Table of Contents

About this Lab	2
Requirements	2
About This Solution	3
Tasks	4
Task 1 - Claiming the UCS Domain (Review-Only(Do Not Attempt))	5
Task 2 – Intersight Dashboard Overview	11
Task 3 – Add and Remove a Dashboard Widget	15
Task 4 – Activate Trial Essentials License (Review-Only(Do Not Attempt))	17
Task 5 – Domain Policy Creation	19
Task 6 – Domain Profile Deployment (Review-Only(Do Not Attempt))	41
Task 7 – Updating Firmware <mark>(Review-Only(Do Not Attempt)</mark>)	45
Task 8 – Creating Server Pools	49
Task 9 – Server Policy Creation	56
Task 10 – Server Profile Deployment	68
Task 11 – Server Profile Template Deployment	74
Task 12 – Virtual Media Using OS Links	78
Task 13 – Installing VMware ESXi	79
Task 14 – Accessing the KVM and Installing an Operating System(Do Not Attempt)	83
Task 15 – Server Profile Deployment(Do Not Attempt)	92
Task 16 – Submitting Feedback and Further Information	99
What's Next1	100

About this Lab

This lab provides an overview of Cisco UCS management via Cisco Intersight, and the embedded analytics that allow organizations to analyze, simplify, and automate their environments.

This Cisco Intersight[™] environment is Read/Write and provides Administrator access to an emulated UCS infrastructure. This lab walks users through creating a Cisco Intersight account and using the functionality provided as part of the Cisco Intersight Essentials licensing within the account.

Requirements

The table below outlines the requirements for performing the steps in this preconfigured lab.

Required	Optional
Personal Computer	Cisco AnyConnect [®] (required only for
Supported Web Browser*	task 1)
Cisco CCO account	

*See the Supported Browsers section at https://Cisco Intersight.com/help/getting_started.

About This Solution

Cisco Intersight[™] provides intelligent cloud-based infrastructure management with embedded analytics for the Cisco Unified Computing System X[™] (Cisco UCS X-Series[®]) and Cisco HyperFlex[®] platforms.



Tasks

This lab will walk you through viewing or performing the following tasks related to managing a UCS-X Series environment through Cisco Intersight.

- 1. <u>Claiming the UCS Domain (Review-Only(Do Not Attempt)</u>)
- 2. Intersight Dashboard Overview
- 3. Add and Remove a Dashboard Widget
- 4. Activate Trial Essentials License (Review-Only(Do Not Attempt))
- 5. Domain Policy Creation
- 6. <u>Domain Profile Deployment (Review-Only(Do Not Attempt)</u>)
- 7. Updating Firmware (Review-Only(Do Not Attempt))
- 8. <u>Creating Server Pools</u>
- 9. <u>Server Policy Creation</u>
- **10.** Server Profile Deployment
- 11. Server Profile Template Deployment
- 12. Virtual Media Using OS Links
- **13.** <u>Installing VMware ESXi</u>
- 14. Accessing the KVM and Installing an Operating System (Do Not Attempt)
- 15. <u>Server Profile Deployment (Do Not Attempt)</u>
- **16.** <u>Submitting Feedback and Further Information</u>

Task 1 - Claiming the UCS Domain (Review-Only)

In this task, the instructor will walk through the steps needed to claim your UCS domain in Cisco Intersight. Claiming the domain sets up the connection between your domain and Intersight so that you can manage the domain through Intersight.

Note: Since this lab uses a shared UCS domain, claiming the domain in Intersight can be performed a single time. You may follow along with the instructor, but you will not be able to perform the claiming yourself.

Procedure

- **Step 1** Open one of the supported browsers indicated in the <u>Requirements</u> section above.
- **Step 2** In the address bar, enter the URL <u>https://intersight.com</u>
- Step 3 Click the Sign In with Cisco ID button.

dude Intersight	© Engl
Welcome to Inter	sight
Don't have an intersight Account? Create	an account
Sign In with Cisco ID	
Don't have a Cisco ID? Sign Up	
Or	
Email	
Sign In with SSO	

- **Step 4** Log in to Intersight using the credentials provided to you by the lab administrator.
- Step 5Verify that you can now view the Intersight dashboard. The screen will say
OVERVIEW at the top left, like the graphical view below.

≡	cisco Intersight	*	Infrastructure Service 🗸		Q Search	৩ ধ্বা	Q 02 A2	0	۹
(¢.	Overview		Dashboard Getting Started						
0	Operate	^	Health Summary						^
	Servers		Server Health Summary	Server HCL Status Summary	Fabric Interconnect H	ealth Summary			
	Chassis		•	۵	•				
	Fabric Interconnects		6 Healthy	5 1 Incomplete Not Listed		2 Critical			
	HyperFlex Clusters								J.
,c	Configure	^	HyperFlex Cluster Health Summary	FlexPod Fabric Interconnects Health Summary					
	Profiles		0	6					
	Templates		No Hyperflex Clusters	No Fabric Interconnects					
	Policies								
	Pools		Capacity Utilization						
			Top 5 HyperFlex Clusters by Storage Utilization	HyperFlex Clusters Capacity Runway	Top 5 FlexPod by Cap	acity Utilization			
			No Hyperfex Clusters	No Hyperflex Clusters		No Flexpods			

- **Note:** To perform the steps in the remainder of this task, ensure you are connected to the SLI VPN using Cisco AnyConnect. If you are not able to connect, please read the remaining steps or follow along as the instructor performs the demonstration.
 - **Step 6** Open a second browser tab and navigate to the UCS Fabric Interconnect at <u>https://10.10.63.131</u>

Note: If you receive security warnings, proceed past the warnings to connect to the system.

- **Step 7** Log in to the Fabric Interconnect using the credentials provided to you by the lab administrator.
- **Step 8** Verify that you can now view the DEVICE CONSOLE (like the graphic below).



Step 9 In your Device Console, click on **Device Connector**. Your screen should look like The one below:



- **Step 10** Copy and save the **Device ID** and **Claim ID** to a notepad document.
- **Step 11** At the top of the screen, select **System** from the dropdown. Return to the **Intersight** tab on your browser and click on **Targets** under the **Admin** tab on the left-hand side of the Intersight screen.

See Infrastructure Service								
~	Infrastructure Service							
	My Dashboard							
	System							
Explore More Services								

Step 12 Click on the **Claim Target** button to start the Claim Wizard.

≡	Cisco Intersight	∎∎ S	ystem ∽
0	Settings		Settings
U.	Admin	^	
	Targets		GENERAL
	Software Repository		Account Details
	Tech Support Bundles		Access Details
	Audit Logs		Notifications
	Sessions		AUTHENTICATION
	Licensing		Single Sign-On

Step 13 Click on the **Cisco UCS Domain (Cisco Intersight Managed)** selection box.



Note: Be careful not to select the UCS Domain (UCSM Managed) box by mistake.

Step 14 Click the **Start** button at the bottom right of the screen to start the claiming process.



Step 15 Paste the **Domain ID** and **Claim Code** from notepad to the respective line and then click the **Claim** button at the bottom right of the screen.

General				
Dovico ID *	Olaim Codo *			0
Device iD	o claim code			
Resource Groups				
 Select the Resource Groups if re Organizations with the Resource 	equired. However, this selection is not m e Group type 'All'.	andatory as one or more Resource Gro	up type is 'All'. The claimed tar	get will be part of all
		0 items fo	ound 10 v per page 🔣 🤇	0 of 0 > 🖂 🚯
Name		Usage	Description	
	NO I	TEMS AVAILABLE		
				K < 0 of 0 > >

Step 16 Verify that the target has been claimed in the next window.

rgets								Claim a Ne	w Tar
* All Targets +					🕒 Export 1	items found	10 v per page 📧 🛛]_1_of1.≥	
Connection Connected 1	Top Targets by Types T	1 Vendor 1 • Cisco 5	Systems, Inc. 1						N K N K
Name :	Status 0	Туре	Vendor Clai	imed Time 3	Claimed By	: Re	esource Groups	÷.	ş

Task 1 has been completed!

Note: A connection to the SLI VPN (via AnyConnect) is not required for the remaining tasks in this lab guide. If you had connected to the SLI VPN, you may now disconnect.

Task 2 – Intersight Dashboard Overview

The Cisco Intersight dashboard displays information about the claimed UCS Domains. In a production environment, the dashboard would show all Fabric Interconnects, Servers, and HyperFlex Clusters that have been registered and are currently under management by Cisco Intersight, as well as high-level information about alarms.

and the state of t		Q search 🥹 🕫 🕫 🖉 🖉 🤉
Main © +		
∑ Add Filter		Add Wildget
Fabric Interconnect Inventory	Networking Stuff	HyperFlex Clusters Capacity Runway
Models	■ 2 Ottical	
• 6454 2	HyperFlex Cluster Health Summary	8
108 25 82 Pots Used Areliate	No Hyperflex Clusters	No Hyparflax Clusters
Device Contract Coverage		Fabric Interconnects Bundle Version Summary
Servers 0		
Chassis	(8 ,	
Fabric Interconnects	No Fabric Interconnects	
Des Mar Jun Des Des 2022 2022 - 2022	Mar Jun Sep Seo Mar Jun Sep 2001 - 2001	
Cool Cisco Servers	Server HCL Status Summary	John's Server Model Summary

Procedure

Step 1 Click the **Profile Menu** in the upper right corner of the top toolbar.



Step 2 Click **User Settings** in the resulting menu to see how the new features are controlled.

User Settings	×
Allow User Session Recording	
 Allow user session logging to optimize the client experience. Learn more at Cisco Intersight Platform Privacy Data Sheet (PDS) 	
Language English	~
Theme	
Light Dark The Dark Theme is currently available as a Tech Preview for testing and feedback numpers	
Cancel Save	

- **Step 3** Click the **Language** drop-down to show the language option for the Cisco Intersight dashboard.
- **Step 4** If desired, change the theme from **Dark** to **Light** to show the difference.

- **Step 5** Click **Save** to save the changes or **Cancel** to discard them.
- **Step 6** Click the **OVERVIEW** tab to return to the Intersight dashboard. Note the overall health bars for the currently managed UCS servers and Fabric Interconnects. Also, note the alarm indicators in the top toolbar. Then click the **alarm** (



Step 7 Click the **All** tab at the top or the **View All** button at the bottom of the list of alarms to open a full list of the alarms in the workpane.

Ala	Alarms ×									
Activ	Active Acknowledged									
* A	IActive +									
ß	Add Filter			Export 12 items four	nd 18 v per page 🔣 🤇	1 of 1 D				
	Message	÷	Severity :	Code 2	Source Name	Source Ty	ş			
	Power supply CiscoLab/chassis-1/psu-6 has no AC input		▲ Warning	EquipmentChassisPsuInputLc	CiscoLab/chassis-1/psu-€	Intersight				
	Power supply CiscoLab/chassis-1/psu-3 has no AC input		▲ Warning	EquipmentChassisPsuInputLo	CiscoLab/chassis-1/psu-3	Intersight				
	Port CiscoLab/switch-A/slot-1/fcport-2 has no transceiver inserted		o Info	FcTransceiverNotPresent	CiscoLab/switch-A/slot-1,	Intersight				
	Port CiscoLab/switch-A/slot-1/fcport-3 has no transceiver inserted		0 Info	FcTransceiverNotPresent	CiscoLab/switch-A/slot-1,	Intersight				
	Port CiscoLab/switch-A/slot-1/fcport-4 has no transceiver inserted		O Info	FcTransceiverNotPresent	CiscoLab/switch-A/slot-1,	Intersight				
	Port CiscoLab/switch-A/slot-1/ethport-18 has no transceiver inserted		O Info	EtherTransceiverNotPresent	CiscoLab/switch-A/slot-1,	Intersight				
	Port CiscoLab/switch-A/slot-1/ethport-17 has no transceiver inserted		o Info	EtherTranscelverNotPresent	CiscoLab/switch-A/slot-1,	Intersight				
	Port CiscoLab/switch-B/slot-1/fcport-2 has no transceiver inserted		O Info	FcTransceiverNotPresent	CiscoLab/switch-B/slot-1,	Intersight				
	Port CiscoLab/switch-B/slot-1/fcport-3 has no transceiver inserted		0 Info	FcTransceiverNotPresent	CiscoLab/switch-B/slot-1,	Intersight				
	Port CiscoLab/switch-B/slot-1/fcport-4 has no transceiver inserted		o Info	FcTransceiverNotPresent	CiscoLab/switch-B/slot-1,	Intersight				
	Power supply CiscoLab/switch-A/psu-2 is shutdown		Critical	EquipmentSwitchPsuPowered	CiscoLab/switch-A/psu-2	Intersight				
	Power supply CiscoLab/switch-B/psu-2 is shutdown		Critical	EquipmentSwitchPsuPowered	CiscoLab/switch-B/psu-2	Intersight				
4							•			
ø						1 of 1 >				

Step 8 Choose one alarm code from the list and click on it.

Alarms			×
Active Acknowledged			
* All Active ⊙ + ∅ ∅ Add Filter			G Export 1 items found 18 ∨ per page K < 1 of 1 > >
✓ Message	÷	Severity 0	Code to Source Name to Source Ty 🖗
Power supply CiscoLab/chassis-1/psu-6 has no AC input		▲ Warning	EquipmentChassisPsuInputLc CiscoLab/chassis-1/psu-£ Intersight
<			•
Selected 1 of 1 Show All Unselect All			K < <u>1</u> of 1 > >

Step 9 Observe that you are taken to the **Alarms** page and the source of the alarm code is shown.

Ala	rms								\times
Activ	e Acknowledged								
* AI	I Active ⊙ + √9 Q. Add Filter				F Export 1 items found	18 √ per pag	ie K <	1 of 1 🕞	
	Message	÷	Severity ‡	(Code ÷	Source Name	÷	Source Ty	Ģ
	Power supply CiscoLab/chassis-1/psu-6 has no AC input		▲ Warning	E	EquipmentChassisPsuInputLc	CiscoLab/chassis-	-1/psu-€	Intersight	••••
									E.
ø	Selected 1 of 1 Show All Unselect All							1 of 1 ≥	

Step 10 You may also search the system for a specific alarm code. Copy the **alarm code** from the **Alarms** list. In this example, the alarm code is **EquipmentChassisPSUInput**.

Alarms				×
Active Acknowledged				
× All Active ⊙ +				
🖉 🖉 🔍 Add Filter				C Export 1 items found 18 ∨ per page K ≤ 1 of 1 > >
	÷	Severity	÷	Code
Jly CiscoLab/chassis-1/psu-6 has no AC input		▲ Warning		EquipmentChassisPsuInputLost CiscoLab/chassis-1/psu-f Intersight Ma ···
4				5
💋 🧷 Selected 1 of 1 Show All Unselect All				K < 1 of 1 > >

Step 11 Enter the alarm code into the search field on the toptoolbar, to see a list of all the occurrences of that alarm code. As before, you can click on any occurrence in the list to locate the source of that code.

Q EquipmentChassisPsuInp 🛞	⊘ ⊈1 0 02 42 ?	l A
	Top Results	×
	Alarms 2	
	EquipmentChassisP Nov 23, 3 8:57 AM	2022
HyperFlex Clusters Capacity Runway	Power supply CiscoLab/chassis-1/ has no AC input	psu-3
	▲ EquipmentChassisP Nov 23, 7 8:57 AM	2022
	Power supply CiscoLab/chassis-1/ has no AC input	psu-6

Step 12 Close the search results window.

Step 13 In the navigation pane on the left, click the **Servers** tab located underneath **OPERATE** to show the list of currently managed UCS servers, which includes a health indicator, Model, the License Tier, and other helpful information.

=	diada Intersight	🖧 Infrastructure Service 🗸				Q EquipmentC	nassisPsulnp 🛞	D ⊗ ⊄	1 0 02 42 (<u>୭</u> ୧
:@:	Overview	Servers								
(0)	Operate	^								
	Servers	* All Servers @ +								
	Chassis	🖉 🔍 Add Filter				G	Export 6 item	s found 10 v	per page 🖹 🔄 1 of 1	
	Fabric Interconnects	Health	Power HC	L Status	Models	Contract Status	Profile Sta	itus	Requests (Last	38
	HyperFlex Clusters	0	0 Off 4	Incomplete 5	0	Not Covered 6	0.	Failer 1	1000	
,0	Configure	∧ 6 • Healthy 6	() On 2	Not Listed 1	6 • UCSX 210C-M6 6			Not Assigned 2 OK 1	No Requests	
	Profiles									
	Templates	Name :	Health : Contract S :	License Tier	: Management IP : Serv	rer Profile : Model :	© : M	: Fi :	Utility Storage	9
		CiscoLab-1-1	Healthy Not Covered	Advantage		UCSX-210C-	/ 145.6 204	8.0 5.0(1b)		
	Policies	CiscoLab-1-2	Healthy Not Covered	Advantage		UCSX-210C-	M 99.2 25	6.0 5.0(1b)		
	Pools	CiscoLab-1-3	Healthy Not Covered	Advantage		UCSX-210C-	/ 145.6 51	2.0 5.0(1b)		
		O CiscoLab-1-4	Healthy In Not Covered	Advantage	John	SP1000 Ø UCSX-210C-	/ 145.6 51	2.0 5.0(1b)		
		CiscoLab-1-5	Healthy In Not Covered	Advantage		UCSX-210C-	145.6 51	2.0 5.0(1b)		
		CiscoLab-1-6	Healthy Not Covered	Advantage	TT_S	Server_Profile UCSX-210C-	4 182.4 102	4.0 5.0(1b)		
									E 1 of 1	

Step 14 Click the **Fabric Interconnects** tab to show the currently managed live physical Fabric Interconnects running, including a health indicator, the management IP, and available and used ports.

≡	thersight)¢ Infrastructure Service ∨	🔍 EquipmentChassisPsulnp 🛞 🥝 📢 🗊 🗘 🐽 🖉 🤌
:0:	Overview	Fabric Interconnects	
(<u>©</u>)	Operate	*	
	Servers	* All Fabric Interconn () +	
	Chassis	C Q Add Filter	☐ Export 2 items found 11 v per page K < 1 of 1 >>
	Fabric Interconnects	Health Connection Contract Status Bundle Version	NX-OS Version Models
	HyperFlex Clusters	© Connected 2 B Not Covered 2	
.0	Configure	Oritical 2 No Versions	2 • 9.3(5)(42(11) 2 2 • 6454 2
	Profiles		Basto
	Templates	Name : Health : Contract Status Manag : Model : Expa : B. : UCS D	Domain Profile NX-OS Version
		CiscoLab FI-A Critical Not Covered 10.10.63.131 UCS-FI-645 N/A John D	DomainProfil 9.3(5)142(1f) 54 14 40 ····
	Policies	CiscoLab Fi-B Critical B Not Covered 10.10.63.132 UCS-FI-64! N/A John	DomainProfil 9.3(5)I42(1f) 54 12 42 ····
	Pools		e e <u>1</u> of 1 5 m

Task 2 has been completed!

Task 3 – Add and Remove a Dashboard Widget

The purpose of this section is to understand how to add, configure, and remove a personal dashboard.

Procedure

Step 1 At the top of the page, from the dropdown, select **My Dashboard**. Then click the plus sign (+) along the tabs at the top of the dashboard to add a new dashboard tab.

	 cisco	Intersight	My Dashboard 🗸
Main	⊙ +		

The Widget Library automatically opens in the work pane after adding a new dashboard.

Step 2 Use the **Filters** list to limit the widgets shown to only be widgets for **Fabric Interconnects**.

Chassis Fabric Interconnects FlexPod HyperFlex Clusters		Custom Metric PREVIEW Real-time status of a metric that you want to view. You can choose to create a widget to display graphs/charts for a supported metric type, and select the required time interval More Fabric Interconnects
Servers		Device Contract Coverage Added 3 Reflects the contract status for servers, chassis and Fabric Interconnects over a period of time, distributed by validity of contract. Chassis Fabric Interconnects Servers
	N H C N N H	Health Summary Added 4 Monitor the health for managed devices and hardware. Fabric Interconnects FlexPod HyperFlex Clusters Servers
	1220 1220 220 1 - 12 - 12	Inventory Added 1 Inventory for all managed devices and hardware. Fabric Interconnects HyperFlex Clusters Servers
	500 × 10000 × 10000 × 1000 × 1000 × 1000 × 1000 × 1000 × 1000 × 1000 ×	Version Summary Added 2 Total number of managed targets distributed by the version. Fabric Interconnects FlexPod HyperFlex Clusters Servers Storage

Step 3Choose a widget in the Widget Library list by hovering over it and then clicking
Select. In the example below, the Health Summary widget was selected.



Step 4 The **Settings** menu appears for the selected widget. Here, the title for the selected widget can be customized, if desired. If the widget supports other sources, you may also choose to select a different source. Scroll down and select **Add Widget** to add the widget to the new dashboard.

Widget Library Added 16 of 43 O	
< Health Summary	
Description	
Health Summary for all Fabric Interconnects. Fabric Interconnects FlexPod HyperFlex Clusters Servers	
Settings	
Title * Fabric Interconnect Health Summary	Source * Fabric Interconnects
Preview	
Fabric Interconnect Health Summary	
■ 2 Critical	

- **Step 5** Repeat the above three steps for the desired number of widgets and when you have created enough widgets, click **X** to close the **Widget Library**.
- **Step 6** Your new dashboard tab will be given a default name. In the example below, the default name is **Dashboard1**. Click the **Edit** icon next to the dashboard title name in the work pane and then, select **Rename**.
- Step 7Give the dashboard a name in the Rename Dashboard screen and then, click
Rename.
- **Step 8** If desired, move the widgets around or delete one or two to show the functionality.
- **Step 9** Click the **Edit** icon next to the new dashboard name again then, select **Delete** from the drop-down menu and delete the new dashboard.



Task 3 has been completed!

Task 4 – Activate Trial Essentials License (Review-Only)

This lab uses features of Cisco Intersight that require at a minimum, a **Cisco Intersight Essentials** license. The instructor will demonstrate how to verify licensing. You may follow along, but please do not modify anything in the lab environment as part of this task.

Procedure

Step 1 On the top left ,Next to the Intersight , Choose SYSTEM from the drop down. Now on the top left of the system page, click the Admin drawer just below the settings (②) icon, and then select Licensing .



- **Note:** As a new Intersight user, you can evaluate Intersight for a period of 90 days without a registered license. During this Trial period, the premium features of Intersight are available without a registered license.
 - **Step 2** To use the trial license, in the next screen, select **Start Trial**.

0	Settings	Licensing			Start Trial Actions
0	Admin ^ Targets	Compliance Summary Smart Licensing Deta	ils		
	Software Repository Tech Support Bundles	* General ◎ + □, Add Filter			1 items found 10 - per page E C 1 of 1 > 2
	Audit Logs Sessions	Compliance Trial	Grace Period Expiring Soon	License Usage by Product	**
	sounding	License No Trial	No Grace Period No data available	: In Use Purchased	Next Expiration Time $ar{\phi}$
		Intersight Infrastructure Services - Advant	age O Default O In Compliance	6	0 - ····

Step 3 Check the box for **Intersight** and then click the **Start** button on the confirmation box to start the trial license. The evaluation period is 90 days, and an Essentials (or higher level) license can be registered anytime during the trial period.

Start Trial
Select the Intersight Service to request trial.
Infrastructure Service & Cloud Orchestrator
• Trial option is not available as you are currently registered with Smart Licensing. If trial is needed, please contact your Cisco representative for additional trial options.
Workload Optimizer Registration Required 45 days trial
Cancel Start

Task 4 has been completed!

Task 5 – Domain Policy Creation

The purpose of this section is to create the policies needed to configure the Fabric Interconnects after being claimed. These policies will then be used in the Domain Profile to deploy those configurations. Afterwards, you will verify that the Fabric Interconnects are configured correctly for proper operation.

Procedure

CREATE A PORT POLICY

Step 1 In the left navigation pane of the **Cisco Intersight** home page, click **Policies** under **CONFIGURE**. Then select **Create Policy** in the top right-hand corner of your dashboard.

= dualta Intersight 3	kg Infrastructure Service ∨	🔍 EquipmentChassisPsulnp 🛞 🥥 ⊄ 1 🗘 💷 🚳 🎗
)後: Overview	Policies	Create Policy
Servers Chassis		☐ Export 49 items found 11 ∨ per page @ (1 of 5) >
Fabric Interconnects HyperFlex Clusters Configure	Platform Type UCS Server 38 UCS Chassis 7 UCS Damain 28 UCS Chassis 7 UCS Damain 28	н
Templates	Name : Platform Type Usage	Type 2 Last Update 2 9
Tempinea	z_DemoMW-LANPolicy UCS Server	1 👸 LAN Connectivity Dec 6, 2022 3:40 PM
Policies	TestM.2Policy UCS Server	3 🔞 Storage Dec 6, 2022 3:38 PM
Pools	TestLocalUser UCS Server	2 👸 Local User Dec 6, 2022 3:38 PM
	TestCIMCPolicy UCS Server, UCS Chassis	2 👸 IMC Access Dec 6, 2022 3:38 PM
	z_DemoMW-vMediaPolicy UCS Server	2 👸 Virtual Media Dec 6, 2022 3:37 PM
	TestPowerPolicy UCS Server, UCS Chassis	2 🛱 Power Dec 6, 2022 3:37 PM
	z_DemoMW-BootPolicy UCS Server	2 👸 Boot Order Dec 6, 2022 3:37 PM
	z_DemoMW-BIOSPolicy UCS Server	2 🔞 BIOS Dec 6, 2022 3:37 PM
	SWITCH UCS Domain	8 👸 Switch Control Dec 6, 2022 3:31 PM
	QoSJOHN UCS Domain	10 🔞 System QoS Dec 6, 2022 3:31 PM
	UCS Server, UCS Chassis, UCS Domain	7 🔞 SNMP Dec 6, 2022 3:31 PM
	K. Construction of the second s	· · ·



ilters	Q, Search				
atform Type	Ethernet Network Control	Link Control	O Port	System QoS	
All	Ethernet Network Group	Multicast Policy	◯ SNMP		
UCS Server	Flow Control	O Network Connectivity	Switch Control	VSAN	
UCS Domain	Link Aggregation	O NTP	Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					

NOTE: Familiarize yourself with steps 1 and 2 above. We will be repeating these steps and using the filter option throughout the remainder of this task.

Step 3 Select the **Port** radio button and select **Start** to begin the Port Policy creation wizard.

← Policies Create					
Filters	۹ Search				
Platform Type	Ethernet Network Control	Link Control	Port SNMAR	System QoS	
All UCS Server	Flow Control	Network Connectivity	Switch Control		
UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	Link Aggregation	O NTP	Syslog		
	Cancel				 Start

Step 4 Name the policy **PodX-PortPolicy**, where X is your assigned pod number and click **Next**.

reate		
1 General	General Add a name, description and tag for the policy.	
2 Unified Port	Organization *	
3 Breakout Options		
4 Port Roles	Name * Pod2-PortPolicy	
	Switch Model * UCS-FI-6454	
	Description A	
	< Cancel	

Step 5 We will not be using Fibre Channel ports, so all the Unified Ports will be left as Ethernet ports, click **Next** to continue.

= 🗄 Intersight 🍂	Infrastructure Service 🗸		Q Search) ⊘ ⊄1 ®	Q @2 @2	0	۹
structor Intersight versight version operate servers Chassis Fabric Interconnects HyperFlex Clusters Configure Profilies Templates Pools Pools	Intrastructure Service V Policies > Port Create © General ② Unified Port ③ Breakour Options ④ Port Roles	Unified Port Configure the port modes to carry FC or Ethernet traffic. Move slider to configure unflied ports and select port to Fibre Channel Ports No Fiber Channel Ports	Q Search set breakout.		C C C C C C C C C C C C C C C C C C C		A
	ĸ	Cancel			Back	k Nex	đ

Step 6 On the **Port Roles** page, **select ports 45 through 48** by either: scrolling down the list of ports and selecting ports 45 through 48; or by clicking on ports 45 through 48 on the switch image. If you scrolled down the list, scroll back up to the top of the page. Ensure that ports 45 through 48 show as selected and click the **Configure** button.

=	disco Intersight	ж	Infrastructure Service 🗸				Q Search	Ø	Ø 🕕	Q @2 @2	0	8
(i) (i)	Overview Operate Servers	^	Policies > Port Create									
	Chassis Fabric Interconnects HyperFlex Clusters		Ceneral Culfied Port	Breako Configure	ut Options breakout ports on FC or Ethernet Ethernet Fibre Channel							
,e	Configure Profiles Templates Policies Pools	î	Prot Roles				unutut antar			0 10 10 10 10 10 10 10 10 10 10 10 10 10		
								FC Ethe	net 🗖 E	reskout Capable		
				-	Port Port	Type	Speed	Brea	cout Ports			- 1
					Port 50	Ethernet						
					Port 51	Ethernet		1.71				
					Port 52	Ethernet						
			<	Cancel						Bac	k Ne	oxt

Step 7 In the drop-down under **Role**, select **Server** and click **Save**. This will enable Fabric Extension and allow the Fabric Interconnects to learn the Intelligent Fabric Modules (IFMs) and the Chassis/Servers.

= -it-it- Intersight 🔉 Infras	structure Service 🗸			Q Search	Ø	FI 🗊 🗘 🕼	2 (42)	0	۹
device Intersignt of the end	Atructure Service Atructure Atructure Service Atructure Atructu	Port Roles Configure port roles to define the traffic type Port Roles Port Channels Configure Selected Port	carried through a unified part connection Prin Groups	Q Search		at 3) Q @		•	A
Pools		CORRECT IN ANY		قرقاقا قاة		• Unconf	igured F		
		Name	Type Role	Conne P	ort Channel	C Export	(j) Mode		
		port 1	Ethernet Unconfigured	-					
		port 2	Ethemet Unconfigured	17					
		port 3	Ethernet Unconfigured						
		port 4	Ethernet Unconfigured						
	<	Cancel					Back	Sav	•

- **Step 8** Back on the **Port Roles** page, **select ports 15 and 16**, then click the **Configure** button again.
- **Step 9** These ports will be configured as Ethernet uplinks so you will need to select **Ethernet Uplink** in the **Role** drop-down menu. Leave the other settings at their default values and click **Save**.

Configure P	Port	
Configuration		
Selected Port	Port 1	
Role		
Unconfigured		~
Appliance		
Ethernet Upli	nk	
FCoE Uplink		
Server		
Unconfigure	d	

Step 10 Next, you will create Port Channels by selecting the **Port Channels** tab at the top of the content window.

= titte Intersign	nt As	Infrastructure Service 🗸				0) Swereth	Ø	প কা	0 •••	6.0	0	2
(8) Overview (8) Operate	^	Create											
Serven Charits Fabric Interconnects NyserTies Charters Configure Profiles Templates		Converse Co	Port R Corligue	oles e per roles to define the t Pert Roles Port Cha Configure scoon	taffic type carried through a en annels Pin Groups	lied peri cennecilor.							
Policies						• • • • • • •			e Server				
Policies Pouch				Rame	7410 7410		Cores.	Port Circosol	G and	Export PVEN. W	end × O		
Policies				Report 1	Tren Ethernet	Role	Corres. Auto	Port Channel	Carrier (C)	Export 1000	end Action		
Policies				Barro Fame part 1 part 2	Type Chicrol	Role Server	Corres.	Port Channel	e Sever 1 G A A	Export 100 100 100 100	e de la constante de la consta		
Policies				Remo	Type Ethernet Ethernet	Role Sarver Sarver	Corres.	Port Etransel	G Server	Export wrees W uto	erd ×		
Policies				Barrow Barrow c Barrow	7/270 Chlorost Thereal Chlorost	Role Sorver Barner Barner Barner	Corres. Auto Auto Auto Auto	Port Etransel	General Control of Con	Expert Wrees. M Uto Uto Uto	eed > O		

Step 11 Click the Create Port Channel button and give the port channel a Port Channel ID of X1, where X is your pod number. Leave all other settings at their default values. Then click the Save button. Example of Pod 1's configuration:

E this Intersign	*	Infrastructure Service ~					Q P	arch	0	¢1 🚯	0.82 (4)	•
lt Overview 21 Oceanie		Create										
Servers Chassis Fabric Interconnector HyperFlox Chasters Configure Perflice	~	General General General General Braskoud Options Port Notes	1	Port R	oles sport okriste dellare f Port Rolas Port I Gaada Port Obarrad	ne mellio type carried intrasph e Channailte – Pile Groups	arbied part connection.					
Templabos Policies Pocia					278278294 278278294		rener ar an ar	FUSASA FA	5050505			
Templahas Patholes Patho					r r	PERFORMANCE PERFORMANCE	n Ray Tay Kan Kan Tay Pay ta	A tree blad	Nervensense N- perpagn		entrial (c	
Tengtahas Pakoles Pana					2 F 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	state	ursunsunsunsunsunsunsunsunsunsunsunsunsuns	A tree bins	11~ pr page		• •	
Temptakes Passas					2 FEDTER	sta stanta stanta en	LEGGENERAL FOR	A tree base	18~ pe page		× *****	

Create Port Channel	
Configuration	
The combined maximum number of Ethernet Uplink, FCoE Uplink, and Appliance port channels permitted is 12 and the maximum number of FC port channels permitted is 4.	
Iole theme Uplink Port Channel	
Admin Speed Port Channel ID * 🗘 🖉 Auto 🗸 👳	
themet Network Group O	
elect Policy 🗐	
Tow Control	
Select Policy 🗐	
ink Aggregation	
Select Policy 🗐	
Ink Control	
Select Policy 🗊	
elect Member Ports	
FC or Ethernet ports with unconfigured role are available for port channel creation.	
()	

📩 Intersight 🛛 🏃 Infraetracta	are Service 🗸			
rview Policies Crea	ate			
ate A ensities and a construction of the const	General Livitied Port Breakout Options Port Bolos	Port Roles Configure port roles to d Port Roles Create P	edifies the buffic type carried through a unified part connection. iss Part Channels Pin Orouge And Channel Pin Orouge	
ctes Is		4		
		/ 6 0 200 / 6] 2 Role : Parts 20 Ethemet Lipfek Part Clammi Part 50, Part 51, Part 52 1	1 taxes food <u>9</u> - per page (1) <u>1</u> 41 (1) (
	,	Cancel		ſ
aliala Intersight 🕺	Infrastructure Service $$			Q Search Ø 📢 1 Q 02 62
Verview Overview Operate Servers Chassis	 Infrastructure Service UCS Domain Profiles JohnDoma . 	ainProfile1	1000	Q Search O 411 C 02 A2
overview Operate Chassis Fabric Interconnects	 Infrastructure Service UCS Domain Profiles JohnDoma . Details 	ainProfile1	1000 Policies	Q Search O q2 1 Q 02 82
etitede Intersight > Overview Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Configure ^	Infrastructure Service UCS Domain Profiles JohnDoma . Details Status @ 06	ainProfile1	1000 Policies Perr Configuration UCS Domain Configuration	Q Search O qt 1 Q 62 22
ettele Intersight Overview Operate Chassis Fabric Interconnects HyperFlex Clusters Configure Profiles	Infrastructure Service UCS Domain Profiles JohnDomain . Details Status Status JohnDomainProfiles Name JohnDomainProfiles	ainProfile1	1000 Policies Port Configuration UCS Domain Configuration A Fabric Interconnect A Configured	Q Search O q1 1 Q 02 A2
eterde: Intersight > Diverview > Diperate ^ > Servers > Chassis > Fabric Interconnects > HyperFlex Clusters > Configure ^ > Profiles > Details >	Intrastructure Service UCS Domain Profiles JohnDoma Details Status JohnDomainProfiles JainDomainProfiles Fabric Interconnect Ciccolds Fi-A	ainProfile1	10000 Policies Pert Configuration VLAN & VEAN Configuration UCS Domain Configuration Fabric Interconnect A Configured General Identifiers Connectivity	Q Search O 41 1 0 02 42
dinde Intersight Overview Operate Approx Configure Francis Configure Fremplates Paoloies Pools	Infrastructure Service UCS Domain Profiles JohnDomain Details Status Status Status Status Status Status Status Status Fabric Interconnect Ciccol.45 Fi-8 Fabric Interconnect Ciccol.55 Fi-8 Fabric Interconnect Ciccol.55 Fi-8 Fabric Interconnect Ciccol.55 Fi-9	ainProfile1	10000 Policies Port Configuration VLAN & VSAN Configuration UCS Domain Configuration A Fabric Interconnect A Configurat General Identifiers Connectivity Port	Q Search O C 1 1 Q 2 2 2 Automation of the second
etinde Intersight Overview Operate Chassis Fabric Interconnects HyperFlex Clusters Centigure Profiles Profiles Pools	Infrastructure Service UCS Domain Profiles JohnDoma Details Status Status So eC Name JohnDomainProfiles Fabric Interconnect Ciscol.ab Fi-8 Fabric Interconnect Ciscol.ab Fi-8 Last Update Nov 20 22 856 J	ainProfile1	10000 Policies Pert Configuration VLAN & VBAN Configuration UCS Domain Configuration Fabric Interconnect A Configured General Identifiers Connectivity Port	Q Search O CT C C C C C C C C C C C C C C C C C
ettete Intersight Overview Operate Chassis Earlie Interconnects HyperFiex Clusters Configure Profiles Profiles Profiles Profiles Profiles	Infrastructure Service UCS Domain Profiles JohnDoma Details Status Status Status Some Anno JohnDomainProfiles Fabric Interconnet: Ciscolab FI-A Fabric Interconnet: Ciscolab FI-B Last Update Nov 23, 2022 8:85 J Organizatios default	ainProfile1	1000 Policies Port Configuration VLAN & VSAN Configuration UCS Domain Configuration A Fabric Interconnect A Configured Connect Identifiers Connectivity Port Fort Fort Fort	
ettede Intersight Overview Operate Chassis Fabric Interconnects HyperRec Clusters Configure Profiles Profiles Pools	♦ Infrastructure Service ♦ UCS Domain Profiles JohnDomain Details Status © occ Name JohnDomainProfiles Fabric Interconnect Clacol.ap Fi-8 Last Update Nor 23, 2022 855 / Orgenizations default Tags	ainProfile1	1000 Policies Per Configuration VLAN & VSAN Configuration UCS Domain Configuration Fabric Interconnect A Configured General Identifiers Connectivity Port	Q. Search Image: Comparison of the second secon
Overview Operate ^ Servers Chasis Fabric Interconnects HyperFlex Clusters Configure ^ Profiles Pools	Intrastructure Service I-UCIC Domain Profiles JohnDOmain Details Status Go C Name JohnDomainProfiles Patric Interconnect Ciccula PF-14 Fabric Interconnect Fabric Interconnect Fabric Interconnect Ciccula PF-14 Fabric I	ainProfile1	1000 Policies Port Configuration VLAN & VSAN Configuration UCS Domain Configuration Fabric Interconnect A Configuration Fabric Interconn	Q. Search Q. Q
etités Intersight Overview Operate Servers Chasis Fabric Interconnects HyperFlex Clusters Configure Policies Policies Pools	Intrastructure Service CUCS Domain Profiles JohnDhama Details Status Cucsular Service Name JohnCharter Classical Service Athric Interconnect Athric Interconnect Athric Interconnect Classical Service Athric Interconnect Athric Inter	ainProfile1	1000 Policies Pert Configuration VLAN & VSAN Configuration UCS Domain Configuration Patric Interconnect A Configurat General Identifiers Connectivity Port Fart Fart Type Etheres	Q. Search Q. Q
Normiew Image: Content of the second of th	Intrastructure Service CUCS Domain Profiles JohnDoma Details Status Constructure Ciscolar F1-8 <pciscolar f1-8<="" p=""> Ciscolar F1-8 <pciscolar f<="" td=""><td>ainProfile1</td><td>1000 Policies Pert Configuration UCS Domain Configuration Patric Interconnect A Configuration Patri Interconnect A Configuration Patr Type Etherest 54</td><td>Search Image: Comparison of the search o</td></pciscolar></pciscolar>	ainProfile1	1000 Policies Pert Configuration UCS Domain Configuration Patric Interconnect A Configuration Patri Interconnect A Configuration Patr Type Etherest 54	Search Image: Comparison of the search o

Step 12 Click the **Save** button on the **Port Roles** page to complete the Port Policy Configuration Wizard.

CREATE A VLAN POLICY

Step 13 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **VLAN** radio button and click **Start**.

Create					
Filters	Q, Search				
Platform Type All UCS Server UCS Oramin UCS Chansis HyperFlex Cluster Kuberneter Cluster	Etherret Network Control Ctherret Network Group Prov Control Link Aggregation	Link Control Multicast Policy Network Connectivity NTP	Pert SMAP Switch Control Systep	System QuG VLAN VLAN VSAN	
	Cancel				Start

Step 14 Name your VLAN **PodX-VLANPolicy**, where X is your pod number and click **Next**.

Create		
1 General	General Add a name, description and tag for the policy.	
2 Policy Details	Organization * default ~ Name * Pod2-VLANPOlicy	
	Description <= 1024	
	< Cancel	

Step 15 Click on the Add VLANs button.

Create	
Add VLANS Add VLANs to the policy	
	VLANs should have one Multicast policy associated to it Configuration
	Name / Prefix * VLAN KDs * Ped2VLAN 0 21 0
	Auto Allow On Liptinks O Enable VLAN Sharing O
	Multicast Policy * Select Policy @
Cancel	

Step 16 Name the VLAN **PodXVLAN** and use the use the VLAN ID of **X1**, where **X** is your pod number. The following graphic is an example using Pod 2:

Policies > VLAN				Select Policy	×
Create				Policies 1	Create New
				Q Search	
Add VLANs Add VLANs to the policy				MULTICAST	٢
	VLANs should have one Multicast policy associated to	t			
	Configuration				
	Name / Prefix * Pod2VLAN	VLAN ID5 * © 21	0		
	Auto Allow On Uplinks ©				
	C Enable VLAN Sharing ©				
	Multicast Policy * Select Policy 📾				

- **Step 17** You will also need to select a Multicast Policy. There is a **default** policy created by the lab administrator. Click on **Select Policy** and then click on the **default** policy to select it.
- **NOTE:** Once the policy is selected, your screen should look like the following:

Create				
Add VLANs Add VLANs to the policy				
	VLANs should have one Multicast policy	icy associated to it		
	Configuration			
	Name / Prefix * Pod2VLAN	VLAN IDS * © 21	٥	
	Auto Allow On Uplinks			
	Multicast Policy *			
	Selected Policy MULTICAST ×	•		
Cancel				Ac

- Step 18 Click the Add button.
- **Step 19** On the next screen verify that your VLAN has been added with the correct VLAN name and ID. Then select **Create** to complete the policy.

Create							
General	Policy Details Add policy details						
2 Policy Details	• This policy is applicat	ole only for UCS Domains					
	VLANs						
	Add VLANs Show VLAN Range	ges					
	/ II 9, Ad	d Filter			2 items found 10 v per	page K < 1 of 1 ≥	X ()
	VLAN ID	C Name	C Sharing Type	C Primary VLAN ID	C Multicast Policy	Auto Allow On Uplin	nks 🖗
		1 default	None			Yes	
		21 Pod2VLAN_21	None		MULTICAST	Yes	
						K < 1	of 1 > 刘
	Set Native VLAN ID						
<	Cancel					Bad	ck Create

CREATE AN NTP POLICY

Step 20 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **NTP** radio button and click **Start**.

ters	Search				
tform Type	Ethernet Network Control	Link Control	O Port	System QoS	
All	Ethernet Network Group	Multicast Policy		ULAN	
UCS Server	Flow Control	Network Connectivity	Switch Control	🔿 VSAN	
UCS Domain	Link Aggregation	NTP	Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					

- **Step 21** Name your NTP policy **PodX-NTPPolicy**, where X is your pod number, and click **Next**.
- Step 22 Next, you will need to create an NTP server for the devices in your UCSX deployment to use for time. In the NTP Servers * box, click in that box and enter the IP address of 10.10.63.202. Next, you will need to select the time zone. Click on the Time Zone dropdown and type Denver. Then select the America/Denver option. Your policy should look like the following:

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default Name * PotzeNIPPokcy Set Tags Description <-1024
<	Cancel

Step 23 Click **Create** to complete the NTP policy creation wizard.

Create	
General	Policy Details Ad policy details
Policy Details	V All Platforms UCS Server (Standalone) UCS Domain
	Enable NTP ©
	NTP Servers * 10.10.63.202 0 +
	i mezone America/Denver v 0
<	Cancel Back Create

CREATE AN SNMP POLICY

Step 24 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **SNMP** radio button and click **Start**.

Create					
Filters	Q, Search				
Platform Type	Ethernet Network Control	Link Control	O Port	System QoS	
	Ethernet Network Group	Multicast Policy	 SNMP 	🔿 VLAN	
UCS Server	Flow Control	Network Connectivity	Switch Control	O VSAN	
 UCS Domain 	Link Aggregation	O NTP	Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					
	Cancel				Start

Step 25 Name your SNMP policy PodX-SNMPPolicy, where X is your pod number and click Next.

Create	
(1) General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default ~
	Name * Pod2-SNMPPolicy
	Description <i>n</i>
<	Cancel

Step 26 Next, you will need to fill out the SNMP information. Please fill in the following:

- System Contact = Your Name
- **System Location** = Your Location
- Access Community String = Cisco123!!
- SNMP Community Access = Full
- Trap Community String = Cisco123!!

Below is an example:

Create							
General	Policy Details Add policy details						
2 Policy Details	Enable SNMP		All Platforms	UCS Server (Standalor	UCS Server (FI-Attached)	UCS Domain UCS Chasals	
	v2c Only v3 Only		Both v2c and v3				
	Configuration						
	SNMP Port * 161	0	System Contact * John Doe	٥	System Location * San Jose	0	
	Access Community String Cisco123!!	0	SNMP Community Access Full	~ 0	Trap Community String Cisco123!!	Ø	
	SNMP Engine Input ID	Ø					
	SNMP Users						
	Add SNMP User						
<	Cancel					Back	te

Step 27Scroll down past the Add SNMP Users section. USE Auth Type as SHA
(Auth Type MD5 is depreciated so choose SHA)

Add SNMP User			×
Name *			
Pod2			0
Security Level *			
AuthPriv		~	0
Auth Type			
MD5		~	0
Auth Password *			0
			0
Auth Password Confirmation *			
			0
Privacy Type			-
AES		~	0
Drive and Decomposed *			
Privacy Password *			0
Privacy Password Confirmation *			
			0
	Cancel	Add	
	Calicer	Add	

Step 28 Click the Add SNMP Trap Destination button. In the SNMP Version drop-down, select V2. Then for the Destination Address, please type 10.10.63.202. Click Add.

Add SNMP Trap Destination	\times
Enable O	
SNMP Version *	~ @
VZ	
Community String *	
Cisco123!!	6
Тгар Туре *	
Тгар	~ 0
Destination Address *	
10.10.63.202	٥
Port *	
162	٢
	1 - 65535
Cancel	Add

Step 29 Finally, click the **Create** button to complete the SNMP policy creation wizard.

Create								
 General Policy Details 	SNMP Engine Input ID		Ø					
	SNMP Users							
	Add SNMP User							
								100
	Name		Security Level		Auth Type	Privacy Type		Ģ
	Pod2		AuthPriv		MD5	AES		
	SNMP Trap Destinations							
	Add SNMP Trap Destinat	ion						
								0
	Enable	SNMP Version	Тгар Туре	User	Community String	Destination Address	Port	Ģ
	true	V2	Trap	-	Cisco123!!	10.10.63.202	162	
	< Cancel							Back Crea

CREATE A SYSLOG POLICY

Step 30 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Syslog** radio button and click **Start**.

Filters	Q, Search				
Platform Type	Ethernet Network Control	C Link Control	O Port	System QoS	
	Ethernet Network Group	Multicast Policy		🔿 VLAN	
UCS Server	Flow Control	O Network Connectivity	Switch Control	VSAN	
UCS Domain UCS Chassis	Link Aggregation	O NTP	 Syslog 		
HyperFlex Cluster					
Kubernetes Cluster					

Step 31 Name your Syslog policy PodX-SyslogPolicy, where X is your pod number and click Next.

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Add a name, description and tag for the policy. Organization * default Name * Pod2-SyslogPolicy Set Tags C = 1024
<	Cancel

Step 32Keeping all other defaults, click on the + sign next to Syslog Server 1 under Remote
Logging and use IP address 10.10.63.202 for the Hostname/IP Address. Then click
Create to complete the Syslog policy creation wizard.

Create		
General	Policy Details Add policy details	
2 Policy Details		Il Platforms UCS Server (Standalone) UCS Server (FI-Attached) UCS Domain
	Local Logging	
	- File	
	Minimum Severity to Report * Warning v o	
	Remote Logging	
	- Syslog Server 1	Enable
	Hostname/IP Address * Port * 10.10.63.202 © 514	□ ● Protocol * □ 0 UDP ✓ ● 1 - 65535 ✓ ●
	Minimum Severity To Report * Warning $~~~ \odot$	
<	Cancel	Back Create

CREATE A SWITCH CONTROL POLICY

Step 33 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Switch Control** radio button and click **Start**.

Create					
Filters	Q, Search				
Platform Type	Ethernet Network Control	C Link Control	O Port	System QoS	
	Ethernet Network Group	Multicast Policy	◯ SNMP	🔘 VLAN	
UCS Server	Flow Control	Network Connectivity	 Switch Control 	VSAN	
 UCS Domain 	Link Aggregation	O NTP	Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					
	Cancel				Start

Step 34 Name your Switch Control policy **PodX-SwitchPolicy**, where X is your pod number and click **Next**.

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default Name * Pod2:SwitchPolicy Set Tags Description
<	Cancel

Step 35 Keeping the defaults, click **Create** to complete the Switch Control policy creation wizard.

Create	
General	Policy Details Add policy details
2 Policy Details	This policy is applicable only for UCS Domains
	Switching Mode
	Ethernet O FC O
	End Host Switch End Host Switch
	VLAN Port Count
	C Enable VLAN Port Count Optimization ©
	MAC Address Table Aging Time
	Default Custom Never
	This option sets the default MAC address aging time to 14500 seconds for the End Host mode.
	Link Control Global Settings
	Message Interval
	15 <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>
	Recovery Action ©
	None Reset
<	Cancel Back Create
CREATE NETWORK CONNECTIVITY POLICY

Step 36 Return to the **Policies** in the left navigation pane. Select **Create Policy**. Use the Filter to select the **UCS Domain** radio button again. In the list of policies, select the **Network Connectivity** radio button and click **Start**.

iters	Q, Search				
atform Type	Ethernet Network Control	Link Control	O Port	System QoS	
) All	Ethernet Network Group	Multicast Policy	◯ SNMP	🔿 VLAN	
UCS Server	Flow Control	Network Connectivity	Switch Control	VSAN	
UCS Domain	Link Aggregation		Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					

Step 37 Name your Network Connectivity policy **PodX-NetCon-Policy**, where X is your pod number. Click **Next**.

reate	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default V Name * Pod2 NetConPolicy
	Set Tags
	Description d <= 1024
	< Cancel

Step 38 For the Preferred IPv4 DNS Server use 10.10.63.202. For the Alternate IPv4 DNS Server use 8.8.8.8. Then click Create to complete the Network Connectivity policy creation wizard.

Create				
General	Policy Details			
2 Policy Details			V All Platforms UCS Server (Standalone	e) UCS Domain
	Common Properties Enable Dynamic DNS IPv4 Properties Dotain IPv4 DNS Server Addresses from DHCP			
	Preferred IPv4 DNS Server 10.10.63.202 Enable IPv6 ©	Alternate IPv4 DNS Server		٥
<	Cancel			Back Create

CREATE SYSTEM QOS POLICY

Step 39 Return to the Policies in the left navigation pane. Select Create Policy. Use the Filter to select the UCS Domain radio button again. In the list of policies, select the System QoS radio button and click Start.

reate					
Filters	Q, Search				
Platform Type	Ethernet Network Control	Link Control	O Port	• System QoS	
	Ethernet Network Group	Multicast Policy	◯ SNMP	🔿 VLAN	
UCS Server	Flow Control	O Network Connectivity	Switch Control	O VSAN	
 UCS Domain 	Link Aggregation		Syslog		
UCS Chassis					
HyperFlex Cluster					
Kubernetes Cluster					
					-
	Cancel				8

Step 40 Name your System QoS policy **PodX-SysQoSPolicy**, where X is your pod number and click **Next**.

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default ~ Name * Pod2-QoSPolicy
	Description A <= 1024
	Cancel Next

Step 41 Accepting all defaults, click on **Create** to complete the System QoS policy creation wizard.

Create			
General	Policy Details Add policy details		
2 Policy Details	This policy is applicable only for UCS Domains		
	Configure Priorities		
	Platinum		
	Gold		
	Silver		
	Bronze		
	Best Effort CoS Any Weight 0 5	🗘 💿 🗹 Allow Packet Drops 💿	MTU 1500 🗘 O
	Fibre CoS Weight Channel 3 0 5	0 - 10	1500 - 9216 MTU 2240 O
			1500 - 9216
<	Cancel		Back

Task 5 has been completed!

Task 6 – Domain Profile Deployment (Review-Only)

The purpose of this section is to show how to the policies created in the previous task in the form of a Domain Profile. We will start the Profile creation wizard and deploy a profile to the UCS Fabric Interconnects.

Note: Applying a domain profile affects the entire UCS domain. As a result, you may follow along as the instructor demonstrates this process, but please <u>DO NOT DEPLOY your domain</u> <u>profile.</u>

Procedure

Step 1 In the left-hand menu, select **Profiles** from under **CONFIGURE**.



Step 2 Ensure that you are in the sub-tab named **UCS Domain Profiles**. Then select the **Create UCS Domain Profile** button to start the wizard.

٢of	iles											
/perFle	ex Cluster Profiles	UCS Chassis Profiles	UCS Domain Profiles	UCS Server Profiles								
* Al	II UCS Domain Pr 0	My Custom View Tab 1 -	+				(+ Export	6 items found	50 ~	Create UCS	Domain Pr	rofile
	Name	÷	Status		Fabric Interconr	UCS Domain	connect B	Last Update		per page	÷	Ģ
	TT_Domain_Profile		Not Assigned		10010		ionneet 2	Dec 6, 2022 3:31	PM			
	asdfadsfads		I Not Assigned					Nov 29, 2022 11:0)3 AM			
	JohnDomainProfile100	00	⊚ ок		CiscoLab FI-A	CiscoLab FI	-В	Nov 23, 2022 8:5	5 AM			
	DO_NOT_TOUCH_JOH	IN	Not Assigned					Nov 23, 2022 8:3	7 AM			
	JohnDomainProfile101	I	Not Assigned					Oct 6, 2022 7:17	AM			
	test_MW		Not Assigned					Oct 6, 2022 7:17 A	AM			
											1 of 1	

Step 3 In the **General** page, name the policy **Domain-Profile-XX** (use your initials in place of the XX) and click **Next**.

Create UCS Domain	Profile		
1 General	General Add a name, description and tag for the UCS domain profile.		
2 UCS Domain Assignment		Organization *	
3 VLAN & VSAN Configuration		default	
4 Ports Configuration		Name * Domain-Profile-JG ©	
5 UCS Domain Configuration			
6 Summary			
		Description	
		<= 1024	
<	Close		Back Next

Step 4In the UCS Domain Assignment window, verify the Assign Now button is selected.
Then select the Sunset radio button and click Next.

reate UCS Domair	n Profile
General	UCS Domain Assignment Choose to assign a fabric interconnect pair to the profile now or later.
2 UCS Domain Assignment	
3 VLAN & VSAN Configuration	Assign Now Assign Later
4 Ports Configuration	Choose to assign a fabric interconnect pair now or later. If you choose Assign Now, select a pair that you want to assign and click Next. If you choose Assign Later, click Next to proceed to policy selection.
5 UCS Domain Configuration	
6 Summary	
<	Close Back N

Step 5 In the VLAN & VSAN Configuration window, next to VLAN Configuration under Fabric Interconnect A, click on Select Policy. This will display all the available VLAN policies currently created on the dashboard on the right-hand side of the screen. Select INFRA_VLAN. Do the same for the VLAN Configuration under Fabric Interconnect B. Then click Next.

Create UCS Domain	n Profile		
General UCS Domain Assignment	VLAN & VSAN Configuration Create or select a policy for the fabric interconnect pair.		
3 VLAN & VSAN Configuration	A Fabric Interconnect A 1 of 2 Policies Configured		
Ports Configuration	VLAN Configuration	× 🗇 🖉 INFRA_VLAN 🛱	
5 UCS Domain Configuration	VSAN Configuration	Select Policy 🗐	
6 Summary	Fabric Interconnect B 1 of 2 Policies Configured		
	VLAN Configuration	× (INFRA_VLAN	
	VSAN Configuration	Select Policy 🗐	
<	Close	Back	Next

Step 6 Under both Fabric Interconnects, for the Ports Configuration Policy, click on Select Policy. Under the policy selection pane, select FI_A_Policy for Fabric Interconnect A and FI_B_Policy for Fabric Interconnect B and then click Next.

Create UCS Domain	Profile	
General	Ports Configuration Create or select a port policy for the fabric interconnect	air.
UCS Domain Assignment	Configure ports by creating or selecting	a policy.
Ports Configuration	A Fabric Interconnect A Configured	
5 UCS Domain Configuration	Ports Configuration	Selected Policy FLA_PortPolicy × Φ
6 Summary	-	
	×	Ethernet Uplink FC Uplink Server Unconfigured
	Port Type	Port Role
	Ethernet 54	FC Uplink 4
		Ethernet Uplink
<	Close	Back Next

Step 7 In the UCS Domain Configuration window, select the **Sunset** policies for each of the **Management Policies** and **Network Policies** and click **Next**.

eate UCS Domair	n Profile			
General UCS Domain Assignment VLAN & VSAN Configuration	UCS Domain Select the compu	Configuration te and management policies to be associated with the fabric interco Show Attached Policies (6)	nnect.	
Ports Configuration	^	Management 4 of 4 Policies Configured		
UCS Domain Configuration	1	NTP	× 💿 🖉 NTP 🗑	
3 Summary		Syslog	× @ Ø SYSLOG 🗒	
		Network Connectivity	× @ 🖉 NCP 🛱	
		SNMP	× 🐵 🖉 SNMP 🗐	
	^	Network 2 of 2 Policies Configured		
		System QoS *	× 🗇 🖉 QOS 🛱	
		Switch Control	x 🐵 🖉 SWITCH 🗐	
<	Close			Back

Step 8 Verify your configuration and select **Deploy**.

Create UCS Domair	n Profile	
Ceneral UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration UCS Domain Configuration UCS Domain Configuration Summary	Summary Review the UCS domain profile details, resolve configuration errors and deploy the profile. Central Ports Configuration VLAN & VSAN Configuration UCS Domain Configuration Errors / Warnings Fabric Interconnect A Fabric Interconnect B	
<	Close B	lack Deploy

Step 9 Ensure that a Chassis is now displaying when you click on the **Chassis** menu. You should see something like the one shown below:

hassis											
* All Chassis ◎ + ··· ⊘ ♀ Add Filter							🔂 Export	1 items found	10 ~	per page 🔣 🔇 🔤	of 1 ≥ >
Contract Status	Health	• Warning 1									9.0 7.5
Name ‡	Health	Contract Status	Chassis ID	÷	UCS Domain	Model	÷	Serial	÷	Chassis Profile	ş
CiscoLab-1	▲ Warning	Not Covered		1	CiscoLab	UCSX-950	3	FOX2506P7XV			
										K < 1	of 1 ≥ >

Task 7 – Updating Firmware (Review Only)

The purpose of this section is to show how to use the Intersight dashboard to update the Infrastructure Firmware and the Server Firmware. <u>We will NOT be completing the firmware updates.</u> But we will review the procedure of updating each firmware, respectively.

Procedure

Step 1 On the left-hand side of the screen, under **OPERATE**, click on **Fabric Interconnects**. On the right-hand side of the **CiscoLab FI-A** device, click on the ellipsis (...) to bring up the menu. Select **Upgrade Firmware**.

≡	cisco Intersight	🖧 Infrastructure Service 🗸	Q Search 🥝 🛱 🕚	02 (12) (12)
:@:	Overview	Fabric Interconnects		
<u>,</u> ,	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Configure	All Fateric Intercomee. + Health 2 • Officer Connection : Connection : (InterConnect) No Version No Version	C Expert 2 Rems found 11 per ersion NX-OS Version Models	rpage EC <u>1</u> of 1 2 2
	Profiles Templates Policies Pools	Name : Health : Contract Status Manag : Model : Eppa : 8. Ciscol.ab Fi-8 III Contract IIII Met Covered 103.063.332 UC5-Fi-64! N/A Ciscol.ab Fi-8 III Contract IIII Met Covered 103.063.332 UC5-Fi-64! N/A	: UCS Domain Profile NX:-OS Version : To Juhr@omainProfile 9:35(M-2111) 54 Juhr@omainProfile 9:35(M-2111) 54	Ports φ tal Used φ 14 40 ··· Open TAC Case Upgrade Firmware Replace UCS Domain Collect Tech Support Bundle Collect Tech Support Bundle Collect Tech Support Bundle

Step 2 On the next window, ensure that the **CiscoLab** is selected and click **Next**.

Upgrade Firmware					
1 General	General Ensure selected Fabric Interconnects meet requi	irements for firmware upgrade.			
2 Version	Confirm Fabric Interconnects Selection 1 Selected				
3 Summary	Infrastructure firmware upgrade can be per	formed only on a pair of Fabric Interconnects at or	ce		
	 Add Filter Domain N Compared Model 	Fabric Interconnect A	1 items found	10 ∨ per page K < Fabric Interconnect B	1 of 1 ≥ > ۞
	CiscoLab UCS-FI-6454	FD0245219Z4	UCS-FI-6454	FD025060CM5	bundle versic
	Selected 1 of 1 Show Selected Unselect /	AI			[0] [1] <u>1</u> of 1 [2] [9]
<	Cancel				Back Next

Step 3 Select the **4.2(1#)** firmware version, where **#** is provided to you by your instructor and click **Next**.

Upgrade Firmware		
General	Version Select a firmware version to upgrade the Fabric Interconnects to.	
2 Version	Select Firmware Bundle	Advanced Mode
3 Summary	 The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation exclude Fabric Interconnect traffic evacuation. 	n. Use Advanced Mode to
	Q Add Filter 21 items found 10 √ per page . Version * Size * Release * Description	I of 3 > > > ∅
	4.2(2d) 1.69 GiB Nov 28, 2022 2: Cisco Intersight Infrastructure Bundle	· /
	4.2(2c) 1.69 GiB Sep 20, 2022 11 Cisco Intersight Infrastructure Bundle	•
	4.2(2a) 1.69 GiB Jul 14, 2022 9:5 Cisco Intersight Infrastructure Bundle	٢
	4.2(2.220314) 1.69 GiB May 13, 2022 7: Cisco Intersight Infrastructure Bundle	٢
	4.2(1n) 1.66 GiB Aug 3, 2022 9:5 Cisco Intersight Infrastructure Bundle	\odot
	4.2(1m) 1.66 GiB May 19, 2022 9: Cisco Intersight Infrastructure Bundle	٢
	4.2(11) 1.66 GiB Feb 15, 2022 11 Cisco Intersight Infrastructure Bundle	٢
	4.2(1i) 1.66 GiB Oct 26, 2021 12 Cisco Intersight Infrastructure Bundle	0
	4.2(1h) 1.66 GiB Sep 16, 2021 10 Cisco Intersight Infrastructure Bundle	٢
	4.2(1f) 1.66 GiB Aug 17, 2021 1:2 Cisco Intersight Infrastructure Bundle	٢
	Selected 1 of 21 Show Selected Unselect All	区 < 1 of 3 > >>
<	Cancel	Back Next

Step 4On the next screen, verify your settings BUT DO NOT CLICK THE UPGRADE BUTTON.
Click Cancel to exit out of the upgrade wizard.

Upgrade Firmware	2			
opgrade i i i i i i i i i i i i i i i i i i i	•			
General	Summary Confirm configuration and initiate the up	grade.		
Version	• Selected firmware bundle will be de	ownloaded to the Fabric Interconnects and upgraded	d. Click on Requests to monitor the progress of the firr	nware upgrade.
3 Summary	Firmware			
	Version 4.2(1m) ©	1	Size 1.66 GiB	
	Fabric Interconnects to be Upgraded			
	Add Filter		☐ Export 1 items found 10 ∨ per page	K < 1_of1 ≥ > ∰
	Domain N 0 Model	Fabric Interconnect A Serial Bundle Version	Fabric Interconne Model Serial	ect B Bundle Version
	CiscoLab UCS-FI-6454	FD0245219Z4	UCS-FI-6454 FD025060CM5	٢
				(전 1_ of 1) 원
<	Cancel			Back Upgrade

Step 5 On the left-hand side of the screen, under OPERATE select Servers. In the list of servers, next to the server that has been provided for your pod, click on the ellipsis (...)on the right-hand side of the screen and select Upgrade Firmware.

\equiv "listle" Intersight	🍂 Infrastructure Service 🗸	Q Search	⊘ ⊄1 0 0 0 0 0
(). Overview	Servers		
© Operate Servers Chassis		C Expert 6 items found	1 10 ∨ per page II < 1 of 1 > >
Fabric Interconnects HyperFlex Clusters Configure	Health Power HCL Status Mode 0 * institute 0 0 0fr 4 0 bicomplete 5 0 ^ 0 062 A Med Listed 1 0	s Contract Status Profile Status • UCSX 200C-M6 6 Figure 6	Requests (Last **
Profiles Templates	Name : Health : Contract S : License Tier : Mana O Ciscol.ab-1-1 @ Healthy R Not Covered Advantage	igement IP : Server Profile : Model : O : M : F UCSX-210C-M 145.6 2048.0 9	Fi : Utility Storage : 9 5.0(1b)
Policies Pools	O Ciscolab-1-2 Healthy R Not Covered Advantage O Ciscolab-1-3 B Healthy R Not Covered Advantage	UCSX-210C-M 99.2 256.0 5 UCSX-210C-M 145.6 512.0 5	5.0(1b) Power > 5.0(1b) System >
	O CiscoLab-1-4 Image O CiscoLab-1-5 Image O CiscoLab-1-5 Image Advantage Advantage	JohnSP1000 @ UCSX-210C-M 145.6 512.0 5 UCSX-210C-M 145.6 512.0 5	5.0(1b) Profile > 5.0(1b) Install Operating System
	O Cliscolab-I-6 Healthy R Not Dovered Advantage	TT_Server_Profile 8 UCSX-210C-W 182.4 1024.0 1	5.0(1b) Upgrade Firmware Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier
			Collect Tech Support Bundle

Step 6 In the server list, ensure that you pod's server is selected and click **Next**.

Jpgrade Firmwar	e			
1 General	General Ensure selected servers meet requirements for firmware upgrade.			
2 Version	Confirm Servers Selection 1 Selected			
3 Summary	ු, Add Filter		1 items found 10 v per page	: K < 1 of 1 > > 🔅
	Name Cuser Label	t Model t	Firmware Version	UCS Domain
	CiscoLab-1-1	UCSX-210C-M6	5.0(1b)	CiscoLab
	< Cancel			Back Next

Step 7 In the list of the firmware versions, select the **5.0(2#)** version, where **#** is provided to you by your instructor and click **Next**.

Upgrade Firmware		
General	Version Select a firmware version to upgrade the servers to.	
2 Version	Select Firmware Bundle	Advanced Mode
3 Summary	 The selected firmware bundle will be downloaded from intersight.com. All the server components will be upgrad Advanced Mode to exclude upgrade of drives and storage controllers. 	led along with drives and storage controllers. Use
	Q Add Filter 10 Items	found 10 ∨ per page K < 1 of 1 > > ⊕
	Version C Size C Release C Description	÷ \$
	5.0(2e) 693.59 MiB Nov 29, 2022 11 Cisco Intersight Server Bundle	©
	5.0(2d) 678.01 MiB Sep 20, 2022 12 Cisco Intersight Server Bundle	•
	5.0(2b) 654.02 MiB Jul 14, 2022 9:5 Cisco Intersight Server Bundle	0
	5.0(2.220506) 654.04 MiB May 16, 2022 6: Cisco Intersight Server Bundle	٩
	5.0(1f) 464.34 MiB Sep 1, 2022 11:2 Cisco Intersight Server Bundle	•
	S.0(1e) 460.63 MiB Jun 16, 2022 9: Cisco Intersight Server Bundle	٢
	S.0(1c) 454.58 MiB Feb 2, 2022 12: Cisco Intersight Server Bundle	٢
	5.0(1b) 450.83 MiB Sep 16, 2021 5:1 Cisco Intersight Server Bundle	٢
	S.0(1a) 451.00 MiB Aug 4, 2021 6:5 Cisco Intersight Server Bundle	۵
	4.1(5h) 351.39 MiB Jun 17, 2021 11: Cisco Intersight Server Bundle	•
	Selected 1 of 10 Show Selected Unselect All	K < 1 of 1 > >
<	Cancel	Back Next

Step 8 On the next screen, verify your settings **<u>BUT DO NOT CLICK UPGRADE</u>**. Click **Cancel** to exit the firmware upgrade wizard.

Task 7 has been completed!

Task 8 – Creating Server Pools

The purpose of this section is to create the pools that are required to complete the Server Profile wizard. These pools will be used to assign identities to the compute nodes. We will create a MAC, UUID, WWNN/WWPN pool and assign them in the next section.

Procedure

CREATE A MAC POOL

Step 1 On the left-hand side of the screen, under **CONFIGURE**, click on **Pools**. In the top right-hand corner click on **Create Pool**.



Step 2 Select the **MAC** radio button and click **Start**.

reate			
Q Search			
O IP	MAC	O wwpn	
	C Resource		
Cancel			St

Step 3 Name the pool **PodXMAC-Pool**, where X is your pod number and click **Next**.

Create	
1 General	General Pool represents a collection of MAC addresses that can be allocated to VNICs of a server profile.
2 Pool Details	Organization * default Name * Pod2MAC-Pool Set Tags Description
<	Cancel

Step 4 For the block suffix use **00:00:X0**, where X is your pod number. For the **size**, use **8**. Then click **Create**.

Create			
General	Pool Details Collection of MAC Blocks.		
2 Pool Details	MAC Blocks		
	From 00:25:85:00:00:20	© Size 8	₿ ● 1-1024 +
	< Cancel		Back Create

CREATE A UUID POOL

Step 5 On the left-hand side of the screen, click on **Pools**. And in the top right-hand corner click on **Create Pool**.

Pools						
Pools Reserved Identifiers	/RFs					
	/ Tab 1 +			C Export 9 i	tems found $25 imes { m per}$ per pa	Create Pool
IP x 12 • Available 12	MAC # 1048 • Used 6 • Available 1042	UUID * 40 • Used 2 • Available 38	WWNN R	WWPN R	IQN X NO IQN POOLS	Resource x

Step 6 Select the **UUID** radio button and click **Start**.

reate				
Q, Search				
91 ()	⊖ MAC	() UUID	⊖ wwpn	
	Resource	O WWNN		

- **Step 7** Name the pool **PodXUUID-Pool**, where X is your pod number and click **Next**. Fill out the following fields, where **X** is your pod number:
 - Prefix = **000000X-000X-000X**
 - From = **000X-000000000X0**
 - Size = **8**

Below is an example from Pod **2**:

Create	
1 General	General Pool represents a collection of UUID items that can be allocated to server profiles.
2 Pool Details	Plot Inpresents a conclusion of out-intensis that can be anothered to server promes. Organization * default Name * PostZUUD-Pool Set Tags Description <= 1024
<	Cancel Next

Step 8 Click the **Create** button to complete the pool creation wizard.

Create		
General Pool Details	Collection of UUUD suffix Blocks. Configuration Prefix * 00000002-00002	
	UUID Blocks Size From Size 0002-0000000020 8	() • 1 - 1024 +
<	Cancel	Back Create

CREATE AN IP POOL

Step 9 On the left-hand side of the select **Pools** then click on the **Create Pool** button. Select the **IP** radio button and then click **Start**.

reate				
۹ Search				
91 •	◯ MAC		O WWPN	
O IQN	Resource	O WWNN		
Cancel				Star

Step 10 Name the pool **PodXIP-Pool**, where X is your pod number and click **Next**.

Create	
1 General	General Pool represents a collection of IPv4 and/or IPv6 addresses that can be allocated to other configuration entities like server profiles.
2 IPv6 Pool Details 3 IPv6 Pool Details	Organization * default v Name * PdZIP-Pool Set Tags Cescription e << 1024
	< Cancel Next

Step 11 Fill in the following information:

- Netmask = 255.255.255.0
- Gateway = 10.10.63.254
- Primary DNS = **10.10.63.202**
- Secondary DNS = 8.8.8.8
- From = 10.10.63.14X, where X is your pod number
- Size = **1**

Note: A pool size of 1 is not practical in a production environment, but in the lab, you will need only 1 IP address.

Step 12 Then click Next

Below is an example from Pod 2:

General	IPv4 Pool Details	Siguration data for IDuA interfaces			
IPv4 Pool Details	Network interface con	Configure IPv4 Pool			
IPv6 Pool Details		Configuration			
		Netmask * 255.255.255.0	Gateway © 10.10.63.254	0	
		Primary DNS 10.10.63.202	Secondary DNS © 8.8.8.8	٥	
		IP Blocks			
		From 10.10.63.142	Size © 1	() o 1 - 1024	+

Step 13 Click the **Configure IPv6 Pool** slider bar to disable IPv6. And then click the **Create** button to complete the pool creation wizard.

Create		
General	IPv6 Pool Details Network interface configuration data for IPv6 interfaces.	
3 IPv6 Pool Details	Configure IPv8 Pool You can skip IPv8 Pool configuration for now and configure it later	
<	Close	Back Create

Task 8 has been completed!

Task 9 – Server Policy Creation

The purpose of this section is to create policies required for creating a Server Profile.

Procedure

CREATE A BIOS POLICY

- **Step 1** On the left-hand side of the screen, under **CONFIGURE**, select **Policies** and then the **Create Policy** button.
- Step 2 Under Filters select the UCS Server radio button, select the BIOS radio button and click Start.

Create					
Filters	Q, Search				
Platform Type All UCS Server UCS Domain UCS Chassis HyperFlex Cluster Kubernetes Cluster	Adapter Configuration Adapter Configuration BIOS BIOS Boot Order Certificate Management Device Connector Ethernet Adapter Ethernet Adapter Ethernet Network Ethernet Network Control Ethernet Network Group	Ethernet QoS FC Zone Fibre Channel Adapter Fibre Channel Network Fibre Channel QoS IMC Access IPMI Over LAN ISCSI Adapter ISCSI Boot	ISCSI Static Target LAN Connectivity LDAP Local User NtP Persistent Memory Power SAN Connectivity	SD Card Serial Over LAN SMTP SNMP SSH Storage Syslog Virtual KVM Virtual Media	
	Cancel				Start



Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default
<	Cancel

Step 4 Review the available options. Retain all defaults and click **Create** to complete the policy creation wizard.

Create	
General	Policy Details Add policy details
2 Policy Details	∑ <u>All Partorns</u> UCS Server (Standalove) UCS Server (Fi-Attached)
	The BIOS settings will be applied only on next host reboot.
	+ Boot Options
	+ Intel Directed IO
	+ LOM And PCIe Slots
	+ Main
	+ Memory
	+ PCI
	+ Power And Performance
	+ Dronaceor
<	Cancel Back Create

CREATE A BOOT POLICY

- **Step 5** From the left-hand side of the window, select **Policies** and then click the **Create Policy** button.
- **Step 6** Under **Filter**, select **UCS Server** and click on the **Boot Order** radio button.

Create					
Filters	Q. Sauch				
Planform Type Al UCD Smore UCD Smore UCD Smore UCD Smore UCD Smore UCD Smore UCD Smore Sciences Allower Sciences Sc	Austra Contiguation Basis Data Data Certificato Mangement Pitcenet August Pitcenet August Ethernet Holewah Garted Lilberent Holewah Grupp	Drev Hot Sud His Zane The Channel Adapter The Channel Adapter The Channel Adapter The Channel Adapter Mic Access Mic Access GOL Adapter GOL Adapter GOL Mass	KOD State Target LAR Conventing LOP tool the hears Conventing Netron Conventing NTT Pestate Literary KNT Mol Superschifty	S0 Card Isteral Cherl JAN SMUTP SNUTP S00 S00 S00 S00 S00 S00 S00 S0	
	Canoel				Start

Step 7 Name the policy **PodXBOOT-Policy**, where X is your pod number and click **Next**.

Image: Ceneral Add a name, description and tag for the policy. Image: Criganization * default	Create		
Policy Details Organization * default ~ Name * Pod28001Policy Set Tags Description C 1024	1 General	General Add a name, description and tag for the policy.	
Set Tags Description <= 1024	2 Policy Details	Organization * default ~ Name * Pod2BOOT-Policy	
Description A <= 1024			
		Description A <= 1024	

Step 8 Click the **Add Boot Device** drop-down and select **Local Disk**.

Our sta	
Create	
General	Policy Details
C	Add policy details
2 Policy Details	V All Platforms UCS Server (Standalone) UCS Server (FI-Attached)
	Configured Boot Mode 💿
	Unified Extensible Firmware Interface (UEFI) Legacy
	Enable Secure Boot
	Add Boot Device
	ISCSI Root
	Local COD
	Local Disk
	NVMe
	PCH Storage
	PXE Boot
	SAN Boot
	SD Card
	So card
	UEFI Shell
	USB
	Virtual Media
<	Cancel Back Create

- **Step 9** Use the following information to fill in the fields:
 - Device Name: OS-Disk
 - Slot: **1**
- **Step 10** Click the **Add Boot Device** drop-down again and click **Virtual Media**. Name this device **OS-Install**, and under Sub-Type, select **KVM MAPPED DVD**.

Step 11 Click **Create** to complete the policy creation wizard.

Create		
General Policy Details	Policy Details Add policy details	V All Platforms UCS Server (Standalone) UCS Server (Pi-Attached)
	Configured Boot Mode Configured Boot Mode Cuterative Interface (UEF) Legacy Cuterative Boot Configured Boot Cuterative Interface (UEF) Add Boot Device	
	+ Virtual Media (OS-Install) + Local Disk (OS-Disk)	Enabled 1 A V
	Cancel	Back Create

CREATE A POWER POLICY

- **Step 12** On the left-hand side of the screen, select **Policies** and then click on the **Create Policy** button.
- **Step 13** Under the **Filter** option, highlight the **UCS Server** radio button and then select **Power**. Then click the **Start** button.

ilters	Q, Search				
atform Type	Adapter Configuration	C Ethernet QoS	iscsi static Target	SD Card	
AII (BIOS	O FC Zone	LAN Connectivity	Serial Over LAN	
UCS Server	Boot Order	Fibre Channel Adapter	LDAP	SMTP	
UCS Domain	Certificate Management	Fibre Channel Network	 Local User 	SNMP	
UCS Chassis	O Device Connector	Fibre Channel QoS	Network Connectivity	SSH	
HyperFlex Cluster	Ethernet Adapter	() IMC Access	O NTP	Storage	
) Kubernetes Cluster	Ethernet Network	IPMI Over LAN	Persistent Memory	Syslog	
	Ethernet Network Control	iSCSI Adapter	Power	Virtual KVM	
	Ethernet Network Group	ISCSI Boot	SAN Connectivity	Virtual Media	

- **Step 14** Name the policy **PodXPOWER-Policy**, where X is your pod number and click **Next**.
- **Step 15** Review the available options and then click **Create** to complete the policy creation wizard.

Create			
General Policy Details	Policy Details Add policy details		V All Platforms UCS Server (PI-Attached) UCS Charais
	Configuration		
	Power Profiling © Power Priority Low	Power Restore ~ O Always Off	U (D
	Power Redundancy Grid	~ ©	
	Power Save Mode Dynamic Power Rebalancing		
	Extended Power Capacity © Power Allocation (Watts) 0	0 - 65535	
a a a a a a a a a a a a a a a a a a a	Cancel		Back Create

CREATE A VIRTUAL KVM POLICY

- **Step 16** Click on **Create Policy** again and then under the filter option select **UCS Server**. Scroll down the list of policies; select the **Virtual KVM** radio button and click **Start**.
- **Step 17** Name the policy **PodXKVM-Policy**, where X is your pod number and click **Next**.

Organization * default	×		
Name *			
rouzitvini rolicy			
Description	<= 1024		
Cancel			

Step 18 Review the available options and then click **Create** to complete the policy creation wizard.



CREATE A VIRTUAL MEDIA POLICY

Step 19 Click on **Create Policy** again and then under the filter option select **UCS Server**. Scroll down the list of policies; select the **Virtual Media** radio button and click **Start**.

Step 20	Name the policy PodXVirtMedia-Polic	y, where X is your pod number and click Next
---------	-------------------------------------	--

reate	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default ~ Name * PodZVirtMedia-Policy
	Description A <= 1024
	< Cancel

Step 21 Review the available options and then click **Create** to complete the policy creation wizard.

Create					
General Policy Details	Policy Details Add policy details			All Platforms	UCS Server (Standalone) UCS Server (FI-Attached)
	Configuration				
	Enable Virtual Media Enable Virtual Media Encry Enable Low Power US8 Add Virtual Media	ption ©			
				0 items found	10 - v per page ≤ ≤ 0 of 0 > > 3
	Name	Туре	Protocol		File Location
¢	Cancel				Back Create

CREATE AN IMC ACCESS POLICY

Step 22 Click on the **Create Policy** button and under the filter option select **UCS Server**. Scroll down the list of policies; select **IMC Access** radio button and click **Start**.

Step 23 Name the policy **PodXIMC-Policy**, where X is your pod number and then click **Next**.

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default Name * PodzIMC-Policy Set Tags Description
	Cancel

Step 24 For the **VLAN ID**, use vlan **63**. Then you will need to click on the **Select IP Pool** link to select the Pool you created earlier. Then click on the **Create** button to complete the policy creation wizard.

Create	
General	Policy Details Add policy details
2 Policy Details	V All Platforms UCS Server (FI-Attached) UCS Chassis
	A minimum of one configuration must be enabled. Policies like SNMP, vMedia and Syslog are currently not supported via Out-Of-Band and will require an In-Band IP to be configured. Check here for more info, Help Centre
	In-Band Configuration $_{\odot}$ Enabled
	VLANID* 63 0 0 4 - 4003
	IPv4 address configuration ○
	□ IPv6 address configuration ◎ IP Pool *
	Selected IP Pool Pod2IP-Pool × @ Ø
	Out-Of-Band Configuration © Enabled
<	Cancel Back Create

CREATE A LOCAL USER POLICY

Step 25Click on the Create Policy button and under the filter option, select the UCS Server
option. Then ensure that the Local User policy radio button is selected and then click the
Start button.

ilters	Q, Search			
atform Type	Adapter Configuration	Ethernet QoS	iSCSI Static Target	SD Card
) All	BIOS	FC Zone	LAN Connectivity	Serial Over LAN
) UCS Server	O Boot Order	Fibre Channel Adapter	◯ LDAP	◯ SMTP
) UCS Domain	Certificate Management	Fibre Channel Network	 Local User 	SNMP
UCS Chassis	O Device Connector	Fibre Channel QoS	Network Connectivity	⊖ ssн
) HyperFlex Cluster	Ethernet Adapter	IMC Access		Storage
Kubernetes Gluster	Ethernet Network	IPMI Over LAN	O Persistent Memory	Syslog
	Ethernet Network Control	iscsi Adapter	O Power	Virtual KVM
	Ethernet Network Group	iscsi Boot	SAN Connectivity	Virtual Media

Step 26 Name the policy **PodXUSER-Policy**, where X is your pod number and click **Next**.

Create	
1 General	General Add a name, description and tag for the policy.
2 Policy Details	Organization * default V Name * Pod2USER-Policy
	Description <= 1024
	Cancel

- **Step 27** Click the **Add New User** button at the bottom of the wizard. Then click on the **+** icon next to **New User**. Use the following credentials:
 - Username: **PodXUser** (where X is your pod number)
 - Password: **Cisco123!!** (You will also need to confirm the password.)

Step 28 Click **Create** to complete the policy creation wizard.

Create		
	Enforce Strong Password	
General	C Enable Password Expiry ○	
2 Policy Details	Password History 5 0 - 5 Always Send User Password Cool Users This policy will remove existing user accounts other than the ones configured with this policy. However, the default admin device. You can only enable/disable or change account password for the admin account by creating a user with the user the policy, only the admin user account will be available on the endpoint device. By default, IPMI support is enabled for a	n user account is not deleted from the endpoint name and role as 'admin'. If there are no users in Il users
	Add New User Pod2User (readonly)	Cnable 🗊
	Username * Role Pod2User © readonly	v 0
	Password * Password Confirmation *	۵ و
<	Cancel	Back Create

CREATE A SERIAL OVER LAN POLICY

Step 29 Click on Create Policy. Under the filter option select UCS Server and then select the Serial Over LAN policy radio button and click Start.

	Search			
atform Type	Adapter Configuration	Ethernet QoS	ISCSI Static Target	SD Card
) All	BIOS	FC Zone	LAN Connectivity	Serial Over LAN
) UCS Server	Boot Order	Fibre Channel Adapter	◯ LDAP	◯ SMTP
UCS Domain	Certificate Management	Fibre Channel Network	Local User	◯ SNMP
UCS Chassis	Device Connector	Fibre Channel QoS	Network Connectivity	🔾 ssh
HyperFlex Cluster	C Ethernet Adapter	IMC Access		Storage
Rubernetes Cluster	Ethernet Network	IPMI Over LAN	Persistent Memory	Syslog
	Ethernet Network Control	iSCSI Adapter	O Power	Virtual KVM
	Ethernet Network Group	iscsi Boot	SAN Connectivity	Virtual Media

Step 30 Name the policy **PodXSerialLAN-Policy**, where X is your pod number and click **Next**.

reate		
1 General	General Add a name, description and tag for the policy.	
2 Policy Details	Organization * default ~	
	Name * Pod2SerialLAN Policy	
	Description	
	< Cancel	

Step 31 Review the available options but leave them at their default values and click on **Create** to complete the policy creation wizard.

Task 9 has been completed!

Task 10 – Server Profile Deployment

In this section, you will create and deploy a Server Profile to an available server using the policies and pools we have previously created.

Procedure

Step 1 On the left-hand side of the screen, under CONFIGURE, select Profiles. Then click on the UCS Server Profiles tab.

=	cisco Intersight	*	Infrastructure Service 🗸			Q Search	📄 ତ ଶ୍ର ପ୍ରଭ୍ରେ	0.
e.	Overview		Profiles					
0	Operate Servers	^	HyperFlex Cluster Profiles UCS Chassis	Profiles UCS Domain	Profiles UCS Server Profiles			
	Chassis Fabric Interconnects HyperFlex Clusters		* All UCS Server Prof +			🕒 Export 💠 4	Create UCS	Server Profile
6	Configure	^	Name :	Status :	Target Platform : UCS Server Templa	te Server	Resource Pool	Last 9
	Profiles		Johnspace	() OK	UCS Server (FI-Attached)	CiscoLab-1-4		Dec ···
	Templates		TT_Server_Profile z_DemoMW-ServerProfileTemplate_D.	Faled	UCS Server (FI-Attached) UCS Server (FI-Attached) TEST_TEMPLATE	Ciscol ab-1-6		Dec ···· Nov ···
	Policies		TestServiceProfile	Not Assigned	UCS Server (FI-Attached)			Nov

- **Step 2** Click on the Create UCS Server Profile button.
- **Step 3** Name the Server Profile **PodXServerProfile**, where X is your pod number and ensure that the **UCS Server (FI -Attached)** radio button is highlighted. Then click **Next**.

Create UCS Server F	Profile	
Ceneral Server Assignment Configuration Management Configuration Storage Configuration Storage Configuration Network Configuration Network Configuration To Summary	Cherenel Comparison of detault Constrained of detault Constrained o	
<	Close	Back

Step 4 Select the server that corresponds to your Pod X and click **Next**.

Create UCS Server	Profile
General	Server Assignment Choose to assign a server now, from a resource pool, or later.
2 Server Assignment	Assign Now Assign Server from a Resource Pool Assign Later
Compute Configuration Management Configuration	 Click the appropriate button to assign a server now, from a resource pool, or later. If you choose to assign a server now, select the server, click Next, and select and attach policies to the server profile.
5 Storage Configuration	Q, Add Filter C 4 items found 10 ∨ per page K < 1 of 1 > > ③
6 Network Configuration	Name User Label Health Model UCS Domain Serial Nu CiscoLab-1-1 CiscoLab-1-1 @ Healthy UCSX-210C-M6 CiscoLab FCH243974WA
7 Summary	Image: CliscoLab-1-2 Image: Healthy UCSX-210C-M6 CliscoLab FCH2446721K CliscoLab-1-3 Image: Healthy UCSX-210C-M6 CliscoLab FCH250671MR CliscoLab-1-5 Image: Healthy UCSX-210C-M6 CliscoLab FCH250671FA
	Selected 1 of 4 Show Selected Unselect All
<	Close Back Nex

Step 5Select the UUID Pool you created earlier and select the corresponding BIOS, Boot
Order, Power, and Virtual Media policies that you previously created. Then click
Next.

Create UCS Server F	Profile	
General	Compute Configuration Create or select existing Compute policies that you want to associate with this profile.	
Server Assignment	UUID Assignment	
3 Compute Configuration	Pool Static	
4 Management Configuration	UUID Pool	
5 Storage Configuration	Selected Pool Pod2UUID-Pool × Ф 🖉	
6 Network Configuration	BIOS Pod2BIOS-Policy fil	
	Boot Order Pod2BFS-BOOT	
7 Summary	Virtual Media Pod2Power-Policy	
<	Close	Back Next

Step 6 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.

eate UCS Server	Profile			
General	Management Conf Create or select existing	iguration Management policies that you want to associate with this profile.		
Server Assignment		Certificate Management		
Compute Configuration		IMC Access	Pod2IMC-Policy	
Management Configuration		IPMI Over LAN		
		Local User	Pod2USER-Policy	
Storage Configuration		Serial Over LAN	Pod2SerialLAN-Policy	
Network Configuration		SNMP	SNMP 🗐	
Summary		Syslog	SYSLOG	
Summary		Virtual KVM	Pod2KVM-Policy	
<	Close			Back

Step 7 Skip the Storage Configuration by clicking **Next**.

Step 8 Click on **Select Policy** to the right of **LAN Connectivity** and then select **Create New**.

Create LICS Server I	Profile	Select LAN Connectivity	×
		Policies 2	Create New
		Q Search	
General	Network Configuration	Z_DemoMW-LANPolicy	۲
Ŭ	Create or select existing Network Configuration policies that you want to associate with this profile.	TestLCP	٢
Server Assignment	LAN Connectivity		
Compute Configuration	SAN Connectivity		
Management Configuration	 Auto Placement Configuration for vNICs & vHBAs 		
Storage Configuration	Graphical representation of vNICs & vHBAs placement is only applicable for Auto Configuration		
6 Network Configuration			
7 Summary	зœ		
	No vNICs & vHBAs Placement Available Assign server and attach LAN/SAN connectivity policies to view representation		

Step 9 Name the policy **PodXLAN-Policy**, where X is your pod number and click **Next**.

olicy Details							
I policy details							
Enable Azure Stack H	ost QoS 💿						
QN							
None	Pool	Static)				
• This option ensures the	IQN name is not a	ssociated with the polic	cy .				
NIC Configuration							
Manual vNICs Plac	ement	Auto vNICs Place	ement				
• For auto placement opt	ion the vNICs will I	be automatically distribu	ited between adaptors	during profile depl	oyment. Learn more	at Help Center	
Add vNIC							
	dd Filter				0 items found	50 ∨ perpage K < 0 of 0 > >	(c)
Name	≎ Swit	ch ID	C Failover	÷	Pin Group	C MAC Pool	÷
			NO TI LIVIS AV	AILABLL			

Step 10 Make sure you select the **Auto vNICs Placement** option and then click **Add vNIC**.

Step 11 Name the vNIC **PodX-vNIC0**, where X is your pod number. For the MAC address pool, select the pool you previously created.

General			
Name * Pod2-vNIC0	0	Pin Group Name	~ 0
MAC			
Pool Static MAC Pool * ○ Selected Pool Pod2MAC-Pool × ●			

- **Step 12** Scroll down the page. For the required policies, select the following:
 - Ethernet Network Group Policy: ENG
 - Ethernet Network Control Policy: EnableCDP
 - Ethernet QoS Policy: AdapterQoS
 - Ethernet Adapter: AdapterPolicy

Step 13 Then click **Add**.

Ethernet Network Group Policy * O
Selected Policy ENG × 💿 🖉
Ethernet Network Control Policy * 💿
Selected Policy EnableCDP × ©
Ethernet QoS * O
Selected Policy AdapterQOS × ③
Ethernet Adapter * 🛛
Selected Policy AdapterPolicy × © 🖉

Step 14 On the next screen click **Create**. And on the following screen, click **Next**.

d policy details				
Enable Azure Stack Host QoS \odot				
IQN				
None Pool	Static			
• This option ensures the IQN name is no	associated with the policy			
vNIC Configuration				
Manual vNICs Placement	Auto vNICs Placement			
For auto placement option the vNICs will be a set of the vNICs will be a	I be automatically distributed between adaptors	during profile deployment. Learn mo	re at Help Center	
For auto placement option the vNICs wi Add vNIC	I be automatically distributed between adaptors	during profile deployment. Learn mo	re at Help Center	
For auto placement option the vNICs will Add vNIC Q	I be automatically distributed between adaptors	during profile deployment. Learn mo	re at Help Center 50 ∽ per page ເ≮ < 1 of 1 > [X ©
For auto placement option the vNICs will Add vNIC Add vNIC Add vNIC Name Swi	II be automatically distributed between adaptors tch ID : Failover	during profile deployment. Learn mo 1 items found : Pin Group	50 ~ per page K < 1 of 1 > : MAC Pool	× \$
For auto placement option the vNICs will Add vNIC Add vNIC Name Swi Pod2-vNIC0 A	II be automatically distributed between adaptors tch ID : Failover Disabled	during profile deployment. Learn mo 1 items found : Pin Group -	50 ~ per page (K < 1 of 1)	× © : Ø
For auto placement option the vNICs with add vNIC Add vNIC Name Swi Pod2-vNIC0 A	Il be automatically distributed between adaptors tch ID : Failover Disabled	during profile deployment. Learn mo 1 items found : Pin Group -	Fe at Help Center 50 ∽ per page € € 1 of 1 2 C MAC Pool Pod2MAC-Pool € € 1 c	X ♀
-	Network Configuration			
--------------------------	--	--	--	
General	Create or select existing Network Configuration policies that you want to associate with	In this profile.		
Server Assignment	LAN Connectivity	Pod2LAN-Policy		
Compute Configuration	SAN Connectivity			
Management Configuration				
Storage Configuration				
Network Configuration	I	:@		
Summary	No VNICs & VHE	SAs Placement Available		
	Assign server and attach LAN/SAN	connectivity policies to view representation		

Step 15 Review your configuration. Click on the Network Configuration tab to see a graphical view of your vNIC configuration. When you are done reviewing, click Deploy. When asked to confirm, verify that you are deploying to the server for your pod, then click Deploy again.

Create UCS Server	Profile
General	Summary Verify details of the profile and the policies, resolve errors and deploy.
Server Assignment	General
Compute Configuration	Organization Status default <u>A Not Deployed</u>
Management Configuration	Name Management IP Pod2ServerProfile -
Storage Configuration	Assigned Server CiscoLab-1-2
Network Configuration	Target Platform UCS Server (FI-Attached)
Summary	
	Compute configuration wanagement Configuration Storage Configuration Retwork Configuration Enors/Wannings (0)
	BIOS Pod2BIOS-Policy
	Power Pold2Power-Policy
	UUID Pod2UUID-Pool 💥
	Virtual Media Pod2VMedia-Policy
<	Close Back Deploy

Task 10 has been completed!

Task 11 – Server Profile Template Deployment

In this section, you will create and deploy a Server Profile Template to an available server using the policies and pools we have previously created.

Procedure

Step 1 In the menu, click on Templates and then select Create UCS Server Profile Template.

Templates			Create UCS Server Profile Template
UCS Server Profile Templates			
* All UCS Server Prof ◎ +			C Export 2 items found 10 ∨ per page K < 1 of 1 ≥ ≥
Name	t Usage	Target Platform Description	Last Update 2 🖗
TEST_TEMPLATE	1	UCS Server (FI-Attached)	Nov 30, 2022 2:39 PM ····
JohnTemplate	0	UCS Server (Standalone)	Sep 15, 2022 2:47 PM
0 0 ti			K C 1 of 1 2 X

Step 2 Name the template **PodXServerProfileTemplate**, where X is your pod number. Also, ensure that the **UCS Server (FI-Attached)** radio button is selected and click **Next**.

Cre	ate UCS Server F	Profile Template
1	General	General
2	Compute Configuration	Enter a name, description, tag and select a platform for the server profile template. Organization *
3	Management Configuration	default ~
4	Storage Configuration	Name * 0 Pod2ServeProfileTemplate 0
5	Network Configuration	Target Platform 0
6	Summary	UCS Server (Standatone) UCS Server (FI-Attached)
		Description
	<	Close Next

Step 3 On the Compute Configuration page, select the UUID pool for your pod and the corresponding policies you previously created for BIOS, Boot Order, Power, and Virtual Media and click Next.

	- (1) - 1			
Create UCS Server	Profile Templa	ate		
	Compute Configur	ation		
General	Create or select existing (Compute policies that you want to associate with this template.		
2 Compute Configuration		UUID Assignment		
3 Management Configuration		UUID Pool		
		Select Pool		
4 Storage Configuration		BIOS	Pod2BIOS-Policy	
5 Network Configuration		Boot Order	Pod2BOOT-Policy	
		Power	Pod2Power-Policy	
6 Summary		Virtual Media	Pod2VMedia-Policy	
l				
<	Close			Back Next

Step 4 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.

Edit UCS Server Pro	file Template	(Pod2ServerProfileTemplate)		
General	Management Confi Create or select existing M	guration Management policies that you want to associate with this template.		
Compute Configuration		Certificate Management		
3 Management Configuration		IMC Access	Pod2IMC-Policy	
4 Storage Configuration		IPMI Over LAN		
		Local User	Pod2USER-Policy	
5 Network Configuration		Serial Over LAN	Pod2SerialLAN-Policy	
6 Summary		SNMP	SNMP 🗐	
		Syslog	SYSLOG	
		Virtual KVM	Pod2KVM-Policy	
<	Close			Back Next

Step 5 Click **Next** on the Storage Configuration screen.

Step 6 On the **Network Configuration** screen, select the **LAN Connectivity** policy that you previously created and then click **Next**.

Edit UCS Server Pro	ofile Template	(Pod2ServerProfileT	emplate)		
General	Network Configura Create or select existing t	tion Vetwork Configuration policies that you want to a	ssociate with this template.		
Compute Configuration		LAN Connectivity		Pod2LAN-Policy	
Management Configuration		SAN Connectivity			
Storage Configuration					
5 Network Configuration					
6 Summary					
<	Close				Back Next

Step 7 Review your configuration and then click **Derive Profiles**. On the next screen, select **Assign Later** and click **Next**.

Derive		
1 General	General Select the server(s) that need to be assigned to profile(s) or specify the number of profiles that you want to derive and assign the servers later.	
2 Details	UCS Server Profile Template	
3 Summary	Name Organization Pod2ServerProfileTemplate default Target Platform UCS Server (FI-Attached)	
	Server Assignment	
	Assign Now Assign Server from a Resource Pool Assign Later	
	Number of Profiles to derive * 1 1 1 1 1	
<	Cancel	Next

Step 8 Accept the defaults on the next screen and then click **Next**.

Derive					
General	Details Edit the description, tage	s, and auto-generated names of the profiles.			
2 Details		General			
3 Summary		Organization * default	~	Target Platform UCS Server (FI-Attached) ~ 0	
		Description	<i>#</i> <= 1024		
		Derive			
		1 Name * Pod2ServerProfileTemplate_DERIVED-1			
	(Close				Rock New

Step 9 Review your configuration and then click **Derive**.

erive							
General		Summary Summary of the profiles that r	leed to be derived from the profile to	emplate.			
Oetails		General					
3 Summary	I	Template Name Pod2ServerProfileTemplat Target Platform UCS Server (FI-Attached)	e	Organization default	1		
		UCS Server Profiles		Assigned 5	Server		
		Pod2ServerProfileTempla	te_DERIVED-1	-			
		Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)	
		BIOS				Pod2BIOS-Policy	
		Boot Order				Pod2BOOT-Policy	1
		Power				Pod2Power-Policy	1
		Virtual Media				Pod2VMedia-Policy	
	<	Close					Back

Task 11 has been completed!

Task 12 – Virtual Media Using OS Links

The purpose of this section is to introduce the learning to the concept of using OS links. OS links are used to enable to a remote repository to install an operating system from. We will guide the student to where the OS links are located and then how to use the OS links to do an installation of ESXi.

Procedure

- Step 1On the left-hand side of the screen, click on Software Repository under the ADMIN
menu. This brings you to the area of the dashboard that is used to map remote
- **Step 2** On the top of the page, you will see links to different types of ISOs (Firmware, OS Image, SCU, OS Configuration) that can be used. Click on the **OS Image Links** tab. This will display the available OS ISOs available for mapping.

o	Settings	Software	e Reposi	tory								
U	Admin ^	Eirmutere Linke	OC Image Links	CCI Linke	OS Configurat	on Fil						
	Targets	FILLIWATE LITKS	OS Image Links	SCO LINKS	05 Comigurat		45					
	Software Repository										Add Os	8 Image Link
	Tech Support Bundles											
	Audit Logs	* All OS Imag	ge Links 🐵 🕂									
	Sessions		Add Filt	er				C Export	1 items found	10 v per	page 🖂 🗧 d	of 1 > 기
	Licensing	Name	\$	/endor	: Version	÷	File Location		0 Descr	iption :	Last Update	÷ 9
		VMware	7.0.2	/Mware	ESXi 7.0 U2		https://content.sunsetlearning.com/UCSX_Files/VMware_ESXi_7.0.2_1786	7351_Custom_0	Cisco_4.		Nov 2, 2021 2:15	5 PN
											K < 1 ¢	of 1 🗵 🗵

Step 3 Click on the **SCU Links** tab to view the available Server Configuration Utility ISOs that are available. These files are used to download the drivers for the selected operating system.

Soft	oftware Repository											
Firmware	Links OS Image Links	SCU Links	OS Configuration Fil	es								
											Add SCU Lin	ık
* A	ISCU Links ⊚ +											
Ū	🖉 🧷 🔤 🔍 Add Fi	Iter						🕒 Export	1 items found	10 🗸 per page 📧 <	1 of 1 > >	
	Name	C Version	\$	Supported Models	¢	File Location	÷	Description	÷	Last Update	÷ 4	
	SCULink	6.2.1		x210c		https://content.sur	nsetlearning.co			Nov 15, 2021 10:24 AM		
Ū											1 of 1 🗵 🗵	

- **Step 4** To use these remote file links, click on the **Servers** menu under **OPERATE** on the left navigation pane.
- **Step 5** Then click on the ... next to your server and you will see **Install Operating System** option. You will use this option in the next task.

Task 12 has been completed!

Task 13 – Installing VMware ESXi

In this section you will go through the steps of installing ESXi on one of the servers via Intersight.

Note: There are two ways to install an operating system on a server:

- 1. Via Intersight (as shown in this task); and
- 2. Via the vKVM (as you will do in the next task)
- **Caution** In this task, you will go through the steps to install an OS via Intersight, but you will not perform the actual OS installation. In the next task, you will install the OS via the vKVM on the server.

Procedure

Step 1 On the left-hand side of the screen, under **OPERATE**, click on **Servers**, and then select the **ellipsis** (...) next to your server. You will see in the drop-down that there is an **Install Operating System** option, select it.

··· 🖉 🔍 Add Filt	r				Export 6 items found 10	Power
Health	Power	HCL Status	Models	Contract Status	Profile Status	System
6 • Healthy 6	© Off 3 © On 3	Incomplete 5 A Not Listed 1	6 • UCSX 210C-M6 @	Not Covered 6 6	5 • Failed 2 • Not Assigned 2	Install Operating System
						Launch vKVM
Name :	Health : Contr	act S CLicense Tier	C Management IP C S	Server Profile : Model	0 0 M 0 Fi 0	Launch vKVM
Name : O CiscoLab-1-1	Health : Contr Healthy © No Healthy © No	act S : License Tier t Covered Advantage t Covered Advantage	: Management IP : 1	Server Profile : Model UCSX-21 Dod2ServerProfile II UCSX-21	C-M 145.6 2048.0 5.0(1b)	Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier
Name : O CiscoLab-1-1 O CiscoLab-1-2 @ O CiscoLab-1-3	Health : Contr Healthy © No Healthy © No Healthy © No Healthy © No	act S : License Tier t Covered Advantage t Covered Advantage t Covered Advantage	Management IP 10.10.63.142	Server Profile : Model UCSX-211 Pod2ServerProfile @ UCSX-21 UCSX-21	C-M 145.6 512.0 5.0(1b)	Launch vKVM Launch vKVM Qpen TAC Case Set License Tier Collect Tech Support Bunc
Name : O CiscoLab-1-1 O CiscoLab-1-2 @ O CiscoLab-1-3 O CiscoLab-1-4	Health : Contr Healthy © No Healthy © No Healthy © No Healthy © No Healthy © No	act S : License Tier t Covered Advantage t Covered Advantage t Covered Advantage t Covered Advantage	Management IP : 1 10.10.63.142	Server Profile Model UCSX-211 UCSX-211 Pod2ServerProfile UCSX-211 UCSX-211 UCSX-211 JohnSP1000 UCSX-211	: O : M : FL. : c: 0 : M : FL. : 0 : : 0 : 0 : 0 : : : 0 : <td>Launch vKVM Launch vKVM Open TAC Case Set License Tier Collect Tech Support Bunc</td>	Launch vKVM Launch vKVM Open TAC Case Set License Tier Collect Tech Support Bunc
Name : O Ciscolab-1-1 O Ciscolab-1-2 G O Ciscolab-1-3 O Ciscolab-1-4 O Ciscolab-1-4 O Ciscolab-1-5	Health : Contr Healthy © No Healthy © No Healthy © No Healthy © No Healthy © No Healthy © No	act S : License Tier t Covered Advantage t Covered Advantage t Covered Advantage t Covered Advantage t Covered Advantage	Management IP 2 10.10.63.142 1	Server Profile Model UCSX-21 UCSX-21 Pod2ServerProfile UCSX-21 UCSX-21 UCSX-21 JohnSP1000 UCSX-21 UCSX-21 UCSX-21	: 0 : M : FL : DC-M 145.6 2048.0 5.0(1b) DC-M 99.2 256.0 5.0(1b) DC-M 145.6 512.0 5.0(1b)	Launch YKVM Launch TKNHeled YKVM Open TAC Case Set License Tier Collect Tech Support Bunc

Step 2 On the **General** screen, ensure that only your server is selected and click **Next**.

General	General Select the servers for the	the Operating System installation				
Operating System		Select Servers				
Configuration						
Server Configuration Utility		Add Filter Name : User Label	G 6 items found : Health :	10 ∨ per page K C Model :	1 of 1 D D O Serial Number :	
Installation Target		CiscoLab-1-1	Healthy	UCSX-210C-M6	FCH243974WA	
		CiscoLab-1-2	© Healthy	UCSX-210C-M6	FCH2446721K	
Summary		CiscoLab-1-3	© Healthy	UCSX-210C-M6	FCH250671MR	
		CiscoLab-1-4	O Healthy	UCSX-210C-M6	FCH250671QN	
		CiscoLab-1-5	Healthy	UCSX-210C-M6	FCH250671FA	
		CiscoLab-1-6	Healthy	UCSX-210C-M6	FCH251372QT	
		Selected 1 of 6 Show Selected Uns	slect All			

Step 3 Next, you will select the operating system that will be installed on the server. In the list of operating systems, select the **VMware7.0.2** radio button and then click **Next**.

2	Operating System	Select Operating System Image	
3	Configuration	Add OS Image Link	
4	Server Configuration Utility		
5	Installation Target	 Selected servers belong to single organization: 'default'. You can choose to install Operating System from one of the common organizations. Learn more at Help Center. 	
6	Summary	1 items found 10 - per page (if < 1 of 1 >))	
		Q Add Filter	
		Name C File Location C V. C	
		VMware7.0.2 https://content.sunsetlearning.com/UCSX_Files/VMware_ESXi_7.0.2_17867351_CustomVMw	
		Selected 1 of 1 Show Selected Unselect All C C 1 of 1 2	

- **Step 4** Now, you will create the configuration for the server. Click on the + next to your server and fill in the following information:
 - Keep Static IP selected
 - Keep the **IPv4** radio button selected
 - IP Address = 10.10.63.14X (Where X is your Pod number)
 - Netmask = **255.255.255.0**
 - Gateway = **10.10.63.254**
 - Name Server = **8.8.8.8**
 - Hostname = **PodXServer** (Where X is your Pod number)
 - Password = Cisco123!!

Step 5 Click Next.

Install Operating Sys	tem				
General Operating System Gonfiguration Server Configuration Utility Installation Target		CiscoLab-1-2 Static IP DHCP Configuration PConfiguration PY4 IPY6 PAddress * 0.10.63.142	Ø	Netmask * 255 255 255 0	
6 Summary	G 10 N. 8.	ateway * 0.10.63.254 iame Server * .8.8.8	0	Hostname * Pod2Server 0	
	Pr 	letwork Device assword *	0	<u>VLAN ID β ο</u> 1 - 4095	
<	Cancel				Back Next

Step 6 On the next page, you will find the SCU link. This is the Server Configuration Utility that is used to download drivers for the operating system during the installation. Select **SCULink** and press **Next**.

	Server Configuration Utility
General	Select a Software Configuration Utility from the list or add a new image to the repository
Operation Sustem	Select Server Configuration Utility
Operating System	
Configuration	Add SCU Link
Server Configuration Utility	
Installation Target	 Server Configuration Utility images are filtered based on the Operating System image selection. Learn more at Help Center.
Summary	 Installing an Operating System is supported only if the Server Configuration Utility image is at version 8.1.3(x) and later.
	1 Items found <u>10 ∨</u> per page <u>01</u> (<u>1</u> of 1 (10) (2) Q. Add Fitter
	Name : File Location : V. : S. :
	SCULink https://content.sunsetlearning.com/UCSX_Files/ucs-cxxx-scu-(6.2.1 x210c
	Selected 1 of 1 Show Belected Unselect All

Step 7 On the Installation Target screen, you will see a drop-down under Prefill with Installation Target*. Click the drop-down and select the MRAID VD option and then click Next.

Note: The options shown in the drop-down list may be different from what is shown below. Select the option that includes MRAID VD as part of the name.

istall Operating S	ystem				
General	Installation Ta	arget			
	Set the installation	in larger for selected servers			
Operating System		Select Installation Target			
Configuration		• You can prefill or manually se	t the installation targets for selected serve	rs. When you prefill, installation targets apply to	
		corresponding servers with t about the installation target v	ne selected target type. Only valid installati alidation criteria at Help Center.	on targets are shown for selection. Learn more	
Server Configuration Utility		Ŭ			
5 Installation Target		 Virtual drives must be in the Learn more at Help Center. 	optimal state and physical disks must be in	the healthy state to be listed as valid install targets.	
	1				
6 Summary			× 0		
		Show Servers Without Sele	cted Target (0)		
		Name	Serial	Installation Target	
		CiscoLab-1-2	FCH2446721K	MRAID VD: 239 - Boot Drive v	
<	Cancel				Back

Step 8 On the **Summary** screen, review your configuration then click **Cancel** to cancel out of this OS installation.

stall Operating Sy	/stem	
General	Summary Verify details of your selections, make changes where required and proceed to install the Operating System	
Operating System	Selected Servers	
Configuration		
Server Configuration Utility	Q, Add Filter	
Installation Target	Name : User Label : Health : Model : Serial Nu : Installation Tar	
6 Summary	CiscoLab-1-2 • Healthy UCSX-210C-M6 FCH2446721K MRAID VD: 239 # (1 of 1) #	
	Operating System image	
	Name Version VMware70.2 ESXi 7.0 U2 Vendor VMware	
	Server Configuration Utility	
<	Cancel	Back

Step 9 You will receive a pop up stating your changes will not be saved. Click the **Leave** button to leave the OS installation wizard.

Leave Page?		
Changes you made may not t	be saved.	
	Cancer	Leave

Note If you had started the OS install process, you could review the progress of the installation by click on the Requests link at the top of the screen. You should see your installation In Progress and can click on the In Progress entry to get a more detailed view of the installation process.

Task 13 has been completed!

Task 14 – Accessing the KVM and Installing an Operating System (Do Not Attempt)

In this section you will be using the Virtual Media option in the KVM to install an Operating System.

Note: You will need to be connected to the SLI VPN before you can perform this task.

Procedure

Step 1 On the left-hand side of the screen, under **OPERATE**, click on **Servers**, and then select the **ellipsis** (...) next to your server. You will see in the drop-down that there is a Launch **KVM** option, select it.

Vers										
* All Servers ⊚ + ··· ⊘ ♀ Add Filter					G	Export 6	items found	10 v p	Power	
Health 6 • Healthy 6	Power © Off 3 © On 3	HCL State	USX 2100	Contract 5	Status d 6	Profile	• Status • Failed 2 • Not Assig • OK 1	gned 2	System Profile Install Operating System Upgrade Firmware	
									Launch vKVM	
Name :	Health :	Contract S CLice	nse Tier C Management IP	C Server Profile C	Model :	0 : M 145.6	M : Fi.	: l	Launch vKVM Launch Tunneled vKVM Open TAC Case	
Name : CiscoLab-1-1 CiscoLab-1-2 I	Health : Healthy Healthy	Contract S CLice Not Covered Adva Not Covered Adva	nse Tier : Management IP	Server Profile Pod2ServerProfile D	Model : UCSX-210C-N UCSX-210C-N	© ≎ M 145.6 M 99.2	M. C Fi. 2048.0 5.0 256.0 5.0	¢ l 0(1b) 0(1b)	Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier	
Name : (2) CiscoLab-1-1 (2) CiscoLab-1-2 (2) CiscoLab-1-3	Health : Healthy Healthy Healthy	Contract S : Lice © Not Covered Adva © Not Covered Adva © Not Covered Adva © Not Covered Adva	nse Tier : Management IP antage antage 10.10.63.142 antage	Server Profile Pod2ServerProfile	Model : UCSX-210C-1 UCSX-210C-1 UCSX-210C-1	© : M 145.6 M 99.2 M 145.6	M : Fi. 2048.0 5.0 256.0 5.0 512.0 5.0	÷ l 0(1b) 0(1b) 0(1b)	Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier Collect Tech Support Bur	ndl
Name : O CiscoLab-1-1 O CiscoLab-1-2 Ø O CiscoLab-1-3 O CiscoLab-1-3 O CiscoLab-1-4 O CiscoLab-1-4	Health : Healthy Healthy Healthy Healthy Healthy	Contract S : Lice © Not Covered Adva © Not Covered Adva © Not Covered Adva © Not Covered Adva	Inse Tier C Management IP Inse Tier C Management IP Insertion II Insert IP Insert II I	Server Profile S Pod2ServerProfile JohnSP1000	Model : UCSX-210C-1 UCSX-210C-1 UCSX-210C-1 UCSX-210C-1	© : M 145.6 M 99.2 M 145.6 M 145.6	M. C. Fi. 2048.0 5.0 256.0 5.0 512.0 5.0	0 (1b) 0(1b) 0(1b) 0(1b) 0(1b)	Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier Collect Tech Support Bur	ndk
Name : O CiscoLab-1-1 O CiscoLab-1-2 O CiscoLab-1-3 O CiscoLab-1-3 O CiscoLab-1-4 O CiscoLab-1-5	Health : Healthy Healthy Healthy Healthy Healthy Healthy	Contract S : Lice O Not Covered Adva	Inse Tier C Management IP Instage 10.10.63.142 Instage 10.10.63.142 Instage Instage In	Server Profile C Pod2ServerProfile C	Model : UCSX-210C-1 UCSX-210C-1 UCSX-210C-1 UCSX-210C-1 UCSX-210C-1	© : M 145.6 M 99.2 M 145.6 M 145.6 M 145.6	M. Fil. 2048.0 5.0 256.0 5.0 512.0 5.0 512.0 5.0 512.0 5.0	0 (1b) 0(1b) 0(1b) 0(1b) 0(1b) 0(1b)	Launch vKVM Launch Tunneled vKVM Open TAC Case Set License Tier Collect Tech Support Bur	ndl

Step 2 A new window will pop up with a button that says **Load KVM Certificate**, click that button. You may get a security warning. Accept the security warning to display the KVM.





Step 3When the KVM loads, click on the Virtual Media menu option, and select vKVM-
mapped vDVD option. This will bring up the option to browse for the installation ISO
file.



NOTE: If the instructor has not already provided the link, please ask them for it now.



≡	.1 1.1 1. cisco	
5-		Reboot and Select proper Boot device
		or Insert Boot Media in selected Boot device and press a key
0		
(⁶)		
×		Map Virtual Media - CD/DVD
\bigcirc		Browne Calacted File VAAware ESVi 7.0.2.1796
		Cancel Map Drive

Step 5Click on the Boot Device menu option. Select vKVM-Mapped vDVD from the select
list. Then read the Boot Device message and click Confirm to confirm your choice.

_					
	Boot Device	>	None		
	Virtual Media	>	vKVM-Mapped vDVD		
	Chat		Local HDD		
E	Boot Device		♥		
You are about to change the one-time boot device. The server will boot from the selected boot device only for the next server boot, without disrupting the currently configured boot order. Once the server boots from the one-time boot device, all its future reboots occur from the previously configured boot order. Are you sure you want to continue?					
Y fi d ti c	You are about to change f rom the selected boot de lisrupting the currently co he one-time boot device, onfigured boot order. Are	the one- evice on onfigure all its fu e you su	time boot device. The server will boot ly for the next server boot, without d boot order. Once the server boots from iture reboots occur from the previously re you want to continue?		

Step 6 Another way to boot from the virtual media is to reset the server, and after the RAID controller BIOS message completes, press <F6> for the Boot Menu. You can select **Cisco kVM-Mapped vDVD2.00** from there.

CISCO Copyright (c) 2021 Cisco Systems, Inc	For the boot menu, immediately press <f6> when you see this screen.</f6>
Press <f2> Setup : <f6> Boot Menu : Bios Version : X210M6.5.0.di.0.081621 Platform ID : X210M6</f6></f2>	<f12> Network Boot 1754</f12>
Please select boot Cisco vKVM-Mapped vDVD UEFI: Built-in EFI She Enter Setup	2.00 211
↑ and ↓ to move se ENTER to select boo ESC to boot using	election ot device defaults

Step 7 To get the installation going, you will need to reset the server. Select the **Power** menu option and then click on **Reset System**. Confirm the warning message by clicking **Confirm**.

≡	cisco	Intersight	Sunset-1-4 KVM Console	
5-			Reboo	t and Select momer Boot device
			or In	sert Boot Media in selected Boot device and press a key_
0				
୍ ଡୁଡ଼ି ଡ				
×				\wedge
\bigcirc				
	Boot Devic			You are about to execute a server control action. Are you sure you want to
٥	Virtual Me			continue?
	Chat			Cancel

Step 8 The server should automatically boot the installation ISO and begin the installation process.



Loading ESXi installer

Loading /b.b00 Loading /b.b00 Loading /junpstrt.gz Loading /vseropts.gz Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /procfs.b00		
Loading /b.b00 Loading /junpstrt.gz Loading /vseropts.gz Loading /features.gz Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /procfs.b00	Loading	/boot.cfg
Loading /jumpstrt.gz Loading /veropts.gz Loading /features.gz Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vwx.v00	Loading	/b.b00 -
Loading /useropts.gz Loading /features.gz Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vnx.v00	Loading	/jumpstrt.gz
Loading /features.gz Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vwx.v00	Loading	/useropts.gz
Loading /k.b00 Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vnx.v00	Loading	/features.gz
Loading /uc_intel.b00 Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vnx.v00	Loading	/k.b00
Loading /uc_and.b00 Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vmx.v00	Loading	/uc_intel.b00
Loading /uc_hygon.b00 Loading /procfs.b00 Loading /vmx.v00	Loading	/uc_and.b00
Loading /procfs.b00 Loading /vmx.v00	Loading	/uc_hygon.b00
Loading /vmx.v00	Loading	/procfs.b00
	Loading	/vmx.v00



Step 9 Please wait several minutes for the installation ISO to load the installer. You will then be prompted to continue the installation; press **Enter** to continue.



Step 10 Accept the EULA by pressing **F11**.



Step 11 Next, you will be presented with the installation location. Ensure that the **RAIDF** option is selected, and then press **Enter**.



Step 12 You will then be asked to select the language. Select the **US Default** and press **Enter**.

Please select a keyboard layout
Swiss French Swiss German Turkish US Default US Dvorak Ukrainian United Kingdom
Use the arrow keys to scroll.
(Esc) Cancel (F9) Back (Enter) Continue

Step 13 Now you will create the password for root console access to the server. Use the password of **Cisco123!!** and confirm it before pressing **Enter** to continue.



Step 14 The last step is to confirm the installation options and press **F11** to install.



Step 15 The installation should begin.



Step 16 The last step of the installation is to reboot the server. Press **Enter** to reboot the server.



Step 17 Observer the boot up process and ensure that the login screen is displayed before moving forward.

Task 14 has been completed!

Task 15 – Server Profile Deployment (Do Not Attempt)

In this section, you will create and deploy a Server Profile to an available server using the policies and pools we have previously created.

Procedure

Step 1 On the left-hand side of the screen, under CONFIGURE, select Profiles. Then click on the UCS Server Profiles tab.

≡	disco Intersight	*	Infrastructure Service 🗸				Q Search	ା ତ ସା ଦ୍	م ا 🕲 🚥
	Overview		Profiles						
0	Operate Servers	^	HyperFlex Cluster Profiles UCS Chassis Pro	ofiles UCS Domain F	Profiles UCS Server Profi	05			
	Chassis Fabric Interconnects HyperFlex Clusters		+ All UCS Server Prof.,				G Expert	Altems found 16 ~ per page .	CS Server Profile
.0	Configure	~	Name :	Status :	Target Platform	UCS Server Template	Server	Resource Pool	Last 9
	Profiles		JohnSP1000	() OK	UCS Server (FI-Attached)		CiscoLab 1-4		Dec ···
	Templates		TT_Server_Profile	III Falled	UCS Server (FI-Attached)		CiscoLab-1-6		Dec ····
	remponent		Z_DemoMW-ServerProfileTemplate_D	(E) Not Assigned	UCS Server (FI-Attached)	TEST_FEMPLATE			Nov ····
	Policies		Test ServiceProfile	() Not Assigned	UCS Server (FI-Attached)				Nov ····
	Pools		a. 						1 of 1 🗍 🕅

- Step 2 Click on the Create UCS Server Profile button.
- **Step 3** Name the Server Profile **PodXServerProfile**, where X is your pod number and ensure that the **UCS Server (FI -Attached)** radio button is highlighted. Then click **Next**.

Create UCS Server	Profile		
1 General	General Enter a name, description, tag and select a platform for the server profile.		
2 Server Assignment	Organization * default	U.S. C.	
3 Compute Configuration			
4 Management Configuration	Name * Pod2ServerProfile	٥	
5 Storage Configuration	Target Platform		
6 Network Configuration	UCS Server (Standalone) UCS Server	r (FI-Attached)	
7 Summary			
	Description		
		<= 1024	
<	Close		Back Next

Step 4 Select the server that corresponds to your Pod X and click **Next**.

Create UCS Server	Profile
General	Server Assignment Choose to assign a server now, from a resource pool, or later.
2 Server Assignment	Assign Now Assign Server from a Resource Pool Assign Later
3 Compute Configuration	 Click the appropriate button to assign a server now, from a resource pool, or later. If you choose to assign a server now, select the server click Next and select and attach onlicies to the server profile.
4 Management Configuration	
5 Storage Configuration	Q_ Add Filter G 4 items found 10 ∨ per page K 1 of 1 > I
6 Network Configuration	Name User Label Health Model UCS Domain Serial Nu Ciscolab Ciscolab-1-1 © Healthy UCSX-210C-M6 Ciscolab FCH243974WA
7 Summary	CiscoLab-1-2 O Healthy UCSX-210C-M6 CiscoLab FCH2446721K
	CiscoLab-1-3 C Healthy UCSX-210C-M6 CiscoLab FCH250671MR
	Selected 1 of 4 Show Selected Unselect All Show Selected 1 of 4 Show Selected 1 of 5 Selected 1
<	Close Back Next

Step 5Select the UUID Pool you created earlier and select the corresponding BIOS, BOOT
FROM SAN POLICY, Power, and Virtual Media policies that you previously created.
Then click Next.

Compute Configuration							
Create or select existing Compute policies that you want to associate with this profile.							
	UUID Assignment						
	Pool Static						
	UUID Pool						
	Selected Pool Pod2UUID-Pool × 💿 🖉						
	BIOS	Pod2BIOS-Policy					
	Boot Order	Pod2BFS-BOOT					
	Power	Pod2Power-Policy					
	Virtual Media	Pod2VMedia-Policy					

Step 6 Continue to select the corresponding policies that you previously created and then click **Next**.

NOTE: We are not going to be using the Certificate Management or IPMI policies.

Ceneral	Profile Management Conf	iguration		
Server Assignment		Certificate Management		
Compute Configuration		IMC Access	Pod2IMC-Policy	
Management Configuration		IPMI Over LAN		
management configuration	I	Local User	Pod2USER-Policy	
Storage Configuration		Serial Over LAN	Pod2SerialLAN-Policy	
Network Configuration		SNMP	SNMP	
0		Syslog	SYSLOG	
Summary		Virtual KVM	Pod2KVM-Policy	
<	Close			Back

Step 7 Skip the Storage Configuration by clicking **Next**.

Step 8 Click on **Select Policy** to the right of **LAN Connectivity** and then select **Create New**.

Create LICS Server	Create UCS Server Profile						
	rionic		Policies 2	Create New			
			Q Search				
General	Network Configuration		Z_DemoMW-LANPolicy	۲			
	Create or select existing Netw	TestLCP	٢				
Server Assignment	L	AN Connectivity					
Compute Configuration	S	AN Connectivity					
Management Configuration		Auto Placement Configuration for vNICs & vHBAs					
Storage Configuration		Graphical representation of vNICs & vHBAs placement is only applicable for Auto Configuration					
Network Configuration							
7 Summary		εœ					
		No vNICs & vHBAs Placement Available					
		Assign server and attach LAN/SAN connectivity policies to view representation					

Step 9 Name the policy **PodXLAN-Policy**, where X is your pod number and click **Next**.

Policy Details Add policy details Enable Azure Stack Host QoS © IQN None Pool Static • This option ensures the IQN name is not associated with the policy vNIC Configuration Manual vNICs Placement Auto vNICs Placement • For auto placement option the vNICs will be automatically distributed between adaptors during profile deployment. Learn more at Help Cent Add vNIC 🗎 🥒 🔲 🔍 Add Filter $0 \text{ items found} \qquad 50 \lor \text{ per page } \boxtimes \boxdot 0 \text{ of } 0 \mathrel{>} \bowtie \qquad \textcircled{3}$ Name Switch ID Failover Pin Group C MAC Pool NO ITEMS AVAILABLE ancel Back Crea

Step 10 Make sure you select the Auto vNICs Placement option and then click on Add vNIC.

Step 11 Name the vNIC **PodX-vNICO**, where X is your pod number. For the MAC address pool, select the pool you previously created.

General			
Name * Pod2-vNIC0	0	Pin Group Name	× 0
MAC			
Pool Static			
MAC Pool * © Selected Pool Pod2MAC-Pool × ©			

Step 12 Scroll down the page. For the required policies, select the following:

- Ethernet Network Group Policy: ENG
- Ethernet Network Control Policy: EnableCDP
- Ethernet QoS Policy: AdapterQoS
- Ethernet Adapter: AdapterPolicy

Ethernet Network Group Policy * O					
Selected Policy ENG × 💿 🧷					
Ethernet Network Control Policy * O					
Selected Policy EnableCDP × 💿 🖉					
Ethernet QoS * 0					
Selected Policy AdapterQOS × © 🖉					
Ethernet Adapter * ©					
Selected Policy AdapterPolicy × 💿 🖉					

Step 13 Click Add.

Step 14 On the next screen click **Create**. And on the following screen, click **Next**.

Policy Details				
Add policy details				
Enable Azure Stack Host QoS \odot				
IQN				
None Pool	Static			
 This option ensures the IQN name is no 	t associated with the policy			
vNIC Configuration				
Manual vNICs Placement	Auto vNICs Placement			
• For auto placement option the vNICs w	ill be automatically distributed between adap	tors during profile deployment. Learn mo	re at Help Center	
Add vNIC				
🗊 🥒 🗍 🔍 Add Filter		1 items found	50 v per page 📧 < 1 of 1 [
Name 🗘 Sw	itch ID 🗘 Failover	2 Pin Group	C MAC Pool	÷ 9
Pod2-vNIC0 A	Disabled	-	Pod2MAC-Pool	
			K < _1	of 1 🗵 🗵
Cancel				Back Create

Create UCS Server	Profile		
General Server Assignment	Network Configuration Create or select existing Network Configuration policies that you want to associate with this profile.		
Compute Configuration	LAN Connectivity SAN Connectivity	PodZLAN-Policy	
Management Configuration	 Auto Placement Configuration for vNICs 8 vHBAs. 		
Storage Configuration			
Network Configuration	l.	:®	
7 Summary	No vNICs & vHBAP Placement Available Assign server and attach LANUSAK connectivity policies to view representation		
	Chan		Dask New

Step 15 Review your configuration. Click on the Network Configuration tab to see a graphical view of your vNIC configuration. When you are done reviewing, click Deploy. When asked to confirm, verify that you are deploying to the server for your pod, then click Deploy again.

Create UCS Server Profile			
General	Summary Verify details of the profile and the policies, resolve errors and deploy.		
Server Assignment	General		
Compute Configuration	default A Not Deployed		
Management Configuration	Name Management IP Pod2ServerProfile -		
Storage Configuration	Assigned Server CiscoLab-1-2		
Network Configuration	Target Platform		
7 Summary	UCS Server (FF-Attached)		
	Compute Configuration Management Configuration Storage Configuration Network Configuration Errors/Warnings (0)		
	BIOS Pod2BIOS-Policy		
	Boot Order Pod2BFS-BOOT		
	Power Pod2Power-Policy		
	UUID Pod2UUID-Pool 🕅		
	Virtual Media Pod2V/Media-Policy 🗐		
<	Close Back Deploy		

Step 16 Once the Server Profile deploys, the compute node will boot to a SAN device as an available option to install on. This is the FC NetApp Storage array. Please use that as the installation location for the ESXi OS.

Task 10 has been completed!

Task 16 – Submitting Feedback and Further Information

The Feedback form is the Cisco Intersight user's primary means of communication with the Cisco engineering team. It is used to submit feedback, request feature enhancements, and report issues.

Procedure

- **Step 1** In the top toolbar of the Cisco Intersight dashboard, click the **Help** icon and then, select **Send Us Feedback** from the resulting menu.
- **Step 2** Briefly show the form then, explain its purpose and then, click **Cancel**.

Send Us Feedback ×				
Send Feedback	Report Defect			
Rate your experience of using Intersig	Ilent			
Leave your comment or enhancement				
	Cancel Submit			

What's Next

For More Information

For more information on Cisco UCS Cisco Intersight, visit the following websites:

cisco.com/go/Cisco Intersight

https://Cisco Intersight.com

communities.cisco.com/ucs

How to Find Support Information

The purpose of this section is to show where to locate the latest support information for Cisco Intersight. Click the links below:

https://Cisco Intersight.com/help/ https://Cisco

Intersight.com/help/supported_systems