

Build a Scalable Storage Infrastructure with Cisco UCS and Cisco Intersight



This document describes how to use the Cisco Unified Computing System™ (Cisco UCS®) together with the Cisco Intersight™ platform to build a scale-out storage infrastructure. This guide provides an overview of the design and deployment of a software-defined storage solution using Cisco UCS and a Cisco Intersight virtual appliance.

Contents

- Executive summary 3
- Introduction..... 3
- Software-defined storage solution with Cisco UCS and Cisco Intersight 5
 - Validated computing design 6
- Deploying Cisco Intersight and Cisco UCS for software-defined storage 7
 - Install and configure the Cisco Intersight virtual appliance on VMware vSphere..... 7
 - Claim a Cisco IMC device with Cisco Intersight appliance 13
 - Configure policies for scale-out storage 16
 - Policy type: Adapter 16
 - Policy type: Boot order 17
 - Policy type: Disk group 18
 - Policy type: Ethernet adapter..... 18
 - Policy type: Ethernet network 19
 - Policy type: Ethernet quality of service 19
 - Policy type: LAN connectivity 20
 - Policy type: Network Time Protocol 21
 - Policy type: Storage..... 21
 - Policy type: Virtual media..... 22
 - Create and deploy server profiles for scale-out storage 23
- Conclusion 24
- For more information..... 24

Executive summary

This document describes how to use the Cisco Intersight™ and Cisco Unified Computing System™ (Cisco UCS®) platforms to deploy a software-defined storage solution without using Cisco UCS fabric interconnects. This design and deployment guide provides the framework for deploying a software-defined storage solution on Cisco UCS C240 rack servers. Cisco UCS provides computing, network, and storage components as a unified platform for software-defined storage solutions. Cisco Intersight software is Cisco's systems management platform that delivers intuitive computing through cloud-powered intelligence. Cisco Intersight software provides infrastructure management for the Cisco UCS and Cisco HyperFlex™ platforms.

Introduction

Software-defined storage replaces traditional, purpose-built storage. It can be managed as a single platform and automates delivery of services based on built-in intelligence and best practices. The preconfigured, standardized storage components that are typical of today's software-defined storage solutions deliver many of the same task-specific capabilities as standalone systems. They just use a different approach to get there: a faster, easier, more cost-effective approach that relies on software-based specialization and automation to meet different requirements quickly and economically. This approach leads to more consistent, predictable storage solutions that don't require proprietary expertise to build or maintain them.

Today many storage solutions don't address the diversity of the underlying hardware. They just define the various components that are part of the overall solution and assume that the IT engineer can build that overall solution in a professional manner. Almost all software-defined storage solutions use standardized server hardware with local storage. Configuring and building such a solution doesn't appear to be especially complex when considering the hardware for a single server, but the process can be time-consuming and complicated when a solution consists of tens or hundreds of such servers. At scale, a manual process is prone to errors and does not provide a simple way to reliably build a flexible and simplified storage solution.

From the beginning, Cisco UCS was designed with the entire state of each server—identity, configuration, and connectivity—abstracted into software. This foundation makes the system 100 percent programmable and easy to adapt to the requirements of both modern workloads and traditional monolithic business applications. With a completely programmable system, your clients get the level of control they need to manage their workloads. Cisco Intersight software helps precisely align the infrastructure with the needs of the business. It enables administrators to automate configurations or tasks based on specific requirements that are tied to business objectives and application performance. Rather than having to be concerned with every detail of system configuration, intent-based management describes the accomplishment. The policy-based approach to management provides the simplicity, automation, and capabilities needed to increase productivity and support a fast-paced business environment.

Cisco UCS is the only system designed from the beginning to enable every aspect of system personality, configuration, and connectivity to be abstracted from the hardware and configured through software. This foundation makes Cisco UCS a fully composable infrastructure. With everything from firmware revisions to network profiles abstracted into more than 125 configuration variables that fully specify each server, the system is, essentially, stateless.

Cisco UCS can solve the problem of complex configurations and installations for software-defined storage infrastructure through several approaches:

- Cisco® fabric interconnects plus Cisco UCS Manager
- Cisco UCS Unified API
- Cisco Intersight software

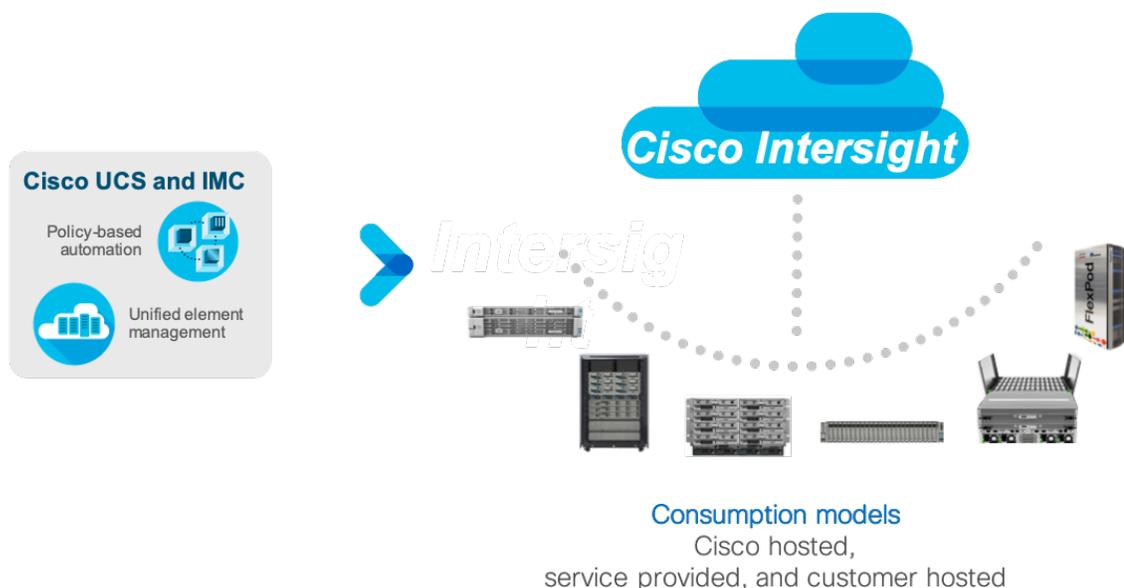
The first two approaches have been demonstrated in many solutions and documentation since Cisco UCS was released 10 years ago. The combination of Cisco Intersight software, Cisco UCS, and software-defined storage provides a new approach that can deliver the same benefits, building a flexible and simplified storage solution. Cisco Intersight software helps you build policies for the overall storage infrastructure and summarize them in a service profile. The service profiles can then be assigned to servers to

configure them to support the storage infrastructure. This approach can significantly reduce the amount of time needed to set up a software-defined storage environment, especially for larger environments.

Cisco Intersight software provides infrastructure management for the Cisco UCS and Cisco HyperFlex platforms. It offers intelligent management that enables IT organizations to analyze, simplify, and automate their environments in more advanced ways than with previous generations of tools.

Figure 1 shows the Cisco Intersight consumption model.

Figure 1. Cisco Intersight consumption model



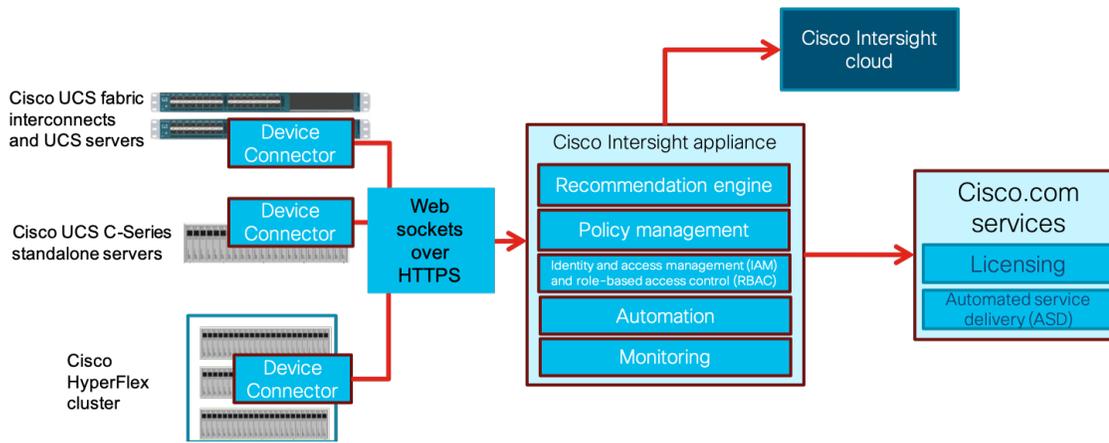
The Cisco Intersight virtual appliance delivers the management features of the Cisco Intersight software for the Cisco UCS and Cisco HyperFlex platforms in an easy-to-deploy VMware open virtual appliance (OVA) file that allows you to determine which system details leave your premises. The virtual appliance form factor meets additional data locality, security, and compliance needs that are not completely met through the Intersight.com website. The Cisco Intersight virtual appliance requires a connection back to Cisco and Cisco Intersight services for updates and to access required services to unlock the full capabilities of Intersight.com. The Cisco Intersight software monitors the health and relationships of all the physical and virtual infrastructure components. Telemetry and configuration information is collected and stored in accordance with Cisco's information security requirements. The data is isolated and displayed through an intuitive user interface. The virtual appliance feature enables users to specify which data is sent back to Cisco with a single point of egress from the customer network.

Data sheets about Cisco Intersight software and Cisco Intersight privacy can be found here:

- Cisco Intersight data sheet: <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/intersight/datasheet-c78-739433.html>
- Cisco Intersight privacy data sheet: <https://www.cisco.com/c/en/us/products/collateral/switches/asset-management-suite/datasheet-c78-741197.html>

Figure 2 shows the architecture of the Cisco Intersight virtual appliance.

Figure 2. Cisco Intersight appliance architecture



Software-defined storage solution with Cisco UCS and Cisco Intersight

This Cisco Intersight design provides a comprehensive architecture for deploying software-defined storage on Cisco UCS C240 servers in infrastructure made possible by Cisco Intersight software and Cisco Nexus® 9336C-FX2 Switches.

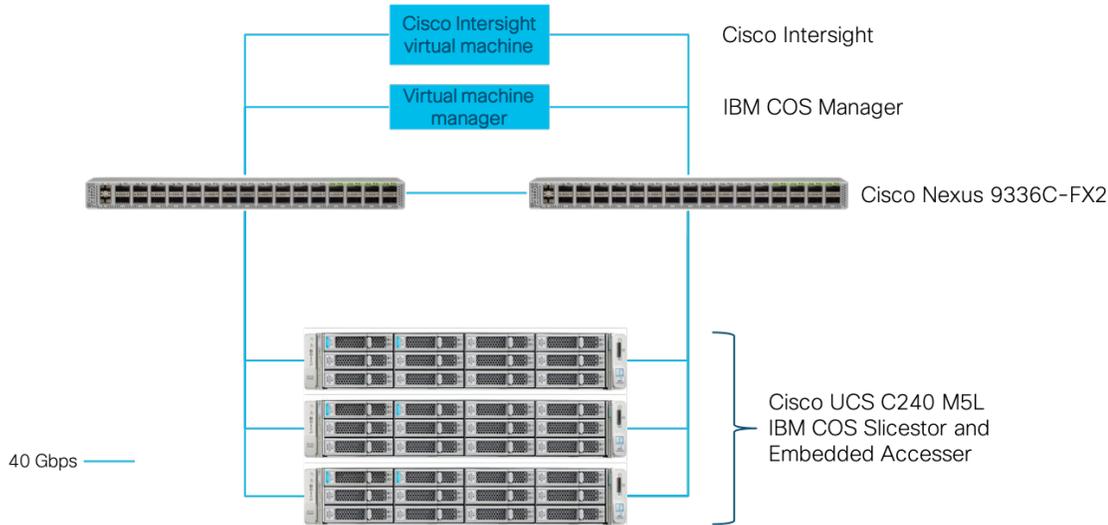
One of the primary design goals of this scale-out architecture was to deploy all elements on 40 Gigabit Ethernet networking end to end using Cisco Intersight software. The whole solution uses the robust throughput and low latency provided by the Cisco Nexus 9336C-FX2. Additionally, software-defined storage takes advantage of the flexibility provided by the stateless nature of Cisco UCS service profiles within the Cisco Intersight solution.

This design uses the Cisco Nexus 9000 Series Switches in Cisco NX-OS Software standalone mode (NX-OS mode), but it provides investment protection through the capability to migrate to Cisco Application Centric Infrastructure (Cisco ACI™) or higher network bandwidths (1, 10, 25, 40, 50, or 100 Gbps). It also enables innovative analytics and visibility using the Cisco Tetration Analytics™ platform and automation, with in-device and off-device Python scripting and Cisco Open NX-OS, supporting Dev/Ops tools (such as Chef, Puppet, and Ansible).

The example used here to demonstrate the design and deployment of software-defined storage infrastructure with Cisco Intersight software on Cisco UCS uses IBM Cloud Object Storage (COS) software deployed on the Cisco UCS C240 M5L Rack Server to show how such a solution can be built. Figure 3 shows the design. Other software-defined storage solutions can be designed in a similar way.

The example here focuses on the configuration of the IBM COS Slicestor modules. The installation of the virtual IBM COS Manager appliance is not covered in this document.

Figure 3. Design of IBM COS with Cisco UCS C240 M5L and Cisco Intersight software



- Cisco Intersight software deployed as a virtual machine OVA file
- IBM COS Manager instance deployed as virtual machine OVA file
- IBM COS Embedded Accesser deployed on IBM COS Slicestor
- IBM COS Slicestor deployed on Cisco UCS C240
- Cisco UCS C240 connected to Cisco Nexus 9336C-FX2 with 40-Gbps line speed

Each Cisco UCS C240 rack server is equipped with a Cisco UCS virtual interface card (VIC) supporting dual 40-Gbps fabric connectivity. The Cisco UCS VICs eliminate the need for separate physical interface cards on each server for data and management connectivity. For this solution with IBM COS ClevOS, the VIC is configured with two virtual network interface cards (vNICs): one on each physical VIC interface. IBM COS is configured to use these two vNICs to provide operational active backup redundancy in software.

Validated computing design

The connectivity of the solution is based on 40 Gbps. All components are connected together through 40-Gbps Quad Small Form-Factor Pluggable (QSFP) cables except the virtual IBM COS Manager node and the Cisco Intersight virtual appliance, which use a 10-Gbps connectivity. Between both Cisco Nexus 9336C-FX2 Switches are two 40-Gbps cables. Each Cisco UCS C240 M5L Rack Server is connected with a single 40-Gbps cable to each Cisco Nexus switch.

Cisco UCS provides redundancy at the component and link levels and end-to-end path redundancy to the LAN. The Cisco UCS C240 server is highly redundant, with redundant power supplies and fans. Each server is deployed using vNICs that provide redundant connectivity through Link Access Control Protocol (LACP) at the OS level. This setup is used for all IBM COS Slicestor with Embedded Accesser node vNICs. Each IBM COS Slicestor with Embedded Accesser node is configured in mode 1, with active backup LACP bonding, at the ClevOS layer.

Deploying Cisco Intersight and Cisco UCS for software-defined storage

The deployment of the whole solution consists of several main steps:

1. Install the Cisco Intersight virtual appliance on VMware vSphere.
2. Configure the Cisco Intersight virtual appliance.
3. Claim a Cisco Integrated Management Controller (IMC) device.
4. Configure server policies and profiles.
5. Deploy server profiles.

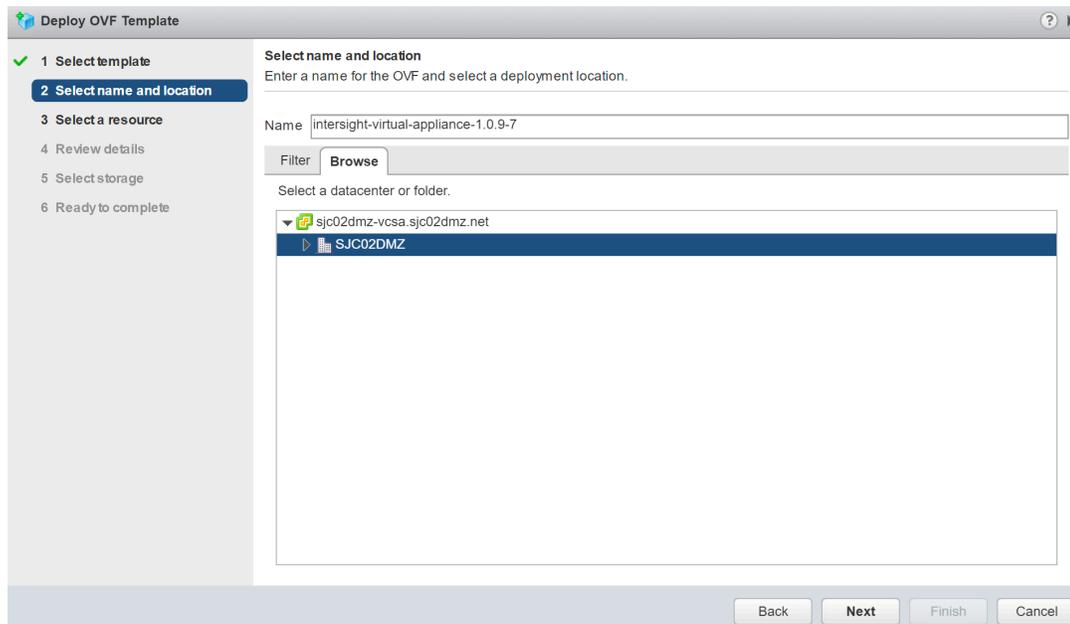
The configuration of the Cisco IMC is not covered in this deployment guide, because the IMC is assumed to be already configured on each server.

Install and configure the Cisco Intersight virtual appliance on VMware vSphere

To deploy the Cisco Intersight virtual appliance on VMware vCenter, follow these steps:

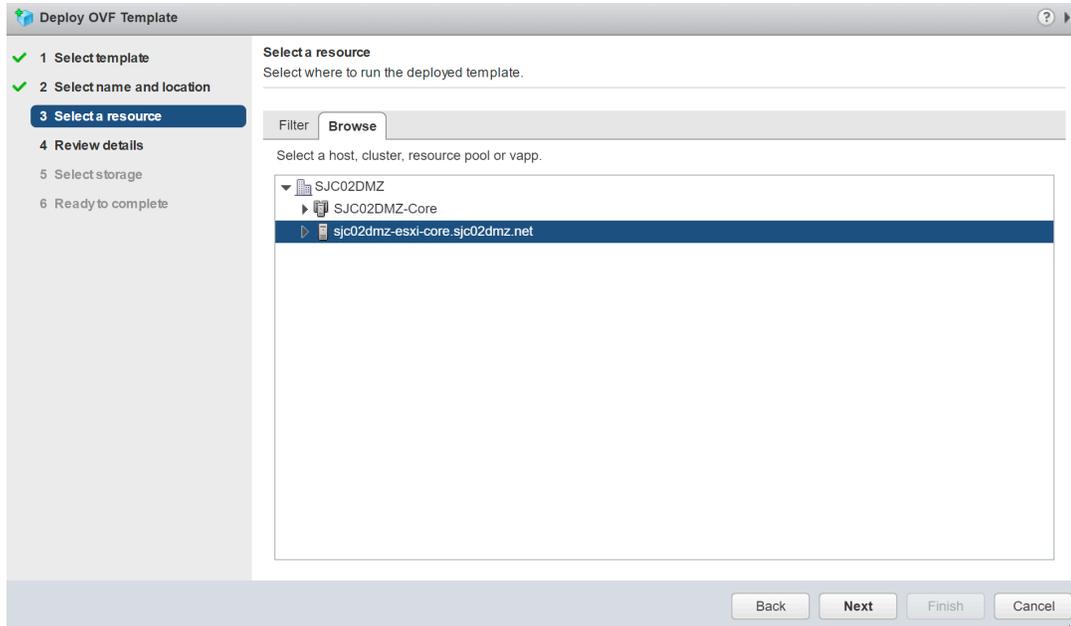
1. Log in to your local vCenter and select the VMware ESXi host that you want to use for deploying the virtual appliance.
2. Under Actions, choose Deploy OVF Template.
3. Select the template intersight-virtual-appliance-1.0.9-7.ova on your local file system and then click Next to select your data center (Figure 4).

Figure 4. Data center in which the appliance is located



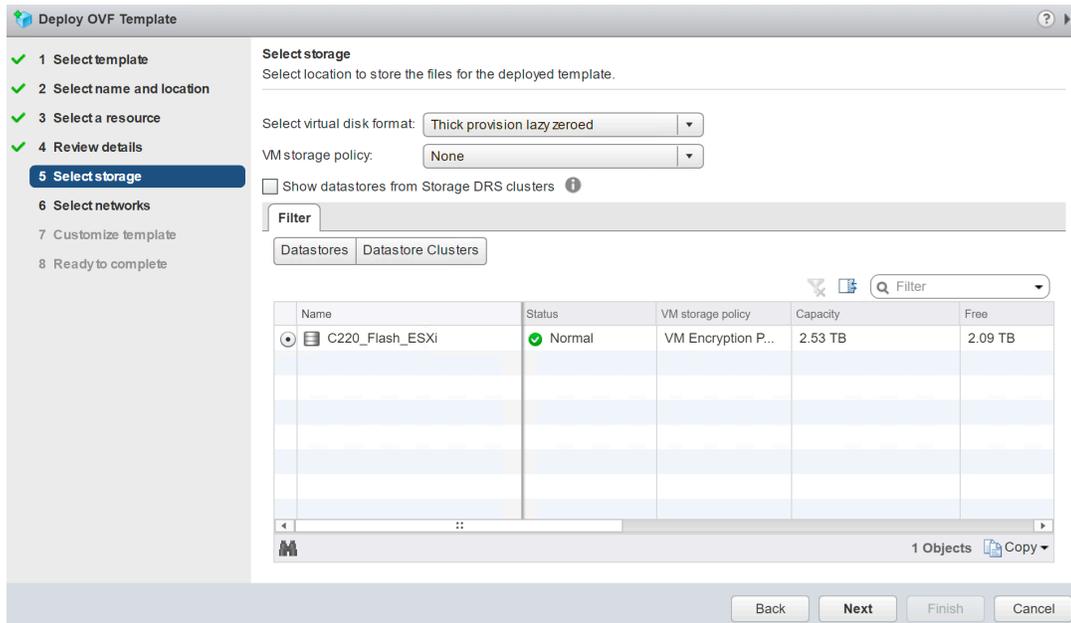
4. Click Next to choose the resource for the appliance and then click Next again (Figure 5).

Figure 5. Resource for the appliance



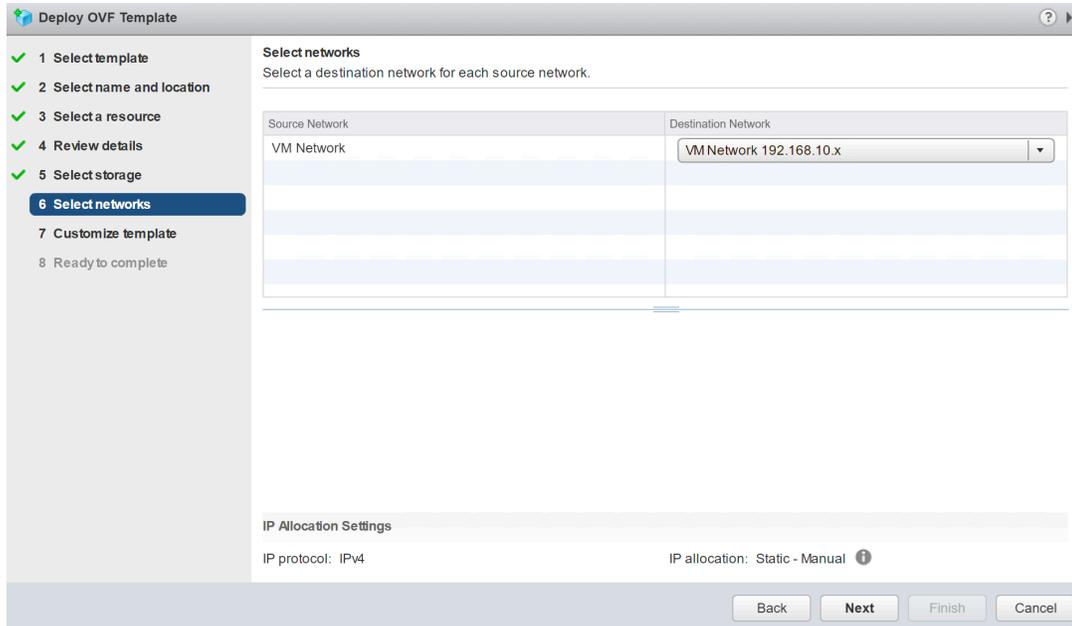
5. Review the details and click Next to select the storage location (Figure 6).

Figure 6. Select the storage location



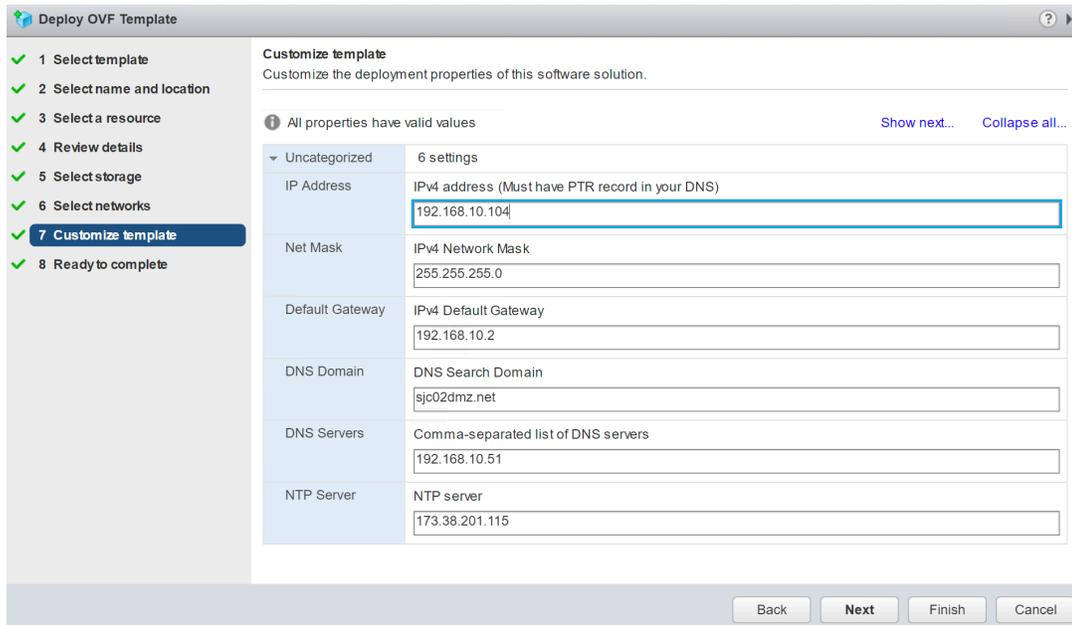
6. Click Next and select the network for the virtual appliance (Figure 7).

Figure 7. Select the network to use for the virtual appliance



7. Click Next and fill in all the data you need for the virtual appliance (Figure 8).

Figure 8. Customizing the template for the virtual appliance

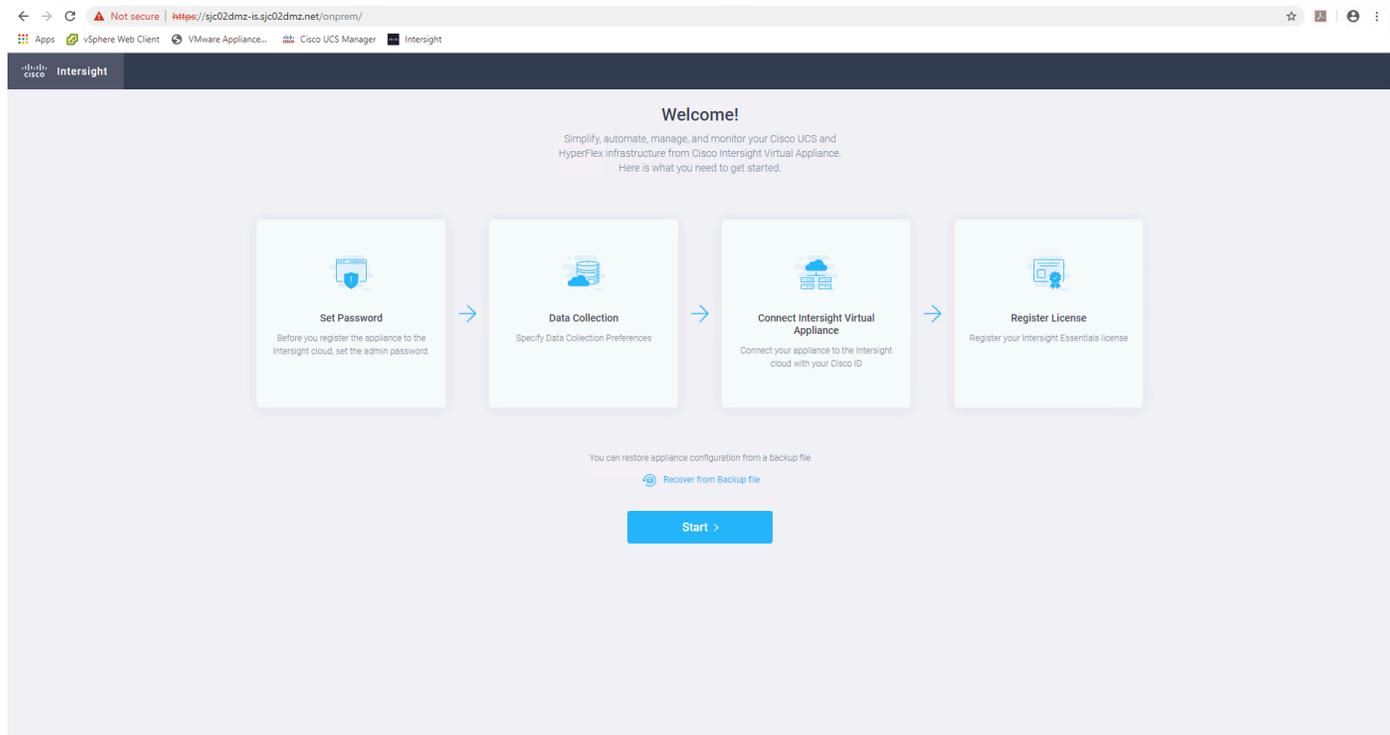


8. Review the final screen and deploy the OVA file.

9. When the deployment is complete, click the virtual appliance and power it on.

10. After 10 or 15 minutes, connect in a browser to the Cisco Intersight virtual appliance by typing the full domain name you configured in your Domain Name System (DNS). The example here uses the domain `sjc02dmz-is.sjc02dmz.net`¹ (Figure 9).

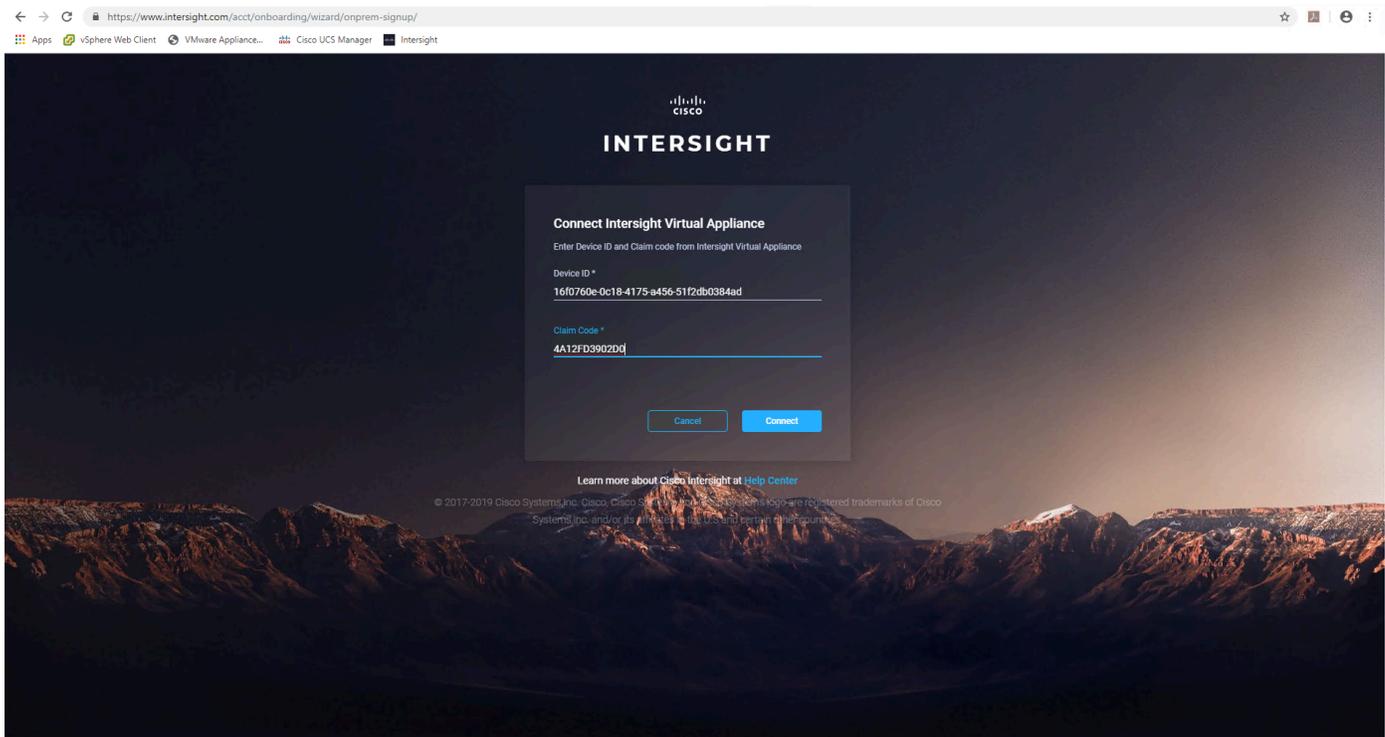
Figure 9. Connect to the virtual appliance in a browser



11. Click Start to begin configuring the virtual appliance.
12. Set the password and click Continue.
13. If you want Cisco to collect data from the Cisco Intersight appliance, click Continue. Otherwise, change the option.
14. Register the appliance by clicking Connect Intersight Virtual Appliance. A new browser tab opens. Click Continue.
15. Register using your Cisco credentials.
16. Read the offer description and scroll to the end. Click Accept and then click Next.
17. Enter your device ID and claim code (Figure 10).

¹ Make sure you have an alias DNS configured, which starts with `dc-` and links to the same IP address as the main fully qualified domain name (FQDN) for the appliance. The example here uses `dc-sjc02dmz-is.sjc02dmz.net`.

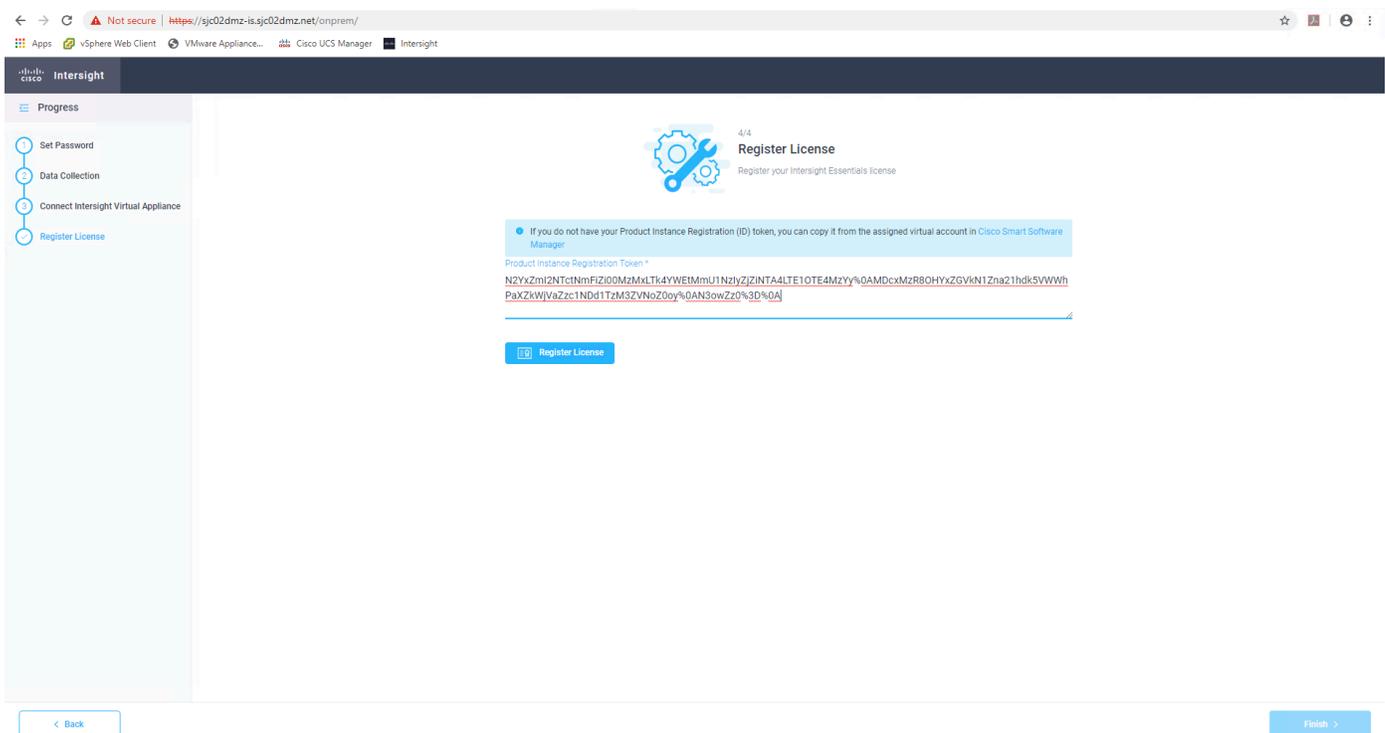
Figure 10. Register device and claim code



18. Click Close, and on the original browser tab click Continue.

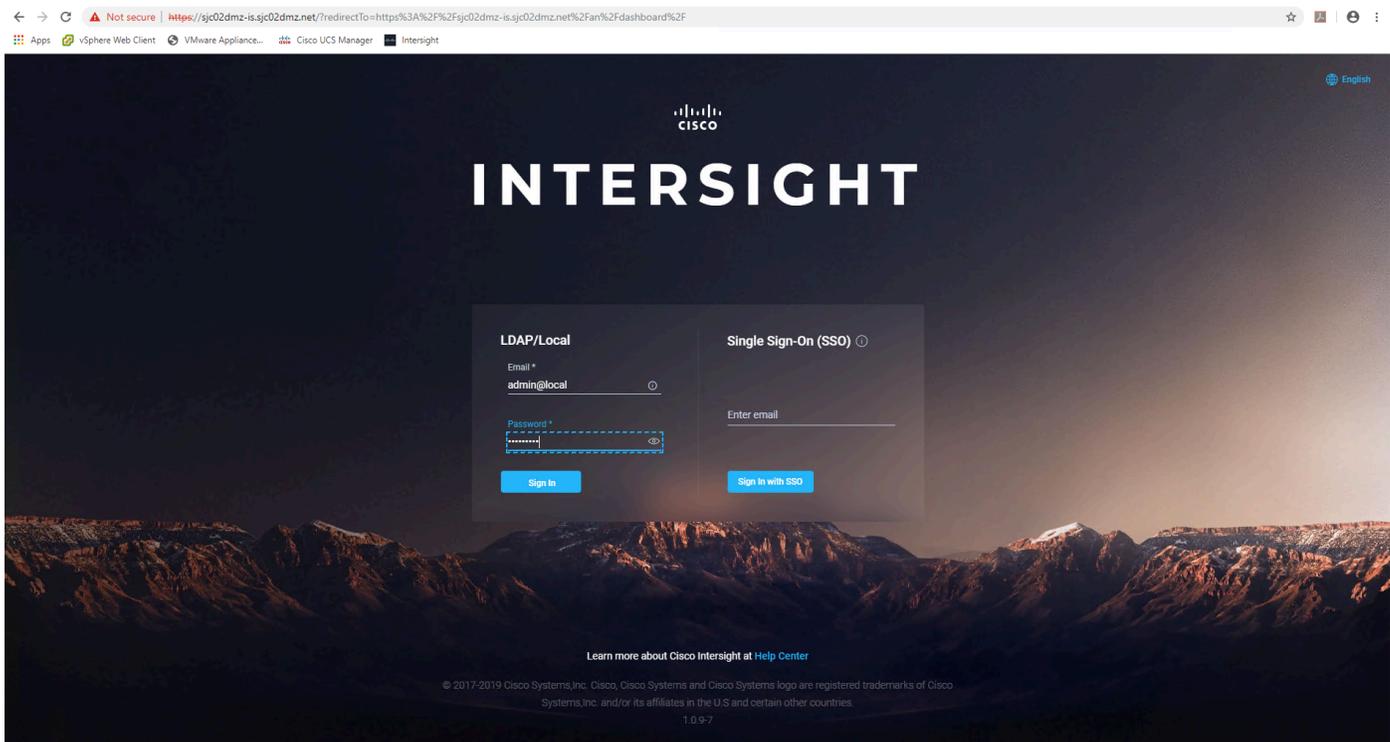
19. Register your appliance with a license (Figure 11).

Figure 11. Appliance license registration



20. After the registration process ends successfully, click Close.
21. Log in to the appliance by entering the DNS name in the browser (Figure 12).

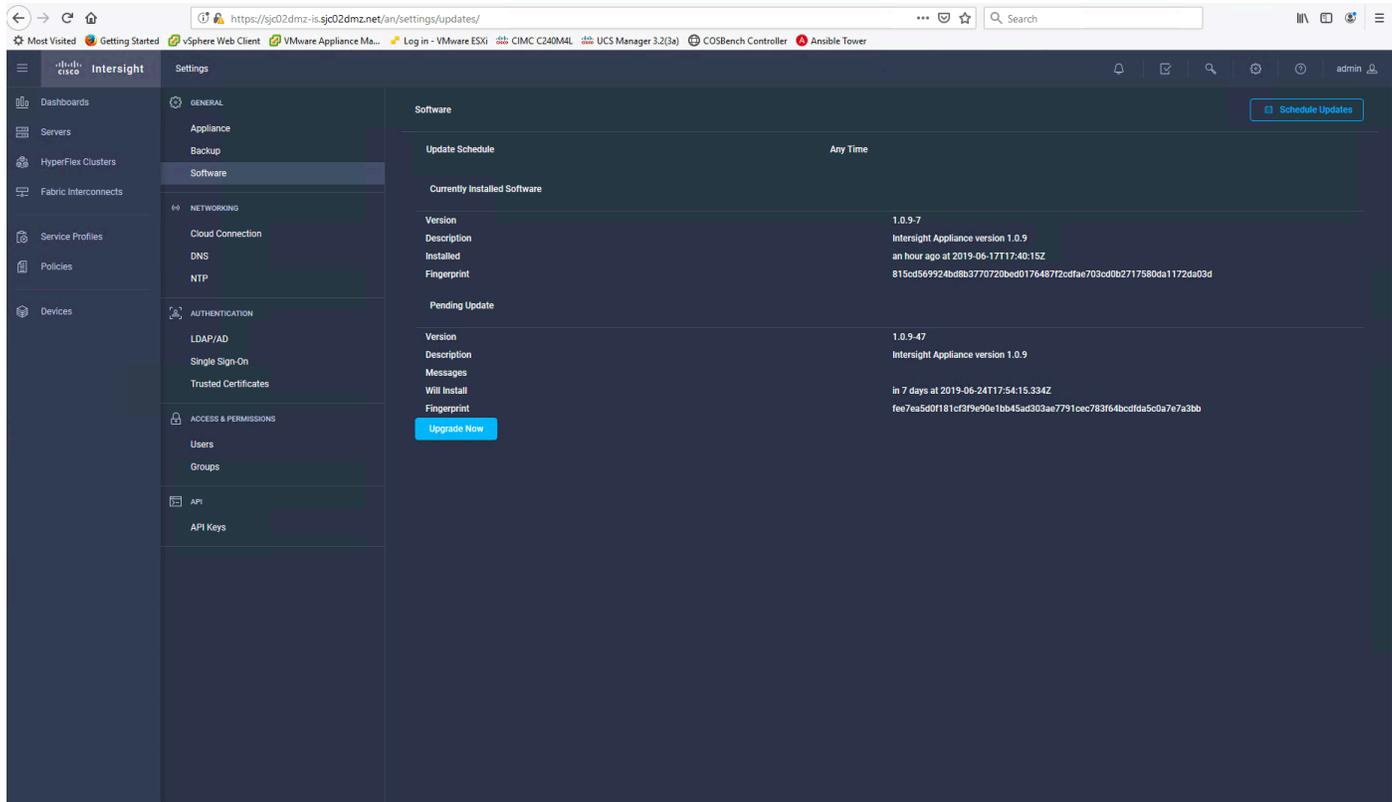
Figure 12. Log in to the Cisco Intersight appliance



22. Choose Settings > Settings in the top menu bar.

23. Under General, click Software and click Update Now. The Update process starts and finishes after a while (Figure 13).

Figure 13. Update Software



The installation and basic configuration are now finished. In the next steps, you claim the devices and configure the policies and server profiles for a three-node Cisco UCS C240 M5L scale-out storage environment.

Claim a Cisco IMC device with Cisco Intersight appliance

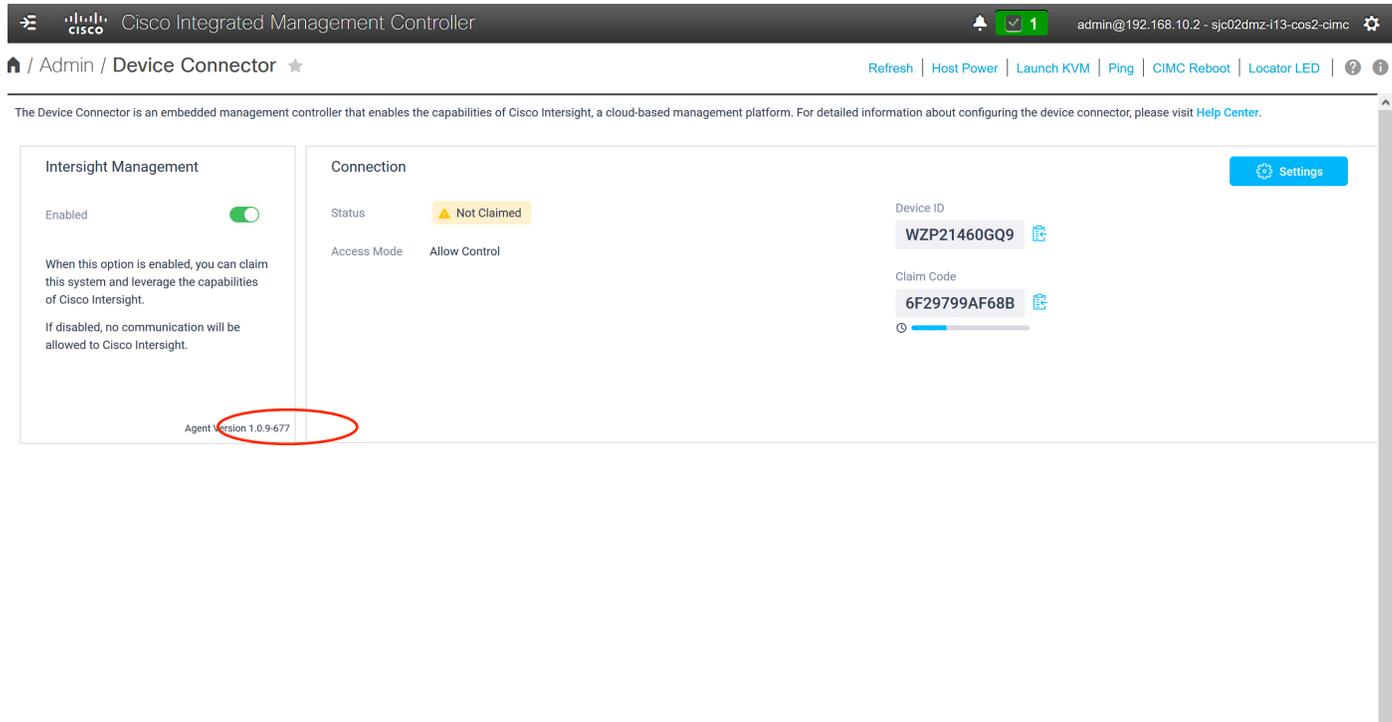
In the next task, you claim a Cisco IMC device with the Cisco Intersight appliance. Before you claim the device, you should perform a preliminary check of the Cisco Intersight device connector in the IMC. The current device connector requirements are described in https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/b_Cisco_Intersight_Appliance_Install_and_Upgrade_Guide_chapter_010.pdf and summarized in Table 1.

Table 1. Device connector requirements

Component	Minimum software version	Supported device connector version	Releases that include supported device connectors
Cisco UCS Manager	3.2(l)	1.0.9-2290	4.0(2a) or later
Cisco IMC Supervisor	For M5 servers: 3.1(3a) For M4 servers: 3.0(4)	1.0.9-335	4.0(2c) or later
Cisco HyperFlex Connect and Cisco HyperFlex HX Data Platform	2.6	1.0.9-1335	3.5(2a) or later

1. To verify the current version of the device connector in the Cisco IMC, log on to the IMC and from the top-left menu choose Admin > Device Connector. The red circle in the Figure 14 shows the device connector version.

Figure 14. Device Connector screen in Cisco IMC



2. Make sure that Intersight Management is enabled.
3. If the device connector does not meet the requirements, follow the steps described in https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Cisco_Intersight_Appliance_Getting_Started_Guide/b_Cisco_Intersight_Appliance_Install_and_Upgrade_Guide_chapter_010.pdf, page 1.
4. After verifying and, if necessary, upgrading the device connector, log on to the Cisco Intersight appliance. From the Cisco Intersight dashboard, choose Devices > Claim a New Device.
5. From the drop-down list, choose the device type Integrated Management Controller.
6. Enter the IP address and host name of the device that you want to claim.
7. Enter the user name for the device. This user must have administrative privileges.
8. Enter the password for the user. The click Claim to initiate device claiming (Figure 15).

Figure 15. Claiming a Cisco IMC device

Claim a New Device

Device Type *
Integrated Management Controller (IMC) ▾

IP/Hostname *
sjc02dmz-i13-cos2-cimc.sjc02dmz.net

Username *
admin

Password *
●●●●●●●●

Cancel Claim

The device claim process could take a few minutes. If required, the device connector will automatically be upgraded as part of the process.

9. Repeat the same steps for the other two Cisco UCS C240 M5L devices.

After you claim all three devices, you should see the devices under the server tab on the left (Figure 16).

Figure 16. Server summary

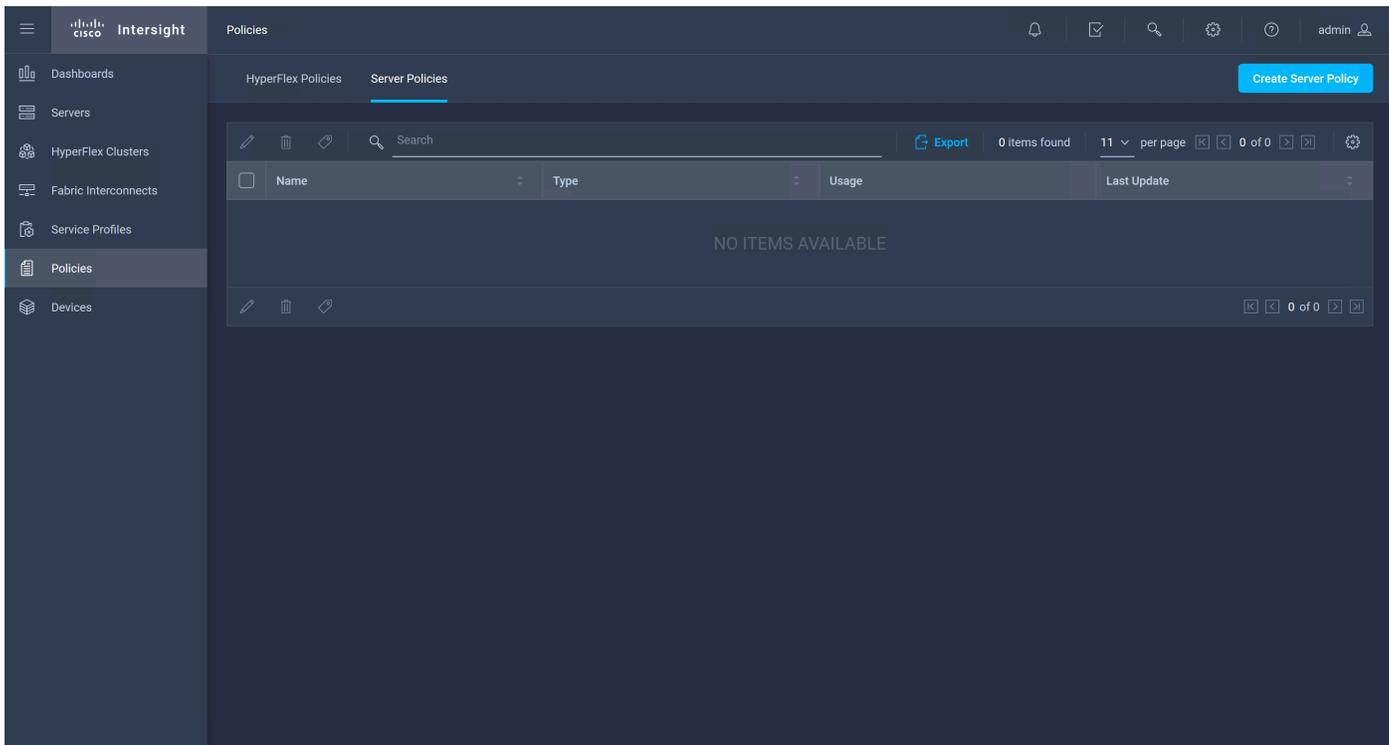
Name	Health	Managemen...	Model	CPU...	Memory ...	CPUs	CPU Cores	Firmware...
sjc02dmz-i13-cos2-cimc	Healthy	192.168.10.151	UCSC-C240-M5L	20.4	256.0	2	12	4.0(4e)
sjc02dmz-i13-cos3-cimc	Healthy	192.168.10.152	UCSC-C240-M5L	20.4	256.0	2	12	4.0(4e)
sjc02dmz-i13-cos4-cimc	Healthy	192.168.10.153	UCSC-C240-M5L	20.4	256.0	2	12	4.0(4e)

Configure policies for scale-out storage

This scale-out storage example uses a three-node IBM COS cluster. You need to configure the necessary server policies.

1. Log in to the Cisco Intersight appliance and select Policies at the left and then Server Policies at the top.
2. To create a server policy, click Create Server Policy (Figure 17).

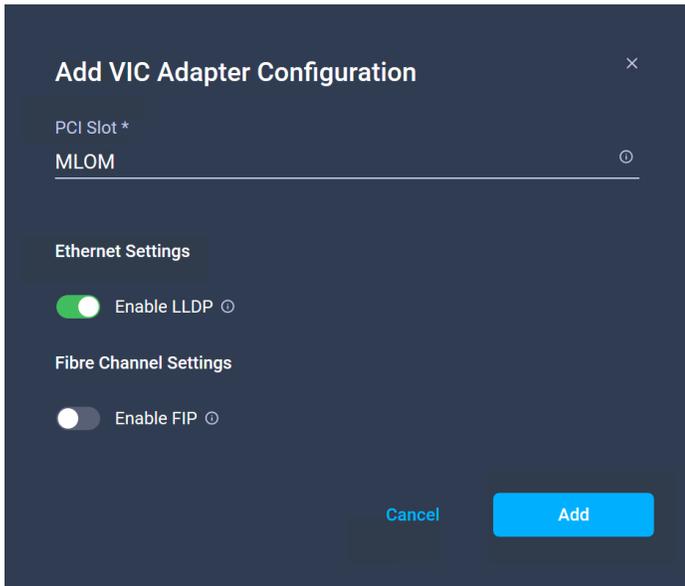
Figure 17. Server policies overview



Policy type: Adapter

In the first task, you configure the adapter with the appropriate transmit and receive queues.

- Click Adapter Configuration and then Next.
 - Type a name and click Next.
 - Click Add VIC Adapter Configuration.
 - Under PCI Slot, enter MLOM if you have a modular LAN-on-motherboard (mLOM) VIC adapter.
 - Disable Fibre Channel over Ethernet Initialization Protocol (FIP) and click Add.
 - Click Create (Figure 18).

Figure 18. Ethernet adapter configuration


Add VIC Adapter Configuration ✕

PCI Slot *
MLOM ⊙

Ethernet Settings

Enable LLDP ⊙

Fibre Channel Settings

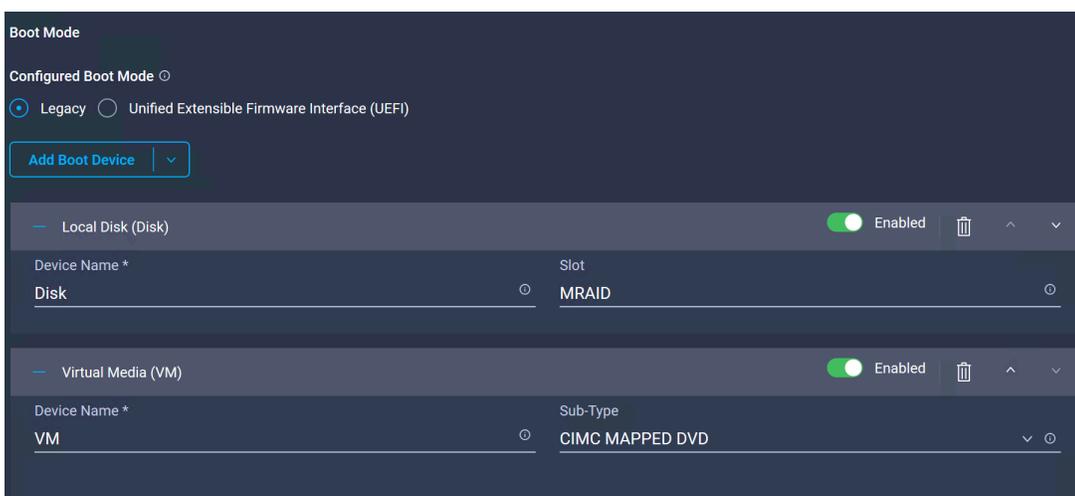
Enable FIP ⊙

Cancel Add

Policy type: Boot order

The next configuration sets the boot order.

- Choose Policy Type > Boot Order and click Next.
 - Type a name and click Next.
 - Select Legacy and click Add Boot Device.
 - Type a device name.
 - Type MRAID for the boot drives in slots 13 and 14 of the Cisco UCS C240 M5L configuration.
 - Click Add Boot Device again.
 - Select Virtual Media.
 - Type a device name.
 - For Sub-Type, choose CIMC Mapped DVD and click Create (Figure 19).

Figure 19. Boot order configuration


Boot Mode

Configured Boot Mode ⊙

Legacy Unified Extensible Firmware Interface (UEFI)

Add Boot Device ▾

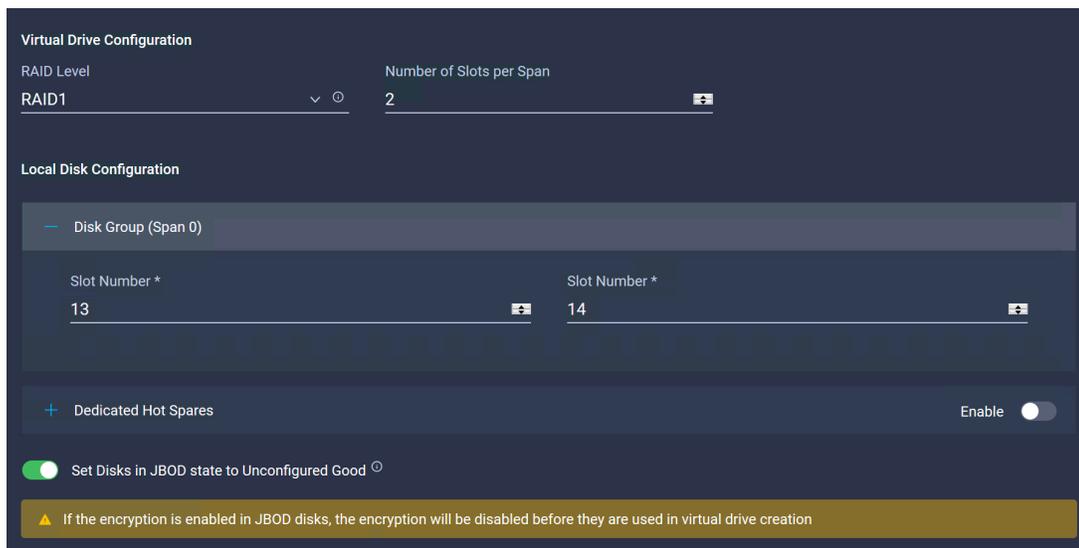
Local Disk (Disk) Enabled ⊙ ⊙	
Device Name *	Slot
Disk ⊙	MRAID ⊙
Virtual Media (VM) Enabled ⊙ ⊙	
Device Name *	Sub-Type
VM ⊙	CIMC MAPPED DVD ⊙

Policy type: Disk group

IBM COS requires only the boot disks in a RAID configuration. The data disks remain in a JBOD architecture.

- Create the disk group policy by selecting Disk Group and then Next.
 - Type a name and click Next.
 - Select RAID Level 1.
 - Under Slot Number, type 13 and 14.
 - Enable “Set Disks in JBOD state to Unconfigured Good.”
 - Click Create (Figure 20).

Figure 20. Disk group configuration for boot disks



The screenshot displays the 'Virtual Drive Configuration' interface. Under 'Virtual Drive Configuration', 'RAID Level' is set to 'RAID1' and 'Number of Slots per Span' is set to '2'. The 'Local Disk Configuration' section shows a 'Disk Group (Span 0)' with two 'Slot Number' fields containing '13' and '14'. Below this, there is a 'Dedicated Hot Spares' section with an 'Enable' toggle switch. At the bottom, a green toggle switch is labeled 'Set Disks in JBOD state to Unconfigured Good'. A yellow warning banner at the very bottom states: 'If the encryption is enabled in JBOD disks, the encryption will be disabled before they are used in virtual drive creation'.

Policy type: Ethernet adapter

The next configuration contains the settings for the Ethernet adapter.

- Choose Policy Type > Ethernet Adapter and click Next.
 - Type a name and click Next.
 - For Interrupts, type 32.
 - Type 8 for Receive Queue Count and type 4096 for Receive Ring Size.
 - Type 8 for Transmit Queue Count and type 4096 for Transmit Ring Size.
 - For Completion Queue Count, type 16.
 - Leave everything else at the default settings and click Create (Figure 21).

Figure 21. Ethernet adapter policy configuration



Enable RDMA

Interrupt Settings

Interrupts: 32

Interrupt Mode: MSix

Interrupt Timer, us: 125

Interrupt Coalescing Type: Min

Receive

Receive Queue Count: 8

Receive Ring Size: 4096

Transmit

Transmit Queue Count: 8

Transmit Ring Size: 4096

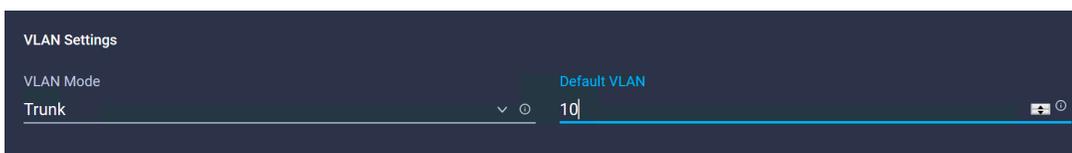
Completion

Completion Queue Count: 16

Policy type: Ethernet network

- Create a policy for the Ethernet network.
 - Choose Policy Type > Ethernet Network and click Next.
 - Type a name and click Next.
 - For VLAN Mode, choose Trunk.
 - Type the number of your default VLAN and click Create (Figure 22).

Figure 22. Ethernet network policy configuration



VLAN Settings

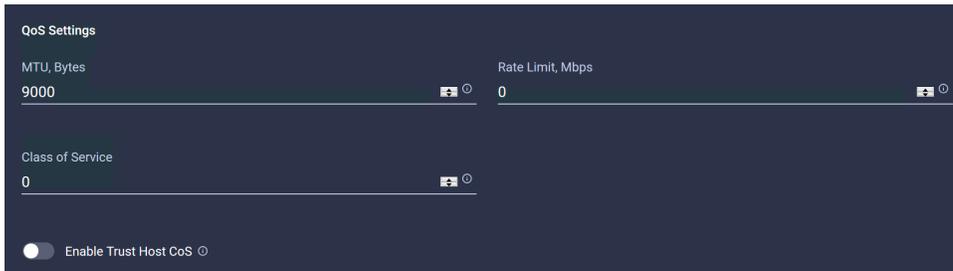
VLAN Mode: Trunk

Default VLAN: 10

Policy type: Ethernet quality of service

In the next task, create a policy for quality of service (QoS).

- Choose Policy Type > Ethernet QoS and click Next.
 - Type a name and click Next.
 - For MTU, Bytes, enter 9000 and click Create (Figure 23).

Figure 23. Policy configuration for Ethernet QoS

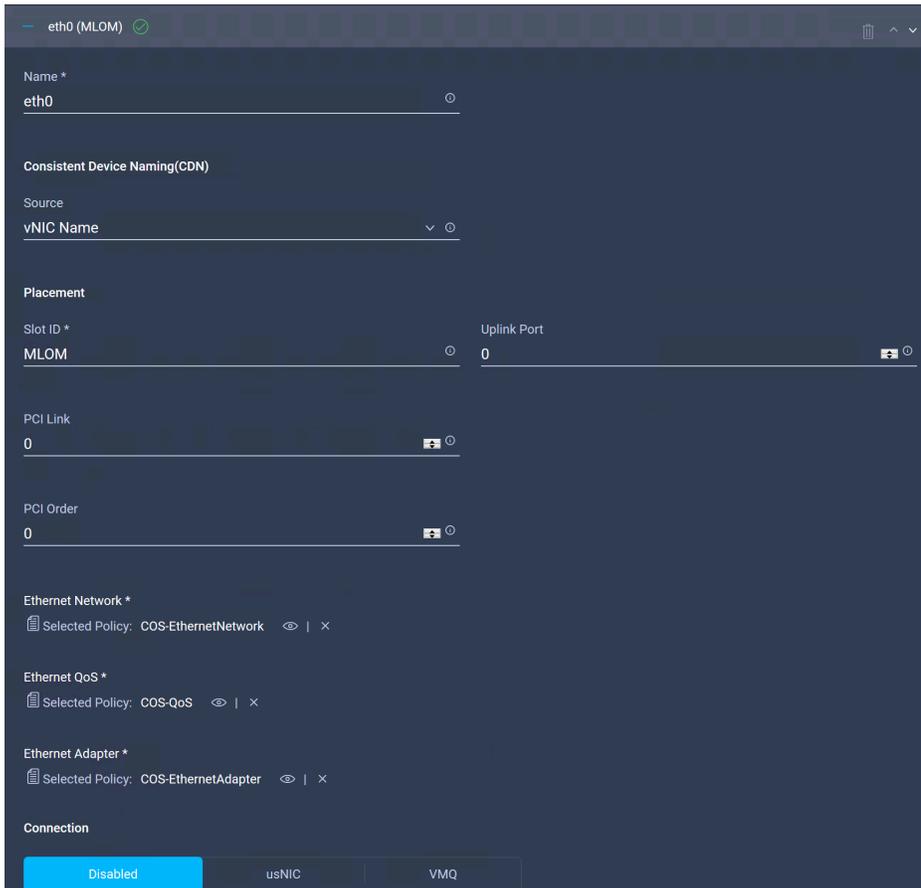
The screenshot shows the 'QoS Settings' configuration page. It features three input fields: 'MTU, Bytes' with a value of 9000, 'Rate Limit, Mbps' with a value of 0, and 'Class of Service' with a value of 0. Each field has a small icon to its right. At the bottom left, there is a toggle switch for 'Enable Trust Host CoS' which is currently turned off.

Policy type: LAN connectivity

The next configuration contains the LAN settings. The example here for IBM COS uses one physical adapter port for data and management.

- Choose Policy Type > LAN Configuration and click Next.
 - Type a name and click Next.
 - Open eth0 and configure the following:
 - For Slot ID, type MLOM.
 - Under Ethernet Network, select your previously configured policy.
 - Under Ethernet QoS, select your previously configured policy.
 - Under Ethernet Adapter, select your previously configured policy.
 - Repeat the same steps for eth1 but change the uplink port to 1.
 - Click Create (Figure 24).

Figure 24. LAN connectivity policy configuration for eth0



eth0 (MLOM) ✓

Name *
eth0

Consistent Device Naming(CDN)
Source
vNIC Name

Placement
Slot ID *
MLOM Uplink Port
0

PCI Link
0

PCI Order
0

Ethernet Network *
Selected Policy: COS-EthernetNetwork

Ethernet QoS *
Selected Policy: COS-QoS

Ethernet Adapter *
Selected Policy: COS-EthernetAdapter

Connection
Disabled usNIC VMQ

Policy type: Network Time Protocol

In the next task, you create a policy for Network Time Protocol (NTP).

- Choose Policy Type > NTP and click Next.
 - Type a name and click Next.
 - Under NTP Server, type an IP address or DNS name and click Create (Figure 25).

Figure 25. NTP policy configuration



Enable NTP

NTP Server *
173.38.201.115

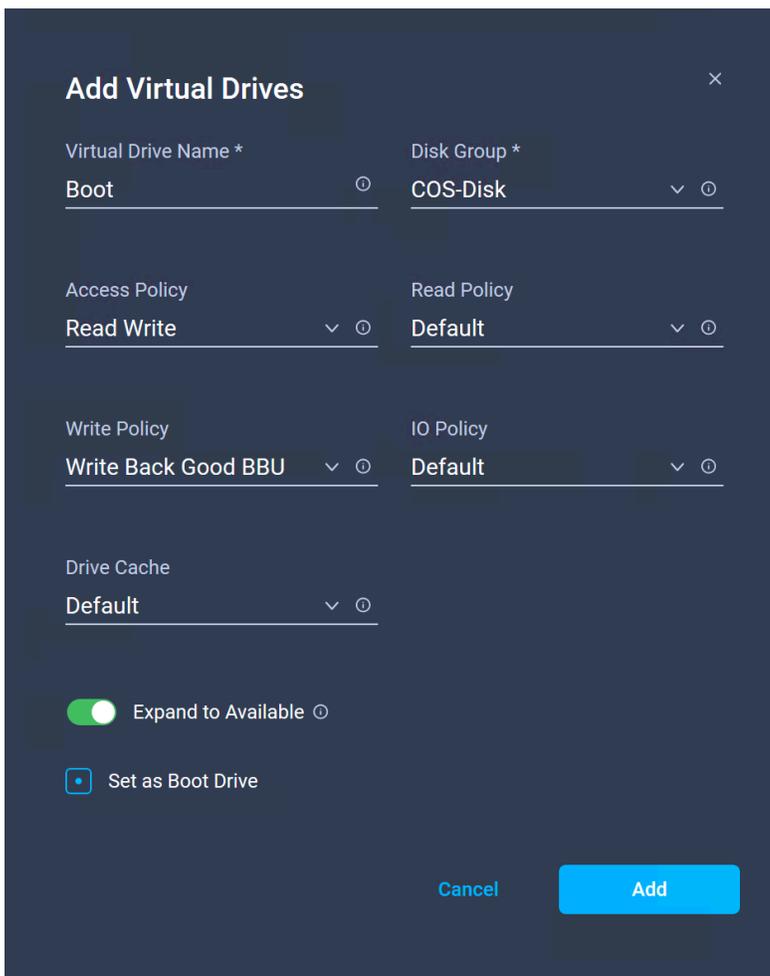
Policy type: Storage

Now create the storage policy.

- Choose Policy Type > Storage and click Next.
 - Type a name and click Next.
 - Under Unused Disk State, choose JBOD.

- Click Add Virtual Drives and configure the following:
- Type a name for the virtual drive.
- For Access Policy, choose Read Write.
- For Write Policy, choose Write Back Good BBU.
- Select Expand to Available.
- Select Set as Boot Drive and click Add.
- Click Create (Figure 26).

Figure 26. Virtual drive boot configuration



The screenshot shows a dark-themed dialog box titled "Add Virtual Drives" with a close button (X) in the top right corner. The dialog contains several configuration fields:

- Virtual Drive Name ***: A text input field containing "Boot".
- Disk Group ***: A dropdown menu showing "COS-Disk".
- Access Policy**: A dropdown menu showing "Read Write".
- Read Policy**: A dropdown menu showing "Default".
- Write Policy**: A dropdown menu showing "Write Back Good BBU".
- IO Policy**: A dropdown menu showing "Default".
- Drive Cache**: A dropdown menu showing "Default".
- Expand to Available**: A toggle switch that is turned on (green).
- Set as Boot Drive**: A radio button that is selected (blue square).

At the bottom of the dialog, there are two buttons: "Cancel" and "Add".

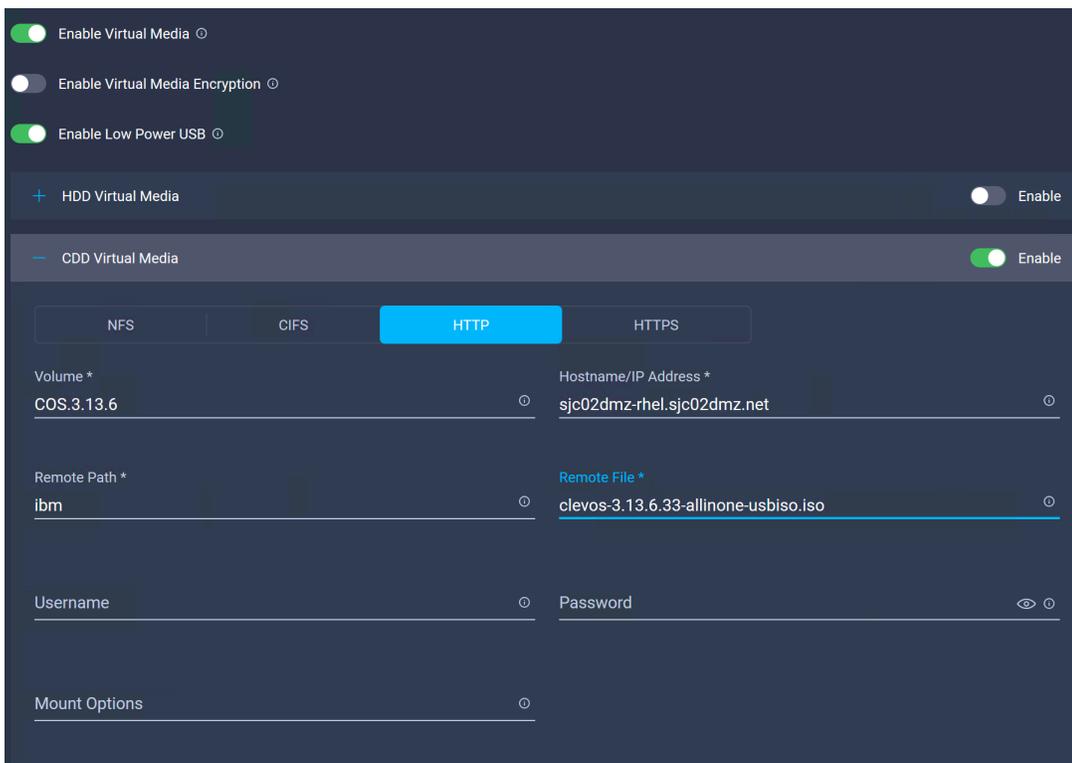
Policy type: Virtual media

In the last task in this section, you create the virtual media policy to be used when booting the server for the first time.

- Choose Policy Type > Virtual Media and click Next.
 - Type a name and click Next.
 - Enable CDD Virtual Media.
 - Click HTTP.
 - Under Volume, type a name.

- Under Hostname/IP Address, type an IP address or DNS name.
- Under Remote Path, type the path to the location of the ISO image.
- Under Remote File, type the file name of the ISO image.
- Click Create (Figure 27).

Figure 27. Virtual media policy type configuration



The formal process of creating the policies is now finished, and you can move on to the next step: the creation of the service profiles.

Create and deploy server profiles for scale-out storage

You have now created the policies. The next step is to create the service profiles for the Cisco UCS C240 M5 servers.

1. Click Service Profiles in the left pane and then click Server Profiles at the top. Click Create Server Profile.
 - Type a name for the server profile and click Next.
 - Under Compute, select the Boot Order, NTP, and Virtual Media policies.
 - Under Network, select the Adapter Configuration and LAN Connectivity policies.
 - Under Storage, select the Storage policy and click Next.
 - Select the server to which you want to assign the profile and click Next.
 - Click Deploy (Figure 28).

Figure 28. Server profile for Cisco UCS C240 M5L server

General					
Server Profile Name	COS1	Assigned Server	sjc02dmz-i13-cos2-cimc	Management IP	192.168.10.151
Server Profile Status	Not Deployed	Management Platform	IMC		
Configuration Errors (0)					
Adapter Configuration				COS-Adapter	
Boot Order				COS-Boot	
LAN Connectivity				COS-LAN	
NTP				COS-NTP	
Storage				COS-Storage	
Virtual Media				COS-VM	

You can monitor the server profile deployment process with the tasks buttons at the top.

- Repeat the same steps for the other two service profiles and deploy them on the remaining two Cisco UCS C240 M5L servers. The formal process of deploying service profiles is now finished, and you can install and configure the scale-out storage software on each of the three servers.

Conclusion

The Cisco Intersight platform transforms the way that customers deploy and manage Cisco UCS and Cisco HyperFlex systems. This platform offers a more intelligent level of management that enables IT organizations to analyze, simplify, and automate their environments in ways that were not possible with prior generations of tools. The new Cisco Intersight virtual appliance provides users with the benefits of the Cisco Intersight software while allowing more flexibility for those with additional data locality and security requirements. In addition, it provides a simple way to configure multiple Cisco UCS instances in a way that reduces the overall configuration and scales up to enterprise environments. It offers an excellent way to build scale-out storage environments with Cisco UCS servers connected to a switched environment.

For more information

For additional information, see the following:

- Cisco Intersight virtual appliance blog: <https://blogs.cisco.com/datacenter/intersight-virtual-appliance>
- Cisco Intersight data sheet: <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/intersight/datasheet-c78-739433.html#FlexibleDeploymentOptions>
- IBM Cloud Object Storage on Cisco UCS C240 Deployment Guide https://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/UCS_CVDs/VersaStackforIBMCloudObjectStorageonCiscoUCSC240forConcentratedDispersalMode.pdf

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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