmware

Source Name: C225-WZP290297P1

Initiator: andhiman@cisco.com

Start Time: Jun 19, 2025 7:38 PM

Execution Flow

Progress: 29%

Wait for the server reboot.

Ensure server meet requirements to continue upgrade. Please acknowledge to continue with server power cycle. Learn more at Help Center.

Terminate Proceed

- Wait for firmware staging to complete. Staging 4.3(5.250030) completed successfully. Jun 19, 2025 7:57 PM
- Initiate firmware upgrade. Initiated upgrade from 4.3(5.250001) to 4.3(5.250030) successfully. Image: ucs-c225m8-huu-4.3.5.250030.iso Jun 19, 2025 7:49 PM
- Find image source to download. Jun 19, 2025 7:46 PM
- Wait for image download to complete in endpoint. Download completed successfully. Jun 19, 2025 7:45 PM
- Initiate image download to endpoint. Download request for version 4.3(5.250030) submitted successfully. Jun 19, 2025 7:38 PM

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

Servers

All Servers 12 results

Name	Health	Model	Management IP	Server Profile	Firmware Version	CPU Capaci...	UCS Domain
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.180	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.177	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.175	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.173	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.181	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.176	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.171	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.172	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.179	vast-template...	4.3(5.250030)	132.0	...
C225-WZP29...	Healthy	UCSC-C225-M8N	10.108.0.182	vast-template...	4.3(5.250030)	132.0	...

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 (vmmedia) has the lowest priority in the Boot Order policy. This is displayed in screenshot below:

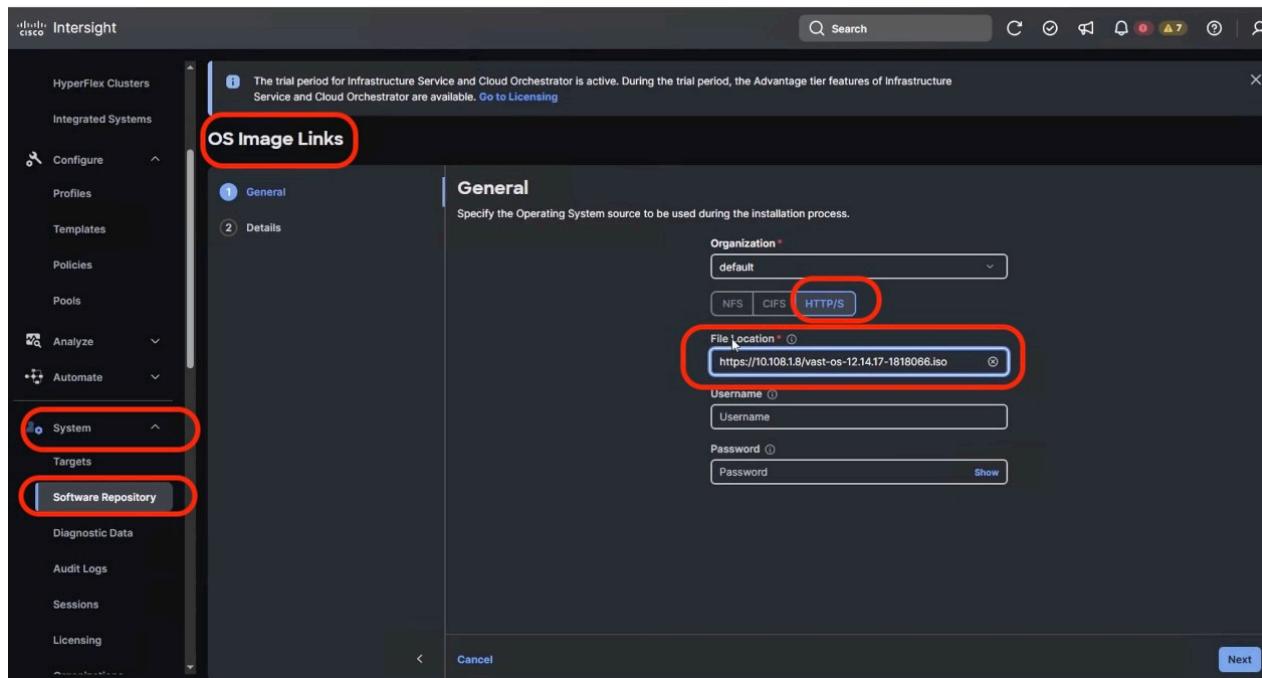
The screenshot shows the Cisco Intersight web interface. On the left, the navigation sidebar is visible with sections like Dashboards, Operate, Configure, and Policies. The 'Policies' section is highlighted with a red box. In the center, a policy named 'vast-bootorder' is selected, indicated by a red box around its name. The 'Details' tab is active, showing the policy's name, description, type (Boot Order), target platform, last update (Jun 19, 2025 4:33 PM), organization (default), and tags (No Tags). The 'Usage' tab shows 13 results for the 'vast-template' server profile across various UCS servers. The 'Configuration' tab is also highlighted with a red box, displaying settings for Configured Boot Mode (Unified Extensible Firmware Interface (UEFI)), Enable Secure Boot (Off), and a detailed view of the Boot Devices configuration. Under Boot Devices, Local Disk is expanded, showing Virtual Media (Enable: Yes, Device Name: vmmedia, Type: Virtual Media, Sub-Type: None).

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

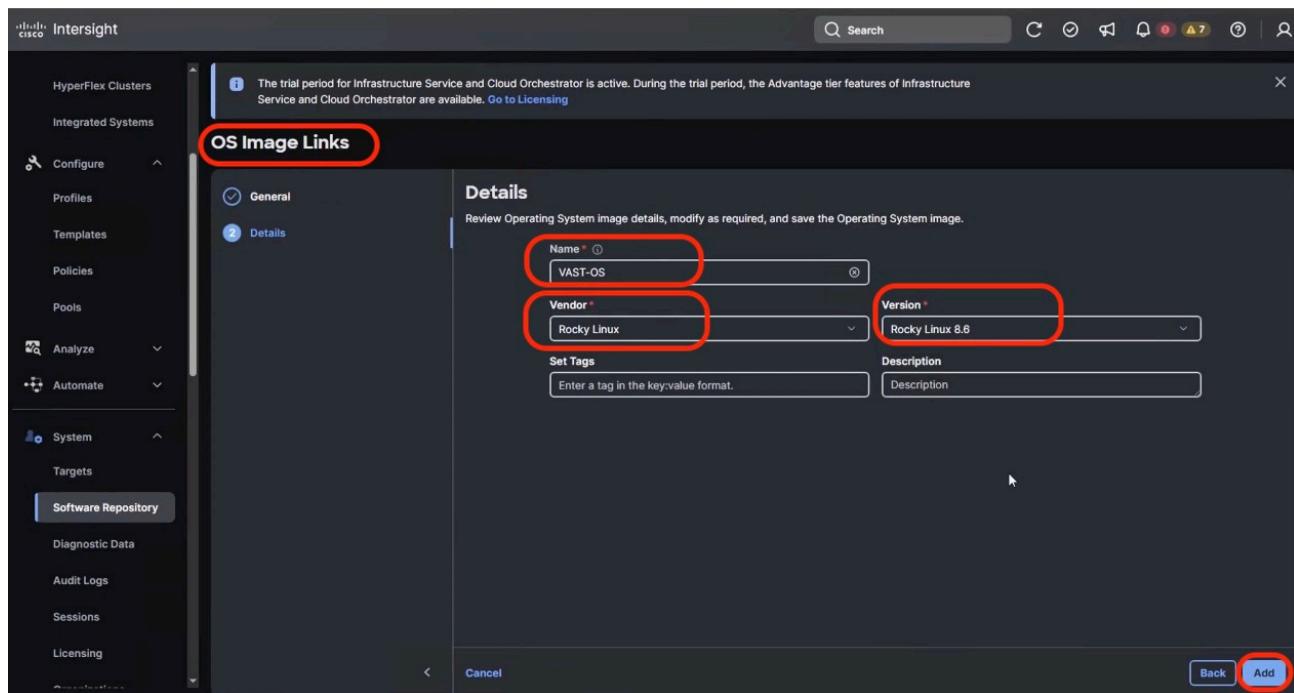
Note: Make sure the VAST operating system ISO is available from a local repository, for example an HTTPS/NFS/CIFS server. This is a one-time process for each version of the VAST OS ISO.

- 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.

The screenshot shows the Cisco Intersight Software Repository interface. The left navigation pane includes options like HyperFlex Clusters, Integrated Systems, Configure, Profiles, Templates, Policies, Pools, Analyze, Automate, and System. The main content area is titled "Software Repository" and has tabs for Firmware Links, OS Image Links (which is selected), SCU Links, and OS Configuration Files. A success message at the top right says "Successfully created VAST-OS." Below the tabs is a search bar and a "Filters" section. The main table displays "1 results" with columns: Name, Vendor, Version, File Location, Description, and Last Update. The single row in the table is highlighted with a red box. The table also includes an "Export" button and a "Rows per page" dropdown set to 10.

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.

The screenshot shows the Cisco Intersight Servers page. The left navigation pane is identical to the previous screenshot. The main content area is titled "Servers" and displays 12 results. It includes various metrics like Power, HCL Status, Bundle Version, Utility Storage, Firmware Version, and Models. Below these metrics is a table with columns: Health, Model, Management IP, Server Profile, Firmware Version, CPU Capacit., and UCS Domain. Two servers are listed: one healthy (UCSC-C225-M8N) and one with a warning (UCSC-C225-M8N). A context menu is open over the first server, showing options: Install Operating System, Upgrade Firmware, Start Alarm Suppression, Stop Alarm Suppression, and Set License Tier. The "Install Operating System" option is highlighted with a red box. The table includes "Show Selected" and "Unselect All" buttons at the bottom.

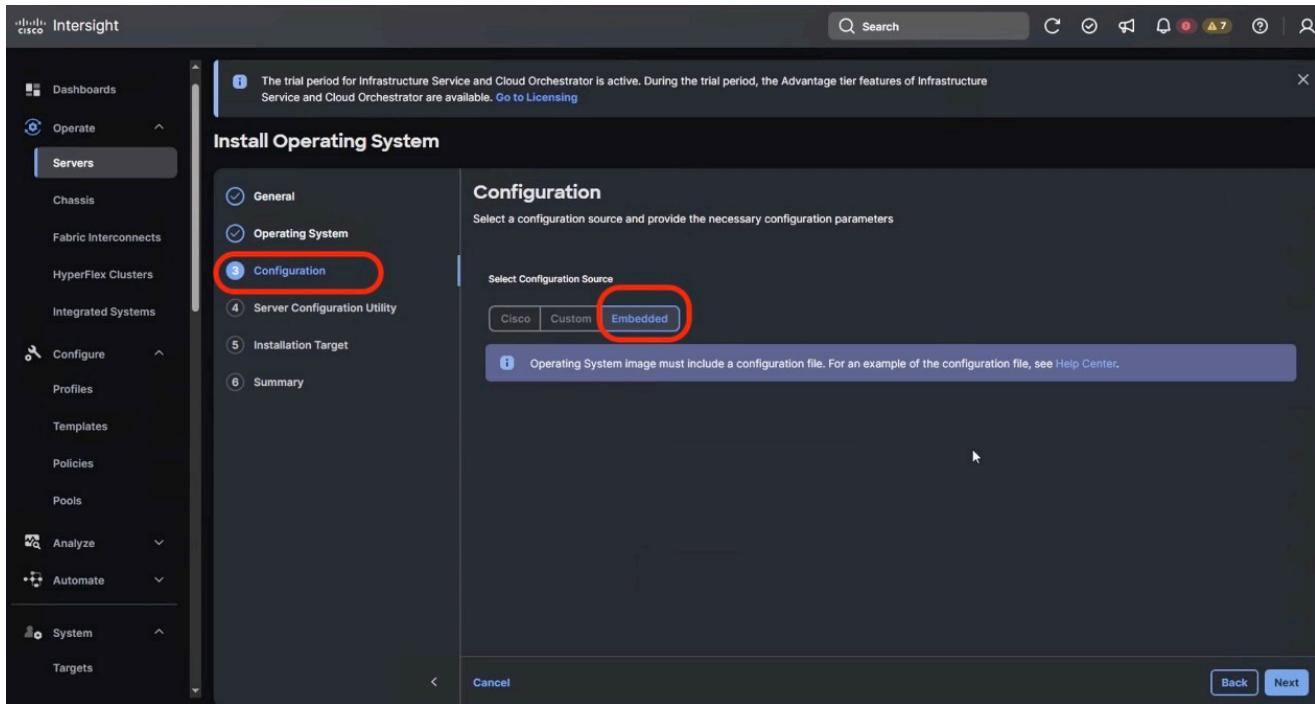
Step 9. Make sure the servers are already selected and click Next.

Name	User Label	Health	Model	Serial Number
C225-WZP2902...		Healthy	UCSC-C225-M8N	WZP290297MY
C225-WZP2902...		Warning	UCSC-C225-M8N	WZP290297N1
C225-WZP2902...		Healthy	UCSC-C225-M8N	WZP290297NK
C225-WZP2902...		Warning	UCSC-C225-M8N	WZP290297NS
C225-WZP2902...		Warning	UCSC-C225-M8N	WZP290297NU
C225-WZP2902...		Warning	UCSC-C225-M8N	WZP290297NZ
C225-WZP2902...		Healthy	UCSC-C225-M8N	WZP290297P0
C225-WZP2902...		Healthy	UCSC-C225-M8N	WZP290297P1
C225-WZP2902...		Healthy	UCSC-C225-M8N	WZP290297P5

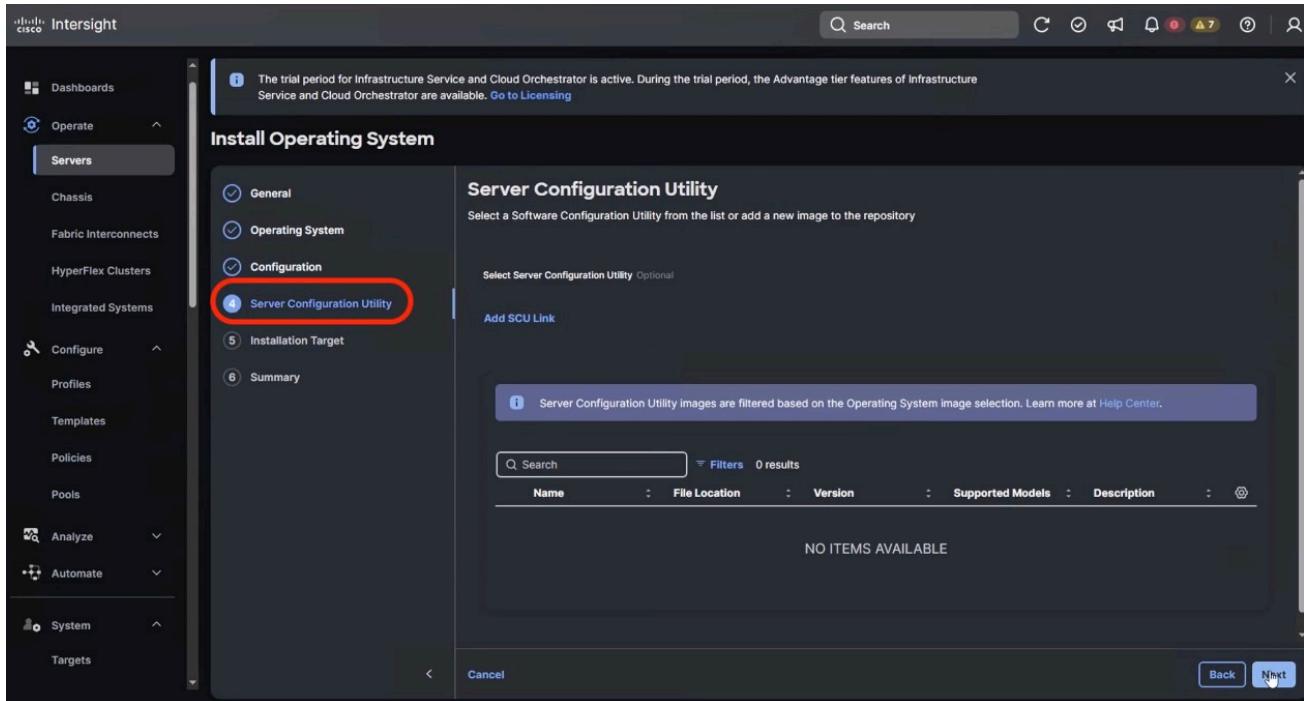
Step 10. Select the Operating System repository which was previously created with the VAST operating system ISO and click Next.

Name	File Location	Vendor	Version	Description
VAST-OS	https://10.108.1.8/vast-os	Rocky Linux	Rocky Linux 8.6	

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.

The trial period for Infrastructure Service and Cloud Orchestrator is active. During the trial period, the Advantage tier features of Infrastructure Service and Cloud Orchestrator are available. [Go to Licensing](#)

Install Operating System

Summary

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

Operating System Image

Name	VAST-OS	Version	Rocky Linux 8.6
Vendor	Rocky Linux		

Configuration

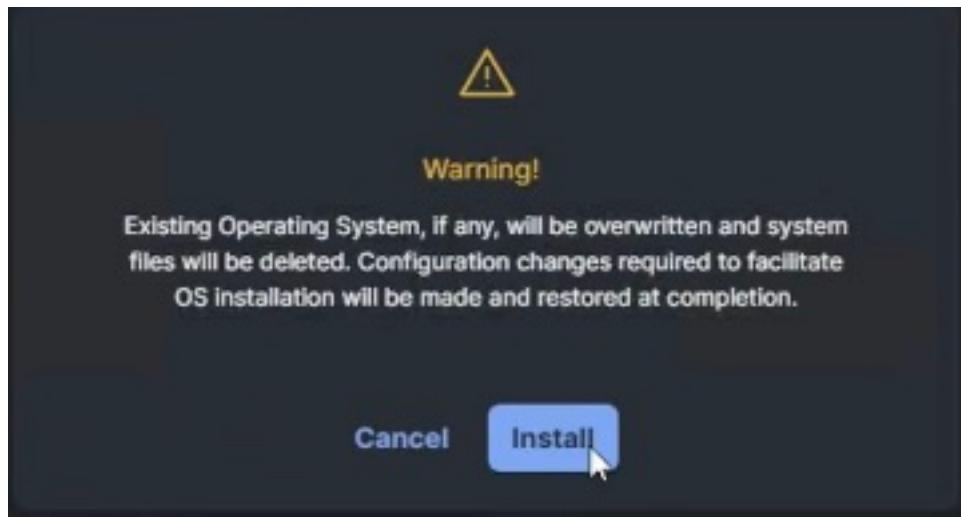
Configuration Source
Embedded

Selected Servers

C225-WZP290297MY Serial: WZP290297MY	View Details
C225-WZP290297N1 Serial: WZP290297N1	View Details
C225-WZP290297NK Serial: WZP290297NK	View Details

[Back](#) [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.

Operating System Install on Cisco UCS Server

Details

- Status: Success
- Name: InstallOSIMM
- ID: 6854801f696f6e3101ab8e03
- Target Type: Rack Server
- Target Name: C225-WZP290297MY
- Source Type: Rack Server
- Source Name: C225-WZP290297MY
- Initiator: andhiman@cisco.com
- Start Time: Jun 19, 2025 5:24 PM

Execution Flow

- Set Server Power State (Success) Jun 19, 2025 5:27 PM
- Set Server Boot Order (Success) Jun 19, 2025 5:27 PM
- Validate Mount Status (Success) Jun 19, 2025 5:27 PM
- Mount Virtual Media (Success) Jun 19, 2025 5:27 PM
- Validate Install Configuration (Success) Jun 19, 2025 5:27 PM
- Handle Staged Policies on Cisco UCS Server (Success) Jun 19, 2025 5:27 PM
- Validate Vmedia On Server (Success) Jun 19, 2025 5:26 PM
- Retrieve Server Configuration (Success) Jun 19, 2025 5:24 PM
- Process Workflow Input Task (Success) Jun 19, 2025 5:24 PM

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:

```

[ OK ] Started Setup Virtual Console.
[ OK ] Stopping iSCSI UserSpace L0 driver...
[ OK ] Closed Open-iSCSI iscsid Socket.
[ OK ] Stopped iSCSI UserSpace I/O driver.
[ OK ] Started Cleaning Up and Shutting Down Daemons.
[ OK ] Closed Open-iSCSI iscsiuiio Socket.
[ OK ] Started Plymouth switch root service.
[ OK ] Stopped udev Kernel Device Manager.
[ OK ] Stopped Hardware RNG Entropy Gatherer Daemon...
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create list of required statdevice nodes for the current kernel.
[ OK ] Stopped dracut pre-udev hook.
[ OK ] Stopped dracut cmdline hook.
[ OK ] Closed udev Kernel Socket.
[ OK ] Closed udev Control Socket.
[ OK ] Starting Cleanup udevd DB...
[ OK ] Stopped Hardware RNG Entropy Gatherer Daemon.
[ OK ] Started Cleanup udevd DB.
[ OK ] Reached target Switch Root.
[ OK ] Starting Switch Root...
[ OK ] Started Tell Plymouth To Write Out Runtime Data.
[ OK ] Started Rebuild Journal Catalog.
[ OK ] Started Import network configuration from initramfs.
[ OK ] Starting Create Volatile Files and Directories...
[ OK ] Started Create Volatile Files and Directories.
[ OK ] Started Update UTPM about System Boot/Shutdown...
[ OK ] Started Update UTPM about System Boot/Shutdown...
[ OK ] Started Rebuild Dynamic Linker Cache.
[ OK ] Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Reached target System Initialization.
[ OK ] Listening on Open-iSCSI isciuiio Socket.
[ OK ] Listening on D-Bus System Message Bus Socket.
[ OK ] Listening on Open-iSCSI iscsid Socket.
[ OK ] Reached target Sockets.
[ OK ] Reached target Basic System.
[ OK ] Starting OpenSSH ed25519 Server Key Generation...
[ OK ] Starting OpenSSH rsa Server Key Generation...
[ OK ] Starting Anaconda NetworkManager configuration...
[ OK ] Starting Hardware RNG Entropy Gatherer Wake threshold service...
[ OK ] Starting OpenSSH ecdsa Server Key Generation...
[ OK ] Starting Login Service...
[ OK ] Starting Terminate Plymouth Boot Screen...
[ OK ] Started Daily Cleanup of Temporary Directories.
[ OK ] Reached target Timers.
[ OK ] Starting pre-anaconda logging service...
[ OK ] Starting Hold until boot process finishes up...

```

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

The screenshot shows the Cisco Intersight KVM Console interface. The left sidebar contains navigation links: Console, File, View, Macros, Tools, Power, Boot Device, Virtual Media, and Chat. The 'Power' link is currently selected. The main pane displays a terminal session on a Rocky Linux 8.6 node. The session output includes:

```

Rocky Linux 8.6 (Green Obsidian)
Kernel 4.18.0-425.13.1.el8.ciqfipscompliant.37.1.x86_64 on an x86_64
localhost login: vastdata
Password:
Last login: Thu Jul 10 23:58:08 GMT 2025 on tty1
Last login: Tue Jul 15 03:19:58 GMT 2025 on tty1
Last login: Tue Jul 15 03:19:58 on tty1
[vastdata@localhost ~]$ 

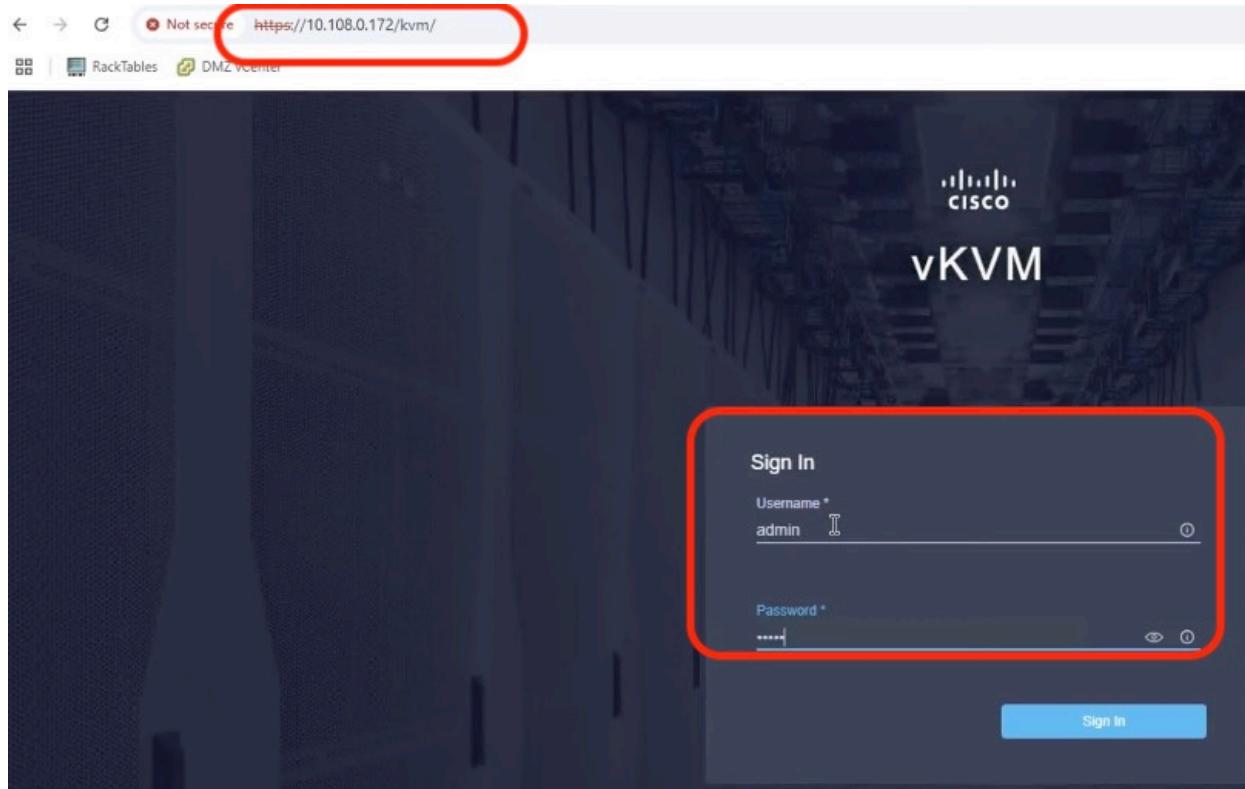
```

Procedure 2. Install the VAST OS through virtual media

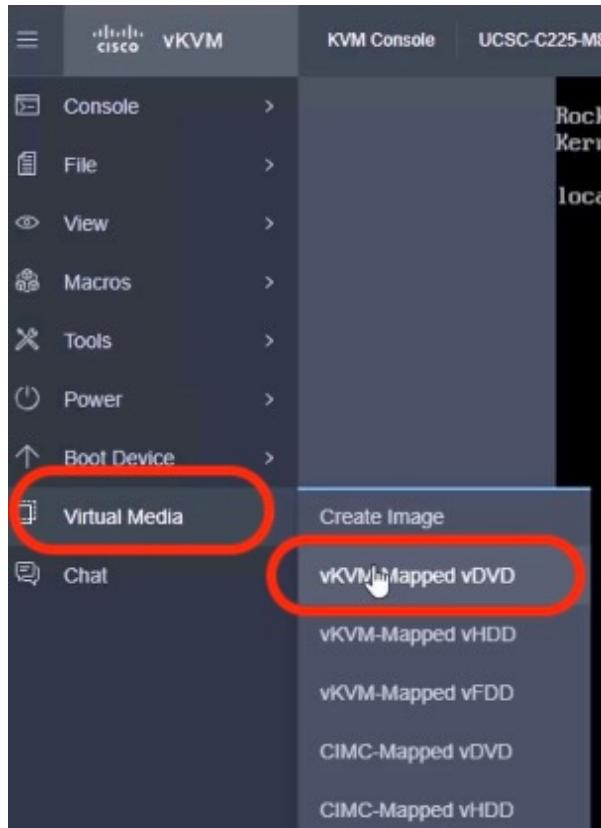
This procedure expands on the process to install the operating system through virtual media. You need to open a virtual KVM session for each node. Virtual KVM session can be accessed through Cisco Intersight or logging into node CIMC IP. During the OS installation, it is recommended to open vKVM through 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>)



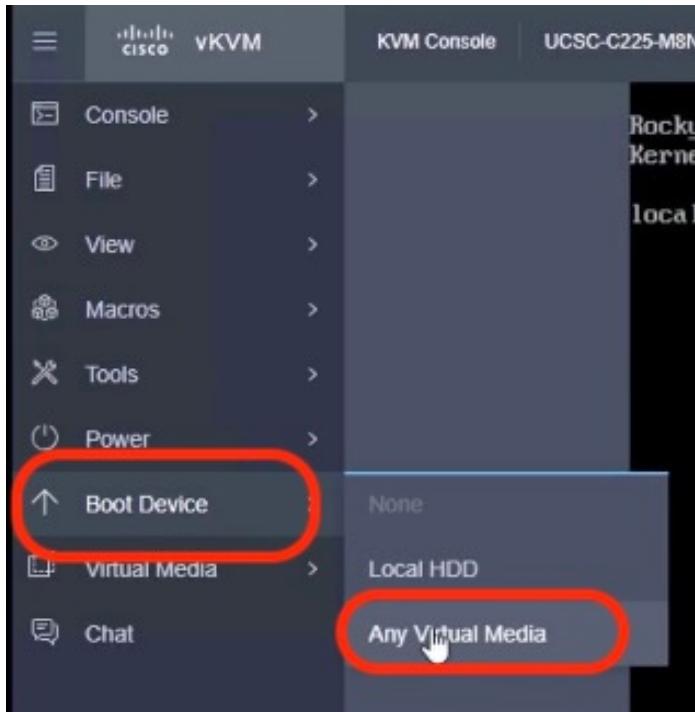
Step 3. On KVM screen, navigate to Virtual Media → vKVM Mapped vDVD



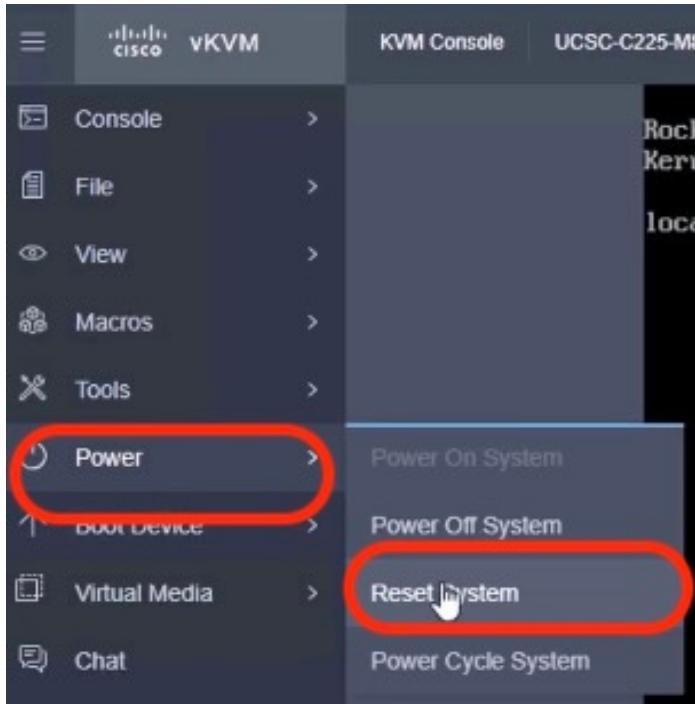
Step 4. Select the VAST operating system ISO from your local file system and click Map Drive.



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 boot 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](#)
- [Appendix B – References Used in Guide](#)
- [Appendix C – Known Issues and Workarounds](#)
- [Appendix D-Sample Network configuration for split network deployment](#)

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'.

Name	Disk Firmware Version	Size (MiB)	PID	Part Nu...	Serial
FRONT-NVME-1	E2XC000	915715	UCS-NVB960MTH	16-102...	MSA291500DG
FRONT-NVME-10	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4241004B15PHGN
FRONT-NVME-2	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4241005015PHGN
FRONT-NVME-3	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4241002Z15PHGN
FRONT-NVME-4	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4241004915PHGN
FRONT-NVME-5	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4241008N15PHGN
FRONT-NVME-6	E2XC000	915715	UCS-NVB960MTH	16-102...	MSA291500DK
FRONT-NVME-7	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4234003V15PHGN
FRONT-NVME-8	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4234005X15PHGN
FRONT-NVME-9	N/A	14651290	UCS-NVMEQ-1536	16-101...	PHAC4234004L15PHGN

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 queueing ROCE_QUEUEING_OUT
  class type queueing 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 queueing c-out-8q-q2
  bandwidth remaining percent 0
class type queueing c-out-8q-q1
  bandwidth remaining percent 0
class type queueing c-out-8q-q-default
  bandwidth remaining percent 50
!
system qos
  service-policy type network-qos ROCE_NETWORK_POLICY
  service-policy type queueing output ROCE_QUEUEING_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 queueing ROCE_QUEUING_OUT
  class type queueing c-out-8q-q3
    bandwidth remaining percent 50
    random-detect minimum-threshold 150 kbytes maximum-threshold 3000 kbytes drop-probability 7 weight 0ecn
  class type queueing c-out-8q-q2
    bandwidth remaining percent 0
  class type queueing c-out-8q-q1
    bandwidth remaining percent 0
  class type queueing c-out-8q-q-default
    bandwidth remaining percent 50
!
system qos
  service-policy type network-qos ROCE_NETWORK_POLICY
  service-policy type queueing 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
!

```