..|...|.. cisco

White Paper Public

# Configure Cisco Intersight Managed Mode for FlexPod and Deploy Red Hat Enterprise Linux

## Contents

Executive summary	3
Overview	3
Solution design	7
Automated provisioning using Terraform infrastructure as code	15
Conclusion	16
Appendix: Configuration details	18

This document presents the new Cisco Intersight<sup>™</sup> Managed Mode (IMM) strategies, constructs, policies, and workflow involved in deploying the Cisco Unified Computing System<sup>™</sup> (Cisco UCS<sup>®</sup>) with SAN boot (iSCSI and Fibre Channel) in a FlexPod Datacenter environment and details steps to install Red Hat Enterprise Linux 8. It also describes automated provisioning of solution using Terraform infrastructure as code.

## Executive summary

The FlexPod solution delivers an integrated architecture that incorporates compute, storage, and network design best practices to reduce IT risks by validating the integrated architecture and helping ensure compatibility among the components. The solution addresses IT challenges by providing documented design and deployment guidance and solution support that can be used in various stages—in the planning, design, and implementation—of a deployment.

The Cisco Intersight<sup>™</sup> platform is a management solution delivered as a service with embedded analytics for Cisco<sup>®</sup> and third-party IT infrastructures. Cisco Intersight managed mode (also referred to as Cisco IMM or Intersight managed mode) is a new implementation of concepts previously introduced with Cisco UCS<sup>®</sup> Manager and moves ownership of the policy model into the Cisco Intersight platform. The Cisco Unified Computing System<sup>™</sup> (Cisco UCS) functions previously configured in a FlexPod environment using Cisco UCS Manager will now be delivered through the Cisco Intersight portal, which provides global visibility into the infrastructure health and status along with advanced management and support capabilities.

This document helps Cisco customers and business partners with the new Cisco Intersight managed mode strategies, constructs, policies, and workflow involved in deploying Cisco UCS with SAN boot in a FlexPod Datacenter environment and describes steps to install Red Hat Enterprise Linux (RHEL) 8.3. It details SAN boot configuration for both Fibre Channel and iSCSI boot scenarios. It also describes automated provisioning of solution using Terraform infrastructure as code.

Although the focus of this document is the Cisco UCS and Cisco Intersight managed mode platforms, customers interested in understanding FlexPod design and deployment details, including configuration of other elements of design and associated best practices, should refer to Cisco Validated Designs for FlexPod Datacenter at <a href="https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html">https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html</a>.

## Overview

This section provides an overview of the Cisco Intersight and FlexPod platforms.

## **Cisco Intersight overview**

The Cisco Intersight platform is a software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. With the Cisco Intersight platform, customers get all the benefits of SaaS delivery and the full lifecycle management Cisco Intersight connected distributed servers and third-party storage systems such as NetApp across data centers, remote sites, branch offices, and edge environments (Figure 1).

The Cisco Intersight platform is designed to be modular, so customers can adopt services based on their individual requirements. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers and hypervisors to serverless applications, thereby reducing costs and mitigating risk. This unified SaaS platform uses a unified OpenAPI design that natively integrates with the third-party platforms and tools.



Figure 1. Cisco Intersight overview

The main benefits of Cisco Intersight infrastructure services are summarized here:

- Simplify daily operations by automating many daily manual tasks.
- Combine the convenience of a SaaS platform with the capability to connect from anywhere and manage infrastructure through a browser or mobile app.
- Stay ahead of problems and accelerate trouble resolution through advanced support capabilities.
- Gain global visibility of infrastructure health and status along with advanced management and support capabilities.
- Upgrade to add workload optimization and Kubernetes services when needed.

## Cisco Intersight managed mode

Cisco Intersight managed mode is a new architecture that manages Cisco UCS fabric interconnected systems through a Redfish-based standard model. Cisco Intersight managed mode unifies the capabilities of Cisco UCS and the cloud-based flexibility of the Cisco Intersight platform, thus unifying the management experience for both standalone and fabric interconnect-attached systems. The Cisco Intersight management model standardizes policy and operation management for fourth-generation fabric interconnects and Cisco UCS M5 servers.

You can choose between the native Cisco UCS Manager managed mode and Cisco Intersight managed mode for fabric-attached Cisco UCS deployments during initial setup of the fabric interconnects or in a running system. The latter option is disruptive and negatively affects the endpoints and the existing configurations. If you choose to switch back to Cisco UCS Manager mode from Cisco Intersight managed mode, an option is provided to restore from a full-state Cisco UCS Manager backup.

#### **Cisco Intersight Connected Virtual Appliance and Private Virtual Appliance**

In addition to the SaaS deployment model running on Intersight.com, on-premises options can be purchased separately. The Cisco Intersight Connected Virtual Appliance and Cisco Intersight Private Virtual Appliance are available for organizations that have additional data locality or security requirements for managing systems. The Cisco Intersight Connected Virtual Appliance delivers the management features of the Cisco Intersight platform in an easy-to-deploy VMware Open Virtualization Appliance (OVA) or Microsoft Hyper-V Server virtual machine that allows you to control the system details that leave your premises. The Cisco Intersight Private Virtual Appliance is provided in a form factor specifically designed for users who operate in disconnected (air gap) environments. The Private Virtual Appliance requires no connection to public networks or back to Cisco to operate. At this time, Cisco Intersight managed mode configuration is available only through the Cisco Intersight SaaS platform and Connected Virtual Appliance.

## **FlexPod Datacenter overview**

Customers seeking to deploy applications using a shared data center infrastructure face several challenges. A recurring infrastructure challenge is achieving the required levels of IT agility and efficiency to effectively meet the organization's business objectives. Addressing these challenges requires an optimal solution with the following main characteristics:

- Availability: Help ensure that applications and services are available at all times, with no single point of failure.
- Flexibility: Support new services without requiring changes to the underlying infrastructure.
- Efficiency: Facilitate efficient operation of the infrastructure through reusable policies.
- Manageability: Facilitate ease of deployment and ongoing management, reducing operating costs.
- Scalability: Support easy expansion and growth, providing significant investment protection.
- Compatibility: Reduce risk by helping ensure compatibility of integrated components.

Cisco and NetApp have partnered to deliver a series of FlexPod solutions that enable strategic data center platforms with these characteristics. FlexPod delivers an integrated architecture that incorporates compute, storage, and network design best practices, reducing IT risks by validating the integrated architecture to help ensure compatibility among the system components.

FlexPod architecture can "flex" the environment to suit a customer's requirements. A FlexPod deployment can easily be scaled as compute, network, or storage requirements and or demands change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units). This wire-once fully validated architecture is highly resilient and cost effective and reduces customer risk.

## FlexPod components

FlexPod architecture includes the following core components (Figure 2):

- Cisco UCS
- Cisco Nexus® Family switches
- Cisco MDS Family switches
- NetApp AFF/FAS storage systems



#### Figure 2.

FlexPod Datacenter components

All the FlexPod components have been integrated so that customers can deploy the solution quickly and economically while eliminating many of the risks associated with researching, designing, building, and deploying similar solutions from the foundation. One of the main benefits of FlexPod is its ability to maintain consistency at scale. Each of the component families shown in Figure 2 (Cisco UCS, Cisco Nexus, Cisco MDS, and NetApp controllers) offers platform and resource options to scale the infrastructure up or down while supporting the same features and functions that are required under the configuration and connectivity best practices of FlexPod.

## Solution design

This section discusses the infrastructure setup, software and hardware requirements, and some of the design details of the Cisco Intersight managed mode deployment model. Specific hardware and software requirements must be followed to configure Cisco UCS using Cisco Intersight managed mode. The selection of FlexPod infrastructure components presented here closely aligns with Cisco Intersight managed mode requirements. This section does not cover the design details of FlexPod components such as Cisco Nexus and Cisco MDS switches and NetApp storage systems because their design and configuration conform to various Cisco Validated Designs for FlexPod and are covered widely elsewhere. This document focuses on the design elements of the new Cisco Intersight managed mode configuration.

## **Cisco Intersight managed mode**

Cisco Intersight managed mode enables complete configuration of multiple Cisco UCS domains and servers directly from the Cisco Intersight platform. Cisco Intersight managed mode introduces a new implementation of concepts previously introduced with Cisco UCS Manager and moves ownership of the policy model into Cisco Intersight. Fabric configuration in Cisco Intersight is first set up by deploying a Cisco UCS domain profile that encompasses all the policies related to the configuration of the switches and then associating it with server profiles. A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, simplifies the deployment of fabric interconnect pairs, allows configuration of ports and port channels, and configures the VLANs and VSANs in the network. Hence, policies, VLANs, and VSANs are created in-advance and built into a server profile. Then the server profile is assigned and deployed to a Cisco Intersight discovered Cisco UCS B-Series Blade Server or managed Cisco UCS C-Series Rack Server.

During initial fabric interconnect setup for a fabric-attached Cisco UCS deployment, customers can choose to deploy fabric interconnects and Cisco UCS in the native Cisco UCS Manager managed mode or in the new Cisco Intersight managed mode. This document discusses Cisco UCS deployment using Cisco Intersight managed mode, and all the configuration steps are performed using the Cisco Intersight SaaS platform.

Before setting up Cisco Intersight managed mode, review the supported hardware, software, and licensing requirements that follow.

## Supported hardware for Cisco Intersight managed mode

The hardware listed in Table 1 is required to deploy Cisco UCS using Cisco Intersight managed mode.

Component	Model number
Fabric interconnect	Fourth-generation fabric interconnect: UCS-FI-6454 or UCS-FI-64108
Cisco UCS B-Series Blade Servers	Cisco UCS B-Series M5: UCSB-B200-M5 or UCSB-B480-M5
Cisco UCS C-Series Rack Servers	Cisco UCS C-Series M5: UCSC-C220-M5, UCSC-C240-M5, or UCSC-C480-M5
Chassis	N20-C6508 or <b>UCSB-5108-AC2</b>
I/O module (IOM)	UCS-IOM-2204XP, UCS-IOM-2208XP, or UCS-IOM-2408
Fabric extenders	Cisco Nexus 2232PP 10GE Fabric Extender

Table 1. Cisco Intersight managed mode supported hardware

Component	Model number
Adapters	Cisco UCS B-Series: <b>UCSB-MLOM-40G-04</b> , UCSB-MLOM-PT-01, or UCSB-VIC- M84-4P Cisco UCS C-Series: UCSC-MLOM-C25Q-04 or UCSC-PCIE-C25Q-04
Topologies	Direct-attached racks through 10/25 Gigabit Ethernet connections Fabric extender-attached racks through 10 Gigabit Ethernet connections Chassis through 10 Gigabit Ethernet connections
Storage controller	Cisco UCS B-Series M5: UCSB-MRAID12G Cisco UCS C-Series M5: UCSC-RAID-M5HD or UCSC-RAID-M5
Trusted Platform Module (TPM)	UCSX-TPM1-001, UCSX-TPM2-001, UCSX-TPM2-002, or UCSX-TPM3-002
Minimum supported software version	Release 4.1(2a)

For the most up-to-date support information for Cisco Intersight managed mode, see <a href="https://www.cisco.com/c/en/us/td/docs/unified\_computing/Intersight/b\_Intersight\_Managed\_Mode\_Configurat\_ion\_Guide.html">https://www.cisco.com/c/en/us/td/docs/unified\_computing/Intersight/b\_Intersight\_Managed\_Mode\_Configurat\_ion\_Guide.html</a>.

**Note:** This document does not cover the migration of policies from a Cisco UCS Manager managed system to a Cisco Intersight managed mode system. The configuration parameters and procedures for the two configuration modes are quite different and require manual translation of policies when you move from one mode to the other.

## Validated hardware and software

Make sure all Cisco UCS components, including servers and adapters, have been upgraded to the correct version. Device discovery will fail if an unsupported version is installed on the Cisco UCS components. In Table 1, the items highlighted in bold were used during the validation process discussed in this document.

The solution was validated with software release 4.1(3d).

## Licensing requirements

The Cisco Intersight platform uses a subscription-based license with multiple tiers. You can purchase a subscription duration of one, three, or five years and choose the required Cisco UCS server volume tier for the selected subscription duration. Each Cisco endpoint automatically includes a Cisco Intersight Base license at no additional cost when you access the Cisco Intersight portal and claim a device. You can purchase any of the following higher-tier Cisco Intersight licenses using the Cisco ordering tool:

- Cisco Intersight Essentials: Essentials includes all the functions of the Base license plus additional features, including Cisco UCS Central Software and Cisco Integrated Management Controller (IMC) supervisor entitlement, policy-based configuration with server profiles, firmware management, and evaluation of compatibility with the Cisco Hardware Compatibility List (HCL).
- Cisco Intersight Advantage: Advantage offers all the features and functions of the Base and Essentials tiers. It includes storage widgets and cross-domain inventory correlation across computing, storage, and virtual environments (VMware ESXi). It also includes OS installation for supported Cisco UCS platforms.

 Cisco Intersight Premier: In addition to the functions provided in the Advantage tier, Premier includes full subscription entitlement for Cisco Intersight Orchestrator, providing orchestration across Cisco UCS and third-party systems.

Servers in the Cisco Intersight managed mode require at least the Essentials license. The validation process for this document used a Premier license; however, all the functions covered in this document are supported with the Essentials license. For more information about the features provided in the various licensing tiers, see <a href="https://intersight.com/help/getting\_started#licensing\_requirements">https://intersight.com/help/getting\_started#licensing\_requirements</a>.

View the current Cisco Intersight Infrastructure Service licensing.

## FlexPod setup for Cisco Intersight managed mode configuration

Figure 3 shows the connectivity between the various elements in this setup.



#### Figure 3.

Topology to verify Cisco Intersight managed mode configuration in a FlexPod environment

To validate the Cisco Intersight managed mode configuration in a FlexPod environment, the components were set up as follows:

Cisco UCS 6454 Fabric Interconnects provide the chassis and network connectivity.

- The Cisco UCS 5108 Blade Server Chassis connects to fabric interconnects using Cisco UCS 2208XP IOMs, where four 10 Gigabit Ethernet ports were used on each IOM to connect to the fabric interconnect.
- Cisco UCS B200 M5 servers contain fourth-generation Cisco virtual interface cards (VICs): UCSB-MLOM-40G-04.
- Cisco Nexus 9336C Switches running in Cisco NX-OS mode provide the switching fabric.
- Cisco UCS 6454 Fabric Interconnect 100 Gigabit Ethernet uplink ports connect to Cisco Nexus 9336C Switches in a virtual port channel (vPC).
- Cisco UCS 6454 Fabric Interconnects are connected to the Cisco MDS 9132T switches using 16-Gbps Fibre Channel connections configured as a port channel for SAN connectivity.
- The NetApp AFF controller connects to the Cisco Nexus 9336C Switches using 10 Gigabit Ethernet ports configured as a vPC.
- The NetApp AFF controller connects to the Cisco MDS 9132T switches using 16-Gbps Fibre Channel connections for SAN connectivity.
- The RHEL 8.3 operating system is installed on Cisco UCS B200 M5 servers to validate the infrastructure.

## **Configuration constructs for Cisco Intersight managed mode**

Cisco Intersight managed mode unites the capabilities of the Cisco UCS platform and the cloud-based flexibility of the Cisco Intersight platform, thus unifying the management experience for standalone and fabric interconnect-attached systems. Cisco Intersight managed mode standardizes policy and operation management for fourth-generation fabric interconnects and Cisco UCS M5 servers.

At a high level, configuring Cisco UCS using Cisco Intersight managed mode consists of the steps shown in Figure 4. The details of these steps are presented in the following sections.





Configure Cisco UCS fabric interconnect for Cisco Intersight managed mode

Claim Cisco UCS fabric interconnect in Cisco Intersight

platform



Configure Cisco UCS domain profile



Configure server profile



Deploy server profile

#### Figure 4.

Steps for configuring Cisco UCS using Cisco Intersight managed mode

#### Setting up Cisco UCS fabric interconnects for Cisco Intersight managed mode

The initial configuration for a fabric interconnect can be performed using the serial console when the fabric interconnect boots for the first time. This can happen either during factory installation or after the existing configuration has been erased. During the initial configuration, for the management mode the configuration wizard enables customers to choose whether they want to manage the fabric interconnect through Cisco UCS Manager or the Cisco Intersight platform. Customers can switch the management mode for the fabric interconnects between Cisco Intersight and Cisco UCS Manager at any time. However, this is a disruptive process because it causes all endpoint configurations to be reset and results in the loss of the current

configuration. In the validation process described here, the existing configuration on the Cisco UCS fabric interconnects was cleared, and the system was set up for Cisco Intersight managed mode.

Figure 5 shows the output from the fabric interconnect console to enable Cisco Intersight managed mode.



#### Figure 5.

Fabric interconnects set up for Cisco Intersight managed mode

#### Claiming a Cisco UCS fabric interconnect in the Cisco Intersight platform

After you set up the Cisco UCS fabric interconnect for Cisco Intersight managed mode, you can add the fabric interconnects to a new or an existing Cisco Intersight account (Figure 6). The details of the device claim process are covered in the appendix. When a Cisco UCS fabric interconnect is successfully added to the Cisco Intersight platform, all future configuration steps are completed in the Cisco Intersight portal.

≡	cisco Intersight	t	OPER	ATE > Fab	ic Interco	onnects								Q   [	Y	₽	Q	\$	0	Paniraja Ko	oppa 🕰
<u>00o</u>																					
Ŷ	OPERATE		Hea	lth		Connection	n Firm	nware Versions		Mo	dels	Co	ntract Status Not Covere	d 2							
	Servers				lealthy 2							2									
	Chassis																				
	Fabric Interconnects			Q _A	ld Filter										2 items fo		14 ∨ per	page 🗵	] < _1_ of		
	Networking Sites			Name		Health 🗘	Manage 🗘	Model 🗘	Expansi			Total	Ports Used	Available			Serial		Organizations		
	HyperFlex Clusters					Healthy	192.168.160	UCS-FI-6454				54			7.0(3)	2(4.13	FD02331	IOPL2			
	Storage					Healthy	192.168.160	UCS-FI-6454				54			7.0(3)	2(4.13	FD02331	17PH			
	Virtualization																				
	Kubernetes																				
×	CONFIGURE																				
ē	ADMIN																				

#### Figure 6.

Cisco Intersight platform: Adding fabric interconnects

You can verify whether a Cisco UCS fabric interconnect is in Cisco UCS Manager managed mode or Cisco Intersight managed mode by clicking the fabric interconnect name and looking at the detailed information screen for the fabric interconnect, as shown in Figure 7.

≡	نابیان cisco Intersight	OPERATE > Fabric Int	erconnects > AA04-6	454 FI-B		Ĺ	2 2 6	ଦ୍ ଚ୍ଚ	🕜 🛛 Paniraja Koppa 🚨
<u>00o</u>		General Inventory	Connections UCS	Domain Profile					Actions v
	OPERATE ^	Details		Properties				Events	
		Health	Healthy	UCS-FI-6454			Front View Rear View	— Alarms	No Alarms
	Chassis	Name	AA04-6454 FI-B	entendendendendendenter	<b>d</b> etetetetete	ledest esterioriorio			
	Fabric Interconnects	Peer Switch	AA04-6454 FI-A	6000 VCS-11-4444			IIIIIIIII atata atata atata		
	Networking Sites	Model	UCS-FI-6454	Locator LED			Health Overlay 🌉	+ Advisories	No Advisories
	HyperFlex Clusters	Expansion Modules Serial	0 FD023310PL2						
	Storage	Contract Status	Not Covered	моде		Access			
	Virtualization	Management IP	192.168.160.184	Ethernet Switching	end-host	IP Address	192.168.160.184		
	Virtualization	Mode	Intersight	FC Switching Mode	end-host	Subnet Mask	255.255.255.0		
	Kubernetes			Admin Evac State	⊘ Disabled	Default Gateway	192.168.160.254		
×	CONFIGURE V	UCS Domain Profile	AA04-6454-	Oper Evac State	Ø Disabled	MAC	N/A		
¢	ADMIN ~	UCS Domain Profil	© OK						
		Firmware Version	7.0(3)N2(4.13b)	High Availiability Details		VLAN Port Count			
		Organizations	default	Ready	No	VLAN Port Limit	16000		
			IMM	State		Access VLAN Port C	39	·	
				Leadership		Border VLAN Port C	9		
		Ports 54		Cluster Link State		Compressed Optimi	0		
		Used	12			Compressed VLAN	0		
		Available	42			Uncompressed VLA	0		

#### Figure 7.

Fabric Interconnect in Cisco Intersight managed mode

## Configuring a Cisco UCS domain profile

A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs to be used in the network. It defines the characteristics of and configures the ports on the fabric interconnects. The domain-related policies can be attached to the profile either at the time of creation or later. One Cisco UCS domain profile can be assigned to one fabric interconnect domain, and the Cisco Intersight platform supports the attachment of one port policy per Cisco UCS domain profile. Policies that are attached to a Cisco UCS domain profile can be created either before or during the creation of the profile.

Some of the characteristics of the Cisco UCS domain profile set up for this validation are as follows:

- A single domain profile is created for the pair of Cisco UCS fabric interconnects.
- Separate port policies are defined for the two fabric interconnects because each fabric interconnect uses unique Fibre Channel and VSAN configurations. If boot from SAN were not required, the same port policy could have been reused across the two fabric interconnects.
- The VLAN configuration policy is common to the fabric interconnect pair because both fabric interconnects are configured for same set of VLANs. You can also keep iSCSI VSANs unique to each fabric interconnect. In such a case, separate VLAN policies would be required.
- The VSAN configuration policies are unique for the two fabric interconnects because the VSANs are unique.
- The Network Time Protocol (NTP), network connectivity, and system quality-of-service (QoS) policies are common to the fabric interconnect pair.

After the Cisco UCS domain profile has been successfully created, the fabric interconnects in FlexPod environment can do the following:

- Form an Ethernet port channel with the Cisco Nexus switch.
- Form a Fibre Channel port channel with the Cisco MDS switch.
- Discover the Cisco UCS chassis and the blades.

Figure 8 shows a summary of the Cisco UCS fabric interconnect and the port configuration after the Cisco UCS domain profile was deployed.

=	diada Intersight	CONFIGURE > UCS Domain Profiles > AA04-	i454-DomProf		
<u>00o</u>					Actions ~
		Details	Policies		
×	CONFIGURE	Status Ø. OK	Port Configuration VLAN & VSAN Configuration UCS Domain Config		
	Orchestration	Name AA04-6454-DomProf	Fabric Interconnect A Configured		
	Profiles	Fabric Interconnect A AA04-6454 FI-A			
	Templates	Fabric Interconnect B AA04-6454 FI-8	Port		AA04-6454-A-PortPol 🗐
		Last Update Feb 22, 2021 2:51 PM			Ports Port Channels
		Ornanizations IMM			DAYN BAYN DAYN BAYN BAYN
ē					
		Tags Set	GIGO UCS-17-464		
				Ethernet Uplink Port Channel Member FC Uplink Port	rt Channel Member 🔹 Server 🔹 Unconfigured
				Port Channel Type	
				4 FC Uplink	
			Ethernet 5		
			Port Role	Port Channel Role	
				4 Ethernet Uplink	

## Figure 8.

Cisco UCS domain profile

#### Creating and deploying a server profile

A server profile enables resource management by simplifying policy alignment and server configuration. You can create server profiles using the server profile wizard to provision servers, create policies to help ensure smooth deployment of servers, and eliminate failures caused by inconsistent configurations. The server profile wizard groups the server policies into the following four categories to provide a quick summary view of the policies that are attached to a profile:

- Compute policies: BIOS, boot order, and virtual media policies
- Management policies: Device connector; Intelligent Platform Management Interface (IPMI) over LAN; Lightweight Directory Access Protocol (LDAP); local user; network connectivity; Simple Mail Transfer Protocol (SMTP); Simple Network Management Protocol (SNMP); Secure Shell (SSH); Serial over LAN (SOL); syslog; and virtual keyboard, video, and mouse (KVM) policies
- Storage policies: Secure Digital (SD) card and storage policies (not used in this document)
- Network policies: LAN connectivity and SAN connectivity policies
  - The LAN connectivity policy requires you to create Ethernet network policy, Ethernet adapter policy, and Ethernet QoS policy.

 The SAN connectivity policy requires you to create Fibre Channel network policy, Fibre Channel adapter policy, and Fibre Channel QoS policy.

#### Server profile for SAN boot

The server profile enables resource management by simplifying policy alignment and server configuration. The server profile groups the server policies. Some of the policies used to create the server profile for this validation are as follows:

- BIOS policy is created to specify various server parameters in accordance with FlexPod best practices.
- Boot-order policy defines the following:
  - Virtual media (KVM mapper DVD)
  - Two vNICs to provide iSCSI LUN for boot from SAN linked to four SAN paths for NetApp iSCSI interfaces.

OR

Two vHBAs to provide FC LUN for boot from SAN linked to four SAN paths for NetApp Fibre Channel interfaces

- IMC access policy defines the management IP address pool for KVM access.
- Local user policy is used to create KVM access.
- LAN connectivity policy for iSCSI boot from SAN will use three vNICs: one for management and two overlay vNICs for iSCSI to provide multipathing and high availability.

OR

LAN connectivity policy for Fibre Channel boot from SAN will use single vNICs for management

 SAN connectivity policy is used to create two vHBAs—one for SAN A and one for SAN B—along with various policies and pools.

Figure 9 shows various policies associated with the server profile, and Figure 10 shows a successfully deployed server profile and associated blade.

CONFIGURE >	Server Profiles > SP-FlexPod-03		5 R	¢7 Q	😳 🕜 Paniraja Koppa ዿ
General Server	Inventory Identifiers Conn	ectivity			Actions
Details		Configuration			
Status	⊘ ок		A	Compute	Management Network Storage
Name	SP-FlexPod-03	BIOS			AA04-6454-BiosPol 🗐
Target Platform Server	UCS Server (FI-Attached)	Boot Order			AA04-FP-SAN-BootPol 🗐
Template Name		IMC Access Policy			AA04-6454-IMCPol 🗐
Last Update	a few seconds ago	LAN Connectivity			AA04-FP-FC-RHEL-LanConn 🗐
Description		Local User			AA04-6454-LocalUser-Pol 🗐
•		SAN Connectivity			AA04-FP-SanConn 🗐
Organization					
Tags					

Figure 9. Server profile policies

OPERATE > Servers	> AA04-6454-1-3		Q [
General Inventory U	ICS Server Profile HCL		
Details		Properties	
Health	Healthy	Cisco UCSB-B200-M5	Front View Top \
Name	AA04-6454-1-3		
Jser Label			
Management IP	192.168.160.202	*	
Serial	Responsible Report		
PID	UCSB-B200-M5		(at 0)?
/endor	Cisco Systems Inc		
Revision	÷.		** OP11
Asset Tag	Unknown		
icense Tier	Premier		
Contract Status	Not Covered		
Management Mode	Intersight	abab	
Chassis	AA04-6454-1	¢isco	1 1
UCS Server Profile	SP-FlexPod-03	Power 🕐 Locator LED 📀	Health Overlay
UCS Server Profile Sta	⊚ ок		
Firmware Version	4.1(33a)	CPUs 2 ID	3
Firmware Status	⊘ Success	Threads 0 Adapters	
		CPU Cores 0 NIC Interfaces	3
Organizations	default	CPU Cores Enabled 0 HBA Interfaces	
	IMM	Memory Capacity 192.0 UUID	
Tags	Set	CPU Capacity (GHz) 160.0	

## Figure 10.

Server profile details

After a server profile has been successfully deployed, the server successfully boots from SAN storage hosted on the NetApp storage. Additional server profiles are created simply by cloning the first server profile and programming the Cisco MDS switches and NetApp controllers for various SAN parameters. For step-by-step deployment guidance for Cisco UCS and Cisco Intersight managed mode, refer to the appendix.

## Automated provisioning using Terraform infrastructure as code

Terraform is an open-source infrastructure as code software tool that enables you to safely and predictably create, change, and improve infrastructure.

Terraform helps with

- Increased agility with reduced time to provision from weeks to minutes with automated workflow
- Control costs systematically as users and applications scale
- Reduce risk and discover errors before they happen with code reviews and embed provisioning guardrails

## **Terraform Providers**

Providers are plugins that implement resource types likes Intersight.

Terraform CLI finds and installs providers when initializing a working directory. It can automatically download providers from a Terraform registry or load them from a local mirror or cache.

## Why Terraform provider for the Cisco Intersight?

The Cisco Intersight platform supports the Terraform provider. The Terraform provider allows organizations to develop Cisco Intersight resources as self-service infrastructure using code rather than manual provisioning.

This approach provides several benefits:

- You can more quickly and easily scale Cisco Intersight resources. You can provision infrastructure in minutes, with little effort, using the automated workflows, performing the same tasks that used to take days.
- The operating model of Terraform is well suited for the Cisco Intersight platform, because it accommodates the shift from static to dynamic infrastructure provisioning. For example, if a resource is deleted in the Terraform configuration, it will be reflected in the Cisco Intersight platform when the new configuration is applied.
- Terraform maintains a state file, which is a record of the currently provisioned resources. State files provide a version history of Cisco Intersight resources, enabling a detailed audit trail of changes.
- The provider enables idempotency, producing the same result and state with repeated API calls.

The set of files used to describe infrastructure in Terraform is known as a Terraform configuration. The configuration is written using HashiCorp Configuration Language (HCL), a simple human-readable configuration language, to define a desired topology of infrastructure resources.

## **Automated Solution Deployment**

The Terraform provider for Intersight offers an excellent way to easily build, scale, and manage the lifecycle of the FlexPod Datacenter. We can use it to automate entire infrastructure provisioning and for day-2 operations.

GitHub link below provides details of how to automate infrastructure provisioning detailed in this document. It has detailed steps and Terraform configurations for deploying the Cisco UCS with SAN boot (iSCSI and Fibre Channel) in a FlexPod Datacenter environment.

Link: https://github.com/ucs-compute-solutions/ConvergedInfrastructure IMM Terraform

REDAME file of the GitHub repository details the steps to automate the infrastructure provision for FlexPod using Terraform.

## Conclusion

The Cisco Intersight platform is a SaaS infrastructure lifecycle management solution that delivers simplified configuration, deployment, maintenance, and support. The FlexPod solution delivers an integrated architecture that incorporates computing, storage, and network design best practices to reduce IT risk by validating the integrated architecture and helping ensure compatibility among the components.

Integrating the Cisco Intersight platform into a FlexPod environment provides global visibility of infrastructure health and status along with advanced management and support capabilities. The Cisco Intersight platform delivers a convenient SaaS solution with the capability to connect from anywhere and manage infrastructure

through a browser or mobile app while allowing customers to stay ahead of problems and accelerate trouble resolution through advanced support capabilities.

## For more information

Consult the following references for additional information about the topics discussed in this document.

### Automated Provisioning using Terraform

https://github.com/ucs-compute-solutions/ConvergedInfrastructure IMM Terraform

#### **Products and solutions**

- Cisco Intersight platform: <u>https://www.intersight.com</u>
- Cisco Intersight managed mode configuration guide: <u>https://www.cisco.com/c/en/us/td/docs/unified computing/Intersight/b Intersight Managed Mode Con</u> <u>figuration Guide.html</u>
- Cisco Unified Computing System: <a href="http://www.cisco.com/en/US/products/ps10265/index.html">http://www.cisco.com/en/US/products/ps10265/index.html</a>
- Cisco UCS 6454 Fabric Interconnect: <u>https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html</u>
- Cisco UCS 5100 Series Blade Server Chassis: <u>http://www.cisco.com/en/US/products/ps10279/index.html</u>
- Cisco UCS B-Series Blade Servers: <u>http://www.cisco.com/en/US/partner/products/ps10280/index.html</u>
- Cisco UCS adapters: <a href="http://www.cisco.com/en/US/products/ps10277/prod">http://www.cisco.com/en/US/products/ps10277/prod</a> module series home.html
- Cisco Nexus 9000 Series Switches: <u>http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html</u>
- NetApp ONTAP 9: <u>http://www.netapp.com/us/products/platform-os/ontap/index.aspx</u>

#### Interoperability matrixes

- Cisco UCS Hardware Compatibility Matrix: <u>https://ucshcltool.cloudapps.cisco.com/public/</u>
- NetApp Interoperability Matrix Tool: <u>http://support.netapp.com/matrix/</u>

#### **Configuration guides**

- FlexPod Datacenter Design Guide: https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/fp\_dc\_ontap\_97\_ucs\_4\_vm w\_vs\_67\_U3\_design.html
- FlexPod Datacenter Deployment Guide: https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/fp\_dc\_ontap\_97\_ucs\_4\_vm w\_vs\_67\_U3.html

## Appendix: Configuration details

This appendix describes how to set up a Cisco UCS fabric in Cisco Intersight managed mode and specify the FlexPod-related computing configuration using the Cisco Intersight platform. This appendix does not discuss how to set up the switching infrastructure or the storage. Refer to the relevant FlexPod deployments guides for details about these components:

https://www.cisco.com/c/en/us/td/docs/unified computing/ucs/UCS CVDs/fp dc ontap 97 ucs 4 vmw vs 67 U3.html.

## Set up Cisco Intersight managed mode on Cisco UCS fabric interconnects

The Cisco UCS fabric interconnects need to be set up to support Cisco Intersight managed mode. If you are converting an existing pair of Cisco UCS fabric interconnects, first erase the configuration and reboot your system. Converting fabric interconnects to Cisco Intersight managed mode is a disruptive process, and configuration information will be lost. Customers are encouraged to make a backup of their existing configuration if they plan only to test Cisco Intersight managed mode and then revert to Cisco UCS Manager managed mode.

1. Erase the configuration on existing fabric interconnects. Connect to each of the fabric interconnect consoles, log in as admin, and enter the following commands:

**Note:** This erasure process is not needed on brand-new fabric interconnects that have not been configured yet.

UCS-A# connect local-mgmt UCS-A(local-mgmt)# erase configuration All UCS configurations will be erased and system will reboot. Are you sure? (yes/no): yes

 Configure Fabric Interconnect A (FI-A). On the Basic System Configuration Dialog screen, set the management mode to Intersight. All the remaining settings are similar to those for the Cisco UCS Manager managed mode (UCSM-Managed). Note that there is not a virtual IP address setting anymore when Cisco Intersight managed mode is selected.

---- Basic System Configuration Dialog ----This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps. Type Ctrl-C at any time to abort configuration and reboot system. To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration. Enter the configuration method. (console/gui) ? console Enter the management mode. (ucsm/intersight)? intersight You have chosen to setup a new Fabric interconnect in "intersight" managed mode. Continue? (y/n): y Enforce strong password? (y/n) [y]: Enter the password for "admin": Confirm the password for "admin": Enter the switch fabric (A/B) []: A Enter the system name: AA04-6454 Physical Switch Mgmt0 IP address : 192.168.160.183 Physical Switch Mgmt0 IPv4 netmask : 255.255.252.0 IPv4 address of the default gateway : 192.168.160.1 DNS IP address : 192.168.160.53 Configure the default domain name? (yes/no) [n]: yes Default domain name : cspg.local Following configurations will be applied: Management Mode=intersight Switch Fabric=A System Name=AA04-6454 Enforced Strong Password=yes Physical Switch Mgmt0 IP Address=192.168.160.183 Physical Switch Mgmt0 IP Netmask=255.255.252.0 Default Gateway=192.168.160.1 DNS Server=192.168.160.53 Domain Name=cspg.local

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):

- After applying the settings, make sure you can ping the fabric interconnect management IP address. When Fabric Interconnect A is correctly set up and is available, Fabric Interconnect B will automatically discover Fabric Interconnect A during its setup process as shown in the next step.
- 4. Configure Fabric Interconnect B (FI-B). For the configuration method, choose console. Fabric Interconnect B will detect the presence of Fabric Interconnect A and will prompt you to enter the admin password for Fabric Interconnect A. Provide the management IP address for Fabric Interconnect B and apply the configuration.

```
---- Basic System Configuration Dialog ----
 This setup utility will guide you through the basic configuration of
 the system. Only minimal configuration including IP connectivity to
 the Fabric interconnect and its clustering mode is performed through these steps.
 Type Ctrl-C at any time to abort configuration and reboot system.
 To back track or make modifications to already entered values,
 complete input till end of section and answer no when prompted
 to apply configuration.
 Enter the configuration method. (console/gui) ? console
  Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cl
uster. Continue (y/n) ? y
  Enter the admin password of the peer Fabric interconnect:
   Connecting to peer Fabric interconnect... done
   Retrieving config from peer Fabric interconnect... done
   Peer Fabric interconnect management mode
                                             : intersight
   Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.160.183
   Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.252.0
   Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
 Physical Switch Mgmt0 IP address : 192.168.160.184
 Local fabric interconnect model (UCS-FI-6454)
 Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with the installer...
 Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):
```

## Set up a Cisco Intersight account

In this step, using the unique device information for the Cisco UCS, you set up a new Cisco Intersight account. Customers also can choose to add the Cisco UCS devices set up for Cisco Intersight managed mode to an existing Cisco Intersight account; however, that procedure is not covered in this document.

#### Claim a device

After completing the initial configuration for the fabric interconnects, log in to Fabric Interconnect A using your web browser to capture the Cisco Intersight connectivity information.

1. Use the management IP address of Fabric Interconnect A to access the device from a web browser and the previously configured admin password to log in to the device.



2. Under DEVICE CONNECTOR, you should see the current device status as "Not claimed." Note, or copy, the Device ID and Claim Code information to use to set up a new Cisco Intersight account.

**Note:** The Device ID and Claim Code information can also be used to claim the Cisco UCS devices set up with Cisco Intersight managed mode in an existing Cisco Intersight account.

CISCO DEVICE CONSOLE AA04-6454	
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center	
Device Connector	Settings C Refresh
ACCESS MODI: ALLOW CONTROL       Device II         Image: Connector       Image: Connector         Internet       Image: Connector         Image: Connector       Image: Connector         Image: Connector	D Defe Defe Defense and the fight

### Create a new Cisco Intersight account

Next, create a new Cisco Intersight account.

- 1. Visit https://www.intersight.com and click "Don't have an Intersight Account? Create an account."
- 2. Provide an account name and the device information captured in the preceding steps to create the account. This step will automatically add the Cisco UCS device to the new Cisco Intersight account.

Account Creation	
Account Name *	
CSPG-RTP-IMM	<u>»</u>
You can find the Device ID and Claim Code in the Device	
Connector for the selected device. (1)	
Device ID *	
FEOCIALITY PROPOSILIES INFLZ	
370	
Cancel	
Cancer Courte	
The second s	and the second s
and in Total a	Destruction of the

3. After the account has been created successfully, click Go To Intersight.



4. You should see a screen with your Cisco Intersight account.

≡ <sup>•1 •1 •</sup> Intersight	MONITOR		
	Main 🖉 🕂		<u>lo</u> : Add Widget
OPERATE ^	Server Health Summary	HyperFlex Cluster Health Summary	Fabric Interconnect Health Summary
Servers Chassis Fabric Interconnects HyperFlex Chisters			•
X CONFIGURE ^	Server Inventory	HyperFlex Cluster Inventory	Fabric Interconnect Inventory
Profiles Policies Pools Devices			моеця 2 тотоц + каза 2 108 рогта 108 жилалае
	Server Version Summary	HyperFlex Version Summary	Fabric Interconnect Version Summary
			VERSIONS 2 TOTAL * 7.00(N2(<120) 2

### Verify the addition of Cisco UCS fabric interconnects to Cisco Intersight

Now verify that Cisco UCS fabric interconnects are added to your account in Cisco Intersight.

- 1. Go back to the web GUI of the Cisco UCS fabric interconnect and click the Refresh button.
- 2. The fabric interconnect status should now be set to Claimed.

CISCO DEVICE CONSOLE AA04-6454			0	
DEVICE CONNECTOR SYSTEM INFORMATION SERVER	RS TECHNICAL SUPPORT			
The Device Connector is an embedded management controller that Center	enables the capabilities of Cisco Intersight, a cloud-base	ed management platform. For detailed information	about configuring the device connector, pl	ase visit He
Device Connector			<li>Settings</li>	$ $ $\square$ Ref
	ACCESS MODE ALLOW CONTROL		Device ID	
				-
<b>—</b>	·····	~~~~	Claimed to Account	
	Internet	Intersight	CSPG-RTP-IMM U	
Claimed				

#### Set up licensing

When setting up a new Cisco Intersight account (as discussed in this document), the account needs to be enabled for Cisco Smart Software Licensing.

- 1. Associate the Cisco Intersight account with Cisco Smart Licensing by following these steps:
  - Log in to the Cisco Smart Licensing portal: <u>https://software.cisco.com/software/csws/ws/platform/home?locale=en\_US#module/SmartLicensing</u>.
  - Select the correct virtual account.
  - Under Inventory > General, generate a new token for product registration.
  - Copy this newly created token.

Create Registration Token									
This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.									
Virtual Account:	Intersight Demo TME								
Description :	Token for RTP IMM Intersight Account	1							
* Expire After:	365 Days								
Max. Number of Uses:	Between 1 - 365, 30 days recommended								
✓ Allow export-controlled fun	The token will be expired when either the expiration or the maximum uses is reached ctionality on the products registered with this token (1)								
	Create Token Ca	ancel							

2. With the Cisco Intersight account associated with Cisco Smart Licensing, log in to the Cisco Intersight portal and click Settings (the gear icon) in the top-right corner. Choose Licensing.



3. Under Cisco Intersight > Licensing, click Register.

	cisco Intersight	Licensing	
<u>00o</u>	MONITOR	Subscription	Licenses
	OPERATE ^	Last Updated 🌐 Never Updated	
	Servers		
	Chassis		Base o
	Fabric Interconnects	Register	
	HyperFlex Clusters		Status • Not Used
≫	CONFIGURE ^		
	Profiles		
	Policies		
	Pools		
ø	ADMIN ^		
	Devices		

4. Enter the copied token from the Cisco Smart Licensing portal.



5. Click Register and wait for registration to go through. When the registration is successful, the information about the associated Cisco Smart account is displayed.

≡	راسان Intersight	Licensing
	Subscription	
× Į	Last Updated 💭 Smart Account Virtual Account	May 11, 2021 11:19 PM BU Production Test Intersight Demo TME
	Deregister	Start Trial

6. For all new accounts, the default licensing tier is set to Base. For Cisco Intersight managed mode, the default tier needs to be changed to Essential or a higher tier. To make this change, click Set Default Tier.

Products								
Intersight							Set Def	ault Tier
Base $\circ$	se o Essentials o			Advantage $\circ$				
	O Not Used		O Not Used		O Not Used		O Not Used	

7. Select the tier supported by your Smart License.

Set Default Tier	×
New servers which are claimed to this account will be part of the selected license tier by default.	
Default Tier * Base	
Base	
Essentials	
Essentials Advantage	

8. In this deployment, the default license tier is set to Premier.

≡	cisco Intersight Licensing			Q 🛛	🔍 😳 🕜 Paniraja Koppa 🖉
ŵ	Subscription	Products			
×	Last Updated 💭 May 11, 2021 11:19 PM Smart Account BU Production Test	Intersight			
-	Virtual Account Intersight Demo TME	Base ⊙	Essentials ₀	Advantage $\circ$	Premier o
	Deregister Start Trial				

## Set up Cisco Intersight organization

You need to define all Cisco Intersight managed mode configurations for Cisco UCS, including policies, under an organization. To define a new organization, follow these steps:

- 1. Log in to the Cisco Intersight portal.
- 2. Click Settings (the gear icon) and choose Settings.
- 3. Click Organizations in the middle panel.
- 4. Click Create Organization in the top-right corner.

≡	cisco Intersight Settings							۵						
@ % @	<ul> <li>GENERAL</li> <li>Account Details</li> <li>Access Details</li> </ul>	Organiza	tions									+ 0	Create Organ	ization
-1-	authentication	0 Us	Use organizations to manage access to your infrastructure. Learn more about Organizations at Help Center.									×		
	Single Sign-On Cisco ID		/ 10 QAdd Filter							10 ~ per	page 🔣 🖣			
	ACCESS & PERMISSIONS		Name			Memberships	Usage							
	IP Access Management									Use	in a Default	Organizatio	on automa	
	Security & Privacy													
	Users Groups													
	Roles Organizations													
	₽ API													
	API Keys OAuth2 Tokens													

- 5. Provide a name for the organization (for example, **FlexPod**).
- 6. Under Memberships, select Custom.
- 7. Select the recently added Cisco UCS device for this organization.
- 8. Click Create.

≡	الالالالالالالالالالالالالالالالالالال	Organizations >	Create				Ą	ß	ø	Q,	٢	0	Paniraja Koppa 🖉
				{ <b>`</b> }	Create Organization	on nanage access to your							
≫				~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	logical and physical resour	ces.							
			General										
			Name * FlexPod O	Description									
			Memberships										
			Custom										
			<ul> <li>Select targets to create a Cus targets in the same Organizat</li> </ul>	tom Organization. Profile ion.	es and Policies that are creat	ed within a Custom Organiza	ation are applicable (	only to					
						nd 10 v per page							
			Name 🗘	Status 🗘	Туре	IP Address 0	Target ID						
			MA04-6454	Connected	UCSFIISM	192.168.160.183,192	FD0233117PH,FI	0023310PL2					
			Selected 1 of 1 Show Selected										
													Create

## **Configure a Cisco UCS domain profile**

A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs in the network. It defines the characteristics of and configures ports on fabric interconnects. The domain-related policies can be attached to the profile either at the time of creation or later. One Cisco UCS domain profile can be assigned to one fabric interconnect domain.

To create a Cisco UCS domain profile, follow these steps:

- 1. Log in to the Cisco Intersight portal
- 2. Click to expand CONFIGURE in the left pane and select Profiles.
- 3. In the main window, select UCS Domain Profiles and click Create UCS Domain Profile.

≡	-ili-ili- cisco	Intersight		CONFIGURE > Profiles						4 E	q	۲	⑦ Paniraja K	oppa 🕰
Ŷ	OPERATE					UCS Domain Profiles							Create UCS Domain	Profile
×	CONFIGURE		^											
	Profiles				Add Filter									
	Templates			Name		≎ Status		Fabric Interconnect	UCS Domain A Fabric In	terconnect B	Last Upd	ate		
	Policies													
ø	ADMIN													
	Targets													

4. On the Create UCS Domain Profile screen, click Start.



## Step 1: General

Follow these steps for the general configuration:

- 1. Choose the organization from the drop-down menu (for example, FlexPod).
- 2. Provide a name for the domain profile (for example, AA04-6454-DomProf).

CONFIGURE > Create UCS Domain Profile	다. 🖸 📢 오, 🔅 ⊘ Paniraja Koppa ዾ
─ Progress	Step 1
General	Add a name, description and tag for the UCS domain profile.
2 UCS Domain Assignment	
3 VLAN & VSAN Configuration	Organization * FlexPod ∽
4 Ports Configuration	
5 UCS Domain Configuration	Name *
6 Summary	
	Set Tags
	<= 1024

3. Click Next.

### Step 2: UCS Domain Assignment

Follow these steps for Cisco UCS domain assignment:

1. Assign the Cisco UCS domain to this new domain profile by clicking Assign Now and selecting the previously added Cisco UCS domain (AA04-6454).

CONFIGURE > Create UCS Domain Profile	C 🗹 🗘 🔞 🔿 Paniraji	ja Koppa 🚨								
─ Progress	Step 2									
1 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										
5 UCS Domain Configuration	Assign Later, click Next to proceed to policy selection.									
6 Summary	Show Assigned									
	Q _ Add Filter   1 items found   10 ∨ per page K < 1 _ of 1 > >   ③									
	Domain Name  Fabric Interconnect A Model Serial Firmware Version Model Serial Firmware Version									
	AA04-6454     UCS-FI-6454     FD0233117PH     7.0(3)N2(4.13b)     UCS-FI-6454     FD023310PL2     7.0(3)N2(4.13b)									
	Selected 1 of 1         Show Selected         Unselect All         K          of 1         >          > <th></th>									

2. Click Next.

## Step 3: VLAN and VSAN Configuration

In this step, you create a single VLAN policy for both fabric interconnects, but you create individual policies for the VSANs because the VSAN IDs are unique for each fabric interconnect. Separate VLAN policies can be created if you want to keep VLANs unique to each fabric interconnect.

## **Create and apply VLAN policy**

Follow these steps to create and apply the VLAN policy:

1. Click Select Policy next to VLAN Configuration under Fabric Interconnect A. Then, in the pane on the right, click Create New.

CONFIGURE > Create UCS Domain Profile	Ç	\ [2] [4] Q	© ©	Paniraja Koppa 🚨
즌 Progress	Step 3			
(1) General	VLAN & VSAN Cc Create or select a policy fr pair.	nfiguration or the fabric interconnect		
2 UCS Domain Assignment				
VLAN & VSAN Configuration	Fabric Interconnect A 0 of 2 Policies Configured			^
Ports Configuration	VLAN Configuration		Select Policy	
5 UCS Domain Configuration	VSAN Configuration		Select Policy	
6 Summary				
	Fabric Interconnect B 0 of 2 Policies Configured			^
	VLAN Configuration		Select Policy 🗐	
	VSAN Configuration		Select Policy	

2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-VLANPol**).

CONFIGURE > Create UCS Domain Profile > Create VLAN	ධ 🗹 📢 Q, (ටී) ⑦ Paniraja Koppa &
⊂ Progress	Step 1
General	General Add a name, description and tag for the policy.
2 Policy Details	
	FlexPod
	Name *
	A004-6454-VLANPol
	Set Tags
	Description
	VLAN Policy for both FIs

- 3. Click Next.
- 4. Click Add VLANs.

CONFIGURE > Create UCS Domain Pro	ofile > Create VLAN	4			¢	☑ ♥			Paniraja Koppa 🚨
<ul> <li>Progress</li> <li>General</li> <li>Policy Details</li> </ul>		ſ		Step 2 <b>Policy Details</b> Add policy details					
		This policy is applicable only for UCS	S Domains						
		VLANs							
		Add VLANs Show VLAN Ranges							
						50 ∨ per page	区 < 0 of		
			Name	Mul	lticast		Auto Allow C	)n Uplinks	
								< 0 of 0	
		Set Native VLAN ID							

5. Provide a name and VLAN ID for the native VLAN (for example, Native-Vlan and 2).

CONFIGURE > Create UCS Domai	n Profile > Create VLAN		4 C	€1 Q	③ Paniraja Koppa &
		Add VLANS Add VLANs to the policy			
	VLANs should have one Multicast policy associated to	it			
	Configuration				
	Name / Prefix * Native-Vlan	VLAN IDS * <u> </u> 2			<u>o</u>
	■ Auto Allow On Uplinks ○           Multicast *           Select Policy				

- 6. Click Select Policy for Multicast and then, in the pane on the right, click Create New.
- 7. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-MCastPol**).

CONFIGURE > Create UCS Domain Profile > Create VLAN > Create Multicast	C K K C 🔅	ා Paniraja Koppa යු
─ Progress	Step 1	
General	General Add a name, description and tag for the policy.	
2 Policy Details		
	Organization * FlexPod ~	
	Name * AA04-6454-MCastPol	
	Set Tags	
	Description	
	<≃ 1024	

8. Keep the default setting of Snooping state enabled and Querier state disabled and click Create

CONFIGURE > Create UCS Domain	Profile > Create VLAN	N > Create Multicast			Q	ľ	Ą	q	0	Paniraja Koppa 🚨
─ Progress			~~~	Step 2						
1 General				Policy Details Add policy details						
2 Policy Details										
		Multicast								
		Snooping State 🛈								
		Querier State 🛈								
										т. 

## 9. Click Add

10. Select Set Native VLAN ID and enter the VLAN number (for example, 2) under VLAN ID.

CONFIGURE > Create UCS Domain Profile > Create VLA	N		Q 🛛 🖓	o ۋ (	Paniraja Koppa 🙎
Œ Progress	_~	Step 2			
1 General	<del>ر</del> ر	Add policy details	IS		
2 Policy Details					_
	This policy is applicable only for UCS Dependence on the second secon	omains			
	VLANs				
	Add VLANs				
	Show VLAN Ranges				
		1 item	ns found 50 v per page 🗵	< <u>1</u> of 1 > >   🔅	
	VLAN ID	Name	Multicast	Auto Allow On Uplinks	
		Native-Vlan_2	AA04-6454-MCastPol	Yes	
				K < <u>1</u> of 1 > >	
	Set Native VLAN ID				
	VLAN ID	A			
	2				

11. Add the remaining VLANs for FlexPod by clicking Add VLANs and entering the VLANs one by one. Select the same multicast policy for all the VLANs. The VLANs used for this validation are shown in the screen image here.

CONFIGURE > Create UCS Domain Profile > Create VLA	N			¢ 🛛 🕻	୍ଦ୍ର କ୍ଷ	Paniraja Kopp
⊆ Progress           1         General		Ę	Step 2 Policy Detail Add policy details	s		
Policy Details	This po	olicy is applicable only for UCS D	omains			
	VLANs					
	Add V	/LANs				
	She	ow VLAN Ranges				
			5 item	is found 50 ∨ per page		
		VLAN ID	Name	Multicast	Auto Allow On Uplinks	
			Native-Vlan_2	AA04-6454-MCastPol	Yes	
			management_511	AA04-6454-MCastPol	Yes	
		3010	iSCSI-A_3010	AA04-6454-MCastPol	Yes	
		3020	iSCSI-B_3020	AA04-6454-MCastPol	Yes	
		3050	nfs_vlan_3050	AA04-6454-MCastPol	Yes	
					K < 1 of 1	
	🔽 Set Na	lative VLAN ID				
	VLAN ID					
	<u> </u>					

**Note:** The iSCSI VLANs shown in the screen image above are needed only if you are using iSCSI boot from SAN. Include the NFS VLAN if you are using an NFS datastore.

- 12. Click Create at the bottom right to create all the VLANs.
- 13. Click Select Policy next to VLAN Configuration for Fabric Interconnect B and select the same VLAN policy that was created in the preceding step.

CONFIGURE > Create UCS Domain Profile		Q Q 44 Q 69 00	Paniraja Koppa 🚨
		Step 3 VLAN & VSAN Configuration Create or select a policy for the fabric interconnect pair.	
3 VLAN & VSAN Configuration	Fabric Interconnect A 1 of 2 Policies Configured		^
4 Ports Configuration	VLAN Configuration	X   🖉   AA04-6454-VLANPoi 🗐	_
5 UCS Domain Configuration	VSAN Configuration	Select Policy 🗐	
6 Summary			-
	Fabric Interconnect B 0 of 2 Policies Configured		^
	VLAN Configuration	Select Policy 🗐	_
	VSAN Configuration	Select Policy 🗐	

## Create and apply VSAN policy (Fibre Channel Only)

Follow these steps to create and apply the VSAN policy. These steps apply only for Fibre Channel SAN configuration.

- 1. Click Select Policy next to VSAN Configuration under Fabric Interconnect A. Then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-A-VSANPol**).

CONFIGURE > Create UCS Domain Profile > Create VSAN		¢		\$7		Paniraja Koppa 🙎
	Step 1					
General	Add a name, descrip	tion and tag f	or the polic			
2 Policy Details						
	Organization *					
	Name *					
	AA04-6454-A-VSANPol					
	Set Tags					
	VSAN Policy for FI-A					
				<= 1024		

- 3. Click Next.
- 4. Click Add VSAN and provide a name (for example, **VSAN-A**), VSAN ID (for example, 111), and the associated Fibre Channel over Ethernet (FCoE) VLAN ID (for example, 111) for SAN A.
- 5. Click Add.

Name * VSAN-A	
VSAN ID *	
111	) O
	1 - 4093
FCoE VLAN ID *	
111	<b>)</b> 0
	> 2
FC Zoning 🛈	

## 6. Enable uplink trunking for this VSAN.

CONFIGURE > Create UCS Domain	Profile > Create VSA	N				Q	ß	<b>\$</b> 2	Q,		0	Paniraja Koppa 🚨
⊂ Progress				~~,	Step 2	-						
1 General			ç		Add policy details	5						
Policy Details												
		0 T	his policy is applicable only for UCS	Domains								
			Uplink Trunking ①									
		Ad	d VSAN									
					1 ite	ems found	50 v p	ber page 🔣		of 1 >		
			VSAN ID	Name		FCoE VLAN	N ID		Default Zo	ning		
				VSAN-A					Disabled			
											of 1 方 河	

- 7. Click Create.
- 8. Repeat the same steps to create a new VSAN policy for SAN B. Click Select Policy next to VSAN Configuration under Fabric Interconnect B. Then, in the pane on the right, click Create New.
- 9. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-B-VSANPol**).

CONFIGURE > Create UCS Domain Profile > Create VSAN	ධ 🕑 🕫 🔾 🧿 Paniraja Koppa گ
⊡ Progress	Step 1
U General	General Add a name, description and tag for the policy.
2 Policy Details	
	FlexPod ~
	Name *
	AA04-6454-B-VSANPol
	Set Tags
	Description
	VSAN Policy for FI-B
	<= 1024

- 10. Click Next.
- 11. Click Add VSAN and provide a name (for example, **VSAN-B**), a VSAN ID (for example, 112), and the associated FCoE VLAN ID (for example, 112) for SAN-B.
- 12. Click Add.

Name * VSAN-B			0
VSAN ID *			
112		Ĵ	<u>(</u> )
		1 - 4	4093
FCoE VLAN ID *			
112			()
			> 2
FC Zoning 💿			

13. Enable uplink trunking for this VSAN.
| CONFIGURE > Create UCS Domain Profile > Create VSA | N   |                                   |       |         |                    | ¢         | ß    |        | ¢\$   | Q,         |          |        | Paniraja Koppa 🚨 |
|--|-----|-----------------------------------|-------|---------|--------------------|-----------|------|--------|-------|------------|----------|--------|------------------|
|  |     |                                   | ~     | <u></u> | Step 2             |           |      |        |       |            |          |        |                  |
| 1 General  |     |                                   | کر    |         | Add policy details | S         |      |        |       |            |          |        |                  |
| 2 Policy Details                                   |     |                                   |       |         |                    |           |      |        |       |            |          |        |                  |
|  | о 1 | his policy is applicable only for | UCS D | omains  |                    |           |      |        |       |            |          |        |                  |
|  |     | Uplink Trunking O                 |       |         |                    |           |      |        |       |            |          |        |                  |
|  | Ac  | dVSAN                             |       |         |                    |           |      |        |       |            |          |        |                  |
|  |     |                                   |       |         | 1 it               | ems found | 50   | ∽ perp | age 🖂 |            | of 1 > 🕽 |        |                  |
|  |     | VSAN ID                           |       | Name    |                    | FCoE VLA  | N ID |        |       | Default Zo | ning     |        |                  |
|  |     | 1                                 | 112   | VSAN-B  |                    |           |      |        |       | Disabled   |          |        |                  |
|  |     |                                   |       |         |                    |           |      |        |       |            |          | f1 > 洌 |                  |

- 14. Click Create.
- 15. Verify that a common VLAN policy and two unique VSAN policies are associated with the two fabric interconnects.

CONFIGURE > Create UCS Domain Profile		¢ ⊵ ¢ ¢ ©	Paniraja Koppa 🙎
⊡ Progress		Step 3	
(1) General		VLAN & VSAN Configuration Create or select a policy for the fabric interconnect	
2 UCS Domain Assignment		pair.	
3 VLAN & VSAN Configuration	Fabric Interconnect A 2 of 2 Policies Configured		
4 Ports Configuration	VLAN Configuration	×   🖉   AA04-6454-VLANPOI 🗐	
5 UCS Domain Configuration	VSAN Configuration	×   🖉   AA04-6454-A-VSANPOI 🗐	
6 Summary			
	Fabric Interconnect B 2 of 2 Policies Configured		
	VLAN Configuration	×   🆉   AA04-6454-VLANPOI 🗐	
	VSAN Configuration	×   🖉   AA04-6454-B-VSANPol 🗃	

16. Click Next.

# **Step 4: Ports Configuration**

Follow these steps to configure the ports:

1. Click Select Policy for Fabric Interconnect A.

CONFIGURE > Create UCS Domain Profile	¢   ⊠   ¢¢   ¢,	ې 🕲 🕐 Paniraja Koppa 🖉
─ Progress	Step 4	
1 General	Create or select a port policy for the fabric interconnect pair.	
2 UCS Domain Assignment		
3 VLAN & VSAN Configuration	Configure ports by creating or selecting a policy.	
Ports Configuration	Fabric Interconnect A Not Configured	^
5 UCS Domain Configuration	Ports Configuration	Select Policy 🗐
	NOT CONFIGURED	
	Fabric Interconnect B Not Configured	^
	Ports Configuration	Select Policy 🗐
	NOT CONFIGURED	

2. Click Create New in the top-right pane to define a new port configuration policy.

**Note:** This document uses separate port policies for the two fabric interconnects because each fabric interconnect uses unique Fibre Channel and VSAN information. If boot from SAN were not required, the same port policy could have been reused across the two fabric interconnects.

- 3. Choose the organization from the drop-down menu.
- 4. Provide a name for the policy (for example, **AA04-6454-A-PortPol**). Change the switch model if it is not 6454.

CONFIGURE > Create UCS Domain Profile > Create Port	🗘 🗹 📢 🖓 🧭 Paniraja Koppa 🕰
⊂ Progress	Step 1
General	General Add a name, description and tag for the policy.
2 Unified Port	Our sector to a t
3 Port Roles	FlexPod
	Name*
	Switch Model *
	UCS-FI-6454 ~
	Set Tags
	Description
	Port Policy for FI-A
	<= 1024

5. Move the slider to set up unified ports. In this example, the first four ports were selected as Fibre Channel ports. Click Next.



6. Verify that ports 1 to 4 are indeed configured as Fibre Channel ports.

CONFIGURE > Create UCS Domain Profile > Create	ate Port		Q 🛛 🕫	ං හා වි ඉතා දි ප්රතාන වේ ප්රතාන වේ ප්රතානය වේ ප්රතානය සහ සංකාශය සහ සංකාශය සහ සංකාශය සහ සහ සහ සහ සහ සහ සහ සහ සහ
⊆ Progress ① General		Step 3 Port Roles Configure port role through a unified p	es to define the traffic type carried port connection.	
2 Unified Port				
9 Port Roles	Port Roles Port Channels			
	Configure Selected Ports			
				Unconfigured
	Name	Туре	Role	Port Channel
	Port 1	FC	Unconfigured	
	Port 2	FC	Unconfigured	
	Port 3	FC	Unconfigured	
	Port 4	FC	Unconfigured	
	Port 5	Ethernet	Unconfigured	
	Port 6	Ethernet	Unconfigured	
	Port 7	Ethernet	Unconfigured	
	Port 8	Ethernet	Unconfigured	

7. Select all the ports that need to be configured as server ports by clicking the ports in the graphics (or from the list below the graphic). When all ports are selected, click Configure.



8. From the drop-down menu, choose Server as the role. Leave Forward Error Correction (FEC) set to Auto and click Save.

		Configure (8 Ports)
Configuration		
Selected Ports Role Unconfigured	Ports 5-8, Ports 17-20	
Server		
Ethernet Uplink FCoE Uplink Appliance <b>Unconfigured</b>		

9. Configure the Ethernet uplink port channel by selecting the port channel in the main pane and then clicking Create Port Channel.

			Step 3 Port R Configur through a	toles e port roles to defin a unified port conne	e the traffic type carrie	ed		
Port Roles	Port Channels							
Create Port Cl	nannel	134714 354716 174716 1947	20 21 A¥ 22 23 A¥ 24 25 A¥	10 27 AV 28 20 AV 30 31 AV 32	<u>31 A V 34 35 A V 36 37 A V 38 39 A V 40</u>	414442 (SA444 451446 (SA4	40 40 A ¥50 51 A ¥5	53A ¥54
CISCO UCS-FI-6454		PTEPTE PTEPT						

10. Choose Ethernet Uplink Port Channel as the role, provide a port-channel ID (for example, 15), and choose a value for Admin Speed (Auto is used in this example).

CONFIGURE > Create UCS Domain Pr	ofile > Create Port					Q	$\square$	₽	q	0	Paniraja Koppa 🖉
			<u>دې</u>	Create Port Chann	el						
	Configuration										
	Role Ethernet Uplink Port Channel										
	Port Channel ID *		Admin	Speed							
	15	0	Auto								
	Flow Control Select Policy 🗐	1 200									
	Link Aggregation Select Policy 僵										
	Link Control Select Policy 🗐										

- 11. Click Save.
- 12. Configure a Fibre Channel Port Channel by selecting the port channel in the main pane again and clicking Create Port Channel.
- 13. In the drop-down menu under Role, choose FC Uplink Port Channel.
- 14. Provide a port-channel ID (for example, 111), choose a value for Admin Speed (16Gbps is used here), and provide a VSAN ID (for example, 111).

CONFIGURE > Create UCS Domain P	ofile > Create Port		¢ 🛛 🗗	ଦ୍ ଞ	ල Paniraja Koppa ዾ
	ξ	Create Port Channel			
	Configuration Role FC Uplink Port Channel				
	Port Channel ID * 111 (	Admin Speed Ĵ ○ 1-256	VSAN ID * 111	) © 1 - 4093	
	Select Ports <ul> <li>FC or Ethernet ports with unconfig</li> </ul>	igured role are available for port channel creation.			
			Ethernet Uplink Port Chan	nel Member	

- 15. Click Save.
- 16. Verify the port-channel IDs and ports after both the Ethernet uplink port channel and the Fibre Channel uplink port channel have been created.

					Configure por through a unif	<b>?S</b> t roles to define the fied port connectio	e traffic type n.	carried			
Port	Roles	Port Chanr	nels								
Creat	e Port Cha	innel									
						28 29 4 7 30 31 4 7 32 10 33 4 7 3	4 35 A¥ 36 37 A¥ 38	39 AT 40 41 AT 42 43 AT 44 45 4	¥46 47 A¥ 48 49 A	¥50 51▲ ¥52	53 A ¥54
1472			114412 13441								15
IAY2	3A¥4 5A¥				₽₸₽₽₸₽₽₸₽₸						15 4 15
	3 A Y 4 5 A Y						Ethernet Up	ink Port Channel Merr	nber • FC L	plink Port Cha	nnel Mem
	5474 54					2 items for	Ethernet Up	ink Port Channel Merr	nber • FCU	plink Port Cha	nnel Mem
	ID				Role	2 items for	Ethernet Up und 50	ink Port Channel Merr	nber • FC L	plink Port Cha	nnel Mem
	ID			15	Role Ethernet Uplink Por	2 items for	Ethernet Up	ink Port Channel Men v per page Ports Port 53, Port 54	nber • FC L	plink Port Cha	nnel Mem
	1D			15 111	Role Ethernet Uplink Port	2 items for t Channel	Ethernet Up	ink Port Channel Merr v per page Ports Port 53, Port 54 Port 1, Port 2	aber • FC L	plink Port Cha	nnel Mem

17. Click Save to create the port policy for Fabric Interconnect A. Use the summary screen here to verify that the ports were selected and configured correctly.

	Step 4 Ports Col Create or sele interconnect	nfiguration ect a port policy for the fabric pair.	
• Configure ports by creating or selecting a polic	cy.		
Fabric Interconnect A Configured			
Ports Configuration		×	//   AA04-6454-A-PortPol
	Ethernet Uplink Port Chan	nel Member • FC Uplink Port Channel Me	Ports Port Channels
Port Type		Port Channel Type	
FC	4	FC Uplink	1
Ethernet	50	Ethernet Uplink	1
Port Role		Port Channel Role	
	8	EC Unlink	2
Server		РС Оршик	£

- 18. Now create policy for Fabric Interconnect B. Click Select Policy for Fabric Interconnect B, and in the pane at the right, click Create New.
- 19. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-B-PortPol**).

50%	Step 1 General Add a name, description and tag for the policy.	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
Organization *		
FlexPod		
Name *		
AA04-6454-B-Por	rtPol	
Switch Model *		
UCS-FI-6454		~
Set Tags		
Description		
Port Policy for FI-	B	

20. Repeat the steps you used for Fabric Interconnect A to configure Fibre Channel ports, server ports, and Ethernet and Fibre Channel port channels with appropriate IDs (for example, Ethernet port-channel ID 16 and Fibre Channel port-channel ID 112).

reate Port Chan						
1472 3474 5476	7448 94410 114412 134414 154416	17 AV 18 19 AV 20 21 AV 22 23 AV 24	25 A¥ 26, 27 A¥ 28, 29 A¥ 30, 31 A¥ 32, 33,	AV 34 35 AV 36 37 AV 38 39 AV 40 41 AV 43	43 87 44 45 87 46 47 87 48 49 8 750	51A ¥52 53A ¥5
						16
112		تصيد فجد تجتد بإدار	والمراجع بكريكم	كر كر كر كر كر ال	يس الورية بور	16

21. Use the summary screen shown here to verify that the ports were selected, port channels for Ethernet and FC are configured correctly for Fabric Interconnect B.

CONFIGURE > Create UCS Domain Profile			0 R 4	<b>९ @</b> Ø	Paniraja Koppa 🖉		
─ Progress							
(1) General	Fabric Interconnect B Configured				^		
2 UCS Domain Assignment	Ports Configuration	Ports Configuration			1		
3 VLAN & VSAN Configuration				Ports Port Channels			
Ports Configuration			ana mananananana		]		
5 UCS Domain Configuration	CIECO UCS-11-6454	000005-0-444					
6 Summary		Ethernet Uplink Port Chann	el Member 🛛 💿 FC Uplink Port Channel Me	mber 💿 Server 💿 Unconfigure	ed		
	Port Type		Port Channel Type				
	FC		FC Uplink				
	Ethernet	50	Ethernet Uplink				
	Port Role		Port Channel Role				
	Server		FC Uplink				
	Unconfigured	42	Ethernet Uplink				

22. When the port configuration for both fabric interconnects is complete and looks good, click Next.

# Step 5: UCS Domain Configuration

You need to define some additional policies, such as NTP, network connectivity, and system QoS, for the Cisco UCS domain configuration.

CONFIGURE > Create UCS Domain Profile		¢ 🛛 🕫	<b>୯</b> ଓ ଡ	Paniraja Koppa 🚨
⊆ Progress	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Step 5 UCS Domain Configuration		
1 General		Select the compute and management policies to be associated with the fabric interconnect.		
2 UCS Domain Assignment				
3 VLAN & VSAN Configuration	Show Attached Policies (0)			
4 Ports Configuration	Management 0 of 4 Policies Configured			
5 UCS Domain Configuration				
6 Summary	NTP		Select Policy 🗐	
	Syslog		Select Policy	
	Network Connectivity		Select Policy	
	SNMP		Select Policy	
	Network 0 of 2 Policies Configured			
	System QoS		Select Policy	
	Switch Control		Select Policy	

### **Configure NTP policy**

To define an NTP server for the Cisco UCS domain, configure NTP policy.

- 1. Click Select Policy next to NTP and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-NTPPol**).

	Step 1 General Add a name, description and tag for the policy.
Organization *	
FlexPod	
Name *	
AAAA-6454-NITDD	al
Set Tags	
Set Tags	
Set Tags	

- 3. Click Next.
- 4. Enable NTP, provide the NTP server IP addresses (for example, **192.168.160.254**), and select the time zone from the drop-down menu (for example, America/Los\_Angeles).

CONFIGURE > Create UCS Domain	Profile > Create NTP			Q	Ľ		₽	Q		0	Paniraja Koppa 🚨
─ Progress		~~~	Step 2								
1 General	Ę		Policy Details Add policy details								
2 Policy Details											
					All Platfor	ms	UCS Se	rver (Stand	alone)	UCS Domai	n
	Enable NTP O										
	NTP Servers *										
	192.168.160.254										
	Timezone										
	America/Los_Angeles									~ 0	) _

5. Click Create.

## Configure network connectivity policy

To define the Doman Name Service (DNS) servers for Cisco UCS, configure network connectivity policy.

- 1. Click Select Policy next to Network Connectivity and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-NetConnPol**).

~~~ <b>~</b>	Step 1 General
~~ <u>(</u> )}	Add a name, description and tag for the policy.
Organization *	
FlexPod	
Name *	
AA04-6454-NetCo	onnPol
Set Tags	
Set Tags Description	
Set Tags Description Network Connect	ivity Policy

3. Provide DNS server IP addresses for Cisco UCS (for example, 192.168.160.53 and 192.168.160.54).

CONFIGURE > Create UCS Domain Profile > Create N	etwork Connectivity		¢ ⊻	¢¶ °		Paniraja Koppa 🚨
⊂ Progress	~~~	Step 2				
1 General	Ę CAR	Add policy details				
Policy Details			All Platforms	UCS Server (Sta	ndalone) UCS Doma	ain
						<u> </u>
	Common Properties					
	IPv4 Properties					
	Preferred IPv4 DNS Server					
	192.168.160.53	<u> </u>	2.168.160.54			0
	Enable IPv6 ①					

4. Click Create.

# Configure system QoS policy

To define the QoS settings for Cisco UCS, configure system QoS policy.

- 1. Click Select Policy next to System QoS and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-SystemQoSPol**).

	Step 1 General Add a name, description and tag for the policy.
Organization *	
FlexPod	
Name *	
AA04-6454-Syste	mQoSPol
Sot Togo	
Description	
Description QoS Policy for UC	S

3. Keep the default selections or change the parameters if necessary. In this document, the MTU setting for Ethernet traffic is kept as 9216.

CONFIGURE > Create UCS Domain Profile > Create S	System QoS	ධ 🔽 📢 🔍 💭 ⑦ Paniraja Koppa ይ
☑ Progress ① General	Step 2 Policy Do Add policy do	Details Setails
Policy Details	This policy is applicable only for UCS Domains	
	Configure Priorities	
	Platinum	
	Gold	
	Silver	
	Bronze	
	CoS         Weight           255         0         5	Allow Packet o 9216 0 - 100 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	CoS         Weight           Tribre Channel         3         ©         5           06         06         06         06	MTU 000 9216 0 ○ Allow Packet © 2240 0 0 - 10 1500 - 9216

- 4. Click Create.
- 5. Click Next.

# **Configure other policies**

You can optionally configure syslog policy if you want to keep the logs in a syslog server. If you want a custom MAC address aging time or link control settings, you can create a switch control policy.

# Step 6: Summary

Verify all the settings (including the fabric interconnect settings, by expanding the settings) and make sure that the configuration is correct.

<ul> <li>Progress</li> <li>General</li> <li>UCS Domain Assignment</li> </ul>		Step 6 Summary Review the UC configuration of	r S domain profile details, resolve errors and deploy the profile.		
3 VLAN & VSAN Configuration	General				
4 Ports Configuration	Name AA04-6454-DomPro	f	Status 🔥 Not Deployed		
5 UCS Domain Configuration		a			
5 Summary	Fabric Interconnect 🗘	Model	Serial	Requires Reboot	
		UCS-FI-6454	FD0233117PH	No	
		UCS-FI-6454	FD023310PL2	No	
	Ports Configuration VLAN & VSAN	Configuration UCS Domain Configu	uration Errors / Warnings		
	Fabric Interconnect A				
	Fabric Interconnect B				
< Back Close					Deploy

# Deploy the Cisco UCS domain profile

After verifying the configuration, deploy the Cisco UCS profile.

1. Click Deploy.



2. Acknowledge the warning and click Deploy again.

The system will take some time to validate and configure the settings on the fabric interconnects. You can log into the terminal or console servers to see when the Cisco UCS fabric interconnects have finished configuration and are successfully rebooted.

# Verify Cisco UCS domain profile deployment

When the Cisco UCS domain profile has been successfully deployed, the Cisco UCS chassis and the blades should be successfully discovered.

1. Log in to the Cisco Intersight portal. Under CONFIGURE > Profiles > UCS Domain Profiles, verify that the domain profile has been successfully deployed.

≡	iliali، cisco Intersigh	nt	CONFIGURE > Profiles				Q	⊡ ¶	¢   0	٢	0	Paniraja Kop	ppa 🕰
<u>00o</u>			HyperFlex Cluster Profiles UCS Chassis Profiles	UCS Domain Profiles UCS Server Profiles	Kube	netes Cluster Profiles					Create	UCS Domain P	rofile
Ŵ	OPERATE												
×	CONFIGURE		🖉 🗇 🛍 🛛 🔍 Add Filter							per page 🛛 🕅			
	Orchestration		Name S	Status		UCS D Fabric Interconnect A	omain Fabric In		Last Update				
	Profiles			📀 ок					2 minutes a	<b>j</b> o			
	Templates												
	Policies												
Q	ADMIN												

2. Verify that the chassis has been discovered and is visible under OPERATE > Chassis.

=	،را،،را،، دוدده Intersight	OPERATE > Chassis	🗘 🖸 📢 🔍 🕄 🔿 Paniraja Koppa 🕰						
<u>00o</u>	MONITOR	Contract Status - NO DATA AVAILABLE	52						
	OPERATE ^	CONNELL SIGUES NU DATA AVAILABLE	act status NO DAIA AVAILABLE						
	Servers	··· 🖉 9. Add Filter	G Export         1 items found         10 ∨ per page         C         1         O         O						
	Chassis	Name         Health         Contract Status         Chassis ID         UCS Domain	Model Serial Chassis Profile §						
	Fabric Interconnects	AA04-6454-1         O Healthy         -         1         AA04-6454	UCSB-5108-AC2						
	Networking Sites								
	HyperFlex Clusters								

3. Verify that the servers have been successfully discovered and are visible under OPERATE > Servers.

≡	cisco Intersight	t	OPERATE > Servers						¢				Paniraja Ko	
<u>00o</u>														
Ŵ	OPERATE		Health	Power	HCL Status A Not Listed 2	Models		Contract Status <ul> <li>Not Covered 7</li> </ul>	Server Profile		Request	is (Last 24h)		
	Servers		7 • Healthy 7		Incomplete 5	7				<ul> <li>Not Assigned 16</li> </ul>	(7			
	Chassis													
	Fabric Interconnects		··· 🧷 🔍 Add Filt	er								r page 🔣 🔇 🔤		
	Networking Sites		Name		Server Profile		Health 🗘	Contract Status	Manage 🗘	Model			Memory 🗘	
	HyperFlex Clusters						Healthy			UCSB-B200-M5		160.0		
	Storage						Healthy			UCSB-B200-M5		128.0	192.0	
	Virtualization						Healthy			UCSB-B200-M5		80.0		
	Kubernetes						Healthy			UCSB-B200-M5		128.0	256.0	
$\times$	CONFIGURE						Healthy			UCSB-B200-M5		128.0		
¢	ADMIN						Healthy			UCSB-B200-M5		160.0		
							Healthy			UCSB-B200-M5		80.0		
			🧷									Я	] < _1_ of 1 [	N

# **Configure the server profile**

In the Cisco Intersight platform, a server profile enables resource management by simplifying policy alignment and server configuration. You can create server profiles using the server profile wizard to provision servers, create policies to help ensure smooth deployment of servers, and eliminate failures that are caused by inconsistent configuration. After creating server profiles, you can edit, clone, deploy, or unassign them as required.

To configure a server profile, follow these steps:

- 1. Log in to the Cisco Intersight portal.
- 2. Go to Configure > Profiles and in the main window select UCS Server Profile.
- 3. Click Create UCS Server Profile.
- 4. Click Start.

	ໍາມາປາ Intersight	CONFIGURE > Create UCS Server Profi			₽		
	MONITOR						
	OPERATE V						
*	CONFIGURE ^		Create UCS Server Profile				
	Orchestration		A UCS server profile enables resource management by streamlining po server configuration.	blicy alignment, and			
	Profiles						
	Templates						
	Policies						
			Server Assignment				
	ADMIN ~		Choose to assign a server to the profile now or assign it later.				
			• • •				
			Do not show this page again				
							Start >

## Step 1: General

Follow these steps for the general configuration:

- 1. Choose the organization from the drop-down menu (for example, **FlexPod**) and provide a name for the server profile (for example, **FlexPod-RHEL-Host-1**).
- 2. Select UCS Server (FI-Attached).

CONFIGURE > Create UCS Server Profile	ධ 🗹 🕫 Q, 🕄 ⊘ Paniraja Koppa ዿ
⋶ Progress	Step 1
General	General Enter a name, description, tag and select a platform for the server profile.
2 Server Assignment	
	Organization *
3 Compute Configuration	FlexPod v
4 Management Configuration	
	Name *
5 Storage Configuration	ElexPod-RHEL-Host-1
6 Network Configuration	Town I Blad and A
	larget Platform O
7 Summary	UCS Server (Standalone) O UCS Server (FI-Attached)
	Set Tags
	Description
	Server Profile for RHEL host-1
	<= 1024

3. Click Next.

# Step 2: Server Assignment

Follow these steps for server assignment:

- 1. Make sure server assignment is set to Assign Now.
- 2. Select a server (for example, AA06-6454-1-1) and click Next.

CONFIGURE > Create UCS Server Profile		🗘 🗹 📢 🔍 🕄 🕜 Paniraja Koppa
œ Progress	Step 2	income and
1 General	Choose to assign assign it later.	signment In a server to the profile now or
2 Server Assignment		
3 Compute Configuration	Assign Now Assign Later	
4 Management Configuration	<ul> <li>Choose to assign a server now or later. If you choose Assign Server, select a Later, click Next to proceed to select and associate policies.</li> </ul>	a server you want to deploy and click Next. If you choose Assign Server
5 Storage Configuration		
6 Network Configuration	Show Assigned	
7 Summary	Add Filter	7 items found 10 ∨ per page K < 1 of 1 > >
7 Summary	Q.     Add Filter       Name     C       User Label     Health	7 items found     10 v per page     I of 1     D       0     Model     0     UCS Domain   Serial Number
7 Summary	Q.     Add Filter       Name     User Label       Image: Add4-6454-1-1     Image: Healthy	7 items found     10 ∨     per page      1     of 1     >>       Model      UCS Domain     Serial Number       UCSB-B200-M5     AA04-6454
7 Summary	Q.         Add Filter         C           Name         0         User Label         Health           Image: Add4-6454-1-2         Image: Healthy         Image: Healthy           Add4-6454-1-2         Image: Healthy         Image: Healthy	7 items found       10 ∨ per page (< 1 of 1 > >       (3)         0       Model       0       UCS Domain       Serial Number         0       UCSB-B200-M5       AA04-6454       0         0       UCSB-B200-M5       AA04-6454       0
7 Summary	Q.     Add Filter       Name     User Label       AA04-6454-1-1     Image: Healthy       AA04-6454-1-2     Image: Healthy       AA04-6454-1-3     Image: Healthy	7 items found       10 v per page       i       1       of 1       i       iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii
7 Summary	Add Filter       Name     User Label     Health       AA04-6454-1-1     • Healthy       AA04-6454-1-2     • Healthy       AA04-6454-1-3     • Healthy       AA04-6454-1-4     • Healthy	7 items found       10 v per page ( < 1 of 1 > )       ()         Model       2       UCS Domain       Serial Number         UCSB-B200-M5       AA04-6454       1
7 Summary	Add Filter       Name     User Label       AA04-6454-1-1     • Healthy       AA04-6454-1-2     • Healthy       AA04-6454-1-3     • Healthy       AA04-6454-1-4     • Healthy       AA04-6454-1-5     • Healthy	7 items found       10 v per page ( < 1 of 1 > )       ()         1       Model       2       UCS Domain       Serial Number         1       UCSB-B200-M5       AA04-6454       1
7 Summary	Add Filter       Name     User Label       AA04-6454-1-1     • Healthy       AA04-6454-1-2     • Healthy       AA04-6454-1-3     • Healthy       AA04-6454-1-4     • Healthy       AA04-6454-1-5     • Healthy       AA04-6454-1-6     • Healthy	7 items found       10 v per page ( < 1 of 1 ) )       ()         Model       I       UCS Domain       Serial Number         UCSB-B200-M5       AA04-6454       I         UCSB-B200-M5       AA04-6454       I

# **Step 3: Compute Configuration**

Next, configure the computing resources.

# **Configure BIOS policy**

Follow these steps to configure BIOS policy:

- 1. Click Select Policy next to BIOS Configuration and the, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-BiosPol**).

CONFIGURE > Create UCS Server Profile > Create BIOS Policy	
Œ Progress	Step 1
General	General Add a name, description and tag for the policy.
2 Policy Details	
	Organization * FlexPod ~
	Name *
	AA04-6454-BiosPol
	Set Tags
	Description

- 3. Click Next.
- 4. On the Policy Details screen, select appropriate values.

CONFIGURE > Create UCS Server Profile > Create Bi	DS Policy	Ç			R				Paniraja Koppa 🚨
Progress	~~~~	Step 2							
1 General		Add policy details							
2 Policy Details		All Platfo		UCS Serv	er (Standa	lone)	UCS Server	(FI-Attached)	
			'						
	A The BIOS settings will be applied only on next host re	boot.							
	+ Boot Options								
	+ Intel Directed IO								
	+ LOM And PCIe Slots								
	+ Main								
	+ Memory								
	+ PCI								
	+ Power And Performance								
	+ Processor								
	+ QPI								
	+ Serial Port								

The validation described in this document used the following values to align with the Cisco Validated Designs for FlexPod:

- LOM and PCIe Slot > CDN Support for LOM: Enabled
- Processor > DRAM Clock Throttling: Performance
- Processor > Freq Floor Override: Enabled
- Processor > CPU C State: Disabled
- Processor > Processor C1E: Disabled
- Processor > Processor C3 Report: Disabled
- Processor > Processor C6 Report: Disabled
- Processor > Power Technology: Custom
- Processor > Energy Performance: Performance
- Memory > NVM Performance Setting: Balanced Profile
- Memory > Memory RAS Configuration: Maximum Performance
- 5. Click Create.

# Configure boot-order policy

This solution is validated with both iSCSI and Fibre Channel boot-from-SAN configurations. Choose one policy based on your requirements.

### **Configuring boot-order policy for Fibre Channel**

Follow these steps to configure boot-order policy for Fibre Channel:

- 1. Click Select Policy next to Boot Order Configuration and then, in the pane on the right, click Create New.
- Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, AA04-6454-FC-BootPol).

CONFIGURE > Create UCS Server Profile > Create Boot Order Policy	ධ 🗹 📢 🔍 වෘniraja Koppa ቧ
준 Progress	Step 1
General	General Add a name, description and tag for the policy.
2 Policy Details	
	FlexPod ~
	Name *
	AA04-6454-FC-BootPol
	Set Tags
	Boot Order for FC Boot from SAN
	<≈ 1024

- 3. Click Next.
- 4. For Configured Boot Mode, select Unified Extensible Firmware Interface (UEFI).
- 5. From the Add Boot Device drop-down menu, choose Virtual Media.
- Provide a device name (for example, kvm-mapped-iso) and then, for the subtype, choose KVM Mapped DVD.

CONFIGURE > Create UCS Server f	Profile > Create Boot Order Policy - 🗘 🔀 🕫 📀 Panil	iraja Koppa
<ul> <li>Progress</li> <li>General</li> <li>Policy Details</li> </ul>	Step 2 Policy Details Add policy details Mit Platforms UCS Server (Standalone) UCS Server (FI-Attached) Configured Boot Mode O Legacy O Unified Extensible Firmware Interface (UEFI) Enable Secure Boot O	
	Add Boot Device       ~         - Virtual Media (kvm-mapped-iso)       Image: Comparison of the second	

For this validation, all four NetApp controller LIFs will be added as boot options. The four LIFs are named as follows:

- NA-FCP-LIF01a: NetApp Controller 1, LIF for Fibre Channel SAN A
- NA-FCP-LIF02a: NetApp Controller 2, LIF for Fibre Channel SAN A
- NA-FCP-LIF01b: NetApp Controller 1, LIF for Fibre Channel SAN B
- NA-FCP-LIF02b: NetApp Controller 2, LIF for Fibre Channel SAN B
- 7. From the Add Boot Device drop-down menu, choose SAN Boot.
- 8. Provide the device name (for example, **NA-fcp-lif01a**) and the Logical Unit Number (LUN) value (for example, 0).
- 9. Provide an interface name (for example, **vHBA-A**) and note this name for use later in the vHBA definition. This value is important and should match the vHBA name.

**Note: vHBA-A** is used for NA-fcp-lif01a and NA-fcp-lif02a, and **vHBA-B is** used for NA-fcp-lif01b and NA-fcp-lif02b.

 Add the appropriate World Wide Port Name (WWPN) as the target WWPN. You can obtain this value from NetApp after logging in and entering the following command on the NetApp controller: network interface show -vserver <vserver name>.

— SAN Boot (NA-fcp-lif01a)			Enabled	⑪	^	~
Device Name *		LUN				
NA-fcp-lif01a		0			Ĵ	0
					0 -	255
Interface Name *		Target WWPN				
vHBA-A	0	20:01:00:a0:98:5b:4a:86				0
Bootloader Name	(i)	Bootloader Description				(i)
Bootloader Path	0					
	<u> </u>					

- 11. Click Create.
- 12. Repeat these steps three more times to add all the NetApp LIFs. You can rearrange the policies using the arrow keys if needed.

Configuration for NA-fcp-lif02a:

— SAN Boot (NA-fcp-lif02a)			Enabled	Û		
Device Name *		LUN				
NA-fcp-lif02a	0	0			0	0
						255
Interface Name *		Target WWPN				
vHBA-A		20:03:00:a0:98:5b:4a:86				
Bootloader Name		Bootloader Description				
Bootloader Path						

# Configuration for NA-fcp-lif01b:

— SAN Boot (NA-fcp-lif01b)			Enabled	Û		
Device Name *						
NA-fcp-lif01b					0	
					0 -	255
Interface Name *		Target WWPN				
vHBA-B	0	20:02:00:a0:98:5b:4a:86				0
Bootloader Name		Bootloader Description				
Bootloader Path						

# Configuration for NA-fcp-lif02b:

- SAN Boot (NA-fcp-lif02b)		Enabled 📋	^	~
Device Name *		LUN		
NA-fcp-lif02b			Ĵ	
			0 -	255
Interface Name *		Target WWPN		
<u>vHBA-B</u>		20:04:00:a0:98:5b:4a:86		
Bootloader Name	0	Bootloader Description		0
Bootloader Path				

After you have added all the boot devices, they should be listed on the Policy Details screen.

	Step 2 Policy Details Add policy details
	All Platforms UCS Server (Standalone) UCS Server (FI-Attached
Configured Boot Mode $\odot$	
C Legacy 💿 Unified Extensible Firmware Interface (UE	EFI)
● Enable Secure Boot ⊙	
Add Boot Device   >	
+ Virtual Media (kvm-mapped-iso)	Cabled 🛛 🗂 ^ 🗸
+ SAN Boot (NA-fcp-lif01a)	C Enabled 🛛 🗂 🔷 🗸
+ SAN Boot (NA-fcp-lif02a)	C Enabled 🛛 🖞 ^ 🗸
+ SAN Boot (NA-fcp-lif01b)	C Enabled
+ SAN Boot (NA-fcp-lif02b)	Enabled 📋 ^ 🗸

- 13. Click Create.
- 14. Click Next.

# Creating boot-order policy for iSCSI boot from SAN

Follow these steps to configure boot-order policy for iSCSI boot from SAN:

- 1. Click Select Policy next to BIOS Configuration and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-iSCSI-BootPol**).

C Progress C General Policy Details	Step 1 General Add a name, description and tag for the policy.
-	Organization *
	FlexPod ~
	Name *
	AA04-6454-ISCSI-BootPol
	Set Tans
	Description
	Boot Order for iSCSI Boot from SAN
	e= 1024

- 3. Click Next.
- 4. For Configured Boot Mode, select Unified Extensible Firmware Interface (UEFI).
- 5. From the Add Boot Device drop-down menu, choose Virtual Media.

		Step 2 <b>Policy Det</b> Add policy deta	ails <sup>ils</sup>		
			All Platforms	UCS Server (Standalone)	UCS Server (FI-Attac
Configured Boot Mode ①					
🔵 Legacy 💿 Unified Extensi	ble Firmware Interface (L	JEFI)			
Enable Secure Boot ①					
Add Boot Device V					
iSCSI Boot					
Local CDD					
Local Disk					
NVMe					
PCH Storage					
PXE Boot					
SAN Boot					
SD Card					
USB					

6. Provide a device name (for example, **ISO**) and then, for the subtype, choose KVM Mapped DVD.

CONFIGURE > Policies > Boot Order > Create		🗘 🛛 🕫 🔍 😳 🕜 Paniraja Koppa 🤈	2
⊆ Progress ① General	Step 2 Policy Detail Add policy details	ails	
Policy Details	T S S S S S S S S S S S S S S S S S S S	All Platforms UCS Server (Standalone) UCS Server (FI-Attached)	
	Configured Boot Mode ○ ○ Legacy ● Unified Extensible Firmware Interface (UEFI)		
	● Enable Secure Boot ⊘		
	Add Boot Device / ~		
	— Virtual Media (kvm-mapped-iso)	C Enabled 🛗 ^ 🗸	
	Device Name * kvm-mapped-iso ©		
	Sub-Type <u>KVM MAPPED DVD ~ 0</u>		

For this validation, two iSCSI interfaces (iscsi-a and iscsi-b) will be added as boot options. These interfaces with the same name will be created as part of LAN connectivity policy.

- 7. From the Add Boot Device drop-down menu, choose iSCSI Boot.
- 8. For Device Name and Interface Name, enter iscsi-a.

C Progress	Step 2 Policy Details Add policy details
	All Platforms UCS Server (Standalone) UCS Server (Fl-Attached)
	Configured Boot Mode $\odot$
	🔿 Legacy 💽 Unified Extensible Firmware Interface (UEFI)
	● Enable Secure Boot ⊘
	Add Boot Device   ~
	— iSCSI Boot (iscsi-a) 💿 Enabled
	Device Name * Interface Name *
	iscsi-a 0 iscsi-a 0
	Bootloader Name O Bootloader Description O
	Bootloader Path O
	+ Virtual Media (kvm-mapped-iso) Enabled 📋 ^ 🗸

9. Repeat steps 7 and 8 for interface iscsi-b.

<ul> <li>Progress</li> <li>General</li> <li>Policy Details</li> </ul>	Step 2         Policy Details         Add policy details         Ill Platforms       UCS Server (Standalone)         UCS Server (FI-Attached)
	Configured Boot Mode O
	C Legacy   Unified Extensible Firmware Interface (UEFI)
	● Enable Secure Boot ©
	Add Boot Device   ~
	— ISCSI Boot (iscsi-b) The boot (iscsi-b)
	Device Name * Interface Name * iscsi-b O O
	Bootloader Name O Bootloader Description O
	Bootloader Path ©
	+ ISCSI Boot (liscsi-a)
	+ Virtual Media (kvm-mapped-iso) Enabled 📋 🔨 🗸

10. Click Create.

After you have added all the boot devices, they should be listed on the Policy Details screen.

C Progress	Step 2 Policy Details Add policy details
	All Platforms UCS Server (Standalone) UCS Server (FI-Attached)
	Configured Boot Mode $\odot$
	C Legacy 💿 Unified Extensible Firmware Interface (UEFI)
	● Enable Secure Boot ⊙
	Add Boot Device   v
	+ Virtual Media (kvm-mapped-iso) Enabled   📋 ^ 🗸
	+ iSCSI Boot (iscsi-a) Chabled
	+ iSCSI Boot (iscsi-b) Cabled

11. Click Next.

# Step 4: Management Configuration

Next, configure management policy.

co	NFIGURE > Create UCS Server Profi	ile	Paniraja Koppa 🚨
U	Progress	Step 4	
	General	Management Configuration Create or select existing Management policies that you want to associate with this profile.	
2	Server Assignment		
3	Compute Configuration	Show Attached Policies (0)	
	Management Configuration	Certificate Management	
I		IMC Access	
	Storage Configuration	IPMI Over LAN	
6	Network Configuration	Local User	
7	Summary	Serial Over LAN	
		SNMP	
		Syslog	
		Virtual KVM	

### Configure Cisco IMC access policy

Follow these steps to configure Cisco IMC access policy:

- 1. Click Select Policy next to IMC Access and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-IMCPol**).

CONFIGURE > Create UCS Server Profile > Create IMC Access Policy		Q	ß	Ø	Q		Paniraja Koppa 🚨
	Step 1						
General General	Add a name, descrip	ption and tag	for the poli				
2 Policy Details							
	Organization *						
	FlexPoa						
	Name *						
	AA04-6454-IMCPol						
	Set Tags						
	Description						
				<= 1024			

- 3. Click Next.
- 4. Provide the in-band (or out-of-band) management VLAN ID (for example, 511). Also make sure that All Platforms is selected because you will need this policy while creating the chassis profile as well.

CONFIGURE > Create UCS Server Pr	rofile > Create IMC Access Policy			Q	ß		₽	Q			Paniraja Koppa 🚨
⊆ Progress		~~~	Step 2								
General			Policy Details Add policy details								
2 Policy Details											
					All Platforn	ns	UCS Serv	ver (FI-Atta	iched)	UCS Chase	sis
	VLAN ID *										
	511	0									
		4 - 4093									
	IPv4 address configuration 🛈										
	$\Box$ IPv6 address configuration $\odot$										
	IP Pool *										
	Select IP Pool 🗐										

- 5. Select "Configure IPv4 address configuration" and click Select IP Pool to define a KVM IP address assignment pool.
- 6. Click Create New in the menu on the right.
- 7. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-IP-Pool**).

CONFIGURE > Create UCS Server Profile > Create IMC	CAccess Policy > Create IP Pool	Q 🛛 🖌 🗞	ଦ୍ ଞ	🧑 🛛 Paniraja Koppa 🚨
⊂ Progress	st st	tep 1		
General	G C Pe o d	eneral pol represents a collection of IPv4 and/or IPv6 Idresses that can be allocated to other onfiguration entities like server profiles.		
2 IPv4 Pool Details 3 IPv6 Pool Details	Organization * FlexPod			
	<sub>Name</sub> * AA04-6454-IP-Pool			
	Set Tags			
	Description			

8. Select Configure IPv4 Pool and provide the information to define a pool for KVM IP address assignment.

CONFIGURE > Create UCS Server Profile > Create IN	IC Access Policy > Create IP Pool		Q	ß	¢⊈ q	\$		aniraja Koppa 🖉
œ Progress	~~~_	Step 2	ol Dotoilo					
(1) General		Network int interfaces.	erface configura	tion data for IPv4				
2 IPv4 Pool Details								
3 IPv6 Pool Details	Configure IPV4 Pool							
	Configuration							
	Netmask		Gateway					
	255.255.252.0		D <u>192.168.1</u>	60.254				
	Primary DNS		Secondary	DNS				
	192.168.160.53		D <u>192.168.1</u>	60.54				
	IP Blocks							
	From *		ize *					
	192.168.160.196	<u> </u>				0	Ŵ	
						1 - 254		
	From *		ize *					
	192.168.160.201	<u> </u>				0	Û	
						1 - 254		
	From *		ize *					
	192.168.160.205	<u> </u>				U O	÷	
						1 - 254		

**Note:** The management IP pool subnet should be accessible from the host that is trying to open the KVM connection. In the example shown here, the hosts trying to open a KVM connection would need to be able to route to 192.168.160.0 subnet.

- 9. Click Next.
- 10. Unselect Configure IPv6 Pool.
- 11. Click Create to finish configuring the IP address pool.
- 12. Click Create to finish configuring the IMC access policy.

## **Configure local user policy**

Follow these steps to configure local user policy:

- 1. Click Select Policy next to Local User and the, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-LocalUser-Pol**).

CONFIGURE > Create UCS Server P	Profile > Create Local User Policy			۵		₽	q	e	$\bigcirc$	Paniraja Koppa 🚨
			Step 1							
General		General Add a name, description and tag for the policy.								
2 Policy Details										
		Organization *								
		Name *								
		AA04-6454-Local	User-Pol							
		Set Tags								
		Description				<= 1024				

- 3. Verify that UCS Server (FI-Attached) is selected.
- 4. Verify that Enforce Strong Password is selected.

CONFIGURE > Create UCS Server Pr	rofile > Create Local User Policy	다 🗘 🖓 🥵 💮 Paniraja Koppa 🕰
Œ Progress	Step 2	
1 General	Add policy det	talls
2 Policy Details		All Platforms UCS Server (Standalone) UCS Server (FI-Attached)
	Password Properties	
	Enforce Strong Password	
	Call Enable Password Expiry ○	
	Password History <u>5 C</u> O 0 - 5	
	● Always Send User Password ◎	
	Local Users	
	This policy will remove existing user accounts other than the ones con deleted from the endpoint device. You can only enable/disable or chan user name and role as 'admin'. If there are no users in the policy, only the default, IPMI support is enabled for all users	nfigured with this policy. However, the default admin user account is not nge account password for the admin account by creating a user with the the admin user account will be available on the endpoint device. By
	Add New User	

- 5. Click Add New User.
- 6. Provide the username (for example, **flexpodadmin**), choose a role (for example, admin), and provide a password.

**Note:** The username and password combination defined here will be used to log in to KVMs. The typical Cisco UCS admin username and password combination cannot be used for KVM access.

— flexpodadmin (admin) ⊘			Enable 📋
Username *		Role	
flexpodadmin	0	admin	× 0
Password *		Password Confirmation *	
	0 ()		© ()

- 7. Click Create to finish configuring the user.
- 8. Click Create to finish configuring local user policy.
- 9. Click Next.

## **Step 5: Storage Configuration**

Click Next on the Storage Configuration screen. You will not make any changes to this configuration.

# Step 6a: Network Configuration > LAN Connectivity

LAN connectivity policy defines the connections and network communication resources between the server and the LAN on the network. This policy uses pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

The LAN connectivity policy requires you to create Ethernet network policy, Ethernet adapter policy, and Ethernet QoS policy. When you attach a LAN connectivity policy to a server profile, the addresses of the MAC address pool, or the static MAC address, are automatically assigned.

## Configure LAN connectivity policy for iSCSI boot

Follow these steps to define LAN connectivity if you are using iSCSI SAN.

1. Click Select Policy next to LAN Connectivity and then, in the pane on the right, click Create New.

CONFIGURE > Create UCS Server Pr	file 🗘 🗹 📢 🕜 Paniraja K	Coppa 🕰
─ Progress	Step 6	
1 General	Network Configuration Create or select existing Network Configuration policies that you want to associate with this profile	
2 Server Assignment		
3 Compute Configuration	Show Attached Policies (0)	
(4) Management Configuration	LAN Connectivity Select Policy	
5 Storage Configuration	SAN Connectivity	
	Auto Placement Configuration for vNICs & vHBAs	
Network Configuration		
7 Summary	Graphical representation of vNICs & vHBAs placement is only applicable for Auto Configuration mode.	

2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-iSCSI-LanConn**).

CONFIGURE > Create UCS Server Profile > Create LAN Connectivity Policy	ඩු 🛛 🕫 🗘 ⑦ Paniraja Koppa 🗘
Œ Progress	Step 1
General	General Add a name, description and tag for the policy.
- Tondy bottoms	Organization *
	FlexPod
	Name *
	AAU4-0494-ISUSI-Lanconn
	Set Tags
	Description
	LAN Connectivity policy for iSCSI SAN
	<= 1024

This deployment uses three vNICs, as follows:

- mgmt: Fabric Interconnect A vNIC for management and NFS VLANs
- iscsi-a: Fabric Interconnect A vNIC for iSCSI
- iscsi-b: Fabric Interconnect B vNIC for iSCSI
- 3. For the iSCSI qualified name (IQN), select Pool.
- 4. To keep the vNIC placement simple, select Auto vNIC Placement for vNIC configuration.
- 5. Click Add vNIC.

Ć.	Step 2 Policy Details Add policy details	
IQN		
None Pool IQN Pool * Select Pool	Static	
vNIC Configuration		
Manual vNICs Placement	Auto vNICs Placement	
<ul> <li>For auto placement option the vNICs w more at</li> </ul>	ill be automatically distributed between adaptors during profile deployment. Learn Helj	o ter
For auto placement option the vNICs w more at Add vNIC	II be automatically distributed between adaptors during profile deployment. Learn Heip Cen	o ter
For auto placement option the vNICs w more at	II be automatically distributed between adaptors during profile deployment. Learn Help Cen	ter ©
For auto placement option the vNICs w more at  Add vNIC  Name	Il be automatically distributed between adaptors during profile deployment. Learn Help Cen Switch ID Failover	ter O
For auto placement option the vNICs w more at Add vNIC Name	Il be automatically distributed between adaptors during profile deployment. Learn Help Cen Switch ID Failover NO ITEMS AVAILABLE	ter

6. Provide the name of the vNIC (for example, **mgmt**).

CONFIGURE > Create UCS Server	r Profile > Create LAN Connectivity Policy		Q [2]	¢4 0¢	Paniraja Koppa 🔔
				Pool	
	{O <b>X</b>			MAC Address Pools 0	
	ر <b>ن ک</b>				
	Name * mgmt				
	MAC Address				
	Pool Static				
	MAC Address Pool * Select Pool 🗐				
	Placement				
	Switch ID * A				
	Consistent Device Naming (CDN)				
	Source VNIC Name				

### Create the MAC address pool for Fabric A

The MAC address pool has not been defined yet, so a new MAC address pool will be created now for Fabric A. This pool will be reused for all future Fabric-A vNICs.

- 1. Click Select Pool under MAC Address Pool and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **MAC-Pool-A**).

CONFIGURE > Create UCS Server Pro	ofile > Create LAN Connectivity Policy > Create MAC Pool		0 V	ø	୍ ୍	Paniraja Koppa 🗕
₢ Progress	~	Step 1				
( ) General	E	Pool represents a c can be allocated to	collection of MAC addre VNICs of a server profil	sses that le.		
2 Pool Details						
	Organizat	on *				
	FlexPod					
	Name *					
	MAC-Po	ol-A				
	Set Tags					
	Descript	on				
				<= 1024		

- 3. Click Next.
- 4. Provide the starting MAC address. The recommended prefix for MAC addresses is 00:25:B5:xx:xx:xx. As a best practice, in FlexPod some additional information is always coded into the MAC address pool for ease of troubleshooting. For example, in the starting address 00:25:B5:A4:0A:00, A4 is the rack ID and 0A indicates Fabric A.
- 5. Provide the size of the MAC address pool (for example, 64).

CONFIGURE > Create UCS Server P	rofile > Create LAN Connectivity Policy > Create MAC Pool	ධ 🕑 🕫 🔍 🕄 🔿 Paniraja Koppa 🕰
☑ Progress	Step 2	
(1) General	Pool I Collectio	Details on of MAC Blocks.
2 Pool Details		
	MAC Blocks	
		Size *
	00:25:B5:A4:0A:00	© <u>64</u>
		1 - 1000

- 6. Click Create to finish creating the MAC address pool.
- 7. Back in the Add vNIC window, from the drop-down menu, choose A as the switch ID.
- 8. For Consistent Device Naming (CDN), from the drop-down menu, choose vNIC Name.
- 9. Verify that Failover is enabled.

		Add vNIC
Name *		
mgmt		
MAC Address		
Pool S	tatic	
MAC Address Pool *		
Placement		
Switch ID *		<u>v 0</u>
Consistent Device Naming (CDN)		
Source vNIC Name		<u>v 0</u>
Failover		
Enabled O		

#### **Create Ethernet network group policy**

The Ethernet policies have not been created yet, so these policies will be created now. These policies will be reused when additional vNICs are defined.

Ethernet network group policy defines the VLANs allowed for a particular vNIC. Three network group policies will be defined for this deployment:

- Management network group policy, to define the VLANs for management and NFS traffic
- iSCSI-A network group policy, to define the VLANs for iSCSI on Fabric A
- iSCSI-B network group policy, to define the VLANs for iSCSI on Fabric B
- 1. Click Select Policy under Ethernet Network Group Policy and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **Mgmt-NetGrp-Pol**).

CONFIGURE > Create UCS Server P	Profile > Create LAN Connectivity Policy > Create Ethern	net Network Group		Q		₽	Q,			Paniraja Koppa 🚨
至 Progress			Step 1							
General		General Add a name, description and tag for the policy.								
2 Policy Details										
		Organization *								
		FlexPod								
		Name *								
		Mamt-NetGrp-Pol								
		0.17								
		Set rags								
		Description								
		Policy to define th	e VLANs for manag	jement and	i NFS traff	ic /				
						<= 1024				

- 3. Click Next.
- 4. Enter the allowed VLANs (for example, 2,511,3050) and the native VLAN ID (for example, 2).

CONFIGURE > Create UCS Server P	Profile > Create LAN Connectivity Policy > Create Ethernet Network Group	ட 🕑 📢 🔍 🛱 🔿 Paniraja Koppa 🕰
─ Progress	Step 2	
(1) General	Policy Detail Add policy details	ls 
2 Policy Details		
	This policy is applicable only for UCS Servers (FI-Attached)	
	VLAN Settings	
	Allowed VLANs	Native VLAN 2 <u>Ĵo</u> 1 - 4093

5. Click Create to finish configuring the Ethernet network group policy.

## **Create Ethernet network control policy**

Ethernet network control policy is used to enable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for the vNICs. A single policy will be created here and reused for all the vNICs.

- 1. Click Select Policy under Ethernet Network Control Policy and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **Enable-CDP-LLDP**).

CONFIGURE > Create UCS Server	Profile > Create LAN Connectivity Policy	> Create Ethernet Network Control	¢		Ø	q			Paniraja Koppa 🙎	
─ Progress		~~~	Step 1							
General		₹ <b></b>	General Add a name, description and	ral name, description and tag for the policy.						
2 Policy Details		Organization *								
		FlexPod								
		Name *								
		Enable-CDP-LLDP								
		Set Tags								
		Description			<u>/</u>					
					<= 1024					

- 3. Click Next.
- 4. Enable Cisco Discovery Protocol and both Transmit and Receive under LLDP.

CONFIGURE > Create UCS Server Profile >	Create LAN Connectivity Policy 🔸 Create Ethernet Network Control 🗘 🖸 📢 💮 Paniraja Koppa	
<ul> <li>Progress</li> <li>General</li> <li>Policy Details</li> </ul>	Step 2 Policy Details Add policy details	
	<ul> <li>This policy is applicable only for UCS Servers (FI-Attached)</li> <li>Table CDP ©</li> <li>Mac Register Mode ©</li> <li>Only Native VLAN () All Host VLANs</li> <li>Action on Uplink Fai ©</li> <li>I unk Down () Warning</li> <li>Amportant If the Action on Uplink is set to Warning, the switch will not fail over if uplink connectivity is lost.</li> <li>MAC Security</li> <li>Forge O</li> <li>O Now () Deny</li> </ul>	

5. Click Create to finish creating Ethernet network control policy.

# **Create Ethernet QoS policy**

Ethernet QoS policy is used to enable jumbo maximum transmission units (MTUs) for all the vNICs. A single policy will be created and reused for all the vNICs.

- 1. Click Select Policy under Ethernet QoS and in then, the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **Jumbo-MTU-QoS**).

CONFIGURE > Create UCS Server Pro	file > Create LAN Connectivity Policy > Create Ethernet	QoS		Q		Ø	Q		Paniraja Koppa 🗕
☑ Progress		~~~	Step 1						
1 General			General Add a name, descriptio	n and tag					
2 Policy Details									
		FlexPod							
		Name *							
		Jumbo-MTU-QoS							
		Set Tags							
		Departmen							
					<	1024			

- 3. Click Next.
- 4. Change the MTU, Bytes value to 9000.

CONFIGURE > Create UCS Server F	Profile > Create LAN Connectivity Policy > Create Ethernet QoS		¢   ⊻   ¢	୍ ଞ ୯	) Paniraja Koppa 🚨
─ Progress	~~~	Step 2			
(1) General		Policy Det Add policy deta	tails ails		
2 Policy Details			7	(0to deleta)	1 <b>4 4 5 5 6</b>
			All Platforms UCS Server	(Standalone) UCS Server (F	I-Attached)
	QoS Settings				
	MTU, Bytes		Rate Limit, Mbps		
	9000	() ©			<u>)</u> 0
		1500 - 9000			0 - 100000
	Burst		Priority		
	1024	<u> (</u>	Best-effort		<u>~ 0</u>
		024 - 1000000			
	■ Enable Trust Host CoS ○				

5. Click Create to finish setting up the Ethernet QoS policy.

## **Create Ethernet adapter policy**

Ethernet adapter policy is used to set the interrupts and the send and receive queues. The values are set according to the best-practices guidance for the operating system in use.

- 1. Click Select Policy under Ethernet Adapter and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **RHEL-Ether-AdapterPol**).
3. Click Ethernet Adapter Default Configuration and choose Linux.

CONFIGURE > Create UCS Server Profile > Create LAN Connectivity Policy	Create Ethernet Adapter	Q [	∑ <b>4</b> 0,		Paniraja Koppa 🚨						
⊂ Progress	Step 1		Default Configurat	Default Configuration							
General	General	ription and tag for t	Policies 16	Policies 16							
	Add a hame, descr	nption and tag for i	Search	Q Search							
2 Policy Details	Organization *		MQ-SMBd								
	FlexPod		SMBServer								
			SMBClient								
	RHEL-Ether-AdapterPol		🗐 Solaris								
			usNICOracleRAC	sNICOracleRAC							
	Set Tags		WIN-AzureStack	WIN-AzureStack							
			Win-HPN-SMBd	Win-HPN-SMBd							
	Description		Win-HPN	- 🗐 Win-HPN							
	Ethernet Adapter Default Configuration *		Linux-NVMe-RoC	Linux-NVMe-RoCE							
	Select Default Configuration		∰ MQ	∰ MQ							
			🗐 usNIC								
			SRIOV								
			VMWarePassThr	u							
			☐ ∨MWare								
			Windows								

4. Change the Interrupts, Receive Queue Count, Transmit Queue Count, and Completion Queue Count values to 16, 8, 1, and 9, respectively, as shown here:

CONFIGURE > Create UCS Server Profile > C	reate LAN Connectivity Policy > Create Ether	rnet Adapter		Q [	¢₽	Q (3	) 🧿 Panira	ja Koppa 🖉
⊂ Progress	Enable Virtual Extensible LAN							
	Enable Network Virtualization u	ising Generic	Routing Encapsulation ①					
1 General	Enable Accelerated Receive Flo	w Steering 🛈						
2 Policy Details	Enable Advanced Filter 💿							
	Enable Interrupt Scaling O							
	RoCE Settings							
	Enable RDMA over Converged E	Ethernet ©						
	Interrupt Settings							
	Interrupts		Interrupt Mode		Interrupt Timer,			
	16	<b>)</b> 0	MSIx	~ 0	125		<u> </u>	
	Interrupt Coalescing Type							
	Min	× 0						
	Receive							
	Receive Queue Count		Receive Ring Size					
	8	<ol> <li>Image: Image: Ima</li></ol>	512	() c				
		1 - 1000		64 - 409	- 6			
	Transmit							
	Transmit Queue Count		Transmit Ring Size					
		Ĵ 0	256	() (				
		1 - 1000		64 - 409				
	Completion							
	Completion Queue Count		Completion Ring Size					
	9	<u> </u>		<u> </u>	-			
		1 - 2000		T - 25	0			
	Uplink Failback Timeout (seconds)	6 0						
		0 - 600						
		0.000						

5. Verify that all the policies are assigned to vNIC mgmt.



### 6. Click Add to add the vNIC.

Ę	Step 2 Policy Details Add policy details		
IQN			
None Pool	Static		
IQN Pool * Select Pool 個			
vNIC Configuration			
Manual vNICs Placement	Auto vNICs Placement		
<ul> <li>For auto placement option the vNICs will more at</li> </ul>	be automatically distributed between a	adaptors during profile deployment. Learn	Help Center
Add vNIC			
Name	Switch ID	Failover	
mgmt		Disabled	

### Add iSCSI vNICs to LAN connectivity policy

**Note:** Repeat all the step under Step 6a: Network Configuration > LAN Connectivity to create additional vNICs. Most of the policies created for the mgmt vNIC will be reused for the remaining vNICs (iscsi-a and iscsi-b).

You will map iSCSI-a to Fabric Interconnect A, and you will use the MAC address pool created previously. It can also use Ethernet network control, Ethernet QoS, and Ethernet adapter policies. It uses a different network group policy. You will map iSCSI-b to Fabric Interconnect B, and you can create a MAC address pool dedicated to Fabric Interconnect B. It also needs a different network group policy. It can use existing Ethernet network control, Ethernet adapter policies.

The MAC pool and network group policies used for subsequent vNICS are discussed in the following steps.

1. When adding the iscsi-a vNIC, click Select Policy under Ethernet Network Group Policy and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **iSCSI-A-NetGrp-Pol**).

CONFIGURE > Create UCS Server F	Profile > Create LAN Connectivity Policy > Create Ethern	et Network Group		۵		₽	Q		Paniraja Koppa 🚨
─ Progress			Step 1						
1 General		ξO <sub>k</sub>	General Add a name, descripti	tion and tag fo	or the policy				
2 Policy Details		• చా							
		Organization * FlexPod							
		Name *							
		iSCSI-A-NetGrp-Pe	ol						
		Set Tags							
		Description							
						= 1024			

2. Enter the allowed VLANs (for example, **3010**) and the native VLAN ID (for example, 3010).

CONFIGURE > Create UCS Server P	Profile > Create LAN	N Connectivity Policy	> Create Ethernet M	Network Group		¢	\$	Q		Paniraja Koppa 🚨
─ Progress				~~~	Step 2					
1 General					Add policy details	ils <sup>5</sup>				
2 Policy Details										_
		<ul> <li>This policy is ap</li> </ul>	plicable only for UCS	Servers (FI-Attache	d)					
		VLAN Settings								
		Allowed VLANs 3010				Native VLAN 3010			) © 1 - 4093	- - 3

- 3. Click Create to finish configuring the Ethernet network group policy.
- When adding the iscsi-b vNIC, click Select Pool under MAC Address Pool and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, MAC-Pool-B).

CONFIGURE > Create UCS Server Profile > Create LAN Connectivity Policy > Create MAC F	Pool		¢		ø	Q,		Paniraja Koppa 🚨
	~~~~~	Step 1						
General	Ē	General Pool represents a c can be allocated to	ollection of N VNICs of a se	/IAC addres erver profile	ses that			
2 Pool Details								
	Organization *							
	FlexPod							
	Name *							
	MAC-Pool-B							
	Set Tags							
	Description							
					<= 1024			

5. Note that the same prefix, 00:25:B5, is used for MAC Pool B, but 0B in the second-to-the-last octet signifies the these MAC addresses are assigned to vNICs associated with Fabric B.

CONFIGURE > Create UCS Server Profile > Create	LAN Connectivity Policy > Create MAC Pool	¢ ⊠ ≮ ¢,	හා විසින් වේ විසාහන් වේ සංවේශය වේ වේ සංවේ සංවේ සංවේ සංවේ සංවේ සංවේ සංව
☑ Progress	Step		
(1) General	Colle	bl Details ction of MAC Blocks.	
2 Pool Details			
	MAC Blocks		
	From *	Size *	
	00:25:B5:A4:0B:00	<u>©</u> <u>64</u>	<u> </u>
			1 - 1000

- 6. Click Create to finish creating the MAC address pool.
- 7. Click Select Policy under Ethernet Network Group Policy and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **iSCSI-B-NetGrp-Pol**).

CONFIGURE > Create UCS Server P	Profile > Create LAN Connectivity Policy > Create Ethernet Netv	work Group		Q		₽	o,	ි Paniraja Koppa 🕰	
─ Progress		~~~	Step 1						
1 General	2		General Add a name, descripti	ion and tag f	for the polic				l
2 Policy Details									
	Orga	anization *							
	Flex	xPod							
	Nam								
	iSCS	SI-B-NetGrp-Pol	I						
	Set	Tags							
	Dee	orintion							
	Des	scription							

8. Enter the allowed VLANs (for example, 3020) and the native VLAN ID (for example, 3020).

CONFIGURE > Create UCS Server Pr	rofile > Create LAI	N Connectivity Policy	> Create Ethernet	Network Group		Q	₽	Q Q		Paniraja Koppa 🙎
─ Progress					Step 2					
1 General					Policy Detail Add policy details	s				
2 Policy Details										_
		This policy is applicable	blicable only for UC	S Servers (FI-Attache	d)					
		VLAN Settings								
		Allowed VLANs 3020			۸ 	lative VLAN 1020			) () 1 - 409	<u>)</u> 13

9. Click Create to finish configuring the Ethernet network group policy.

### Add iSCSI boot policy to iSCSI vNICs

iSCSI vNICs need an attached iSCSI boot policy if you are planning to use iSCSI boot from SAN. If iSCSI boot from SAN is not required and you are planning to use iSCSI storage in the operating system, then you do not need to attach the iSCSI boot policies to iSCSI vNICs. In the validation presented here, two targets-primary and secondary-are mapped per vNIC, and hence you will have four paths to the boot LUN.

Follow the steps here to create and attach iSCSI boot policies to iSCSI vNICs.

 When adding the iscsi-a vNIC, click Select Policy under iSCSI Boot and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, iSCSI-A-Boot-Pol).

CONFIGURE > Create UCS Server P	rofile > Create LAN Connectivity Policy >	Create iSCSI Boot	٩		₽	٩		Paniraja Koppa 🗕
⊆ Progress		Step 1						
General 2 Policy Details		Add a name	e, description and tag	) for the poli				
		Organization *						
		FlexPod						
		Name *						
		iSCSI-A-Boot-Pol						
		Set Tags						
		Description			<= 1024			

2. For Policy Details > Configuration, select Static.

CONFIGURE > Create UCS Server Profile > Create LAN	Connectivity Policy > Create iSCSI Boot		Q	¢‡	q		Paniraja Koppa 🙎
Œ Progress	~~~~	Step 2 Policy Details					
1 General		Add policy details					
2 Policy Details							
	This policy is applicable only for UCS Servers (FI-Atta Intersection of the server	ched)					
	Configuration						
	Auto Static						
	Primary Target *						
	Secondary Target Select Policy 🗐						
	iSCSI Adapter						
	Select Policy 🗐						
	Authentification						
	CHAP ©						
	☐ Mutual CHAP ⊙						
	Initiator IP Source						
	Pool DHCP	Static					
	IP Pool *						
	Select Pool E						

3. Click Select Policy under Primary Target and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **FP-iSCSI-A-Primary-Target**).

CONFIGURE > Create UCS Server Pr	rofile > Create LAN Connectivity Policy	> Create iSCSI Boot > Create iSCSI	Static Target	) D	<b>F</b> 3	Q		Paniraja Koppa 🚨
		~~~~	Step 1					
1 General			General Add a name, description a	and tag for the po	olicy.			
2 Policy Details								
		Organization *						
		FlexPod						
		Name *						
		FP-iSCSI-A-Prima	ry-Target					
		Set Tags						
		Description						
		Primary target for	iscsi-a interface					
					<= 1024			

### 4. Enter the target configuration for the primary target.

CONFIGURE > Create UCS Server Profile > Cre	eate LAN Connectivity Policy > Create iSCSI Boot > Create iSCSI Static Target 🗘 🔀 🥵 📀 Pa	aniraja Koppa 🚨
₢ Progress	Step 2 Policy Details	
(1) General	Add policy details	
2 Policy Details		
	This policy is applicable only for UCS Servers (FI-Attached)	
	Configuration	
	Target Name * IP Address * Port *	
	iqn.1992-08.com.netapp:sn.e461ee9 <sup>©</sup> <u>192.168.31.101</u> <u>3260</u> <u>3260</u> <u>1 csrcs</u>	
	0 C O	

- 5. Click Create.
- 6. Repeat the steps 3, 4, and 5 for the secondary target, naming the target, for example, **FP-iSCSI-A-Secondary-Target**.

CONFIGURE > Create UCS Server Pr	Profile > Create LAN Connectivity Policy > Create iSCSI Boot > Create iSCSI Static Target 🗘 🔀 🖓 🖓 Panir	aja Koppa 🖉
─ Progress	Step 2	
(1) General	Policy Details Add policy details	
2 Policy Details		
	This policy is applicable only for UCS Servers (FI-Attached)	
	Configuration	
	Target Name * IP Address * Port *	
	ign.1992-08.com.netapp:sn.e461ee9 $^{\odot}$ 192.168.31.102 $^{\odot}$ 3260 $^{\bigcirc}$ $^{\odot}$	
	Lun ID*	
	0 D O	

7. Click Select Policy under iSCSI Adapter and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **FP-iSCSI-adapter-Pol**).

CONFIGURE > Create UCS Server Profile > Create LAN Connecti	vity Policy > Create iSCSI Boot > Create iSCSI Adapter	다 🖸 📢 🔍 🕄 🕜 Paniraja Koppa 요
⊂ Progress	Step 1	
General	General Add a name, descri	ription and tag for the policy.
2 Policy Details		
	Organization *	
	Flex Pod	
	Name *	
	FP-iSCSI-adapter-Pol	
	Set Tags	
	Description	<u>^</u>
		<= 1024

8. This document retains the default configuration. Change the configuration if required.

CONFIGURE > Create UCS Server P	Profile > Create LAN Connectivity Policy > Create iSCSI Boo	ot > Create iSCS	Adapter	Q [7]	<b>F</b> 3	¢ (۵	3 0	Paniraja Koppa 🗕
⊆ Progress		~~~	Step 2					
(1) General			Policy Details Add policy details					
2 Policy Details								
	This policy is applicable only for U	ICS Servers (FI-Atta	ched)					
	Configuration							
	TCP Connection Timeout * 15	DHCF <u>0</u> 0 0 - 255	Timeout *	<u>)</u> © 60 - 300	LUN Busy Retry 15		<u>ලි</u> ල 0 - 60	

9. Click Create.

- 10. Configure authentication as CHAP or Mutual CHAP.
- 11. Make sure that Pool is selected under Initiator IP Source.
- 12. Click Select Pool under IP Pool and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **iSCSI-IP-Pool-A**).

CONFIGURE > Create UCS Server Profile > Create LAN Connectivity Policy	> Create ISCSI Boot > Create IP Pool	¢ ⊻ ¢	Q,	Paniraja Koppa 🚨
至 Progress	Step 1			
General	General Pool represents a c addresses that can	collection of IPv4 and/or IPv6		
2 IPv4 Pool Details	configuration entitie	es like server profiles.		
	Organization *			
3 IPv6 Pool Details	FlexPod			
	Name *			
	iSCSI-IP-Pool-A			
	Set Tags			
	December			
		<= 1024		

13. Select Configure IPv4 Pool and provide the information to define a pool for iSCSI IP address assignment.

CONFIGURE > Create UCS Server Profile > Create LA	AN Connectivity Policy > Create iSCSI Boot > Create IP Po	ool 🗘 🗹 🛱 🤇	பல் கார்கள் கிறைக பிரைகள் கிறைகள் பிரைகள் பிரைகள் பிரைகள் பிரைகள் பிரைகள் பிரிகள் பிகளை பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பிகள் பி பிகள் பி பி பி பி பி பி பி பி பி பி பி பி பி
☑ Progress		<sub>Step 2</sub> IPv4 Pool Details	
(1) General		Network interface configuration data for IPv4 interfaces.	
2 IPv4 Pool Details			
3 IPv6 Pool Details	Configure IPv4 Pool		
	Configuration		
	Netmask 255.255.255.0	Gateway 0 192.168.31.254	o
	Primary DNS	© Secondary DNS	
	IP Blocks		
	From *	Size *	
	192.168.31.201	32	<u> </u>
			1 - 234

- 14. Click Next.
- 15. Deselect Configure IPv6 Pool.
- 16. Click Create to finish configuring the IP address pool.

CONFIGURE > Create UCS Server Profile > Create	LAN Connectivity Policy > Create ISCSI Boot 🗘 🔀 🧭 Paniraja Koppa 🔔
<ul> <li>Progress</li> <li>General</li> <li>Policy Details</li> </ul>	Step 2 Policy Details Add policy details
	This policy is applicable only for UCS Servers (FI-Attached) Configuration
	Auto Static
	Selected Policy: FP-ISCSI-A-Primary-Target
	iSCSI Adapter இ Selected Policy: FP-ISCSI-adapter-Pol @   × Authentification
	CHAP 0 Mutuel CHAP 0
	Initiator IP Source Pool DHCP Static IP Pool *
	Selected Pool: iSCSI-IP-Pool-A

- 17. Click Create to complete creating the iSCSI boot policy for the iscsi-a vNIC.
- 18. For iscsi-b, create another iSCSI boot policy (for example, **iSCSI-B-Boot-Pol**) with a different primary target, secondary target, and IP address pool. You can use the iSCSI adapter policy created earlier.

● This policy is applicable only for UCS Servers (FI-Attached)         Configuration         Auto       Static         Primary Target *            Selected Policy: FP-ISCSI-B-Primary-Target			Step 2 Policy Details Add policy details	
Configuration         Auto       Static         Primary Target *       Selected Policy: FP-ISCSI-B-Primary-Target @   ×         Secondary Target       @   ×         Selected Policy: FP-ISCSI-B-Secondary-Target @   ×       Selected Policy: FP-ISCSI-B-Secondary-Target @   ×         SCSI Adapter       @   ×         Selected Policy: FP-ISCSI-adapter-Pol @   ×       Authentification         CHAP 0	This policy is applicable	only for UCS Servers (FI-Atta	ched)	
Auto       Static         Primary Target * <ul> <li>                 Selected Policy: FP-ISCSI-B-Primary-Target ①   ×</li> </ul> Secondary Target                    Selected Policy: FP-ISCSI-B-Secondary-Target ①   ×                        ScSI Adapter	Configuration			
Auto       Static         Primary Target * <ul> <li>Selected Policy: FP-ISCSI-B-Primary-Target</li> <li>Selected Policy: FP-ISCSI-B-Secondary-Target</li> <li>Selected Policy: FP-ISCSI-B-Secondary-Target</li> <li>Selected Policy: FP-ISCSI-adapter-Pol</li> <li>X</li> </ul> SCSI Adapter <ul> <li>Selected Policy: FP-ISCSI-adapter-Pol</li> <li>X</li> </ul> Authentification <ul> <li>CHAP ©</li> <li>Mutual CHAP ©</li> </ul> Initiator IP Source <ul> <li>DHCP</li> <li>Static</li> </ul> IP Pool * <ul> <li>Selected Pool: ISCSI-IP-Pool-B</li> <li>X = X</li> </ul>				
Primary Target *                 Selecited Policy: FP-ISCSI-B-Primary-Target	Auto	Static		
Gelected Policy: FP-ISCSI-B-Primary-Target	Primary Target *			
Secondary Target	Selected Policy: FP-ISC	SI-B-Primary-Target 💿		
Selected Policy: FP-ISCSI-B-Secondary-Target	Secondary Target			
iSCSI Adapter  Selected Policy: FP4SCSI-adapter-Pol   Authentification  CHAP ○  Initiator IP Source  Pod DHCP Static  IP Pool *  Selected Pool: ISCSI-IP-Pool-B	Selected Policy: FP-ISC	CSI-B-Secondary-Target 👁		
Belected Policy: FP-ISCSI-adapter-Pol	iSCSI Adapter			
Authentification CHAP © Mutual CHAP © Initiator IP Source DHCP Static IP Pool* Selected Pool: iSCSHP-Pool-B ©   ×	Selected Policy: FP-iSC	SI-adapter-Pol 💿   🗙		
CHAP ⊙         Mutual CHAP ⊙         Initiator IP Source         Pool       DHCP         Static         IP Pool *            Selected Pool: ISCSHP-Pool-B ③   ×	Authentification			
Mutual CHAP ⊙         Initiator IP Source         Pool       DHCP         Static         IP Pool *            Selected Pool: iSCSHP-Pool-B ③   ×				
Initiator IP Source Pool Pool DHCP Static IP Pool *	Mutual CHAP o			
Pool DHCP Static  IP Pool *	Initiator IP Source			
IP Pool * 創 Selected Pool: iSCSHIP-Pool-8 ③   ×	Pool	DHCP	Static	
II Selected Pool: iSCSI-IP-Pool-B  ◎   ×	IP Pool *			
	Selected Pool: iSCSI-IF	-Pool-B		

#### Add the IQN pool for LAN connectivity policy

The last step is to add an IQN pool. Note that you add an IQN pool only if you are using an iSCSI SAN. If you are using only Fibre Channel SANs, you do not need to create and map IQN policy.

Follow these steps to create and attach an IQN pool to the LAN connectivity policy.

1. Click Select Pool under IQN Pool and click Create New in the pane on the right. Select the organization (for example, FlexPod) and provide a name (for example, **FlexPod-IQN-Pool**).

CONFIGURE > Create UCS Server Profile > Create LAN Connectivity Policy > Create Iqnpo	ool:Pool	Q		¶2	Q		Paniraja Koppa 🗕
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Step 1					
Ceneral General	Ē	General Pool represents a collection Names (IONs) for use as init	of iSCSI Qualit	fied s by iSCSI			
Pool Details		vNICs.		0000			
	Organization *						
	FlexPod						
	Name *						
	FlexPod-IQN-Pool						
	Sat Tago						
	Description						
				<= 1024			

 Provide the information to define a pool for iSCSI IP address assignment. For FlexPod, the recommended approach is to use iqn.2010-11.com.flexpod as the prefix and ucs-host as the suffix. Also, if multiple Cisco UCS domains are in use, a more specific suffix, such as AA04-6454-host, can also be used.

CONFIGURE > Create UCS Server Profile > Create LAN C	onnectivity Policy > Create Iqnpool:Pool		<del>0</del>		¢ \$		Paniraja Koppa 🚨
☑ Progress	~~~~	Step 2					
1 General		Collection of IQN Blocks					
2 Pool Details							
	Configuration						
	Prefix *						
	iqn.2010-11.com.flexpod O						
	IQN Blocks						
	Suffix * F	rom *		Size *			
	ucs-host 0 1	1	0	64	0	<u> </u>	
						1000	

- 3. Click Create.
- 4. Verify that all the vNICs have been added successfully before moving on to create SAN connectivity policy.

CONFIGURE > Create UCS Server Profile >	Create LAN Connectivity Policy	0 0 <b>6</b> 0 0	Paniraja Kop
C Progress	Star Provide Action	ep 2 olicy Details dd policy details	
	IQN		
	None Pool	Static	
	IQN Pool * ∰ Selected Pool: FlexPod-IQN-Pool @   ×		
	vNIC Configuration		
	Manual VNICs Placement	uto vNICs Placement	
	For auto placement option the vNICs will be automatic     more at	cally distributed between adaptors during profile deployment. Learn Help Center	
	Add vHIC		
	Name Slot ID Switch		
	_ mgmt A	Enabled ····	
	iscsi-a A	Disabled	
	iscsi-b B	Disabled	
	û / 🗆		

### Create LAN connectivity policy for Fibre Channel boot

If you are planning to deploy only Fibre Channel SANs and are not planning to use any iSCSI SAN at all, then you do not need to create iSCSI vNICs and map an IQN policy to the LAN connectivity policy. Note that the boot policies also differ for Fibre Channel and iSCSI.

CONFIGURE > Policies > LAN Connectivity > Create				
	ξ <b>ω</b>	Step 2 Policy Details		
Policy Dataile	۲ <mark>۰۰</mark> ۰۰	Add policy details		
Poincy Details	IQN			
	None Pool	Static		
	• This option ensures the IQN name is not associate	ed with the policy		
	vNIC Configuration			
	Manual vNICs Placement	Auto vNICs Placement		
	<ul> <li>For auto placement option the vNICs will be autom more at</li> </ul>	natically distributed between adaptors during	profile deployment. Learn Help Center	
	Add vNIC			
	mgmt A		Enabled	

### Summary of LAN connectivity policies

Table 2 summarizes the LAN connectivity policy for iSCSI used in this validation.

Interface	Placement	Failover	MAC address pool	Network policies	iSCSI boot policy	IQN Pool
mgmt	Fabric Interconnect A	Enabled	MAC-Pool-A	Mgmt-NetGrp-Pol Enable-CDP-LLDP Jumbo-MTU-QoS RHEL-Ether-AdapterPol		
iscsi-a	Fabric Interconnect A	Disabled	MAC-Pool-A	iSCSI-A-NetGrp-Pol Enable-CDP-LLDP Jumbo-MTU-QoS RHEL-Ether-AdapterPol	iSCSI-A- Boot-Pol	FlexPod- IQN-Pool
iscsi-b	Fabric Interconnect B	Disabled	MAC-Pool-B	iSCSI-B-NetGrp-Pol Enable-CDP-LLDP Jumbo-MTU-QoS RHEL-Ether-AdapterPol	iSCSI-B- Boot-Pol	

 Table 2.
 LAN connectivity policy for iSCSI

Table 3 lists details of the iSCSI boot policy associated with the iSCSI interfaces used in this validation.

### Table 3. iSCSI boot policy associated with iSCSI interfaces

iSCSI boot policy	IP address pool	iSCSI targets
iSCSI-A-Boot-Pol	iSCSI-IP-Pool-A	FP-iSCSI-A-Primary-Target FP-iSCSI-A-Secondary-Target
iSCSI-B-Boot-Pol	iSCSI-IP-Pool-B	FP-iSCSI-B-Primary-Target FP-iSCSI-B-Secondary-Target

Table 4 summarizes the LAN connectivity policy when only Fibre Channel is used for this validation.

Table 4.	LAN connectivity policy when only Fibre Channel is used
----------	---------------------------------------------------------

Interface	Placement	Failover	MAC address pool	Network policies
mgmt	Fabric	Enabled	MAC-Pool-A	Mgmt-NetGrp-Pol
	Interconnect A			Enable-CDP-LLDP
				Jumbo-MTU-QoS
				RHEL-Ether-AdapterPol

### Step 6b: Network Connectivity > SAN Connectivity

A SAN connectivity policy determines the network storage resources and the connections between the server and the storage device on the network. This policy enables you to configure the vHBAs that the servers use to communicate with the SAN.

Include SAN connectivity policy only if you have Fibre Channel SAN. This policy is not required if you just have iSCSI SAN.

- 1. Click Select Policy next to SAN Connectivity and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **AA04-6454-SanConn**).

CONFIGURE > Create UCS Server Profile > Create SAN Connectivity Policy	다. 🗹 📢 Q, 🖏 ⑦ Paniraja Koppa 🕰
	Step 1
General	General Add a name, description and tag for the policy.
2 Policy Details	
	Organization *
	Name *
	AA04-6454-SanConn
	Target Platform O
	🕕 UCS Server (Standalone) 💿 UCS Server (Fl-Attached)
	Set rags
	Description
	SAN Connectivity Policy for FlexPod DataCenter
	<= 1024

This deployment uses two vHBAs, as follows:

- vHBA-A: Fabric Interconnect A vHBA for SAN A
- vHBA-B: Fabric Interconnect B vHBA for SAN B
- To keep the vHBA placement simple, select Auto vHBAs Placement. Make sure that Pool is selected for WWNN Address.

				رې دې	Step 2 <b>Policy Detail</b> Add policy details	s				
	Manual	/HBAs Placemen	t	į	Auto vHBAs Placeme	ent				
WW	NN Address									
	Pool		Static							
WWNN A	Address Poo	ement option the	vHBAs will be	automati	cally distributed betw	veen adaptor	s during profile de	ployment, Learn	n more at <u>Help C</u>	enter
Ad	d vHBA									
										£33
	Name					Switch ID				

### Create the WWNN address pool

The WWNN address pools have not been defined yet, so you will now create a new WWNN address pool.

- 1. Click Select Pool under WWNN Address Pool and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **WWNN-Pool**).

CONFIGURE > Create UCS Server Profile > Create SAN Connectivity Policy > Create F	Pool Q Q Q	දි 🔅 🧷 Paniraja Koppa 🕰
Œ Progress	Step 1	
General Pool Details	General Pool represents a collection of WWN addresses that can be allocated to VHBAs of a Server Profile	
	Organization *	
	FlexPod ~	
	Name * WWNN-Pool	
	Sat Tans	
	Description <= 1024	

3. Click Next.

 Provide the starting WWNN block address. The recommended prefix for WWNN addresses is 20:00:00:25:B5:xx:xx:xx. As a best practice, in FlexPod some additional information is always coded into the WWNN address pool for ease of troubleshooting. For example, in the address 20:00:25:B5:A4:00:00, A4 is the rack ID.

CONFIGURE > Create UCS Server Profile > Create SAN Cor	nectivity Policy > Create FC Pool		\$	ø		Paniraja Koppa 🚨
⊆ Progress	~~~~	Step 2				
1 General 2 Pool Details		Pool Details Block of WWNN Identif	fiers.			
	WWNN Blocks					
	From *					
	20:00:00:25:B5:A4:00:00	© 32			Ĵ 0	

5. Click Create to finish creating the WWNN address pool.

#### Create the vHBA for SAN A

Now create a vHBA for SAN A.

- 1. Click Add vHBA.
- 2. Provide the name of the vNIC (for example, vHBA-A).
- 3. For vHBA Type, choose fc-initiator from the drop-down menu.
- 4. Choose Switch ID A from the drop-down menu.

CONFIGURE > Create UCS Server	Profile > Create SAN Connectivity Policy			0 E	₽3	<b>∿</b> (‡	Paniraja Koppa 🚨
		Add vHBA					
	Name *		vHBA Type				
	VHBA-A					~ 0	
	WWPN Address						
	Pool Static						
	WWPN Address Pool * Select Pool 🗐						
	Placement						
	Switch ID * A	× 0					
	Persistent LUN Bindings						
	Persistent LUN Bindings ()						
	Fibre Channel Network * Select Policy 🗐						

#### Create the WWPN pool for SAN A

The WWPN address pool has not been defined yet, so you will now create a WWPN address pool for Fabric A.

- 1. Click Select Pool under WWPN Address Pool and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **WWPN-Pool-A**).

CONFIGURE > Create UCS Server Profile > Create SAN Connectivity Policy > Create FC Po	р Д	₽ <b>₽</b>	¢ ¢	ල Paniraja Koppa
	Step 1			
General General	General Pool represents a collection can be allocated to VHBAs	n of WWN addresses that of a Server Profile		
2 Pool Details				
	Organization * FlexPod			
	Name *			
	WWPN-Pool-A			
	Set Tags			
	Description			
		<= 1024		

 Provide the starting WWPN block address for SAN A. The recommended prefix for WWPN addresses is 20:00:00:25:B5:xx:xx:xx. As a best practice, in FlexPod some additional information is always coded into the WWPN address pool for ease of troubleshooting. For example, in the address 20:00:00:25:B5:A4:0A:00, A4 is the rack ID and 0A signifies SAN A.

CONFIGURE > Create UCS Server F	Profile > Create SAN Conr	ectivity Policy > Create FC Pool			Q	₽	o,	\$	0	Paniraja Koppa 🙎
₢ Progress			~~~	Step 2						
1 General 2 Pool Details		ſ		Pool Details Block of WWPN Ident	lifiers.					
		WWPN Blocks								
		From * 20:00:00:25:85:A4:0A:00		Size * <u>32</u>		 		<u>()</u> (0) 1 - 1000	+	

- 4. Provide a size of the pool.
- 5. Click Create.

### Create Fibre Channel network policy for SAN A

A Fibre Channel network policy governs the VSAN configuration for the virtual interfaces. VSAN 111 will be used for vHBA-A, and VSAN 112 will be used for vHBA-B.

- 1. Click Select Policy under Fibre Channel Network and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **SAN-A-Network**).

CONFIGURE > Create UCS Server F	Profile > Create SAN Connectivity Policy > Create Fib	re Channel Network	Ç		₽4	<b>с</b>	© ©	Paniraja Koppa 🙎
─ Progress		~~~~	Step 1					
2 Policy Details		Organization * FlexPod	General Add a name, description a	and tag for the p	olicy.			
		SAN-A-Network Set Tags Description			∠ <= 1024			

- 3. For the scope, select UCS Server (FI-Attached).
- 4. Under Default VLAN, provide the VSAN information (for example, 111).

CONFIGURE > Create UCS Server P	rofile > Create SAN Connectivity Policy > Create Fibre Channel Network	ධ 📝 🕫 🔍 🔅 🧿 Paniraja Koppa 🖉
₢ Progress	-7	Step 2
(1) General		Policy Details Add policy details
2 Policy Details		V All Platforms   UCS Server (Standalone)   UCS Server (FLAttachad)
	Fibre Channel Network	
	VSAN ID	
	111	
		1 - 4094

5. Click Create to finish creating the Fibre Channel network policy.

### Create Fibre Channel QoS policy

The Fibre Channel QoS policy assigns a system class to the outgoing traffic for a vHBA. This system class determines the quality of service for the outgoing traffic. The Fibre Channel QoS policy used in this deployment uses default values and will be shared by both vHBA-A and vHBA-B.

- 1. Click Select Policy under Fibre Channel QoS and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **FC-QoS**).

CONFIGURE > Create UCS Server F	Profile > Create SAN Connectivity Policy > Create Fibre Channel QoS	Q []	Ø 0	🕜 🛛 Paniraja Koppa 🚨
─ Progress	-74	Step 1		
General     Policy Details	Ę.	Add a name, description and tag for the policy.		
	Organization FlexPod			
	Name * FC-QoS			
	Set Tags			
	Descriptio		- 1004	
			= 1024	

- 3. For the scope, select UCS Server (FI-Attached).
- 4. Do not change the default values on the Policy Details screen.

CONFIGURE > Create UCS Server F	Profile > Create SAN Connectivity Policy > Create Fibre Channel QoS	ධ 🔽 📢 🔍 😳 Paniraja Koppa 🖉
─ Progress	Step 2	
1 General	Policy De	tails <sub>laifs</sub>
Policy Details		
		All Platforms UCS Server (Standalone) UCS Server (FI-Attached)
	Fibre Channel QoS	
	Rate Limit, Mbps	Maximum Data Field Size, Bytes
	o	<u>2112</u>
	0 - 100000	
	Burst	Priority
	<u>1024</u>	FC ~ 0
	1024 - 1000000	

5. Click Create to finish creating the Fibre Channel QoS policy.

### **Create Fibre Channel adapter policy**

A Fibre Channel adapter policy governs the host-side behavior of the adapter, including the way that the adapter handles traffic. This validation uses the default values for the adapter policy, and the policy will be shared by both vHBA-A and vHBA-B.

- 1. Click Select Policy under Fibre Channel Adapter and then, in the pane on the right, click Create New.
- 2. Choose the organization from the drop-down menu (for example, FlexPod) and provide a name for the policy (for example, **FC-Adapter**).
- 3. Choose Linux for the default configuration for the Fibre Channel adapter.

CONFIGURE > Create UCS Server Profile > Create SAN Connectivity Policy > Create Fibre (	Channel Adapter	¢	ß	₽;	q	æ	0	Paniraja Koppa 🚨	
⊆ Progress	~~~	Step 1	Default Configuration						
	20%	General		Policies 9					
General	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Add a name, description an	nd tag for the p						
2 Policy Details				WindowsBoot					
	FlexPod			Solaris					
				FCNVMeTarget					
	FC-Adapter			FCNVM	lelnitiator				
				🗐 Target					
	Set Tags			🗐 Initiator					
			🗐 VMWare						
	Description		- 🗐 Windows						
	Fibre Channel Adap								

- 4. For the scope, select UCS Server (FI-Attached).
- 5. Do not change the default values on the Policy Details screen.

CONFIGURE > Create UCS Server Profile > Crea	ate SAN Connectivity Policy > Create Fibre Channel Adapter		Q 🗹 🗗	ට <b>ද</b> දිමු ⑦ Pan	niraja Koppa 🚨
⊂ Progress	~~~~_	Step 2	toilo		
1 General		Add policy det	ails		
2 Policy Details			All Platforms   UCS Server (Standalone)	UCS Server (FI-Attached)	
	Error Recovery				
	FCP Error Recovery O				
	Port Down Timeout, ms		Link Down Timeout, ms		
	30000	0	30000	<u>)</u> o	
		0 - 240000		0 - 240000	
	I/O Retry Timeout, Seconds		Port Down IO Retry, ms		
		0	30	() ©	
		1 - 59		0 - 255	
	Error Detection				
	Error Detection Timeout				
	2000	<u> </u>			
		1000 - 100000			
	Resource Allocation				
	Resource Allocation Timeout				
	10000	<u> </u>			
		5000 - 100000			
	Flogi				
	Flogi Retries		Flogi Timeout, ms		
	8	0 0	4000	) o	
		> 0		1000 - 255000	
	Plogi				
	Plogi Retries		Plogi Timeout, ms		
	8	0 ()	20000	) o	

- 6. Click Create to finish creating the Fibre Channel adapter policy.
- 7. Click Add to create vHBA-A.

### Create the vHBA for SAN B

Repeat the preceding steps to add vHBA-B for SAN B.

- Use switch ID B for this vHBA. The WWPN pool and Fibre Channel network policy (VSAN) for this vHBA are unique, but the Fibre Channel QoS and Fibre Channel adapter policies defined previously for vHBA-A will be reused.
- 2. Note the WWPN-Pool-B information used for this validation.

CONFIGURE > Create UCS Server Profile > Create SAN Connectivity Policy > Create FC Po	ol		¢		₽	Q,		Paniraja Koppa 🚨
존 Progress		Step 1						
General	Ē	General Pool represents a co	llection of W	WN address	es that			
2 Pool Details	Organization *							
	FlexPod							
	Name *							
	WWPN-Pool-B							
	Set Tags							
	Description							
					<= 1024			

The recommended prefix for WWPN addresses is 20:00:00:25:B5:xx:xx: As a best practice, in FlexPod some additional information is always coded into the WWPN address pool for ease of troubleshooting. For example, in the address 20:00:00:25:B5:A4:0B:00, A4 is the rack ID and 0B signifies SAN B.

CONFIGURE > Create UCS Server P	ofile > Create SAN Connectivity Policy > Create FC Pool	ධ 🖸 📢 🔍 🐯 ⊘ Paniraja Koppa 🖉	
⊆ Progress	Step 2		
1 General 2 Pool Details	Pool Block	Details of WWPN Identifiers.	
	WWPN Blocks		
	From * 20:00:00:25:B5:A4:0B:00	<u>○</u> <u>32</u> <u>C</u> ○ + 1 - 1000	

3. Note the Fibre Channel network policy for SAN B used in this validation.

CONFIGURE > Create UCS Server F	Profile > Create SAN Connectivity Policy > Create Fibre	Channel Network		Q		ø		Paniraja Koppa 🖉
E Progress		~~~	Step 1					
General		₹ <b>Ç</b>	General Add a name, description	ion and tag	for the polic			
2 Policy Details								
		Organization *						
		FlexPod						
		Name *						
		SAN-R-Network						
		Set Tags						
		Description						
						<= 1024		

4. For the scope, select UCS Server (FI-Attached) and enter the VSAN information (for example, 112) under Default VLAN.



After all the configuration is completed, vHBA-B should look like the following screen:

CONFIGURE > Create UCS Server P	rofile > Create SAN Connectivity Policy			۵	ſ	₽	Q,	٢	0	Paniraja Koppa 🗕
	Ę.	Add vHBA								
	Name * vHBA-B		vHBA Type fc-initiator					<u>0</u>		
	WWPN Address									
	Pool Static									
	WWPN Address Pool * ∰ Selected Pool: WWPN-Pool-B									
	Placement									
	Switch ID * B									
	Persistent LUN Bindings									
	Persistent LUN Bindings ①									
	Fibre Channel Network *									
	Fibre Channel QoS ★									
	Fibre Channel Adapter *									

SAN connectivity policy will be listed as shown on the following screen:

	Add p	olicy details	
	Manual vHBAs Placement Auto vH	IBAs Placement	
ww	NN Address		
	Pool Static		
Sele	cted Pool: WWNN-Pool 💿   X		
Selei G F	cted Pool: WWNN-Pool $   \times$ for auto placement option the vHBAs will be automatically dis	stributed between adaptors during profile deploymen	t. Learn more at Help Center
Selec F	cted Pool: WWNN-Pool I X	stributed between adaptors during profile deploymen	t. Learn more at Help Center
C F Ad	cted Pool: WWNN-Pool I ×	stributed between adaptors during profile deploymen	t. Learn more at Help Center
Seler C F Ad	cted Pool: WWNN-Pool I ×	stributed between adaptors during profile deploymen Switch ID B	t. Learn more at Help Center
C F	cted Pool: WWNN-Pool I ×	stributed between adaptors during profile deploymen Switch ID B A	t. Learn more at Help Center

5. After adding all the vNICs and vHBAs, verify their placement by expanding the vNICs and vHBAs Placement option.



5. Click Next.

### Step 7: Summary

On the summary screen, verify which policies are mapped to various settings and the status of the server profile. The server profile has not been deployed yet, so the status will be Not Deployed.

CONFIGURE > Create UCS Server Profile			Q	₽ \$		Paniraja Koppa 🔔
─ Progress			Step 7			
1 General		) 	Verify details of the profile and t errors and deploy.	the policies, resolve		
2 Server Assignment						_
3 Compute Configuration	General					
	Organization	FlexPod	Status	🔺 Not Depl	oyed	
Management Configuration	Name	FlexPod-RHEL-Host-1	Management IP			
5 Storage Configuration	Assigned Server					
I I I I I I I I I I I I I I I I I I I	Target Platform	UCS Server (FI-Attached)				
6 Network Configuration						
Summary	Description Server Profile for RHEL	host-1				
	Compute Configuration	Management Configuration	Storage Configuration	Network Configuration		
	BIOS				AA04-6454-BiosPol	1
	Boot Order				AA04-6454-FC-BootPol	1

# **Deploy the server profile**

After verifying the settings on the server profile Summary screen, deploy the server profile.

Click Deploy and then Deploy again to deploy the server profile. You would see a task in progress in the topright corner. You can click the task icon to view the details of the task in progress.

≡	cisco Intersight	CONFIGURE > Server Profiles > FlexPod-RHE	L-Host-1	₽ 01 ¢	
000		General Server Inventory Identifiers Con			Requests All Active Completed ×
Ŵ	OPERATE	Details	Configuration		Deploy Server Profile     In Progress
×	CONFIGURE	Status O Validating		All	
	Orchestration	Name FlexPod-RHEL-Host-1	BIOS		
	Profiles	Target Platform UCS Server (FI-Attached)	Boot Order		
	Templates	Server AA04-6454-1-1 Template Name	IMC Access Policy		
		Last Update a few seconds ago	LAN Connectivity		
			Local User		
٩	ADMIN	Server Profile for RHEL host-1	SAN Connectivity		
		Organization FlexPod			
		Tags Set			

After few minutes, you should see that the server profile is deployed.

Requests > Deploy Server Profile			Q 🖸	<b>\$</b> 3	ଦ୍ ଞ		Paniraja Koppa 🚨
Details		Execution Flow					
Status		Inventory Server Configuration					
Name         Deplo           ID         60a80e15696	oy Server Profile 6f6e2d30fb6f1e	<ul> <li>Deploy SAN Connectivity Policy on Fabric Interconnect</li> </ul>					
Target Type	Blade Server	Opploy Boot Order Policy					
Target Name		Deploy I AN Connectivity Policy on Fabric Interconnect					2021 12:47 PM
Source Type	Server Profile						
Source Name FlexPo	od-RHEL-Host-1	<ul> <li>Deploy SAN Connectivity Policy</li> </ul>					
Initiator pkoppa@cisco.com Start Time May 21, 2021 12:46 PM	ppa@cisco.com , 2021 12:46 PM	⊘ Deploy LAN Connectivity Policy					
End Time May 21,	, 2021 12:47 PM	⊘ Deploy BIOS Policy					
Duration	1 m 5 s	⊘ Deploy the User Policy					
Organizations	FlexPod	⊘ Deploy the Access Policy					
		⊘ Deploy IMC Access VLAN on Fabric Interconnect					
		⊘ Validate LAN Connectivity Policy for Fabric Interconnect					
		Validate SAN Connectivity Policy     Completed					
		Validate BIOS Policy     Completed					
		⊘ Validate User Policy				May 21,	2021 12:46 PM

### Verify LAN, SAN, and IQN addresses

After the server profile has been deployed successfully, gather the information about the MAC addresses assigned to vNICs and the WWPN addresses assigned to vHBAs by following these steps:

- 1. Log in to Cisco Intersight portal.
- 2. Go to CONFIGURE > Profiles and select the server profile you just deployed.
- 3. In the main window, click LAN Connectivity.

	dialli Intersight	CONFIGURE > Server Profiles > FlexPod-RH	IEL-Host-1	
		General Server Inventory Identifiers Co		Actions 🗸
	OPERATE ~	Details	Configuration	
×	CONFIGURE ^	Status 🥥 OK		All Compute Management Network Storage
	Orchestration	Name FlexPod-RHEL-Host-1	BIOS	AA04-6454-BiosPol 🗐
	Profiles	Target Platform UCS Server (FI-Attached)	Boot Order	AA04-6454-FC-BootPol 📶
	Templates	Server AR04-0454-1-1 Template Name	IMC Access Policy	AA04-6454-IMCPol 🗐
		Last Update May 21, 2021 12:47 PM	LAN Connectivity	AA04-6454-iSCSI-LanConn 🗐
		Description	Local User	AA04-6454-LocalUser-Pol f
	ADMIN ~	Server Profile for RHEL host-1	SAN Connectivity	AA04-6454-SanConn 🏢
		Organization FlexPod		
		Tags Set		

4. In the pane on the right, each NIC is listed along with the assigned MAC address. This information is useful for identifying the management vNICs for installing Red Hat Enterprise Linux on the server and setting up the initial management access.

CONFIGURE > S	Server Profiles > FlexPod-RHEI	L-Host-1				Q		₽				Paniraja Koppa 🖉	
General Server	General Server Inventory Identifiers Connectivity												
Details		Configuration							LAN Conne	ctivity Details			
Status	⊘ ок		All	Compute	Management	Network	Storage		General				
Name	FlexPod-RHEL-Host-1	BIOS				AA04-6454	4-BiosPol 📋		Name		AA04-	6454-iSCSI-LanConn	
Target Platform	UCS Server (FI-Attached)	Boot Order				AA04-6454-FC	C-BootPol 🗐		Organizatio			FlexPod	
Server		IMC Access Policy				AA04-645	4-IMCPol 🗐		Description				
Template Name	May 21, 2021 12-47 PM								LAN Conne	ctivity policy	for iSCSI SA	'N	
	may 21, 2021 12.47 1 m	LAN Connectivity			AA0	4-6454-iSCSI-	-LanConn 📋		Policy Detai				
Description Server Profile for RH	IFL host-1	Local User			AA	04-6454-Loca	ilUser-Pol 📋		IQN Allocati	on Type		Pool	
		SAN Connectivity				AA04-6454-	-SanConn 🗐		IQN Pool			FlexPod-IQN-Pool	
Organization									IQN Identifie				
Tags									Placement I	Mode	Au	to vNICs Placement	
									Eth Ife 3				
									iscsi-a				
									mgmt				
									Name			mgmt	
									MAC Add	iress Pool		MAC-Pool-A	
									Pool MA	C Address		00:25:B5:A4:0A:0B	
									Failover			On	
									Placeme	nt			
									Slot ID			MLOM	
									Uplink Po	ort		0	
									PCI Link				
									Switch IE				
									Туре				
									PCI Orde				

5. Click SAN Connectivity to gather the information about the WWPN address assigned to vHBA-A and vHBA-B. This information is required to set up Cisco MDS zoning and to map boot LUNs on NetApp.

CONFIGURE > Server Profiles > FlexPod-RHEL-Host-1							ø			Paniraja Koppa &	
General Server Inventory Identifiers Connectivity											
Details		Configuration							SAN Connec	tivity Details	
Status	⊘ ок		All	Compute	Management	Network	Storage		General		
Name FlexPoo	d-RHEL-Host-1	BIOS				AA04-6454	4-BiosPol 🗐		Name		AA04-6454-SanConn
Target Platform UCS Server	r (FI-Attached)	Boot Order				AA04-6454-FC	-BootPol 🗐		Organizatior		FlexPod
Server A		IMC Access Policy				AA04-645			Description		
Template Name	2021 12-47 PM								SAN Connec	tivity Policy fo	r FlexPod DataCenter
	2021 12. <del>4</del> 7 TW	LAN Connectivity			AA0	14-6454-iSCSI-	LanConn 📋		Policy Detail		
Description Server Profile for RHFL bost-1		Local User			AA	04-6454-Loca	lUser-Pol 📋		Placement N	/lode	Auto vHBAs Placement
		SAN Connectivity				AA04-6454-	SanConn 🗐		WWNN Addr	ess Pool	WWNN-Pool
Organization									E-14- 0		
Tags	Set								FC Its 2		
No Taos									vHBA-A		
									Namo		VHRA-A
									WWPN A	dress Pool	WW/PN-Pool-4
									Pool WWI	PN	20:00:00:25:B5:A4:0A:01
									Placemer		
									Slot ID	n.	MLOM
									Switch ID		
									Uplink Po	rt	0
									PCI Order		
									Persisten	t LUN Bindings	No
									Fibre Cha Policy	nnel Network	
									Fibre Cha Policy	nnel QoS	

- Choose CONFIGURE > Pools and select the IQN address pool you created (for example, FlexPod-IQN-Pool).
- 7. Navigate to the Usage tab and note the IQN address for the server profile FlexPod-RHEL-Host-1.

≡ <sup>illulli</sup> Intersight	CONFIGURE > Pools > FlexPod-IQN-Pool	ධ 🗹 🕫 Q, (ඊ) ⊙ Paniraja Koppa යු
		Actions 🗸
📦 OPERATE 🗸 🗸	Details	Configuration & Usage
X CONFIGURE	Name FlexPod-IQN-Pool	Configuration Usage
	Type IQN	
Orchestration		QAdd Filter         ☐ Export         1 items found         10 v         per page         反         1         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○         ○
Profiles		IQN Address Server Profile
Tomplatos	Available 63	
remplates	Last Update May 21, 2021 12:47 PM	Ign 2010-11.com.flexpod.ucs-host.5 FlexPod.RHELHost-1
		K ( 1 of 1 ) 저
Pools	Description -	
_		
역 ADMIN ~		
	Tags Set	

Table 5 lists the MAC and IQNaddresses for the server profile FlexPod-RHEL-Host-1 used for iSCSI SAN

 Table 5.
 MAC and IQN addresses for the server profile for iSCSI SAN

Interface	MAC address	IQN address
mgmt	00:25:B5:A4:0A:0B	
iscsi-a	00:25:B5:A4:0A:0A	
iscsi-b	00:25:B5:A4:0B:04	Iqn.2010-11.com.tiexpoa:ucs-host:5

Table 6 lists the MAC and WWPN addresses for the server profile used for iSCSI SAN

Table 6. MAC and WWPN	addresses for the	e server profile f	for FC SAN
-----------------------	-------------------	--------------------	------------

Interface	MAC address	WWPN address
mgmt	00:25:B5:A4:0A:0B	
vHBA-A		20:00:00:25:B5:A4:0A:01
vHBA-B		20:00:00:25:B5:A4:0B:01

### Configure Cisco MDS zoning

The Cisco MDS configuration for zoning is no different than the typical Cisco MDS configuration in FlexPod. Refer to the Cisco MDS configuration for zoning in the FlexPod deployment guide: <u>https://www.cisco.com/c/en/us/td/docs/unified computing/ucs/UCS CVDs/fp dc ontap 97 ucs 4 vmw vs</u> <u>67\_U3.html#\_Toc46246585.</u>

### Configure NetApp LUNs

The NetApp LUN configuration is no different than the typical NetApp storage configuration in FlexPod. Refer to the NetApp configuration for LUN creation and LUN and igroup mapping in the FlexPod deployment guide:

- <u>https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/fp\_dc\_ontap\_97\_ucs\_4\_v</u> <u>mw\_vs\_67\_U3.html#\_Toc46246513</u>
- <u>https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/fp\_dc\_ontap\_97\_ucs\_4\_v</u> <u>mw\_vs\_67\_U3.html#\_Toc46246596</u>

## Create a template and deploy additional server profiles

You can create a template from a server profile that you can use to derive and deploy multiple server profiles. Any property modification made in the template synchronizes with all the derived profiles. You can deploy these modified profiles individually. This feature facilitates quick and easy configuration because multiple profiles can be created and edited simultaneously.

When a server profile deployment is complete, you can deploy additional server profiles simply by cloning an existing server profile.

To create additional server profiles by cloning, follow these steps:

1. Go to Profile and click the Options icon (...). Choose Create Template.

≡	cisco Intersight	CONFIGURE > Profiles Q 😨 😨 Paniraja Kop	
<u>00o</u>		HyperFlex Cluster Profiles UCS Chassis Profiles UCS Domain Profiles UCS Server Profiles Kubernetes Cluster Profiles Dreate UCS Server Profiles Dreate UCS Server Profiles	rofile
Ŷ			
×	CONFIGURE ^	··· / / 1 items found 14 v per page K < 1 of 1 >>	
	Orchestration	Name     :     Status     :     Target Platform     :     UCS Server Te     Last Upd     :     Server	
	Profiles	FloxPod-RHEL-Host-1         © OK         UCS Server (FrAttached)         May 21, 2021         AA04-6454-1-1	
	Templates	··· // /2 mm Kill Deploy	
	Policies	Unassign Serve	
	Pools	Clone	
-			
Ŵ	ADMIN Y	Delete	
		Attach to Temp	plate
			late

2. Provide a name for the template (for example, FlexPod-RHEL-Host-Template).

CONFIGURE > Create a Template	🗘 🗹 🕫 🖓 Paniraja Koppa 🕰
∠ Progress	Step 1
General	General General
	for the server profile template.
2 Summary	
	Attach UCS Server Profile to Profile Template
	Organization *
	FlexPod ~
	Name*
	Toront Blatform ()
	UCS Server (Standalone) (ICS Server (FI-Attached)
	Set Tags
	Description
	Template created for host to deploy RHEL in FlexPod datacenter
	<u>~</u> <= 1024

- 3. Click Next and click Close.
- 4. Navigate to CONFIGURE > Templates. Select the template you created and choose Derive.
- 5. Choose the server to assign and click Next.
- 6. Choose a name for the profile prefix (for example, FlexPod-RHEL-Host) and a start index (for example, 2).

CONFIGURE > UCS Server Profile Templat	tes > FlexPod-RHEL-Host-Template > Derive	유 🛛 이 1 🕫 🍳 🕄 🕥 Paniraja Koppa <u>유</u>
⊂ Progress       1     General       Datails	Step 2 Details Edit the desc of the profile	cription, tags, and auto-generated names es.
3 Summary	General Organization * FlexPod	Target Platform UCS Server (Fl-Attached) v ©
	Description Template created for host to deploy RHEL in FlexPod datacenter <= 1024 Derive 1	r <u>Set Tags</u> 4
	Profile Name Prefix FlexPod-RHEL-Host-	Start Index for Suffix 2 ③ > 0
	1 Name * FlexPod-RHEL-Host-2	Assig AA04-6454-1-2 

- 7. Click Next and click Derive.
- 8. Repeat steps 4 through 7 for all the servers.

# Install Red Hat Enterprise Linux 8 on a server profile

After a server profile has been deployed successfully, install an operating system by following these steps:

1. Go to OPERATE > Servers and click the server. Click Actions and choose Launch vKVM.

≡ distlis Intersight	OPERATE > Servers > AA04-6454-1-1				
	General Inventory UCS Server Profile HCL				Actions
OPERATE ^	Details	Properties		Events	Power Off
Servers	Health © Healthy	Cisco UCSB-B200-M5	Front View Top Vie	w — Alarms	Power Cycle 15
Chassis Fabric Interconnects Networking Sites HyperFlex Clusters Storage Virtualization	Name AA04-6454-1-1 User Label - Management IP 192.168.160.203 Serial E PID UCSB-8200-MS Vendor Cisco Systems Inc Revision - Asset Tag -			+ Requests 6 + Advisories	Hard Reset Reboot Cisco IMC Shut Down Operating System Turn On Locator Install Operating System Upgrade Firmware
Kubernetes	License Tier Premier Contract Status ONt Covered				Rediscover
🗶 CONFIGURE 🗸 🗸	Management Mode Intersight	aluale			Decommission
ا ADMIN ۲	Chassis AA04-6454-1	()(C)		-	Open TAC Case
	UCS Server Profile FlexPod-RHEL-	Power 🔘 Locator LED 💿	Health Overlay		Set License Tier
	Host-1 UCS Server Profile Sta 🞯 OK	CPIIs D		-	Set Asset Tags
	Firmware Version 4.1(33a)	Threads 0	Adapters 1		Set User Label
	Organizations default IMM FlexPod	CPU Cores 0 CPU Cores Enabled 0 Memory Capacity 192 CPU Concerts (CH2) 198	NIC Interfaces 3 HBA Interfaces 2 0 UUID	-	
	Tags Set	CPO Capacity (GHZ) 128.			

2. On the new KVM tab on the browser, click Virtual Media and choose Activate Virtual Devices.

cisco Intersigi	it AA04	-6454-1-1   vKVM	
File View Macro	os Tools Power	Virtual Media Help	
		Create Image	
		Activate Virtual Devices	

- 3. Click Virtual Media again and choose Map CD/DVD.
- 4. Browse to RHEL8 Update 3 ISO and click Map Drive.
- 5. In the Cisco Intersight portal, select the server and choose Power Cycle from the Actions menu.

OPERATE > Servers > AA04-6454-1-1		Q 2 4		ා Paniraja Koppa වූ
General Inventory UCS Server Profile HCL				Actions
Details	Properties		Events	Power Off
Health O Healthy	Cisco UCSB-B200-M5	Front View Top View	— Alarms	Power Cycle
Name AA04-6454-1-1				Hard Reset
User Label -				Reboot Cisco IMC
Management IP 192.168.160.203			- Ponijoete 12	Shut Down Operating System
Serial LICSP P200 MG			T nequests 12	Turn On Locator
Vendor Cisco Systems Inc			+ Advisories	Install Operating System
Revision -	Antonio antoni	Transmission and the second se		Upgrade Firmware
Asset Tag -				Launch vKVM
License Tier Premier				Rediscover
Contract Status Rot Covered		1		Decommission
Management Mode Intersignt				Open TAC Case
Chassis AA04-6454-1	[	C		Set License Tier
UCS Server Profile FlexPod-RHEL-				Cot Accot Tage
Host-1 UCS Server Profile Status OK				Ort Hose Label
Firmware Version 4.1(33a)	Power O Locator LED	Health Overlay 🌉		Set User Laber
Organizations default	CPI/s 2 ID			
Urganizauons denaun. IMM	Threads 0 Adapters			
FlexPod	CPU Cores 0 NIC Interfac	es 3		
Tags Set	CPU Cores Enabled 0 HBA Interfac	ces 0		
OS RHEL Host FlexPod	Memory Capacity (GiB) 192.0 UUID	CREATE STATISTICS		
	CPU Capacity (GHz) 128.0			

6. Select Set One Time Boot Device and choose ISO (the label previously created for the CD/DVD) from the Boot Device drop-down menu.

ower Cycle S	erver		
Server 'AA04-6454-1-1' will be Power Cycled.			
oot Device kvm-mapped-iso			~ 0
oot Device kvm-mapped-iso iscsi-a		_	~ 0

- 7. Click Power Cycle.
- 8. From the Actions tab, choose Launch vKVM. In the KVM window, you should see the server being power cycled.

If you are performing iSCSI boot, then you should see that the server has successfully discovered the boot LUN over all four paths.

cisco Intersight	AA04-6454-1-1   vKVM
File View Macros Tools	s Power Virtual Media Help
Cisco	VIC iSCSI, Boot Driver Version 5.1(3a)
(C) 20	016 Cisco Systems, Inc.
00:2	25:b5:a4:0a:12 iSCSI NETAPP
00:2	25:b5:a4:0a:12 iSCSI NETAPP
00:2	n ROM installed successfully
Cisco	VIC iSCSI, Boot Driver Version 5.1(3a)
(C) 20	016 Cisco Systems, Inc.
00:2	25:b5:a4:0b:0b iSCSI NETAPP
00:2	25:b5:a4:0b:0b iSCSI NETAPP
00:2	n ROM installed successfully

If you are performing Fibre Channel boot, then all Fibre Channel paths should be visible.



**Note:** This boot firmware execution screen is visible only in the Legacy BIOS mode. If you select uEFI while configuring boot-order policy, these screens will be different.

If you press F6 and enter boot options, you should see all the boot options (Only in Legacy BIOS mode)
 For iSCSI, you should see options similar to those shown here:

Please select boot device:
Cisco vKVM-Mapped vDVD1.24
00:25:b5:a4:0a:12 iSCSI NETAPP
00:25:b5:a4:0a:12 iSCSI NETAPP
00:25:b5:a4:0b:0b iSCSI NETAPP
00:25:b5:a4:0b:0b iSCSI NETAPP
UEFI: Built-in EFI Shell
Enter Setup
↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

For Fibre Channel boot, you should see options similar to those shown here:

Please select boot device:
Cisco vKVM-Mapped vDVD1.24 NETAPP 200100a0985b4a86:000 NETAPP 200300a0985b4a86:000 NETAPP 200200a0985b4a86:000 NETAPP 200400a0985b4a86:000 UEFI: Built-in EFI Shell Enter Setup
↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

10. If you are installing RHEL 8 on a Fibre Channel boot disk, you do not need to pass any parameters to the Anaconda installer program. You can directly choose Install Red Hat Enterprise Linux 8.3 to start the installation.

If you are installing RHEL 8 on an iSCSI boot disk, then you need to append the **ip=ibft** parameter. To connect to an iSCSI target automatically, you must activate a network device to access the target. The recommended way to activate a network is to use the **ip=ibft** boot option.



11. Continue with the OS installation wizard. When you click Installation Destination, you should see the boot LUN under Specialized and Network Disks.

INSTALLATION DESTINATION	RED HAT ENTERPRISE LINUX 8.3 INSTALLATION
Done	Help!
Device Selection	
Select the device(s) you'd like to install to. They will be left untouched until you click	k on the main menu's "Begin Installation" button.
Local Standard Disks	
	Disks left unselected here will not be touched.
Specialized & Network Disks	
100 GiB	
Add a disk 600a09	
3600a09803830344a332b52317a527a79 / 1023 KiB free	
	Disks left unselected here will not be touched.
Storage Configuration	
Automatic     Ocustom	
I would like to make additional space available.	
Encryption	
Encrypt my data. You'll set a passphrase next.	
Full disk summary and boot loader	1 disk selected; 100 GiB capacity; 1023 KiB free Refresh
12. To confirm that the multipath driver is loaded, click "Add a disk" and select Multipath Devices. You should see four disks listed.

Done	TION DES	TINATIO	N			RED HAT ENTERPRISE LIN	IUX 8.3 INSTALLATION
Search	Multipath	Devices	Other SAN	Devices NVDIMM [	levices		
Filter By: N	one 🖣	•					
WWID	Capacity	Vendor	Interconnect	Paths			
	100 GiB	NETAPP		sdf sdd sdg sde			
				Add iSCSI Target	Add FCoE SAN	Reconfigure NVDIMM	Refresh List

 Complete the OS installation on the SAN LUN. For more information about the installation process, refer to the Red Hat Linux installation document available at <u>https://access.redhat.com/documentation/en-US/Red Hat Enterprise Linux/8/.</u>

## Install network and storage drivers

Make sure that the drivers are always updated and compatible as described at the Cisco UCS Hardware and Software Compatibility portal.

Here, two important drivers need to be upgraded:

- fnic: For Fibre Channel storage
- enic: For Ethernet
- 1. Open the terminal to see the versions of the drivers currently installed.



 Go to the Cisco UCS Hardware and Software Compatibility portal at <u>https://ucshcltool.cloudapps.cisco.com/public/.</u> Enter the server model you are using and the operating system you want to install.

Select the firmware version and adapter model and see what the recommended driver version is.

-	- Cisco UCSB-MLOM-40G-04: Cisco UCS 1440 Virtual Interface Card	Firmware Version Driver Version	5.1(3) 2.0.0.69-178.0 fnic 🕔
		Adapter BIOS	5.1(3)
		Notes	<none></none>
- Cisco Ll	- Cisco UCSB-MI OM-40G-04: Cisco UCS 1440 Virtual Interface Card	Firmware Version	5.1(3)
		Driver Version	4.0.0.13-802.74 usnic_verbs 🕔
		Adapter BIOS	5.1(3)
		Notes	38
	- Cisco UCSB-MI OM-40G-04: Cisco UCS 1440 Virtual Interface Card	Firmware Version	5.1(3)
		Driver Version	4.0.0.14-802.74 enic 🕔
		Adapter BIOS	5.1(3)
		Notes	<none></none>

- 3. If your systems does not have recommended fnic version (2.0.0.69–178.0) or the recommended enic version (4.0.0.14-802.74), follow the steps below to upgrade the drivers.
- 4. Download the driver ISO file.

Search By

SSD

Storage

~

- Adapters

- - CNA

<ul> <li>Servers</li> <li>B-Series, C-Series, HX-Series, M-Series</li> </ul>	B,	Operating Systems VMware, Microsoft, RedHat,	<ul> <li>Products</li> <li>Adapters, Storage, Software,</li> </ul>		
Search Options				Reset All	
Server Type	B-Series			~	
Server Model	Cisco UCS B2	Cisco UCS B200 M5 2 Socket Blade Server			
Processor Version	2nd Gen Intel	2nd Gen Intel Xeon Processor Scalable Family			
Operating System	Red Hat			~	
Operating System Version	Red Hat Enterp	orise Linux 8.3		~	
Advisories ^					
Date Updated	Туре	Title			Details
May 22, 2020	EOL Advisory	End-of-Sale and End-of-Life Announceme	nt for the Cisco Select Unified C	omputing Systems Accessories	Advisory
Search Results					
Refine by Select All   Clear All	Expand All	All			Export Excel
Product Category	Component 🗸		Details		Documents
Adapters V	- 4.1(3) last published 2021-05-19	(change log)	Firmware Bundle		View Notes

5. Mount the ISO file as a vKVM-mapped DVD. Navigate to the kernel module (KMOD) Red Hat Package Manager (RPM) location and install the driver.

	root@localhost:/run/media/root/CDROM/Storage/Cisco/VIC/RHEL/RHEL8.3									×	
File	Edit	View	Search	Terminal	Tabs	Help					
				oot@locall	nost:~			root@localhost:/run/media/root/CDROM/Stora	age/Cisco/V ×	Æ	•
[rod [rod Ver: Prep Upda [rod [rod	ot@lo ot@lo ifyin parin ating l:kmo ot@lo ifyin parin ating l:kmo	ocalh ocalh ng g / j od-er ocalh ng g / j od-fr ocalh	nost R nost R instal nic-4. nost R nost R nic-2. nost R	HEL8.3 HEL8.3 0.0.14 HEL8.3 HEL8.3 Ling 0.0.69 HEL8.3	]# ]# rp -802 ]# co ]# rp -178 ]# ∎	om -ivh .74.rhe d /run/n om -ivh .0.rhela	kmod-eni ##### l8u3##### media/roo kmod-fni ##### 8u3 #####	Lc-4.0.0.14-802.74.rhel8u3.x86	_64.rpm [100%] [100%] L/RHEL8.3 64.rpm [100%] [100%]		

 Verify that the fnic and enic drivers are updated to the correct versions after you have installed the KMOD RPMs.

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

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

Printed in USA