Deployment Guide Cisco Public



# Cisco and Hitachi Adaptive Solutions with Cisco UCS X-Series, VMware 8U1, and Hitachi VSP 5600

Deployment Guide for the Adaptive Solutions Virtual Server Infrastructure with Cisco Intersight Managed Mode, VMware 8.0U1, and Hitachi VSP 5600 Published: January 2024



In partnership with:



# About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to: <a href="http://www.cisco.com/go/designzone">http://www.cisco.com/go/designzone</a>.

# **Executive Summary**

Cisco Validated Designs consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a a portfolio of solutions that have been developed to address the business needs of our customers.

Cisco and Hitachi have joined forces to provide a converged infrastructure solution designed to address the current challenges faced by enterprise businesses and position them for future success. Drawing upon their extensive industry knowledge and innovative technology, this collaborative Cisco CVD presents a robust, flexible, and agile foundation for today's businesses. Moreover, the partnership between Cisco and Hitachi goes beyond a a singular solution, allowing businesses to leverage their ambitious roadmap of progressive technologies including advanced analytics, IoT, cloud, and edge capabilities. By partnering with Cisco and Hitachi, organizations can confidently embark on their modernization journey and position themselves to capitalize on emerging business opportunities facilitated by groundbreaking technology.

This document explains the deployment of the Cisco and Hitachi Adaptive Solutions for Converged Infrastructure as a Virtual Server Infrastructure (VSI), as it was described in the Cisco and Hitachi Adaptive Solutions with Cisco UCSX, VMware 8U1, and Hitachi VSP 5600 Design Guide. The recommended solution architecture is built on Cisco Unified Computing System (Cisco UCS) using the unified software release to support the Cisco UCS hardware platforms for Cisco UCS X series servers, Cisco UCS 6500 Fabric Interconnects, Cisco Nexus 9000 Series switches, Cisco MDS Fibre channel switches, and the Hitachi Virtual Storage Platform (VSP) 5600. This architecture is implemented on VMware vSphere 8.0 U1 to support the leading virtual server platform of enterprise customers.

Additional Cisco Validated Designs created in a partnership between Cisco and Hitachi can be found here: <u>https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/data-center-design-guides/ata-center-design-guides/data-center-desig</u>

# Solution Overview

This chapter contains the following:

- Introduction
- <u>Audience</u>
- Purpose of this Document
- What's New in this Release?

## Introduction

Modernizing your data center can be overwhelming, and it's vital to select a trusted technology partner with proven expertise. With Cisco and Hitachi as partners, companies can build for the future by enhancing systems of record, supporting systems of innovation, and growing their business. Organizations need an agile solution, free from operational inefficiencies, to deliver continuous data availability, meet SLAs, and prioritize innovation.

Cisco and Hitachi Adaptive Solutions for Converged Infrastructure as a Virtual Server Infrastructure (VSI) is a best practice datacenter architecture built on the collaboration of Hitachi Vantara and Cisco to meet the needs of enterprise customers utilizing virtual server workloads. This architecture is composed of the Hitachi Virtual Storage Platform (VSP) 5000 series connecting through the Cisco MDS multilayer switches supporting both FC-SCSI and FC-NVMe protocols to Cisco Unified Computing System X-Series Servers managed through Cisco Intersight, and further enabled with the Cisco Nexus family of switches.

These deployment instructions are based on the buildout of the Cisco and Hitachi Adaptive Solutions for Converged Infrastructure validated reference architecture, which describes the specifics of the products utilized within the Cisco validation lab, but the solution is considered relevant for equivalent supported components listed within Cisco and Hitachi Vantara's published compatibility matrixes. Supported adjustments from the example validated build must be evaluated with care as their implementation instructions may differ.

## Audience

The intended audience of this document includes but is not limited to IT architects, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

## **Purpose of this Document**

This document provides a step by step configuration and implementation guide for the Cisco and Hitachi Adaptive Solutions for the Converged Infrastructure solution. This solution features a validated reference architecture composed of:

- Cisco UCS Compute
- Cisco Nexus Switches
- Cisco Multilayer SAN Switches

• Hitachi Virtual Storage Platform

For the design decisions and technology discussion of the solution, please refer to the Cisco and Hitachi Adaptive Solutions for Converged Infrastructure Design Guide: https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/hitachi\_adaptive\_vmware\_vsp\_des ign.html

## What's New in this Release?

The following design elements distinguish this version of the Adaptive Solutions Virtual Server Infrastructure from previous models:

- Cisco UCS X210c M7 servers with Intel Xeon Scalable Processors with up to 60 cores per processor and up to 8TB of DDR-4800 DIMMs
- 100Gbps Ethernet and 32Gbps Fibre Channel in Adaptive Solutions
- Integration of the 5th Generation Cisco UCS 6536 Fabric Interconnect into Adaptive Solutions
- Integration of the 5th Generation Cisco UCS 15000-series VICs into Adaptive Solutions
- Integration of the Cisco UCS X9108-100G Intelligent Fabric Module into the Cisco UCS X-Series X9508 Chassis
- Deployment of Cisco UCS with Cisco Intersight Managed Mode (IMM)
- Nexus Dashboard Fabric Controller
- VMware vSphere 8.0 Update 1
- FC-NVMe connectivity
- VMware vVols Datastores
- Hitachi Virtual Storage Platform (VSP) 5600
- Hitachi Ops Center release version 10.9.3
- Hitachi Storage Provider for VMware vCenter release version 3.7.3

# Deployment Hardware and Software

This chapter contains the following:

- <u>Physical Topology</u>
- Software Revisions
- VLAN Configuration
- Device Connectivity

## **Physical Topology**

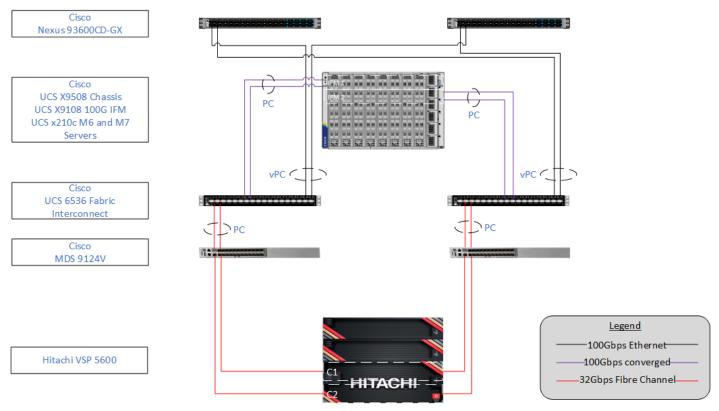
The Adaptive Solutions Virtual Server Infrastructure consists of a high-performance Fibre Channel network built using the following hardware components:

- Cisco UCS X9508 Chassis with Cisco UCSX-I-9108-100G Intelligent Fabric Modules (IFMs) and up to eight Cisco UCS X210c M7 Compute Nodes with 4th Generation Intel Xeon Scalable CPUs.
- Fifth-generation Cisco UCS 6536 Fabric Interconnects to support 100GbE, 25GbE, and 32GFC connectivity as needed.
- High-speed Cisco NX-OS-based Nexus 93600CD-GX switching design to support up to 100GE .
- Hitachi 5600 Virtual Storage Platform NVMe storage with 32G Fibre Channel connectivity.
- Cisco MDS 9124V switches to support Fibre Channel storage configuration.

The software components of the solution consist of:

- Cisco Intersight SaaS platform to deploy, maintain and support the Adaptive Solutions infrastructure.
- Cisco Intersight Assist Virtual Appliance to connect the Hitachi VSP 5600, VMware vCenter, and Cisco Nexus and MDS switches with Cisco Intersight.
- Cisco Nexus Dashboard Fabric Controller to give expanded insight and management into the MDS switching.
- Hitachi Ops Center Administrator is an infrastructure management solution that unifies storage provisioning, data protection, and storage management.
- Hitachi Ops Center API Configuration Manager to help connect the Hitachi VSP 5600 to the Intersight platform.
- VMware vCenter to set up and manage the virtual infrastructure as well as Cisco Intersight integration.

<u>Figure 1</u> shows the validated hardware components and connections used in the Adaptive Solutions Virtual Server Infrastructure design.



## Figure 1. Adaptive Solutions Virtual Server Infrastructure Physical Topology

The reference hardware configuration includes:

- Two Cisco Nexus 93600CD-GX Switches in Cisco NX-OS mode provide the switching fabric.
- Two Cisco UCS 6536 Fabric Interconnects (FI) provide the chassis connectivity. One 100 Gigabit Ethernet port from each FI, configured as a Port-Channel, is connected to each 93600CD-GX. Four FC ports are connected to the Cisco MDS 9124V switches via breakout using 32-Gbps Fibre Channel connections configured as a single port channel for SAN connectivity.
- One Cisco UCS X9508 Chassis connects to fabric interconnects using Cisco UCSX 9108-100G Intelligent Fabric Modules (IFMs), where four 100 Gigabit Ethernet ports are used on each IFM to connect to the appropriate FI. If additional bandwidth is required, all eight 100G ports can be utilized.
- The Cisco MDS 9124V sits between the compute and storage delivering 32Gbps Fibre Channel connectivity, as well as interfacing to resources present in an existing data center.
- The Hitachi VSP 5600 controllers connect with two 32Gbps FC ports from each controller to each Cisco MDS 9124V for delivering to the SAN network.

## Software Revisions

<u>Table 1</u> lists the software revisions for various components of the solution.

#### Table 1. Software Revisions

Layer	Device	Image	Comments
Network	Cisco Nexus 93600CD-GXNX-OS	10.2(5)M	
	Cisco MDS 9124V	9.3(2)	Requires SMART Licensing
	Nexus Dashboard	2.3(2d)	
	Cisco Nexus Dashboard Fabric Controller	12.1.2e on Nexus Dashboard 2.3(2d)	
Compute	Cisco UCS Fabric Interconnect 6536 and UCS 9108-100G IFM	4.3(2b)	Cisco UCS GA release for infrastructure including FIs and IOM/IFM.
	Cisco UCS X210c M7	5.1(1.230052)	
	Cisco UCS C220 M7	5.1(1.230052)	Connected but not a focus in the validation.
	Cisco UCS Tools	1.3.3-10EM	
	VMware ESXi nfnic FC Driver	5.0.0.41	Supports FC-NVMe
	VMware ESXi nenic Ethernet Driver	2.0.11.0	
	VMware ESXi		Build 21813344 included in Cisco Custom ISO, updated with patch 8.0 Update 1c
	VMware vCenter Appliance	8.0 Update 1c	Build 20395099
	Cisco Intersight Assist Appliance	1.0.9-588	1.0.9-588 initially installed and then automatically upgraded
Storage	Hitachi VSP 5600	SVOS 90-09-21-00/01	
	Hitachi Ops Center Administrator/CM Rest	10.9.3	
	Hitachi Storage Provider for VMware vCenter	3.7.3	

## **VLAN Configuration**

Table 2 lists the VLANs that are configured in the environment and details their usage.

## Table 2. VLAN Usage

VLAN ID	Name	Usage	IP Subnet used in this deployment
2	Native-VLAN	Use VLAN 2 as native VLAN instead of default VLAN (1).	
19	OOB-MGMT-VLAN	Out-of-band management VLAN to connect management ports for various devices	192.168.168.0/24; GW: 192.168.168.254
119	IB-MGMT-VLAN	In-band management VLAN utilized for all in-band management connectivity - for example, ESXi hosts, VM management, and so on.	10.1.168.0/24; GW: 10.1.168.254
1000	vMotion	VMware vMotion traffic	10.0.0/24 *
1100	VM-Traffic	VM data traffic sourced from FI-A and FI-B	10.1.100.0/24; GW: 10.1.100.254
1101	VM-Traffic-A	VM data traffic sourced from FI-A	10.1.101.0/24; GW: 10.1.101.254
1101	VM-Traffic-B	VM data traffic sourced from FI-B	10.1.101.0/24; GW: 10.1.101.254

\* IP gateway is not needed since no routing is required for these subnets

<u>Table 3</u> lists the infrastructure VMs necessary for the VSI environment hosted on pre-existing management infrastructure.

# Table 3. Virtual Machines

Virtual Machine Description	VLAN	IP Address
Cisco Intersight Assist	119	10.1.168.99
vCenter Server	119	10.1.168.100
Active Directory	119	10.1.168.101
Hitachi Ops Center	119	10.1.168.105

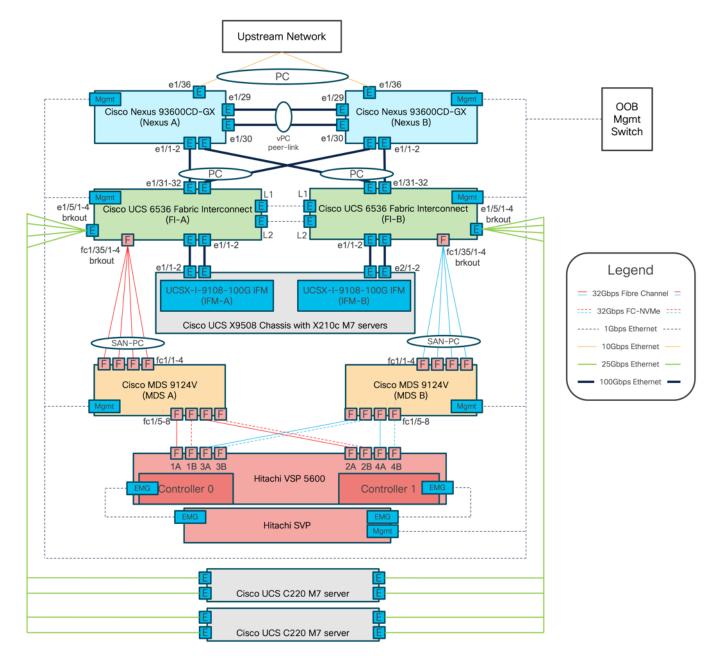
## **Device Connectivity**

The information in this section is provided as a reference for cabling the physical equipment in the environment. This includes a diagram, as well as tables for each layer of infrastructure detailing the local and remote port locations.

**Note:** If you modify the validated architecture, see the <u>Cisco Hardware Compatibility Matrix</u> and the <u>Hitachi</u> <u>Product Compatibility Guide</u> for guidance.

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps.

Figure 2 details the cable connections used in the validation lab for the Adaptive Solutions VSI topology based on the Cisco UCS 6536 fabric interconnect and the Hitachi VSP 5600. Four 32Gb uplinks via breakout connect as SAN port-channels from each Cisco UCS Fabric Interconnect to the MDS switches, and a total of eight 32Gb links connect the MDS switches to the VSP controller ports. 100Gb links connect the Cisco UCS Fabric Interconnects as port-channels to the Cisco Nexus 93600CD-GX switch pair's vPCs, while upstream of the Nexus switches, 400G uplink connections are possible for the model. Additional 1Gb management connections will be needed for an out-of-band network switch that sits apart from the Adaptive Solutions infrastructure. Each Cisco UCS fabric interconnect and Cisco Nexus switch is connected to the out-of-band network switch, and the VSP is front-ended by the SVP, which has a connection to the out-of-band network switch. Layer 3 network connectivity is required between the Out-of-Band (OOB) and In-Band (IB) Management Subnets.



## Figure 2. Adaptive Solutions Cabling with Cisco UCS 6536 Fabric Interconnect

## **Adaptive Solutions Cabling**

Tables listing the specifics of the connections for each component are provided below.

## Table 4. Cisco Nexus 93600CD-GX A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93600CD-GX	1/1	QSFP-100G-AOC2M	Cisco UCS 6536 FI A	1/31

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 12 of 367

Local Device	Local Port	Connection	Remote Device	Remote Port
A	1/2	QSFP-100G-AOC2M	Cisco UCS 6536 FI B	1/31
	1/29	QSFP-100G-AOC1M	Cisco Nexus 93600CD-GX B	1/29
	1/30	QSFP-100G-AOC1M	Cisco Nexus 93600CD-GX B	1/30
	1/36	10Gbase-SR	Upstream Network	
	Mgmt	Cat 5	Management Switch	

## Table 5. Cisco Nexus 93600CD-GX B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93600CD-GX B	1/1	QSFP-100G-AOC2M	Cisco UCS 6536 FI A	1/32
	1/2	QSFP-100G-AOC2M	Cisco UCS 6536 FI B	1/32
	1/29	QSFP-100G-AOC1M	Cisco Nexus 93600CD-GX A	1/29
	1/30	QSFP-100G-AOC1M	Cisco Nexus 93600CD-GX A	1/30
	1/36	10Gbase-SR	Upstream Network	
	Mgmt	Cat 5	Management Switch	

## Table 6. Cisco UCS 6536 Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS 6536 FI A	1/1	QSFP-40/100-SRBD	Cisco UCS 9108-100G IFM A	1/1
	1/2	QSFP-40/100-SRBD	Cisco UCS 9108-100G IFM A	1/2
	1/5/1	QSFP-4SFP25G-CU2M	UCSC-C220-M7S-1	1
	1/5/2		UCSC-C220-M7S-1	2
	1/5/3		UCSC-C220-M7S-2	1
	1/5/4		UCSC-C220-M7S-2	2
	1/31	QSFP-100G-AOC2M	Cisco Nexus 93600CD-GX A	1/31

Local Device	Local Port	Connection	Remote Device	Remote Port
	1/32	QSFP-100G-AOC2M	Cisco Nexus 93600CD-GX A	1/31
	1/35/1		Cisco MDS 9124V A	1/1
	1/35/2	DS-SFP-4x32G-SW to MPO-LC breakout	Cisco MDS 9124V A	1/2
1/35/3 1/35/4 L1 L2	1/35/3		Cisco MDS 9124V A	1/3
	1/35/4		Cisco MDS 9124V A	1/4
	L1	Cat 5	Cisco UCS 6536 FI B	L1
	L2	Cat 5	Cisco UCS 6536 FI B	L2
	Mgmt	Cat 5	Management Switch	

## Table 7. Cisco UCS 6536 Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS 6536 FI B	1/1	QSFP-40/100-SRBD	Cisco UCS 9108-100G IFM B	1/1
	1/2	QSFP-40/100-SRBD	Cisco UCS 9108-100G IFM B	1/2
	1/5/1		UCSC-C220-M7S-1	3
	1/5/2	QSFP-4SFP25G-CU2M	UCSC-C220-M7S-1	4
	1/5/3		UCSC-C220-M7S-2	3
	1/5/4		UCSC-C220-M7S-2	4
	1/31	QSFP-100G-AOC2M	Cisco Nexus 93600CD-GX B	1/32
	1/32	QSFP-100G-AOC2M	Cisco Nexus 93600CD-GX B	1/32
	1/35/1		Cisco MDS 9124V B	1/1
	1/35/2	Cisco 128G FC QSP DS-SFP-4x32G-SW to	Cisco MDS 9124V B	1/2
	1/35/3	MPO-LC breakout	Cisco MDS 9124V B	1/3
	1/35/4		Cisco MDS 9124V B	1/4

Local Device	Local Port	Connection	Remote Device	Remote Port
	L1	Cat 5	Cisco UCS 6536 FI A	L1
L2	L2	Cat 5	Cisco UCS 6536 FI A	L2
	Mgmt	Cat 5	Management Switch	

## Table 8. Cisco UCS 9124V A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9124V A	1/1	DS-SFP-FC32G-SW	Cisco UCS 6536 FI A	1/35/1
	1/2	DS-SFP-FC32G-SW	Cisco UCS 6536 FI A	1/35/2
	1/3	DS-SFP-FC32G-SW	Cisco UCS 6536 FI A	1/35/3
	1/4	DS-SFP-FC32G-SW	Cisco UCS 6536 FI A	1/35/4
	1/5	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 1	1A
	1/6	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 1	1B
	1/7	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 2	2A
	1/8	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 2	2B
	Mgmt	Cat 5	Management Switch	

## Table 9. Cisco UCS 9124V B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9124V B	1/1	DS-SFP-FC32G-SW	Cisco UCS 6536 FI B	1/35/1
	1/2	DS-SFP-FC32G-SW	Cisco UCS 6536 FI B	1/35/2
	1/3	DS-SFP-FC32G-SW	Cisco UCS 6536 FI B	1/35/3
	1/4	DS-SFP-FC32G-SW	Cisco UCS 6536 FI B	1/35/4
	1/5	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 1	3A
	1/6	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 1	3B

Local Device	Local Port	Connection	Remote Device	Remote Port
	1/7	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 2	4A
	1/8	DS-SFP-FC32G-SW	Hitachi VS 5600 Controller 2	4B
	Mgmt	Cat 5	Management Switch	

#### Table 10. Hitachi VSP 5600 Controller 1

Local Device	Local Port	Connection	Remote Device	Remote Port
Hitachi VSP 5600 Controller 1	1A	DS-SFP-FC32G-SW	Cisco UCS 9124V A	1/5
	1B	DS-SFP-FC32G-SW	Cisco UCS 9124V A	1/6
	ЗА	DS-SFP-FC32G-SW	Cisco UCS 9124V B	1/5
	3В	DS-SFP-FC32G-SW	Cisco UCS 9124V B	1/6

## Table 11. Hitachi VSP 5600 Controller 2

Local Device	Local Port	Connection	Remote Device	Remote Port
Hitachi VSP 5600 Controller 2	2A	DS-SFP-FC32G-SW	Cisco UCS 9124V A	1/7
	2B	DS-SFP-FC32G-SW	Cisco UCS 9124V A	1/8
	4A	DS-SFP-FC32G-SW	Cisco UCS 9124V B	1/7
	4B	DS-SFP-FC32G-SW	Cisco UCS 9124V B	1/8

#### Table 12. VSP Service Processor (SVP)

Local Device	Local Port	Connection	Remote Device	Remote Port
VSP Service Processor (SVP)	Public LAN	Cat 5	Management Switch	User Defined

The cables and transceivers used in the validated environment are not prescriptive to the solution but are examples of transceivers and cable connections that are valid in the design. Visit the specific product spec sheets and the Cisco Optics-to-Device Compatibility Matrix <u>https://tmgmatrix.cisco.com/</u> to identify additional supported options.

# Cisco Nexus LAN Switch Configuration

This chapter contains the following:

- <u>Physical Connectivity</u>
- Initial Configuration
- Cisco Nexus Switch Configuration

This chapter provides a detailed procedure for configuring the Cisco Nexus 93600CD-GX switches for use in the LAN switching of the Adaptive Solutions Virtual Server Infrastructure.

The following procedures describe how to configure the Cisco Nexus switches for use in a base Adaptive Solutions VSI environment. This procedure assumes the use of Cisco Nexus 9000 10.2(5)M.

## **Physical Connectivity**

Follow the physical connectivity guidelines for infrastructure cabling as explained in the <u>Adaptive Solutions Ca-</u> <u>bling</u> section.

## **Initial Configuration**

The following procedures describe this basic configuration of the Cisco Nexus switches for use in the Adaptive Solutions VSI. This procedure assumes the use of Cisco Nexus 9000 10.2(5)M, the Cisco suggested Nexus switch release at the time of this validation.

## Procedure 1. Set up Initial Configuration

To set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>, follow these steps from a serial console:

**Step 1.** Configure the switch.

**Note:** On initial boot, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic configuration,
no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: yes
Disabling POAP.....Disabling POAP
poap: Rolling back, please wait... (This may take 5-15 minutes)
         ---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": sword>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <nexus-A-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-A-out of band mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-A-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-A-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
```

```
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: Enter
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: n
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

**Step 2.** Review the configuration summary before enabling the configuration.

Use this configuration and save it? (yes/no) [y]: Enter

**Step 3.** To set up the initial configuration of the Cisco Nexus B switch, repeat steps 1 and 2 with the appropriate host and IP address information.

## **Cisco Nexus Switch Configuration**

To manually configure the Nexus switches, follow these steps:

#### **Procedure 1.** Enable Nexus Features

Cisco Nexus A and Cisco Nexus B (steps should be performed on both switches)

**Step 1.** Log in as admin using ssh.

Step 2. Run the following commands to enable Nexus features:

config t
feature nxapi
feature hsrp
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp

**Procedure 2.** Set Global Configurations

Cisco Nexus A and Cisco Nexus B (steps should be performed on both switches)

**Step 1.** Run the following commands to set global configurations:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ip name-server <dns-server-1> <dns-server-2>
ip domain-name <dns-domain-name>
ip domain-lookup
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
clock timezone <timezone> <hour-offset> <minute-offset>
```

(For Example: clock timezone EST -5 0)

clock summer-time <timezone> <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month> <end-time> <offset-minutes>

(For Example: clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60)

```
copy run start
ip route 0.0.0.0/0 <oob-mgmt-vlan-gateway>
```

**Note:** For more information on configuring the timezone and daylight savings time or summer time, see Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 10.2(x).

#### Procedure 3. Create VLANs

Cisco Nexus A and Cisco Nexus B (steps should be performed on both switches)

**Step 1.** From the global configuration mode, run the following commands:

```
vlan <ib-mgmt-vlan-id for example, 19>
name ib-mgmt
vlan <native-vlan-id for example, 2>
name native-vlan
vlan <vmotion-vlan-id for example, 1000>
name vmotion
vlan <vm-traffic-vlan-id for example, 1100>
name vm-traffic
vlan <vm-traffic-a-vlan-id for example, 1101>
name vm-traffic-a
vlan <vm-traffic-b-vlan-id for example, 1102>
name vm-traffic-b
```

## Procedure 4. Add NTP Distribution Interface in IB-MGMT Subnet (Optional)

This procedure will configure each IB-MGMT SVI to be available for redistribution of the NTP service to optionally configured application networks that might not be set up to reach an upstream NTP source.

## Cisco Nexus A

## **Step 1.** From the global configuration mode, run the following commands:

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
ntp peer <nexus-B-mgmt0-ip> use-vrf management
```

## Cisco Nexus B

**Step 1.** From the global configuration mode, run the following commands:

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
ntp peer <nexus-A-mgmt0-ip> use-vrf management
```

## **Procedure 5.** Create Application Network Interfaces (Optional)

This procedure creates Switched Virtual Interfaces (SVI) and Hot Standby Router Protocol (HSRP) configurations for each of these SVIs. The HSRP relationship allows an active/standby relationship between the two Nexus switches for these interfaces. The IB-Mgmt network is implemented for routing upstream of the Nexus switches, and these application networks could similarly be handled.

## Cisco Nexus A

int vlan 1100
no shutdown
ip address <<var\_nexus\_A\_App-1100>>/24
hsrp 100
preempt
ip <<var\_nexus\_App-1100\_vip>>

**Note:** When HSRP priority is not set, it defaults to 100. Alternating SVIs within a switch are set to a number higher than 105 to set those SVIs to default to be the standby router for that network. Be careful when the VLAN SVI for one switch is set without a priority (defaulting to 100), the partner switch is set to a priority with a value other than 100.

int vlan 1101
no shutdown
ip address <<var\_nexus\_A\_App-1101>>/24
hsrp 101
preempt
priority 105
ip <<var nexus App-1101 vip>>

int vlan 1102
no shutdown
ip address <<var\_nexus\_A\_App-1102>>/24
hsrp 102
preempt
ip <<var\_nexus\_App-1102\_vip>>

#### **Cisco Nexus B**

int vlan 1100
no shutdown
ip address <<var\_nexus\_B\_App-1100>>/24
hsrp 100
preempt
priority 105
ip <<var\_nexus\_App-1100\_vip>>

int vlan 1101
no shutdown
ip address <<var\_nexus\_B\_App-1101>>/24
hsrp 101
preempt
ip <<var\_nexus\_App-1101\_vip>>

int vlan 1102
no shutdown
ip address <<var\_nexus\_B\_App-1102>>/24
hsrp 102
preempt
priority 105
ip <<var\_nexus\_App-1102\_vip>>

#### Procedure 6. Create Port Channels

## **Cisco Nexus A**

**Note:** For fibre optic connections to Cisco UCS systems (AOC or SFP-based), entering udld enable will result in a message stating that this command is not applicable to fiber ports. This message is expected. This command will enable UDLD on twinax connections.

**Step 1.** From the global configuration mode, run the following commands:

```
interface Pol0
description vPC peer-link
interface Eth1/29
description <nexus-b-hostname>:Eth1/29
interface Eth1/30
description <nexus-b-hostname>:Eth1/30
interface Eth1/29-30
channel-group 10 mode active
no shutdown
! UCS Connectivity
interface Poll
description <ucs-domainname>-a
interface Eth1/1
udld enable
description <ucs-domainname>-a:Eth1/35
channel-group 11 mode active
no shutdown
interface Pol2
description <ucs-domainname>-b
interface Eth1/2
udld enable
description <ucs-domainname>-b:Eth1/35
channel-group 12 mode active
no shutdown
1
! Uplink Switch Connectivity
interface Pol36
description MGMT-Uplink
interface Eth1/36
description <mgmt-uplink-switch-a-hostname>:<port>
channel-group 136 mode active
no shutdown
exit
copy run start
```

## **Cisco Nexus B**

**Note:** For fibre optic connections to Cisco UCS systems (AOC or SFP-based), entering udld enable will result in a message stating that this command is not applicable to fiber ports. This message is expected. This command will enable UDLD on twinax copper connections.

**Step 1.** From the global configuration mode, run the following commands:

```
interface Pol0
```

```
description vPC peer-link
interface Eth1/29
description <nexus-a-hostname>:Eth1/29
interface Eth1/30
description <nexus-a-hostname>:Eth1/30
interface Eth1/29-30
channel-group 10 mode active
no shutdown
1
! UCS Connectivity
1
interface Poll
description <ucs-domainname>-a
interface Eth1/1
udld enable
description <ucs-domainname>-a:Eth1/36
channel-group 11 mode active
no shutdown
interface Pol2
description <ucs-domainname>-b
interface Eth1/2
udld enable
description <ucs-domainname>-b:Eth1/36
channel-group 12 mode active
no shutdown
1
! Uplink Switch Connectivity
interface Pol36
description MGMT-Uplink
interface Eth1/36
description <mgmt-uplink-switch-a-hostname>:<port>
channel-group 136 mode active
no shutdown
exit
copy run start
```

## Procedure 7. Configure Port Channel Parameters

## Cisco Nexus A and Cisco Nexus B (steps should be performed on both switches)

Note: To configure port channel parameters, follow this step on both switches.

**Step 1.** From the global configuration mode, run the following commands to set up the VPC Peer-Link port-channel:

```
interface Po10
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan
<ib-mgmt-vlan-id>,<vmotion-vlan-id>,<vm-traffic-vlan-id>,<vm-traffic-a-vlan-id>,<vm-traffic-b-vlan-id>
spanning-tree port type network
speed 100000
duplex full
```

**Step 2.** From the global configuration mode, run the following commands to set up port-channels for UCS FI 6536 connectivity:

interface Poll
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan
<ib-mgmt-vlan-id>,<vm-traffic-vlan-id>,<vm-traffic-a-vlan-id>,<vm-traffic-b-vlan-id>
spanning-tree port type edge trunk
mtu 9216
!
interface Pol2
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan
<ib-mgmt-vlan-id>,<vm-traffic-b-vlan-id>,<vm-traffic-b-vlan-id>
spanning-tree port type edge trunk
mtu 9216

**Step 3.** From the global configuration mode, run the following commands to setup port-channels for connectivity to existing management switch(es):

interface Po136
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan <ib-mgmt-vlan-id>
spanning-tree port type network
mtu 9216
!
exit
copy run start

## Procedure 8. Configure Virtual Port Channels

#### **Cisco Nexus A**

**Step 1.** From the global configuration mode, run the following commands:

```
vpc domain <nexus-vpc-domain-id for example, 10>
role priority 10
peer-keepalive destination <nexus-B-mgmt0-ip> source <nexus-A-mgmt0-ip> vrf management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
interface Pol0
vpc peer-link
interface Poll
vpc 11
I.
interface Pol2
vpc 12
I.
interface Po136
vpc 136
1
exit
copy run start
```

#### **Cisco Nexus B**

#### **Step 1.** From the global configuration mode, run the following commands:

vpc domain <nexus-vpc-domain-id for example, 10>

<pre>role priority 20 peer-keepalive destination <nexus-a-mgmt0-ip> source <nexus-b-mgmt0-ip> vrf management peer-switch peer-gateway auto-recovery delay restore 150 ip arp synchronize !</nexus-b-mgmt0-ip></nexus-a-mgmt0-ip></pre>	
interface Pol0	
vpc peer-link	
1	
interface Poll	
vpc 11	
1	
interface Pol2	
vpc 12	
interface Pol36	
vpc 136	
exit	
copy run start	

# Hitachi Ops Center Configuration and Initial VSP Settings

This chapter contains the following:

• Configure Hitachi Ops Center

Hitachi Ops Center VM must be deployed on Cisco UCS Management cluster and the Ops Center environment must meet minimum system requirements to support management of various storage systems and servers. For additional details on Hitachi Ops Center, go to:

https://knowledge.hitachivantara.com/Documents/Management Software/Ops Center/Administrator/10.9.x/Get ting started/02 Hitachi Ops Center Administrator environment#r hid system req

The software can be obtained from your respective Hitachi representative, alternatively for partner access software can be downloaded here: <u>https://support.hitachivantara.com/en/user/answers/downloads.htm</u>

For additional information, see the Hitachi Ops Center document library: <u>https://knowledge.hitachivantara.com/Documents/Management\_Software/Ops\_Center/10.9.x/Ops\_Center\_10.9.x</u>

## **Configure Hitachi Ops Center**

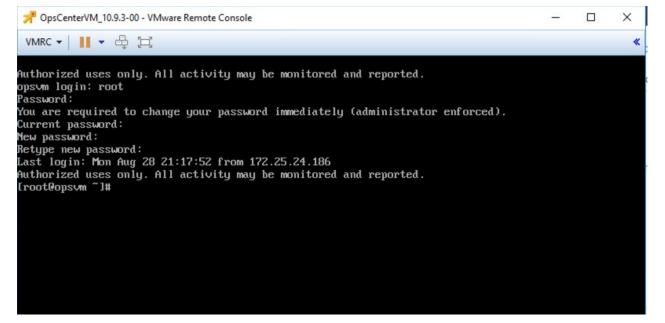
Procedure 1. Initial Configuration of the Hitachi Ops Center

Proceed with the following steps to configure the Hitachi Ops Center after deploying the OVA template:

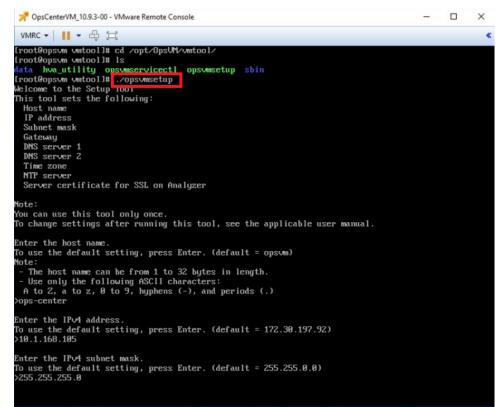
**Step 1.** Log in with the following credentials:

Username: root

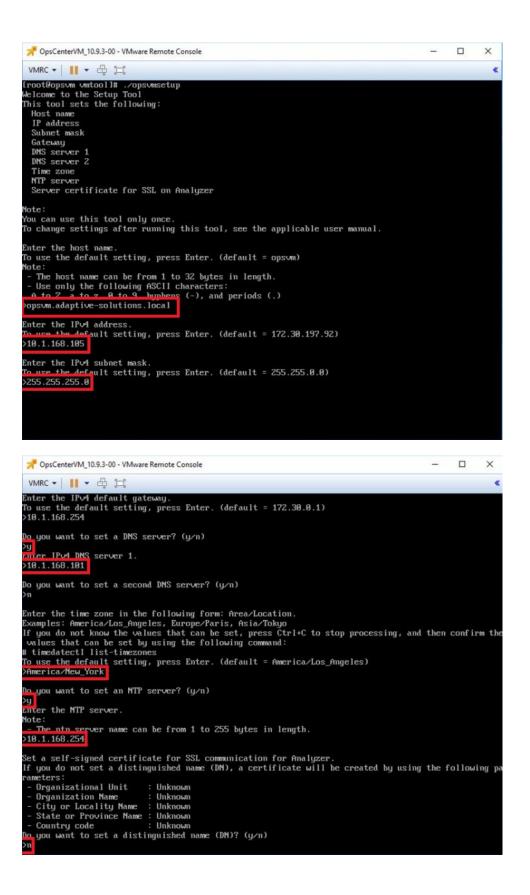
Password: manager



Step 2. Run the opsvmsetup command to start the setup tool.

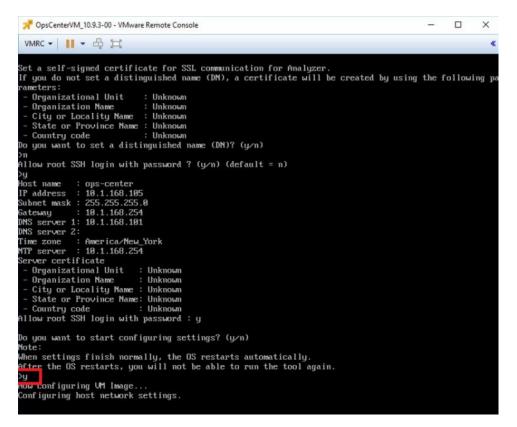


**Step 3.** Enter the Hostname (FQDN), IP Address, Subnet mask, Gateway, DNS, Time zone, and NTP details, as shown in the following figures.



**Step 4.** After providing the initial setup information, enter "**y**" to start the configuration.

**Note:** Do not press or enter any key while running the configuration setup. The OS will restart automatically after the configuration is completed.



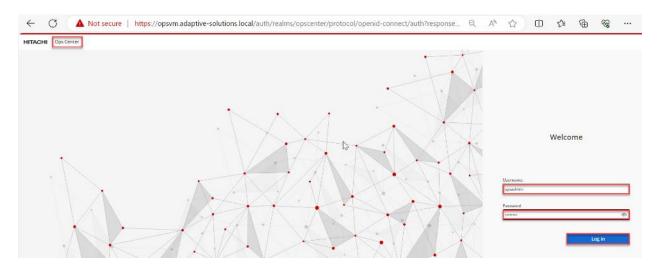
## Procedure 2. Access Hitachi Ops Center Administrator

After the Ops Center configuration is completed, open a browser, and enter https://[FQDN or IP Address]/portal/#/inventory/products.

Step 1. Enter the following credentials and click Log in:

Username: sysadmin

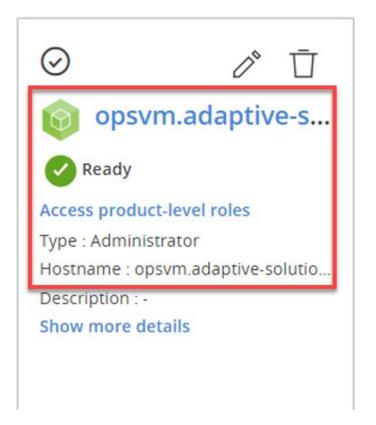
Password: sysadmin



**Step 2.** After logging into the Hitachi Ops Center UI, you will find different product types such as **Administrator**, **Analyzer**, **Analyzer** detail view, **Automator**, and **Protector**.

Products   set type   I type   I damaistrater (1)	ACHI Ops Center	In	ventory Manag	e users Data cente	ers	
Products   Products   Image: service of type   Products   Image: service of type   Image: servic		Products				
<ul> <li>Administrator (1)</li> <li>Analyzer (1)</li> <li>Access product-level roles (1)</li> <li>Box more details</li> <li>Box more details</li> <li>Box more details</li> </ul>	Products					55
Reach (2)	Administrator (1)     Analyzer (1)     Analyzer (1)     Analyzer detail view (1)     Automator (1)     Protector (1)     Status	opsvm.adaptive-s     License not activated  Access product-level roles  Type : Automator  Hostname : opsvm.adaptive-solicito  Description :	opsvm.adaptive-s     construct-level roles     Type : Administrator     Hostneme : opsvm.adaptive solutio     Description :	Opsvm.adaptive-s     Ucesse not activated     Access product-level roles     Type : Analyzer     Hossname : opsvm.adaptive solutio     Description :	opsym.adaptive-s     Ready     Access product-level roles     Type : Protector     Hestname : opsym.adaptive solutio     Description :	opsvm.adaptive-     Ucense not activated     Access product-level roles     Type : Analyzer detail view     Hostnarme : opsvm.adaptive solu     Description :

Step 3. Select the highlighted icon to launch **Ops Center Administrator**.



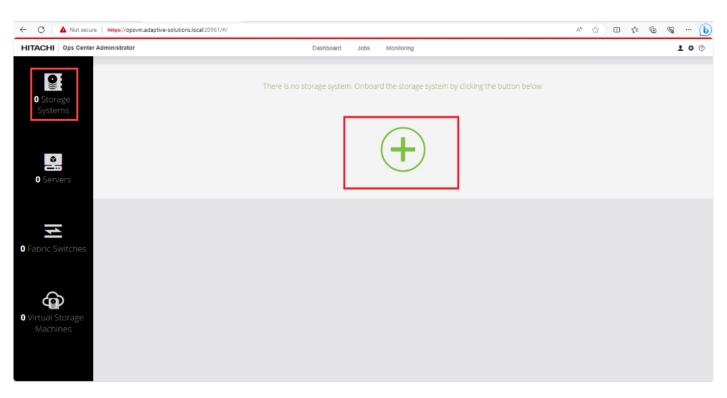
## Procedure 3. Onboarding Hitachi Virtual Storage Platform to Ops Center Administrator

Onboarding a storage system is the process of associating it with Ops Center Administrator. After onboarding the storage system, you can manage it from the Ops Center Administrator dashboard.

Before you begin, verify the following:

- The service processor (SVP) username used to onboard a storage system in Ops Center Administrator has access to all resource groups on the storage system, including custom resource groups and meta resource groups, to ensure workflows function correctly.
- The user is a member of the Administration Users Group.

**Step 1.** On the **Ops Center Administrator** dashboard, click **Storage Systems**, and click the plus sign (+) to add a storage system.



Step 2. In the Onboard Storage System window, enter values for the following parameters:

• IP Address:

For a storage system with an SVP, enter the IP address (IPv4) of the SVP for the storage system you want to discover.

**Note:** For the VSP E1090, if there is no SVP, you can onboard storage using the IP address of the controllers.

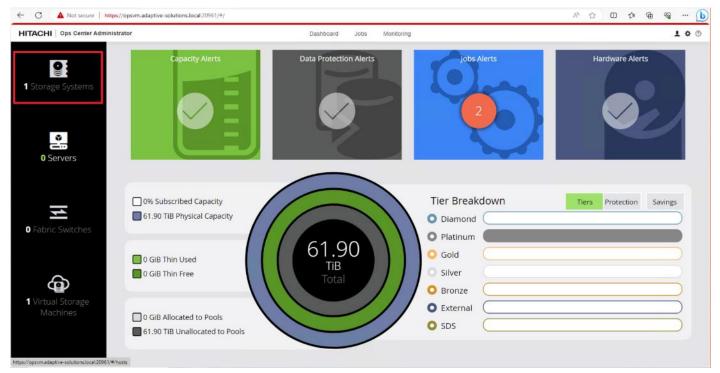
• Username and password:

Onboard the VSP system as a user with administrator privileges on the storage system. For example, you can use the following username and password:

- Username: maintenance
- Password: raid-maintenance
- Step 3. Click Submit.

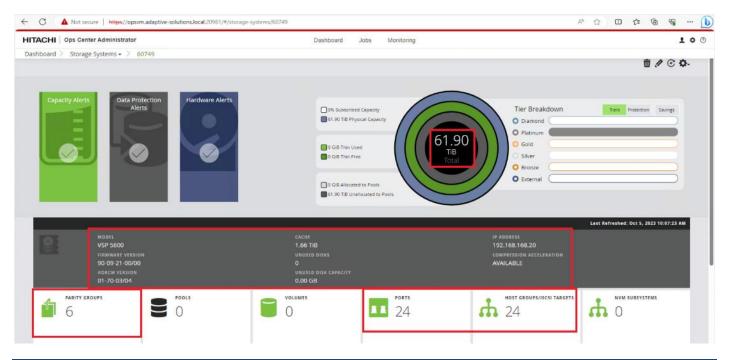
← C ▲ Not secure   https://opsvm.adap	tive-solutions.local:20961/#/storage-systems/add				A & & C & A	à 🧠 🜔
HITACHI Ops Center Administrator		Dashboard	Jobs Monitoring			100
Dashboard > Storage Systems -> Onboar						
Conboard S	itorage System					
Onboard Storag	e System 192.168.168.20					
USERNAME			PASSWORD			
maintenance				]	<u></u>	
					Cancel Submit -	

**Step 4.** The dashboard now shows that the number of storage systems has been increased by one. Additionally, when you click **Storage Systems,** you are redirected to the storage system inventory window where you can see the newly-added storage system.



When a storage system is onboarded, the Ops Center Administrator undergoes an initialization process to gather information about the current configuration of the storage system. During this time, you may observe that the ports,

volumes, pools, and Parity Groups in the storage system are "Not accessible." After the initialization is completed, you can view information about PARITY GROUPS, POOLS, VOLUMES, PORTS, HOST GROUPS/SCSI TARGETS, and NEW SUBSYSTEMS in the Storage System tab.



**Procedure 4.** Configure Fibre Channel Ports on the Hitachi Virtual Storage Platform from Ops Center Administrator (FC-SCSI)

Before the Ops Center Administrator can create a host storage domain (HSD) on a port, you must change the port security and port attributes settings.

Port security must be enabled for fibre ports. By default, security is disabled on the VSP storage ports. Additionally, for VSP 5000 series systems, you must verify that the port attribute is set to TARGET.

**Step 1.** Log in to Hitachi Ops Center Administrator. From the navigation pane, click **Storage Systems**.

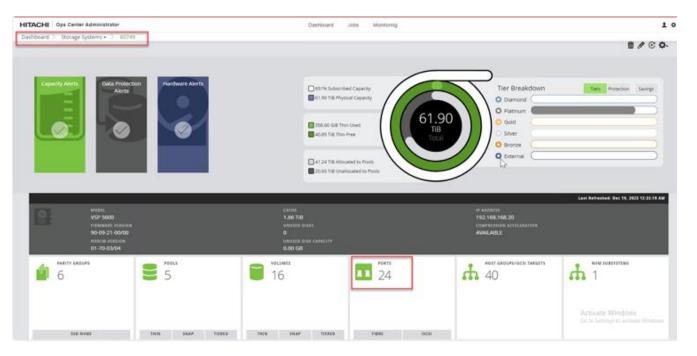
TACHI Ops Center Administrator	Dashboard Jobs Monitoring		1
Capacity Alerts	Data Protection Alerts	jobs Alerts	Hardware Alerts
C Fabric Switches	61.90 Тів Тотаі	Tier Breakdown  Diamond  Platinum Gold Silver Bronze	Tiers Protection Saving



Click the **S/N** listing of the Storage System.

HITACHI Ops Center Administrator Deshboard > Storage Systems =			Dashboard	Jobs Monitoring					1 0 0
Storage Systems									
f Summary									
Copuently Allerts	an Pibly Alerts	Harthware Alerts	214.35 CB 2041 TB 7		61.90 18 10 10	Tier Breakdow Diatrond Gold Silver External Sos	VN Tert	Prosection Salvings	
- 🗊 🖉 Actions									
L.									
NAME S/R	IP ADDRESS	MODEL	TOTAL	19039-0819	THIN USED	USAGE	INCOMPLETE HA ARRAY	NIGRATION TASK	COUNT
AA22-5600 60749	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GIB	0.98	-	0	
Items 0 selected							and the second se	200 🛩 items	- 8

**Step 3.** Click **PORTS** to see the configured storage ports for the storage systems.



**Step 4.** To modify ports, select one or more Fibre Channel ports, and then click the edit pencil icon in the Actions pane.

				orts		) 🖞 🕀	କ୍ଷ
HITACHI Ops Cente	r Administrator		Dashboard Jobs Monitoring				1
Dashboard > Storage	Systems • > 60749 > Ports •						
Ports							虚罚
Summary							
Jannary							
	Fibre				ISCSI		
	SCSI				NVMe		
1							
2							
PORT ID	wwn	SPEED	FABRIC, CONNECTION TYPE	SECURITY	VSM PORT	ATTRIBUTE	
O CL1-A	50:06:0E:80:08:ED:4D:00	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL1-C	50:06:0E:80:08:ED:4D:02	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL2-A	50:06:0E:80:08:ED:4D:10	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL2-C	50:06:0E:80:08:ED:4D:12	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL3-A	50:06:0E:80:08:ED:4D:20	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL3-C	50:06:0E:80:08:ED:4D:22	Auto	Fabric ON / Point-	No	No	Target	
O CL4-A	50:06:0E:80:08:ED:4D:30	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL4-C	50:06:0E:80:08:ED:4D:32	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL5-A	50:06:0E:80:08:ED:4D:40	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL5-B	50:06:0E:80:08:ED:4D:41	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL5-C	50:06:0E:80:08:ED:4D:42	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL6-A	50:06:0E:80:08:ED:4D:50	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL6-8	50:06:0E:80:08:ED:4D:51	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL6-C	50:06:0E:80:08:ED:4D:52	Auto	Fabric ON / Point-to-point	No	No	Target	
0 017-0	50:06:0E:80:08:ED:40:60	Auto	Fabric ON / Point-to-point	No	No	A	

**Step 5.** In the **Edit Fibre Port** dialog box, you can change the security settings and port attributes. Verify that port settings for fibre ports used in FC-SCSI connectivity have **SCSI Mode**, **Enable Security**, and **Target** selected as the port attribute. In the context of this document, these settings apply to fibre ports CL1-A, CL2-A, CL3-A, and CL4-A.

Step 6. Click OK.

HITACHI Ops Center			Dashboard Jobs Monitoring			
Dashboard > Storage S	ystems + > 60749 > Ports +					
				_		រងំរ
		🛕 Edit Fibr	e Port	×		
		Modify port s	ettings for the 1 selected ports to:			
	SCSI		SCSI Mode NVMe Mo	de .	NVMe	
		E	hable Security Disable Security	urity		
		Target		~		
PORT ID	WWN				VSM PORT	ATTRIBUTE
CL1-A					No	Target
	50:06:0E:80:08:ED:4D:02		Cancel OK -		No	Target
CL2-A	50:06:0E:80:08:ED:4D:10	Auto	Fabric ON / Point-to-point	Yes	No	Target
	50:06:0E:80:08:ED:4D:12	Auto	Fabric ON / Point-to-point	No	No	Target
CL3-A		Auto	Fabric ON / Point-to-point	Yes	No	Target
		Auto	Fabric ON / Point-to-point	No	No	Target
CL4-A		Auto				

# Cisco Intersight Managed Mode Configuration

This chapter contains the following:

- <u>Cisco Intersight Setup</u>
- Onboarding to Intersight
- <u>Cisco UCS Domain Configuration</u>
- <u>Configure Server Profile Template</u>
- <u>Cisco UCS IMM Setup Completion</u>

# Cisco Intersight Setup

The Cisco Intersight platform is a management solution delivered as a service with embedded analytics for Cisco and third-party IT infrastructures. The Cisco Intersight managed mode (also referred to as Cisco IMM) is a new architecture that manages Cisco Unified Computing System (Cisco UCS) fabric interconnect-attached systems through a Redfish-based standard model. Cisco Intersight managed mode standardizes both policy and operation management for the Cisco UCS X210c M7 compute nodes used in this deployment guide.

Cisco UCS C-Series M7 servers, connected and managed through Cisco UCS FIs, are also supported by IMM. For a complete list of supported platforms, go to:

https://www.cisco.com/c/en/us/td/docs/unified computing/Intersight/b Intersight Managed Mode Configurati on Guide/b intersight managed mode guide chapter 01010.html

# Procedure 1. Set Up Cisco Intersight Account

When setting up a new Cisco Intersight account (as explained in this document), the account must be enabled for Cisco Smart Software Licensing. Skip this step if starting out with a trial, or if a token has already been generated.

**Step 1.** Log into the Cisco Smart Licensing portal: <u>https://software.cisco.com/software/smart-licensing/alerts</u>.

**Step 2.** Verify that the correct virtual account is selected.

**Step 3.** Under **Inventory** > **General**, generate a new token for product registration.

# **Create Registration Token**

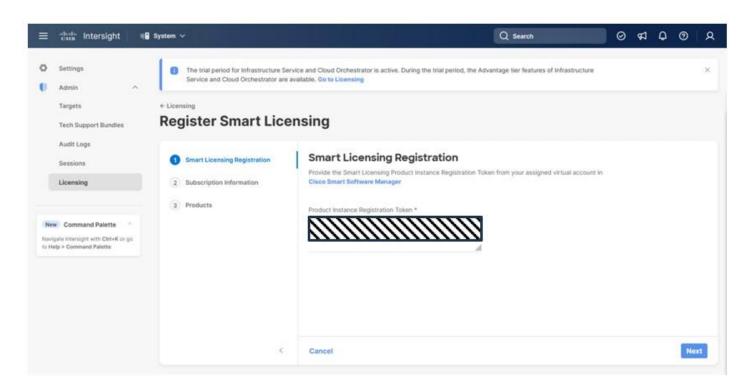
This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

unire After		Dava
Expire After:	30	Days
	Between 1 - 365, 30	) days recommended
fax. Number of Uses:		
		pired when either the expiration or the maximum uses is reached
Allow export-controlled	functionality on the produc	cts registered with this token 1

**Step 4.** Copy this newly created token.

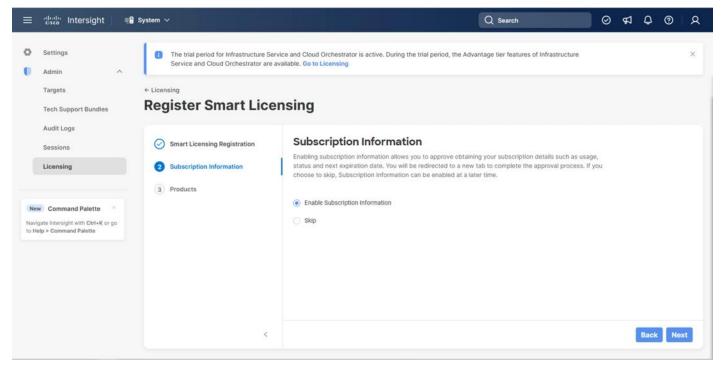
Procedure 2.	Set Up Cisco Intersight Licensing
Step 1.	Go to https://intersight.com and click Create an account if not using an existing account.
Step 2.	Select the appropriate region for the account. Click Next.
Step 3.	Read and accept the license agreement. Click Next.
Step 4.	Provide an Account Name. Click <b>Create</b> .
Step 5.	Select to either Register Smart Licensing if that has been established or Start Trial.
Step 6.	If registering, the <b>Register Smart Licensing</b> will take you to System > Admin > Licensing.
Step 7.	Provide the copied token from the Cisco Smart Licensing Portal. Click Next.

0 ×

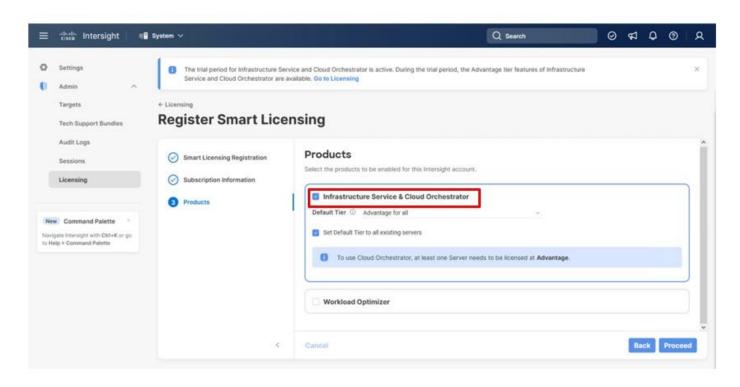




Select Enable or Skip subscription information and click Next.



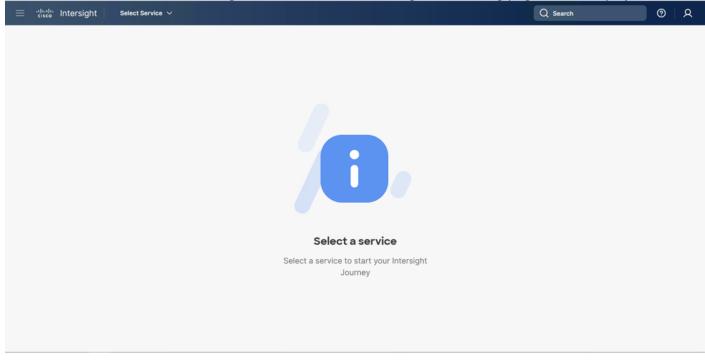
**Step 9.** Select the **Infrastructure Service & Cloud Orchestrator** option, adjust the default tier for licensing if needed, and if this should be used for existing servers, click **Proceed**. Click **Confirm** when asked to verify options.



On successfully syncing of Smart Licensing, the following page will be displayed:

=	cisco Intersight	📲 System 🗸	Q	Search 🥑 🕫 🗘 🕐 🎗
0	Settings Admin Targets	Compliance Summary Smart Licensing Detail	s	Start Trial Actions 👻
	Tech Support Bundles Audit Logs Sessions Licensing		There are no products in use.	
Navi	Command Palette			

On successful creation of the Intersight account with trial licensing, the following page will be displayed:



# Procedure 3. Configure Cisco Intersight Resource Group

In this procedure, a Cisco Intersight resource group is created where resources such as targets will be logically grouped. In this deployment, a single resource group is created to host all the resources, but you can choose to create multiple resource groups for granular control of the resources.

- Step 1. Log in to Cisco Intersight.
- Step 2. At the top, select System. On the left, click Settings (the gear icon).
- Step 3. Click Resource Groups in the middle panel.
- Step 4. Click + Create Resource Group in the top-right corner.

Admin     Admin     Targets     CEN     Tech Support Bundles     Act     Audit Logs     Sessions     No	ttings NERAL count Details cress Details Hiffications	Resource Groups		+ Create Resource Group
Targets dev Tech Support Bundles Acc Audit Logs Acc Sessions No	count Details			+ Create Resource Group
	THENTICATION ngle Sign-On	Resource Oroups are now available, and associate with the Organization     Resource Groups 0 +     Q_ Add Fitter     Name	atowing you to logically group the resources. You ca at For more information, see Resource Groups in Het 1 items found 1 Used Organizations Membership	n create multiple Resource Groups p Center. 0 ~ per page () 1 of 1 () 2 Description : 0
Navigate interstigte with Chrisk or go to Help > Command Palette Try Act	International Control	dofault	default All	The Default Resour

**Step 5.** Provide a name for the **Resource Group** (for example, AA21-rg).

=	cisco Intersight	RB System ~ Q Search	0	Ø	٥	0	8
0	Settings Admin	Create Resource Group					
	Targets Tech Support Bundles Audit Logs Sessions Licensing	Create Resource Group Create a Resource Group to manage and access the targets. General Name * A221-fg © Description	4				Î
Nav	Command Palette     gate Intersight with Ctol-K or go     b > Command Palette						
		Cancel				Crea	te

Step 6. Click Create.

Procedure 4. Configure Cisco Intersight Organization

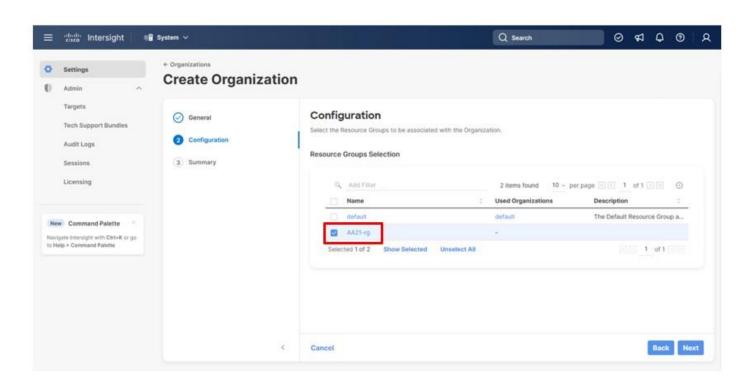
This procedure creates an Intersight organization where all Cisco Intersight managed mode configurations including policies are defined. To create a new organization, follow these steps:

- Step 1. Log in to the Cisco Intersight portal.
- Step 2. At the top, select System. On the left, click Settings (the gear icon).
- Step 3. Click Organizations in the middle panel.
- Step 4. Click + Create Organization in the top-right corner.

**Step 5.** Provide a name for the organization (for example, AA21) and click **Next**.

=	duale Intersight	¶₿ System ∨		Q Search	Ø	ø	٥	0	8
0 0	Settings Admin ^	Create Organization							
	Targets Tech Support Bundles Audit Logs Sessions Licensing	<ul> <li>General</li> <li>Configuration</li> <li>Summary</li> </ul>	General Add a name and description for the organization.	0					
Nec	Command Palette     Source of the second secon		Cancel	<i>A</i>				Next	

**Step 6.** Select the **Resource Group** created in the last step (for example, AA21-rg) and click **Next**.



**Step 7.** Review the **Summary** and click **Create**.

# **Onboarding to Intersight**

The UCS domain contained within the Fabric Interconnects will be added directly to the account as targets. The other infrastructure components will be onboarded as targets through the Intersight Assist Appliance after it has been deployed, covered later in the Management section.

# Procedure 1. Set Up Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects

The Cisco UCS fabric interconnects must be set up to support Cisco Intersight managed mode. When converting an existing pair of Cisco UCS fabric interconnects from Cisco UCS Manager mode to Intersight Managed Mode (IMM), 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. You are encouraged to make a backup of you existing configuration. If a software version that supports Intersight Managed Mode (4.1(3) or later) is already installed on Cisco UCS Fabric Interconnects, do not upgrade the software to a recommended recent release using Cisco UCS Manager. The software upgrade will be performed using Cisco Intersight to make sure Cisco UCS X-series firmware is part of the software upgrade.

**Step 1.** Configure Fabric Interconnect A (FI-A) by connecting to the FI-A console. On the Basic System Configuration Dialog screen, set the management mode to Intersight.

Asco UCS Fabric Interconnect A Enter the configuration method. (console/gui) ? console
The Fabric interconnect will be configured in the intersight managed mode. Choose $(y/n)$ to proceed: y
Enforce strong password? (y/n) [y]: Enter
Enter the password for "admin": <password></password>

```
Confirm the password for "admin": <password>
 Enter the switch fabric (A/B) []: A
 Enter the system name: <ucs-cluster-name>
 Physical Switch Mgmt0 IP address : <ucsa-mgmt-ip>
 Physical Switch Mgmt0 IPv4 netmask : <ucs-mgmt-mask>
 IPv4 address of the default gateway : <ucs-mgmt-gateway>
   DNS IP address : <dns-server-1-ip>
 Configure the default domain name? (yes/no) [n]: n <optional>
Following configurations will be applied:
   Management Mode=intersight
   Switch Fabric=A
   System Name=<ucs-cluster-name>
   Enforced Strong Password=yes
   Physical Switch Mgmt0 IP Address=<ucsa-mgmt-ip>
   Physical Switch Mgmt0 IP Netmask=<ucs-mgmt-mask>
   Default Gateway=<ucs-mgmt-gateway>
   DNS Server=<dns-server-1-ip>
 Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

**Step 2.** 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.

**Step 3.** 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.

```
Cisco UCS Fabric Interconnect B
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 cluster. Continue (y/n) ? y
  Enter the admin password of the peer Fabric interconnect: cpassword>
   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: <ucsa-mgmt-ip>
   Peer Fabric interconnect Mgmt0 IPv4 Netmask: <ucs-mgmt-mask>
    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
  Physical Switch Mgmt0 IP address : <ucsb-mgmt-ip>
  Local fabric interconnect model(UCS-FI-6536)
  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): yes
```

```
Procedure 2. Claim Cisco UCS Fabric Interconnects in Cisco Intersight
```

**Note:** With the initial Basic System Configuration Dialog previously completed for the fabric interconnects, log into the Fabric Interconnect A Device Console using a web browser to capture the Cisco Intersight connectivity information.

**Step 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 into the device.

	cisco DEVICE CONSOLE AA21-6536			© B
	SYSTEM NFORMATION DEVICE CONNECTOR INVENTORY	DIAGNOSTIC DATA		
	Fabric Interconnect A (Primary)		Fabric Interconnect B (Sebordinate)	
	Management IPs	192 168 168 11	Management Ps	192 168 168 12
	Madei	UCS F1-6536	Model	UC8-F1-6536
,	Secul		Senal	
	Firmware Version	9.3(5)442(36)	Fermilian Version	9.3(5)(42(36)
	Available Memory	23.22 MB	Available Memory	23.22 MB
	Total Memory	3131MB	Tatal Memory	31.31 MB

**Step 2.** Under **DEVICE CONNECTOR**, the current device status will show "Not claimed." Note or copy the **Device ID** and **Claim Code** information for claiming the device in Cisco Intersight.

EXERCISE       DECISE CONNECTION       NENTORY       DEMONSTRATE ALLOW DOINTS    The Device Connector is an entreaded management controller that madies the capabilities of Caclo Intersigit, a cloud based management plathors. For stealed information atout controllering the device connector	cisco DEVICE CONSOLE AA21-8536	0 B
Device Connector Device Conne		
Device Connector     Not Claimed     The connectors to the Cisco Intersignt Portal is successful, but device is still not claimed. To claim the device open Cisco Intersignt, create a Copen Intersignt.		etailed information about configuring the device connector,
Image: Connector     Internet     Internet <td>Device Connector</td> <td>② Settings   〇 Refresh</td>	Device Connector	② Settings   〇 Refresh
	Internet     Internet	Cam Code 0346D588239F

- Step 3. Log in to Cisco Intersight.
- Step 4. At the top, select System. On the left, click Administration > Targets.
- Step 5. Click Claim a New Target.
- Step 6. Select Cisco UCS Domain (Intersight Managed) and click Start.

≡ diada Intersight	n System 🗸			Q Search		0	₽	٥	0	٩
Cece Settings Admin Targets Tech Support Bundles	+ Targeta Claim a New Tar	get	Select Targ	et Type						
Audit Logs Sessions Licensing		Iters Available for Claiming egories	Compute / Fabric	Cisco UCS Domain (Intersight Managed)	Cisco UCS Domain (UCSM Managed)	Î				
Navigate Intersight with Ctrl+K or go to Help > Command Palette		All     Cloud     Compute / Fabric     Hyperconverged	uterio esse Cisco UCS C890	Redfish Server						
		Hypervisor v	Platform Services	Cisco Intersight		÷				

**Step 7.** Copy and paste the Device ID and Claim Code from the Cisco UCS FI to Intersight.

Step 8. Select the previously created resource group and click Claim	m.
--	----

=	diala Intersight	📲 System 🗸					Q Search		0	\$	٥	0	R
0	Settings Admin	+ Targets Claim a New Ta	rget										
	Targets												1
	Tech Support Bundles	General											
	Sessions	Device ID *		Claim Code * 3346D588239F							0		
		Resource Groups											
Nev	Command Palette     super-super			ed. However, this sele t will be part of all Org									
						G Export	1 items found	10 - per page	1 of	100	0		
		🔄 Name			Usage			Description					
		C AA21-rg			AA21								
		Selected 1 of 1 Sho	w Selected Unse	elect All						1 of	1918		
		Back Cancel										Cla	im

On a successful device claim, Cisco UCS FI appears as a target in Cisco Intersight:

≡	الالمان Intersight				Q Search	. ⊘ .	A Q	0	R
0	Settings	Targets					Clai	m a New '	Target
Ű	Admin Admin Admin Admin Admin Admin Admin Admin Administration Administratio Administration Administration Administration Admi	All Targets      +     All Targets      +     Add Filter     Connection      (© Connected 1)	Top Targets by Types 7	Vendor 1 • Cisco Systems, In	Export 1 items found	10 – per page 📧	< 1		X
Nav	ew Command Palette × rigate Intersight with Ctrl+K or go telp > Command Palette	Name           AA21-6536	Status :	Type : Intersight Managed Domain	Claimed Time : a few seconds ago	Claimed By rci@cisco.com	< 1	≎ ; • of 1 ⊇ [	

**Step 9.** Log in to the web GUI of the Cisco UCS fabric interconnect and click the browser refresh button.

The fabric interconnect status is now set to Claimed:

cisco DEVICE CONSOLE AA21-6536		0	G
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. Fr please visit Help Center	r detailed information about configuring the dev	ice connecto	or,
Device Connector	Settings	🗇 Refres	sh
ACCESS LICOR ALLOW CONTROL Device Connector Intersight Internet Intersight 1.031-064	Device ID Claimed to Account RTP-Adaptive-Solutions O Unclaim	3 6	

#### Procedure 3. Upgrade Fabric Interconnect Firmware using Cisco Intersight

**Note:** If your UCS 6536 Fabric Interconnects are not already running firmware release 4.3(1), upgrade will be required to support M7 servers.

**Note:** If Cisco UCS Fabric Interconnects were upgraded to the latest recommended software using Cisco UCS Manager, this upgrade process through Intersight will still work and will copy the X-Series firmware to the Fabric Interconnects.

Step 1. Log into the Cisco Intersight portal.

**Step 2.** At the top, from the drop-down list to select **Infrastructure Service** and then select **Fabric Interconnects** under Operate on the left.

**Step 3.** Click the ellipses "..." at the end of the row for either of the Fabric Interconnects and select **Up-grade Firmware**.

Step 4. Click Start.

tion.

**Step 5.** Verify the Fabric Interconnect information and click **Next**.

Step 6. Enable Advanced Mode using the toggle switch and uncheck Fabric Interconnect Traffic Evacua-

**Step 7.** Select the **4.3(2)** release from the list and click **Next**.

**Step 8.** Verify the information and click **Upgrade** to start the upgrade process.

**Step 9.** Watch the Request panel of the main Intersight screen as the system will ask prompt for user permission before upgrading each FI. Click on the Circle with Arrow and follow the prompts on the screen to grant permission.

**Step 10.** Wait for both the FIs to successfully upgrade.

# Cisco UCS Domain Setup

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 configured 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.

Procedure 1.	Configure a Cisco UCS Domain Profile
Step 1.	Log into the Cisco Intersight portal.
Step 2. Profiles.	At the top, from the drop-down list to select Infrastructure Service. Then, under Configure, selec
Step 3.	In the main window, select UCS Domain Profiles and click Create UCS Domain Profile.

=	dealer Intersight	🎉 Infrastructure Service 🗸			Q Search		0	\$	٥	0	<u> </u>
*	Overview	Profiles									
0	Analyze	HyperFlex Cluster Profiles UCS Chassis Profiles	UCS Domain Profiles	UCS Server Profiles							
0	Operate Servers Chassis	At UCS Domain Pr., 0 +							Domai		-
	Fabric Interconnecta	A Add Filter     Name	: Status	UCS I Fabric Interconnect A	C Expert Domain Fabric Interconnect 8	0 items found Last Update	10 - per p	age (-)	23 O M	:	
	HyperFlex Clusters Integrated Systems			NO ITEMS AVAILABLE							
0	Configure	·							0.01	0	
	Profiles										

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

=	cisco Intersight	🔆 Infrastructure Service 🗸 Q. Search		Ø	₽	φ	0	R
\$ 0	Overview Analyze	<ul> <li>← Profiles</li> <li>Create UCS Domain Profile</li> </ul>						
0	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters	UCS Domain Profile A UCS domain profile streamlines fabric interconnect assignment, port, and fabric interconnect configuration to eliminate failures caused by inconsistent configuration.						
<u>ە</u> ر	Integrated Systems Configure Profiles Templates Policies	UCS Domain Assignment Create a Fabric Interconnect pair and assign to a domain profile immediately or later.	>					
Nav	Command Palette     Sate Intersight with Ctrl+K or graps     Command Palette	About UCS Domain Profile Creation     Do not show this page again						
		Cancel					Star	t

# Procedure 2. UCS Domain Profile General Configuration

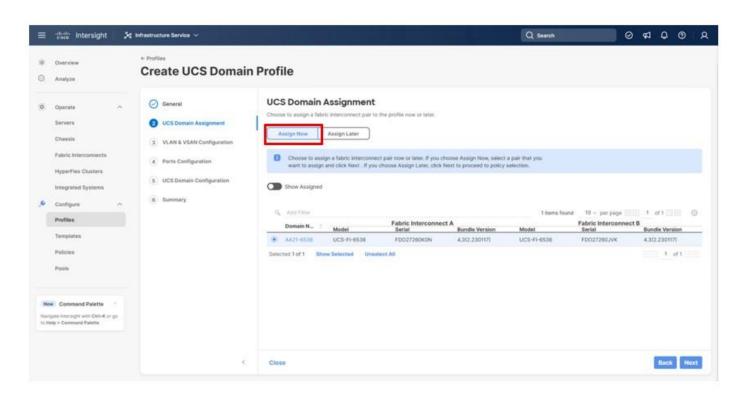
- **Step 1.** Choose the organization from the drop-down list (for example, AA21).
- **Step 2.** Provide a name for the domain profile (for example, AA21-6536-Domain-Profile).
- **Step 3.** Provide an optional Description.

=	cisco Intersight	🍂 Infrastructure Service 🗸		Q Search	0 4 0	۲	۹
*	Overview Analyze	+ Profess Create UCS Domain					
0	Operate ^  Servers Chassis Fabric Interconnects Integrated Systems	Ceneral     Control     UCS Domain Assignment     VLAN & VSAN Configuration     Ports Configuration     SUCS Domain Configuration	General Add a name, description and tag for the UCS domain profile. Drighnization * AA21 *				
	Configure ^  Profiles Policies Pools	(B) Summary	Set Tags Description				
Net	Command Palette     Service with Convex or go     Command Palette						
			Close		Bac	k Ne	et

Step 4. Click Next.

# **Procedure 3.** UCS Domain Assignment

**Step 1.** Assign the Cisco UCS domain to this new domain profile by clicking **Assign Now** and selecting the previously added Cisco UCS domain (for example, AA21-6536).



#### Step 2. Click Next.

# Procedure 4. VLAN and VSAN Configuration

In this procedure, a single VLAN policy is created for both fabric interconnects and two individual VSAN policies are created because the VSAN IDs are unique for each fabric interconnect that will be applied to the UCS Domain.

#### **VLAN Configuration**

Step 1. Click Select Policy next to VLAN Configuration under Fabric Interconnect A.

$\equiv$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$	😂 infrastructure Service 🛩		Q Search	0 4 0 0 A
律 Overview ① Analyze	+ Profiles Create UCS Domain	Profile		
0.     Operate     ^       Servers     Chassis       Chassis     Fabric Interconnects       HyperFire Chasters     Integrated Systems       Integrated Systems     ^       Profiles     _       Templates     _       Policies     _	Coneral CUCS Domain Assignment CUCS Domain Configuration CuCs Domain CuCs Domain CuCs Domain Cuc Summary	VLAN & VSAN Configuration Create or select a policy for the fabric interconnect pail.		Select Policy @ Select Policy @ Select Policy @ Select Policy @
Podis Here: Command Palette  Nonigate Interruptin with CMI+K or go to Help > Command Palette	×	Close		Back Next

**Step 2.** In the pane on the right, click **Create New**.

**Step 3.** Verify the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-VLAN).

=	disce Intersight	🎉 Infrastructure Service \vee		Q Search	0 4 0 0 A
# ©	Overview Analyze	Profiles > Create UCS Domain Profile Create VLAN			
0	Operate ^ ^ Servers ^ / Chassis / Pabric Interconnects / HyperFiles Clusters / Coofigure / Poofiles / Pools / Pools /	General     Zentry Details	General Add a name, description and tag for the policy. Criganization * Add		
Ner	Command Palette				
		e	Cancel		Next

- Step 4. Click Next.
- Step 5. Click Add VLANs.
- **Step 6.** Provide a name and VLAN ID for the native VLAN.

=	tisco Intersight	34 Infrastructure Service ~	Q Search	0	\$3	٥	۲	۹
*	Overview Analyze	Profiles > Create UCS Domain Profile Create VLAN						
ø	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Add VLANs Add VLANs to the policy	VLANs should have one Multicast policy associated to 8 Configuration Name / Prefix * Native YUN VLAN IDS * 2					
Nev			Auto Allow On Uplinks  Come Enacte VLAN Sharing  Multicast Policy* Select Policy B					
		Cancel					K	su i

- Step 7. Make sure Auto Allow On Uplinks is enabled.
- Step 8. To create the required Multicast policy, click **Select Policy** under **Multicast\***.

=	2000 Intersight	🍂 Infrastructure Service 🗸		Q Search	0 4 0 0	0 A
*	Overview Analyze	Profiles > Create UCS Domain Profile Create VLAN				
9.	Servers Chassis	Add VLANs	VLANs should have one Multicast policy associated to it			
,e		•	Configuration Name/Prefix * VLAN ID5 * Name-VLAN = 2 Auto Adow On UpleAs =			
	Profiles Templates Policies Pools		Auto Adow On Optimas      O     Enable VLAN Sharing . 0      Multicast Policy *     Select Policy ®			
Ner	Command Palette     Jarle Intersight with Colf+K or g     leg > Command Palette					
		Cancel				Add

- **Step 9.** In the window on the right, click **Create New** to create a new Multicast Policy.
- **Step 10.** Provide a Name for the Multicast Policy (for example, AA21-MCAST).
- **Step 11.** Provide an optional Description and click **Next**.
- **Step 12.** Leave the default settings selected and click **Create**.

≡	elision Intersight 🍂	Infrastructure Service $$		Q Search	⊘ ⊄	ı Q	0	ዾ
۱ ان ان	Overview Analyze	Profiles > Create UCS Domain Profile > Create Multicast Poli						
0	Operate  Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure  Profiles Templates Policies	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy details Multicast Policy Snooping State  Querier St					
Na	Pools Command Palette Agate Intersight with Ctri-K or go telp > Command Palette	<	Cancel			Back	Creat	te

Step 13. Click Add to add the VLAN.

**Step 14.** Add the remaining VLANs by clicking Add VLANs and entering the VLANs one by one. Reuse the previously created multicast policy for all the VLANs

**Step 15.** Select **Set Native VLAN ID** and enter the VLAN number (for example, 2) under VLAN ID.

Overview Analyze	Profiles  Create UCS Domain Profile Create VLAN									
* Overview	<ul> <li>General</li> <li>Policy Details</li> </ul>	0.000					Same food 10 - our oue	910 1 <b>4</b> 10		
			VLAN ID	Name	Sharing Type					
				0.475020 1.1. 	None		2	Yes		
	Create VLAN     © General     VLANS     © Briery Details     VLANIB     VLANIB     VLANIB     Name     Sitems found     1 of 1     1 of 1     1 of 1     I of 1              I of 1									
Profiles		Teste U2 Domain Profile         test Domai								
Templates			1000	vMotion_1000	None		AA21-MCAST	Yes		(e)
Policies			1100	VM-Traffic_1100	None		AA21-MCAST	Yes	1444	ee -
Pools			LAN ID	ngei						
ights Intersight with Ctrl+K or go		2				2				0

**Step 16.** Click **Create** in the bottom right to finish creating the VLAN policy and associated VLANs.

**Step 17.** Click **Select Policy** next to VLAN Configuration for Fabric Interconnect B and select the same VLAN policy.

# VSAN Configuration

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

**Step 2.** Verify the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-VSAN-A).

Note: As mentioned previously, a separate VSAN-Policy is created for each fabric interconnect.

Step 3. Click Next.

Step 4. Optionally, enable Uplink Trunking.

**Step 5.** Click **Add VSAN** and provide a name (for example, VSAN-A), VSAN ID (for example, 101), and associated Fibre Channel over Ethernet (FCoE) VLAN ID (for example, 101) for SAN A.

Step 6. Set VLAN Scope as Uplink.

= the Intersight 🔅	Infrastructura Service 🛩		Q: Search	© ¢1 Q ® A
* Overview O Analyze	Profiles > Create UCS Contain Profile Create VSAN			
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clustery</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Paticies</li> </ul>	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Patale Add per Add VSAN  Filme* VSAN Boope  VSAN Boope  Storage & Uplink  VSAN Boope  Storage & Uplink  Storage & Storage & Storage  Storage & Storage & Storage & Storage & Storage  Storage & S	0 items found 16 - per VSAN Scope	page 20 0 of 0 2 2 0 FCGE VLAN ID
Pools  Rec Command Palette  Assigns interrupte anth Chlink or go to Heig > Command Palette		Cancel		Back Cruste

Step 7. Click Add.

**Step 8.** Click **Create** to finish creating the VSAN policy for fabric A.

**Step 9.** Repeat steps 1 – 8 to create a new VSAN policy for SAN-B. Name the policy to identify the SAN-B configuration (for example, AA21-VSAN- B) and use appropriate VSAN and FCoE VLAN IDs (for example, 102).

**Step 10.** Verify that a common VLAN policy and two unique VSAN policies are associated with the two fabric interconnects.

Overview     Analyze     Operate	← Profiles Create UCS Domain			
	General			
Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Templates Policies Pools	<ul> <li>UCS Domain Assignment</li> <li>VLAN &amp; VSAN Configuration</li> <li>Ports Configuration</li> <li>UCS Domain Configuration</li> <li>Surgers</li> </ul>	VLAN & VSAN Configuration         Create or select a policy for the fabric interconnect pair. <ul> <li>Fabric Interconnect A 2 of 2 Policies Configured</li> <li>VLAN Configuration</li> <li>VSAN Configuration</li> <li>VLAN Configuration</li> <li>VLAN Configuration</li> <li>VLAN Configuration</li> <li>VLAN Configuration</li> <li>VLAN Configuration</li> <li>VLAN Configuration</li> </ul>	×     2     ∞     AA21-VLAN     1       ×     2     ∞     AA21-VSAN-A     1       ×     2     ∞     AA21-VLAN     1       ×     2     ∞     AA21-VLAN     1       ×     2     ∞     AA21-VSAN-B     1	
New Command Palette × Navigate Interright with Ctri-K or go to Help > Command Palette		Close	Back	Next

#### Step 11. Click Next.

# **Procedure 5.** Ports Configuration

This procedure creates the Ports Configuration policies for Fabric Interconnect A, and these steps will be repeated for Fabric Interconnect B with certain specified differences. Using separate policies provides flexibility when port configuration (port numbers or speed) differs between the two FIs.

**Note:** Use two separate port policies for the fabric interconnects. When configuring Fibre Channel, two port policies are required because each fabric interconnect uses a unique Fibre Channel VSAN ID.

Step 1. Click Select Policy for Fabric Interconnect A.

$\equiv$ $\stackrel{+++}{\underset{iuss}{\longrightarrow}}$ Intersight	Je infrastructure flavokse 🗸		Q Seath	0 4 0 0 A
@ Outview	Create UCS Domain	n Profile		
Operate     Arrows     Arrows     Chanals     Autric Insectionauts     HyperFiles Chanales     Virtualization     Insegrated Systems     C     Analyze     Analyze     Keylows     Keylows     Keylows     Keylows     Keylows     Keylows     Keylows     Keylows     Keylows	General     UCS Domain Assignment     VLAN & VLAN & VLAN     VLAN & VLAN Configuration     Parts Configuration     UCS Domain Configuration     Generacy	Ports Configuration Create or select a port police for the Tealer Interconnect part.  Configure parts by creating or selecting a party:  Partic Interconnect & Not Configured  Partic Interconnect & Not Configured		Seriest Postey S
Configure     Note     Configure     Note     Contract     Contrat     Contrat     Contrat     Contrat     Contrat     Contrat		Paris Configuration		Satest Policy 2

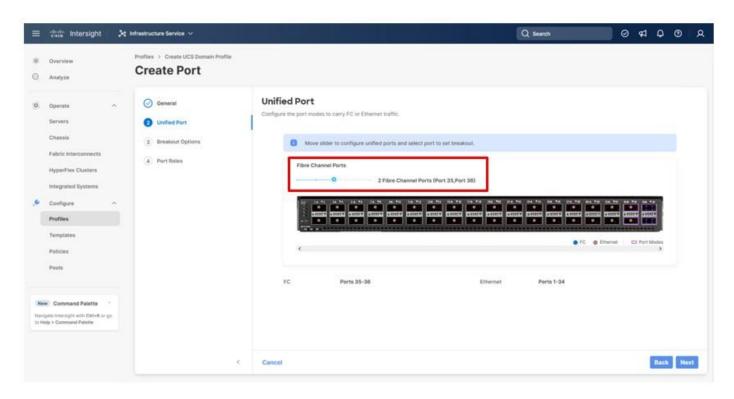
**Step 2.** Click **Create New** in the pane on the right to define a new port configuration policy.

**Step 3.** Verify that the correct organization is selected from the drop-down list (for example, AA02) and provide a name for the policy (for example, AA21-6536-Port-A). Select the UCS-FI-6536 Switch Model.

≡	disco Intersight	📚 Infrastructure Service 🗸		Q Search	ø	¢۵	Q (	Ð	ዾ
*	Overview	Profiles > Create UCS Domain Profile							
Nev	Operate     ^       Servers        Chassis        Habris Interconnects        HyperFlex Clusters        Integrated Systems        Configure     ^       Porfees        Policies        Policies        Policies        Policies        Policies        Policies        Policies        Policies        Policies        Policies	<ul> <li>Contral</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>	Ad a name, description and tag for the policy.   Organization *   Robids Feet   Name *   Ad214505 FornA   SetCh Model *   UC5-FR4505						
		<	Cancel					Next	

Step 4. Click Next.

**Step 5.** Move the slider to set up unified ports. In this deployment, the last two ports were selected as Fibre Channel ports as 4x32G breakouts. Click **Next**.



**Step 6.** If any Ethernet ports need to be configured as breakouts, either 4x25G or 4x10G, for connecting C-Series servers or a UCS 5108 chassis, configure them here. In the list, select the checkbox next to any ports that need to be configured as breakout or select the ports on the graphic. When all ports are selected, click **Configure** at the top of the window.

≡ ded: Intersight	🔆 Infrastructure Service 🗸			Q Search	0 4 0	•
lt Overview D. Analyze	Profiles > Create UCS Domain Profile Create Port					
<ul> <li>Operate</li> <li>Servera</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFitex Clusters</li> <li>Integrated Systems</li> </ul>	Ceneral Cubified Port Breakout Options  A Port Roles					
Configure		e		• fc • t	Dhemet C3 Port Modes	
Configure / Profiles Templates Policies Posts		Port           Port 3	Type Ethernet	Speed Breaks	, o	
Profiles Templates Policies Pools		Port	177	Speed Breaks	, o	
Profiles Templates Policies		Port     Port 1     Port 2     Port 3	Ethernet Ethernet Ethernet	Speed Break 	, o	

😑 📲 enco	🖇 Infrastructure Service 🤝			Q Search	0 4 4 6	0   A
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Profiles  Create UCS Domain Profile Create Port					
0. Operate	General	Ethernet Fibre Char	nel			î
Servers Chassis	Unified Port	Configure Selecte	Ports Port 5 Clear Selection			
Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles	Breakout Options     A Port Roles	will result in the roles and port of Selected Ports Port	peed of an existing FC breakout port, deletion of previously configured port hannel roles.	00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       0     00     00     00     00     00     00     00       0     00     00     00     00     00     00     00		
Templates					©	
Policies			Cancel Set	Speed Breakout P	orts	
Pools		Port 2	Ethernet			
		Port 3	Ethernet			
New Command Palette		Port 4	Ethernet			
Navigate Intersight with Ctrl+K or go to Help > Command Palette		Port 5	Ethernet			
		Port 6	Ethernet	17 ( 17 )		
		Port 7	Ethernet			~
	×	Cancel			Back	Next

In the Set Breakout popup, select either 4x10G or 4x25G and click Set.

**Step 8.** Under Breakout Options, select **Fibre Channel**. Select any ports that need the speed changed from 16G to 32G and click **Configure**.

**Step 9.** In the Set Breakout popup, select 4x32G and click **Set**.

Step 7.

≡ diado Intersight .≯	Infrastructure Service  Profiles  Create UCS Domain Profile			Q Search	⊙ � ♀ ♀ ⊘
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Create Port				
Operate     Servers     Chassis     Fabric Interconnects     HyperFlex Clusters     Integrated Systems      Configure     Profiles     Templates	<ul> <li>General</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>	will result in the roles and port of Selected Ports Port 3	nel nel need of an existing FC breakout port, deletion of previously configured port nannel roles.		A 4 0 A 40 A 40 B 10 F 1 A 40 A 40
Policies Pools		Port	Cancel Set	Speed	© Breakout Ports
New Command Palette		Port 36	FC	16G	Port 36/1, Port 36/2, Port 36/3, Por
Navigate Intersight with Ctrl+K or go to Help > Command Palette		Port 35	FC	16G	Port 35/1, Port 35/2, Port 35/3, Por
to Help > Command Palette	¢	Selected 1 of 2 Show 1	Selected Unselect All		Back

© 2024 Cisco and/or its affiliates. All rights reserved.

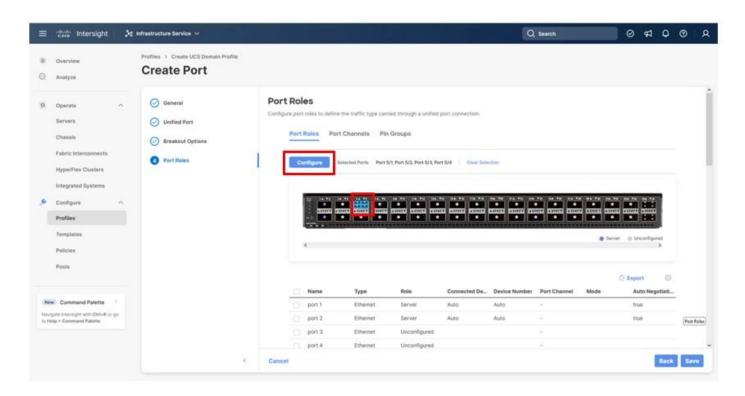
Page 62 of 367

# Step 10. Click Next.

**Step 11.** In the list, select the checkbox next to any ports that need to be configured as server ports, including ports connected to chassis or C-Series servers. Ports can also be selected on the graphic. When all ports are selected, click **Configure**. Breakout and non-breakout ports cannot be configured together. If you need to configure breakout and non-breakout ports, do this configuration in two steps.

=	the Intersight	🎉 Infrastructure Service 🛩							Q	Search		0	41	٥	0	۹
* ©	Overview Analyze	Profiles > Create UCS Domain Profile Create Port														
9	Servers Chessis Fabric Interconnects HyperFiex Clusters Integrated Systems	<ul> <li>General</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>		port roles ort Role Contain	s Port Cr	annels Pir	Port2 Clear Selection	Tean 14 HA 19 HA 19 H 14 EXEL 14 EXEL		IN ADDIS ADDIS				d d		
	Pools			Nar	me	Туре	Role	Connected De	Device Number	Port Channel	Mode	G Expe	rt .to Nego	©		
He	Command Palette			🖬 por	11	Ethernet	Unconfigured			3				_		
	pate Intersight with Cell+K or ge rtp > Command Palette			por	12	Ethernet	Unconfigured			Si						
				por	13	Ethernet	Unconfigured			12						
				por	4	Ethernet	Unconfigured			8						Ŷ
		×	Cancel											Back	Sev	ra

- **Step 12.** Specify the Role of Server for the selected IFM ports.
- Step 13. Click Save.
- **Step 14.** Select any breakout ports intended for C-Series and click **Configure**.



- **Step 15.** Repeat the selection of *Server* for the Role and click **Save**.
- Step 16. Click the **Port Channels** tab under Port Roles.
- Step 17. Click Create Port Channel.

≡ diada Intersight 🔀	Infrastructure Service 🗸					Qs	arch	0	¢1 I	0 0	A
<ul> <li>Overvlew</li> <li>Analyze</li> </ul>	Profiles > Create UCS Domain Profile Create Port										
Operate     Servers     Chasals     Fabric Interconnects     HyperFiles Clusters     Integrated Systems     Configure     Profiles     Templates     Policies	<ul> <li>General</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>	Create Port C	Port Channels	Pin Groups				10 No 10 10			~
Pools  New Command Patette  Reviser Interview with Chill & Crigo In Help > Command Patette		2.1			ID Role NO ITEM	0 items fo :			0 0 0	0	
		Cancel								lack S	Save

**Step 18.** To create the network uplinks to the Nexus 93600CD-GX switches, leave the Role as **Ethernet Uplink Port** selected.

**Step 19.** Specify a Port Channel ID (example 11). Specify an Admin Speed if the upstream ports require it, otherwise leave it as **Auto**.

= their Intersight 🔉 infrastructur	* Service ~	Q Search 🛛 🖓 4 Q 💿	۹
IE Overview	Create UCS Domain Profile		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> </ul>	Configuration Configuration The combined maximum number of Ethernet Uplink, FCoE Uplink, and A is 12 and the maximum number of FC port channels permitted is 4.	splance port channels permitted	
Enlegrated Systems Configure Profiles Templates Policies Pools	Role Ethernet Uptrik Port Channel - Port Channel ID • 11 C © Admin Speed Admin Speed Lipse Ethernet Network Oroup 0 Select Portory 3		
New Command Palette " Novigen Interview with CBAX or ga to Help > Command Palette	Flow Control Select Policy (1) Link Aggregation Select Policy (1)		2
Canoo	и.	Sav	

**Note:** Ethernet Network Group, Flow Control, and Link Aggregation policies for defining a disjoint Layer-2 domain or fine tune port-channel parameters can be configured here, but these policies were not used in this deployment and system default values were utilized.

**Step 20.** Scroll down if Link Control and Select Member Ports is not visible within the **Create Port Channel** dialogue, click **Select Policy** under Link Control, and then select **Create New** in the upper area of the right-side pane.

=	disclar Intersight	×	Infrastructure Service 🐱	Q Search	0	\$ ٥	۲	R
*	Overview Analyze		Profiles  Create UCS Domain Profile Create Port					
0	Operate Servers Chaosis	~		Here Control Select Pullcy II				*
,0	Fabric Interconnects HyperFlex Clusters Integrated Systems Configure			Link Aggregation Select Pulicy S Link Control Select Pulicy S				Port Rak
	Profiles Templates Policies Pools			Select Member Parts  FC or Ethernet ports with unconfigured role are available for port channel creation.				1
Ner	Command Palette     Gate Hensight with Christian get     by - Command Palette							
			Cancel	0			Sav	•

**Step 21.** Provide a name for the policy (example, AA21-UDLD-Link-Control), and click **Next**.

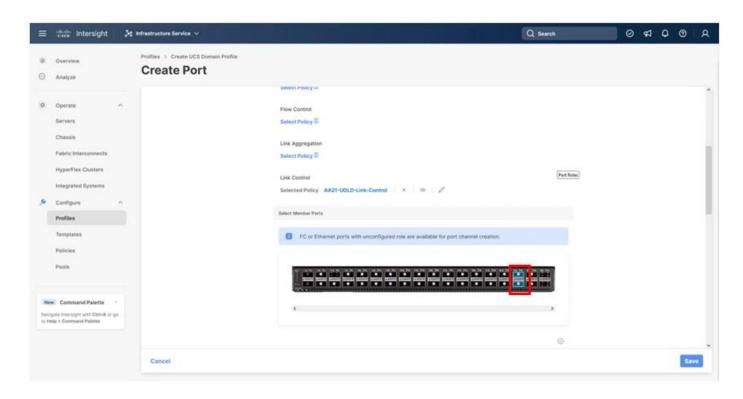
=	their Intersight	34 Infrastructure Service 🗠		Q Search	0	\$ ٥	۲	۹
*	Overview Analyze	Profiles > Create UCS Domain Profile > Cre Create Link Control						
0	Operate ^  Servers Chassis Fabric Interconnects HyperFlex Chasters Integrated Systems	Policy Details     Policy Details	General Add a name, description and tag for the policy. Organization * Add a Name * Add to the second secon					
	Configure ^  Profiles Templates Policies Pools		Set Tags Description					
Not	Command Palette  galet Interrupte with Christ or po- table > Command Palette							
		5	Cancel				No	et

**Step 22.** Leave the default values selected and click **Create**.

**Step 23.** Select the ports connected to the upstream Nexus switches (example, port 31 and 32).

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 66 of 367



Step 24. Click Save.

# **Procedure 6.** Configure FC Port Channel

This procedure will create the Fibre Channel Port Channel for Fabric Interconnect A, and these steps will later be repeated for Fabric Interconnect B with certain specified differences. A difference is needed for these Fibre Channel Port Channel configurations because of the use of a unique Fibre Channel VSAN ID.

**Step 1.** Configure a Fibre Channel Port Channel by selecting the **Port Channel** in the main pane again and clicking **Create Port Channel**.

their Intersight	S Indirecture Service ~			Q Seeth	0 4 0 00 0
Overview	Profiles - Create UCS Danais Profile Create Port				
Openins ^ Bervers Chassis Fatrix Interconnector HyperFlas Chasters Vertualization Marguet Dystems Anatys Configure Sequence Templares	Ourneral     Unities Part     Ori     Unities Part     President Options     President Solution				The first sector of the fi
Patria		2.01 0	Role     To Role     To Channel     To Channel	1 Rema Round 10 - Ports Port 31, Port 32	(C) (C) Physical Action (C)
Command Palette			A Company Open visit Comma	1013,00132	1 of 1
		4 Cancel			Rect. Sev

Step 2. In the drop-down list under Role, choose FC Uplink Port Channel.

	the Intersight	>t Infrastructure Service ∨	Q. Search (	9 9	n 0	0	R
*	Overview Analyze	Profiles > Create UCS Domain Profile Create Port					
0	Servers Chassis Fabric Interconnects		Create Port Channel Configuration The contineed maximum number of Ethernet Uplink, FCoE Uplink, and Applance port channels permitted is 12 and the maximum number of FC port channels permitted is 4.				Î
	HyperFiles Clusters Integrated Systems Coofigure Profiles Templates Policies Pools		Role Ethernet Uplink Port Channel FC Uplink Port Channel Admin Speed Admin Speed Admin Speed Admin Speed Select Port Channel Ethernet Network Group © Select Portog				
Nev	Command Palette		Flow Control Select Pullcy 3				v
		Cancel				Gar	Ye

**Step 3.** Provide a port-channel ID (for example, 101), select a value for Admin Speed (for example, 32Gbps), and provide a VSAN ID (for example, 101).

=	the Intersight	34 1	disatustus Service 👻				Q Seath	0 #	0.000	۲	۹
*	Overview		Prefies > Create UCS Screate Prefie Create Port								
-	Servers Chassis Fabric Interconnects HyperFlex Chasters Virtualization Integrated Dystems Analysis Explorer Inter			Is 12 and there Rule PC spins Part Channel Part Cristion 2011 301 Sensit Montee Parts PC or Ethermote	nivinum number of Etherm warmen number of Ethern Distance of Ethern Distance of Ethern Distance of Ethern Distance of Ethern	NI D <sup>1</sup>					
			Cencel							Sav	

**Step 4.** Select ports (for example, 35/1,35/2,35/3,35/4).

😑 🚓 intersight 🎝 intranscense tervice 🗸	Q. seed. 0 47 Q. 0 47 Q
Overview     Profiles = Create UCS Duraite Prof     Create Port	
Operate     O     Servers     Descript     Descript     Patrici: bitansconnectin     HyperFiles Displayme     Virsunitation     steagrated Dynkees	Cretate Port Channel Configuentian The considered maintains number of Ethernet Lightine, Food Lightine, and Appliance port channels permitted In 12 and the maintains number of FC port channels permitted is 4. Refer Refer Capable For Channel
Analyse     Explorer     Explorer     Fordiare      Profiler      Profile      Profile	Pert Channel D* Admin Epsed VEAN D* 301 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Conversant Painties Records: Intercord Painties to trace - Constant Painties	Charter Lipsk For Charter      Charter      Charter      Charter Lipsk For Charter
Cancel	port 35/1         FC         Unconfiguret         320           R         port 35/2         FC         Unconfiguret         320

Step 5. Click Save.

**Step 6.** Verify the port-channel IDs and ports after both the Ethernet uplink port channel and the Fibre Channel uplink port channel have been created.

	dece Intersight	🔆 Infrastructure Service 🗸			Q Search	⊙ ⊄ Q <b>@</b>	0	۹
*	Overview	Profiles > Create UCS Domain Profile Create Port						
0	Servers Chassis Fabric Interconnects HyperFlex Clusters Virtualization Integrated Systems Analyze Explorer New	<ul> <li>General</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>		Pin Groups				•
Na	Policies Pools Command Palette agate Interruph with Chink or go tags - Command Palette		<ul> <li>a</li> <li>a</li> <li>a</li> <li>c</li> <li>a</li> <li>c</li> <li>c</li></ul>	ID Role 11 Ethernet Uplink Port Channel 101 FC Uplink Port Channel	2 Items found 10 - po Ports Port 31, Port 32 Port 35/7, Port 35/2, Port 35	rpage 1 of 1 1 of 1	Save	, ř.

Step 7. Click Save to create the port policy for Fabric Interconnect A.

#### Procedure 7. Fabric Interconnect B Ports and Port Channel Configurations

**Step 1.** Repeat the steps in <u>Ports Configuration</u> and <u>Configure FC Port Channel</u> to create the port policy for Fabric Interconnect B including the Ethernet port-channel and the FC port-channel. Use the following values for various parameters:

- Name of the port policy: AA21-6536-Port-B
- Ethernet port-Channel ID: 12
- FC port-channel ID: 102
- FC VSAN ID: 102

**Step 2.** When the port configuration for both fabric interconnects is complete and looks correct, click **Next**.

#### Procedure 8. UCS Domain Configuration

Under UCS domain configuration, additional policies can be configured to set up NTP, Syslog, DNS settings, SNMP, QoS and the UCS operating mode (end host or switch mode). For this deployment, four policies (NTP, Network Connectivity, SNMP, and System QoS) will be configured, as shown below:

#### **Configure NTP Policy**

**Step 1.** Click **Select Policy** next to NTP and in the pane on the right, click **Create New**.

$\equiv$ $\frac{1}{1000}$ Intersight	k; Infrastructure Service 🗸		Q search	୍ କ <b>ଦ ଡ</b> ାନ
<ul><li>Øvervlew</li><li>Ø Analyze</li></ul>	+ Profiles Create UCS Domain	Profile		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> </ul>	General     UCS Domain Assignment     VLAN & VEAN Configuration	UCS Domain Configuration Select the compute and management policies to be associated with the fabric interconnect.		
HyperFlox Clusters Integrated Systems	Ports Configuration     UCS Domain Configuration     Summary	Management: 0 of 4 Policies Configured      NTP      Syslog		Select Policy 🗟
Profiles Templates Policies		Network Connectivity Share		Select Policy II Select Policy II
Pools		Network 0 of 2 Policies Configured     ■		
New Command Palette " Novigate Intersight with Cirl+K or ge to Help - Command Palette		System QoS. * Switch Control		Salect Policy E
		Close		Back Next

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-NTP).

Step 3. Click Next.

**Step 4.** Enable NTP, provide the first NTP server IP address, and select the time zone from the drop-down list.

**Step 5.** (Optional) Add a second NTP server by clicking + next to the first NTP server IP address.

=	the intersight 34	Infrastructure Service ~		Q Seen	<b>D</b> A
*	Overview	Profiles > Create UCS Domain Profile Create NTP			
Painto Interconnection HyperFlee Clusteres Intergrated Systems Analyze ~ Explored Inter	<ul> <li>General</li> <li>Price Desain</li> </ul>	Policy Details Act policy details  Act policy details  Intro Servers*  Intro Servers*  Intro Servers*  +	. At Partneys [ ] ht3 herer (Basialawa)		
Explored New Configure * Profiles Templates Publices Publ		Emergina Mara			
		2	Cantel	Bank C	reste

# Step 6. Click Create.

# **Configure Network Connectivity Policy**

**Step 1.** Click **Select Policy** next to Network Connectivity and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-NetConn).

Step 3. Click Next.

**Step 4.** Provide the appropriate DNS server IP addresses for the Cisco UCS domain.

Cisco Intersight 🏃 Infrastructure Service 🗸		Q Search	0 4 4 0
Overview Profiles > Create UCS Domain Profiles > Create Network			
Operate   Servers   Chastili   Fabric Interconnects   HyperFlex Clusters   Integrated Systems   Configure   Policies   Policies   Policies	Policy Details Add policy details Common Properties IPv4 Properties Performed IPv4 CRC Server 192:168:160:53	Al Platforme Mannatis IIPv4 CitAS Server 192:168:160.54	UCS Server IStantisland: UCS Domain
Command Palette   rigste Intercept with Chile K ar ge tage > Command Palette			
	< Cancel		discost discost

Step 5. Click Create.

**Configure SNMP Policy (Optional)** 

**Step 1.** Click **Select Policy** next to SNMP and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-SNMP).

Step 3. Click Next.

**Step 4.** Provide a System Contact email address, a System Location, and optional Community Strings.

Step 5. Under SNMP Users, click Add SNMP User.

$\equiv$ $\frac{1}{2}$ escolution $\frac{1}{2}$	Infrastructure Service 🐱		Q Search	0400
* Overslaw	Profiles > Create UCS Domain Profile Create SNMP	Add SNMP User	×	
10. Operate  Motograted Systems Configure	General     Policy Details	Add por Add por Security Level * AuthPriv		A Server (F)-Atlacted) UCE Domain UCE Daware
Profiles Templates Policies		Co Auth Password *		
Poets New Command Palette		Sys Auth Password Confirmation *	• • • Access	Community String 0
Navigati Internigit with Othek or pr 15) Help + Command Palette		Privacy Type AES		
		Privacy Password *	Auth Type	O Privacy Type
	e	Cancel	Add	Beck Cruste

**Step 6.** Optionally, add an SNMP Trap Destination (for example, the NDFC IP Address). If the SNMP Trap Destination is V2, you must add a **Trap Community String**.

=	cisco Intersight	📲 Infrastructure Service 🗸			Q Sear	ch 🥥	A 0 0 A
* 0	Overview Analyze	Profiles > Create UCS Domain Profile					
0	Operate Servers Chassis	Ceneral     Policy Details	Policy Details Add policy details	V AD PL	atforms UCS Server (Standalor	ne) UCS Server (FI-Attached) U	CS Domain UCS Chassia
	Fabric Interconnects HyperFlex Clusters Integrated Systems		Configuration System Contact *	System Location *			
,e	Configure Profiles Templates	Ô	snmp-admin@adaptive-solutions.local	<ul> <li>Cisco RTP, Building 9, AA2</li> </ul>	0	Access Community String	0
	Policies Pools		public SNMP Users	0			_
Nav	Command Palette gate Intersight with Ctrl+K or g	× 10	Add SNMP User				٥
to H	elp > Command Palette		Name	Security Level	Auth Type	Privacy Type	9
			snmp-admin	AuthPriv	NA	AES	
		<	Cancel				Back Create

Step 7. Click Create.

#### **Procedure 9.** Configure System QoS Policy

The System QoS policy will be adjusted to expand the capacity of the Ethernet uplinks to support jumbo frames. All Ethernet traffic is set within a common class of Best Effort in this design, which will have the MTU adjusted. Different strategies can be implemented for QoS giving weighted priorities, but any such effort would need to take care to match settings implemented upstream of the fabric interconnects.

**Step 1.** Click **Select Policy** next to System QoS\* and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-QoS).

Step 3. Click Next.

Step 4. Change the MTU for Best Effort class to 9216.

=	esco Intersight	🍂 Infrastructure Service 🗸		Q Search	0 \$ 0 0 A
* 0	Overview Analyze	Profiles > Create UCS Domain Profile Create System QoS			
8	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	General Ceneral Policy Dutails	Policy Details Add policy details This policy is applicable only for UCS Domains Configure Priorities  Platnum Platnum		
•			Cost Silver Bronze Best Effori Coll Weight Any C S	🖞 🗢 📑 Adam Pachet Janga. 🗢 😫	16 0 0
Navi	Command Palette		Channel CoS Weight	0 × 0 0 0 Mos Pacet Drops 0 22 0 × 0	



$\equiv$ $\frac{1}{c_{15co}}$ Intersight	🔆 Infrastructure Service 🗸		Q Search	2 @ 4 P @ X
<ul> <li>Øverview</li> <li>Analyze</li> </ul>	← Profiles Create UCS Domain	Profile		
0 Operate Servers Chassis Fabric Interconnects	C General G UCS Domain Assignment VLAN & VSAN Configuration Ports Configuration	UCS Domain Configuration Select the compute and management policies to be associated with the fabric interconnect.  Show Attached Policies (4)  Management 3 of 4 Policies Configured		
HyperFlex Clusters Integrated Systems Configure Profiles	G UCS Domain Configuration     (6) Summary	NTP Syslog Network Connectivity	× 2	AA21-NTP     Select Policy     AA21-NTP     AA21-NetConn
Templates Policies Pools		SNIMP  ^ Network 1 of 2 Policies Configured	x   Ø   @	
New Command Palette Navigate Intensight with Ctrl+K or g to Help > Command Palette		System QoS * Switch Control	×   2	AA21-QoS      Select Policy
	8	Close		Back Next



### Procedure 10. Deploy the UCS Domain Profile

**Step 1.** Verify that all the settings including the fabric interconnect settings, by expanding the settings and making sure that the configuration is correct.

=	Q Sea	reh Ø A Q Ø A
© Analyze ← Profiles Create UCS Domain	Profile	
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Poolicies</li> <li>Pools</li> <li>Configuration</li> <li>Summary</li> </ul>	Summary         Review the UCS domain profile details, resolve configuration errors and deploy the profile. <ul> <li>General</li> </ul> Ports Configuration       VLAN & VSAN Configuration       UCS Domain Configuration       Errors / Warr <ul> <li>Fabric Interconnect A</li> <li> <li>Fabric Interconnect B</li> </li></ul>	ings
New: Command Palette * Navigate Intersight with Chri+K or go to Help > Command Palette		
×.	Close	Back Deploy

Step 2. Click Deploy.

**Step 3.** Acknowledge any warnings and click **Deploy** again.

**Note:** The system will take some time to validate and configure the settings on the fabric interconnects. Log into the console servers to see when the Cisco UCS fabric interconnects have finished configuration and are successfully rebooted.

#### Procedure 11. 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.

**Note:** It takes a while to discover the blades for the first time. Watch the number of outstanding requests in Cisco Intersight:

	Overview Da	Re	quests									
)	Analyze He	* /	All Requests © +									
	ne		Q Status Suc	cess x Add Filter				× G Ex	port 53 items four	nd 10 v per pa	ge K < 5 of 6	22
i)	Operate ^ S Servera Chassia		Status Success 53	Execution T Execute 53	уре							22
	Fabric Interconnects HyperFlex Clusters		Name	Status :	Initiator :	Target Type	Target Name	Start Time	Duration	ID	Execution Type	ş
	Integrated Systems		Rack Server Dis	O Success	system@intersi	Rack Server	AA21-6536-2	Sep 25, 2023 0	7 m 39 s	6511e27f696f6	Execute	22
	Configure ^		Rack Server Dis	O Success	system@intersi	Rack Server	AA21-6536-1	Sep 25, 2023 0	7 m 29 s	6511e26c696f6	Execute	
			Chassis Inventory	O Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	1 m 12 s	6511e25a696f6	Execute	
	Profiles		Chassis Inventory	Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	1 m 14 s	6511e259696f6	Execute	
	Templates Ca		Chassis Discove	Ø Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	5 s	6511e244696f6	Execute	
	Policies	0	Chassis Discove	O Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	5 s	6511e241696f6	Execute	
	Pools		Chassis Discove	O Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	7 s	6511e241696f6	Execute	
			Chassis Discove	O Success	system@intersi	Chassis	AA21-6536-1	Sep 25, 2023 0	5 s	6511e23f696f6	Execute	
			Deploy Domain	O Success	rci@cisco.com	Fabric Interconn	AA21-6536 FI-B	Sep 25, 2023 0	36 s	6511e21d696f6	Execute	
erv.	Command Palette	B	Deploy Domain	@ Success	rci@cisco.com	Fabric Interconn	AA21-6536 FI-A	Sep 25, 2023 0	36 s	6511e21d696f6	Execute	

**Step 1.** Log in to **Cisco Intersight**. Go to **Infrastructure Service > Configure > Profiles > UCS Domain Profiles**, verify that the domain profile has been successfully deployed.

≡	داندان Intersight ، درمانده درم	Infrastructure Service 🗸		Q Search	◎ ⊄ ♀ ◎ 🜆	2 @ \ A
یں: ص	Overview Analyze	Profiles HyperFlex Cluster Profiles UCS Chassis Profile	s UCS Domain Profiles UCS Ser	ver Profiles		
0	Operate ^ Servers Chassis	* All UCS Domain Pr 0 +			Create UCS D	omain Profile
	Fabric Interconnects	··· 2 2 1 Q Add Filter :	Status	1100 Demola	found 10 ∨ per page ⊠ < ast Update	1_of1 ≥ > ≎ ∮
	HyperFlex Clusters	AA21-6536-Domain-Profile	(© OK)	AA21-6536 FI-A AA21-6536 FI-B S4	ep 25, 2023 3:40 PM	1_of 1 > >
,e I	Configure ^ Profiles					
	Templates Policies					
	Pools					
	Command Palette     Sector Certer K or     Sector Sec					

**Step 2.** Verify that the chassis (either UCSX-9508 or UCS 5108 chassis) has been discovered and is visible under **Infrastructure Service > Operate > Chassis**.

≡	ntersight	🖇 Infrastructure Service 🗸			Q Search	⊘ ⊄ ♀ @ 🜆	ଡ ନ
\$ 0	Overview Analyze	Chassis					
0	Operate ^	* All Chassis © +			G Export 1 items	s found 10 v per page 🔣 🔇 1	
	Chassis Fabric Interconnects	Health					22
	HyperFlex Clusters	Name	: Health	2 UCS Domain	Model	: Chassis Profile	g.
,¢	Configure ^	AA21-6536-1	O Healthy	AA21-6536	UCSX-9508		of 1 🔄 🖃
	Templates Policies Pools						
	Command Palette     Amount of the Amoun						

**Step 3.** Verify that the servers have been successfully discovered and are visible under **Infrastructure Service > Operate > Servers**.

	risco Intersight 🦂 😽 🖛	nfrastructur	e Service 🗸				Q Sear	:h	Ø ⊄ Q <b>@</b> @ĭ	0
k )	Overview Analyze	Serv	ers							
	Operate ^		All Servers 🐵 +				G	xport 10 items found	10 - per page 🖻 🕄 1 .	x1))))
	Servers Chassis Fabric Interconnects		Health	Power G off 10	HCL Status	Models 10 • UCSX 210 • UCSX 210 • C220 M75	DC-M6 4 DC-M7 4 S 2	Contract Status  Not Covered 10	Profile Status	<b>XX</b> + +
	HyperFlex Clusters Integrated Systems		Name	: Health		1000 000 000 000 000 000 000 000 000 00	nory Ca	UCS Domain : Server		: 9
	Configure ^		@ AA21-6536-1	© Healthy	UCSC-C220-M7S	256.0		AA21-6536	4.3(1.230138)	***
	Profiles		© AA21-6536-1-1	O Healthy	UCSX-210C-M7	128.0		AA21-6536	5.1(0.230122)	
	Templates		© AA21-6536-1-2	O Healthy	UCSX-210C-M7	128.0		AA21-6536	5.1(0.230122)	***
	Policies		O AA21-6536-1-3	Healthy     Healthy	UCSX-210C-M7 UCSX-210C-M7	128.0		AA21-6536	5.1(0.230122)	
			O AA21-6536-1-5	O Healthy	UCSX-210C-M7	128.0		AA21-6536	5.1(0.230122) 5.1(0.230075)	
	Pools		Q AA21-6536-1-6	O Healthy	UCSX-210C-M6	50.4		AA21-6536	5.1(0.230075)	
			Q AA21-6536-1-7	O Healthy	UCSX-210C-M6	50.4		AA21-6536	5.1(0.230075)	
	Command Palette				UCSX-210C-M6	50.4		AA21-6536	5.1(0.230075)	
			AA21-6536-1-8	O Healthy						

#### Procedure 12. Update Server Firmware

**Step 1.** With the servers recognized, the servers can be upgraded from the most recent Servers view in **Infrastructure Service > Operate > Servers**.

**Step 2.** Optionally, specify the desired model to work with from the list (example UCSX-210C-M7) and enter it within the filter box near the top.

=	disce Intersight	A Infrastructu	re Service 🗸			Q	Search		0
# 2	Overview Analyze	Serv	/ers						
í.	Operate ^	-	All Servers 9 +	ol			G Export 10 items for	and 10 - perpage ( 1 of 1	
	Servers Chassis Fabric Interconnects		Health	C off 30	HCL Status	Models	Contract Stat	No Server Profiles	11 + +
	HyperFlex Clusters Integrated Systems			Health	Model : 0	PU Ca : Memory Ca 256.0	: UCS Domain :	Server Prof : Firmware V : 4.3(1.2:30138)	ø
	Configure ^			O Healthy	UCSX-210C-M7		512.0 AA21-6536	5.1(0.230122)	
	Templates			O Healthy	UCSX-210C-M7 UCSX-210C-M7		512.0 AA21-6536	5.1(0.230122) 5.1(0.230122)	1995
								5.1(0.230122)	
	Policies		AA21-6536-1-4	O Healthy	UCSX-210C-M7	128.0	512.0 AA21-6536	31102301211	***
	Policies Pools		O AA21-6536-1-5	O Healthy O Healthy O Healthy	UCSX-210C-M7 UCSX-210C-M6 UCSX-210C-M6	50.4	512.0 AA21-6536 256.0 AA21-6536 256.0 AA21-6536	5.1(0.230075) 5.1(0.230075)	•••
			O AA21-6538-1-5 O AA21-6538-1-0	O Healthy	UCSX-210C-M6	50.4	256.0 AA21-6536	5.1(0.230075)	

**Step 3.** Select all servers from the resulting list by clicking the left side box of the column header, or manually select a specific set from the results.

= cisco Intersight Q Search A 0 m 0 A 🍂 Infrastructure Service 🗸 Servers \* Overview O Analyze All Servers 0 Operate Gearch UCEX-2500-467 x) Add Filter C Export 4 items found 10 - per page 2 2 1 of 1 2 2 н Servers Health Power HCL Status Models Contract Status Profile Status Chassis () Off 4 Incomplete 4 O Not Covered 4 4 · Heattry 4 4 • UCSX 210C-M7 4 No Server Profiles Fabric Interconnects HyperFlex Clusters Model CPU Ca\_ O Mer ory Ca... UCS Domain Server Profile Firmware V... Health integrated Systems Nat O AA21-6530-1-1 O Healthy 5.1(0.230122) . UCSX-210C-M7 128.0 512.0 AA21-6530 Configure .6 O Healthy 100 C AA21-0530-1-2 UCSX-210C-M7 128.0 \$12.0 AA21-6538 5.1(0.230122) Profiles Q AA21-6536-1-3 O Healthy UCSX-210C-M7 128.0 512.0 AA21-6538 5.1(0.230122) Template Q AA21-0530-1-4 O Healthy UCSX-210C-M7 128.0 512.0 AA21-6530 5.1(0.230122) Policies C Selected 4 of 4 Show Selected 1 of 1 Unselect All Pools New Command Palette C 3

**Step 4.** Click the ellipsis (...) near the top left for the drop-down list.



	Overview	Servers						
2	Analyze	* All Servers @ +						
e.	Operate ^	···· 0 9 Gearch UCEX 21	Add Filler		×	G Export 4 items found	10 - per page 💮 🔄 1 of 1	
	Servers	Power > System >	Power	HCL Status	Models	Contract Status	Profile Status	H A
	Fabric Interconnects	Profile > Install Operating System	O Off 4	(@ Incomplete 4)	4 + UCSX 2100-M7 4	Not Covered 4	No Server Profiles	
	HyperFlex Clusters Integrated Systems	Upgrade Firmware Set License Tier	: Health	: Model :	CPU Ca O : Memory Ca	. : UCS Domain : Ser	ver Profile : Firmware V_ :	1
e.	Configure ^	M WHENDERSON	O Healthy	UC5X-210C-M7	128.0	512.0 AA21-6538	5.1(0.230122)	100
	Profiles	AA21-6536-1-2	O Healthy	UCSX-210C-M7	128.0	512.0 AA21-6536	5.1(0.230122)	
		AA21-6536-1-3	O Healthy	UCSX-210C-M7	128.0	512.0 AA21-8538	5.1(0.230122)	775
	Templates	AA21-0536-1-4	O Healthy	UC5X-210C-M7	128.0	512.0 AA21-6536	5.1(0.230122)	- 111
	Policies	···· /? Selected 4 of 4 Show	Selected Unselect	All			1 of 1	

**Step 6.** Click **Start** on the resulting page and click **Next** after confirming that the servers to be upgraded have been selected.

=	cisco Intersight	📽 infrastructure Service 🗸		Q Search	Ø \$	Q <b>●  ▲ 1</b>
18 ()	Overview Analyze	← Servers Upgrade Firmware				
0	Operate ^ Servers	<ol> <li>General</li> <li>Version</li> </ol>	General Ensure selected servers meet requirements for firmware upgrade Confirm Servers Selection 4 Selected	0.		
	Chassis Fabric Interconnects HyperFlex Clusters	3 Summary	Q, Add Filter  Name : User Label :	4 items Model :	found 10 v per page I	C 1 of 1 D X O
,u	Integrated Systems Configure Profiles		<ul> <li>AA21-6536-1-1</li> <li>AA21-6536-1-4</li> <li>AA21-6536-1-3</li> </ul>	UCSX-210C-M7 UCSX-210C-M7 UCSX-210C-M7	5.1(0.230122) 5.1(0.230122) 5.1(0.230122)	AA21-6536 AA21-6536 AA21-6536
	Templates Policies Pools		AA21-8536-1-2 Selected 4 of 4 Show Selected Unselect All	UCSX-210C-M7	5.1(0.230122)	AA21-6536
	Command Palette     secto. Interclab. with. Creta X ar     x	¢	Cancel			Back Next

**Step 7.** Select the version to upgrade the servers to and click **Next**.

Ξ	cisco Intersight 🔉 Int	rastructure Service 🤟	Q Search () 41 Q		ତ ନ
*	Overview	- Servers Upgrade Firmware			
0	Operate ^	General     Version	Version Select a firmware version to upgrade the servers to.		-
	Chassis Fabric Interconnects HyperFlex Clusters	3 Summary	Select Perware Bundle The selected firmware bundle will be downloaded from intersight.com. All the server components will be upgraded along with drives and storage controllers. Use Advanced Mode to exclude upgrade of drives and storage controllers.	Advanced Mode	
,o	Integrated Systems Configure  Profiles		C.         Add Filter         4 items found         10 v per page         10           Version         Size         Release Date         Description           5.2(0.230041)         703.72 MB         Aug 16, 2023 2:40         Cisco Intersight Server Bundle	1 of 1 1	0
	Templates Policies		S.311.230052)     S23.88 Mi8 Jun 6, 2023 12:44 Cisco Intensight Server Bundle     S.10.230122)     S23.50 Mi8 Mar 31, 2023 8:37 Cisco Intensight Server Bundle     S.10.230096)     S21.31 Mi8 Mar 9, 2023 10:17 Cisco Intensight Server Bundle		9
	Poals			1 of 1	
1	Command Palette	¢	Cancel	Back	Next

Step 8.Click Upgrade, select the toggle to Reboot Immediately to Begin Upgrade, and click Upgradeagain.

Overview Analyze	• Servers Upgrade Firmware					
Operate ^	General     Version	Summary Confirm configuration and initiate the up	yrada.			
Chassis Fabric Interconnects HyperFilex Clusters Integrated Systems	Summary	Upgrade Firmware Firmware will be installed on next boot. To reboo enable the option below.		Size 523.88 Mill		
Configure ^		Cancel	Upgrade	Export 4 items found Firmware Versi	50 - per page 🛞 🔄 Requires Reboot O	1 of 1 🗊 💮 💮
		AA21-6530-1-1	UCSX-210C-M7	53(0.230122)	Yes	AA21-6536
Templates		AA21-6530-1-4	UCSX-210C-M7	53(0.230122)	Yes	AA21-6538
Policies		AA21-6536-1-3	UCSX-210C-M7	5.1(0.230122)	Yes	AA21-6536
Pools		AA21-6530-1-2	UC5X-210C-M7	53(0.230122)	Yes	AA21-6538
						1 of 1

Firmware upgrade times will vary, but 30-45minutes is a safe estimate to completion.

#### **Configure Cisco UCS Chassis Profile (Optional)**

The Cisco UCS Chassis profile in Cisco Intersight allows you to configure various parameters for the chassis, including:

- IMC Access Policy: IP configuration for the in-band chassis connectivity. This setting is independent of Server IP connectivity and only applies to communication to and from the chassis.
- SNMP Policy, and SNMP trap settings.
- Power Policy to enable power management and power supply redundancy mode.
- Thermal Policy to control the speed of FANs (only applicable to Cisco UCS 5108)

A chassis policy can be assigned to any number of chassis profiles to provide a configuration baseline for a chassis. In this deployment, no chassis profile was created or attached to the chassis, but you can configure policies to configure SNMP or Power parameters and attach them to the chassis.

#### **Configure Server Profile Template**

In the Cisco Intersight platform, a server profile enables resource management by simplifying policy alignment and server configuration. The server profiles are derived from a server profile template. A server profile template and its associated policies can be created using the server profile template wizard. After creating the server profile template, you can derive multiple consistent server profiles from the template.

The server profile templates captured in this deployment guide support Cisco UCS X210c M7 compute nodes with 5<sup>th</sup> Generation VICs. Cisco UCS C-Series connections were shown during the creation of the port profile policies used for the FIs to illustrate breakout ports but are otherwise not part of this validation. In deployments, Cisco UCS

C-Series profile templates can be nearly identical to configurations used for Cisco UCS X-Series or B-Series but might differ in aspects such as power policies.

#### vNIC and vHBA Placement for Server Profile Template

This section explains the vNIC and vHBA layout used in this deployment.

Four vNICs and four vHBAs are configured to support FC boot from SAN. The vNICs are split up into a pair uplinking to the standard vSwitch supporting the management vmkernel, and the remaining two connecting into a vSphere Distributed Switch (VDS) to carry vMotion and application traffic. Two vHBAs (FC-A and FC-B) are used for boot from SAN connectivity and the remaining two vHBAs (FC-NVMe-A and FC-NVMe-B) are used to support FC-NVMe. These devices are manually placed as listed in <u>Table 13</u>.

vNIC/vHBA Name	Slot	Switch ID	PCI Order
00-vSwitch0-A	MLOM	А	0
01-vSwitch0-B	MLOM	В	1
02-VDS0-A	MLOM	А	2
03-VDS0-В	MLOM	В	3
FC-A	MLOM	A	4
FC-B	MLOM	В	5
FC-NVMe-A	MLOM	A	6
FC-NVMe-B	MLOM	В	7

#### Table 13. vHBA and vNIC placement

#### **Procedure 1.** Server Profile Template Creation

Step 1. Log in to Cisco Intersight.

Step 2. Go to Infrastructure Service > Configure > Templates and in the main window click Create UCS Server Profile Template.

#### **Procedure 2.** General Configuration

Step 1.	Select the organization from the drop-down list (for example, AA21).
Step 2.	Provide a name for the server profile template. (for example, FC-Boot-FC-NVMe-Template)
Step 3.	Select UCS Server (FI-Attached).
Step 4.	Provide an optional description.
•	

=	dialis intersight	😂 infrastructure Service 🗠	Q Search	Ø ⊄ Q @ A D	ତ
*	Overview Analyze	Templates     Create UCS Server F	Profile Template		
ö.	Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Ceneral     Compute Configuration     Management Configuration     Storage Configuration     Seconfiguration     Seconfiguration	General Enter a name, description, tag and select a platform for the server profile template. Criganization * AA21		
,e 	Configure ^ Profiles Templates Policies Pools	0 Summary	Target Platform O UCS Server (Standalone) UCS Server (Fr-Attached) Set Tags Description		
	Command Palette	c	Close		Next

#### Step 5. Click Next.

#### **Compute Configuration**

The following subcomponents of pools and policies will be addressed in the Compute Configuration:

- A UUID Pool will be created to be used for the identities of Server Profiles derived from the Server Profile Template
- A BIOS Policy to set the available settings for the underlying hardware of the UCS Compute Nodes
- A Boot Order Policy to set the boot order of the Compute Nodes
- A Virtual Media Policy to enable virtual media accessibility to the KVM

#### **Procedure 1.** Configure UUID Pool

**Step 1.** Click **Select Pool** under UUID Pool and then in the pane on the right, click **Create New**.

	tions Intersight 34 Infrastructure Service			Q lease	A @ 4 P @ A
*	Duerview + Tempietos Create U	CS Server P	Profile Template		
Part	Operate     Image: Constant in the c	n Configuration	Compute Configuration Oranic or select existing Compute policies that you want to issuectane with this temptate. UUD Assignment UUD Assignment Refer Boos Boot Other Prever Tremul Virtual Media		
	telp + Convessell Publits	4	Class		Reck Rect

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the UUID Pool (for example, AA21-UUID-Pool).

Step 3. Provide an optional Description and click Next.

**Step 4.** Provide a hexadecimal UUID Prefix (for example, a prefix of AA210000-0000-0001 was used).

**Step 5.** Add a UUID block specifying a From starting value and a Size.

Ξ	disele Intersight	\$ Infrastructure Service ↔		Q. Search	0 41 Q 🚥 0 A
*	Overview Analyze	Templates > Create UCS Server Profile Tee Create UUID	state		
Ø	Operate  Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Ceneral Pool Details	Pool Details Collection of UUID suffix Blocks. Configuration Prefix * Au21000-0000-0001 0 UUID Blocks		
,6 	Configure  Profiles  Templates  Policies  Pools  Command Palette		From AA21-00000000001	Gize 64	5 a 1-1014 +
	· · · · · · · · · · · · · · · · · · ·	<u>\$</u>	Cancel		Back Create

Step 6. Click Create.

#### Procedure 2. Configure BIOS Policy

**Step 1.** Click **Select Policy** next to BIOS and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-Intel-M7-VSI-BIOS).

Step 3. Click Next.

**Step 4.** On the Policy Details screen, select the appropriate values for the BIOS settings. In this deployment, the BIOS values were selected based on recommendations in the performance tuning guide for Cisco UCS M7 BIOS:

<u>https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/ucs</u> <u>-m7-platforms-wp.html</u>. Set the parameters below and leave all other parameters set to **platform-default**.

≡	iliuli: Intersight 🌲 infrastructure Ser	vice ~	Q Search	ତ <b>ସ ଦ୍ © ଘା</b> ହ ତ   ୧
:@: 	Overview	reate UCS Server Profile Template BIOS Policy		
0	Operate	Add policy details	V All Platforms   U	CS Server (Standalone) UCS Server (FI-Attached)
,c	Fabric Interconnects HyperFlex Clusters Integrated Systems Configure	The BIOS settings will I     Boot Options     Intel Directed IO	be applied only on next host reboot.	
	Profiles Templates Policies Pools	+ LOM And PCIe Slots + Main		
	Command Palette     Second Palette	< Cancel		Back Create

- Processor > Processor C6 Report: Enabled
- Processor > Workload configuration: Balanced
- Server Management > Consistent Device Naming: Enabled
- Step 5. Click Create.

#### **Procedure 3.** Configure Boot Order Policy

**Note:** The FC boot order policy applies to all FC hosts including hosts that support FC-NVMe storage access.

**Step 1.** Click **Select Policy** next to Boot Order and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-Boot-Order).

Step 3. Click Next.

**Step 4.** For Configured Boot Mode, select Unified Extensible Firmware Interface (UEFI).

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 86 of 367

#### **Step 5.** Turn on Enable Secure Boot.

=	dealer Intersight	🍇 Infrastructure Service 🗸		Q Search	୦ ସ ଦେ 🎟 💿 ସ
*	Overview Analyze	Templates > Create UCS Server Profile Te Create Boot Order			
9 9	Operate ^  Servers /  Chassis /  Fabric Interconnects /  HyperFlex Clusters /  HyperFlex Clusters /  Configure ^  Profiles /  Profiles /  Pools /  Prools /  Profiles /  Pools /  Profiles /  Pools /  Profiles /	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add poicy details Configured Boot Mode @ Duffed Extensible Firmware Interface (UEFI) Legacy Enable Secure Boot @ Add Boot Device v	S As Partonne	UCS Server (Sh-Attached)
	Command Palette	¢	Cancel		Back Cruste

Step 6. From the Add Boot Device drop-down list, select Virtual Media.

Step 7.Provide a Device Name (for example, KVM-Mapped-ISO) and for the Sub-Type, select KVMMapped DVD.

=	esce Intersight	🔆 Infrastructure Service 🗸		Q Search	0	<b>¢</b> 1	00	<b>(42)</b>	0	۹
*	Overview Analyze	Templates > Create UCS Server Profile Temp Create Boot Order P								
9	Operate ^ Servers Chassis Fabric Interconnects	<ul> <li>General</li> <li>Policy Details</li> </ul>	Configured Boot Mode ©  (a) Unified Extensible Firmware Interface (UEFI) () Legacy  () Enable Secure Boot ©  Add Boot Device							Î
	HyperFlex Clusters Integrated Systems Configure ^ Profiles		<ul> <li>Virtual Media (KVM-Mapped-ISO)</li> <li>Device Name *</li> <li>KVM-Mapped-ISO</li> </ul>	e. Sue-Type			Enabled	8	с ж -	
	Templates Policies Pools			KVM MAPPED DVD					~ D	
	Command Palette	•	Cancel					lack	Creat	•

Step 8. From the Add Boot Device drop-down list, select SAN Boot.

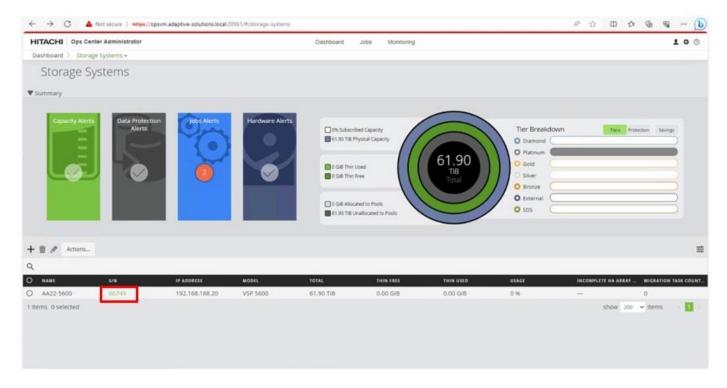
**Step 9.** Provide the Device Name: vsp-ctl0-1a and the Logical Unit Number (LUN) value (for example, 0).

**Step 10.** Provide an interface name FC-A. This value is important and should match the vHBA name.

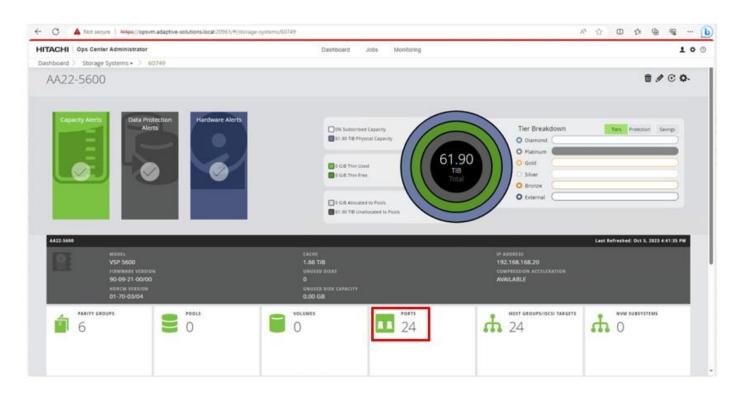
**Step 11.** Add the appropriate World Wide Port Name (WWPN) as the Target WWPN (referenced within Hitachi Ops Center as World Wide Name (WWN)).

**Note:** To determine these, you need to reference the Port information from within Ops Center. All four Hitachi VSP WWN will be added as boot options.

Step 12.	Open Ops Center	Administrator	Dashboard >	Storage Systems	> [S/N of VSP listing]
	open ops denter	Administrator	Dustibulur	otoruge oystering ,	



Step 13. From the resulting view, click Ports.



#### **Step 14.** Find and add the WWN for each port connected to the MDS.

HITACHI Ops Center	Administrator		Dashboard Jobs Monitoring			10
Dashboard > Storage Systems - > 60749 > Ports -			Charles and Charles			
						1.00
Ports						rên 🕫
Summary						
	Fibre				ISCSI	
	509				NVMe	
1						
م						
PORTID	www	19110	FABRIC, CONNECTION TYPE	SECURITY	VIM PORT	ATTRIBUTE
CL1-A	50:06:0E:80:08:ED:4D:00	Auto	Fabric ON / Point-to-point	No	No	Target
CL1-8	50:06:0E:80:08:ED:4D:01	Auto	Fabric ON / Point-to-point	No	No	Target
J CLI-0						
	50:06:0E:80:08:ED:40:02	Auto	Fabric ON / Point-to-point	No	No	Target
0 cu1-c	50:06:0E:80:08:ED:40:02 50:06:0E:80:08:ED:40:10	Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No	No No	Target Target
0 cu1-c 0 cu24						
0 al-c 0 al-c 0 al-c 0 al-c 0 al-c	50:06:0E:80:08:ED:40:10	Auto	Fabric ON / Point-to-point	No	No	Target
0 0.1-C 0 0.2-A 0 0.2-8 0 0.2-2	50:06:0E:80:08:ED:40:10 50:06:0E:80:08:ED:40:11	Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No	No No	Target Target
0 (1-C 0 (124) 0 (124) 0 (124) 0 (124) 0 (124) 0 (134)	50:06:0E:80:08:ED:40:10 50:06:0E:80:08:ED:40:11 50:06:0E:80:08:ED:40:12	Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No	No No No	Target Target Target
0 (1-C 0 (12-A 0 (12-B ) (12-B ) (12-C ) (13-A ) (13-B	50:06:0E:80:08:ED:40:10 50:06:0E:80:08:ED:40:11 50:06:0E:80:08:ED:40:12 50:06:0E:80:08:ED:40:12	Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No	No No No	Target Target Target Target
0 (1-C) (12-A) (12-B) (12-B) (12-C) (13-A) (13-A) (13-B) (13-C) (13-C) (13-C)	50:06:0E30:08:ED:40:10 50:00:0E30:08:ED:40:11 50:06:0E30:08:ED:40:12 50:06:0E30:08:ED:40:20 50:06:0E30:08:ED:40:21	Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No	No No No No	Target Target Target Target Target
0 (1-C) 0 (22A) 0 (228) 0 (226) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (23A) 0 (24A) 0 (22A) 0 (	\$0:06:0E30:08:ED:40:10 \$0:06:0E30:08:ED:40:11 \$0:06:0E30:08:ED:40:12 \$0:06:0E30:08:ED:40:20 \$0:06:0E30:08:ED:40:21 \$0:06:0E30:08:ED:40:22	Auto Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No No	No No No No No No	Target Target Target Target Target Target
0 c1-c 0 c224 0 c228 0 c226 0 c33A 0 c338 0 c336 0 c336 0 c336 0 c336 0 c448	\$0:06:0E30:08:ED:40:10 \$0:06:0E30:08:ED:40:11 \$0:06:0E30:08:ED:40:12 \$0:06:0E30:08:ED:40:20 \$0:06:0E30:08:ED:40:21 \$0:06:0E30:08:ED:40:22 \$0:06:0E30:08:ED:40:30	Auto Auto Auto Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No No No No	No No No No No No	Target Target Target Target Target Target Target
0 c1-c 0 c22A 0 c228 0 c226 0 c23A 0 c23A 0 c338 0 c38 0 c38 0 c38 0 c24A 0 c24A 0 c24A 0 c24A 0 c24B	\$0:06:0E30:08:E0:40:10 \$0:06:0E30:08:E0:40:11 \$0:06:0E30:08:E0:40:12 \$0:06:0E30:08:E0:40:20 \$0:06:0E30:08:E0:40:21 \$0:06:0E30:08:E0:40:22 \$0:06:0E30:08:E0:40:30 \$0:06:0E30:08:E0:40:31	Auto Auto Auto Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No No No No	No No No No No No No	Target Target Target Target Target Target Target Target

- vsp-ctl0-1a: VSP Controller 0, LIF for Fibre Channel SAN A 50:06:0E:80:08:ED:4D:00
- vsp-ctl0-3a: VSP Controller 0, LIF for Fibre Channel SAN B 50:06:0E:80:08:ED:4D:20

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 89 of 367

- vsp-ctl1-2a: VSP Controller 1, LIF for Fibre Channel SAN A 50:06:0E:80:08:ED:4D:10
- vsp-ctl0-4a: VSP Controller 1, LIF for Fibre Channel SAN B 50:06:0E:80:08:ED:4D:30

=	esco Intersight	🎉 Infrastructure Service 🗸		Q Search	0 4 <b>0 0</b>	۹
*	Overview Analyze	Templates > Create UCS Server Profile Tem Create Boot Order P				
ø.	Servers Chaesis Fabric Interconnects HyperFlex Clusters Integrated Systems	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy datalls Configured Boot Mode  Unified Extensible Firmware Interface (UEFI) Legacy Table Secure Boot  Add Boot Device	2 Al Partores   UCS 5	erver (Standatone) UCS Server (PI-Attached)	1
	Profiles Templates Policies Pools		- SAN Boot (vsp-ct0-ta) Device Name * vsp-ct0-ta Interface Name * FC-A	UUN     0     Target WW9N *     50:06.0E-80.40.00	Enabled 🖻 ^ 🗡	l
Net	Command Palette	.6	Bootloader Name	Bootloader Description	Create	•

- **Step 15.** Repeat steps 8-14 for the remaining VSP ports.
- Step 16. From the Add Boot Device drop-down list, select Virtual Media.
- **Step 17.** Add the Device Name example (CIMC-Mapped-ISO) and select the subtype **CIMC MAPPED DVD**.

=	ence Intersight	😂 Infrastructure Service 🗸		Q Search	
*	Overview Analyze	Templates > Create UCS Server Profile Temp Create Boot Order P			
Ø.	Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure ^	General     Policy Details	Policy Details Add policy datalls Configured Boot Mode © Unified Extensible Firmware Interface (UEFI) O Legacy Enable Secure Boot © Add Boot Device V	V Al Padores	UCS Server ISlandatonel UCS Server IFI-Attached
	Profiles Templates Policies Policies Command Palette Command Palette		Virtual Media (CIMC-Mapped-ISO)  Device Name * CIMC-Mapped-ISO	© Sud-Type CIMC MAPPED DVD	Enabled 🔒 🔨 👻
	igana intersight with Chri+K or go elp > Command Palette	¢.	SAN Boot (vsp-ct/0-4a)     Cancel     Cancel		Enabled B ^ Y Enabled B ^ Y Black Create

**Step 18.** Verify that the order of the boot policies and adjust the boot order as necessary using arrows next to the trashcan button.

=	ence Intersight	😂 Infrastructure Service 🗸		Q Search	
*	Overview Analyze	Templates > Create UCS Server Profile Tem Create Boot Order P			
0	Operate ^ Servers ^ Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure ^	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy datalls Configured Boot Mode @ © Unified Extensible Firmware Interface (UEFI) Legacy © Enable Secure Boot @ Add Boot Device	See Al Patterns	UCS Server (Standatore) UCS Server (FI-Attached)
1	Profiles Templates Policies Pools Command Palette		<ul> <li>Virtual Media (CIMC-Mapped-ISO)</li> <li>Device Name *</li> <li>CIMC-Mapped-ISO</li> </ul>	© Sub-Type CIMC MAPPED DVD	Enabled 😭 A 🗸
	gase intensight with Chri+K or go eip > Command Palette		+ SAN Boot (vsp-ct/0-4a) + CAN Boot (vsn-ct/1-2a) Cancel		Enabled B A Y Enabled B A Y Back Create

Step 19. Click Create.

## Procedure 4. Configure Virtual Media Policy

**Step 1.** Click **Select Policy** next to Virtual Media and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-KVM-Mount-Media).

Step 3. Turn on Enable Virtual Media, Enable Virtual Media Encryption, and Enable Low Power USB.

**Step 4.** Do not select Add Virtual Media at this time, but the policy can be modified and used to map an ISO for a CIMC Mapped DVD.

≡	ence Intersight	🔆 Infrastructure Service 🗸		Q Search	0 4 0 00 0 0
	Overview Analyze	Templates > Create UCS Server Profile T Create Virtual Med			
	Operate - Servers Chassis	General     Policy Details	Policy Details	🝸 🛛 Al Pathena	UCS Server (Standalone) UCS Server (Pr-Attached)
•	Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Templates		Configuration Enable Virtual Media  Enable Virtual Media Encryption  Enable Low Power USB		
	Policies Pools		Add Virtual Media	0 items found Protocol	50 - per page I 0 of 0 I I O File Location
Navrgar	Command Palette * in Intersight with Chrisk or go > Command Palette			NO ITEMS AVAILABLE	0 of 0
			Cancel		Back Create

Step 5. Click Create.

#### Step 6. Click Next to go to Management Configuration.

#### **Management Configuration**

The following policies will be added to the management configuration:

- IMC Access to define the pool of IP addresses for compute node KVM access
- IPMI Over LAN to allow Intersight to manage IPMI messages
- Local User to provide local administrator to access KVM
- Virtual KVM to allow the Tunneled KVM

=	the Intersight	🎉 Infrastructure Service 🗸		Q Search	A 0 4 4 0 4
*	Overview	+ Templates Create UCS Server	Profile Template		
0	Servers Chassis Fabric Interconnects HyperFlex Chasters Vietualization Integrated Systems Analyze Explorer Rec	Ceneral Compute Configuration Management Configuration Storage Configuration Network Configuration Retwork Configuration	Management Configuration         Create or select existing Management policies that you went to associate with this template.         Certificate Management         MC Access         IPMI Over LAN         Local User         Senal Over LAN         SNMP         Systog         Virtual XVM		
Nav	Command Palette	• •			
		ć.	Close		Back Next

#### Procedure 5. Configure Cisco IMC Access Policy

**Step 1.** Click **Select Policy** next to IMC Access and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-IMC-Access-Policy).

Step 3. Click Next.

Step 4. Click UCS Server (FI-Attached) if not selected.

**Step 5.** Select the toggle to enable **Out-of-Band Configuration**. Click **Select IP Pool** and in the pane on the right, click **Create New.** 

≡	dudi: Intersight	🎉 Infrastructure Service 🗸		Q Search	📄 ଡ 🕫 🗘 🖲 🕼 ଡ 🛛 ନ
*	Overview Analyze	Templates > Create UCS Server Profi Create IMC Acce			
Nev	Servers Chassis Fabric Interconnects HyperFiex Clusters Integrated Systems		Policy Details Add policy details Add policy details Add ninimuus of one configuration must for more info, Help Centre in-Band Configuration () in-Band Configuration () iP Pool * () Select IP Pool *	at be enabled. Policies like SNMP, vMedia, KMIP and Systog a	Partons UCS Server (FI-Anached) UCS Chessis are supported via Out-Of-Band. Check here
			< Cancel		Back

**Note:** This example will use the Out-Of-Band configuration that will pass through the configured management interfaces of the fabric interconnect. The In-Band configuration option will use the fabric interconnect uplinks for connectivity and must specify the VLAN for the connectivity.

**Step 6.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-OOB-Mgmt-Pool). Click **Next**.

**Step 7.** Select **Configure IPv4 Pool** and provide the information to define a pool for KVM IP address assignment including an IP Block.

$\equiv$ $\frac{\mathrm{dealer}}{\mathrm{csce}}$ Intersight	🍂 Infrastructure Service 🗸		Q Search	
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates  Create UCS Server Profile Temp Create IP Pool	slate > Create IMC Access Policy		
Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	General     General     Pv& Pool Details     The Pool Details	IPv4 Pool Details Network interface configuration data for IPv4 interfaces. Configuration Netmask * 255.255.255.0 Primary DM5 192.168.160.53 IP Blocks	Gateway 192.108.108.254 Secondary DNS 192.108.160.54 Size 24	0 0 0 0 0
Nove Command Palette Navigate Intersight with Ctri+K or gr to Help > Command Palette				
	c	Close		Back Next

**Note:** For tunneled KVM to work, the management IP pool subnet should be accessible from the Fabric Interconnect management interfaces.

- Step 8. Click Next.
- Step 9. Deselect Configure IPv6 Pool.
- **Step 10.** Click **Create** to finish configuring the IP address pool.
- **Step 11.** Click **Create** to finish configuring the IMC access policy.

**Procedure 6.** Configure IPMI Over LAN Policy

**Step 1.** Click **Select Policy** next to IPMI Over LAN and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-Enable-IPMIoLAN-Policy).

**Step 3.** Leave the default settings in place for this policy.

≡ disco Intersight	est Infrastructure Service ∨		Q Search	ା ତ ସ ଢ଼ 🛯 🐼 ଡ଼ା ନ
<ul> <li>Øverview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile T Create IPMI Over L			
<ul> <li>Operate Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Poolicies</li> <li>Pools</li> </ul>	Ceneral  Concertails  Concerta	Policy Details     Add policy details     Privilege Level   admin     Privilege Level     admin     © ©	All Platforms	UCS Server (Fi-Attached)
New Command Palette Navigate Intersight with Ctrl+K o to Help > Command Palette	× 60			
	<	Cancel		Back Create

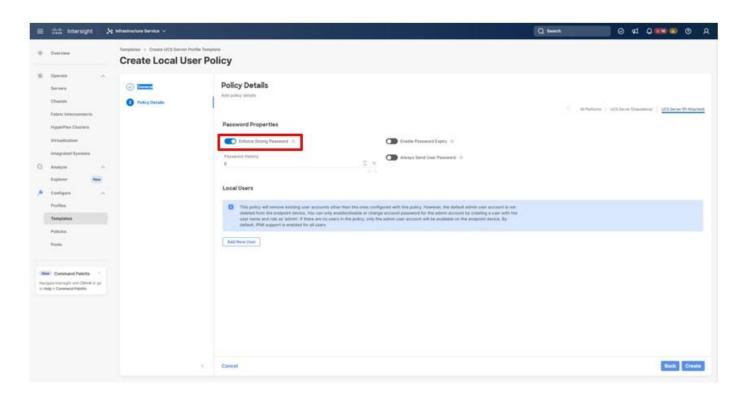
Step 4. Click Create.

# Procedure 7. Configure Local User Policy Step 1. Click Select Policy next to Local User and in the pane on the right, click Create New.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-LocalUser).

Step 3. Verify that UCS Server (FI-Attached) is selected.

**Step 4.** Verify that **Enforce Strong Password** is selected.



Step 5. Click Add New User and then click + next to the New User.

**Step 6.** Provide the username (for example, vsiuser), choose a role (for example, admin), and provide a password.

9	bevers Chamit Feletic Interconnectio	Create Local	Issues Parties Tangatara al User Policy Policy Details Are party strate			
	lersers Chanilà Feldris Inflamanneschi	@ General				
0	fapturer 🐜		deleted from the endpoint device. You can	Concern Password Equipy      Arrays Sand (yaar Password —      Arrays Sand yaar      Arrays Sand (yaar Password —      Arrays Sand yaar      Arrays      Arrays Sand yaar      Arrays      Arrays Sand yaar      Arrays      Arrays	T and	re   UCS Sever Handstoor   <u>UCS Sever Hondensed</u>
			- valueer (admin) 🛞			Chatter (1)
Parties	Command Palette * a topologic with Denot in go + Command Palette		Upaninasha * trajaat	9 Adres		
			famera *	= 0		End. Create

**Note:** The username and password combination defined here will be used as an alternate to log in to KVMs and can be used for IPMI.

- Step 7. Click Create to finish configuring the user.
- Step 8. Click Create to finish configuring the Local User Policy.

#### Procedure 8. Configure Virtual KVM Policy

**Step 1.** Click **Select Policy** next to Virtual KVM and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-KVM-Policy).

Step 3. Verify that UCS Server (FI-Attached) is selected.

#### Step 4. Turn on Allow Tunneled vKVM.

=	citco Intersight	🍂 Infrastructure Service 🗸		Q Search	ତ <b>ମ ଦ୍@୍ର</b> ଡ ୍ ୍
*	Overview Analyze	Templates > Create UCS Server Profile Create Virtual KV			
Nev	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems		Policy Details Add policy details The Enable Virtual KVM (*) Max Sessions * 4 (*) Enable Video Encryption (*) Allow Tunneled vKVM (*)	2	UCS Server (IN-Attached)
			Cancel		Back Create

Step 5. Click Create.

Step 6. To fully enable Tunneled KVM, after the Server Profile Template has been created, go to System > Settings > Security and Privacy and click Configure. Turn on Allow Tunneled vKVM Launch and Allow Tunneled vKVM Configuration.

**Step 7.** Click **Next** to continue to Storage Configuration.

**Storage Configuration** 

The Storage Configuration section of the Server Profile Template is not required for internal storage in the UCS servers because all storage for this solution is provided by the VSP. Click Next on the Storage Configuration screen.

#### **Network Configuration**

This section details how to create the LAN Connectivity and SAN Connectivity policies used by the derived Server Profiles.

#### LAN Connectivity

#### **Procedure 1.** Create Network Configuration - LAN Connectivity Policy

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

For consistent vNIC placement, manual vNIC placement is used. The four vNICs configured are listed in Table 14.

#### vNIC/vHBA Name Switch ID PCI Order VLANs Slot ID 0 **IB-MGMT** 00-vSwitch0-A MLOM А 01-vSwitch0-B MLOM В 1 **IB-MGMT** 02-vDS0-A MLOM А 2 VM Traffic, VM Traffic-A, VM Traffic-B, vMotion 03-vDS0-B MLOM 3 VM Traffic, VM Traffic-A, VM Traffic-B, vMotion В

Table 14. vNICs defined in LAN Connectivity

Click Select Policy next to LAN Connectivity and in the pane on the right, click Create New from Step 1. the column that appears to the right.

= :	it intersigne	A Maninetan Sanka v			Q form	8 0 4 4 0 A
* *		Create UCS Server	Profile Template			
	room anala lais internamenta querttan Dawlans maalaattan maalaattan		Network Configuration	t that yes were to assurate with the heymon.		
			Omer			Tes Sec

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-Boot-LanCon-Pol). Click **Next**.

**Step 3.** Click **Add vNIC** under the vNIC Configuration section.

=	ritada Intersight 🕺	Infrastinacture Service 🗸		Q Search	0 4 4 0	A
*	Overslew	Templates > Create UCS Server Profile Templ Create LAN Connect				
0	Operate        Servers        Channik        Fabric Interconnection        HyperFiles Chanters        Versalization        HyperFiles Chanters        Versalization        HyperFiles Chanters        Versalization        HyperFiles Chanters        Versalization        HyperFiles Chanters        Configure        Patieles        Patieles        Patieles	General     Poley Details	Policy Details Ast princy details C  C  C  C  C  C  C  C  C  C  C  C  C			
Ne	Command Palette     '     command Palette     v		Cancel	0 Aems found 10 - per page	Craphic (NCs. Lattur)	J.

Step 4.Referencing values from Table 14, specify the Name for the vNIC, and under MAC Pool, clickSelect Pool.

=	the Intersight	$\mathcal{M}_{\mathrm{c}}$ infrastructure Service $\sim$		Q, Seech	0 4 0 0 8
*	Overview	Templates + Create UCS Server Profile Template Create LAN Connectivity Policy			
100	Explorer New	Add vNIC	Seneral         Imme *         Imme		
		Cancel			(m)

**Note:** When creating the first vNIC, the MAC address pool has not been defined yet therefore a new MAC address pool will need to be created. Two separate MAC address pools are configured for each fabric. MAC-Pool-A will be reused for all Fabric-A vNICs, and MAC-Pool-B will be reused for all Fabric-B vNICs.

Pool Name	Starting MAC Address	Size	vNICs
MAC-Pool-A	00:25:B5:21:0A:00	256	00-vSwitch0-A, 02-VDS0-A
MAC-Pool-B	00:25:B5:21:0B:00	256	01-vSwitch0-B, 03-VDS0-B

Table 15. MAC Address Pools

**Note:** Each server requires 3 MAC addresses from the pool. Adjust the size of the pool according to your requirements.

**Step 5.** Select the MAC Pool appropriate fabric or click **Create New** if one has not been created yet.

**Step 6.** If creating a new pool, verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a Name for the pool from <u>Table 15</u> depending on the vNIC being created (for example, MAC-Pool-A for Fabric A).

=	the intersigne	🗙 aflastuitus farvice 🤟	والعار فالتجاري والمحادث والمحاد	Q Seens		8
*	Overview	Templere 1. Create UCS larger Parties for Create MAC Pool	ane > Creare LAN Europeanitely Policy			
	Openane no se	Const     The Densis	Second all         Provide the second back addresses that set as advanced in VMCs of a server profile.         Mail         Mail         Second back         Description			
			Canad		-	a 🕛

Step 7. Click Next.

**Step 8.** Provide the starting MAC address from <u>Table 14</u> (for example, 00:25:B5:21:0A:00)

**Step 9.** Provide the size of the MAC address pool from <u>Table 15</u> (for example, 256).

=	The Attensight.	34 Information Device			Q hard	0440	А
*	Descent	Create MAC Pool	splate - Create LAN Constructivity Policy				
0	Servers Durwith Falses interconnection Hyposifies Disalace Versalization Singurand Systems Adaptes Explores Inter		Pool Details Concerned MAC Blocks : The Blocks : BLOBE 219 648	a di si		<u>* *</u> (1997)	
		3	Cannot			Bath Court	Ι.

**Step 10.** Click **Create** to finish creating the MAC address pool.

Step 11.Confirm the Switch ID and PCI Order values are correct for the vNIC being configured per Table14.

=	the Intersight	×	Infrastructure Service 🗸		Q teach	0	<b>4</b> 1	٥	۲	R
+	Overview		Templates Create UCS Server Politic Template Create LAN Connectivity Policy							
. Nov	Openste Servers Chassis Eduit Interevents Eduit Interevents Experite Chasses Virautization Experite Spatners Configure Openste Positie Configure Openste Opens		Add vNIC	Centeral     Name*   Bases        MAC     Mass   Session     Mass     Session     Mass   Session     Mass   Session     Mass   Session     Session </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
			Count							Ĩ,

Step 12. Click Select Policy for Ethernet Group Policy.

= ***	Intersight	💥 lefeatuetue Service 🗸		Q, Seech	0 4 0 0 A
il) Overvie	the state	Templates > Create UCS Server Profile Template Create LAN Connectivity Policy			
Hyper Pi Virtuella	n Management Inter Deaters Author Management Managemen				
Nordganis Solar II Si Helgi + Canton	uging with Calif-Al as go: keend Publishe	Cent	IdOS Book 0 Select Putoy D Connection Disatlet weRC VHO		

**Note:** Two Ethernet Network Group Policies will be created, one for vSwitch0 and one for vDS0 to detail the Native VLAN and VLANs that will be carried within the vNICs.

**Step 13.** When creating the vSwitch0 vNICs and the vSwitch0 Ethernet Network Group Policy is not created, select the **Create New** option. Select the appropriate policy if it is created and skip the next two steps.

**Step 14.** Provide a Name for the policy and click **Next**.

=	these intersight	jet infrastructure Service ~		Q Beenh	0 4 0	<b>ଡ</b> ଼ନ	L
+	Overview	Templates - Create UCE Server Profile Temp Create Ethernet Net					
	Bervers Daasie Faktie Interconnexies HopperFles Daatees Verbaeikastion Analyzes Explorer Inter	Convert 2 Petry Datains	General Add a name, description and hap for the policy. Digensation * Add * Ad				
22	gana treangar with Data di or ga agi a Comment Patron		Cancel		1	Next	

**Step 15.** Specify the Native VLAN to be used and any VLANs allowed and click **Create**.

=	तीती Intersight अ	Infrastructure Service 🗸				Q Search	0	41	٥	•	A
*	Overview	Templates > Create UCS Server Profile Templ Create Ethernet Net									
14	Operation	Control     Procey Destants	Policy Details Ant policy deals VLAN Settings The Setting Constitution of Cons	2.4 *							
			Cantal					Beth	0	wate .	

**Step 16.** When creating the vDS0 vNICs and the vDS0 Ethernet Network Group Policy is not created, select the **Create New** option. Select the appropriate policy if it is created and skip the next two steps.

**Step 17.** Provide a Name for the policy and click **Next**.

=	tta Intersight	X Infrastructure Service ~		Q teent	0	<b>\$</b> ]	0 0	Ð	۹
+	Overview	Templates + Create UCS Server Public Temp Create Ethernet Net							
100	Openitie A de la construction de	General     Peircy Details	General Add a verse, description and lag for the policy: Add						
			Cancel				E	ext	Ļ

Step 18. Specify the Native VLAN to be used and any VLANs allowed and click **Create**.

	The Intersight	👔 🔆 infrastructure Service 🗸		Q Search Ø 4	100	D S	2
+	Overview	Create Ethernet Netw					
1000	Servers Classis Fabric Interconnents HyperFlee Classers Versatization Interconnents Serverstation Adaptes Explorer		Policy Details Add policy serves VLAN Settings				
		<u>.</u>	Carcel		Back Dre	470	

**Step 19.** For either type of vNIC, click **Select Policy** under Ethernet Network Control Policy.

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 107 of 367

=	the Intersight	🔆 Infrastructure Service 🛩		Q Search	0 4 0 0 8
+	Overview	Trendeter + Create UCS Server Prefix Trendets Create LAN Connectivity Policy			
0	Operate Servers Chamin		a 👙 a Gonsistent Device Naming (CDN)		**
	Fabric Interconnects HyperPlos Chaters Versalization		Source = 0		
0	Integrated Systems Analyze Explorer New		Fallover Clim Ensteid II Ethernet Hetwork Group Policy * II		
,0	Configure Profiles Templates		Selected Prility: A421-vLeeted Heldop Pelicy ( × ) ( ( ) ) Ethernet Heldop Control Pelicy * () Select Pelicy ()		- 1
	Publies Paula		Ethernet Guil * = Senet Policy II Ethernet Adapter * =		
the	Command Polette		Search Policy () RCDI Buck II Search Policy ()		
			Connection Discline wHC VMC		
		Careat			

**Step 20.** Click **Create New** from the right-hand column that appears or select the Ethernet Network Control Policy if it has already been created and skip the next two steps.

**Step 21.** Provide a Name for the policy and click **Next**.

=	their Intersight	×	i Infrastructure Service 🛩			Q Search	0	<b>9</b> 3	٥	۲	A
*	Overview		Create Etherne		www.s.Constructivity.Priday						
184am	Servers Cremits HyperFlex Chotes Wheelastion Integrated Springers Analyze Explorer		Constat     2     Policy Details		General Atta same, decorption and tay for the policy. Department Auto Tarne * Auto Bet Tags Description						
				ų.	Cancel					Next	

**Step 22.** Select the **Enable CDP** toggle and the **Enable Transmit** and **Enable Receive** toggles under LLDP, and then click **Create**.

=	命章 Intersight	×	infrastructure Service 🗸		Q Search	0	<b>\$1</b>	٥	۲	۹
*	Querview		Templates > Create UCS Server Profile Templa Create Ethernet Netw							
	Openein Servers Unservers Highen Enforcemente Highen Enforcemente Highen Enforcemente Parleine Coorfigues Coorfigues Parleine Parleine Coorfigues Coorfigu		Countal     Party Details	Policy Details Are policy details This policy is regulateries any for ICOS Servers ITH-Attachuest Conformation Servers (Conformation Servers ITH-Attachuest Conformation Servers (Conformation Servers) Conformation						*
				Canal			C		Creater	Ļ

**Step 23.** For either type of vNIC, click **Select Policy** under Ethernet QoS.

=	the Intersight	×	behastructure Service 🛩		Q Search	0	41	0 (	@ A	
	Overview		Templates - Could UCS Server Profile Template Create LAN Connectivity Policy							
	Operate Servers	~		* *					1	i
	Chassis			Consistent Device Naming (CDN)						
	Fales: Interconvects Hyperflex Duaters			Source Mot Name - 0						
	Virtualization			Fallover						
Q	integrated Systems Analyze			Con Excised a						
	Explorer	•		Ethemet Network Group Policy * 0						
	Configure	÷.		Selected Policy AA21-vSelan0-NetDip-Policy   +   +   #						
	Profiles			Elf-lement Network Control Policy * ()					- 16	
	Templates			Sensitive Policy AA21-Enable-COP-LLDP   +   +   #						
	Paleire Paule			Ethernet Guid * 0 Select Aulty S Ethernet Adapter * 0						
	Command Palette			Environ Adapter = 0 Existen Putary II						
144	gate was optig with Delek is y ing > Command Palette			ISCSI Boot 9 Swinst Pulling ()						
				Connection Doutent unter VMD						
			Creat						-	

**Step 24.** Click **Create New** from the right-hand column that appears or select the Ethernet QoS Policy if it has already been created and skip the next two steps.

=	the Intersight	N Infrastructure Service -		Q Search	0	41	٥	۲	R
+	Overview	Templates + Chaile UCS Server Profile Temp Create Ethernet QoS							
fore	Operane     ·       Servers     ·       Servers     ·       Patricis timesarvestis     ·       Hyperfree Clusters     ·       Viriautization     ·       Explorer     ·       Configure     ·       Patricis     · </th <th>Consul</th> <th>General Ad a sume, mescription and tag for the paths  Coperation* Add  Farms* Add  Farms*  Add</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Consul	General Ad a sume, mescription and tag for the paths  Coperation* Add  Farms* Add  Farms*  Add						
		- e.	Canor					Real	÷

**Step 25.** Change the MTU Bytes settings to 9000 and click **Create**.

Ξ	the Intersight	20	lefrastructum Eardoa 🛩				Q Search	0	41	0 0	R
	Overview		Temptates > Create UCS Server Profile Tem Create Ethernet Qo								
	Servers Chessis Fabric Internetioners HiggerFless Chesters Versaalzetten Hengesten Speteren Analyse Explorer Internetioners		<ul> <li>Cannad</li> <li>Pathy Databa</li> </ul>	Policy Details Ant policy details GoS Settings Mitty, Ryres Bout 10369 Bout B	t a norm som til konsen	Resclint, Maps 0 Prostly Beer effort	T Rhaines U.S.S	eve Steaterst	<u>001 les</u>	0	
			¢	Encol					Rec.	Creek	

**Step 26.** For either type of vNIC, click **Select Policy** under Ethernet Adapter.

=	the Intersight 🔀	i infrastructum Sarvice 🛩		Q Search	0 4	1 0	۲	R
*	Overview	Templates - Create UCS Server Profile Template Create LAN Connectivity Policy						
-	Openation     -       Servers     -		Consistent Device Naming (CDN)         Source and Channe         Source and Channe         Fallower         Channet National Group Policy * 0         Demont National Group Policy * 0         Demont National Control Policy * 0         Demont Co					**
		Canval						ι.

**Step 27.** Click **Create New** from the right-hand column that appears or select the Ethernet Adapter Policy if it has already been created and skip the next two steps. One policy will be created for the vSwitch0 vNICs, and a different policy will be created for the vDS0 vNICs.

**Step 28.** To create the vSwitch0 policy, specify a Name for the policy, and click **Select Default Configu**ration.

=	the intersight	M Infrastructure Dervice ~		Q. Search	0	41	٥	۲	R
*	Overview	Templates + Create UCS Server Profile Temp Create Ethernet Ada							
-	Operate	Connext	Add a name, descriptions and has for the policy.         Organization *         Add *         Add *         Math         Math						
		8	Count					Next	

**Step 29.** Select the **VMWare** option from the column that appears to the right and click **Next**.

**Step 30.** Leave all options set to their default settings in the resulting screen and click **Create**.

**Step 31.** To create the vDS0 policy, specify a Name for the higher traffic settings used in the policy, and click **Select Default Configuration**.

=	thit Intersight	×	i Infrastructure Dervice 🛩			Q teach	0	41	٥	۲	۹
*	Overview		Samplates + Create UCS Server Pr Create Ethernet		ala > Casala LAM Connectivity Policy <b>pter</b>						
iler.	Servers Chumis Hubric Interconnects HyperFlee Chatlers Virbaelizetter Integrated Systems Anatys Explorer Inter		Constit     Poing Datais		General         Add a name, description and lag for the policy.         Opposizion: *         Add: -         Torror *         Add: -         Central         Set Tags         Description         Central Adapter Default Configuration :         Termor turinant Configuration ?						
				×.	Canad					Next	

**Step 32.** Select the **VMWare** option from the column that appears to the right and click **Next**.

Step 33. Change the Interrupts to 11, the Receive Queue Count to 8, the Receive Ring Size to 4096, the Transmit Ring Size to 4096, and the Completion Queue Count to 9. Click Create.

≡	cisco Intersight	📽 Infrastructure Service 🗸			Q Search	Ø ⊄ Q Ø A
:@:	Overview	Templates > Create UCS Server Profile Temp Create Ethernet Ada				
244°	Operate ^ Storage Virtualization	<ul><li>General</li><li>Policy Details</li></ul>	Enable GENEVE Offload      RoCE Settings     Enable RDMA over Converged Etherr     Interrupt Settings	net O		^^
୍	Analyze A Explorer New Configure A Profiles		Interrupt Sectings	Interrupt Mode ■ MStx 1 - 1024 ✓ ●	Interrupt Timer, us	<b>0</b> • 65535
	Templates Policies Pools		Receive Receive Queue Count 8 Transmit	C Colve Ring Size	<b>0</b> 64 - 16384	- 1
Naviga	Command Palette × te Intersight with Ctrl+K or go >> Command Palette		Transmit Queue Count 1 Completion Completion Queue Count 9	Completion Ring Size     Completion Ring Size     1 - 1000     Completion Ring Size     1 - 2000     1 - 2000		
		<	Cancel			Back Create

### Step 34. Click Add.

≡	disco Intersight	ж	nfrastructure Service 🗸		Q Search	41	٥	0	A
*	Overview		Templates > Create UCS Server Profile Template Create LAN Connectivity Policy						
0	Operate	^							^ ^
	Servers			Consistent Device Naming (CDN)					
	Chassis								
	Fabric Interconnects			Source vNIC Name v o					
	HyperFlex Clusters								
	Virtualization			Failover					
	Integrated Systems			Enabled 0					
O,	Analyze	^		—					
	Explorer New			Ethernet Network Group Policy * 0 Selected Policy AA21-vSwitch0-NetGrp-Policy   ×   Φ   D					
,0	Configure	^		and a star					
	Profiles			Ethernet Network Control Policy * 0					11
	Templates			Selected Policy AA21-Enable-CDP-LLDP   ×					
	Policies			Ethernet QoS * O					
	Pools			Selected Policy AA21-EthernetQos-Policy X @					
				Ethernet Adapter * O					
N	w Command Palette			Selected Policy AA21-EthAdapter-VMware-Policy   ×   ©   D					
	igate Intersight with Ctrl+K or go felp > Command Palette			iSCSI Boot O					
toP	rep # Command Palette			Select Policy 🗊					
				Connection					
				Disabled usNIC VMQ					
									v
			Cancel					Add	
									-

**Step 35.** Repeat steps 3-34 for each additional vNIC, creating the appropriate pools and policies as required.

### Step 36. Click Create to finish the LAN Connectivity Policy.

• Out (bill (b))       • Out (b)       • Out (b										
Servers										
Overview Operate Operate Servers Chassis Fabric Interconnects HyperFlex Chasters Vertualization Integrated Systems Analyze Configure Configure Profiles Poticies Poti	Add policy details  Table Ature Stack Hes  NON  Non  Non  Non  Non  Non  Non  Non	Pool 5 IGN name is not associat exit Auto	ed with the policy	an more at Hulp Center			Graphic vi	NICs Editor		
	1 / D 9 Ad							0		
						Pin Group				
						*:				
						5.				
	02-v050-A	Auto			Disabled	£				
	03-vDS0-B	Auto	в	3	Disabled		MAC-Pool-B			
							1000	of 1		

### **SAN Connectivity**

### **Procedure 1.** Create 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.

<u>Table 16</u> lists the details of four vHBAs that are used to provide FC connectivity, FC boot from SAN functionality, and FC-NVMe connectivity.

### Table 16. SAN Connectivity vHBAs

vNIC/vHBA Name	Slot	Switch ID	PCI Order
FC-A	MLOM	A	4
FC -B	MLOM	В	5
FC-NVMe-A	MLOM	A	6
FC-NVMe-B	MLOM	В	7

**Step 1.** Click **Select Policy** next to SAN Connectivity and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a Name for the policy (for example, AA21-FC-NVMe-FC-SAN). Click **Next**.

Step 3. Select Manual vHBAs Placement.

Step 4. Click Select Pool under WWNN Address.

ence Intersight	为 Infrastructure Service ←		Q Search	] ⊘ ⊄	000	0	
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile Templ Create SAN Connect						
Analyze     Analyze     Operate     Servers     Chassis     Fabric Interconnects     HyperFlex Clusters     Integrated Systems     Configure     Profiles     Templates     Policies     Pools	Policy Details	Policy Details Add policy details Manual VHBAs Placement Auto vi WWNN Pool Static WWNN Pool * © Select Pool © C For manual placement option you need to specify placement option you need to	RBAs Placement	Center	Graphic vHIIAs 1		
Pools . New Command Palette . Navigate intersight with Chirk or go to telep - Cemmand Palette	×	D / D Q Add Filler		50 – per page Nin Group	Back	© ;	

#### **Procedure 2.** Create the WWNN Address Pool

The WWNN address pools have not been defined yet therefore a new **WWNN Address Pool** has to be defined. To create the WWNN address pool, follow these steps:

Step 1. Click Select Pool under WWNN Address Pool and in the pane on the right, click Create New.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-WWNN-Pool).

Step 3. Click Next.

**Step 4.** Provide the starting WWNN block address and the size of the pool.

and the state of t	💈 Infrastructure Service 🤟		Q Search	S 4 0 00 0 2
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile Tem Create FC Pool	plate > Create SAN Connectivity Policy		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFiex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Policies</li> <li>Pools</li> </ul>	General     Pool Details	Pool Details Block of WWNN Identifiers. WWNN Blocks From 20 00 00 25 85 21 00:00	© Site 254	<u>0 0</u> 11000
New Command Palette * Havgate Intensight with Chri-K or go to Help > Command Palette				
	×	Cancel		Back Create

**Note:** As a best practice, some additional information can be coded into the WWNN address pool for ease of troubleshooting. For example, the address 20:00:00:25:B5:21:00:00 contains a reference to the AA21 rack ID.

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

#### Procedure 3. Create the vHBA-A for SAN A

Step 1. Click Add vHBA.

**Step 2.** Provide the Name (for example, FC-A) and vHBA Type and choose **fc-initiator** from the drop-down list.

### Procedure 4. Create the WWPN Pool for SAN A

The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric A will be defined. This pool will also be used for the FC-NVMe vHBAs if the vHBAs are defined.

**Step 1.** Click **Select Pool** under WWPN Address Pool an in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-WWPN-Pool-A).

**Step 3.** Provide the starting WWPN block address for SAN A and the size.

**Note:** As with the WWNN, some additional information can be coded into the WWPN address pool for ease of troubleshooting. For example, the address 20:00:00:25:B5:21:0A:00, 21 references Rack ID 21 and 0A signifies SAN A.

≡ dudu Intersight	🎉 Infrastructure Service 🗸		Q Search	୍ର ସ ହ <b>ା</b> ରେ ନ ତ
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile Temp Create FC Pool	late > Create SAN Connectivity Policy		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Policies</li> <li>Pools</li> </ul>	Ceneral  Control  Ceneral  Control  Contro  Control  Control  Control  Control  Control  Control  Con	Pool Details Block of WWPN Identifiers. WWPN Blocks From 2000/00/25/85/21/0A/00	9 <mark>5/29 256</mark>	<u><u><u></u></u> <u></u> +</u>
Novigate Intensight with Coll+K or y to Help > Command Palette				
	· · ·	Cancel		Back Create

**Step 4.** Click **Create** to finish creating the WWPN pool.

=	disco Intersight	🖧 Infrastructure Service 🗸		Q Search	Ø \$	Q 🔘 🗛	0	<u>8</u>
:0:	Overview	Templates > Create UCS Server Prof						
O.	Analyze		lectivity Policy					~ ~
0	Operate ^	Add vHBA						
	Servers		General					
	Chassis Fabric Interconnects		Name * FC-A O	vHBA Type fc-initiator ~ 0	0			
	HyperFlex Clusters		Pin Group Name 🗸 👳					
,0	Configure		WWPN					
	Templates		Pool Static					
	Policies Pools		WWPN Pool * ○           Selected Pool AA21-WWPN-Pool-A × 0					
			Placement					
Navi	Command Palette     Section 2		Simple Advanced					
		Cancel	returnate out to readyment				Add	× ,

**Step 5.** Back in the **Create vHBA** window, using Advanced Placement, specify the **Slot ID**, **Switch ID** (for example, A) and **PCI Order** from <u>Table 16</u>.

=	dealer Intersight	🎉 Infrastructure Service 🗸	Q Search	Ø \$	000	۲	۹
*	Overview Analyze	Templates > Create UCS Server Profile Template Create SAN Connectivity Policy					
0.	Operate  Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Placement Simple Advanced Automatic Stot ID Assignment © Stot ID MLOM					
,0	Configure ^ Profiles Templates Policies Pools	Automatic PCI Link Assignment © Load-Balanced © Custom PCI Link 0 0 0 0					
Navig	Command Palette * an Intersight with Cot+K or go p > Command Palette	PCI Order 4 G o				Add	

### Procedure 5. Create Fibre Channel Network Policy for SAN A

A Fibre Channel network policy governs the VSAN configuration for the virtual interfaces. In this deployment, VSAN 101 will be used for vHBA-A.

**Step 1.** Scroll down within the Create SAN Connectivity Policy dialogue and click **Select Policy** under Fibre Channel Network and in the pane on the right, click **Create New**.

≡	dualus Intersight	2 Infrastructure Service ~			Q Search	₽ ©	۵ 💿 🚳	0	R
*	Overview Analyze	Templates > Create UCS Server Pr Create SAN Con							
ø	Operate Servers Chassis Fabric Interconnects	~	Switch ID * A PCI Order 4	5.0					**
•	HyperFlex Clusters Integrated Systems Configure Profiles Templates Policies Pools	ĥ	Persistent LUN Bindings  Persistent LUN Bindings  Fibre Channel Network *  Fibre Channel QoS *  Select Policy						
Nev	Command Palette     Gate Intersignt with Ctri+K or gr up > Command Palette		Fibre Channel Adapter * © Select Policy 🗐 FC Zone © Select Policy(s) 🗐						
		Cancel						Add	Ļ

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-Network-SAN-A).

**Step 3.** Specify the VSAN ID for Fabric A, (for example, 101).

$\equiv \frac{-de de}{e \pi e}$ Intersight	👌 Infrastructure Service 🗸		Q Search	A 0 41 0 49 0 19
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profit Create Fibre Chai	e Template > Create SAN Connectivity Policy		
	Ceneral Ceneral Policy Details	Policy Details Add policy details Fibre Channel Network VSAN ID 101	2 o 1 - 6001	UCS Server (Standalone)
		Cancel		Back Create

**Step 4.** Click **Create** to finish creating the Fibre Channel network policy.

### Procedure 6. 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 all vHBAs.

Step 1. Click Select Policy under Fibre Channel QoS and in the pane on the right, click Create New.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-QoS-Policy).

**Step 3.** Do not change the default values on the Policy Details screen.

**Step 4.** Click **Create** to finish creating the Fibre Channel QoS policy.

### Procedure 7. 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 all the vHBAs.

**Step 1.** Click **Select Policy** under Fibre Channel Adapter and in the pane on the right, click **Create New.** 

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-Adapter).

**Step 3.** Under Fibre Channel Adapter Default Configuration, click **Select Default Configuration**.

=	esce Intersight	🔆 Infrastructure Service 🗸		Q Search	<b>I</b> 0 4	0 💿 🚳	0	R
*	Overview Analyze	Templates > Create UCS Server Profi	te Template  Create SAN Connectivity Policy nnel Adapter					
Nev	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	General     Constants     Policy Details	General         Add a name, description and tag for the policy.         Organization *         Add1         Add1         Mame *         Add1+PC-Adapter         Set Tags         Description         Fibre Channel Adapter Default         Configuration         Selected Default         Configuration         VMWare         X	]				
			Cancel				Next	

Step 4. Select VMWare and click Next.

**Step 5.** Do not change the default values on the Policy Details screen.

Step 6. Click Create to finish creating the Fibre Channel adapter policy.

Step 7. Click Add to create vHBA FC-A.

**Procedure 8.** Create the vHBA for SAN B

Step 1. Click Add vHBA.

Step 2. For vHBA Type, choose fc-initiator from the drop-down list.

### **Procedure 9.** Create the WWPN Pool for SAN B

The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric B will be defined. This pool will also be used for the FC-NVMe vHBAs as well.

**Step 1.** Click **Select Pool** under WWPN Address Pool and in the pane on the right, click **Create New**.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-WWPN-Pool-B).

**Step 3.** Provide the starting WWPN block address for SAN B and the size.

**Note:** As a best practice, some additional information is once again coded into the WWPN address pool for ease of troubleshooting. For example, the address 20:00:00:25:B5:21:0B:00, 21 contains the rack ID and 0B signifies SAN B.

≡ "thete intersight	🔆 Infrastructure Service 🗸		Q Search	9 4 0 🚳 9 A
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile Temp Create FC Pool	plate > Create SAN Connectivity Policy		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Policies</li> <li>Pools</li> </ul>	Control Contr	Pool Details Block of WWPN Identifiers. WWPN Blocks From 20 00 00 25 85 21 08 00	्र 25स्	<u>5 +</u> T-MEN +
New Command Palette Navigate Intersight with Oble K or g to Help > Command Palette				
		Cancel		Back Create

**Step 4.** Click **Create** to finish creating the WWPN pool.

≡	disco Intersight	🔆 Infrastructure Service 🗸	Q Search	Ø	42 Q 💿 🚾	0	R
@ ©	Overview Analyze	Templates > Create UCS Server Profile Template Create SAN Connectivity Policy					
Nav	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	Add vHBA	<ul> <li>✓ ●</li> </ul>	~ 0			
		Cancel				Add	ľ,

Step 5.	Scroll down if needed to	add the Slot ID, Switch ID (fo	or example, A) and PCI Order from Table 15.
---------	--------------------------	--------------------------------	---

≡	dudu Intersight	🎉 Infrastructure Service 🗸	Q. Search	 00.00	0	۹
* ©	Overview Analyze	Templates > Create UCS Server Profile Template Create SAN Connectivity Policy				
0 ,0	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure Profiles Profiles Pools	Placement  Simple Advanced  Advanced  Advanced  Advanced  Advanced  Advanced  Advanced  Advanced  Cutomatic Stot ID Assignment  Advanced  Cutomatic Stot ID Assignment  Advanced  Cutom  PCI Link  PCI Link PCI Link PCI Link PCI Link PCI Li				
Nev	Command Palette  usts Intersight with Ctrl+K or gi     Command Palette	PCI Order 5 0				
		Cancel			Add	Ĩ.

### Procedure 10. Create Fibre Channel Network Policy for SAN B

**Note:** In this deployment, VSAN 102 is used for vHBA FC-B.

**Step 1.** Scroll down within the Create SAN Connectivity Policy dialogue and click **Select Policy** under Fibre Channel Network and in the pane on the right, click **Create New.** 

=	dudu Intersight	🔆 Infrastructure Service 🗸			Q Search	Ø	<b>4</b> 1	000	0	R
* 0	Overview Analyze	Templates > Create UCS Server Prof								
0	Servers	^	Switch ID * B PCI Order	× 0						
	Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems		5 Persistent LUN Bindings	0.0						
,0	Configure Profiles	·	Persistent LUN Bindings © Fibre Channel Network * © Select Policy							
	Templates Policies Pools		Fibre Channel GoS * © Select Policy							1
Nav	Command Palette     Gate Intercept with Ctel+K or gr		Fibre Channel Adapter * © Select Policy 🖥 FC Zone ©							
to H	elp > Command Paletta	Cancel	Select Policy(s)						Add	

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-Network-SAN-B).

**Step 3.** Specify the VSAN ID for Fabric B (for example, 102).

≡ dada Intersight	🍂 Infrastructure Service 🗸		Q Search	0 4 0 🚥 0 A
<ul> <li>Overview</li> <li>Analyze</li> </ul>	Templates > Create UCS Server Profile Create Fibre Chan	Template  Create SAN Connectivity Policy Network		
Servers Chassis Fabric Interconcects HyperFiex Clusters Integrated Systems	Ceneral Ceneral Policy Details	Policy Details Add policy details Fibre Channel Network VSAN ID 102	₹ 6 1 april	UCS Server (Bitendatione) UCS Server (PI-Attached)
Navigale Intersight with Coll+K or g to Help > Command Palette		Cancel		Back Create

Step 4. Click Create.

**Step 5.** Select the Fibre Channel QoS Policy for SAN B. Click **Select Policy** under Fibre Channel QoS and in the pane on the right, select the previously created QoS policy **AA21-FC-QoS-Policy**.

**Step 6.** Select the Fibre Channel Adapter Policy for SAN B. Click **Select Policy** under Fibre Channel Adapter and in the pane on the right, select the previously created Adapter policy **AA21-FC-Adapter-Policy**.

Step 7. Click Add to add the vHBA FC-B.

#### Procedure 11. Create the FC-NVMe vHBAs

**Note:** To configure the FC-NVMe, two vHBAs, one for each fabric, must be added to the server profile template. These vHBAs are in addition to the FC boot from SAN vHBAs, FC-A and FC-B.

Table 17.	vHBA	placement	for	NVMe-o-FC

vNIC/vHBA Name	Slot	Switch ID	PCI Order
FC-NVMe-A	MLOM	A	6
FC-NVMe-B	MLOM	В	7

### Procedure 12. Configure vHBA FC-NVMe-A

### Step 1. Click Add vHBA.

**Step 2.** Name the vHBA **FC-NVMe-Fabric-A**. For vHBA Type and choose **fc-nvme-initiator** from the drop-down list.

**Step 3.** Click **Select Pool** under WWPN Address Pool and in the pane on the right, select the previously created pool AA21-WWPN-Pool-A.

=	cisco Intersight	🚴 Infrastructure Service 🗸	Q Search	A D ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (
ی ان	Overview Analyze	Templates > Create UCS Server Profile Template Create SAN Connectivity Policy		
0	Operate ^ Servers Chassis Fabric Interconnects	Add vHBA General Name * FC-NVMe-A	vHBA Type fc-nvme-initiator v 0.	
,o	HyperFlex Clusters Integrated Systems Configure Profiles	Pin Group Name v o		_
	Templates Policies Pools	WWPN Paol * © Selected Pool AA21-WWPN-Pool-A × Φ Ø		
Navi	Command Palette	Simple Advanced		~
		Cancel		Add

**Step 4.** With the **Advanced** option of **Placement** selected, scroll down if required to add the **Slot ID**, **Switch ID** (for example, A), and **PCI Order** from <u>Table 16</u>.

$\equiv$ $\frac{-\mathrm{dealer}}{\mathrm{case}}$ Intersight	🍂 Infrastructure Service 🛩	Q Search	A © 🕫 ¢ 🕫 O 🖌
Øverview Overview Analyze	Templates > Create UCS Server Profile Template Create SAN Connectivity Policy		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> </ul>	Placement  Simple Advanced  Advanced  Advanced  Advanced  Advanced  Advanced  Control  Advanced  Control  Contr		
Templates Policies Pools	PCLUrix 6 C C Switch ID * A C C		_
New Command Palette Navigate intersight with Cb1+K or g to Help > Command Palette	PCI Order	1	
	Cancel		Add

**Step 5.** Scroll down within the Create SAN Connectivity Policy dialogue and click **Select Policy** under Fibre Channel Network and in the pane on the right, select the previously created policy for SAN A, **AA21-FC-Network-SAN-A**.

**Step 6.** Click **Select Policy** under Fibre Channel QoS and in the pane on the right, select the previously created QoS policy **AA21-FC-QoS-Policy**.

#### Procedure 13. Create FC-NVMe-Initiator 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. The FC-NVMe-Initiator Fibre Channel Adapter Policy is optimized for FC-NVMe.

Step 1. Click Select Policy under Fibre Channel Adapter and in the pane on the right, click Create New.

**Step 2.** Verify that the correct organization is selected from the drop-down list (for example, AA21) and provide a name for the policy (for example, AA21-FC-NVMe-Initiator-Adapter-Policy).

**Step 3.** Under Fibre Channel Adapter Default Configuration, click **Select Default Configuration**.

Step 4. Select FCNVMelnitiator and click Next.

≡ "bubb Intersig	iht 📔 🕽	\$ Infrastructure Service ∨		Q Search	0	₽	Q 🙆 🗛	0	<u>م</u>
<ul> <li>Overview</li> <li>Analyze</li> </ul>		Templates > Create UCS Server Profile Create Fibre Char	Template > Create SAN Connectivity Policy						
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconne</li> <li>HyperFlex Cluste</li> <li>Integrated System</li> </ul>	'5	General     Policy Details	General Add a name, description and tag for the policy. Organization * AA21 ~ Name * AA21-FC-NVMe-initiator-Adapter-Policy						
Configure Profiles Templates Policies Pools New Command Palette Navigate Intersight with Ctr to Help > Command Palette	+K or go		Set Tags Description Fibre Channel Adapter Default Configuration Selected Default Configuration FCNVMelnitiator ×						
			< Cancel					Next	ļ

**Step 5.** Do not change the default values on the Policy Details screen.

**Step 6.** Click **Create** to finish creating the Fibre Channel adapter policy.

Step 7. Click Add to create vHBA FC-NVMe-A.

#### **Procedure 14.** Configure vHBA FC-NVMe-Fabric-B

Step 1. Click Add vHBA.

Step 2. Name the vHBA FC-NVMe-B. For vHBA Type, select fc-nvme-initiator from the drop-down list.

**Step 3.** Click **Select Pool** under WWPN Address Pool and in the pane on the right, select the previously created pool **AA21-WWPN-Pool-B**.

	cisco Intersight	🔆 Infrastructure Service 🗸		Q Search	⊘ ⊄	1 0 💷 🏧	0	۹
*	Overview Analyze	Templates > Create UCS Server Profile Templa Create SAN Connect						~~
Nov	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	A WWF WWFM Selection Place	roup Name. v @	vHBA.Type fc-rivme-initiator - 0				
		Cancel	Automatic Slot ID Assignment 0				Add	, ,

Step 4.Under Advanced Placement, provide the slot ID, Switch ID (for example, B) and PCI Order fromTable 16.

=	ence Intersight	💐 Infrastructure Service 🗸		Q Search	0	41	0 0 43	0	۹
*	Overview Analyze	Templates > Create UCS Server Profile							~ ~
ø ,e [	Operate ^ Servers / Chassis / Fabric Interconnects / HyperFlex Clusters / Integrated Systems / Configure ^ Profiles / Policies / Policies // Policies		Placement Simple Advanced Advanced Advanced Advanced Advanced Advanced Control Advanced Control Contro	0 0 0-1					
Nev	Command Palette     sate Intersight with Ctrl+K or go     sip > Command Palette		PCI Order 21	<u>5 e</u>					v
		Cancel						Add	

**Step 5.** Scroll down within the Create SAN Connectivity Policy dialogue and click **Select Policy** under Fibre Channel Network and in the pane on the right, select the previously created policy for SAN B, AA21-FC-Network-SAN-B.

**Step 6.** Click **Select Policy** under Fibre Channel Network and in the pane on the right, select the previously created policy for SAN B, AA21-FC-Network-SAN-B.

**Step 7.** Click **Select Policy** under Fibre Channel QoS and in the pane on the right, select the previously created QoS policy AA21-FC-QoS-Policy.

**Step 8.** Click **Select Policy** under Fibre Channel Adapter and in the pane on the right, select the previously created Adapter policy AA21-FC-NVMe-Initiator-Adapter-Policy.

Step 9. Click Add to add the FC-NVMe vHBA.

#### **Procedure 15.** Verify and create all vHBAs

**Step 1.** Verify that all four vHBAs are added to the SAN connectivity policy.

	Templates > Create UCS Server	Profile Template					
Overview		nnectivity Policy					
) Analyze	Cleate SAN CO	Intectivity Folicy					
0) Operate	∧	WWNN					
Servers	2 Policy Details	Pool Static					
Chassis		WWNN Pool * ©					
Fabric Interconnects		Selected Pool AA21-WWNN-Pool	×   ©   Ø				
HyperFlex Clusters							
Integrated Systems		For manual placement option	you need to specify placement for eac	th vHBA. Learn more at Help (	Center		
Configure	~	Add vHBA				Graphic vHBA	s Editor
Configure Profiles	^			Aitams found 55		<u></u>	
Conniguro	^	Add vHBA	: Switch ID		0 – per page Group	Graphic vHBA	
Profiles		Add Filter	Switch ID			EE 1 of 1 2 2	© : \$
Profiles Templates		Add Filter		PCI Order : Pin C		WWPN Pool	: \$ 
Profiles Templates Policies		Name Slot D	A	PCI Order : Pin C 4 -		E C 1 of 1 2 2 WWPN Pool AA21-WWPN-Pool	© : Ø 
Profiles Templates Policies		Name Stot ID FC-A MLOM	A B	PCI Order         Pin 0           4         -           5         -		K C 1 of 1 2 2     WWPN Pool     AA21-WWPN-Pool     AA21-WWPN-Pool	. Ø . Ø 

**Step 2.** Click **Create** to create the SAN connectivity policy with FC-NVMe support.

### Procedure 16. Review Summary

**Step 1.** After the LAN connectivity policy and SAN connectivity policy have been created, click **Next** to continue to the **Summary** screen.

**Step 2.** On the **Summary** screen, verify that the intended policies are mapped to the appropriate settings.

### Figure 3. Compute Configuration

≡	disco Intersight	🖧 Infrastructure Service 🗸		Q Search	ତ ୟ ଦ <b>ଭ</b> 🐼 ତ   ୧
	Overview Analyze Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	<ul> <li>Infrastructure Service</li> <li>Templates</li> <li>Create UCS Server F</li> <li>Oreneral</li> <li>Ormpute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Profile Template Summary Verify details of the template and the poli General Template Name FC-Boot-FC-NVMe-Template Target Platform UCS Server (FI-Attached) Compute Configuration	icles, resolve errors and deploy. Organization AA21 ement Storage Network	Errors/Warnings
Nav	Templates Policies Pools Command Palette Kgate Intersight with Ctrl+K or go leip > Command Palette		BIOS Boot Order Virtual Media		AA21-Intel-M7-VSI-BIOS AA21-FC-Boot-Order AA21-KVM-Mount-Media 🗐

### Figure 4. Management Configuration

=	"listly Intersight	🚴 Infrastructure Service 🗸			Q Search	0	¢1 Q 🙆 🜆	ଡ	
\$ 0	Overview Analyze	← Templates Create UCS Server I	Profile Template	9					
Ø	Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems	<ul> <li>General</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Summary Verify details of the template of General Template Name FC-Boot-FC-NVMe-Templo Target Platform UCS Server (FI-Attached)		rs and deploy. Organization AA21				
	Profiles		Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warning (0)	š	
	Templates		IMC Access				AA21-IMC-Access-Po	licy 🗐	
	Policies		IPMI Over LAN				AA21-Enable-IPMIoLAN-Po	licy 🗐	
	Pools		Virtual KVM				AA21-KVM-Po	licy 🗊	
Nav	Command Palette	٢.	Close				Back Derive S	rofiles	

### Figure 5. Network Configuration

≡	۰۱۱۰۰۱۱۰ Intersight 🌲	Infrastructure Service 🗸			Q Search	Ø	¢1 Q 🐽 💿	R
:@: ©	Overview Analyze	← Templates Create UCS Server P	rofile Template					
(Ø)	Operate     ^       Servers     -       Chassis     -       Fabric Interconnects     -       HyperFlex Clusters     -       Integrated Systems     -	<ul> <li>General</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> </ul>	Summary Verify details of the template and General Template Name FC-Boot-FC-NVMe-Template Target Platform UCS Server (FI-Attached)		teploy. Organization AA21			
<u>م</u>	Configure ^ Profiles Templates Policies Pools	3 Summary		fanagement configuration	Storage Configuration	Network Configuration	Errors/Warnings (0) AA21-FC-Boot-LanCon-Pol AA21-FC-NVMe-FC-SAN	
Navi	Command Palette × gate Intersight with CtrI+K or go elp > Command Palette	K	Close				Back Derive Profiles	

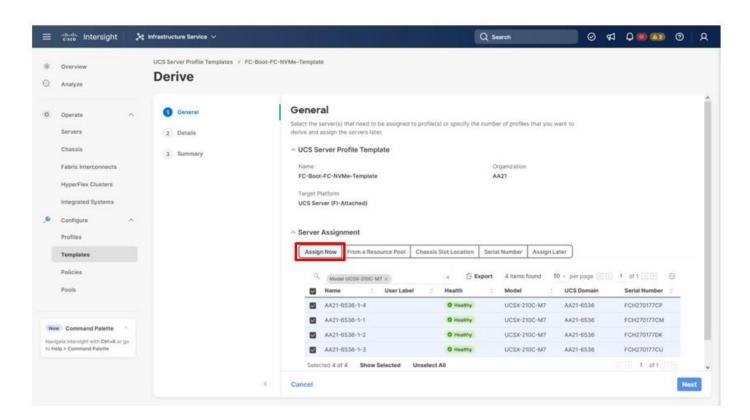
# **Cisco UCS IMM Setup Completion**

#### **Procedure 1.** Derive Server Profiles

**Step 1.** From the Server profile template Summary screen, click **Derive Profiles**.

**Note:** This action can also be performed later by navigating to **Templates**, clicking "..." next to the template name and selecting **Derive Profiles**.

**Step 2.** Under Server Assignment, select **Assign Now** and select Cisco UCS X210c M7 server(s). You can select one or more servers depending on the number of profiles to be deployed. Optionally, provide a Model filter in this screen to exclude additional connected servers as required.



Step 3. Click Next.

Note: Cisco Intersight will fill in the default information for the number of servers selected (4 in this case).

**Step 4.** Adjust the fields as needed. It is recommended to use the server hostname for the Server Profile name.

≡ disco Intersight	📲 Infrastructure Service 🛩		Q Search	0 4 0	
<ul> <li>Overview</li> <li>Analyze</li> </ul>	UCS Server Profile Templates > FC-Boot-FC Derive	-NVMe-Template			
0. Operate Servers Chassis Fabric Interconnects	Cenerat     Details     Summary	Description	Set Tags		
HyperFlex Clusters Integrated Systems	^	Profile Name Prefix aa21-eso1 Name * aa21-eso1	Digits Count 1 0 Organization * AA21	1	Assigned Serv AA21-0538-1- 4
Templates Policies Pools		2 Name * aa21-eso-2	Organization * AA21		Assigned Ser AA21-6536-1-1
New Command Palette		3 Name* a#21+tsxl-3	Organization * AA21	× .	Assigned Ser AA21-6536-1- 2
to Help > Command Palette		4 Name * as21-exi-4	Organization * AA21	ų,	Assigned Serv AA21-6536-1- 3

Step 5. Click Next.

**Step 6.** Verify the information and click **Derive** to create the Server Profile(s).

E disco Intersight 🎝	€ Infrastructure Service →		Q	Search	ମ କ୍ 🌒 🐼 🕅
I Overview ), Analyze	UCS Server Profile Templates > FC-Boot-FC Derive	C-NVMe-Template			
Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems Configure ^	<ul> <li>General</li> <li>Details</li> <li>Summary</li> </ul>	Summary Summary of the profiles that need to Ceneral Template Name FC-Boot-FC-NVMe-Template Target Platform UCS Server (FI-Attached)		d from the profile template. Organization AA21	
Profiles Templates		UCS Server Profiles	Assigned Server	Organization	
		aa21-esxi-1	AA21-6536-1-4	AA21	
Policies		aa21-esxi-2	AA21-6536-1-1	AA21	
Pools		aa21-esxi-3	AA21-6536-1-2	AA21	
		aa21-esxi-4	AA21-6536-1-3	AA21	
Command Palette     sate Intensight with Ctrl+K or go			igement Storage iguration Configu	Network ration Configuration	Errors/Warnings (0)
elp > Command Palette		BIOS			AA21-Intel-M7-VSI-BIOS
	¢	Close			Back Deri

**Step 7.** In the **Infrastructure Service > Configure > Profiles > UCS Server Profiles** list, select the profile(s) just created and click the ... at the top of the column and select **Deploy**. Click Deploy to confirm.

**Step 8.** Cisco Intersight will start deploying the server profile(s) and will take some time to apply all the policies. Use the Requests tab at the top right-hand corner of the window to see the progress.

When the Server Profile(s) are deployed successfully, they will appear under the Server Profiles with the status of OK.

=	tude Intersight	🕯 Infrastructure Service 🗸						Q Search		
ł.	Overview	Profiles								
¢	Operate ^	HyperFlex Cluster Profiles	UCS Chassis Profiles U	CS Domain Profiles	S Server Profiles Kubernetes C	luster Profiles				
	Chassis	* All UCS Server Prof @	.+						Create UCS Server Profile	
	Fabric Interconnects HyperFlex Clusters	-ZOBLAS	P O B   - 9, Add Fitar					Export 4 items found 19 v per page 1 1 of 1 1		
	Storage Virtualization Integrated Systems	(D OK 4)	nconsistency Reason	Target Platform					н	
	Analyze ^	Name	Status		Target Platform	UCS Server Tomplate	Server	Last Update	: 4	
	Explorer New	aa21-esxi-4	() OK		UCS Server (FI-Attached)	FC-Boot-FC-NVMe-Template	AA21-6536-1-4	4 hours ago		
	Configure ^	aa21-essi-2	() OK		UCS Server (FI-Attached)	FC-Boot-FC-NVMe-Template	AA21-6536-1-2	4 hours ago		
	Profiles	🗋 aa21-esxi-3	(C OK)		UCS Server (FI-Attached)	FC-Boot-FC-NVMe-Template	AA21-6538-1-3	4 hours ago		
	Templates	aa21-esxi-1	(C) OK		UCS Server (FI-Attached)	FC-Boot-FC-NVMe-Template	AA21-6536-1-1	4 hours ago		
	Policies								1 of 3 1	
	Pools									
lavi	Command Palette     P     Gate Intersight with Ctrl+K or go     letp > Command Palette									

# **Tunneled KVM Setting within System**

Additional settings within the System section of Intersight were mentioned during the Server Profile Template creation process to fully enable Tunneled KVM.

If this is still needed, complete the following procedure.

Procedure 1. Tunneled KVM Setting

Step 1. Go to System > Settings > Security and Privacy and click Configure.

dade Intersight al	System ~	and the second	Q Search	0440
Settings	Settings			
Admin	Access Details Access Details Notifications			Configure
Sessions Licensing	AutheamCatton Adversal Single Tige-On Denset Names Case ID Disablesed	rsight		
registe hitsrught with DNHK or ge- Help - Command Pasitio	Trusted Certificans Turned Certificans Turned Certificans Access & RewardsCert PAccess Management Becarty & Privacy Users	Iguardian		
	Groups Bales Organizations			
	Ani u			

### Step 2. Turn on Allow Tunneled vKVM Launch and Allow Tunneled vKVM Configuration.

≡ thete Intersight al	Bystam -	Q Search	0 4	#1 C	0	A
View Intersignt     Sommark     Somma	Settings Configure Security & Privacy Settings	Q Seers		<i>a</i> (		<u>д</u>
	Back				E	lave

Step 3. Click Save to apply the changes.

# Cisco MDS SAN Switch Configuration

This chapter contains the following:

- <u>Physical Connectivity</u>
- Base Configuration
- Global Configuration on Both Switches
- Port and Port-Channel Configuration
- <u>Configure Device Aliases and SAN Zoning</u>

This section explains how to configure the Cisco MDS 9000s for use in the environment. The configuration detailed in this section covers configuring Fibre Channel and FC-NVMe storage access.

### **Physical Connectivity**

Follow the physical connectivity guidelines explained in the <u>Physical Topology</u> section.

### **Base Configuration**

The following procedures describe how to configure the Cisco MDS switches for use in the Adaptive Solutions VSI environment. This procedure assumes you are using the Cisco MDS 9124V with NX-OS 9.3(2).

#### Procedure 1. Set up Cisco MDS 9124V A and 9124V B

**Note:** On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning. Enter y to get to the System Admin Account Setup.

**Step 1.** Configure the switch using the command line:

```
---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]: Enter

Enter the password for "admin": <password>

Confirm the password for "admin": <password>

Would you like to enter the basic configuration dialog (yes/no): yes

Create another login account (yes/no) [n]: Enter

Configure read-only SNMP community string (yes/no) [n]: Enter

Configure read-write SNMP community string (yes/no) [n]: Enter

Enter the switch name : <mds-A-hostname>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter

Mgmt0 IPv4 address : <mds-A-mgmt0-ip>

Mgmt0 IPv4 netmask : <mds-A-mgmt0-netmask>

Configure the default gateway? (yes/no) [y]: Enter
```

IPv4 address of the default gateway : <mds-A-mgmt0-gw> Configure advanced IP options? (yes/no) [n]: Enter Enable the ssh service? (yes/no) [y]: Enter Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter Number of rsa key bits <1024-2048> [1024]: Enter Enable the telnet service? (yes/no) [n]: Enter Configure congestion/no credit drop for fc interfaces? (yes/no) [v]: Enter Enter the type of drop to configure congestion/no credit drop? (con/no) [c]: Enter Enter milliseconds in multiples of 10 for congestion-drop for logical-type edge in range (<200-500>/default), where default is 500. [d]: Enter Enable the http-server? (yes/no) [y]: Enter Configure clock? (yes/no) [n]: Enter Configure timezone? (yes/no) [n]: Enter Configure summertime? (yes/no) [n]: Enter Configure the ntp server? (yes/no) [n]: Enter Configure default switchport interface state (shut/noshut) [shut]: Enter Configure default switchport trunk mode (on/off/auto) [on]: auto Configure default switchport port mode F (yes/no) [n]: y Configure default zone policy (permit/deny) [deny]: Enter Enable full zoneset distribution? (yes/no) [n]: y Configure default zone mode (basic/enhanced) [basic]: Enter Review the configuration. Step 4.

Would you like to edit the configuration? (yes/no) [n]: Enter Use this configuration and save it? (yes/no) [y]: Enter

**Step 5.** To set up the initial configuration of the Cisco MDS B switch, repeat steps 1 and 2 with appropriate host and IP address information.

## **Global Configuration on Both Switches**

#### **Procedure 1.** Enable Features

Note: Run on both Cisco MDS 9124V A and Cisco MDS 9124V B Switches.

Step 1. Log in as admin.

Step 2. Run the following commands:

configure terminal feature npiv feature fport-channel-trunk

### **Procedure 2.** Add NTP Servers and Local Time Configuration

Note: Run on both Cisco MDS 9124V A and Cisco MDS 9124V B.

**Step 1.** From the global configuration mode, run the following command:

```
ntp server <ntp-server-ip>
clock timezone <timezone> <hour-offset> <minute-offset>
clock summer-time <timezone> <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month>
<end-time> <offset-minutes>
```

**Note:** It is important to configure the network time so that logging time alignment, any backup schedules, and SAN Analytics forwarding are correct. For more information on configuring the timezone and daylight savings time or summer time, see <u>Cisco MDS 9000 Series Fundamentals Configuration Guide. Release 9.x.</u> Sample clock commands for the United States Eastern timezone are:

clock timezone EST -5 0
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60

### **Port and Port-Channel Configuration**

#### Procedure 1. Configure Individual Ports on Cisco MDS 9124V A

**Step 1.** From the global configuration mode, run the following commands:

```
interface port-channel101
channel mode active
switchport trunk allowed vsan <vsan-a-id for example, 101>
switchport description <ucs-domainname>-A
switchport speed 32000
no shutdown
interface fc1/1
switchport description <ucs-domainname>-A:1/35/1
channel-group 101 force
port-license acquire
no shutdown
interface fc1/2
switchport description <ucs-clustername>-A:1/35/2
channel-group 101 force
port-license acquire
no shutdown
interface fc1/3
switchport description <ucs-domainname>-A:1/35/3
channel-group 101 force
port-license acquire
no shutdown
interface fc1/4
switchport description <ucs-clustername>-A:1/35/4
channel-group 101 force
port-license acquire
no shutdown
interface fc1/5
switchport description <vsp-name>-0:1a
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
interface fc1/6
switchport description <vsp-name>-0:1b
```

```
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
interface fc1/7
switchport description <vsp-name>-1:2a
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
interface fc1/8
switchport description <vsp-name>-1:2b
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
```

**Note:** If VSAN trunking was not being configured for the port-channel connecting the Cisco UCS Fabric Interconnects to the Cisco MDS switches, do not enter "switchport trunk allowed vsan <vsan-a-id>" for interface port-channel101.

#### Procedure 2. Configure Individual Ports on Cisco MDS 9124V B

**Step 1.** From the global configuration mode, run the following commands:

```
interface port-channel102
channel mode active
switchport trunk allowed vsan <vsan-b-id for example, 102>
switchport description <ucs-domainname>-B
switchport speed 32000
no shutdown
interface fc1/1
switchport description <ucs-domainname>-B:1/35/1
channel-group 102 force
port-license acquire
no shutdown
interface fc1/2
switchport description <ucs-clustername>-B:1/35/2
channel-group 102 force
port-license acquire
no shutdown
interface fc1/3
switchport description <ucs-domainname>-B:1/35/3
channel-group 102 force
port-license acquire
no shutdown
interface fc1/4
switchport description <ucs-clustername>-B:1/35/4
channel-group 102 force
port-license acquire
no shutdown
interface fc1/5
switchport description <vsp-name>-0:3a
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
1
interface fc1/6
```

```
switchport description <vsp-name>-0:3b
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
interface fc1/7
switchport description <vsp-name>-1:4a
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
interface fc1/8
switchport description <vsp-name>-1:4b
switchport speed 32000
switchport trunk mode off
port-license acquire
no shutdown
```

**Note:** If the VSAN trunk was not being configured for the port-channel connecting the Cisco UCS Fabric Interconnects to the Cisco MDS switches, do not enter "switchport trunk allowed vsan <vsan-b-id>" for interface port-channel102.

#### Procedure 3. Create VSANs on Cisco MDS 9124V A

**Step 1.** From the global configuration mode, run the following commands:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/5
Traffic on fc1/5 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-a-id> interface fc1/6
Traffic on fc1/6 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-a-id> interface fc1/7
Traffic on fc1/7 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-a-id> interface fc1/8
Traffic on fc1/8 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-a-id> interface port-channel101
exit
```

#### Procedure 4. Create VSANs on Cisco MDS 9124V B

**Step 1.** From the global configuration mode, run the following commands:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/5
Traffic on fc1/5 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-b-id> interface fc1/6
Traffic on fc1/6 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-b-id> interface fc1/7
Traffic on fc1/7 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-b-id> interface fc1/7
Traffic on fc1/7 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-b-id> interface fc1/8
Traffic on fc1/8 may be impacted. Do you want to continue? (y/n) [n] y
vsan <vsan-b-id> interface port-channel102
```

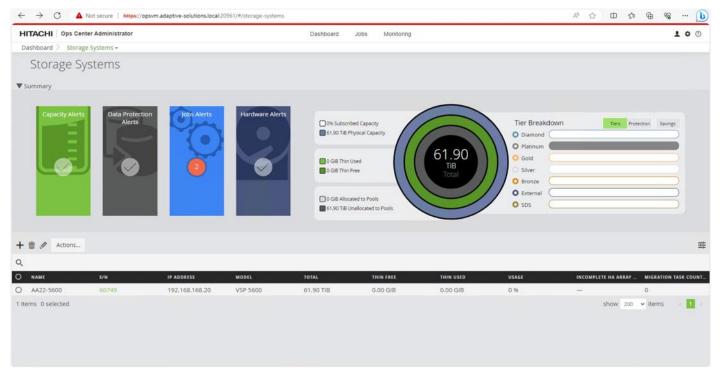
#### exit

## **Configure Device Aliases and SAN Zoning**

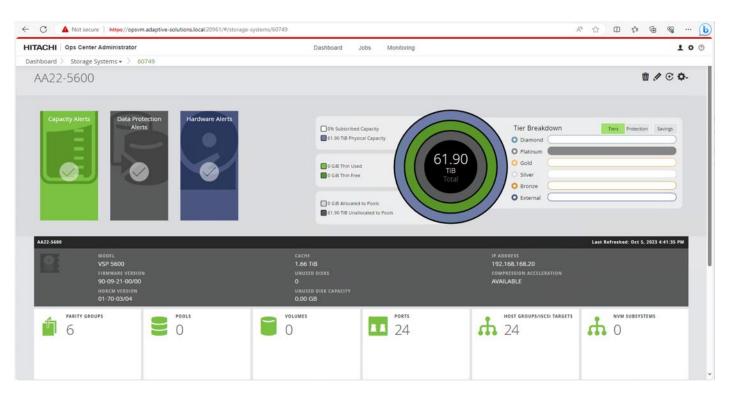
#### Procedure 1. Gather Target and Initiator WWPNs

These procedures will gather the target and initiator WWPN information from the Hitachi VSP controllers and the Server Profiles associated with the UCS X-Series servers.

Step 1. Go to Ops Center Administrator Dashboard > Storage Systems > [S/N of VSP listing]



**Step 2.** From the resulting view, click **Ports**.



**Step 3.** Find and gather the WWN for each port connected to the MDS used for FC-SCSI or FC-NVMe traffic.

HITACHI Ops Center	r Administrator		Dashboard Jobs Monitoring			10
Dashboard > Storage S	Systems + > 60749 > Ports +					
Ports						an 🕫
Summary						
	Fibre				ISCSI	
	SCSI				NVMe	
1						
۹						
) PORT ID	wwn	SPEED	FABRIC, CONNECTION TYPE	SECURITY	VSM PORT	ATTRIBUTE
CL1-A	50:06:0E:80:08:ED:4D:00	Auto	Fabric ON / Point-to-point	No	No	Target
) CL1-B	50:06:0E:80:08:ED:4D:01	Auto	Fabric ON / Point-to-point	No	No	Target
CL1-C	50:06:0E:80:08:ED:4D:02	Auto	Fabric ON / Point-to-point	No	No	Target
CL2-A	50:06:0E:80:08:ED:4D:10	Auto	Fabric ON / Point-to-point	No	No	Target
	50:06:0E:80:08:ED:4D:11	Auto	Fabric ON / Point-to-point	No	No	Target
CL2-B	50:06:0E:80:08:ED:4D:11 50:06:0E:80:08:ED:4D:12	Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No	No No	Target Target
) CL2-8 ) CL2-C						
CL2-8 CL2-8 CL2-C CL3-A	50:06:0E:80:08:ED:4D:12	Auto	Fabric ON / Point-to-point	No	No	Target
CL2-B CL2-C CL3-A CL3-B	50:06:0E:80:08:ED:4D:12 50:06:0E:80:08:ED:4D:20	Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No	No No	Target Target
) CL2-8 ) CL2-C ) CL3-A ) CL3-B ) CL3-C	50:06:0E:80:08:ED:4D:12 50:06:0E:80:08:ED:4D:20 50:06:0E:80:08:ED:4D:21	Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No	No No No	Target Target Target
) CL2-8 ) CL2-C ) CL3-A ) CL3-B ) CL3-B ) CL3-C ) CL4-A	50:06:0E:80:08:ED:4D:12 50:06:0E:80:08:ED:4D:20 50:06:0E:80:08:ED:4D:21 50:06:0E:80:08:ED:4D:22	Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No	No No No	Target Target Target Target
) c12-8 ) c12-c ) c13-A ) c13-8 ) c13-8 ) c13-c ) c14-A ) c14-A ) c14-B	50:06:0E:80:08:ED:4D:12 50:06:0E:80:08:ED:4D:20 50:06:0E:80:08:ED:4D:21 50:06:0E:80:08:ED:4D:22 50:06:0E:80:08:ED:4D:30	Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No	No No No No	Target Target Target Target Target Target
C C2-8 C C2-C C C3-A C C3-8 C C3-8 C C3-8 C C3-C C C4-A C C4-8	50:06:0E:80:08:ED:4D:12 50:06:0E:80:08:ED:4D:20 50:06:0E:80:08:ED:4D:21 50:06:0E:80:08:ED:4D:22 50:06:0E:80:08:ED:4D:30 50:06:0E:80:08:ED:4D:31	Auto Auto Auto Auto Auto Auto	Fabric ON / Point-to-point Fabric ON / Point-to-point	No No No No No	No No No No No	Target Target Target Target Target Target Target

**Step 4.** Connect to Cisco Intersight to gather the initiator WWPN information for the servers.

Step 5. Find the Server Profiles for each host by going to Infrastructure Service > Configure > Profiles > UCS Server Profiles > <Desired Server Profile> > General > Configuration > Connectivity. The required WWPNs can be found under HBA Interfaces.

verview	← Server Profiles									<u> </u>
	aa21-esxi-1								Actio	on
perate ^	General Server Inventory									
hassis	Details	Configuration								
abric Interconnects	Status	General Identifiers Con	nectivity							
rtualization	Name aa21-esxi-1	~ vNICs								
tegrated Systems	User Label	Q_ Add Filter							1 5 8 0	l
nalyze ^	•				PCI Order	Slot ID			·	_
cplorer New	Target Platform									
onfigure										
			00:25:85:21:0A:01							
		03-vSD0-8	00:25:85:21:08:01	MAC-Pool-B	3	MLOM	0 B	Off		
emplates	Last Update 21 hours ago								1 of 1 🗵 🗵	
blicles	Description	vHBAs								
ools	-									
	Organization								1 2 2 0	
	AA21		5-05-01-01-00						-	
	Server Assignment									
Intensight with Ctrl+K or go Command Palette	Assigned Server									
	AA21-6536-1-1									
	Assignment Type Specific Server	FC-NVMe-8 207003012	5/85:21:08:01	AA21-WWPN-P001-B	/		MLOM		1 of 1 🗵 🗵	
	Tags Set									
	No Tags									
	ric Interconnects parFlex Clusters tutalization signated Systems sityze sityze New filigure New filigure  filigure  filigure  sityse si	And a server type to the server	wrice laterconnects   porFree Clusters   hastication   segrated Systems   atyze   atyze   atyze   atyze   atyze   atyze   Trapet Flatform   UCS Server (FF-Attached)   Treplate Name   Febre   Treplate Name   Forstres   Last Update   21 hours ago   Description   -   Organization   Atz1   Server Assignment   Assigned Server   Atz1   Server Assignment   Assigned Server   Assigned Server   Assigned Server   Tags	<ul> <li>Add Selection</li> <li>Add Selectio</li></ul>	Active distances of the formation of	wick laterconnects   por Fee Clusters   haskitation   porters Clusters   haskitation   ag2=esi-1   ter Label   ag2 a b Filter   Triggt Parform   UCS Geners (Ft-Attached)   Disportation   Triggt Parform   UCS Geners   Disportation   Triggt Parform   UCS Geners   Disportation   Attached Parific Parford	wick laterconnects   por Free Clusters   hank   basic   basic <td>skinterconcels   skinterconcels   skint</td> <td>Alas definition of lange of</td> <td>Sala   Sala   Sala</td>	skinterconcels   skint	Alas definition of lange of	Sala   Sala

#### Procedure 2. Create Device Aliases for Fabric A used to Create Zones

**Step 1.** From the global configuration mode of the Cisco MDS 9124V-A, run the following commands:

device-alias r	mode	enhanced
device-alias d	datak	base
device-alias r	name	<vsp-name>-0-1a pwwn <vsp-0:1a-wwpn></vsp-0:1a-wwpn></vsp-name>
device-alias r	name	<vsp-name>-1-2a pwwn <vsp-1:2a-wwpn></vsp-1:2a-wwpn></vsp-name>
device-alias r	name	<server1-hostname> pwwn <server1-wwpna></server1-wwpna></server1-hostname>
device-alias r	name	<pre><server2-hostname> pwwn <server2-wwpna></server2-wwpna></server2-hostname></pre>
device-alias r	name	<server3-hostname> pwwn <server3-wwpna></server3-wwpna></server3-hostname>
device-alias r	name	<server4-hostname> pwwn <server4-wwpna></server4-wwpna></server4-hostname>
device-alias r	name	<vsp-name>-0-1b-fc-nvme pwwn <vsp-0:1b-wwpn></vsp-0:1b-wwpn></vsp-name>
device-alias r	name	<vsp-name>-1-2b-fc-nvme pwwn <vsp-0:2b-wwpn></vsp-0:2b-wwpn></vsp-name>
device-alias r	name	<pre><server1>-fc-nvme pwwn <fc-nvme-server1-wwpna></fc-nvme-server1-wwpna></server1></pre>
device-alias r	name	<pre><server2>-fc-nvme pwwn <fc-nvme-server2-wwpna></fc-nvme-server2-wwpna></server2></pre>
device-alias r	name	<pre><server3>-fc-nvme pwwn <fc-nvme-server3-wwpna></fc-nvme-server3-wwpna></server3></pre>
device-alias r	name	<pre><server4>-fc-nvme pwwn <fc-nvme-server4-wwpna></fc-nvme-server4-wwpna></server4></pre>

#### Step 2. Commi

Commit the device alias database changes:

device-alias commit

#### Procedure 3. Create Device Aliases for Fabric B used to Create Zones

**Step 1.** From the global configuration mode of the Cisco MDS 9124V-B, run the following commands:

```
device-alias mode enhanced
device-alias database
device-alias name <vsp-name>-0-3a pwwn <vsp-0:1a-wwpn>
```

device-alias	name	<vsp-name>-1-4a pwwn <vsp-1:2a-wwpn></vsp-1:2a-wwpn></vsp-name>
		<pre><server1-hostname> pwwn <server1-wwpnb></server1-wwpnb></server1-hostname></pre>
		<pre><server2-hostname> pwwn <server2-wwpnb></server2-wwpnb></server2-hostname></pre>
device-alias	name	<pre><server3-hostname> pwwn <server3-wwpnb></server3-wwpnb></server3-hostname></pre>
device-alias	name	<pre><server4-hostname> pwwn <server4-wwpnb></server4-wwpnb></server4-hostname></pre>
device-alias	name	<vsp-name>-0-3b-fc-nvme pwwn <vsp-0:1b-wwpn></vsp-0:1b-wwpn></vsp-name>
device-alias	name	<vsp-name>-1-4b-fc-nvme pwwn <vsp-0:2b-wwpn></vsp-0:2b-wwpn></vsp-name>
device-alias	name	<serverl>-fc-nvme pwwn <fc-nvme-serverl-wwpnb></fc-nvme-serverl-wwpnb></serverl>
device-alias	name	<server2>-fc-nvme pwwn <fc-nvme-server2-wwpnb></fc-nvme-server2-wwpnb></server2>
device-alias	name	<server3>-fc-nvme pwwn <fc-nvme-server3-wwpnb></fc-nvme-server3-wwpnb></server3>
device-alias	name	<server4>-fc-nvme pwwn <fc-nvme-server4-wwpnb></fc-nvme-server4-wwpnb></server4>
Step 2.	Сс	ommit the device alias database changes:

Commit the device alias database changes:

device-alias commit

#### Procedure 4. Create Zones and Zonesets on Cisco MDS 9124V-A

Step 1. To create the required zones for FC on Fabric A, run the following commands:

configure terminal

```
zone name FC-<vsp-name> vsan <vsan-a-id>
member device-alias <server1-hostname> init
member device-alias <server2-hostname> init
member device-alias <server3-hostname> init
member device-alias <server4-hostname> init
member device-alias <vsp-name>-0-1a target
member device-alias <vsp-name>-1-2a target
exit
```

Step 2.

To create the required zones for FC-NVMe on Fabric A, run the following commands:

```
zone name FC-NVMe-<vsp-name> vsan <vsan-a-id>
member device-alias <server1>-fc-nvme init
member device-alias <server2>-fc-nvme init
member device-alias <server3>-fc-nvme init
member device-alias <server4>-fc-nvme init
member device-alias <vsp-name>-0-1b-fc-nvme target
member device-alias <vsp-name>-0-2b-fc-nvme target
exit.
```

To create the zoneset for the zone(s) defined earlier, run the following command: Step 3.

```
zoneset name Fabric-A vsan <vsan-a-id>
member FCP-<vsp-name>
member FC-NVMe-<vsp-name>
exit
```

Step 4. Activate the zoneset:

zoneset activate name Fabric-A vsan <vsan-a-id>

Save the configuration: Step 5.

copy run start

Note: Because Smart Zoning is enabled, a single zone for each storage protocol (FCP and FC-NVMe) is created with all host initiators and targets for the VSP ports instead of creating separate zones for each host. If a new host is added, its initiator can simply be added to appropriate zone in each MDS switch and the zoneset is reactivated.

#### Procedure 5. Create Zones and Zonesets on Cisco MDS 9124V-B

Step 1. To create the required zones and zoneset on Fabric B, run the following commands:

```
configure terminal
```

```
zone name FC-<vsp-name> vsan <vsan-b-id>
member device-alias <server1-hostname> init
member device-alias <server2-hostname> init
member device-alias <server3-hostname> init
member device-alias <server4-hostname> init
member device-alias <vsp-name>-0-3a target
member device-alias <vsp-name>-1-4a target
exit
```



To create the required zones for FC-NVMe on Fabric B, run the following commands:

```
zone name FC-NVMe-<vsp-name> vsan <vsan-b-id>
member device-alias <server1>-fc-nvme init
member device-alias <server2>-fc-nvme init
member device-alias <server3>-fc-nvme init
member device-alias <server4>-fc-nvme init
member device-alias <vsp-name>-0-3b-fc-nvme target
member device-alias <vsp-name>-0-4b-fc-nvme target
exit
```

**Step 3.** To create the zoneset for the zone(s) defined above, issue the following command:

```
zoneset name Fabric-B vsan <vsan-b-id>
member FC-<vsp-name>-B
member FC-NVMe-<vsp-name>-B
exit
```

#### **Step 4.** Activate the zoneset:

zoneset activate name Fabric-B vsan <vsan-b-id>

#### **Step 5.** Save the configuration:

copy run start

## Hitachi VSP Storage Configuration

This chapter contains the following:

- Hitachi Virtual Storage Platform Configuration for FC-SCSI
- Hitachi Storage Configuration for FC-NVMe

The following procedure explains the initial configuration for the Hitachi Virtual Storage Platform (VSP) storage.

## Hitachi Virtual Storage Platform Configuration for FC-SCSI

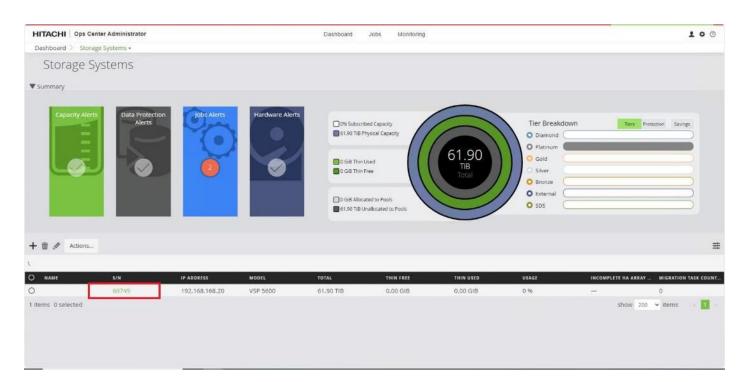
#### Procedure 1. Initialize Parity Groups with Hitachi Ops Center Administrator

The configuration steps in this procedure assume that Parity Groups have already been created by Hitachi professional services or from Hitachi Device Manager-Storage Navigator. To initialize Parity Groups from Hitachi Ops Center Administrator, proceed with the following steps:

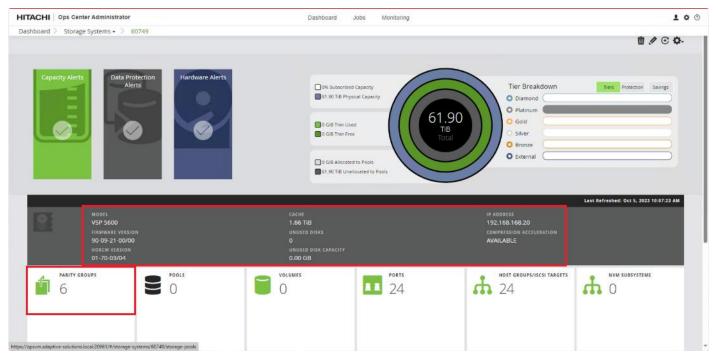
# **Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane, select **Storage Systems**.







#### Step 3. Click the **PARITY GROUPS** icon under the selected storage system to view the Parity Groups.



**Step 4.** Click any **Parity Group ID** that you want to initialize as parity for creating the boot volume pool. From the **Actions** pane, click **Initialize Parity Groups.** 

HITACHI	Ops Center Administrator			Dashboa	rd Jobs Monitoring				1
Dashboard (	> Storage Systems + > 6	0749 🗧 Parity Groups 🕶							
Parity	y Groups								Ę
Summary									
Actions									
Initialize Par	rity Groups								
Enable Com	pression on Parity Groups	RAID TYPE	DISK TYPE	TOTAL CAPACITY	UNINITIALIZED CAPACITY	INITIALIZED	USED	COMPRESSION	USAGE
) 1-1	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB	-	100%
) 1-2	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB	-	100%
) 1-3	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB	-	096
) 1-4	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB	-	0%
) 1.5	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
) 1-6	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
items 1 sele	cted								show 200 🗸 Items «

#### Step 5. Click OK.

Parit	y Groups		1000						5
			🔺 Ini	tialize Parity	Groups Confir	mation	×		
Summary				8					
Actions				ne selected 1 parity gr itialized. Do you want	oups in the current storage sy	stem will be			
			8	itialized. Do you want	to proceed?				
	arity Groups				Cancel OK •				
Enable Co	Ingression on Penty Groups	RAID TYPE	DISK TYPE		Current of		URED	COMPRESSION	USAGE
	IN_USE	RAID6 6D+2P	SSD NVMc 1.90 TB	10.32 118	3.00 MIB	0.00 G/8	10.32 TIB		100%
1-2	INJUSE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 G(B	10.32 TIB		100%
1-3	LININITIALIZED	RAID6 6D 2P	SSD NYMe 1.90 TB	10.32 TIB	10.32 110	0.00 G/B			C46
1.4	UNINITIALIZED	RAID6 60+2P	SSO NVMe 1.90 TB	10.32 118	10.32 118	0.00 GIB	0.00 GIB		CH:
	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 78	10.32 TIB	10.32 TIB	0.00 G(B	0.00 G/B		CH.
	UNINITIALIZED	RAID6 60+2P	SSD NVMe 1.90 TB	10.32 T/B	10.32 TIB				096

**Note:** Created Parity Groups initially have a status of UNINITIALIZED. Upon complete initialization, the status should change into IN\_USE.

**Procedure 2.** Create a Hitachi Dynamic Provisioning Pool for UCS Server Boot LDEVs from Hitachi Ops Center Administrator

When creating a pool, select the basic option to leverage tiers of storage available on the VSP, following best practices. By default, the basic option creates a Hitachi Dynamic Provisioning Pool.

For increased flexibility and if best practices are not essential, choose the advanced option. This enables you to specify Parity Groups and define your pool types as either Tiered, Thin, or Snap.

**Step 1.** Log in to **Hitachi Ops Center Administrator**, and from the navigation pane, click **Storage Systems** to access the inventory of registered storage systems.

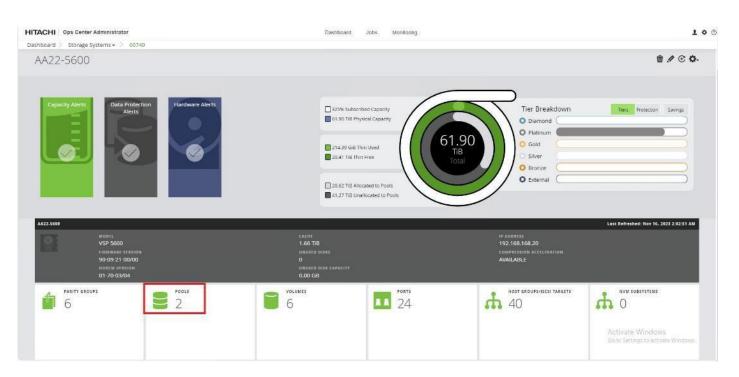
HITACHI Ops Center Administrator	Dashboard Jobs Monitoring		10
Capacity Alerts	Data Protection Alerts	Pois Alerts	Hardware Alerts
Control Contr	61.90 Тів Тоса		Tiers Protection Savings



Click the **S/N** listing of the Storage System.

HITACHI Ops Center Administrator Dashboard 2 Storage Systems -			Dashboard	Jobs Monitoring				10
Storage Systems								
♥ Summary								
Capacity Alerts	in Jedys Alerts	Hardware Alerts	0 214.35 CE 214.35 CE 20.41 TE 1		61.90 18 703	Tier Breakdou Dismond Dismond Dismond Gold Silver Branze Distorna Storna Sos	NN Tes /	
H 🗊 / Actors								
λ,								
) NAME SIR	IP ADDRESS	MODEL	TOTAL	THIN FREE	THIN USED	USACE	INCOMPLETE HA ARRAY	NIGRATION TASK COU
AA22-5600 60719	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GIB	0.96	-	0
Items 0 selected							- The second	200 🛩 items

Step 3. From the selected Storage Systems, click POOLS.



**Step 4.** Click the plus sign (+), to open the **Create Pool** window.

HITACHI	Ops Center Administ	rator		
Dashboard >	Storage Systems 🕶	> 60749 >	Pools -	
Pools				
▼ Summary Ca	pacity Alerts			
+ 🗊 🥒 Ad	ctions			
Q Create St	orage Pool			
O 10	NAME		ТУРЕ	ACTIVE FLASH

#### **Step 5.** Enter the following details:

- a. Enter **POOL NAME** as "UCS\_Boot\_Pool" (pool names can be any combination of alphanumeric characters, hyphens, and underscores only. Initial hyphens are not allowed).
- b. Click an available **Tier** to view the storage capacity and select the required capacity.
- c. Review the **high and low pool utilization thresholds**. By default, the low utilization threshold is set to 70%, and the high threshold is set to 80%. You can customize these thresholds to receive no-tifications based on their specific environment requirements.
- d. To specify over allocation, you can set the limit to **Unlimited**.
- e. Click Submit.

HITACHI Ops Center Administrator	Dashboard J	lobs Monitoring					
Dashboard $\geq$ Storage Systems - $\geq$ 60749 $\geq$ Pools - $\geq$ Crea	te Pool						
Create Pool							
	Basic	Ad	Advanced				
POOL NAME UCS_Boot_Pool	Select capacity from Tiers to alloca	Tier Management 0.00 GiB Available					
STORAGE SYSTEM 60749 USE FOR SNAP?	0.00 GIB PLATINUM 10.32 TIB	10.32 TIB Available					
Yes No BREAKDOWN OF DISKS Total: 10.32 TIB	GOLD 0.00 GIB	0.00 GIB Available v					
Platinum: 10.32 TiB (100.00 %)	SILVER 0.00 GIB Available						
	0.00 GIB						
	UTILIZATION THRESHOLD (LOW) %	SUBSCRIPTION LIMIT					
			Cancel Submit -				

#### Procedure 3. Create FC-SCSI Servers from Hitachi Ops Center Administrator

Hitachi Ops Center Administrator supports provisioning storage from logical containers known as servers. These servers that host Cisco UCS server WWNs and the server IP. After Cisco UCS servers are onboarded in Ops Center Administrator, BOOT LDEVs can be provisioned using servers. Proceed with the following steps to create servers from Ops Center Administrator.

#### **Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane, click **Servers**.

ITACHI Ops Center Administrator		Dashboard Jobs Monito	pring	10
Storage Systems	apacity Alerts	Data Protection Alerts	Jobs Alerts	Hardware Alerts
The least of Country allows and	cribed Capacity 8 Physical Capacity		Tier Breakdown  Diamond	Tiers Protection Savings
Gib Thi Virtual Storage		61.90 <sub>Тів</sub> Total	Platinum     Gold     Silver     Bronze	
Machines				

### **Step 2.** Click the plus sign (+) to open the **Add Server** window.

HITACHI Ops Ce	nter Administrator			Dashboard	Jobs	Monitorin	ng			
Dashboard > Serve	ers +									
Servers										
Summary										
		Servers							Server Groups	
🕂 🛅 🖋 Actions										
Q										
О ю	ALERTS	SERVER NAME	IP ADDRESS	PROTOCOL	WWN/ISCSI INIT	ато н	OST NQN	OS TYPE	VOLUME COUNT	REPLICATION TYPE

Step 3. Click the plus sign (+) under the Fibre Servers and enter the following server information.

- a. SERVER NAME
- b. DESCRIPTION
- c. IP ADDRESS
- d. WWN LIST: Fabric A and Fabric B WWNs of the Cisco UCS Servers
- e. OS TYPE: Select the OS TYPE as VMWARE EX.
- Step 4. Click Submit to add the server.

HITACHI Ops	Center Administrator		Dashboard Jobs	Monitoring		
Dashboard > Se	rvers - > Add Servers					
< !	🚣 Add Servers					
			+			<b>^</b>
	Fibre Servers					
			+			
	SERVER NAME UCS_ESXI_2	DESCRIPTION Description	IP ADDRESS 10.1.168.112	OS TYPE VMWARE EX	~	×
	WWN LIST WWN 20:00:00:25:b	5:21:0a:02, 20:00:00:25:b5:21:0b:02				<sup>n</sup>
	WWN USER-DEFINED NAM Hba_A, Hba_B	AES				
	FC-NVMe Servers					
						-
						Cancel Submit -

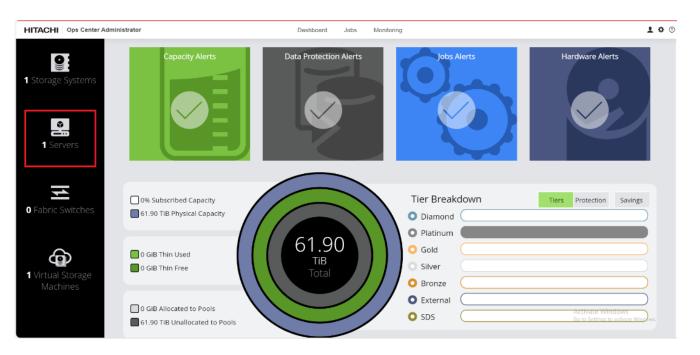
**Step 5.** Repeat **Step 1** through **Step 4** for any additional Cisco UCS servers. Upon completion, you can expect the following representation of Cisco UCS servers.

HITACHI	ps Center Administrat	tor		Dashb	oard Jobs	Monitoring					100
Dashboard >	Servers -										
Servers	S										. € ⊙
Summary											
		Servers							Server Groups		
🗕 💼 🥒 🛛 Actio	ons										
2											
ai C	ALERTS	SERVER NAME	IP ADDRESS	PROTOCOL	WWN/ISCSI IN	IITIATOR NAME	н	OS TYPE	VOLUME COUNT	REPLICATION TYPE	STORAGE SYSTEM
) 2	-	UCS_ESXi_1	10.1.168.111	Fibre	20:00:00:25	:B5:21:0A:00(Hba		VMWARE EX	0	-	
) 3		UCS_ESXi_2	10.1.168.112	Fibre	20:00:00:25	:B5:21:0A:02(Hba		VMWARE EX	0		
) 4		UCS_ESXi_3	10.1.168.113	Fibre	20:00:00:25	:B5:21:0A:04(Hba		VMWARE EX	0		
	_	UCS_ESXi_4	10.1.168.114	Fibre	20:00:00:25	:B5:21:0A:06(Hba		VMWARE EX	0	_	
) 5											

**Procedure 4.** Create FC-SCSI Server Groups from Ops Center Administrator

The Server Groups are created to manage multiple servers and attach volumes using a single workflow.

**Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane, click **Servers.** 



Step 2. Select Server Groups. Click the plus sign (+) icon to open the Add Server Group wizard.

Servers		<u>ځ</u> ۵	
▶ Summary			
Servers		Server Groups	
+ 🛍 🖋 Actions			±
Q			
O SERVER GROUP ID	SERVER GROUP NAME	SERVER COUNT	

Step 3. In the Add Server Group wizard, enter the SERVER GROUP NAME (for exam-

ple,VSI\_UCS\_Cluster\_1) and select the Cisco UCS servers that are going to be added to the server group. Click **Add** to move the selected servers from **AVAILABLE SERVERS** to **ASSIGNED SERVERS**.

	enter Administrator				Dashboard	Jobs	Monitoring				
hboard > Serv	er Groups > Add Server Gro										
	Add Server	Group									
	VSI_UCS_Cluster_1	IE									
	DESCRIPTION (OPTIC Description	UNALJ									
	a source of the										
	AVAILABLE SERVERS							ASSIGNED SERVERS			
	Q							O SERVER NAME	IP ADDRESS	PROTOCOL	OS TYPE
	SERVER NAME	IP ADDRESS	PROTOCOL	OS TYPE							
	⊘ UCS_ESXI_1	10.1.168.111	Fibre	VMWARE EX							
	⊘ UCS_ESXI_2	10.1.168.112	Fibre	VMWARE EX							
	⊘ UCS_ESXI_3	10.1.168.113	Fibre	VMWARE EX							
	O UCS_ESXI_4	10.1.168.114	Fibre	VMWARE EX							
	4 items 4 selected		show 200	🗸 items  🖌 🛛							
						Add >					
						< Remove					

## Step 4. Click Submit.

HITACHI Ops Cente	er Administrator		Dashboard	Jobs	Monitoring				
Dashboard 👌 Server (	Groups > Add Server Group								
<	Add Server Group								
	SERVER GROUP NAME VSLUCS_Cluster_1 DESCRIPTION (OPTIONAL) Description								
	AVAILABLE SERVERS					ASSIGNED SERVERS			
	5					O SERVER NAME	IP ADDRESS	PROTOCOL	OS TYPE
	O SERVER NAME IP ADDRESS	PROTOCOL OS TYPE				O UCS_ESXI_1	10.1.168.111	Fibre	VMWARE EX
	0 items 0 selected	show 200 🗸 Items				O UCS_ESXI_2	10.1.168.112	Fibre	VMWARE EX
						O UCS_ESXI_3	10.1.168.113	Fibre	VMWARE EX
						O UCS_ESXI_4	10.1.168.114	Fibre	VMWARE EX
				Add > < Remove					
									Cancel 🗛

The Server Group (VSI\_UCS\_Cluster\_1) was created and you can find it along with the Server Group ID.

HITACHI Ops Center Administrator		Dashboard Jobs	s Monitoring	
Dashboard > Servers +				
Servers				
Summary				
	Servers			Server Groups
+ 🟛 🖋 Actions				
م				
O SERVER GROUP ID	SERVER GROUP NAI	ME		SERVER COUNT
Ø 2	VSI_UCS_Cluster	c_1		4

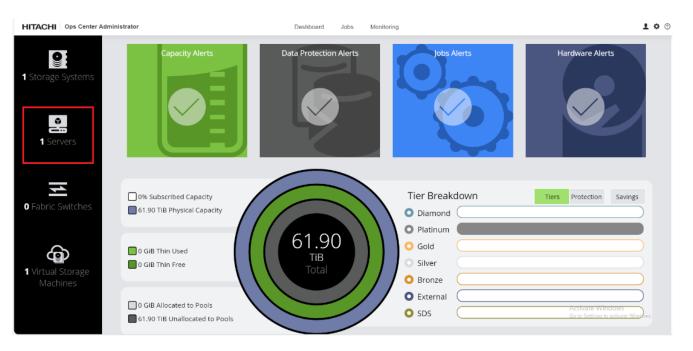
After your server group is created, you can expect the following representation:

ITACHI Ops Center Administrator			Dashboard	Jobs Monitoring			10
ashboard > Server Groups > 2							
VSI_UCS_Cluster_1							<b>m</b> /
Summary							
	Servers				Volumes		
Actions							
			1				
ID ALERTS	SERVER NAME	IP ADDRESS	PROTOCOL	WWN/ISCSI INITIATOR NAME OS TYPE	VOLUME COUNT	REPLICATION TYPE	STORAGE SYSTEM ID
2 —	UCS_ESXL_1	10.1.168.111	Fibre	20:00:00:25:85:21:0A:0 VMWARE EX	3		60749
3 —	UCS_ESXI_2	10.1.168.112	Fibre	20:00:00:25:85:21:0A:0 VMWARE EX	3	-	60749
4 —	UCS_ESXI_3	10.1.168.113	Fibre	20:00:00:25:B5:21:0A:0 VMWARE EX	3	-	60749
	UCS_ESXL4	10.1.168.114	Fibre	20:00:00:25:85:21:0A:0 VMWARE EX	3	_	60749

**Procedure 5.** Allocate Boot LUNs to UCS Servers from Hitachi Ops Center Administrator with Multiple LDEV paths

When allocating Boot LUNs to the Cisco UCS servers, the allocation will be executed on a per-server basis using the Servers logical container.

**Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane, click **Servers**.



#### Step 2. Select the Server ID.

**Step 3.** From the Actions tab, click **Attach Volumes** and select **Create, Attach, and Protect Volumes** with Local Replication.

Dashboard >	Ops Center Administrator			C	Dashboard Jobs	Monitoring					1
Server											<u>.</u>
Summary											
		Servers							Server Groups		
- 💼 🥒 🗛	tions										
	Attach Volumes 🔹 🕨	Attach Existing Volumes									
10 U	Use Existing LUN Paths	Create, Attach and Protect Vo	lumes with Local Replication	ROTOCOL	WWN/ISCSI INITIAT	OR NAME	но_	OS TYPE	VOLUME COUNT	REPLICATION TYPE	STORAGE SYSTEM
2	-	Create, Attach and Protect Vo	lumes with High Availability	lbre	20:00:00:25:85:	21:0A:00(Hba_A), 20:0	-	VMWARE EX	3	-	60749
3		UCS_ESXI_2	10.1.168.112	Fibre	20:00:00:25:B5:	21:0A:02(Hba_A), 20:0	-	VMWARE EX	3	-	60749
4	-	UCS_ESXI_3	10.1.168.113	Fibre	20:00:00:25:85:	21:0A:04(Hba_A), 20:0	-	VMWARE EX	3	-	60749
5	-	UCS_ESXI_4	10.1.168.114	Fibre	20:00:00:25:B5:	21:0A:06(Hba_A), 20:0	-	VMWARE EX	3	-	60749
6	-	ESXi_1_NVMe	10.76.30.50	FC-NVMe	20:00:00:25:B5:	86:0A:13(HBA_A_NVM	nq	VMWARE EX	0	-	
items 1 selecte	ed									show 20	00 🗸 items 👒

**Step 4.** Configure volumes for the specified Storage System. To add the volumes to UCS ESXi servers complete the following steps:

- a. Verify that the required **STORAGE SYSTEM** is selected.
- b. Select the NUMBER OF VOLUMES as 1.
- c. Enter the VOLUME LABEL (for example, ESXi1\_Boot\_Vol).
- d. Enter the volume SIZE (for example, 32 GiB).
- e. Select the **volume unit** as **GiB**.
- f. Select the **POOL TYPE** as **Thin**.

#### Step 5. Click Next to continue.

HITACHI Ops Center Administrator		Dashboard Jobs	Monitoring		
Dashboard $\geq$ Servers $\star$ $\geq$ Create, Attach and Protect Volu	mes with Local Replicati	on			
Create, Attach and	Protect Volur	nes			
1. Create Volumes 2. Attach Settings	3. Path Settings	4. Protect Volumes 5. Op	peration Plan		
STORAGE SYSTEM (60749) 🗸	VOLUME LABEL ESXI1_Boot_Vol	e.g. 1	1	ZE GiB	·
SUBSCRIBED CAPACITY 651% (403.17 TIB / 61.90 TIB)	Auto - From POOL TYPE	- To		- To	
VIRTUAL STORAGE MACHINE No VSM Selected (Default Meta Resi 🗸	Thin capacity saving No	✓ Platinum	UCS_Boot_Pool(10.30 TiB/		
For servers or server groups that have mis-matched Host Modes or Host	• Set "Auto" for t	he Virtual ID/Range field Ds with the physical LDB	d if you want Ops Center Adm EV IDs.	inistrator to attemp	ot to match
Mode Options, please use the "Attach Like Volumes" function from the server's volume inventory, in order to	VOLUME LABEL ESXI1_Boot_Vol	LABEL SUFFIX	NUMBER OF VOLUMES	<b>3</b> 2	GIB 👻
prepopulate paths properly.	VOLUME ID/RANGE Auto 👻		virtual id/range Auto 👻		
	POOL TYPE Thin	POOL TIER	POOL     UCS Boot Pool(10.30 TiB/1	TIERING POLICY	
	CAPACITY SAVING	• Haunum	CS_800_P00[[10.50 HB/		
					Cancel Next

**Step 6.** Select the following parameters:

- a. Set the HOST MODE to VMWARE EX.
- b. Select HOST MODE OPTION 63 (VAAI) Support option for vStorage APIs based on T10 standards.
- c. Specify the HOST GROUP NAME; for VSI deployments in the context of this document, the nomenclature VSI\_x210\_M7\_xx is used, where xx is the ESXi server ID.
- d. Set MANDATE LUN ALIGNMENT as **Yes**; this option determines whether to assign the same LUN number to multiple servers for a volume. If Yes is specified, the same LUN number is always assigned.
- e. Set AUTO CREATE ZONE as No.
- f. Click Next.

HITACHI	Ops Center Administrator			Dashboard	Jobs Mo	nitoring			
Dashboard	and the second								
<	🗊 Create, Atta	ch and P	rotect Vol	umes					
	1. Create Volumes 2. Al	ttach Settings	3. Path Settings	4. Protect Volu	mes 5. Opera	tion Plan			
	STORAGE SYSTEM							View Proposed	Volume ID Selection
	HOST MODE		NUMBER OF VOL	LABEL	LABEL SUFFIX	SIZE	POOL TYPE	TIER	POOL
	VMWARE EX	~	1	ESXi1_Boot_Vol	-	32.00 GIB	Thin	Platinum	UCS_Boot_Po
	63 - (VAAI) Support option	for vStor							
	VSI_x210_M7_01								
	MANDATE LUN ALIGNMEN								
	Yes AUTO CREATE ZONE	No							
	Yes	No							
								Cancel	Previous Next

**Step 7.** In the Path Settings step, you can view servers and their WWNs, along with ports on the storage system and map based on initial zoning configurations. To create a path, click the Cisco UCS server WWNs and click the respective VSP Ports to which it is zoned.

**Step 8.** You can expect the following representation of the mapping after **Path Settings** are completed for a single ESXi host. Upon confirming the paths, click **Next** to view options for protecting volumes.

	ter Administrator	Dashboard Jobs Monitoring			
	s 🔹 ∑ Create, Attach and Protect Volumes with Local Replication				
l	🖥 Create, Attach and Protect Volumes				
	1. Create Volumes 2. Attach Settings 3. Path Settings 4. Protect Volume	rs 5. Operation Plan			
				Exe	sting
	Switch View Suggest			Nev	
	1 Servers			24 Target Storage F	Ports
	UCS_ESXI_1 (VMWARE EX)			2.1 (0) 0-1 210 (00-1)	
	US EST I (VIIIWARE EX)	20:00:00:25:B5:21:0A:00(Hba_A)		CL1-A O	
		20:00:00:25:85:21:08:00(Hba_B)		CL1-B 🚯	
				CL1-C 🛈	e 11
				CL2-A	_
				CL2-B 0 CL2-C 0	
				CL3-A O	
				CL3-B O	
				CTD-D A	
				CL3-C 0	
			$\sim$		



HITACHI Ops Center Administrator	Dashboard Jobs	Monitoring			<b>1</b> 🌣 🔊
Dashboard > Servers - > Create, Attach and Protect Volumes v					
Create, Attach and Prot	ect Volumes				
1. Create Volumes 2. Attach Settings 3. Pa	ath Settings 4. Protect Volu	mes 5. Operation Plan			
REPLICATION TYPE	_				
Snap			None		
VOLUMES	_				
NUMBER OF VOLUMES LABEL	BEL SUFFIX SIZE	POOL TYPE	TIER I	POOL	
1 ESXi1_Boot_Vol —	32.00 GiB	Thin	Platinum	UCS_Boot_Pool(1	
			Cancel Previous	Next Submit 👻	

**Step 10.** View the displayed **Operation Plan**, confirm the settings. For boot LUNs confirm that LUN ID 0 is assigned, if LUN ID 0 is not automatically selected, click **LUN Settings**. If LUN ID 0 is already assigned, go to step 12.

< [	+	Create, A	lttach and P	Protect Volu	umes					
	1.	Create Volumes	2. Attach Settings	3. Path Settings	4. Protect Volumes	5. Operation P	lan			
		Host Group Nam	ie	VSI_x210	_M7_01					
		Mandate LUN Ali	ignment	Yes						
		Auto Create Zone	e	No						
		Mandate Using D	Displayed Volume IDs	No						
		reate Paths Planned Path Co	nfiguration							LUN Settings
		VOLUME ID	SERVER	WWN/ISCSI IM	IITIATOR NAME	STOP	RAGE PORT	PROTOCOL	LUN	

**Step 11.** From the LUN settings window, using the FROM the drop-down list, select **0**, and click **OK**.

LUN Settings				
LUN Range Assignmen NUMBER OF VOLUMES		LABEL SUFFIX	FROM	то
1	ESXi1_Boot_Vol	_	0 🗸	Auto 🗸
				Cancel

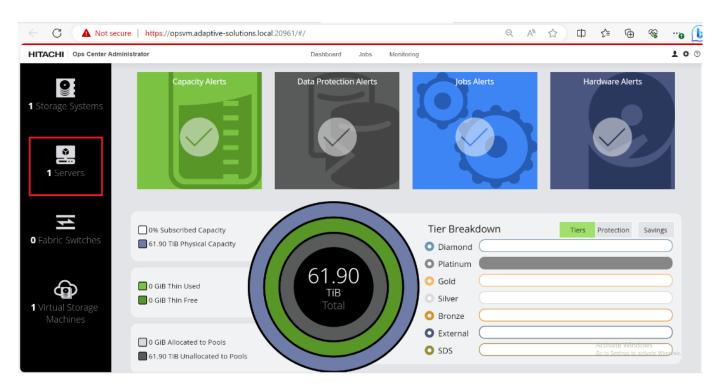
Step 12. Review the Operation plan. Click Submit.

🗄 Create, Attach	h and Protect Volume	s				
1. Create volumes 2. At	tach Settings 3. Path Settings 4. Pr	rotect volumes 5. Operation	n man			
Selected Servers						
SERVER ID	SERVER NAME	SERVER IP ADDRESS	PROTOCOL	OS TYPE	VOLUME COUNT	REPLICATION TYPE
2	UCS_ESXi_1	10.1.168.111	Fibre	VMWARE EX	1	-
Create Volumes						
Volume Location						
LOCATION		VALUE				
Storage System		(60749)				
Virtual Storage Machine	)	-				
Volume Specification						
VOLUME ID/RANGE	VOLUME ID VOLUME LABEL 32 (00:00:20) ESX(1_Boot_Vo	CAPACITY 01 32.00 GIB		ol type pool tier		G POLICY CAPACIT
	32 (00:00:20) E5X01_Boot_V	01 32.00 GIB	Auto I	in Platinum	UCS_Boot_Pool(10.30	None
Attach Settings						
PARAMETER		VALUE				
Host Mode Host Mode Options		VMWARE EX				
Host Group Name						
Mandate LUN Alignmen	Y.	Ves				
Auto Create Zone		No				
Mandate Using Displaye	ed Volume IDs	No				
Create Paths Planned Path Configura	ation					
VOLUME ID	SERVER	WWN/ISCSI INITIATOR NAME	t	STORAGE PORT	PROTOCOL	LUN
32 (00:00:20)	UCS_ESXI_1	20:00:00:25:85:21:0A:00	0(Hba_A)	CL1-A	Fibre	0
	UCS_ESXI_1	20:00:00:25:85:21:0A:00	0(Hba_A)	CL2-A	Fibre	0
32 (00:00:20)					-1	0
32 (00:00:20) 32 (00:00:20)	UCS_ESR(_1	20:00:00:25:85:21:08:00	0(Hba_B)	CL3-A	Fibre	
	UCS_ESR_1 UCS_ESR_1	20:00:00:25:85:21:08:0		CL3-A CL4-A	Fibre Fibre	0
32 (00:00:20)	UCS_ESXL1 red LUN	20:00:00:25:85:21:08:0	0(Hba_B)			
32 (00:00:20) 32 (00:00:20)	UCS_ESXL_1	20:00:00:25:85:21:08:0				
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat	UCS_ESXL1 ed LUN Yes	20:00:00:25:85:21:08:0	0(Hba_B)			
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In	UCS_ESXL1 ved LUN Ves tion formation	20:00:00:25:85:21:08:0	O(Hba_B)	CL4-A	Fibre	0
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 1033 (46047 4447/0031 14	UCS_ESO_1 ed LUN Ves tion formation sect Autos Stoteware Point	20:00:00:25:85:21:08:0	NO(Hoba_B) Hoss Made	CL/+A HOST WORK OFTIN	Fibre NS NEW	0
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 931 (10:00 (MM/001114) VS()x210.047_01	UCS_ESO_1 ed LUN Ves tion formation cL1-A	20:00:00:25:85:21:08:0	VMWARE DX	CL/+A #051 M098 (#711 . 63.	Fibre Inst. New Exist	0 / FXSTONE
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 931 etcel AMURICI IA VS():210./M7_01 VS():210./M7_01	UCS_ESQ_1 ed LUN Ves tion formation cL1-A CL4-A	20:00:00:25:85:21:08:0	NO(H5a_B) NOSE MODE VMWARE EX VMWARE EX	CL/+A MOST MOST OF 21 . 63, 63,	Pibre Nas Na W Exist Exist	o o o o o o o o o o o o o o o o o o o
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 0001 okock AND/ACS IX VSL/210_M7_01 VSL/210_M7_01 VSL/210_M7_01	UCS_ESQ_1 ed LUN Ves tion formation CL1-A CL4-A CL2-A CL2-A	20:00:00:25:85:21:08:0	NO(H5a_B) HASS WORK VHWARE EX VHWARE EX VHWARE EX	CL4-A #051 M084 0#11 . 63, 63, 63, -	Pibre No. No. Dist Dist Dist Dist	0 P # AKS 10H6 ting ting ting
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 9011 40:00 64400 (00) 915():210.047.01 95():210.047.01 95():210.047.01 95():210.047.01	UCS_ESQ_1 ed LUN Ves tion formation cL1-A CL4-A	20:00:00:25:85:21:08:0	NO(H5a_B) NOSE MODE VMWARE EX VMWARE EX	CL/+A MOST MOST OF 21 . 63, 63,	Pibre Nas Na W Exist Exist	0 P # AKS 10H6 ting ting ting
32 (00:00:20) 32 (00:00:20) Mandate Using Display Host Group Informat Planned Host Group In 0001 okock AND/ACS IX VSL/210_M7_01 VSL/210_M7_01 VSL/210_M7_01	UCS_ESQ_1 ed LUN Ves tion formation CL1-A CL4-A CL2-A CL2-A	20:00:00:25:85:21:08:0	NO(H5a_B) HASS WORK VHWARE EX VHWARE EX VHWARE EX	CL4-A #051 M084 0#11 . 63, 63, 63, -	Pibre No. No. Dist Dist Dist Dist	0 P # AKS 10H6 ting ting ting

**Step 13.** Repeat **Steps 1** through **12** for any additional Cisco UCS servers.

## **Procedure 6.** Edit Host Groups from Ops Center Administrator for Fabric A and Fabric B Representation

**Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane select **Servers.** 



#### Step 2.

Click the **Server ID** for **UCS\_ESXi\_1** as shown in the following figure:

HITACHI Ops Center A	dministrator				Dashboard Jobs Monitorin	9				
Dashboard > Servers -										
Servers										
Summary										
		Servers						Server Groups		
+ 🗊 🖉 Actions										
Q										
O 10	ALERTS	SERVER NAME	IP ADDRESS	PROTOCOL	WWN/ISCSI INITIATOR NAME	HOST NON	OS TYPE	VOLUME COUNT	REPLICATION TYPE	STORAGE SYSTEM
Ø 2	-	UCS_ESXi_1	10.1.168.111	Fibre	20:00:00:25:85:21:0A:00(		VMWARE EX	4	-	60749
O 3	-	UCS_ESXi_2	10.1.168.112	Fibre	20:00:00:25:B5:21:0A:02(	-	VMWARE EX	4	-	60749
O 4	-	UCS_ESXL3	10.1.168.113	Fibre	20:00:00:25:B5:21:0A:04(	-	VMWARE EX	4	-	60749
O 5	-	UCS_ESXL4	10.1.168.114	Fibre	20:00:00:25:B5:21:0A:06(		VMWARE EX	4	-	60749
O 8	-	UCS_NVMe_ESXI1	-	FC-NVMe		ngn.2014-08.com.vmwar	VMWARE EX	2	-	60749
O 9	-	UCS_NVMe_ESXI2	-	FC-NVMe		ngn.2014-08.com.vmwar	VMWARE EX	2	-	60749
O 10	-	UCS_NVMe_ESXI3	-	FC-NVMe		ngn.2014-08.com.vmwar	VMWARE EX	2	-	60749
O 11	-	UCS_NVMe_ESXI4	-	FC-NVMe		ngn.2014-08.com.vmwar	VMWARE EX	2	-	60749
8 items 1 selected										show 200 🛩 items

Step 3. Expand the Volume ID of the Boot volume created. Click the Edit pencil icon to edit CL1-A.

HITACH	HI   Ops Cente	r Administrator					Dashboard	Jobs Monitor	ing						1	0
Dashboa	and > Servers -	-> 2														
Ser	rver 2														🖻 🖉 l	8-
V Summar	ny .															
C	Data Protection /	Alerts SERVER NAME UCS_ESKI_1 PROTOCOL Fibre			IP ADDRE 10.1.168.1 DESCRIPT	111			CAPACITY (THI 961.90 Gib / 10. THIN FREE 9.09 TIB				85:21:0A:00(Hba_A) 85:21:08:00(Hba_B)			
Search		alter- BCNB&∡I	ð-													
4 selected															Loaded all 4	4 iter
· 0	VOLUME ID															-
		VIRTUAL ID			MF NAMP D	ATA PROTECTION V		ATTRIBUTE	STATUS	PEOTECTION 19PE	DATA PROTECTION A. C	PACITY SAVING	TOTAL	THIN USED	03869	
0	4 (00:00:04)	4 (00:00:04)				ATA PROTECTION V		ATTRIBUTE	Normal	PEOIDCION 17PD		PACITY SAVING		THIN USED 3.36 GiB		-
-					1_Boot_Vol U			Thin							03869	
ORT	W	4 (00:00:04)		60749 ESXi	1_Boot_Vol U	Inprotected		Thin	Normal		No N		32.00 GiB		03869	6
087 11-A	w 2	4 (00:00:04)		60749 ESXi	1_Boot_Vol U N	Inprotected		Thin HOST I	Normal Mode offices		NO N HOST GROUP NAME		32.00 GiB		03869	6
0 00 00 00 00 00 00 00 00 00 00 00 00 0	2 2	4 (00:00:04)		60749 ESXi tu	1_Boot_Vol U N	Inprotected HOST MODE VMWARE EX		Thin HOST 6:	Normal Made options 3		NO N HOST BROUP NAME VSLx210_M7_01,		32.00 GiB ALUA Preferred		03869	1) 1) 1)
EL1-A EL2-A	2 2 2 2	4 (00:00:04) www 20:00:00:25:B5:21:0A:00 20:00:00:25:B5:21:0A:00		60749 ESXi Lu 0 0	1_Boot_Vol U N	Inprotected Host Mode VMWARE EX VMWARE EX		Thin Host 1 6: 6:	Normal Mose offices 3 3 3		No N HOST BROUP NAME VSI_X210_M7_01 VSI_X210_M7_01		32.00 GiB ALUA Preferred Preferred		03869	6 6 6
11-A 12-A 13-A 14-A	2 2 2 2	4 (00:00:04) www 2000:00:25:B5:21:0A:00 20:00:00:25:B5:21:0A:00 20:00:00:25:B5:21:0B:00	60749	60749 ES30 Lu 0 0 0 0 0	1_Boot_Vol U N	Unprotected HOST MODE VMWARE EX VMWARE EX VMWARE EX	0	Thin KONT ( 6) 6) 5)	Normal Model officies 3 3 3 3		NO         N           H03T 5400P NAME         VSU210_M7_01           VSU210_M7_01         VSU210_M7_01           VSU210_M7_01         VSU210_M7_01		32.00 GiB AUA Preferred Preferred Preferred Preferred		03869	8 8 8
0KT 21.1-A 21.2-A 21.3-A 21.4-A ©	и 2 2 2 2 2 2	4 (00:00:04)	60749	60749 ESX0 1 te 0 0 0 0 0 0 60749 VSLA	1_Boot_Vol U N	Minorotected Host Mobe VMWARE EX VMWARE EX VMWARE EX	0	Thin Host of 6: 6: 6: 6: 6: 6: 6: 6:	Normal Mode offices 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	-	No         N           HOTT SKOUP NAME            VSUJ210_M7_01            VSUJ210_M7_01            VSUJ210_M7_01            VSUJ210_M7_01            VSUJ210_M7_01		32.00 GiB ALUA Preferred Preferred Preferred 5.00 TIB	3.36 GiB	10%	1 1 1 1

**Step 4.** In the **HOST GROUP NAME** text box, update the host group name to include Fabric A. In the specific context outlined in this document, CL1-A for UCS\_ESXi\_1 is assigned VSI\_x210\_M7\_01\_Fab\_A as the host group name. Click **Submit**.

HITACHI Ops Center Administrator	Dashboard	Jobs	Monitoring			
Dashboard $>$ Storage Systems $\star$ $>$ 60749 $>$ Host Groups $\star$ $>$ CL1-A-1 $>$ Edit Host Group	)					
Edit Host Group						
HOST GROUP NAME VSL_x210_M7_01_Fab_A						
HOST MODE VMWARE EX						~
HOST MODE OPTIONS						
63 - (VAAI) Support option for vStorage APIs based on T10 standards						
PREFERRED PATH						
Preferred				Non Preferred		
						_
					Cancel	Submit

**Step 5.** Repeat **Step 2** through **Step 4** for the remaining ports where CL2-A is Fabric A, CL3-A is Fabric B, and CL4- A is Fabric B. When completed, you can expect to see the following:

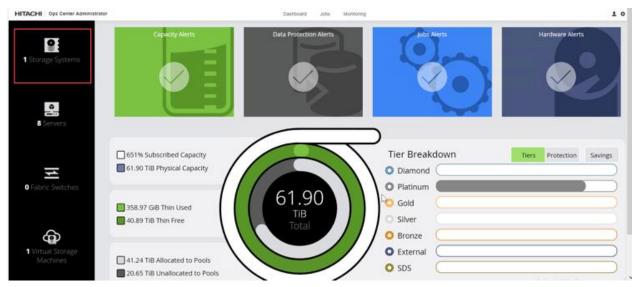
PORT	www	LUN	HOST MODE	HOST MODE OFTIONS	HOST BROUP NAME
CL1-A	20:00:00:25:B5:21:0A:00	0	VMWARE EX	63	VSLx210_M7_01_Fab_A
CL2-A	20:00:00:25:B5:21:0A:00	0	VMWARE EX	63	VSLx210_M7_01_Fab_A
CL3-A	20:00:00:25:85:21:08:00	a	VMWARE EX	53,	VSI_x210_M7_01_Fab_B
CL4-A	20:00:00:25:85:21:08:00	a	VMWARE EX	63	VSI_x210_M7_01_Fab_B

Procedure 7. Create a Hitachi Dynamic Provisioning Pool for FC-SCSI VMFS LDEVs for UCS Servers

When creating a pool, use the basic option to leverage tiers of storage available on the VSP, following best practices. By default, the basic option creates a Hitachi Dynamic Provisioning Pool.

For increased flexibility and if best practices are not essential, choose advanced option. This enables you to select specific Parity Groups and define your pool types as either Tiered, Thin, or Snap.

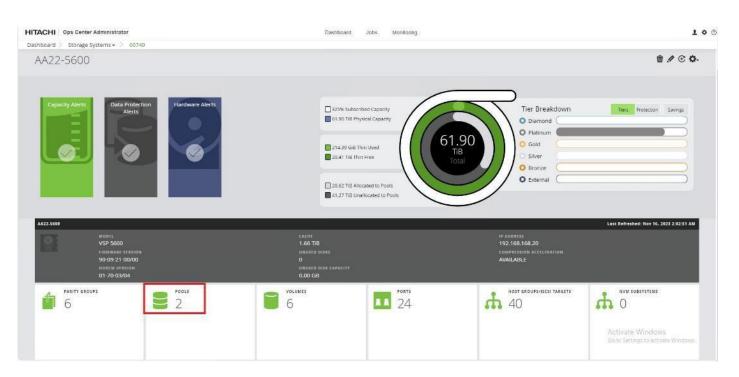
**Step 1.** Log in to **Hitachi Ops Center Administrator**. In the **Dashboard**, click **Storage Systems** to access the inventory of registered storage systems.



Step 2. Click the S/N listing of the Storage System.

HITACHI Ops Center Administrator Dashboard Storage Systems =			Dashboard	Jobs Monitoring					1 0 C
Storage Systems									
<b>F</b> Summery									
Copurity Alerts	DT	Hardware Alerts	■ 61.50 TB 274.35 GI ■ 20.41 TB □ 20.62 TB		61.90 TB TOEN	Tier Breakdo Diatnond Piatnond Gold Silver Bronze Bronze Sos	wn	Get Propertien Seying	
+ 🗊 🖉 Actions									
م									
D HAME SIR	IP ADDRESS	MODEL	TOTAL	THEN FREE	THIN USED	USACE	INCOMPLETE HA A	RRAY NIGRATION TAS	COUNT
O AA22-5600 60749	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GIB	0.96	-	0	
I Rems 0 selected								show 200 v items	- 11

**Step 3.** From the Storage Systems, click **Pools**.



**Step 4.** Click the plus sign (+) to open the **Create Pool** window.

н		ps Center Administrator		
Da	ashboard >	Storage Systems 🔹 > 60749 > Poo	ols <del>-</del>	
	Pools			
VS	Capi	acity Alerts		
+	🗊 🥒 Acti	ions		
٩	Create Stor	rage Pool		
0	ID	NAME	TYPE	ACTIVE FLASH
0	0	UCS_Boot_Pool	Thin	No

#### **Step 5.** Enter the following details:

- a. For the POOL NAME enter **UCS\_Application\_Pool** (Pool names can be any combination of alphanumeric characters, hyphens, and underscores only. Initial hyphens are not allowed).
- b. Click an available **Tier** to view the storage capacity and select the required **capacity**.
- c. Review the **high and low pool utilization thresholds**. By default, the low utilization capacity is set to 70%, and high threshold is set to 80%. You can customize thresholds to receive notifications based on their specific environment requirements.
- d. To specify over allocation, you can set the limit to **Unlimited**.
- e. Click Submit.

HITACHI Ops Center Administrator	Dashboard	Jobs Monitoring	
Dashboard $>$ Storage Systems - $>$ 60749 $>$ Pools - $>$ Creat	te Pool		
Create Pool			
	Basic	Adv	vanced
POOL NAME	Select capacity from Tiers to alloca	ite to Pool	Tier Management
UCS_Application_Pool	DIAMOND		0.00 GiB Available
STORAGE SYSTEM	0.00 GiB		~
60749	PLATINUM		10.32 TiB Available
USE FOR SNAP?	10.32 TIB		v
Yes No	GOLD		0.00 GIB Available
BREAKDOWN OF DISKS	0.00 GIB		~
Total: 10.32 TiB	SILVER		0.00 GiB Available
Platinum: 10.32 TiB (100.00 %)	0.00 GiB		~
	BRONZE		0.00 GiB Available
	0.00 GIB		~
	UTILIZATION THRESHOLD (LOW) %	UTILIZATION THRESHOLD (HIGH) %	SUBSCRIPTION LIMIT
	70	80	Unlimited
		If this threshold is exceeded, snapshots will be disabled to ensure there is enough capacity for user data.	
			Cancel Submit +

#### **Procedure 8.** Allocate FC-SCSI Shared VMFS LDEV and Adding LDEV Paths from Server Groups

Step 1. Log in to Hitachi Ops Center Administrator and from the navigation pane, select Servers.



**Step 2.** From the Servers tab, select **Server Groups**, and then select a SERVER GROUP ID. Under the Actions, pane select, **Attach Volumes**, and then click **Create**, **Attach and Protect Volumes with Local Replica-tion**.

HITACHI Ops Center Admini	strator	Dashboard	Jobs Monitoring	
Dashboard > Servers +				
Servers				
Summary				
	Servers			Server Groups
+ 🖻 🖋 Actions				
Q Attach Volumes >	Attach Existing Volumes			
O SERVER GROUP ID	Create, Attach and Protect Volumes with Local Replication	SERVER GROUP NAME	sr	RVER COUNT
© 2	Create, Attach and Protect Volumes with High Availability	VSI_UCS_Cluster_1	4	

**Step 3.** Configure volumes for the specified Storage System. You can switch to another Storage System using the Storage System drop-down list. To allocate LDEVs for use as VMFS datastores:

- a. For the VOLUME LABEL enter VSI-VMFS-DS.
- b. Select the NUMBER OF VOLUMES.
- c. Enter the Volume SIZE and select the volume unit: GiB, TiB, or Blocks.
- d. Select the POOL TYPE as Thin.
- e. For a Thin pool, select the POOL TIER: Diamond, Platinum, Gold, Silver, or Bronze.
- f. By default, the **POOL** is auto selected. Verify that the chosen **POOL** is the "UCS\_Application\_Pool" for provisioning VMFS datastores.
- g. Click the plus sign (+) to verify volume settings.
- h. Click Next.

ashboard > Servers - > Create, Attach and Protect Volu					
Create, Attach and	Protect Volum	nes			
1. Create Volumes 2. Attach Settings	3. Path Settings 4.	Protect Volumes 5. Op	eration Plan		
STORAGE SYSTEM	VOLUME LABEL VSI-VMFS-DS	e.g. 1	DUMBER OF VOLUMES	size 5 TiB	
SUBSCRIBED CAPACITY 16% (10.13 TIB / 61.90 TIB)	Auto - From	- To	Auto - From	- To	
VIRTUAL STORAGE MACHINE	Thin CAPACITY SAVING	Platinum	UCS_Application_Pool(10.3	TIERING POLICY	
No VSM Selected (Default Meta Resol 🛩	Deduplication and Comp				
For servers or server groups that have mis-matched Host Modes or Host Mode	virtual LDEV IDs w	vith the physical LDEV I	ld if you want Ops Center Ac Ds.	aministrator to attemp	ot to match the
Options, please use the "Attach Like Volumes" function from the server's volume inventory, in order to	VOLUME LABEL VSI-VMFS-DS	LABEL SUFFIX	NUMBER OF VOLUMES 2	size 5	тів -
prepopulate paths properly.	VOLUME ID/RANGE Auto -		VIRTUAL ID/RANGE Auto 👻		
	POOL TYPE Thin	POOL TIER     Platinum	POOL • UCS_Application_Po	TIERING POLICY	
	CAPACITY SAVING Deduplication and Con	npressio <del>n</del>			

**Step 4.** The **HOST MODE** and **HOST MODE OPTIONS** should be selected as follows:

- a. HOST MODE: VMWARE EX.
- b. HOST MODE OPTIONS: 63 (VAAI) Support option for vStorage APIs based on T10 standards.
- c. Select **MANDATE LUN ALIGNMENT** as **Yes**; this option determines whether to assign the same LUN number to multiple servers for a volume. If Yes is specified, the same LUN number is always assigned.
- d. Set AUTO CREATE ZONE as No.
- **Step 5.** Click **Next** to explore options for creating and editing LUN paths.

HITACHI Ops Center Administrator		Dashboa	ard Jobs Mo	onitoring			
Dashboard > Servers - > Create, Attach and Protect Volumes w							
Create, Attach and Pr	otect Vol	umes					
1. Create Volumes 2. Attach Settings	3. Path Settings	4. Protect Volumes	5. Operation Plan				
STORAGE SYSTEM (60749)						View Propo	osed Volume ID Selection
HOST MODE	NUMBER OF VO	LUM LABEL	LABEL SUFFIX	SIZE	POOL TYPE	TIER	POOL
VMWARE EX	2	VSI-VMFS-DS	_	5.00 TIB	Thin	Platinum	UCS_Application
63 - (VAAI) Support option for vStorage							
HOST GROUP NAME							
(Optional)							
MANDATE LUN ALIGNMENT							
Yes No							
AUTO CREATE ZONE							
Yes No							
	_					Can	cel Previous Next

**Step 6.** On the **Path Settings** pane, you need to click the respective server WWNs and map them to the VSP storage ports as based on MDS zoning. When completed, you can expect to see the following:

HITACHI Ops Center Admin	istrator	Dashboard Jobs	Monitoring		
	reate, Attach and Protect Volumes with Local Replication				
< 🛙	Create, Attach and Protect Volumes				
	1. Create Volumes 2. Attach Settings 3. Path Settings 4. Protect Volumes 5	Operation Plan			
	Switch View Suggest				Existing New
	4 Servers			24	Farget Storage Ports
	UCS_ESXI_1 (VMWARE EX)				
			20:00:00:25:85:21:0A:00(Hba_A)	CL1-4	
			20:00:00:25:85:21:08:00(Hbe_8)	C1.1	0
	UCS_ESXI_2 (VMWARE EX)			C114	: 0
			20:00:00:25:B5:21:0A:02(Hba_A)	(12)	0
			20:00:00:25:85:21:08:02(Hba_8)	C124	0
	UCS_ESXI_3 (VMWARE EX)			C124	:θ
			20:00:00:25:85:21:0A:04(Hba_A)	(13)	0
			20:00:00:25:B5:21:0B:04(Hba_B)	034	0
	UCS_ESXI_4 (VMWARE EX)			CL34	:0
			20:00:00:25:85:21:0A:06(Hba_A)	CL44	A <b>O</b>
			20:00:00:25:B5:21:08:06(Hba_B)	CL4-1	8 <b>0</b>
				CL4-0	0
				CL5-	0
				CL5-I	0
				CL5-0	0
				CL6-J	θ
				CL6-1	0
				CL5-1	0
				CL7-4	0
				CL7-1	0
					· · · · · · · · · · · · · · · · · · ·
					Cancel Previous Next

Step 7. For the **REPLICATION TYPE** select **None** and click **Next**.

	ervers 👻 🖒 Create, Attach and Protect	Volumes with Local Repli	ication	Dashboard Jobs	s Monitoring		
<	🛱 Create, Attach	and Protect \	/olumes				
	1. Create Volumes 2. Attach	Settings 3. Path Sett	tings 4. Protect Volum	es 5. Operation Plan			
	REPLICATION TYPE						
		Sna	р			None	
	VOLUMES NUMBER OF VOLUMES	LABEL	LABEL SUFFIX	SIZE	POOL TYPE	TIER	POOL
	2	VSI-VMFS-DS		5.00 TiB	Thin	Platinum	UCS_Application
						Ca	ncel Previous Next
Step 8.	If required to	modify the	LUN ID, click	LUN settings	s. If LUN ID is c	orrect skip to <b>St</b>	ер 10.
<	🕞 Create, Attac	h and Prot	ect Volume	S			
	1. Create Volumes 2. Atta	ach Settings 3. Pa	ath Settings 4. Pro	otect Volumes 5. Op	peration Plan		
	Host Group Name		VSI_x210_M7_01				
	Mandate LUN Alignment	t	Yes				
	Auto Create Zone		No				
	Mandate Using Displaye	d Volume IDs	No				
	Create Paths	tion					
	Planned Path Configura						LUN Settings
					6708165 BODT		
	VOLUME ID S	ERVER	WWN/ISCSI INITIATOR	NAME	STORAGE PORT	PROTOCOL	LUN
<b>Step 9.</b> click <b>OK</b> .	From the LUN	settings wir	ndow, choos	e the appropri	iate <b>LUN ID</b> usir	ng the FROM dro	op-down list,

**Step 10.** Verify the operation plan and click **Submit**.

istrator reate, Attach and Protect Volumes with Local Re	en l'estico		Dashboard Job	s Monitoring			
Greate, Attach and							
1. Create Volumes 2. Attach Settl	ings 3. Path Settings 4. Protect Volumes	s 5. Operation Plan					
Selected Servers							
SERVER ID	SERVER WARS	SERVER IF ADDRESS	PROTOCOL	05 1175	FOLUME COUNT	RAPEIC	ATION TYPE
2	UCS_E5X0_1	10.1.168.111	Fibre	VMWARE EX	4	-	
3	UCS_ESX0_2	10.1.168.112	Fibre	VMWARE EX	4		
4	UCS_ESXU_3	10.1.168.113	Fibre	VMWARE EX	4	_	
5	UCS_ESXL_4	10.1.168.114	Fibre	VMWARE EX	4	-	
Create Volumes							
Volume Location							
LOCATION Storage System		VALUE (60749)					
Virtual Storage Machine		-					
Volume Specification	VOLUME ID POLUME LAR	RL CAPILOTY	VIRTUAL IDARANDI	FOL THE FOR THE	FOR NAME	TIR KING POLICY	CAPACITY SAVING
Auto	32 (00:00:20) VSI-VMFS-0	DS 5.00 GIB	Auto	Thin Platinum	UCS_Application_Pool(10.09 T		Deduplication and Compres
Attach Settings							
Host Mode		VALUE VWWARE EX					
Host Mode Options		63					
Host Group Name		65					
Mandata LUN Alignment		Yes					
Auto Create Zone		No					
Auto create zone		NU					
Mandate Using Displayed Volum	te IDs	No					
Create Paths Planned Path Configuration							LUN Setting
Create Paths Planned Path Configuration	172 <sup>1</sup> 721 <sup>1</sup> 3	AGAINS AS ITS A MENAPITIA (L)			159		LUN Setting
Create Paths Planned Path Configuration -acquatacoay -32 (0000-20)	005,050,7 005,150,3	абылык лапин і алганутар (а) 2000 02 25 85 21 64 Сайнар Ді		0.5× 0.14	rative Fibre	- 4	LUN Setting
Create Paths Planned Path Configuration 22 (000020) 32 (000020)	0.02 120 3 0.02 120 3	2000/02/2010/1100/04/06,07 2000/02/2012/100/24/06,0 2000/02/2012/10/24/06,0		CL2-A	rase Riter Fiber	2 4 4	LUN Setting
Create Paths Planned Path Configuration 22 0000231 32 0000231 32 0000233	0.5,150,2 0.5,150,3 0.5,150,3 0.5,150,3	доологи / ало и таколума, ку 2000 00 2188 21 Ало Алана, А 2000 00 258 21 Ало Алана, А 2000 00 258 21 Алана (Алана, А		CL2-A CL3-A	rase Fibre Fibre Fibre	- - 	LUN Setting
Create Paths Panned Path Configuration ar yearscury 32 0000020 32 0000020 32 0000020 32 0000020 32 0000020	rczienia rczienia rczienia rczienia			0.2-4 0.3-4 0.4-4	rana Filog Filog Filog Filog	2 4 4 4 4	UDI Setting
Create Paths Planned Path Configuration 24 decease 24 d	60,500,7 00,500,3 00,500,3 00,500,3 00,500,4	20000225812108049988_03 200002581210044986_03 20000258121044986_03 2000025812104486_03 2000025812104860306_03 2000025812104860366_03		0.2-4 0.3-4 0.1-4	rator Titor Titor Titor Titor Titor	- 4 4 4 4	LDI Senny
Create Paths Painred Path Configuration as genoses 22 000020 32 000020 32 000020 32 000020 32 000020 32 000020 32 000020	103,550,7 105,550,3 105,560,3 105,560,3 105,560,4 105,560,4	2000012/2010/2710010/0000000000000000000		0.24 0.34 0.44 0.14 0.24		- - - - - - - - - - - - - - - - - - -	LDN Serring
Create Paths Panned Path Configuration ar generatory 32 (000020) 32 (000020) 32 (000020) 32 (000020) 32 (000020) 32 (000020) 32 (000020) 32 (000020)	003,000,7 005,000,3 005,000,3 005,000,3 005,000,4 005,000,4 005,000,4 005,000,4	20000127-000271500127100109984, ay 2000002250021700212602710024040a, 44 2000002716021740021404, 40 200000216021740021404, 40 20000025602160214064044, 40 20000025602160214064044, 40 20000025602174001404044, 40		034 034 034 014 034 034	Fibre	2 4 4 4 4 4 4 4 4 4	UM Sering
Create Paths Painred Path Configuration as genoses 22 000020 32 000020 32 000020 32 000020 32 000020 32 000020 32 000020	60,500,7 (05,500,3 (05,500,3 (05,500,4 (05,500,4 (05,500,4 (05,500,4 (05,500,4	2000012/2010/2710010/0000000000000000000		0.24 0.34 0.44 0.14 0.24	Fibre	2 4 4 4 4 4 4 4 4 4 4 4	UM Sering
Create Paths Parned Path Configuration as generating 22 0000201 22 0000201 23 0000201	60,500,7 (05,500,3 (05,500,3 (05,500,4 (05,500,4 (05,500,4 (05,500,4 (05,500,4	20000127-000271500127100109984, ay 2000002250021700212602710024040a, 44 2000002716021740021404, 40 200000216021740021404, 40 20000025602160214064044, 40 20000025602160214064044, 40 20000025602174001404044, 40		034 034 034 014 034 034	Fibre	4 4 4 4 4 4 4 4 4	LUX Setting
Create Paths Panned Path Configuration 23 0000201 23 00000201 23 0000020 23 0000020 23 0000020 23 0000020 23 0000020 23 0000020 23 0000020 23 0000020 23 000020 23 0000020 23 0000020 23 0000020 23 0000020 23 000020 20 000020 20 000020 20 0000020 20 00000000	000,000,0 000,000,0 000,000,0 000,000,0	20000127-000271500127100109984, ay 2000002250021700212602710024040a, 44 2000002716021740021404, 40 200000216021740021404, 40 20000025602160214064044, 40 20000025602160214064044, 40 20000025602174001404044, 40		034 034 034 014 034 034	Fibre	4 4 4 4 4 4 4 4	LDi Sette
Create Paths Parned Path Configuration as generating 22 0000201 22 0000201 23 0000201	000,000,0 000,000,0 000,000,0 000,000,0	ADDATACA ERISA A REPUBLIQUE, IN 2020/2002/2005/2005/2006/2004 2020/2002/2005/2005/2004/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2004 2020/2005/2005/2005/2005/2004 2020/2005/2005/2005/2005/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004	WANKE IX	034 034 034 014 034 034	Fibre Fibre Fibre	4 4 4 4 4 4 4 4 4 4 5 5000	UN Setting
Create Paths Panned Path Configuration as generative 32 000020 32 000020 30 000020 30 000020 30 000020 30 000020 30 000020 30 000020 30 00000000 30 0000000 30 0000000000	0.03,650,7 0.05,550,3 0.05,550,3 0.05,550,3 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,4 0.05,550,550,5 0.05,550,550,5 0.05,550,550,550,550,550,550,550,550,550			034 034 034 034 034 034 034	Flore Flore Flore Flore	2 4 4 4 4 4 4 4 4 4 2 5 500rg 5500rg	LUN Senny
Create Paths Panned Path Configuration 22 (000020) 22 (000020) 23 (000020) 24 (000020) 25 (000020) 26 (000000) 26 (000000000000000000000000000000000000	0.03,500,7 0.05,500,3 0.05,500,3 0.05,500,3 0.05,500,4 0.05,5	ADDATACIA DE LA TROBUNYEM, (L) 2000027585 17 464 ADDATA, (L) 2000027585 17 465 ADDATA, (L) 2000027585 17 465 ADDATA, (L)		024 0.14 0.14 0.14 0.14 0.14 0.14 0.14	Fibre Fibre Fibre Fibre		LDi Sette
Create Paths Panned Path Configuration as generate 32 000020 32 000020 30 00000 30 000000 30 0000000000	СС, 548, 7 СС, 548, 3 СС, 548, 3 СС, 548, 3 СС, 548, 3 СС, 548, 4 СС, 5	ADDATACA ERISA FINE AUTORNAL (N) 2020/2002/2005/2005/2006/2004 2020/2002/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2000/2005/2005/2006/2004 2020/2005/2005/2005/2006/2004 2020/2000/2000/2000/20000/20000000000	VMWARE EX	024 0.14 0.14 0.14 0.14 0.14 0.14 0.14	Fibre Fibre Fibre	Existing	UM Sering
Create Paths Panned Path Configuration 22 (000020) 22 (000020) 23 (000020) 24 (000020) 25 (000020) 26 (000000) 26 (000000000000000000000000000000000000	ка, сац. / СС, 580, 3 СС, 580, 3 СС, 580, 3 СС, 580, 3 СС, 580, 4 СС, 580, 5 СС, 580, 4 СС, 5	ARGANGA STREE A TREE RAYING (8) 2000007585 (21 GA (A ABINA, 4) 2000007585 (21 GA (A ABINA, 4) 200007585 (21 GA (ABINA, 4) 200007585 (21 GA (ABINA, 4) 200007585 (21 GA (ABINA, 4) 200007585 (21 GA (ABINA, 4) 200007585 (21 GA (AB	VMWARE EX	024 0.14 0.14 0.14 0.14 0.14 0.14 0.14	Fibre Fibre Fibre Fibre	Existing	LUTSerry
Create Paths Planned Path Configuration 23 (200023) 23	0.5, 500, 7 0.55, 500, 3 0.55, 500, 3 0.55, 500, 3 0.55, 500, 4 0.55, 500, 4 0.5		VMWARE EX VMWARE EX	024 0.34 0.14 0.14 0.34 0.34 0.34 0.34 0.34 0.34 0.34 0.3	Riter Filter Filter Filter	Existing Existing Existing	LDI Serie
Create Paths Panned Path Configuration as yearsary 32 0808029 32 0808029 Mandale Using Deplayed LUN Host Group Information Panned Iost Group Information Panned Iost Group Information Panned Iost Group Information Panned Iost Group Information 94 val 30 MZ 32 April 8	دین ایسی ۲     دین ایسی ۲     دری ایسی ۲	Additional Antibioty of Markowsky (Markowsky) 2020/2002 2018 21 (2004 (2004 Markowsky) 2020/2002 2018 21 (2004 (2004 Markowsky)) 2020/2002 2018 21 (2004 (2004 Markowsky))	VMWARE EX VMWARE EX VMWARE EX	034 034 034 034 034 034 034 04 04 04 04 04 04 03 04 00 04 00 04 00 04 00 04 00 04 00 04 00 00	Fibre Fibre Fibre	Existing Existing Existing Existing	UM Sering
Create Paths Panned Path Configuration as generate 32 0000201 32 0000201 30 0000201 30 0000000 30 00000000000000000000000	ка, сац. / UC, 500, 3 UC, 500, 3 UC, 500, 3 UC, 500, 3 UC, 500, 4 UC, 5	200002748127408129184 20000274812740424984 20000274812740424984 20000274812740424984 2000027481274042494 200002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 2000002748127404494 200000000000000000000000000000000	VMVARE EX VMVARE EX VMVARE EX VMVARE EX	034 034 034 034 034 034 034 034 034 034	Fibre Fibre Fibre	Existing Existing Existing Existing Existing	LUI Setting
Create Paths Panned Path Configuration 23 0000201 23 000020000000000000000000000000000000	СС, 580, 7 СС, 580, 3 СС, 580, 3 СС, 580, 3 СС, 580, 4 СС, 5		VMINARE EX VMINARE EX VMINARE EX VMINARE EX VMINARE EX	034 034 034 034 034 034 034 034 034 034	Fibre Fibre Fibre	Existing Existing Existing Existing Existing Existing	LDI Setto
Create Paths Panned Path Configuration as essessing 32 0000201 32 000000000000000000000000000000000000	دین ایمار به     دری ایمار به		VMWARE EX VMWARE EX VMWARE EX VMWARE EX VMWARE EX VMWARE EX	034 034 034 034 034 034 034 04 04 04 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Fibre Fibre Fibre	Existing Existing Existing Existing Existing Existing	LUVServ
Create Paths Panned Path Configuration as generating 22 000020 23 000020 24 000020 24 000020 24 000020 24 000020 25 000000 25 0000000 25 000000 25 000000 25 000000 25 000000 25 000000 25 000000 25 000000 25 000000 25 0000000000	دین ایمار به     دری ایمار به		VMWARE EX VMWARE EX VMWARE EX VMWARE EX VMWARE EX VMWARE EX	034 034 034 034 034 034 034 04 04 04 04 05 05 05 05 05 05 05 05 05 05 05 05 05	Fibre Fibre Fibre	Existing Existing Existing Existing Existing Existing	LUM Series

## Hitachi Storage Configuration for FC-NVMe

**Procedure 1.** Configure Fibre Channel Ports on Hitachi Virtual Storage Platform from Ops Center Administrator for FC-NVMe

**Note:** This procedure must be completed before provisioning the FC-NVMe VMFS datastore.

Step 1.Log in to Hitachi Ops Center Administrator and from the navigation pane, select Storage Systems.





Click the **S/N** listing for the Storage System.

ITACHI Ops Center Administrator			Dashboard Job	is Monitoring				T	<b>\$</b> (
Dashboard > Storage Systems +									
Storage Systems									
Summary									
Caparaly Aierts	Fab's Alerts Harr	ware Alerts	<ul> <li>125% Subscribed</li> <li>61.90 TIB Physica</li> <li>214.39 GIB Thin 14</li> <li>20.41 TIB Thin Fri</li> <li>20.42 TIB Allocatt</li> <li>41.27 TIB Unation</li> </ul>	I Capacity Jsed at to Pools	61.90 Total	Tier Breakdown Diamond Platenum Gold Silver Bronze Distrinal Sob	Ters Pr	mearcian Savingt	
🔟 🥒 Actions									
NAME 5/N	IP ADDRESS	MODEL	TOTAL	THIN FREE	THIN USED	USAGE	INCOMPLETE HA ARRAY	MIGRATION TASK CO	un
AA22-5600 60749	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GIB	0.96	-	0	
ems 0 selected							show 2	100 🗸 Items 👘	100

#### Step 3. Select Fibre Channel Port (for example, CL1-B). Click the Edit sign icon.

HITACHI Ops Cente	er Administrator		Dashboard Jo	bs Monitoring				1 ¢ 🖲
Dashboard > Storage	Systems - > 60749 > Ports -							
Ports								nii (兄
Summary								
	Fibre					iSCSI		
	SCSI					NVMe		
1								***
Q								
	WWN	SPEED	FABRIC,	CONNECTION TYPE	SECURITY	VSM PORT	ATTRIBUTE	
⊘ CL1-B	50:06:0E:80:08:ED:4D:01	Auto	Fabric	ON / Point-to-point	No	No	Target	

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 177 of 367

Step 4. Select NVMe Mode and Disable Security and verify that the port attribute is Target. Click OK.Note: For the VSP E1090 systems, you are not required to modify port attributes.

← C 🔺	Not secure   https://opsvm.adapti	ve-solutions.local:20961/	#/storage-systems/60749/storage	e-ports	Q A <sup>N</sup> ☆		• · · •
HITACHI Ops Center	r Administrator		Dashboard Jobs Monitoring				100
Dashboard > Storage S	Systems + > 60749 > Ports +						
Ports					_		nin 🛱
1 0112		🛕 Edit Fibre	Port		×		
Summary			TOIL				
		Modify port set	tings for the 1 selected ports to:				
	Fibre				ISCSI		
		S	ISI Mode NVMe Mo	ide	NVMe		
		Enal	ble Security Disable Sec	urity			≕
۹		Target		~			
O PORT ID	www.w				VSM PORT	ATTRIBUTE	
O CL1-A	50:06:0E:80:08:ED:4D:00				No	Target	
⊘ CL1-B	50:06:0E:80:08:ED:4D:01		Cancel OK 🗸		No	Target	
	50:06:0E:80:08:ED:4D:02	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL2-A	50:06:0E:80:08:ED:4D:10	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL2-B	50:06:0E:80:08:ED:4D:11	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL2-C	50:06:0E:80:08:ED:4D:12	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL3-A	50:06:0E:80:08:ED:4D:20	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL3-B	50:06:0E:80:08:ED:4D:21	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL3-C	50:06:0E:80:08:ED:4D:22	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL4-A	50:06:0E:80:08:ED:4D:30	Auto	Fabric ON / Point-to-point	Yes	No	Target	
O CL4-B	50:06:0E:80:08:ED:4D:31	Auto	Fabric ON / Point-to-point	No	No	Target	l i i i i i i i i i i i i i i i i i i i
O CL4-C	50:06:0E:80:08:ED:4D:32	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL5-A	50:06:0E:80:08:ED:4D:40	Auto	Fabric ON / Point-to-point	No	No	Target	
O CL5-B	50:06:0E:80:0B:ED:4D:41	Auto	Fabric ON / Point-to-point	No	No	Target	
	50:06:0E:80:08:ED:4D:42	Auto	Fabric ON / Point-to-point	No	No	Activate W	
O CL6-A	50:06:0E:80:08:ED:4D:50	Auto	Fabric ON / Point-to-point	No	No	TageSettings	
24 Items 1 selected						show 200 🗸 Ite	ms 🔹 1 🔹 🔻

#### Step 5. Repeat Step 1 through Step 4 for the remaining Fibre ports CL2-B, CL3-B, and CL4-B.

After all the ports are configured, you can expect the following representation:

HIACHI Ops Center A	Administrator		Dashboard Jobs Monitoring			10
Dashboard 👌 Storage Sy	stems • > 60749 > Ports •					
Ports						包 雪
Summary						
	Fibre				ISCSI	
	SCSI				NVMe	
>						
L.						
<b>`</b>						
PORTID	www	SPEED	FABRIC, CONNECTION TYPE	SECURITY	VSM PORT	ATTRIBUTE
	www 50:06:0E:80:08:ED:4D:01	SPEED	FABRIC, CONNECTION TYPE Fabric ON / Point-to-point	SECURITY No	VSM PORT	Target
PORTID						
PORTID CL1-B	50:06:0E:80:08:ED:4D:01	Auto	Fabric ON / Point-to-point	No	No	Target

## Procedure 2. Initialize Parity Groups from Ops Center Administrator for FC-NVMe

Step 1.Log in to Hitachi Ops Center Administrator and from the navigation pane, select Storage Systems.

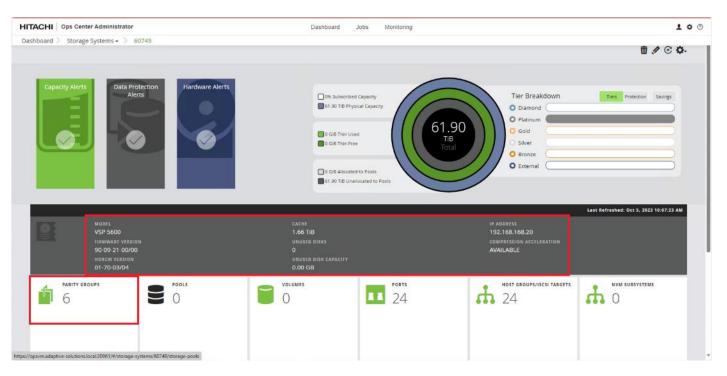




Click the **S/N** listing of the Storage System.

HITACHI Ops Center Administrator			Dashboard	Jobs Monitoring					100
Dashboard 3 Storage Systems +									
Storage Systems									
🛡 Summary									
Capacity Alerts Data Protection Alerts	Picky Alexts	Hardware Alerts	0 51.50 TB 1 214.35 GZ 20.41 TB 1 0 20.62 TB /		61.90 18 753	Tier Breakdo Diamond Pistnam Gold Silver Pistnam External Sos	wn tes /	noartisen Sayinge	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
+ 🗇 / Actors									
Q.									
D NAME SIR	IP ADDRESS	MODEL	TOTAL	THUS FREE	THUN USED	USAGE	INCOMPLETE HA ARRAY	NIGRATION TASK	COUNT
O AA22-5600 60749	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GIB	0.96	-	0	
I Items 0 selected								200 🛩 items	- 0

**Step 3.** Click the **PARITY GROUPS** icon, under the selected storage system, to view parity groups.



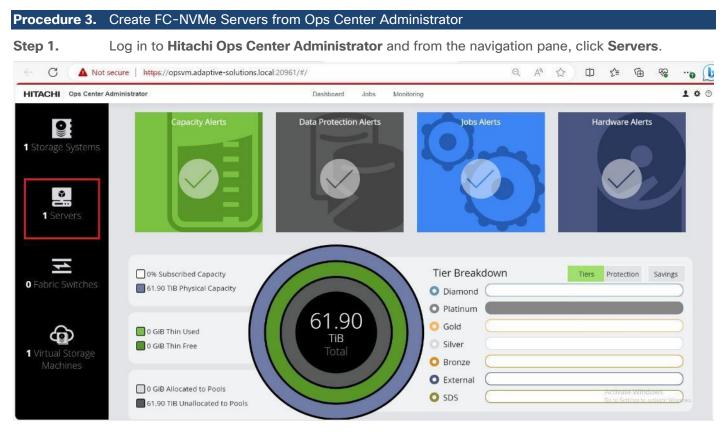
**Step 4.** Select any **Parity Group ID** you want to initialize as parity for creating the FC-NVMe pool. From the **Actions** pane, click **Initialize Parity Groups.** 

HITACHI	Ops Center Administrator			Dashboard	Jobs Monitoring				10
Dashboard 🤇	Storage Systems 🔹 🌾 6	0749 👌 Parity Groups 🕶							
Parity	/ Groups								Ę.
Summary									
Actions									
initialize Par	ity Groups								
Enable Com	pression on Parity Groups	RAID TYPE	DISK TYPE	TOTAL CAPACITY	UNINITIALIZED CAPACITY	INITIALIZED	USED	COMPRESSION	USAGE
) 1- <b>1</b>	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB	-	100%
) 1-2	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB		100%
) 1-3	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		096
) 1-4	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB	-	095
) 1-5	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
) 1-6	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
items 1 selec	ted								show 200 🛩 Items

Step 5. Click OK.

	> Storage Systems - > t	0749 ) Parity Groups -							
Parit	y Groups								t
			🔜 🗛 Ini	tialize Parity	Groups Confir	mation	×		
Summary									
ctions				he selected 1 parity gro nitialized. Do you want t	ups in the current storage sy to proceed?	ystem will be			
Initialize P.	arity Groups						_		
Enable Co	mpression on Pendy Groups	RAID TYPE	DISK TYPE		Cancel OK +		Useo	COMPRESSION	usase
Stat.	IN_USE	RAID6 6D+2P	S5D NVMc 1.90 T6	10:32 116	3.00 MIB	0.00 G/6	10.92 116	24	100%
1-2	INJUSE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.31 TIB	3.00 MIB	0.00 GIB	10.32 718		100%
1-3	LININITIALIZED	RAID6 6D 2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 110	0.00 GIB			C/HE
1.4	UNINITIALIZED	RAID6 6D+2P	S50 NVMe 1.90 FB	10.32 118	10.32 118	0.00 GIB	0.00 GIB		0%
	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 G/B		CH.
	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB				096

**Note:** Created Parity Groups initially have a status of UNINITIALIZED. Upon complete initialization, the status should change into IN\_USE.



**Step 2.** Click the plus sign (+) under **FC-NVMe Servers** section.

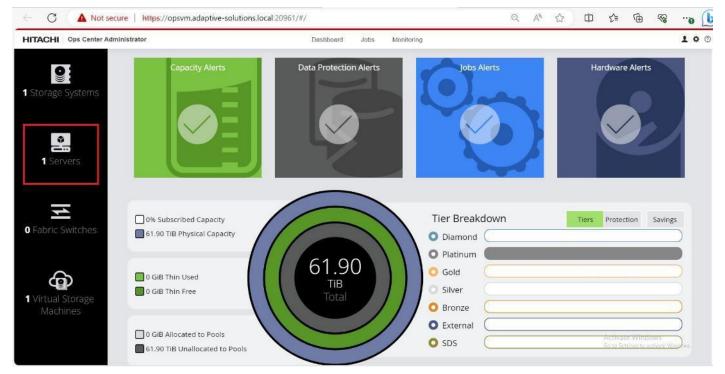
Step 3.Enter the SERVER NAME, IP ADDRESS, OS TYPE as VMWARE EX and HOST NQN, and clickSubmit.

Step 4.Repeat Step 1 through Step 3 to add the remaining Cisco UCS servers that use the FC-NVMeprotocol.

Dashboard > Servers -			Dashboard Jobs Monitoring		
<	Add Servers				
	CSV Import				
			+		
	Fibre Servers				
	FC-NVMe Servers		+		
			•		
	SERVER NAME           UCS_INAL_ESKI           WWN           Socoocococococococococococococococococo	DESCRIPTION Description	IP ADDRESS 10.1168.111 HOST NON ngn.2014.08.com.vmsware.mene.ecsi-1	OS TYPE VANVARE EX	×
	ISCSI Servers				
					Gancel Submit -

#### Procedure 4. Create FC-NVMe Server Groups from Ops Center Administrator

#### Step 1. In the Ops Center Administrator Dashboard, from the navigation pane, click Servers.



**Step 2.** Select the **Server Groups** tab. Click the plus sign (+).

Servers			≛ ⊙
Summary			
	Servers	Server Groups	
+ 🛍 🖉 Actions			#
٩			
O SERVER GROUP ID	SERVER GROUP NAME	SERVER COUNT	

Step 3. In the add Server Group wizard, enter the SERVER GROUP NAME.

#### Step 4. Select the FC-NVMe Servers from AVAILABLE SERVERS and click Add.

HITACHE	Ope Center Admini	abrahor				Dashboard	Jobs	Monitoring		1	<b>o</b> 🙂
Dephopend 3		Add Server Group									
<	-	Add Server Gro	pup								
		SERVER GROUP NAME VSLUCS_NVMe_Custer									
		Description (OPTIONAL) Description									
		AVAILABLE SERVERS							ASSIGNED SERVERS		
		۹							O 101715 AARS IF ADDRESS FRANKLOS 00 1775		
		O UCS_859_1	10.1.168.111	Fearleces. Fibre	AN INVESTIGATION						
		O UCS_ESU_2	10.1.168.112	Fibre	VM/WARE EX						
		O UCS_ESIL_3	10.1.168.113	Fibre	VM/WARE DC						
		O UCS_ESN_4	10.1.168.114	Fibre	VM/WARE EX						
		O UCS_WMe_ESX1	-	FC-NVMe	VM/MARE EX						
		O UCS_NVMe_ESK2	-	PC-NVMe	VM/WARE EX						
		O UCS_NVMe_ESK3	-	PC-NVMe	VM/WARE EX						
		☺ UCS_NVMe_ES04	-	PC-NVMe	VM/WARE EX						
		8 items 4 selected			tow 2. 🛩 items - 🛐 -						
								-			
						L	ASE>				
							< femore				

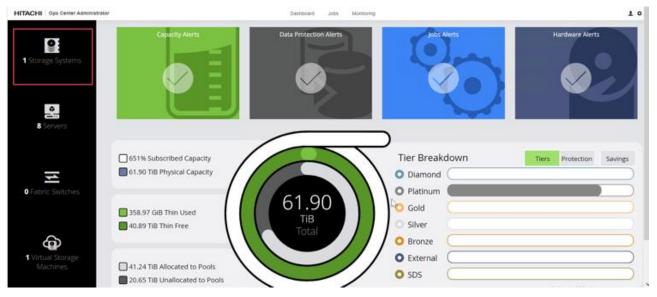
Step 5.The FC-NVMe Servers are moved from the AVAILABLE SERVERS to the ASSIGNED SERVERS list.Click Submit.

Database 2: Server Group:       Add Server Group:         Server Group:       Add Server Group:         Server Group:       Server Group:         Description       Server Group:         Add Server Server Group:       Server Group:         Server Group:       Server Group:         Add Server S	HITACHI Ops Center Adn	ninistrator				Dashboard	Jobs Monitoring					
SREVER GROUP NAME VSU/USL3/VMR2_CUUZEr           DESCRIPTION (OPTIONAL)           Description           AVAILABLE SERVERS           C         ASSIGNED SERVERS           O         URSLIPSION         MATERIAL         MATERIAL           O         URSLIPSION         MATERIAL         MATERIAL         MATERIAL           O         URSLIPSION         MATERIAL         MATERIAL         MATERIAL         MATERIAL           O         MATERIAL         MATERIAL         MATERIAL         MATERIAL         MATERIAL         MATERIAL           O         URSLIPSION         MATERIAL         MATERIAL         MATERIAL         MATERIAL         MATERIAL           O         URSLIPSION         MATERIAL												
V9LUCLJ.VVM.e., Cluster         BESCRIPTION (0PTIONAL)         DESCRIPTION (0PTIONAL)         DESCRIPTION (0PTIONAL)         DESCRIPTION (0PTIONAL)         SAVALAGE SERVICES         COLSPAN= SERVICES         O 1002, ISSN 1       ANOTAL SERVICES         O 1002, JONNAE ESSN 1       C 1000, ISSN 1000 ES <td>&lt; 4</td> <td>Add Server Gr</td> <td>oup</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	< 4	Add Server Gr	oup									
Discription         OPTION (OPTIONAL)           Discription         ASSIGNED SERVERS         ASSIGNED SERVERS         ASSIGNED SERVERS           - <td></td>												
Description           AVAILABLE SERVERS         ASSIGNED SERVERS           V         ASSIGNED SERVERS         PROTOCI         PROTOCI </td <td></td>												
AVAILABLE SERVERS         ASSIGNED SERVERS           V         MATERIAL			)									
D         DEVENTION         PARTINICAL         RATIVATION         RATIVATION         PARTINICAL		Description										
V RAMARTER         RAMARTER         RAMARTER         CLAVANA         VINVARE EX           0         UCS_STOL_1         10.1.168.111         Filter         VINVARE EX         0         UCS_STOL_0         -         FCAVANA         VINVARE EX           0         UCS_STOL_2         10.1.168.112         Fibre         VINVARE EX         0         UCS_STOL_2         -         FCAVANA         VINVARE EX           0         UCS_STOL_2         10.1.168.112         Fibre         VINVARE EX         0         UCS_STOL_2         -         FCAVANA         VINVARE EX           0         UCS_EDX_4         10.1.168.114         Fibre         VINVARE EX         0         UCS_STOL_4/VIN_E_SSS3         -         FCAVANA         VINVARE EX		AVAILABLE SERVERS						ASSIGNED SERVERS				
O         UCS_LSX_1         10.118.111         Filter         VMWARE EX         O         UCS_NVM_E ESc2         -         FCAVMA         VMWARE EX           O         UCS_SEX_2         10.118.112         Titrie         VMWARE EX         O         UCS_VVM_E ESc3         -         FC.WVM         VMWARE EX           O         UCS_SEX_3         10.1168.113         Titrie         VMWARE EX         O         UCS_VVM_E,ESx3         -         FC.WVM         VMWARE EX           O         UCS_SVVM_E,ESx4         10.1168.114         Fbre         VMWARE EX         O         UCS_VVM_E,ESx4         -         FC.WVM         VMWARE EX								C SERVER NAME	IP ADDRESS	PROTOCOL	DS 11/6	
O         UCS_ESX,2         10.1168.112         TBre         VMINARE EX         O         UCS_IVMA_ESX/3         FC.W/ME         VMINARE EX           O         UCS_ESX,4         10.1168.113         TBre         VMINARE EX         O         UCS_IVMA_ESX/3         -         FC.W/ME         VMINARE EX           O         UCS_ISX,4         10.1168.114         FBre         VMINARE EX         O         UCS_IVMA_ELSX/4         -         FC.W/ME         VMINARE EX		O TERVER NAME	IF ADD8755	PROTOCOL	DS TYPE			O UCS_NVMe_ESXI1	-	FC-NVMe	VMWARE EX	
O         UCE_EDD(_2         10.1.66.112         Flow         VMIWARE EX           O         UCE_EDD(_3         10.1.66.113         Flow         VMIWARE EX           O         UCE_EDD(_4         10.1.66.114         Flow         VMIWARE EX           O         UCE_EDD(_4         10.1.66.114         Flow         VMIWARE EX		O UCS_ESN_1	10.1.168.111	Fibre	VMWARE EX			O UCS NVMe ESX2	-	FC-NVMe	VMWARE EX	
O         UCS_ESU(3         10.1.168.113         Fibre         VAINARE EX           O         UCS_ESU(4         10.1.168.114         Fibre         VAINARE DX		O UCS_ESX[_2	10.1.168.112	Fibre	VMWARE EX				-	FC-NVMe	VMWARE EX	
O UC5_E5XL4 10.1.168.114 Fibre V/MWARE EX		O UCS_ESXL3	10.1.168.113	Fibre	VMWARE EX							
4 items 0 selected show 2 🗸 tems 🔹 1		O UCS_ESXL4	10.1.168.114	Fibre	VMWARE EX			C) OCSUMMEDIAM	-	POINTING	THITTERS DA	
		4 items 0 selected		st	ow 2 🗸 items < 1 >							
							Add >					
Add>						-	Remove				Cancel Submit -	
											Repito 28	

#### **Procedure 5.** Create a Hitachi Dynamic Provisioning Pool for UCS Servers for FC-NVMe VMFS Volume LDEVs

When creating a pool, use the basic option to take advantage of tiers of storage available on the VSP, following best practices. By default, the basic option will create a Hitachi Dynamic Provisioning Pool. For increased flexibility and if best practices are not essential, choose the advanced option. This enables you to specify Parity Groups and define your pool types as either Tiered, Thin, or Snap.

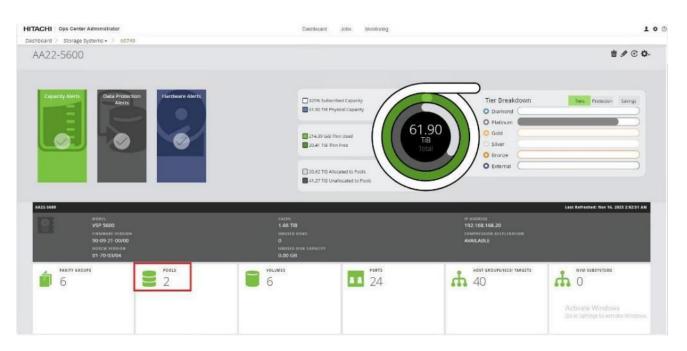
**Step 1.** Log in to **Hitachi Ops Center Administrator** and from the navigation pane, click **Storage Systems** to access the inventory of registered storage systems.



Step 2. Click the S/N listing of the Storage System.

HITACHI Ops Center Administrator			Dashboard	Jobs Monitoring				1	LOG
Dashboard > Storage Systems - Storage Systems									
Coperny Alerts Alerts Alerts		Hardware Alerts	0 61.50 TB 1 214.35 GZ 2041 TB 0 20.42 TB /		61.90 TB TGS	Tier Breakde Diamond Pistmond Gold Silver Bronze External SDS	wn Tes /	Prosettise Sayings	
+ 🗊 🖉 Actors									
م.									
D NAME SIR	IP ADDRESS	MODEL	TOTAL	THUS FREE	THIN USED	USACE	INCOMPLETE HA ARRAY	NIGRATION TASK	COUNT
AA22-5600 607/19	192.168.168.20	VSP 5600	61.90 TIB	20.41 TIB	214.39 GID	0.98	-	0	
Rems 0 selected								200 🛩 items	- 13

Step 3. From the Storage System, click Pools.



**Step 4.** Click the plus sign (+) to open the **Create Pool** window.

HITACHI	Ops Center Administrator		
Dashboard >	Storage Systems 🔹 🎽 6074	9 > Pools +	
Pools			
▼ Summary Ca	pacity Alerts		
+ 🗊 🖉 A	ctions		
	orage Pool		
0 ID 0 0	NAME	түре	ACTIVE FLASH
0 0	UCS_Boot_Pool	Thin	No
0 1	UCS_Application_Pool	Thin	No

#### **Step 5.** Enter the following details:

- a. For the **POOL NAME** enter **UCS\_Application\_NVMe\_pool** (Pool names can be any combination of alphanumeric characters, hyphens, and underscores only. Initial hyphens are not allowed.)
- b. Click an available **Tier** to view the available storage capacity and select the available **capacity**.
- c. Review the **high and low pool utilization thresholds**. By default, the low utilization threshold set to 70% and the high threshold is set to 80%. You can customize thresholds to receive notifications based on their specific environment requirements.
- d. To specify over allocation, you can set the limit to **Unlimited**.
- e. Click Submit.

HITACHI Ops Center Administrator	Dashboard	Jobs Monitoring					
Dashboard > Storage Systems + > 60749 > Pools + > Create	e Pool						
Create Pool							
E	Basic	Ad	vanced				
POOL NAME UCS_Application_NVMe_pool STORAGE SYSTEM	Select capacity from Tiers to alloca DIAMOND	ate to Pool	Tier Management 0.00 GiB Available				
60749 Use for snap?	PLATINUM 10.32 TIB		10.32 TiB Available				
Yes No	GOLD		0.00 GiB Available				
BREAKDOWN OF DISKS Total: 10.32 TIB	0.00 GiB     ~       siLVER     0.00 GiB Available						
Platinum: 10.32 TiB (100.00 %)	0.00 GiB 🗸						
	BRONZE 0.00 GIB Availat						
	0.00 GIB						
	UTILIZATION THRESHOLD (LOW) % 70	UTILIZATION THRESHOLD (HIGH) % 80 If this threshold is exceeded, snapshots will be disabled to ensure there is	SUBSCRIPTION LIMIT				
		enough capacity for user data.	Cancel Submit 💌 ow				

**Procedure 6.** Allocate FC-NVMe Shared VMFS LDEV and Adding LDEV Paths from Server Groups

Step 1. Log in to Hitachi Ops Center Administrator console and click the Servers tab.



Step 2. Select the Server Groups under the Servers tab, and then select Server Group ID.

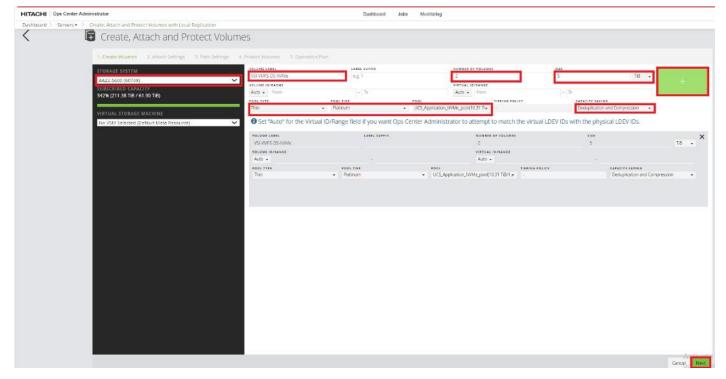
Step 3.Under Actions, click Attach Volumes, select Create, Attach and Protect Volumes with LocalReplication.

HITACHI Opa Center Admini	sirator		Dashboard	Jobs	Monitoring		1 ° 0
Dashboard > Servers + Servers							<u>.</u> ⊙
Summary							
	Servers					Server Groups	
+ 🗊 🖉 Actions				_			표
Q. Attach Volumes >	Attach Existing Volumes						
O SERVER GROUP ID	Greate, Attach and Protect Volumes with Local Replication	SERVER SROUP NAME				SERVER COUNT	
O 2 O J	Create. Attach and Protect Volumes with High Availability	VSI_UCS_Cluster_1				4	
0 1		VSI_UCS_NVMe_Cluster				4	
2 items 1 selected							show 2. 🗸 items 🤘 🚺 >

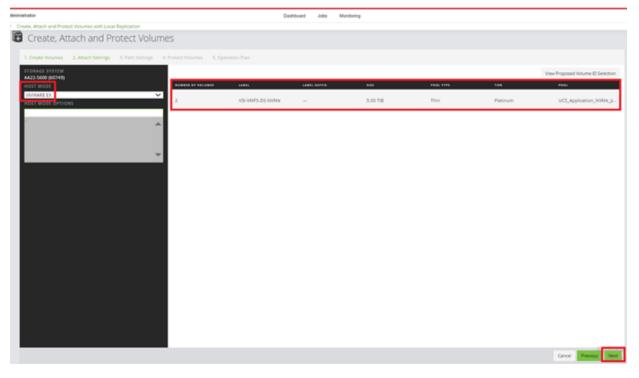
**Step 4.** Configure volumes for the specified storage System. Proceed with the following steps to add the volumes to UCS ESXi servers that use the FC-NVMe protocol.

- a. For the VOLUME LABEL enter VSI-VMFS-DS-NVMe.
- b. Select the NUMBER OF VOLUMES.
- c. Enter the Volume SIZE. And select the volume unit: GiB, TiB, or Blocks.
- d. For the POOL TYPE select Thin.
- e. For a Thin pool, select the POOL TIER: Diamond, Platinum, Gold, Silver, or Bronze
- f. By default, the POOL is auto selected. Verify that the chosen **POOL** is the ''UCS\_Application\_NVMe\_Pool'' for provisioning VMFS datastores.

- g. Click the plus sign (+) to verify the volume settings.
- h. Click Next.



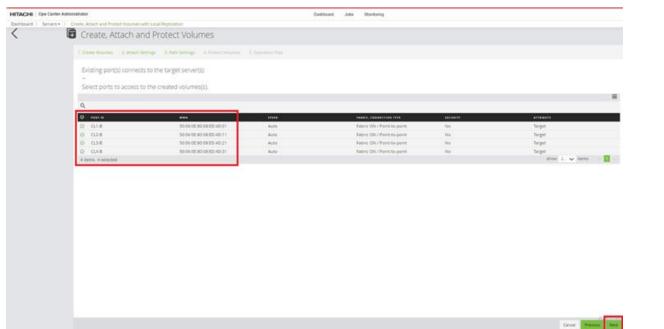
- Step 5. For the HOST MODE select VMWARE EX.
- Step 6. Validate the Volume values and click Next.



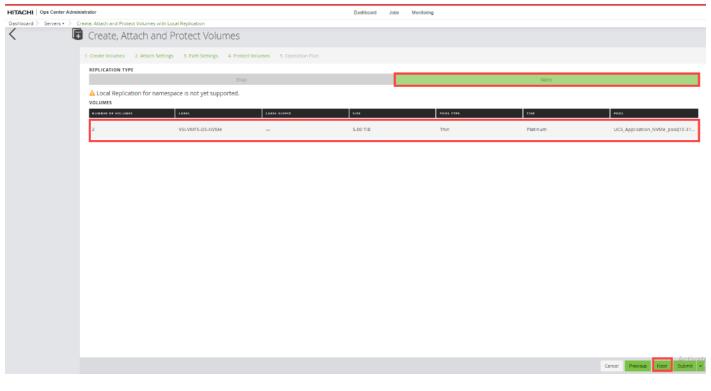
© 2024 Cisco and/or its affiliates. All rights reserved.

Page 188 of 367

Step 7. Under Path Settings, select the VSP ports that are in NVMe mode, and click Next.



Step 8. Select None for Replication Type and click Next.



Step 9. Validate Selected Servers, Volume Specification, and Create Paths. Click Submit.

	nter Administrator				Dashboard	Jobs Monitor	ang .		
and 7 server	rs • > Create, Attach and Protect								
	🛱 Create, Atta	ach and Protec	t volumes						
	1. Create Volumes	2. Attach Settings 3. Pat	h Settings 4. Protect Volu	mes 5. Operation	Plan				
						-			
	Selected Servers								
	110101-0			SERVER IP ADDRESS	#8010C0L		45 TVP4	VOLUME COUNT	REPLICATION TOPE
	2		We_ESU2	-	FC-Wittle FC-Wittle		VMMARE EX VMMARE EX	0	-
	10		Wite_ESI3	-	FC-NMMe		VM/MARE EX	0	-
	11		WMe_ES04	-	FC-W/title		VMMARE EX.	0	-
	Create Volumes Volume Location								
	VACATION			WALOU					
	Storage System			AA22-5600 (60)	1420				
	Virtual Storage Mac	chine		-					
	Volume Specificatio	on							
		¥01.041 m	VOLUME LABOL	CAPACITY	VIETURA IBREAKS	P005, 1171	POOL THER		INTER POLICY CAPACITY LANSING
	Auto	18 (00:00:12) 19 (00:00:13)	VSI-VMPS-DS-NVMe VSI-VMPS-DS-NVMe	5.00 T/B 5.00 T/B	Auto Auto	Thin	Platinum	UCS_Application_NVM	
		19 (PROME 12)	421-440-2-02-046804	5100110	AUC0	inn	Pathum	ors_Approximity -	Desuprication and Lo
	Attach Settings			W81.00					
	Host Mode			VI/VIARE EX					
	Host Mode Options	5							
	Mandate Using Dis	played Volume IDs		No					
	Create Paths								
	VOLUME INCOMES	VOLUME ID	WOLDWE LANDS	GARACITY	WHITERS, ID-MARKED	P005. 1976	Poor Tata	Polis NAME DESIGN	PELICY CAPACITY SAMINS
	Auto	18 (00:00:12)	VSI-VMIS-DS-NVMe	Carecory 5.00 T/8	WIRTERS, HOWANNESS Auto	Thin	Patinum	UCS_Application_NVM	PENDY CAPACITY LAYING Descriptication and Co
	Auto Auto			5.00 T/8 5.00 T/8	Auto Auto				Patiety Extension and Co Deduplication and Co
	Auto Auto Attach Settings	18 (00:00:12)	VSI-VMIS-DS-NVMe			Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings	18 (00:00:12)	VSI-VMIS-DS-NVMe			Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings	18 (00:00:12) 19 (00:00:13)	VSI-VMIS-DS-NVMe	5.00 718		Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings Factoriss Host Mode	18 (00:00:12) 19 (00:00:13)	VSI-VMIS-DS-NVMe	5.00 718		Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings Rest Mode Hest Mode Options Mandaru Using Disp Create Paths	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMIS-DS-NVMe	5.00 718		Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings Reserve Heat Mode Heat Mode Options Manders Using Disp Create Path S Namespace Path Co	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMI5-DS-IVM/e VSI-VMI5-DS-IVM/e	5.00 718		Thin Thin	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settings readwrea Heat Mode Heat Mode Options Mandare Using Disp Create Paths Namespace Path S Namespace Path S	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	123-14875-05-14884 V51-14875-05-14884	5.00 TIB NATURA VINTAINARE EX  No		Thin Thin	Patrum Patrum	UCS_Application_NMM = UCS_Application_NMM =	
	Auto Auto Attach Settings Reserve Heat Mode Heat Mode Options Manders Using Disp Create Path S Namespace Path Co	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMI5-DS-IVM/e VSI-VMI5-DS-IVM/e	5.00 T/8 VI/MARE EX - Nio		Thin Thin Massi Age ngn 2014-08 comu	Patinum	UCS_Application_NVM	
	Auto Auto Attach Settlings Attach Settlings Hest Mode Options Mandairs Using Disp Create Paths Namespace Path Co Prespace Path Namespace Path Co	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	nc2'mm anns Azraniz O2-name Azraniz O2-name	5.00 T/8 ver.es VMMARE DX  No e_ESR1 e_ESR2		7560 7560 7600 7600 7600 7600 7600 7600	Padnum Padnum	UCS_Application_NMM UCS_Application_NMM MAREENACE III Auto	
	Auto Auto Attach Settings Factoriza Heast Mode Heast Mode Options Mandare Using Dap Create Paths Namespace Paths Namespace Paths 18 (po.06.12) 18 (po.06.12) 18 (po.06.12)	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMIS-DS-HAME VSI-VMIS-DS-HAME UCS_NMA UCS_NMA UCS_NMA	5.00 T/8 VAMARE DX  No e_(5301 e_(5302 e_(5304)		Thin Thin ang 2014-08.com v ngn 2014-08.com v ngn 2014-08.com v	Pathum Pathum maar.nmre.essi.1 maar.nmre.essi.2 maar.nmre.essi.3 maar.nmre.essi.4	UCS_Application_MMM UCS_Application_MMM KARS Auts	
	Auto Auto Attach Settings Hest Mole Hest Mole Hest Mole Hest Mole Create Paths Namespece Paths Namespecee 18 (po.oo.12) 18 (po.oo.12) 18 (po.oo.12) 19 (po.oo.13)	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMI5-OS-HAMe VSI-VMI5-OS-HAMe UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 ex.cs - No e.ESS01 e.ESS02 e.ESS03 e.ESS03 e.ESS04 e.ESS01		Thin Thin Market Keye Ngg 2014-08 com v ngg 2014-08 com v ngg 2014-08 com v ngg 2014-08 com v ngg 2014-08 com v	Padnum Padnum maare.nvme.ess6.1 maare.nvme.ess6.2 maare.nvme.ess6.3 maare.nvme.ess6.4 maare.nvme.ess6.4	UCS, Application, MM	
	Auto Auto Auto Attach Settings Attach Settings Manders Wolf Hest Mode Options Manders Using Disp Create Paths Namespace Path Co Verve W 18 (00.00.12) 18 (00.00.12) 18 (00.00.13) 19 (00.00.13)	18 (00:00:12) 19 (00:00:13) slayed Volume IDs	VSI-VMI5-OS-HVMR VSI-VMI5-OS-HVMR UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 •••••• ••••• ••••• ••• ••• •••		Thin Thin 2017 692 ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v	Padnum Padnum Maart nume essi 1 maart nume essi 2 maart nume essi 3 maart nume essi 3 maart nume essi 1 maart nume essi 1 maart nume essi 1 maart nume essi 2	UCS, Application, MM	
	Auto Auto Auto Attach Settlings Mast Mode Options Mandain Using Disp Create Paths Namespace Paths Namespace Path Co Perspace Paths Namespace Path 18 (20:00:12) 19 (20:00:12) 19 (20:00:13) 19 (20:00:13)	18 (00:00:12) 19 (00:00:13) skyed Volume IDs onfiguration	VSI-VMI5-OS-HAMe VSI-VMI5-OS-HAMe UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 •••••• ••••• ••••• ••• ••• •••		Thin Thin 2017 692 ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v	Padnum Padnum maare.nvme.ess6.1 maare.nvme.ess6.2 maare.nvme.ess6.3 maare.nvme.ess6.4 maare.nvme.ess6.4	UCS, Application, MM	
	Auto Auto Auto Attach Settings Autach Settings Autach Settings Mandars Using Dap Create Paths Namespace Path Co Receive Path C	18 (00:00:12) 19 (00:00:13) Hayed Volume IDs onfiguration	VSI-VMI5-OS-HVMR VSI-VMI5-OS-HVMR UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 •••••• ••••• ••••• ••• ••• •••		Thin Thin 2017 692 ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v ngn,2014.08.com v	Padnum Padnum Maart nume essi 1 maart nume essi 2 maart nume essi 3 maart nume essi 3 maart nume essi 1 maart nume essi 1 maart nume essi 1 maart nume essi 2	UCS, Application, MM	
	Auto Auto Auto Attach Settings Fuest Mode Heat Mode Options Mandare Using Dap Create Paths Namespace Paths Nam	18 (00:00:12) 19 (00:00:13) Nayed Volume IDs onfiguration Information ystem Information	VSI-VMIS-DS-HAME VSI-VMIS-DS-HAME USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM	5.00 T/8 VMMARE EX - No 4,05503 4,05505 4,	A./3	Thin Thin Rep 2014-08 com v righ 2014-08 com v	Pathum Pathum Pathum maar.nume.essi.1 maar.nume.essi.2 maar.nume.essi.3 maar.nume.essi.4 maar.nume.essi.4 maar.nume.essi.2 maar.nume.essi.3	UCS, Application, MM	Deduplication and Co
	Auto Auto Auto Attach Settings FuestMode Heat Mode Options Mandare Using Disp Create Paths Network W 18 (pode-12) 18 (pode-12) 18 (pode-12) 18 (pode-12) 19 (pode-13) 19 (pode-13)	18 (p0:00:12) 19 (p0:00:13) skyed Volume KDs onfiguration information stem information	V31-VM15-Q5-HVM/e V51-VM15-Q5-HVM/e V51-VM15-Q5-HVM/e UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 •4.43 • VMMME DX - 160 • (5501 • (5502 • (5503 • (5503) •	A.0	Thin Thin Thin ngn 2014-08 com v ngn 2014-08 com v	Pathum Pathum Pathum maar.nume.essi.1 maar.nume.essi.2 maar.nume.essi.3 maar.nume.essi.4 maar.nume.essi.4 maar.nume.essi.2 maar.nume.essi.3	UCS, Application, MM	
	Auto Auto Auto Auto Attach Settlings Hest Mole Hest Mole Hest Mole Hest Mole Option Create Paths Namespace Paths Namespace Hest Mole Hest Mole Hes	18 (p0:00:12) 19 (p0:00:13) skyed Volume KDs onfiguration information stem information	VSI-VMIS-DS-HAME VSI-VMIS-DS-HAME USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM USS_VMM	5.00 T/8 •4.43 • VMMME DX - 160 • (5501 • (5502 • (5503 • (5503) •	A./3	Thin Thin Thin ngn 2014-08 com v ngn 2014-08 com v	Pathum Pathum Pathum maar.nume.essi.1 maar.nume.essi.2 maar.nume.essi.3 maar.nume.essi.4 maar.nume.essi.4 maar.nume.essi.2 maar.nume.essi.3	UCS, Application, MM	Deduplication and Co
	Auto Auto Auto Attach Settings FuestMode Heat Mode Options Mandare Using Disp Create Paths Network W 18 (pode-12) 18 (pode-12) 18 (pode-12) 18 (pode-12) 19 (pode-13) 19 (pode-13)	18 (p0:00:12) 19 (p0:00:13) skyed Volume KDs onfiguration information stem information	V31-VM15-Q5-HVM/e V51-VM15-Q5-HVM/e V51-VM15-Q5-HVM/e UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM UCS_VMM	5.00 T/8 •4.43 • VMMME DX - 160 • (5501 • (5502 • (5503 • (5503) •	A.0	Thin Thin Thin ngn 2014-08 com v ngn 2014-08 com v	Pathum Pathum Pathum maar.nume.essi.1 maar.nume.essi.2 maar.nume.essi.3 maar.nume.essi.4 maar.nume.essi.4 maar.nume.essi.2 maar.nume.essi.3	UCS, Application, MM	Deduplication and Co

# Management Tools

This chapter contains the following:

- Cisco Intersight Hardware Compatibility List (HCL) Status
- Deploy Cisco Intersight Assist Appliance
- <u>Claim VMware vCenter using Cisco Intersight Assist Appliance</u>
- <u>Claim Cisco Nexus Switches using Cisco Intersight Assist Appliance</u>
- <u>Claim Cisco MDS Switches using Cisco Intersight Assist Appliance</u>
- <u>Claim Hitachi VSP using Cisco Intersight Assist Appliance</u>
- <u>Cisco Nexus Dashboard Fabric Controller</u>

# **Cisco Intersight Hardware Compatibility List (HCL) Status**

Cisco Intersight evaluates the compatibility your UCS system to check if the hardware and software have been tested and validated by Cisco or Cisco partners. Cisco Intersight reports validation issues after checking the compatibility of the server model, processor, firmware, adapters, operating system, and drivers, and displays the compliance status with the Hardware Compatibility List (HCL).

To determine HCL compatibility for VMware ESXi, Cisco Intersight uses Cisco UCS Tools as an installed VIB (vSphere Installation Bundle). The Cisco UCS Tools is part of VMware ESXi Cisco custom ISO, but the version for will be updated later during the vSphere Cluster image update.

For more information about Cisco UCS Tools manual deployment and troubleshooting, go to: <u>https://intersight.com/help/saas/resources/cisco\_ucs\_tools</u>

#### Procedure 1. View Compute Node Hardware Compatibility

**Step 1.** To find detailed information about the hardware compatibility of a compute node, in Cisco Intersight go to **Infrastructure Service > Operate > Servers** in the left menu bar, click a server and select **HCL**.

= dista Intersight 🔉	nfrastructure Service 🗸		Q Search 0 41 Q 10
* Overview © Analyze	+ Servers AA21-6536-1-1 • weatry General Inventory UCS Server Profile <u>HCL</u> Statistics Topolog	κ.	Actions
Operate     O	Details HCL Status CL Status C	HCL Validation	
Integrated Systems . J <sup>6</sup> Configure ^ Profiles Templates Palicies Pasis		Server Software Compliance     OS Vestor VMeasure ESB     OS Vestor     B.0.13	
(New Command Palette * Rodges Interview with Oblek K of ge to Help - Command Palette		Adapter Compliance Wildlife      Q. Adstrow      Model      I: Hardware Status      LOSS W2-HMID-PPS      Wildlife      UCSS W2-HMID-PPS      Wildlife      Voldened      Voldened      Voldened      S2230-4782	2 Nama found 10 - per page 1 st 1

### **Deploy Cisco Intersight Assist Appliance**

Cisco Intersight works with Hitachi VSP and VMware vCenter using third-party device connectors and Cisco Nexus and MDS switches using Cisco device connectors. Since third-party infrastructure and Cisco switches do not contain any usable built-in Intersight device connector, Cisco Intersight Assist virtual appliance enables Cisco Intersight to communicate with these devices.

**Note:** A single Cisco Intersight Assist virtual appliance can support both the Hitachi VSP storage, VMware vCenter, and Cisco Nexus and MDS switches.

To install Cisco Intersight Assist from an Open Virtual Appliance (OVA), download the latest release of the Cisco Intersight Virtual Appliance for vSphere from <a href="https://software.cisco.com/download/home/286319499/type/286323047/release/1.0.9-588?catid=268439477">https://software.cisco.com/download/home/286319499/type/286323047/release/1.0.9-588?catid=268439477</a>

#### Procedure 1. Set up Intersight Assist DNS entries

Setting up Cisco Intersight Virtual Appliance requires an IP address and 2 hostnames for that IP address. The hostnames must be in the following formats:

- **myhost.mydomain.com**: A hostname in this format is used to access the GUI. This must be defined as an A record and PTR record in DNS. The PTR record is required for reverse lookup of the IP address. If an IP address resolves to multiple hostnames, the first one in the list is used.
- **dc-myhost.mydomain.com:** The "dc-" must be prepended to your hostname. This hostname must be defined as the CNAME of myhost.mydomain.com. Hostnames in this format are used internally by the appliance to manage device connections.

In this lab deployment the following example information was used to deploy a Cisco Intersight Assist VM:

- Hostname: as-assist.adaptive-solutions.local
- IP address: 10.1.168.99
- DNS Entries (Windows AD/DNS):
  - A Record: as-assist.adaptive-solutions.local
  - · CNAME: dc-as-assist.adaptive-solutions.local

For more details, go to

https://www.cisco.com/c/en/us/td/docs/unified computing/Intersight/b Cisco Intersight Appliance Getting S tarted Guide/b Cisco Intersight Appliance Install and Upgrade Guide chapter 00.html.

#### Procedure 2. Deploy Cisco Intersight OVA

**Note:** Ensure that the appropriate entries of type A, CNAME, and PTR records exist in the DNS, as explained in the previous section. Log into the vSphere Client and select **Hosts and Clusters.** 

Step 1. From Hosts and Clusters, right-click the cluster and click Deploy OVF Template.

**Step 2.** Select Local file and click **UPLOAD FILES**. Browse to and select the intersight-appliance-installer-vsphere-1.0.9-588.ova or the latest release file and click **Open**. Click **NEXT**.

**Step 3.** Name the Intersight Assist VM and select the location. Click **NEXT**.

Step 4. Select the cluster and click **NEXT**.

Step 5. Review details, click **Ignore**, and click **NEXT**.

**Step 6.** Select a deployment configuration. If only the Intersight Assist functionality is needed, the default configuration of 16 CPU and 32GB of RAM can be used. Click **NEXT**.

**Step 7.** Select the appropriate datastore (for example, VSI-DS-01) for storage and select the **Thin Provision** virtual disk format. Click **NEXT**.

Step 8.Select the appropriate management network (for example, IB-MGMT Network) for the OVA. ClickNEXT.

**Note:** The Cisco Intersight Assist VM must be able to access both the IB-MGMT network if holding the vCenter, OOB for connecting to the switches and the SVP of the 5600, and intersight.com. Select and configure the management network appropriately. If selecting IB-MGMT network on, make sure the routing and firewall is set up correctly to access the Internet and OOB as needed.

Step 9. Fill in all values to customize the template. Click NEXT.

**Step 10.** Review the deployment information and click **FINISH** to deploy the appliance.

**Step 11.** When the OVA deployment is complete, right-click the Intersight Assist VM and click **Edit Set-tings**.

**Step 12.** Expand CPU and verify the socket configuration. For example, in the following deployment, on a 2-socket system, the VM was configured for 16 sockets:

😑 vSphere Client 🛛 Q. Saviti in al and more			C	A ADMINISTRATION CAL -	0.
< @ a	Edit Settings as-	assist	×		
III Summ	Virtual Hardware VM Opti	ons Advanced Parameters	ADD NEW DEVICE -		0
- 🗄 AS-VSI Gu - 🖾 8.0L7 © 101168.111	√сри	<u>s - 0</u>			
(the assist)	Cores per Socket	1 - Societte 16		MHz used	
	CPU Hot Plug	Enable CPU Hot Add		MB unit	
	Reservation	0 V MH2 -			
	Limit	$\underline{\text{Unlimited}} = \underbrace{ \forall \underline{MH}_{\Sigma} = }$		87 GB used	
_	Shares	Normal = v		**	
VN	Hardware virtualization	Expose hardware assisted virtualization to the gue	est OS	s Objects II	
CPV	Performance Counters	Enable virtualized CPU performance counters			
· Incart Tasks Alarms	> Memory	32 <sup>4</sup> <u>GB</u> 4	2	n	
Task have T Target T			CANCEL OK	T Completion Time T Server	
Deputy OVF temporer      AUU  Interf OVF exclusive      More Tables	Consider	610000 10/474/001000	× A4 Im 10/210(11.02	D. 3027/2021,93708. Wateries of	

**Step 13.** Adjust the Cores per Socket so that the number of Sockets matches the server CPU configuration (2 sockets in this deployment):

😑 vSphere Client 🔍 Second in Management				3	anto	American version version of a	0
< @ a	Edit Settings as-	assist			×		
	Virtual Hardware VM Opti	ions Advanced Parameters			î		
vc.adaptive-solutions.local     El AS-VSI     GU				ADD NEW DEVICE -		1	0
- CE 8001	⇒CPU*	<u>16 + (0)</u>				HE 10/27/23, 11.37 AM	
(2) 49-61033	Cores per Socket	B				MHZ uses	
	CPU Hot Plug	Enable CPU Hot Add				MB used	
	Reservation	0					
	Limit	Unlimited	₩ <u>MHz</u> >		L	B7 GB une	
	Shares	Normal ~ 10000	*			n	
VA	Hardware virtualization	Expose hardware assisted	virtualization to the guest OS			I Objects	
cru	Performance Counters	Enable virtualized CPU pe	formance counters				
* Recent Talks Alienta	> Memory	32	Ч <u>св -</u>		÷		
Task Name Tasper				CANCEL ON	c - 1	T Comprehen Time T Server	
Deputy Over Interfaction C. R.D.A.	Companies	7	there by all 2-becarbility	RA HIL 10077230	11. 16.78	0. 0/77/2022.0.27.08. vic.adup IS.A. 85/22/2023.0.32.08. or.adup	

Step 14. Click OK.

**Step 15.** Right-click the Intersight Assist VM and select **Power > Power On**.

**Step 16.** When the VM powers on and the login prompt is visible (use remote console), connect to <u>https://intersight-assist-fqdn</u>.

**Note:** It may take a few minutes for <u>https://intersight-assist-fqdn</u> to respond.

Step 17. Navigate the security prompts and select Intersight Assist. Click Start.

**Note:** If a screen appears prior to the certificate security prompt, the assist may not be ready, and a page refresh may be needed.

	Intersight Appl	iance Ir	staller		
	Intersight Insta	ller Options			
Install Connected Virtual Appliance	Install Private Virtual Appliance	Install Assist	Recover from Backup	Add Node to Appliance	
	Install Assist				
	Cisco Intersight Install Assist ena have a direct path to Intersight a	ind do not have	an embedded Intersig	ht Device	
	Connector. Intersight Assist com the communication bridge to and			s and serves as	
					Start

**Step 18.** Cisco Intersight Assist VM needs to be claimed in Cisco Intersight using the Device ID and Claim Code information visible in the GUI.

	Intersight Appliance Installer	
Connect	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management pl device connector please visit Help Center	atform. For detailed information about configuring the
2 Check Network Requirements	Device Connector	💮 Settings 👘 📿 Refresh
Configure Internal Network     Installation Result	Cum C	
¢		Continue

- **Step 19.** Log into **Cisco Intersight** and connect to the appropriate account.
- **Step 20.** From Cisco Intersight, at the top select **System**, then click **Administration > Targets**.

Step 21. Click Claim a New Target. Select Cisco Intersight Assist and click Start.

Settings     Admin     Admin	t	
Targets Software Repository	Select Target Type	
Sessions Licensing Categ Mark Command Palette Karige Kork for ge Kork Help > Command Palette	Available for Claiming pories	Start

**Step 22.** Copy and paste the Device ID and Claim Code shown in the Intersight Assist web interface to the Cisco Intersight Device Claim window.

**Step 23.** Select the Resource Group and click **Claim**.

=	citce Intersight	ili System ~				Q Search	<b>■</b> ⊘ ⊄	٥	0	۹
0	Settings Admin	+ Targets Claim	n a New Target							
	Targets Software Repository Tech Support Bundles		n Cisco Intersight A your target, provide the Device ID,	ssist Target Claim Code and select the approp	ripte Resource Groups.					Î
	Audit Logs Sessions Licensing		General	Claim Code * 1997A8156785				0		
Navi	Command Palette     gate Intensight with Clrf+K or ge     p > Command Palette			oups if required. However, this sele Organizations with the Resource G		e or more Resource Group type is Alf. The clair	med			
			Name		Usage	1 items found 50 - per page	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0		
		Back	Cancel		AA21				Cia	im

Intersight Assist now appears as a claimed device.

**Step 24.** In the Intersight Assist web interface, verify that Intersight Assist is Connected Successfully, and click **Continue**.

**Step 25.** Step through the additional network requirement checks and internal network configuration before starting the installation update.

	Intersight Appliance Installer
<ul> <li>Connect</li> <li>Check Network Requirements</li> <li>Configure Internal Network</li> <li>Installation Result</li> </ul>	Installation Result         View progress of the Download and Install software packages         Installing Software Version       1.0.9-615         Installation is in progress To download logs, click here         Downloading installation packages 26/125
<	Back
	Help Center Terms Privacy Cookies

**Note:** The Cisco Intersight Assist software will now be downloaded and installed into the Intersight Assist VM. This can take up to an hour to complete and the Assist VM will be rebooted during this process. It may be necessary to refresh the web browser after the Assist VM has rebooted.

When the software download is complete, an Intersight Assist login screen appears.

← → C ▲ Not secure   https://as-assist.adaptive-solutions.local	e 🕈 🛛 😩 :
disco Intersight	English
Intersight Assist	:
Username *	O
Password *	
Sign In	
Help Center Terms Privacy Cookies © 2023 Cisco S	Systems, Inc.

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 198 of 367

# Claim VMware vCenter using Cisco Intersight Assist Appliance

#### **Procedure 1.** Claim the vCenter from Cisco Intersight

Step 1. Log into Cisco Intersight and connect to the account registered to the Intersight Assist.

Step 2. Go to System > Administration > Targets and click Claim a New Target.

Step 3. Under Select Target Type, select VMware vCenter under Hypervisor and click Start.

**Step 4.** In the **VMware vCenter** window, verify the correct Intersight Assist is selected.

**Step 5.** Fill in the vCenter information. Enable Hardware Support Manager (HSM) to be able to upgrade the IMM server firmware from VMware Lifecycle Manager. If Intersight Workflow Optimizer (IWO) will be used, turn on Datastore Browsing Enabled and Guest Metrics Enabled. Click **Claim**.

🚍 號 Intersight 📲 🕫	ntan v	Q Barch	0 4 0 0 4
O Settings	+ Targets Claim a New Target		
Adversion of the second		Port   40   Port   40   Port   40   Port   40   Port   40   Port   41   Port   42   Port   43   Port   44   Port   45   Port   46   Port   47   Port   48   Port   1000000000000000000000000000000000000	
		Exactleng HSM will give exactleted privileges to the vCenter larget to perform Newware operations on UCS servers clasmed in Cesas Intersight.	
	Back Cancel		Claim

**Step 6.** After a few minutes, the VMware vCenter will show Connected in the Targets list and will also appear under **Infrastructure Service > Operate > Virtualization**.

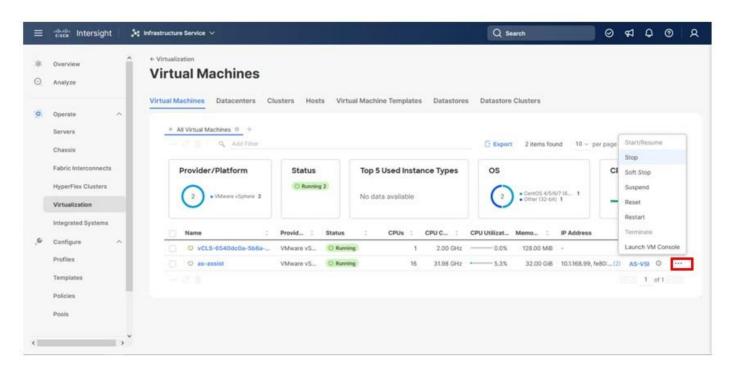
**Step 7.** Detailed information obtained from the vCenter can now be viewed by clicking **Infrastructure Service > Operate > Virtualization** and selecting the Datacenters tab. Other VMware vCenter information can be obtained by navigating through the Virtualization tabs.

■	disco Intersight	📽 Infrastructure Service 🗸			Q Search	0 4 4 0 3
Þ: D	Overview Analyze	Virtualization     Datacenters	Olusters Hasts Method Mar		Dubates Olympic	
j)	Operate ^ Servers Chassis	Virtual Machines Datacenters  All Datacenters  +  All Datacenters  +  All Add Filter	Clusters Hosts Virtual Mac	hine Templates Datastores	G Export 1 items found 10 ~ p	ber page 또 < _1 of 1
	Fabric Interconnects HyperFlex Clusters	Name : Da	2 Networks 2	Clusters C Hosts	Virtual Mac         Hypervisor Mar           1         2         10.1.168.100	na Virtual Mac 2 β 0 ···· Κ ζ 1 of 1 2 Σ
	Virtualization Integrated Systems Configure					
	Profiles Templates					
	Policies Pools					
	>					

#### Procedure 2. Interact with Virtual Machines

VMware vCenter integration with Cisco Intersight allows you to directly interact with the virtual machines (VMs) from the Cisco Intersight dashboard. In addition to obtaining in-depth information about a VM, including the operating system, CPU, memory, host name, and IP addresses assigned to the virtual machines, you can use Cisco Intersight to perform the following actions on the virtual machines:

- Start/Resume
- Stop
- Soft Stop
- Suspend
- Reset
- Launch VM Console
- Step 1. Log into Cisco Intersight.
- Step 2. Go to Infrastructure Service > Operate > Virtualization.
- Step 3. Click the Virtual Machines tab.
- **Step 4.** Click "..." to the right of a VM and interact with various VM options.



Step 5.

To gather more information about a VM, click a VM name.

≡	cisco Intersight 💦 👫 Inf	rastructure Service 🗸	Q Search	ତ <b>ସ</b> ଦ ଡ ର
:@: ©	Overview Analyze	/irtualization > Virtual Machines <b>AS-ASSIST</b> General Virtual Disks Networkir	g Snapshots	Actions
0	Operate ^ Servers Chassis	Details	Summary	Events
	Fabric Interconnects HyperFlex Clusters	Status Constant of	Utilization	Alarms No Alarms
,o	Virtualization	Provider/Platform VMware vSphere	CPU Utilization Memory Utilization Networking Stat 32 • Used 1.70 GHz GHz • Free 30.28 GHz 32 0 GB • Free 28.80 GiB	+ Requests         No Requests           + Advisories         No Advisories
,0	Configure ^ Profiles Templates	IP Address 10.1.168.99 fe80::250:56ff:fe8c:d29c Hostname	Compute	
	Policies	as-assist.adaptive-solutions.local Datacenter AS-VSI	CPUs         CPU Cores         Sockets         Core Per So           16         16         2         8	
<	>	Cluster		v

### Claim Cisco Nexus Switches using Cisco Intersight Assist Appliance

#### Procedure 1. Claim Cisco Nexus Switches (Optional)

Cisco Intersight can give direct visibility to Nexus switches independent of Cisco Nexus Dashboard Fabric Controller.

```
© 2024 Cisco and/or its affiliates. All rights reserved.
```

Step 1. Log into Cisco Intersight.

Step 2. Go to System > Administration > Targets.

Step 3. Click Claim a New Target. In the Select Target Type window, select Cisco Nexus Switch under Network and click Start.

**Step 4.** In the Claim Cisco Nexus Switch Target window, verify the correct Intersight Assist is selected.

**Step 5.** Fill in the Cisco Nexus Switch information and click **Claim**.

=	cisco Intersight	a Bystem ∽	Q. Search	0	a o	0	۹
0	Settings Admin ^	+ Targets Claim a New Target					
	Targets Software Repository Tech Support Bundles Audit Logs Sessions Licensing	Claim Cisco Nexus Switch Target         To claim any on-premises target an intersight Assist Appliance is required. Deploy and claim an Assis Appliance if needed before claiming the target         Intersight Assist *         as assist adaptive-solutions local         Intersight Assist *         Intersight Assist *         as assist adaptive-solutions local         Intersight Assist *         Intersight Assist * <t< td=""><td>irt</td><td></td><td></td><td></td><td>î</td></t<>	irt				î
Nov	Command Palette		esseend *			Cisim	ř

**Step 6.** Repeat **Step 1** through **Step 5** to add the second Cisco Nexus Switch.

**Step 7.** After a few minutes, the two switches will appear under Infrastructure Service > Operate > Net-working > Ethernet Switches.

Overview	Networking						
Analyze	Ethernet Switches SAN Switches						
Operate ^ Servers	All Ethernet Switch ◎ +     O Q Add Filter     C Export	t 2 items fo	bund 10	~ per pag	je 15 🤇	1_of1[	
Fabric Interconnects	Health Connection Firmware Versions Models	ch-cy 2	() Unk	nown 1	tus		32
HyperFlex Clusters		00-07 2	0 Not	Covered 5			
Virtualization	Name : Health : Contract Status Manageme : Model : Expansion .	Total	Ports Used	Avail	Firmware	v :	ş
Integrated Systems	AA21-93600-1 O Healthy O Not Covered 192.168.168.13 N9K-C93600CD	0 36	36	0	10.2(5)		
Configure ^	AA21-93600-2 Ø Healthy Ø Not Covered 192.168.168.14 N9K-C93600CD	0 36	36	0	10.2(5)		
Profiles						1 of 1	
Templates							
	Analyze   Operate  Servers   Chassis Fabric Interconnects  Networking  HyperFlex Clusters  Virtualization  Integrated Systems  Configure	Analyze   Operate   Servers   Chassis   Fabric Interconnects   Networking   HyperFlex Clusters   Virtualization   Integrated Systems   Configure	Analyze   Operate   Servers   Chassis   Fabric Interconnects   Networking   HyperFlex Clusters   Virtualization   Integrated Systems   Configure	Analyze   Operate   Servers   Chassis   Fabric Interconnects   Networking   HyperFiex Clusters   Virtualization   Integrated Systems   Configure	Analyze   Operate   Servers   Chassis   Fabric Interconnects   Networking   HyperFiex Clusters   Virtualization   Integrated Systems   Configure     Mame i Health i Contract Status   Manageme i Model i Expansion i Ports   Manageme i Model i Expansion i Ports   Manageme i Model i Expansion i Ports   Ad21-93600-1 @ Healthy   Not Covered 192.168.168.13 N9K-C93600CD 0 36 36 0	Analyze     Coperate     Servers   Chassis   Fabric Interconnects   Networking   HyperFiex Clusters   Virtualization   Integrated Systems   Configure     Name   Health   Contract Status   Manageme   Model   2   • Health   • Contract Status   (2)   • Health   • Contract Status   (2)   • Health   • Contract Status   • Model   • Health   • Contract Status   • Mane   • Health   • Ad21-93600-1   • Health   • Nat Covered   • Health   • Name   • Health   • Not Covered   • Ports   • Not Covered   • Ports   • Health   • Not Covered   • Ports   • Not Covered   • Ports   • Not Covered   • Ports   • Health   • Ports   •	Analyze   Operate   Servers   Chassis   Fabric Interconnects   Networking   HyperFixe Clusters   Virtualization   Integrated Systems   Configure

**Step 8.** Click one of the switch names to get detailed General and Inventory information on the switch.

### **Claim Cisco MDS Switches using Cisco Intersight Assist Appliance**

#### Procedure 1. Claim Cisco MDS Switches (Optional)

Cisco Intersight can also give direct visibility to the MDS switches independent of Cisco Nexus Dashboard Fabric Controller. At the time of the writing of this document, adding the MDS as targets was still in Tech Preview, so care should be used in relying on received data for this feature in a production setting. To add the MDS switches, follow this procedure:

Step 1. Log in to Cisco Intersight.

Step 2. Go to System > Administration > Targets.

**Step 3.** Click **Claim a New Target**. In the **Select Target Type** window, select Cisco MDS Switch under Network and click **Start**.

**Step 4.** In the **Claim Cisco MDS Switch Target** window, verify the correct Intersight Assist is selected.

**Step 5.** Fill in the Cisco MDS Switch information, including use of Port 8443 and click **Claim**.

**Note:** You can use the admin user login account on the switch.

0	Settings Admin ^	+ Targets Claim a New	Target			
	Targets Software Repository Tech Support Bundles Audit Logs Sessions		DS Switch Target target an Intersight Assist Appliance is require a clasming the target Intersight Assist * as-assist adaptive-solutions.local	d. Deploy and claim an Assist		A
	Licensing		Hostname/IP Address * 192.168.168.15	Port 0 8443	0 e 1 - 10115	
Nov	Command Palette     Split intersight with Ctrik K or go     lip > Command Palette		Username * admin	Password *	- 0	
			Certificate  © Select Certificate			
		Back Cancel				Claim

Step 6. Repeat Step 1 through Step 5 to add the second Cisco MDS Switch.

**Step 7.** After a few minutes, the two switches will appear under Infrastructure Service > Operate > Net-working > SAN Switches.

c	Overview	Networking				
e.	Analyze	Ethernet Switches SAN Switches				
i	Operate ^ Servers	SAN switches inventory support features are currently in Tech Previe environment.	w and are not meant for use in a production Send Us Feedback	e.		
	Chassis Fabric Interconnects	* All SAN Switches  + Q, Add Filter	G Export 2 iter	ms found 10 v p	er page 🔣 🔇 1	of 1 🕞 🗵
	Networking					35
	HyperFlex Clusters Virtualization Integrated Systems	Connection Firmware Versions Me	2 • DS-C0124V-K9 2			
	Configure ^	Name : Contract Status Management	P : Model : Expansion Mo : Tota	Ports Used Avail.	Firmware Vers	: 9
		Name         Contract Status         Management I           AA21-9124V-1         © Unknown         192.168.168.15	P         Model         Expansion Mo         Total           DS-C9124V-K9         0         24		Firmware Vers 9.3(2)	: Ø
	Configure ^		Tota	Used Avail.		
	Configure ^	AA21-9124V-1 OUnknown 192.168.168.15	DS-C9124V-K9 0 24	I <mark>Used Avail.</mark> 8 16	9.3(2)	•••

**Step 8.** Click one of the switch names to get detailed General and Inventory information on the switch.

# Claim Hitachi VSP with Cisco Intersight Appliance

Before onboarding the Hitachi VSP to Cisco Intersight, the prerequisites outlined in the following document need to be completed. Refer to the <u>Integrating Hitachi Virtual Storage Platform with Cisco Intersight Quick Start Guide</u>.

Begin State

- Hitachi virtual storage platform should be online and operational, but not claimed by Cisco Intersight.
- Intersight assist VM should be deployed using the Cisco provided OVA template.
- Hitachi Ops Center API Configuration Manager Rest should also be deployed as a VM or server, from a template or with manual installation, so that we can communicate between Cisco Intersight and Hitachi VSP storage. Hitachi Ops Center API Configuration Manager provides the Web API for getting information or changing the configuration of storage systems. Hitachi Ops Center API Configuration Manager is required to use Hitachi Virtual Storage Platform storage systems with Cisco Intersight.
- Communication between Hitachi Ops Center API Configuration Manager and the REST API client.

End State

- Cisco Intersight is communicating with Intersight assist.
- Hitachi VSP is onboarded via Hitachi Ops Center API configuration manager Rest.
- Hitachi VSP is claimed as a device with Cisco Intersight.

#### Procedure 1. Register Hitachi Virtual Storage Platform to Ops Center Configuration Manager Server

**Step 1.** Open your respective API client.

**Step 2.** Enter the base URL for the deployed Hitachi Ops Center API Configuration Manager IP address. For example, https://[Ops\_Center\_IP]:23450/ConfigurationManager/v1/objects/storages.

- Step 3. Click the Authorization tab.
  - a. Select **Basic** from the **Select authorization** drop-down list.
  - b. Enter the Username and Password for the VSP storage system.

0	History :	API Calent	Environment: Default 🗸
8	TODAY	ager/v1/objects/storages × +	
۲	http://10.1.168.105:23450/ 18 minutes ago at 01:23:0	POST v http://10.1.168.105/23450/ConfigurationManageriV1/objects/storages	<ul> <li>&gt; ±</li> </ul>
0	TODAY	HEADERS BODY AUTHORIZATION C ACTIONS C CONFIG CODE SNIPPETS	
٩	CET http://10.1.168.105:23450/ 3 days ago at 05:16:49 PM	Select aufterstation Basic V User name maintenance	
		Basic authorization allows to send a username and a password in a request header.	
		: Response ×	CLEAR
		(200) OK	Time: 35 ms Size: 18 Bytes
		1 =] ( 2 =] "dese": [] 3 =] "	

**Step 4.** Click the **Body** tab. Enter the VSP storage SVP IP, Serial Number, and Model as indicated in the following examples in JSON format.

Note: If a midrange VSP storage, it will be CTL1 and CTL2 IP instead of SVP IP.

The following example uses a VSP 5600:

```
{
    "svpIp": "192.168.1.10",
    "serialNumber": 60749,
    "model": "VSP 5600"
}
```

The following example uses a VSP E1090:

```
{ "ctll1p": "192.168.1.10",
"ctl21p": "192.168.1.11",
"model": "VSP E1090",
"serialNumber": 451139 }
```

**Step 5.** Under the HEADERS tab verify the following:

a. Accept: application/json

•	History :	API Client	Environment: Default 🗸
8	TODAY ^	ager/v1/objects/storages × +	
	GET http://10.1.168.105:23450/ 19 minutes ago at 01:23:0	POST - http://10.1.168.105.23450/Configuration/Manager/v1/objects/storages	/ > :
	TODAY	HEADERS BODY AUTHORIZATION () ACTIONS () CONFIG CODE SNIPPETS	
٩	GET http://10.1.168.105:23450/ 3 days ago at 05:16:49 PM	COPY Text editor	
Ŭ		Name Value	
		Accept application/ison	Θ
		Response ×	CLEAR
		(200) OK	Time: 35 ms Size: 18 Bytes
		1 =:( 2 =: "data": () 3 = )	
		3 )	

Step 6.

Verify that the REST call is set to **POST**. Click **Submit**.

0	History :	API Client	Environment: Default 🗸
8	TODAY	ager/v1/objects/storages × +	
۲	CET http://10.1.168.105:23450/ 18 minutes ago at 01:23:0	POST v http://10.1.168.105.23450i/ConfigurationManageriv1/objects/storages	<b>Z</b> > 1
0	TODAY	HEADERS BODY AUTHORIZATION O ACTIONS O CONFIG CODE SNIPPETS	
٩	et http://10.1.168.105.23450/ 3 days ago at 05:16:49 PM	Raw input     V       1     (************************************	Mime type V
		Response x	CLEAR
		(200) OK	Time: 35 ms Size: 18 Bytes
		1	

**Step 7.** After successful registration, a response header is displayed as **200 OK**.

**Step 8.** To confirm onboarding, the API parameter can be updated to the **GET** method to retrieve storage system information and can be verified with **200 OK** status.

Histo	ry :	API Client	Environment: Default 🐱
TODAY	^	ager/v1/objects/storages×ager/v1/objects/storages× +	
Post	http://10.1.168.105:23450/ 2 minutes ago at 01:58:04	GET v http://10.1.168.105.23450/ConfigurationManager/v1/objects/storages	/ > =
GET	http://10.1.168.105:23450/ 36 minutes ago at 01:23:0	HEADERS AUTHORIZATION () ACTIONS () CONFIG CODE SNIPPETS	
TODAY	^	COPY Det editor	
GET	http://10.1.168.105:23450/ 3 days ago at 05:16:49 PM	Add a header to the HTTP request.	
		: Response ×	CLEAR
			CLEAR 25 ms Size: 149 Bytes :

#### **Procedure 2.** Onboarding VSP storage to Cisco Intersight via Hitachi Ops Center API Configuration Manager

Step 1. Log in to Cisco Intersight.

	Cisco ID If you do not have a Cisco ID, create one have Son hi with Cisca ID. Don't have an intensight Acco	Single Sign-On (SSO) () Email Fign in with 180
1000	Learn more about Oisco Int	

Step 2. From the Navigation tree, select the **Targets** and click to **Claim a new Target**.

Settings	Targets					Claim a New Ter
Admin O						
Targeta	- All Targets - +					
Software Repository	Add Filter				Export Bitems found	10 - per page 🖂 👔 of t 🖂
Tech Support Bundles	Connection Top Tan	rgets by Types Vendor				11
Audit Logs	Connected 8	Cases MDE Switch 2				
Sessions		Choco MOD Darbith 2     Opco Namo Statish 2     O				
Licensing		+ CD1 # 2				
Licenseig	Name	Status	Type	Claimed Time	Claimed By	
		Connected	Class Nexus Cashooard	Oct 16, 2023 1:54 PM	regease con	
Command Palette	0 19235836816	(i) Connected	Clacy MDS Switch	Oct 27, 2023 10:43 AM	rc/@clace.com	
ata mensight with Delek or ge- ta > Command Palella	192.168.166.15	(3 Connected	Cieco MDS Switch	Oct 27, 2023 10:43 AM	rei@cieco.com	
	192.568.368.14	(i) Convented	Clace Nexus Switch	Oct 27, 2023 10:29 AM	reigeate con	
	102.168.168.13	(C Convented)	Cloco Nexus Switch	Oct 27, 2023 10:15 AM	rcigicisco.com	
	vs.adaptive-solutions.local	(ii) Convected	VMware vCenter	Oct 27, 2023 9:46 AM	rei@cisco.com	
	as-assist_adaptive-solutions.loca	Corrected	Intersight Assist	Oct 27, 2023 6:56 AM	rogosos.com	
	AA21-0530	(2) Connection	Intensight Managed Domain	Sep 29, 2023 12:33 PM	rcigicado.com	
						1 611

Step 3.Select categories list, select Storage as Target Type, and select Hitachi Virtual Storage Plat-<br/>form.

Step 4. Click Start.

≡ slude intersight = system ∨		Q Search	0 4 0 0 A
Settings Admin Targets Claim a New Target Claim a New Target	Select Target Type		
Audit Logis Sessions Licensing	Piters     C. Sauch       Image: Available for Clammag     Storage       Carlogaries     Image: Compare / Fabric       All     Image: Compare / Fabric       Hyperconverged     Myperconverged       Myperconverged     Myperconverged       Mathewise     Compare / Fabric       Hyperconverged     Storage       Storage     Storage	al Storage	
Cancel			Start

#### Step 5.

To claim Hitachi Virtual Storage Platform Target, Enter the following:

- a. From the Intersight Assist list, select the deployed Intersight Assist Virtual Appliance hostname/IP address.
- b. In the Port field, enter 23451.
- c. In the Username field enter the VSP storage system username.

- d. In the Password field enter the VSP storage system password.
- e. Enable the Secure option.
- f. In the Hitachi Ops Center API Configuration Manager Address field, enter the **API Configuration Manager IP address** that has the registered **VSP storage system.**

Step 6. Click Claim.

$\equiv$ $\frac{1}{6}$ $\frac{1}{6}$ intersight $=$		Q Search	ବ୍ୟ	<b>Q</b>	ତ   ନ
	• Targets Claim a New Target				
Targets Software Repository Tech Support Bundles	Claim Hitachi Virtual Storage Platform Target To came any on-premises target an intersignt Assist Appliance is required. Deploy and came an Assist Appliance if needed before claiming the target				
Audit Logs Sessions	Protessigit Assist * as-esset adaptive solutions.local v o 192.168.168.20 0				
Licensing	Port 23451 0 0 0 000005				
Navigate Intensight with CMH-K or go to Help > Command Palette	Usenano* Instremance 0 Fassand* 0 0				
	Certificate O Select Cortificate				
	Nitachi Ops Center API Configuration Manager Address * 10.1.168.106 0				
				_	_
	Back Cancel			L	Claim

**Step 7.** Under **Systems** click **Targets** and **All Targets** to view newly connected Hitachi VSP storage with device type as **Hitachi Virtual Storage Platform.** 

≡ diste Intersight <b>#8 System</b> ∨	Q Search	0 4 0 0 A
Settings + Targets     192.168.168.20		
Targets Details	Events	
Tech Support Bundles	- Reque	sts 1 🐼
Sessions 192368.168.20	© Claim T Sources 1923-19	arget 6 1368.20 a minute ago
Licensing Type Hitachi Virtual Storage Platform		
Vendor Vendor Hetachi Navigate Intercipti with Christ or go		
to Help > Command Pulette External IP Address 64300.255190		
IP Address 192368.148.20		
Target ID 90000000749		
Certificate -		
Last Update 2 minutes ago		
Claimed Time 2 minutes ago		
Claireol By arvin jami@hitachivantara.com		
Connector Version 1.0.11-1604		
Product ID StorageArray		

Step 8.The properties of added VSP storage systems can be found under Infrastructure Service >Storage.

≡ dida Intersight	32 Infrastructure Service ~				Q Search	0 4 <b>0</b> 9
<ul> <li>Overstew</li> <li>Analyze</li> </ul>	+ Sterage AA22-5600 General Inventory					
9 Operate Servers Chassis Palari; Interconnects Metworking HyperFlee Chusters Storage	Details Name A22-5600 Vendor Hitach Maddil Varbisco	Properties Capacity + year 20.6318 (serge, 412616			etso Tie	20.63 Provident Data Robuston Till 10.13 Till 16
Versalization Integrated Systems JG Coofigue Profiles Templates Publices Publices	Yerson 80-01-21(00 80/929 93/929 93/929 C1319 − C1329 − - -	Array Summary Here Onies 40 Disponse 0	Varines 62 Bendia Hanadan Pans 0	Pous 2	Immu heriy Goups 6 Externe felt Graps 0	Enternal Floring Chapter O topoune Migration Rens O
New Command Palente Newspile time upp 4 of the Data A or pr to Help + Command Halette	CTLU Microsobe Vireiden - CTL2 Microsobe Vienden - Target Connolen - Granications default					

### **Cisco Nexus Dashboard Fabric Controller**

Cisco Nexus Dashboard Fabric Controller, (NDFC formerly DCNM-SAN) can be used to monitor, configure, and analyze Cisco Fibre Channel fabrics using NDFC SAN. Cisco NDFC is deployed as an application from within the Cisco Nexus Dashboard that is installed as a virtual appliance from an OVA and is managed through a web browser. Nexus Dashboard Insights can be added to provide extended visibility into your fabric by allowing you to monitor, analyze, identify, and troubleshoot performance issues.

The installation and configuration of Nexus Dashboard can be accomplished by following the instructions within this deployment guide:

https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/deployment/cisco-nexus-dashboard-deployment-guide-23 1.html

A single node is sufficient for NDFC, but a multi-node placement of Nexus Dashboard will be required to use Nexus Dashboard Insights. With the Nexus Dashboard installed, fabric connectivity for managed switches will need to be established as covered in this guide:

https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide-23/cisco-nexus-dashboard-user-guide-231.ht ml

#### **Prerequisites**

The following prerequisites need to be configured:

- Licensing. Cisco NDFC includes a 60-day server-based trial license that can be used to monitor and configure Cisco MDS Fibre Channel switches and monitor Cisco Nexus switches. NDFC and Nexus Dashboard Insights can be enabled with any tier level of switch based licensing of DCN as covered in this document: <u>https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/nexus-dashboard/guide-c07-74</u> <u>4361.html?ccid=cc001903&oid=giddnc023703</u>
- © 2024 Cisco and/or its affiliates. All rights reserved.

- 2. If SAN Analytics will be implemented, the deployment of the Nexus Dashboard should select the Data option as opposed the App option during the OVF deployment.
- 3. Passwords. Cisco NDFC passwords should adhere to the following password requirements:
  - It must be at least eight characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the NDFC password for all platforms: <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , .\*
- 4. NDFC SNMPv3 user on switches. Each switch (both Cisco MDS and Nexus) needs an SNMPv3 user added for NDFC to use to query and configure the switch. On each switch, enter the following command in configure terminal mode (in the example, the userid is snmpadmin):

snmp-server user snmpadmin network-admin auth sha <password> priv aes-128 <privacy-password>

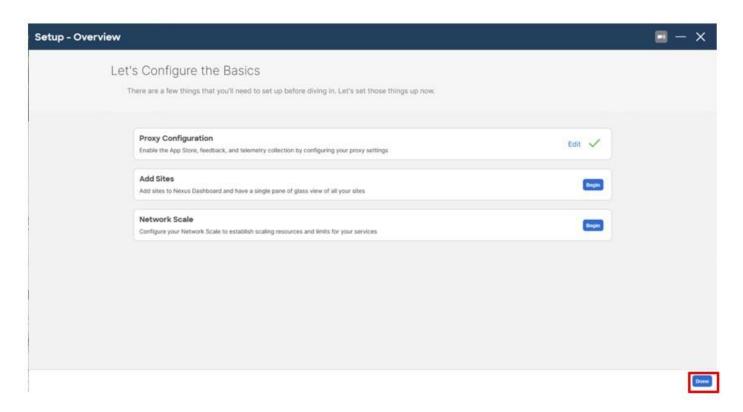
5. On Cisco MDS switches, type show run. If snmpadmin passphrase lifetime 0 is present, enter username snmpadmin passphrase lifetime 99999 warntime 14 gracetime 3.

**Note:** Nexus Dashboard is not supported within vSphere 8 at this time and was deployed for the validation as part of the independent supporting infrastructure hosted within a vSphere 7.0U3 cluster.

#### **Procedure 1.** Install Nexus Dashboard Fabric Controller

With the Nexus Dashboard installed, the initial login screen will present the option to Configure the Basics, this can be skipped for now.

Step 1. Click Done.



**Step 2.** Service IPs will need to be added to the Nexus Dashboard before an App Service can be installed, click through the starting screen, and click **Go To Dashboard**.

Setup	🖬 — 🗙
Setup donel Initial Nexus Dashboard has been configured.	
What's Next?         Add an App Service.         Transform your data center by adding app services.         Let's Get Started	
You might also want to	Go To Dashboard

**Step 3.** From the drop-down list to the left of the Nexus Dashboard, choose **Admin Console**.

cisco Nexus Dashboard	One View -	Feedback 👤 🧿
One View	One View	
	Admin Console Nexus Dathboard Cluster Settings and other system-related information	
	No	Sites Found
		ave any connected sites



cisco Nexus Dashboard	lio Admin Console -			Feedback 👤 🔮
E Overview	0 AS-ND			000
<ul> <li>Sites</li> <li>Services</li> </ul>	System Overview			Refresh
System Resources  Operations	Overview			
h. Infrastructure	Infrastructure	Cluster Health	Intersight Status	
i. Administrative	Cluster Configuration	() ON	There is no intersight set up.	
	Hesource Utilization to Intersight App Infra Services		Setup Intensight	
	Sites and Services	Services by Status	App Infra Services by Status	
	There are no connected sites.	Heading 0     Heading 0     Heading 0     Critical 0	Heading 11 Total	
https://10.1.168.80%/ckusterConfiguration	Inventory Node Role Nodes	Pods Deployments	StatefulSets DaemonSets	

**Step 5.** Scroll down in the Cluster Configuration to the External Service Pools section and click the edit icon.

Overview	C AS-ND		000
Sites Services System Resources Operations	HTTP         http://192.168.168.2518060         -           HTTPS         http://192.166.168.2518060         -           Ignore Hosts         -         -	DNS Domains Providers IP Addresses as-nd.case.local 10.1168.101 Search Domains	/
<ul> <li>Infrastructure</li> <li>Administrative</li> </ul>	Routes // Monagement Network Routes //	Syslog Remote Destinations.	1
	*  External Service Pools Management Service IP Usage Data Service IP Usage Total Total	Network Scale Number of Sites - Number of Switches - Filows per second -	/
	Management Service IP's - Data Service IP's -		

Step 6. Click Add IP Address under the Management Service IP's.

۱۱۱۱۱۱۰۰ Nexus Dashboard دisco		Feedback 👤 📀
Overview	C AS-ND	0 . 0
<ul> <li>Ø. Sites</li> <li>Bervices</li> </ul>	External Service Pools	X nders IP Addresses
11 System Resources	Management Service IP's IP Usage Assignment	0188.101
ii. Infrastructure	Add IP Address      Data Service IP's	/
	IP Usage Assignment O Add IP Address	
	E	
		Cancel Save

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 215 of 367

Step 7.Add IP addresses in the IB-Mgmt network on which the Nexus Dashboard was deployed. ClickSave.

cisco Nexus Dashboard		Feedback 👤 🧕
≣ Overview	AS-ND	000
⊕ Sites	External Service Pools X	/ ^
Services	videra 12 Addresses (168.101	
81 System Resources	Management Service IP's	
Operations	IP Usage Assignment	
5. Infrastructure	10.1.168.93 Not In Use	
a. Administrative	10.1.168.94 Not In Use	
	10.1168.95 Not In Use /	
	10.1.168.96 Not in Use	/
	E Add IP Address	
	Data Service IP's	
	IP Usage Assignment	
	Add IP Address	
	Cancel Save	
	Data Service IPs	

**Step 8.** Repeat these additions for the Data Service IP's associated with the OOB network that the mgmt interfaces of the MDS and potentially the Nexus switches. Click **Save**.

Overview	G AS-ND						0 [] 0
Sites	External Service Pool	ls				×	/
Services	10.1.168.94	Not In Use		1	Ŵ	viders IP Addresses	
System Resources	10.1.168.95	Not In Use		/	ŵ		
Operations	10.1.168.96	Not In Use		/	Ŵ		
Infrastructure	R Add IP Address			2		-	/
	Data Service IP's						
	D IP	Usage	Assignment				
	192.168.168.93	Not In Use		/	1		/
	E 192.168.168.94	Not In Use		1	1		
	192.168.168.95	Not In Use		/	Ť		
	192.168.168.96	Not In Use		/	ŧ	-	
	Add IP Address					-	
					Cancel		
	Data Service IP's					_	

**Note:** The allocation of IPs in our example is four IPs for each service pool but will vary depending on the needs of services being deployed.

**Step 9.** Click the edit icon in the Routes section.

cisco Nexus Dashboard	着 🗴 Admin Console 🐱		Feedback 👤
E Overview	S AS-NO		0 [] 0
<ul> <li>Sites</li> <li>Services</li> </ul>	Name App Subnet AS-ND 172.17.0.1/16	Service Subret 100.80.0.0/16	
System Resources  Operations  Infrastructure	Proxy Configuration Servers Type Server Usern	> NTP 10.1.168.254	~
In Administrative	HTTP         http://192.168.168.251:8080         -           HTTPS         http://192.168.168.251:8080         -           Ignone Hosts         -         -	DNS Domains Providers IP Addresses as-nd.case.local 10.3368.101 Search Domains	/
	Routes Management Network Routes - Data Network Routes	Syslog Remote Destinations	1
	*  External Service Pools  Management Service IP Usage  * Available 4  Table  * Available 4  Seal  * Available 4  ** Available 4	Network Scale Number of Sites - Number of Switches - Flows per second -	/

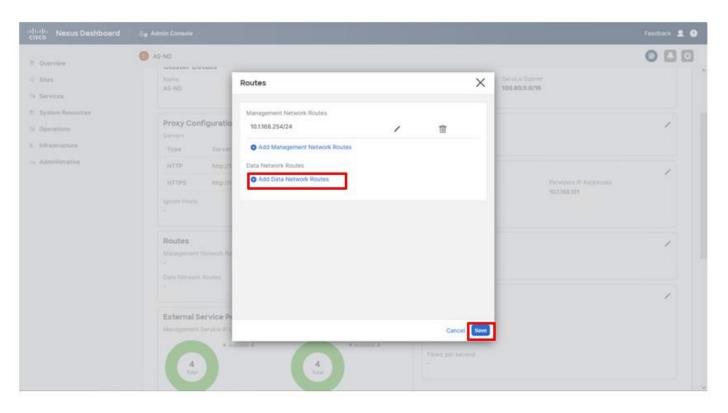
Step 10. Click Add Management Network Routes.

cisco Nexus Dashboard					Feedback 👤 \Theta
E Overview	AS-ND				000
-0 Shee Nr Services	Nums AS-ND	Routes	×	Service Subrest 100.80.0.0(16	
<ul> <li>Bystern Resources</li> <li>Operations</li> <li>Infrastructure</li> </ul>	Proxy Configuration Servers Type Server	Management Network Routes  Add Management Network Routes  Data Network Routes  Add Data Network Routes			1
is Administrative	ATTP http://t HTTP: http://t Sgearn Harts -			Preventers IP Addresses 10.1348.501	1
	Routes Standpartner: National III - Data National Boutes				1
	External Service Per Admensionant Sarvice III	A A A A A A A A A A A A A A A A A A A	Cancel Swe Places per excernt -		

**Step 11.** Repeat the addition for the appropriate Data Network gateway and click **Save**.

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 218 of 367



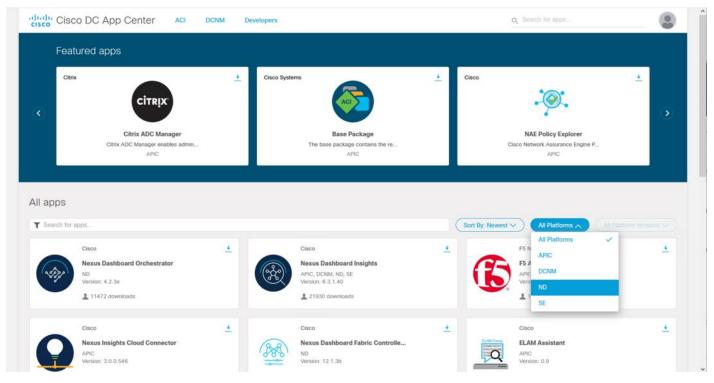
Step 12. Click Services, then click Install Services.

cisco Nexus Dashboard	2 Admin Console -	Feedback 👤 📀
Overview     Sites     Services      System Resources	AS-ND     Service Catalog     Installed Services App Store	💿 👗 🖸 Refresh
<ul> <li>Operations</li> <li>Infrastructure</li> <li>Administrative</li> </ul>	There are no services         Vou have not installed or deployed any servition	ces

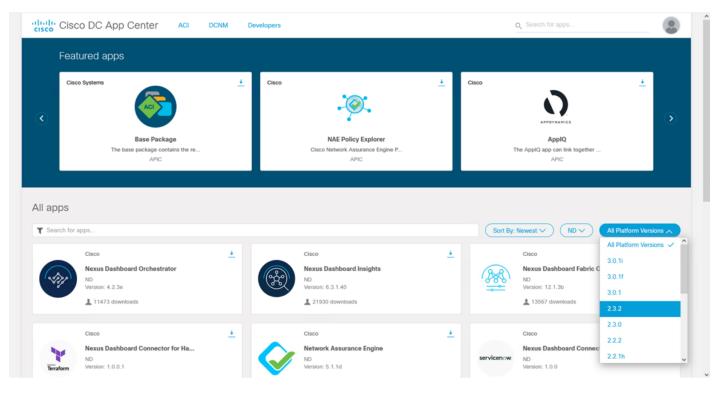
Step 13. Click CISCO DC App Center to access available apps.

cisco Nexus Dashboard	🐌 Admin Console	Feedback 🙎 Θ
T Overview	© x3-H0	000
<ul> <li>Situs</li> <li>Services</li> <li>Tystem Resources</li> </ul>	Installed Services App Store	Refresh
Operations     Monutipathers     Anthirodocative	Upload Service X  Go to the ISCO DC App Center b view and download more apps. For uploading larger apps, we recommend using the remote upload option  Location  URL+	
	s.g. http:///WP gor/l/path/lineares	

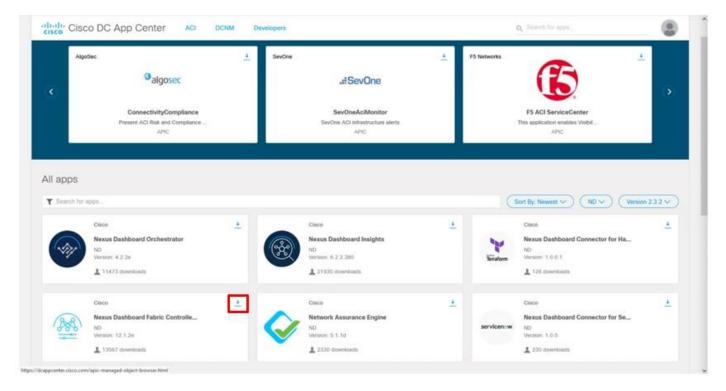
**Step 14.** Within the window that is open for the App Center, choose the **ND** option from the All Platforms drop-down list.



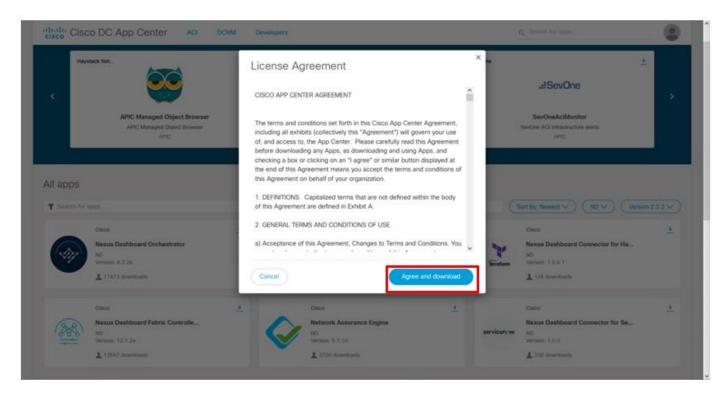
**Step 15.** Choose the **2.3.2** option From the All Platform Versions drop-down list.



**Step 16.** Click the Download icon within the Nexus Dashboard Fabric Controller box.



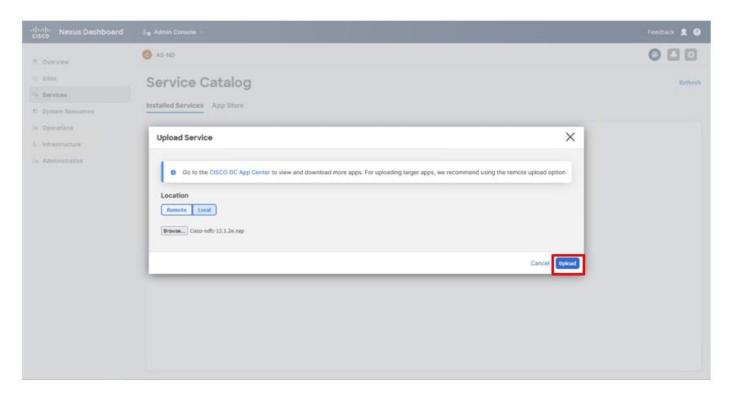
**Step 17.** Log in to id.cisco.com with CCO credentials and click **Agree and Download** within the License Agreement pop-up window.



**Step 18.** Return to the Nexus Dashboard window, click **Local** in the Upload Service dialogue window, and click **Browse...** to select the downloaded .nap application file for NDFC.

cisco Nexus Dashboard		Feedback 🚊 😌
2 Overview	S AS-ND	0 [] []
Sites     Services     System Resources     Operations	Service Catalog	Refresh
h. Infrastructure	Upload Service X	
	Cancel	

Step 19. Click Upload.



**Step 20.** After the upload and installation has completed, click **Enable**.

cisco Nexus Dashboard	Re Admin Console	Feedback 👤 😗
≡ Overview	S AS-ND	000
<ul> <li>Sites</li> <li>Services</li> </ul>	Service Catalog	Refresh
11 System Resources	Installed Services App Store	
Operations     Infrastructure     #     Administrative	Image: Constraint of Market Constraint       ***         Image: Constraint Constraint       ***         I	Actions

## **Procedure 2.** Configure Nexus Dashboard Fabric Controller

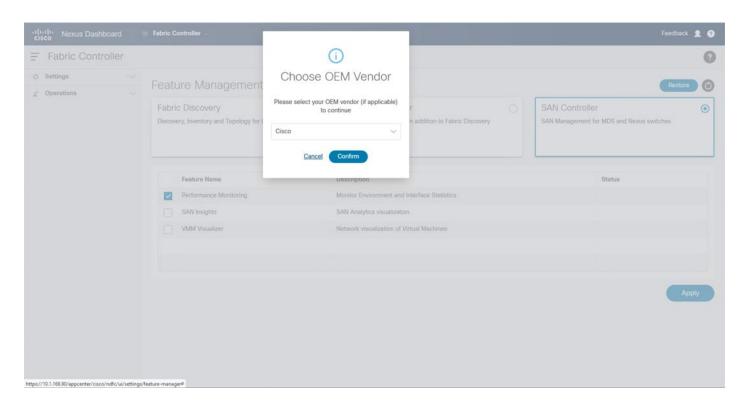
Step 1. Click Open or choose the option Fabric Controller.

cisco Nexus Dashboard	着 Admin Console 🗠	Feedback 👤 📀
■ Overview	One View	0 🖬 🖸
Services     System Resources	Admin Console	Refresh
III Operations III. Infrastructure III. Administrative	Fabric Controller	Actions -

Step 2. Click the SAN Controller option.

cisco	Nexus Dashboard	1	Fabric Controller		Feedback 👤 💿
= Fab	oric Controller				0
O Setting		×.	Feature Management		Restore
<u>⊥</u> ° Opera	rtions	~	Fabric Discovery Discovery, Inventory and Topology for LAN deployments	Fabric Controller Full LAN functionality in addition to Fabric Discovery	SAN Controller SAN Management for MDS and Nexus switches

**Step 3.** Confirm Cisco as the OEM vendor.





cisco Nexus Dashboard	Ţ	Fabric Controller				Feedback 👤 📀
						0
<ul> <li>Settings</li> <li><i>L</i><sup>o</sup> Operations</li> </ul>	3	Feature Management				Restore
		Fabric Discovery Discovery, Inventory and Topology for LAN deployments	0	Fabric Controller Full LAN functionality in addition to Fabric Discovery	0	SAN Controller  SAN Management for MDS and Nexus switches
		Feature Name		Description		Status
		Performance Monitoring		Monitor Environment and Interface Statistics		
		SAN Insights		SAN Analytics visualization		
		VMM Visualizer		Network visualization of Virtual Machines		
						Apply

**Step 5.** The status will display Started when complete and the page will need to be reloaded to continue.

cisco Nexus Dashboard	😵 Fabric Controller 🗸		Feedback 👤 (
	Some features have b	been updated. Reload the page to see latest changes.	
F Fabric Controller			0
🔅 Settings 🗸 🗸	Footure Management		Restore
$_{L^{0}}$ Operations $\sim$	Feature Management		Restore
	Fabric Discovery Discovery, Inventory and Topology for LAN deployments	Fabric Controller	SAN Controller  SAN Management for MDS and Nexus switches  Started
	Feature Name	Description	Status
	Performance Monitoring	Monitor Environment and Interface Statistics	Started
	SAN Insights	SAN Analytics visualization	
	VMM Visualizer	Network visualization of Virtual Machines	Started

Step 6. Expand Virtual Management and click Virtual Infrastructure Manager.

cisco Nexus Dashboard	Fabric Controller			Feedback 🚊 📀
= SAN Controller				00
<ul> <li>R Dashboard</li> <li>≫ Topology</li> <li>≅ SAN ~</li> </ul>	Dashboards Overview Host Storage			۲
Virtual Inhastructure Manager Virtual Inhastructure Manager Settings Virtual Inhastructure Manager Operations Virtual Inhastructure Manager Virtual Inhastr		Event v	Analytics O Alarms O Events-2 db	
https://10.1.188.90/appcanter/clocol/self-Uv/Vetua	Switches Switch Health O Switch (e) Masc (e) Masc (e) Wanning (b) Healthy (e)	Switch Status O Secon	Switch Release Versions	Switch Models



SAN Control	er									00
Dashboard		Vieture	Linfrante	unturn Man						
Topology		virtua	i mirastr	ucture Man	lager					6
SAN	4	Filter by a	attributes							Actions ~
Virtual Management	~	-		122000	agestance.	-		120.200		Add Instance
Virtual Infrastructure Mar	ager	Se Se	BEVEL	Туре	Version	Managed	Status	User	Last Updated Time	Edit Instance
Settings	$\sim$									Delete Instance(s)
Operations	~									Rediscover Instance(s)
							No rows found			

Step 8. From the Add Instance pop-up window, choose vCenter

cisco Nexus Dashboard		Add Instance		Feedback 👤 🕥
F SAN Controller		Add instance	×	00
in Dashbaard Si Tapulagy ⊒ 5AN ∞ Virtual Management	Virtu	Select Type Select an Option VCenter	Cancel (Add	Accordence
Vetual bihastructure Manager				
∑ Operations				
				ap 1 d1 < ( 50 d5 ) >

Step 9.Provide the vCenter IP address or FQDN, and the appropriate Username and Password for access.Click Add.

cisco Nexus Dashboard	😸 Tabric G	Add Instance ×	Feedback 🚊 😡
= SAN Controller		Add Instance ×	00
98 Dashboard	Virtu	Select Type	0
Sc Topology	VIILU	vCenter ~	0
III SAN	- Princip	Virtual Center Server IP Address or Domain*	Actions
as Virtual Management	0	10.1.168.100 Enter a valid IP Address or Domain	Last Updated Time
O Settings		Usemane* administrator@vsphere.local	
		Cencel Add	Page 1 #1 4 4 0.0010 > >

**Step 10.** Select **SAN** and click the **Fabrics** option from the expanded menu.

SAN Controller								00
n Dashboard	Virtual Infrastr	ucture Man	ager					Ø
≣ SAN ^	Filter by attributes							Actions ~
Fabrics Switches	Server	Туре	Version	Managed	Status	User	Last Updated Time	
Links Interfaces End Devices Host Path Redundancy Port Monitoring Zoning Active Zones Storage	<ul> <li>10.1.168.100</li> <li>10.1.168.100</li> <li>10.1.168.100</li> </ul>	vCenter	8.0.1.0	managed	OK	administrator@vsphere.local	Fn, 12 Jan 2024 18:45:07 UTC	
Virtual Management     Virtual Infrastructure Manager								
o Settings 🗸								
£ Operations $\lor$	10 V Rows						Page 1 of 1 《 <	1-1 of 1 > ≫

## Step 11. Click Actions and choose Add Fabric from the drop-down list.

sco Nexus Dashboard		Fabric C	ontroller										Feedback 👤 🕻
SAN Controller													00
Dashboard		-											
Topology		Fabr	ICS										C
SAN	^	Filter	by attributes										Actions ^
Fabrics													Add Fabric
Switches			Fabric Name	Seed Switch	State	SNMP SSH	User/ Community	Auth/ Priva	Licensed	Health	Perform_ Collection	Upd	Edit Fabrics
Links													Delete Fabrics
Interfaces													Rediscover Fabrics
End Devices													Purge Fabrics
Host Path Redundancy													Configure Performance
Port Monitoring													Configure SAN Insights
Zoning													Configure Backup
Active Zones							No rows to	und					
Storage													
Virtual Management	^												
Virtual Infrastructure Manager													
Settings	1												
Operations	~	<											,

**Step 12.** Specify the Fabric Name for the A side Fabric, enter the IP address of the A side MDS, set the Authentication/Privacy to SHA\_AES, provide the snmp user created on the switches, and click **Add**.

Add Fabric				? – ×
	Fabric Name* Fabric -A Fabric Seed Switch Type Cisco Non-Cisco Fabric Seed Switch* 192.168.168.15 Use SNMPy3 / SSH Authentication / Privacy MO5 SHA M05_DES ND5_AES SHA_DES Optional)	Enter a salid IP V4 address or DNS name (e.g. Password	12.3.4 or systems	
	SHA_AES	C	Add	

**Step 13.** Click **OK** upon completion and repeat steps 31-32 for Fabric-B.

												dback 👤 🌘
E SAN Controller					$\bigcirc$							00
Pi Dashboard	Fabr				Success							G
% Topology	Fabi				A fabric is added	I.						6
≣ SAN ^					Ok							Actions ~
Fabrics Switches		Fabric Name	Seed Switch	State	SNMP SSH	User/ Community	Auth/ Priva	Licensed	Health	Perform Collection	Updated Time	Inci. VS
Links Interfaces		Fabric -A	192 168 168 15	Managed Continuously	true	snmpedmin	SHA_AES	. True	© Healthy	or	2024-01-12 18:58:07 284 UTC	
End Devices												
Host Path Redundancy Port Monitoring												
Zoning												
Active Zones Storage												
Virtual Management A												
Settings 🗸												
C Operations										tage 1		, 1 > >>

With NDFC SAN in place, the SAN resources can be seen from the Dashboard view:

،،ا،،،ا،، Nexus Dashboard دוدده	🛞 Fabric Controller 🗸	Feedback 👤 🧿
		00
<ul> <li>n Dashboard</li> <li>☆ Topology</li> <li>■ SAN</li> </ul>	Dashboards Overview Host Storage	Ø
	Fabrics         Event Analytics	Links
<u>⊥</u> <sup>e</sup> Operations	<ul> <li>Name States Health</li> <li>Fabric-A Managed Continuously</li> <li>Healthy</li> <li>Warning (a)</li> <li>Warning (a)</li> <li>Into (2a)</li> </ul>	0 NPV Links SLS
	Switches     Switch Health     Switch Status     Switch Release Versions            2         4         5         wator (e)         Major (e)         Major (e)         Major (e)         Healthy (2)         Switches         • ext(2)         •	Switch Models 2 Switches • D8-C9124V-K9 (2)

The management and operation functions available include SAN zoning, image management of the MDS switches, Device Manager, and Backup/Restore functions.

# VMware vSphere 8.0U1 Setup

This chapter contains the following:

- VMware ESXi Installation
- <u>VMware ESXi Configuration</u>
- <u>vSphere Cluster Image Update</u>
- Add Remaining Hosts to vCenter
- Add VSP Storage to Hosts
- Hitachi Storage Provider for VMware vCenter Initial Configuration
- <u>vVols Storage Configuration</u>
- Storage Policy Based Management (SPBM) for VMFS LDEVs
- Host Image and vSphere Configuration Profiles
- <u>vSphere Additional Finishing Steps</u>

This chapter provides detailed instructions for installing VMware ESXi 8.0U1 within Adaptive Solutions. On successful completion of these steps, multiple ESXi hosts will be provisioned and ready to be added to VMware vCenter.

Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco Intersight to map remote installation media to individual servers.

## VMware ESXi Installation

Step 1. Click the following link: <u>Cisco Custom Image for ESXi 8.0 U1 Install CD</u>.

Note: You will need a VMware user id and password on vmware.com to download this software.

Step 2. Download the .iso file.

Procedure 1. Download VMware ESXi ISO

### Procedure 2. Log into Cisco Intersight and Access KVM

The Cisco Intersight KVM enables the administrators to begin the installation of the operating system (OS) through remote media. It is necessary to log into the Cisco Intersight to access the UCS Server KVM connections.

- Step 1. Log into Cisco Intersight.
- Step 2. From the main menu, go to Infrastructure Service > Servers.
- Step 3. Find the Server with the desired Server Profile assigned and click "..." to see more options
- Step 4. Click Launch vKVM.

	disco Intersight		astructure Service 🗸				~	Search	Ŭ	FJ 🗘 💽 24) 🕼	
	Overview	S	Servers								
2	Analyze										
ži,	Operate	^		K-210C-M7 × Add Filter			×	🕒 Export 4 it	ems found $10 \sim$	per page 🔣 🔇 🛛 1	of 1 🗵 刘
	Servers		Health	Power	HCL Status	Models		Contract Stat	Drof	ile Status	R X
	Chassis		Health	() On 4	© Incomplete 4	Models		Not Covered 4	us Pron	lie Status 7	÷
	Fabric Interconnects		4 • Critical 4			4 • 00	SX 210C-M7 4		4	•ок 4	Nc <
	HyperFlex Clusters										
	Integrated Systems		Name	C Health C	Model	: 0 ;	M C UC C	Server Profile	Firmware Version		÷ 9
5	Configure	~	O AA21-6536-1-1	Critical	UCSX-210C-M7	128.0	512.0 AA2	aa21-esxi-1 🛛 🛇	5.1(1.230052)		
	-		O AA21-6536-1-2	Critical	UCSX-210C-M7	128.0	512.0 AA2	aa21-esxi-2 🛛 🛇	5.1(1.230052)	Power	>
	Profiles		O AA21-6536-1-3	0 Critical	UCSX-210C-M7	128.0	512.0 AA2	aa21-esxi-3 🛛 🛇	5.1(1.230052)	System	>
	Templates		O AA21-6536-1-4	0 Critical	UCSX-210C-M7	128.0	512.0 AA2	aa21-esxi-4 🛛 🛇	5.1(1.230052)	Profile	>
	Policies		··· Ø							Install Operating S	System
	Pools									Upgrade Firmwar	
										Launch vKVM	
										Launch Tunneled	vKVM
Nev	Command Palette	×								Open TAC Case	
Jaule	ate Intersight with Ctrl+K or g lp > Command Palette	go								Set License Tier	
	p - command Parette									Set License file	

**Step 5.** Follow the prompts and ignore certificate workings (if any) and launch the HTML5 KVM console.

**Step 6.** Repeat steps 1 – 5 to launch the vKVM console for all the ESXi servers.

#### **Procedure 3.** Prepare the Server for the OS Installation

Note: Follow these steps on each ESXi host.

**Step 1.** In the KVM window, click **Virtual Media** > **vKVM-Mapped vDVD**.

**Step 2.** Browse and select the ESXi installer ISO image file downloaded in <u>Procedure 1 Download VMware</u> <u>ESXi ISO</u> (VMware-ESXi-8.0.U1a-21813344-Custom-Cisco-4.3.1-a).

Step 3. Click Map Drive.

**Step 4.** Go to **Power > Reset System and Confirm** to reboot the server if the server is showing a shell prompt. If the server is shut down, click **Power > Power On System**.

**Step 5.** Monitor the server boot process in the KVM. The server should find the boot LUNs and begin to load the ESXi installer.

**Note:** If the ESXi installer fails to load because the software certificates cannot be validated, reset the server, and when prompted, press F2 to go into BIOS and set the system time and date to current. The ESXi installer should load properly.

### Procedure 4. Install VMware ESXi onto the bootable LUN of the UCS Servers

Note: Follow these steps on each host.

**Step 1.** After the ESXi installer is finished loading (from the last step), press **Enter** to continue with the installation.

**Step 2.** Read and accept the end-user license agreement (EULA). Press **F11** to accept and continue.

**Note:** It may be necessary to map function keys as User Defined Macros under the Macros menu in the KVM console.

**Step 3.** Select the Hitachi VSP boot LUN that was previously set up as the installation disk for ESXi and press **Enter** to continue with the installation.

**Step 4.** Select the appropriate keyboard layout and press **Enter**.

**Step 5.** Enter and confirm the root password and press **Enter**.

**Step 6.** The installer issues a warning that the selected disk will be repartitioned. Press **F11** to continue with the installation.

**Step 7.** After the installation is complete, press **Enter** to reboot the server. The ISO will be unmapped automatically.

#### Procedure 5. Add the Management Network for each VMware Host

**Note:** This is required for managing the host. To configure the ESXi host with access to the management network, follow these steps on **each** ESXi host.

**Step 1.** After the server has finished rebooting, in the UCS KVM console, press **F2** to customize VMware ESXi.

**Step 2.** Log in as **root**, enter the password set during installation, and press **Enter** to log in.

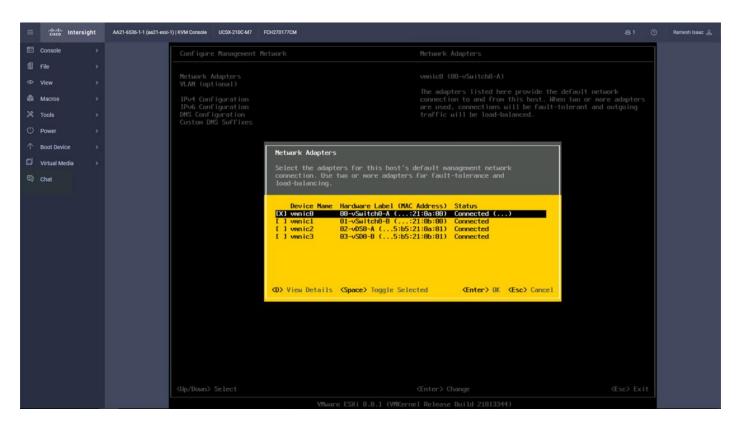
Step 3. Use the down arrow key to choose **Troubleshooting Options** and press **Enter**.

Step 4. Select Enable ESXi Shell and press Enter.

- Step 5. Select Enable SSH and press Enter.
- **Step 6.** Press **Esc** to exit the Troubleshooting Options menu.

Step 7. Select the Configure Management Network option and press Enter.

**Step 8.** Select **Network Adapters** and press **Enter**. Ensure the vmnic numbers align with the numbers under the Hardware Label (for example, vmnic0 and 00-vSwitch0-A). If these numbers do not align, note which vmnics are assigned to which vNICs (indicated under Hardware Label).



Step 9. Arrow down to select vmnic1 and press the spacebar to select it.

## Step 10. Press Enter.

**Note:** In the UCS Configuration portion of this document, the IB-MGMT VLAN was set as the native VLAN on the 00-vSwitch0-A and 01-vSwitch0-B vNICs. Because of this, the IB-MGMT VLAN should not be set here and should remain **Not set**.

## Step 11. Select IPv4 Configuration and press Enter.

**Note:** When using DHCP to set the ESXi host networking configuration, setting up a manual IP address is not required.

**Step 12.** Select the **Set static IPv4 address and network configuration** option by using the arrow keys and space bar.

**Step 13.** Under **IPv4 Address**, enter the IP address for managing the ESXi host.

- Step 14. Under Subnet Mask, enter the subnet mask.
- Step 15. Under Default Gateway, enter the default gateway.
- **Step 16.** Press **Enter** to accept the changes to the IP configuration.
- **Step 17.** Select the **IPv6 Configuration** option and press **Enter**.
- Step 18. Using the spacebar, choose **Disable IPv6 (restart required)** and press **Enter**.
- Step 19. Select the DNS Configuration option and press Enter.

Note: If the IP address is configured manually, the DNS information must be provided.

**Step 20.** Using the spacebar, select the following DNS server addresses and hostname:

- Under **Primary DNS Server**, enter the IP address of the primary DNS server.
- Optional: Under Alternate DNS Server, enter the IP address of the secondary DNS server.
- Under Hostname, enter the fully qualified domain name (FQDN) for the ESXi host.
- Press Enter to accept the changes to the DNS configuration.
- Press **Esc** to exit the Configure Management Network submenu.
- Press **Y** to confirm the changes and reboot the ESXi host.

### Procedure 6. (Optional) Reset VMware ESXi Host VMkernel Port MAC Address

**Note:** By default, the MAC address of the management VMkernel port vmk0 is the same as the MAC address of the Ethernet port it is placed on. If the ESXi host's boot LUN is remapped to a different server with different MAC addresses, a MAC address conflict will exist because vmk0 will retain the assigned MAC address unless the ESXi System Configuration is reset.

Step 1.From the ESXi console menu main screen, select Macros > Static Macros > Ctrl + Alt + F's > Ctrl+ Alt + F1 to access the VMware console command line interface.

Step 2. Log in as root.

**Step 3.** Type "esxcfg-vmknic -1" to get a detailed listing of interface vmk0. vmk0 should be a part of the "Management Network" port group. Note the IP address and netmask of vmk0.

**Step 4.** To remove vmk0, type esxcfg-vmknic -d "Management Network".

**Step 5.** To re-add vmk0 with a random MAC address, type <code>esxcfg-vmknic -a -i <vmk0-ip> -n <vmk0-netmask> ``Management Network''.</code>

**Step 6.** Verify vmk0 has been re-added with a random MAC address by typing esxcfg-vmknic -1.

**Step 7.** Tag vmk0 as the management interface by typing esxcli network ip interface tag add -i vmk0 -t Management.

**Step 8.** When vmk0 was re-added, if a message pops up saying vmk1 was marked as the management interface, type esxcli network ip interface tag remove -i vmk1 -t Management.

Step 9. Press Ctrl-D to log out of the ESXi console.

Step 10.Select Macros > Static Macros > Ctrl + Alt + F's > Ctrl + Alt + F2 to return to the VMware ESXimenu.

## VMware ESXi Configuration

With the UCS servers finished with their ESXi installation and basic configuration, they can now be added to the vCenter.

**Note:** In the validated environment, the vCenter is deployed within an existing management cluster independent of the Adaptive Solutions VSI environment. The vCenter Appliance could be deployed within the VSI itself with a first host that is configured through the vSphere web client and had the VSP VMFS datastores associated to it, but that is not covered in our deployment example.

### Procedure 1. Add deployed ESXi instance to the vCenter

**Step 1.** Open a web browser and navigate to the vCenter server.

**Step 2.** Select the top left tribar symbol to open the menu options and select the **Inventory** option.

E Sphere Client Q Search in	all environments			C & Administratoria	/SPHERELOCAL ~ 😳 🗇 ~
<ul> <li>G Home</li> <li>♦ Shortcuts</li> </ul>					
ஃ Inventory 면 Content Libranes					
<ul> <li>Workload Management</li> <li>Global Inventory Lists</li> </ul>	эе	Memory O B	free	Storage O B	free
B Policies and Profiles 저 Auto Deploy	iz total	0 B used	l Q B total	0 B used	0 B total
<ul> <li>Hybrid Cloud Services</li> <li>Developer Center</li> </ul>		0	Hosts		0
<sup>1</sup> ⊗ Administration I Tasks Events S Tags & Custom Attributes ⇔ Lifecycle Manager	0 Powered Off	O Suspended	O Connected	0 Disconnected	0 Maintenance
Cloud Provider Services		0	Installed Plugins		4
NSX     VMware Aria Operations Configuration	3	🛆 Warnings.	VMware vSphere Lifecycle		^
Skyline Health Diagnostics	8		VMware vSphere Lifecycle VMware Cloud Provider Se VMware vCenter Server Lifecycle	rvices Plugin	
Pin menu	ente Alternationale de la construction		U vmware vCenter Server Li	recycle Manager	

**Step 3.** If there is not an established Datacenter object within the vCenter, right-click the vCenter on the left and select **New Datacenter**... provide the Datacenter with an appropriate name.

D     C     Vc.adaptive-solucione local	Summary N	otive-solutions.local Monitor Configure Permi		Hosts & Clusters VMs	Datastores Netw		s Extensions	 Ø
E Nev C Nev Exp 식 Assi Tag	ss. vr. adaptive-solutions local w Datacenter w Folder bort System Logs sign License ps & Custom Attributes > d Permission rms >	etailis Version: Updates Available Build: Last Updated: Last File-Based Backup: Clusters: Hosts: Virtual Machines:	8.0.1 Updates Available 2208981 Aug 29, 2023, 4:51 PM Not scheduled 0 0 0	Capacity and Last updated at Not CPU O Mitz used Memory O B used Storage O B used	05 AM	Tags II		ğ
Recent Tasks Alarms	Custom A	ttributes j) No custom attributes a	assigned	II vCenter Heal Overall Health ⊘Good	th II			

Step 4. Right-click the Datacenter object and select the New Cluster... option.

	AS-VSI     Summary Moni		re Permissions Hosts & C	usters VI	Ms Datastores	Networks	Updates	e.		
🦻 vc.adaptive-soluti	▼c.adaptive-solutions.local       Datacenter. Delater.         ▲ Actions - AS-VSI       Datacenter. Delater.         ▲ Add Host       ▲ Add Host         ▲ New Cluster       New Folder         > Distributed Switch       >         ▲ New Virtual Machine       ⊕ Deploy OVF Template         Storage       >         Edit Default VM Compatibility       ●         ▲ Migrate VMs to Another Network       ●		alls : : 0 rtual Machines: 0 usters: 0 etworks: 0 atastores: 0			Capacity and Usage Last updated at 10:59 AM CPU O Mitz used Memory O B used Storage O B used VIEW STATS		Tags #		ŝ
	Move To Rename Tags & Custom Attributes	tes		Ш						
Recent Tasks	Add Permission Alarms		Details T	Initiator	т.	Queued T For	Start Time	ь т	Completion Time T	Server
move host	🔀 Delete			VSPHERELO	CAL\Administrator	4 ms	10/26/20	23.10:59:25	10/26/2023, 10:59:25 _	vc.adaptive-solutions

**Step 5.** Provide a name for the Cluster, enable **vSphere DRS** and **vSphere HA**, select **Import image from a new host**, check the box for **Manage configuration at a cluster level**, and click **NEXT**.

😑 vSphere Client 🛛 Q. Saarch in all en	and the second states		C & Administrator	RVSPHERELOCAL ~	© 0×
<	AS-VSI : actions				
	Cluster Basics	8.001		×	~
🗈 AS-VSI 1 Be	Location	AS-VSI			٢
2 im	D vSphere DRS				
3 00	onliguration				
4. RU	VSAN	Enable vSAN ESA ()			
	Choose how to set up Compose a new i	mage m an existing host in the vCenter inventory m a new host		-	
← Recent Tasks Alarms			CANCEL	Ť	
Task Name T Target	T Status T Details	Y Instator Y Descue Y	Start Time J T Complet	ion Time T Server	* <u>^</u>
m Al - More Tasks					C Alema

**Step 6.** Enter the IP or FQDN of the first host, enter root for the username, and provide the password specified during initial setup. Click **FIND HOST**.

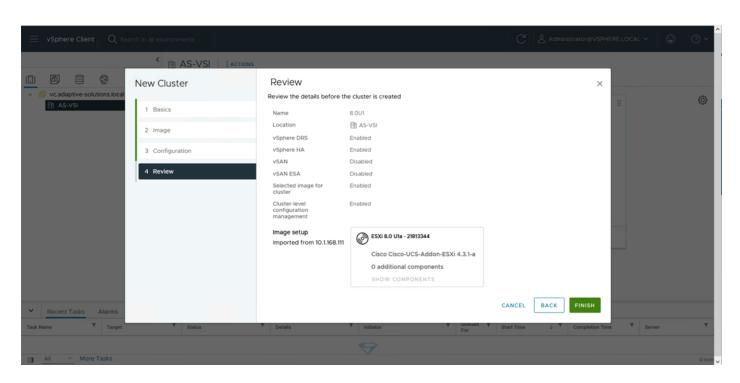
				247 HAR		-
≡ vSphere Client Q Se						
	AS-VSI ACTIONS					
🛄 📴 🛢 🧕	New Cluster	Image Enter the host details		×		0
AS-VSI	1 Basics			_		0
	2 Image	10.1.168.111 FIND HOST	root			
	3 Configuration					
	4 Review					
← Recent Tasks Alarms			CAN	CEL BACK NEXT		
Task Name T Target	T Status	T Details T Issiliator	T Conveil T Start 1	me à Completion Time	T Server	. î
B All - More Tasks						Oltama

**Step 7.** Click **Yes** past the Security Alert if prompted.

Step 8.Confirm the host is found correctly. Leave Also move select host to cluster selected and clickNext.

					) () ·
	K AS-VSI Actions				
vc.adaptive-solutions.local	V Cluster Image Enter the host de Basics Selected Host		CHANGE	× II	٥
3	O additio sноw co				
Recent Tasks Alarms Teik Name     Target	. V Status V Details	V initiator		NEXT Impletion Time Y Server	7
III All · More Tasks					

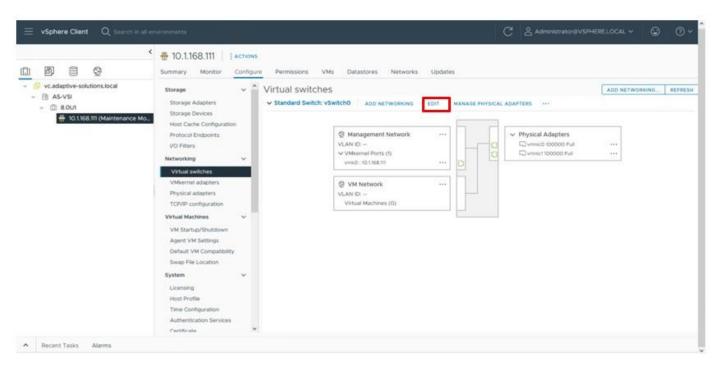
**Step 9.** Click **NEXT** past the Configuration screen dialogue summary. Confirm the cluster options and image setup within Review and click **FINISH**.



**Note:** The added ESXi host will have Warnings that the ESXi Shell and SSH have been enabled. These warnings can be suppressed. The host will also have a TPM Encryption Key Recovery alert that can be acknowledged and reset to green.

## VMware ESXi Configuration for the first ESXi Host

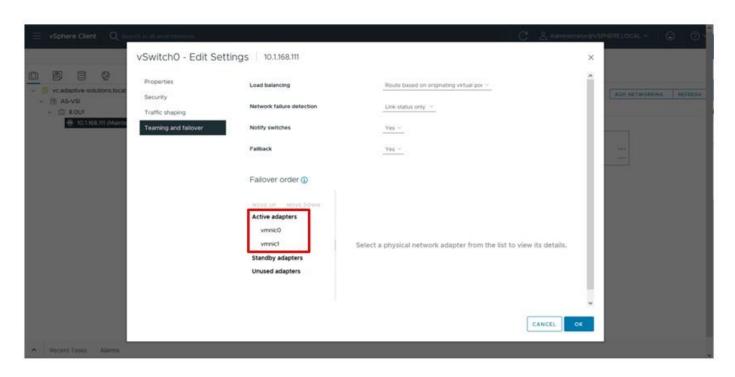
Procedure 1.	Set Up VMkernel Ports and Virtual Switch
Step 1. Switches.	Select the added host from within the new cluster, go to Configure > Networking > Virtual
Step 2.	Click <b>EDIT</b> .



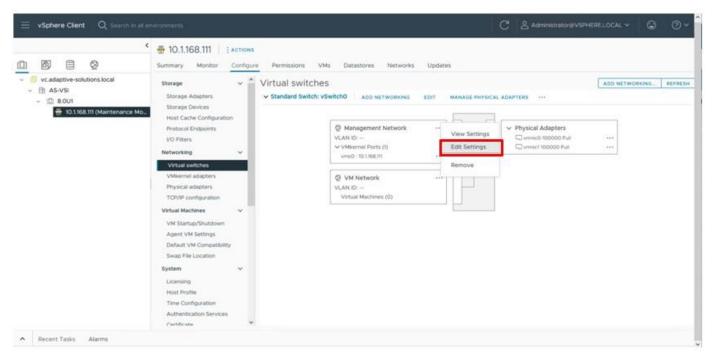
Step 3. Set the MTU to 9000.

😑 vSphere Cliest. 🔘 Issuer's of encourses	C & Administration	ercor · 🕒 🔿 ·
VSohere Circle Q. And the Andreastand	×	
· incont Tana Alarma	CANCEL	

**Step 4.** Select Teaming and failover and confirm that both vmnic0 and vmnic1 are shown as Active adapters for vSwitch0, adjust adapters with **MOVE UP** and **MOVE DOWN** options if needed. Click **OK**.



Step 5. Click the ... next to the VM Network port group and select Edit Settings.



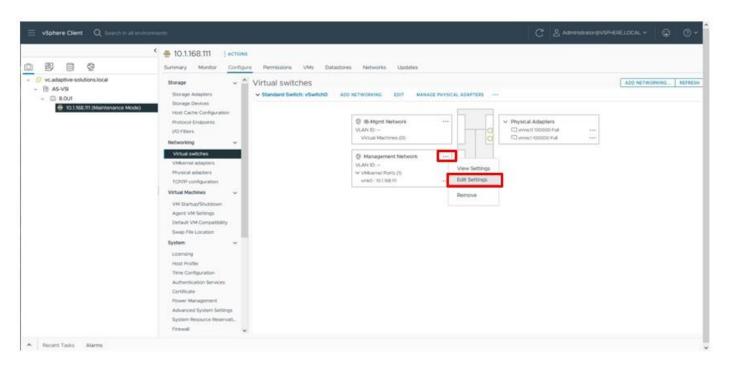
Step 6. Change the name of VM Network to **IB-Mgmt Network** and click **Teaming and failover**.

😑 vSphere Client. Q is	and that serve serveres				C & Administration	MERELOCAL V 🔘 🔘
	VM Network - Edit Set	ttings 10.1.168.111			×	
· · · · · · · · · · · · · · · · · · ·	Properties	Network label	IB-Mgmt Netwo			ADD NETWORKING
- B AS-VSI - D ROUT	Security Traffic shaping	VLAN ID	None (0)	<u>v</u>		
	Teaming and failover					
					CANCEL	
A Recent Tasks Alarma						

Step 7.Select the Override checkbox, select the vmnic1 adapter and click the MOVE DOWN option. ClickOK.

😑 vSphere Client 🛛 Q, s	partition at an of primarity			c	& April March 19		@ 0
	VM Network - Edit S	ettings 10.1.168.111			×		
VCL addeptive solutions local     VCL addeptive solutions local     AS-VSI     SOLI     SOLI     VCL KOS. IN (Manne)	Properties Security Traffic shaping Teaming and failover	Load balancing Network failure detection Notity switches Failback Failbucer order ()	Override Ov	nn analhaithe innan dor * ter *	Î	400 NETWORKS	S. BCTRESP
		MOVE UP MOVE DOWN Active adapters vmnic0 vmnic1 Standby adapters Unused adapters	All Properties COP V Properties Adapter Name Location Driver V Status Status	LLDP Cisco Systems Inc. Osco VIC Ethernet M vinoict PCI 0000 to:00.1 nenic Connected			
A Recent Talks Alarms						li.	

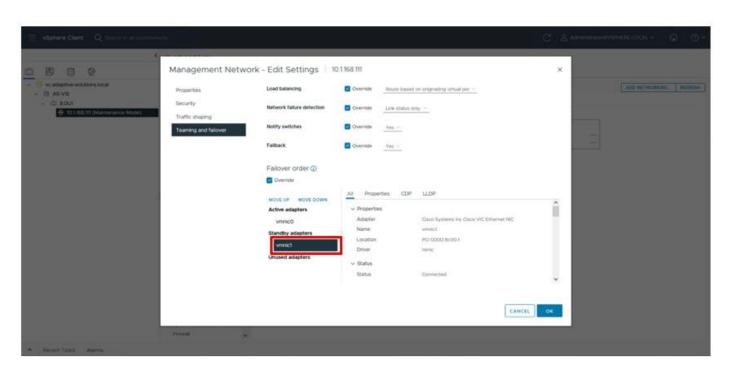
**Step 8.** Click the ... next to the Management Network port group and select **Edit Settings**.



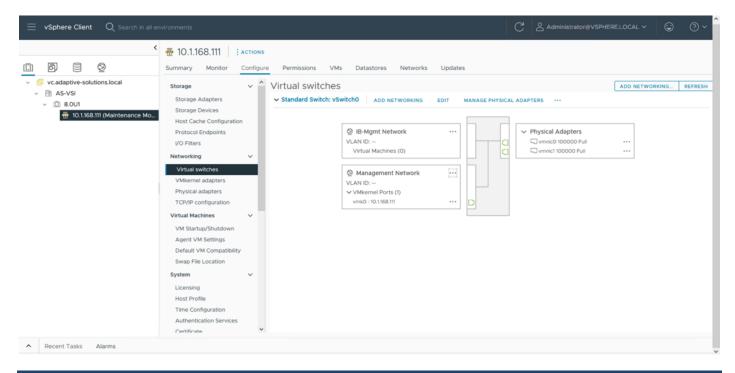
Step 9. Click Teaming and failover.

😑 vSphere Client 🔍 Search in all and con-	noriti-			C 2 Administrativis Presellocal v 😡 🕥
Control Contro Control Control Control Control Control Control Control Control C	Management Network Properties Security Traffic shaping Teaming and failover	<ul> <li>c - Edit Settings 1</li> <li>Load balancing</li> <li>Network failure detection</li> <li>Notify switches</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Failback</li> <li>Governide</li> <li>Move order ()</li> <li>Covernide</li> <li>Move order ()</li> <li>Standby adapters</li> <li>Unused adapters</li> <li>Unused adapters</li> <li>Unused adapters</li> <li>Unused adapters</li> </ul>		
Recent Tasks Alarms	Firewall			

Step 10. Select vmnic1 and move it to the Standby adapters category within Failover order and click OK.



The properties for vSwitch0 appear as shown below:



### Procedure 2. Create VMware vDS for vMotion and Application Traffic

The VMware vDS setup will create a single vDS for vMotion and Application traffic.

To configure the first VMware vDS, follow these steps:

Step 1. Right-click the AS-VSI datacenter and select Distributed Switch > New Distributed Switch...

B Q Summary	SI ACTIONS Monitor Configure Permissions Hosts & Clusters VM	ts Datastores Networks Upd	tates	
vc.adaptive-solutions.local  AS-VS Datace  B.C. B.C. B.Actions - AS-VS  Add Host  New Folder  Distributed Switch  C Storage Edit Default VM Compatibility  & Migrate VMs to Another Network	nter Details I Noste: 1 Virtual Machines: 0 Clustere: 1 Import Distributed Switch Import Distributed Switch	Capacity and Usage II Last updated at 12:34 PM CPU 121 MHz used atlocated Memory 5.5.7 GB used stocated Storage O B used	Tags II No tags assigned	
Move To Rename Tags & Custom Attributes Add Permission Alarms	Attributes II			

**Step 2.** Provide a name for the distributed switch and click **NEXT**.

**Step 3.** Leave 8.0.0 selected for the distributed switch version and click **NEXT**.

**Step 4.** Lower the **Number of uplinks** from 4 to 2 and provide **Port group name** for the default port group to align with the Application traffic. Click **NEXT**.

Sohere Client Q, Savethie at				
C Bill Bill Bill Bill Bill Bill Bill Bil	AS-VSI Excreme New Distributed Switch 1 Name and location 2 Select version 3 Configure settings 4 Ready to complete Cost	Configure settings Specify network offloads compatibility, number of uplink ports, resource atocation and default port group. Network Offloads Compatibility Number of uplinks 2 Default port group Port group name App-1000	×	•
Recent Tasks Alarms	No custom attributes assi	gred		

**Step 5.** Review the settings for the distributed switch and click **FINISH**.

**Step 6.** Click the Networking icon of the left-side menu and right-click the newly created distributed switch. Under **Actions** select **Settings > Edit Settings...** .

n B7 (= <u>Q</u>	VDSO : Summary Monit		missions Ports Hosts	VMs Networks		
<ul> <li>vc.adaptive-solutions.local</li> <li>AS-VSI</li> <li>IB-Mgmt Network</li> <li>M v050</li> </ul>	Switch Detail	snufacturer rision itworks ists rtual machines irts Edit Settings Edit Private VEJ Edit NetFlow	VMware, Inc. S.O.O 3 1 0 18 8 AN	Features  Network Offloads  Network VO Control Network VO Control Network VO Control NetWork VO Control version NetFlow Link Layer Discovery Protocol Link Aggregation Control Protoco Link Aggregation Control Protoco Link Aggregation Timeout Put misroring IOMP/MLD snooping Health check	Not supported Supported 3 Supported Supported Enhanced support Supported Supported Supported Supported	
	Add Permission Alarms	Restore Config	uration_	Custom Attributes		н
	No notes	-	No tags assigned		i) attributes assigned	



Select the Advanced tab and change the MTU from 1500 to 9000. Click OK.

E vSphere Client Q taxable at	end contents			vervetilet.co.et v 🔘 🔘 v
	C vDS0 jacnow Surrowy Montor C	Distributed Switch - Edit vDS0 × Settings		
O voladaptive-solutions.local     Oli A5-VSI     Oli B-Mgmt Network	Switch Details	General Advanced Uplinks MTU (Bytes) 2000 2		: ©
- 0010 App-100 0 x050-0VUpteks-1021 0 VMotion	Manufa Version Network	Multicast filtering mode 30MP/MLD shooping ~	Not supported Supported 3	
101 101	Panels Virtual Parts	Discovery protocol Type Cisco Discovery Protocol	Supported Supported Entercod Support	
		Operation Listen -	Supported Supported Supported	
		Administrator contact		
	Notes	Name		
	-			
Recent Tasks Alarms	No notes assigned	CHINESE ON	tributes assigned	

**Procedure 3.** Create vMotion distributed port group

**Step 1.** Right-click the newly created distributed switch. Within **Actions,** select **Distributed Port Group > New Distributed Port Group...** 

1 8 8	Summary Mo Actions	so	Ports Hosts VMs Networks		
vc.adaptive-solutions.local     ve.adaptive-solutions.local     ve.adaptive-solutions.lo	Switch Deta  Add and Edit Note Upgrade Settings Move To. Rename.	Ad Port Group   Manage Hosts  Manage	New Distributed Port Group Import Distributed Port Group Import Distributed Port Group Inc. Network UC Network UC NetWork UC NetFlow Link Aggreg Link Aggreg	Treads Not supported Control Supported Control Supported Control Version 3 Supported Supported Supported Supported Supported sption Timeout Supported sption Timeout Supported spooping Supported	
	Notes	II Tags	E Custom A	ttributes	H

**Step 2.** Provide a name for the vMotion distributed port group and click **NEXT**.

**Step 3.** Choose **VLAN** from the **VLAN type** drop-down list and specify the appropriate VLAN for vMotion. Select the **Customize default policies configuration** checkbox and click **NEXT**.

E vSphere Client Q taken in a another sector						
✓	[Actions				1	
Voor ad aaster - softwaars boars     Voor ad aaster - softwaars     Voor ad aaster - softwaars	d Port Configure settings Set general properties of the new port group. Port binding Port allocation Number of ports Network resource pool VLAN VLAN VLAN ip Advanced	Static binding Elastic ~ ① 8 (default) ~ VLAN ~ 3000]	 ] 	CANCEL BACK NE	X	٥
Recent Tasks Alarms	notes assigned No tags assigned		No custor	(1) attributes assigned		

**Step 4.** Click **NEXT** through the Security and Traffic shaping dialogue screens.

**Step 5.** Within Teaming and failover, select **Uplink 1** and click **MOVE DOWN** twice to have it set as a standby link. Click **NEXT**.

😑 vSphere Client 🔍 🗤					
	VDS0 Excrame				
vc adaptive-solutions.local Group     El AS-VSI     El B-Mgmt Network     T N	New Distributed Port Group	Teaming and failover Controls load balancing, network failure	detection, switches notification, failback, and up	olink fallover order.	0
	1 Name and location	Load balancing	Route based on originating virtual por $\sim$		
	2 Configure settings	Network failure detection	Link status only -		
E TOROCTORES	3 Security	Notify switches	Yes		
	4 Traffic shaping	Falback	Yes -		
	5 Teaming and failover	Failover order ()		_	
	6 Monitoring	MOVE UP MOVE DOWN			
	7 Miscellaneous	Active uplinks			
	8 Ready to complete	Standby uplinks		1	
		C Uplink 1		~	
			CAN	CEL BACK NEXT	
	No notes assigned	No tags assigned	No custom athilis		
· Recent Taska Alarma					

**Step 6.** Click **NEXT** through the Monitoring and Miscellaneous dialogue screens, review the settings presented within Ready to complete, and click **FINISH** to create the distributed port group.

📃 vSphere Client 🛛 Q Sea					
vc.adaptive-solutions.local	New Distributed Port Group	Ready to complete Review the changes before proceed	ling.	×	 ô
<ul> <li>IB-Mgmt Network</li> <li>IB-Mgmt Network</li> <li>ID-0</li> <li>App-1100</li> <li>VDSO-DVUplinks-tt</li> </ul>	<ol> <li>Name and location</li> <li>Configure settings</li> <li>Security</li> <li>Traffic shaping</li> <li>Teaming and failover</li> <li>Monitoring</li> <li>Miscellaneous</li> <li>Ready to complete</li> </ol>	Distributed port group vMotion name Static t Network resource (defaul pool VLAN ID 1000	inding	CANCEL BACK FINISH	•
Recent Tasks Alarms					

**Step 7.** Repeat steps 1–6 for each VM application network taking note of desired teaming and failover, making both uplinks active if there is no path priority.

## **Procedure 4.** Add ESXi host to the vDS

Step 1.

Select the distributed switch, right-click it and select the Add and Manage Hosts... option.

	all environments				· ·   © _ ? ^
	VDS0 : ACTIONS     Summary Monitor Configure     Switch Details     Switch Details     Arnage Hosts     Arnage Hosts     So Standard Attributes >	VMware, Inc. 8.0.0 3 0 0 16	VMs Networks  Features Network Offloads Network (VO Control Network (VO Control NetFlow Link Layer Discovery Protocol Link Aggregation Timeout Port mirroring IGMP/MLD snooping Health check  Custom Attributes	Not supported Supported 3 Supported Supported	 ©
Recent Tasks Alarms	No notes assigned	No tags assigned	No custom	() attributes assigned	

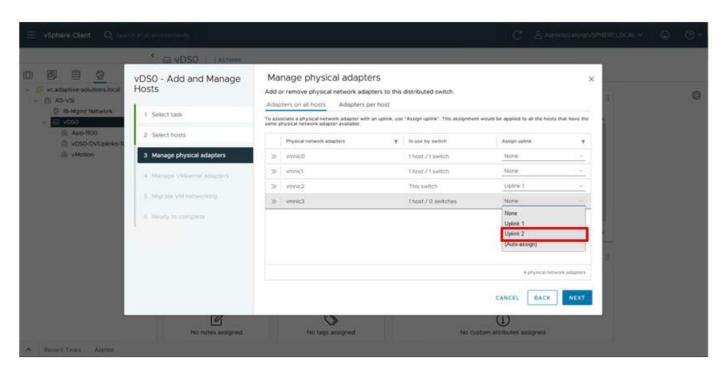
Step 2. Leave Add hosts selected and click NEXT.

Step 3.

3. Select the first ESXi host that was previously added to vCenter and click **NEXT**.

vSphere Client O, Search In all environments			
VDS0 - Add and Manage v c.adaptive-solutions.local v AS-VSI © IB-Mgmt Network	Select hosts Select hosts to add to this distributed switch. All hosts Selected (1)	×	Ø
VDS0	SELECT ALL CLEAR SELECTION	COMPATIBLE INCOMPATIBLE	
		Cluster T Compatibility	
VMotion     3 Manage physical adapters	🕑   🏪 10.1.168.111 Connected (maintenance mode) 👔	🗍 8.0U1 🧹 Compatible	
4 Manage VMkernel adapters			
5 Migrate VM networking			
6 Ready to complete			
		1 hosts	
		CANCEL BACK NEXT	
No notes assigned	No tags assigned No	(j) lo custom attributes assigned	
Recent Tasks Alarms			

**Step 4.** Specify vmnic2 to be Uplink 1 and vmnic3 to be Uplink 2, and then click **NEXT**.



**Step 5.** Click **NEXT** past the Manage VMkernel adapters and Migrate VM networking dialogue screens. Review the summary within the Ready to compete screen and then click **FINISH**.

vSphere Client Q Search in all environments			
<			
VDS0 - Add and Manage voic adaptive-solutions local Hosts	Ready to complete Review your settings selections before finishing the wizard.	×	Ô
	✓ Number of managed hosts Hosts to add 1		
VDSO-DVUplinks-X     vMotion     Select hosts     Select hosts     Amount of the select hosts	Vumber of network adapters for update     Physical adapters 2		
4 Manage VMkernel adapters 5 Migrate VM networking			
6 Ready to complete			
		88	
		CANCEL BACK FINISH	
No notes assigned	No tags assigned	(j) No custom attributes assigned	
Recent Tasks Alarms			

#### **Procedure 5.** Add vMotion vmkernel to the first ESXi host

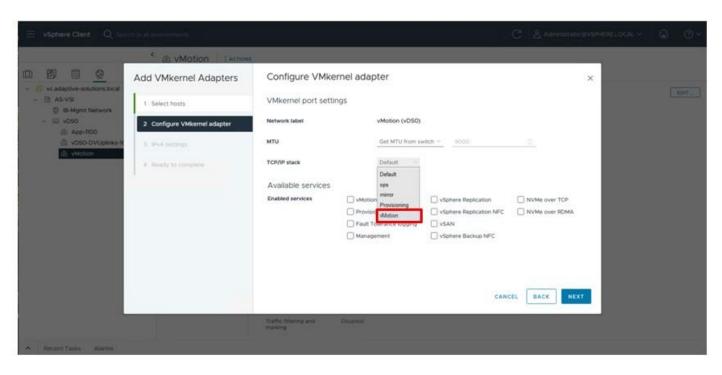
Step 1.Select the vMotion distributed port group, right-click it and select the Add VMkernel Adapters...option.

	Summary Monitor	tions Configure Permissions Ports	Hosts VMs			
Restore Add VM	Distributed Port Gr	oup Details anding Static binding Recation Elastic	Ports Usage Ports O used	E Capacity	Notes II	¢
Rename Tags & C Add Perm S Delete	ustom Attributes >	E Custom Attributes	-	П		

Step 2. Select the first ESXi host and click NEXT.

$\equiv$ vSphere Client $Q_{c}$ Set					
	<				
<ul> <li>B e o</li> <li>v c adaptive-solutions.local</li> <li>A S-VSI</li> <li>B-Migmt Network</li> <li>VDS0</li> <li>App-100</li> <li>vDS0-DVUplinks-tt</li> <li>vMotion</li> </ul>	Add VMkernel Adapters           1         Select hosts           2         Configure VMkernel adapter           3         IPv4 settings           4         Ready to complete	Select hosts          Member hosts       Selected (1)         SELECT ALL       CLEAR SELECTION         Image: Host       Y         Y       Y         Y       Y         Y       Y         Y       Y         Y       Y         Y       Y         Y       Y         Y       Y         Y       Y </th <th>▼ Cluster 11 8.0U1</th> <th>× II</th> <th>٥</th>	▼ Cluster 11 8.0U1	× II	٥
	No tags assigned	I III (j) No custom attributes assigned		1 hosts NEXT	
A Recent Tasks Alarms					

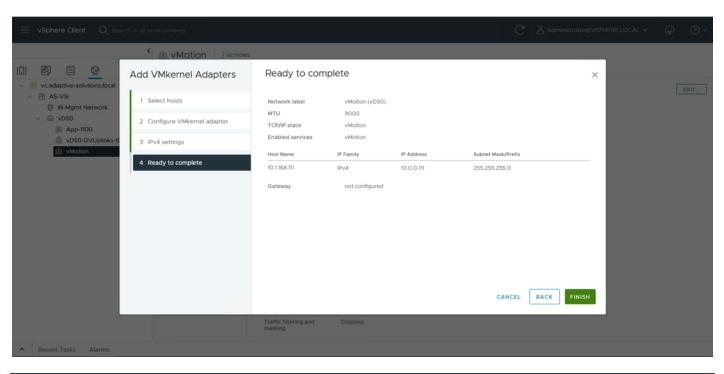
**Step 3.** Select **vMotion** from the TCP/IP stack drop-down list. Click **NEXT**.



Step 4. Select Use static IPV4 settings and provide an IP and netmask for the VMkernel. Click NEXT.

Sphere Clent Q: Sport's at an instruments			
< 🔿 vMotion	Actions		
Acc: 100 Acc: 1	IPv4 settings     Obtain IPv4 settings automatically     Use static IPv4 settings	10 0 0.111     255.255.255.0       Do not configure     •       Units configure     •       Units configure     •       CANCEL	
A Recard Tasks Alarma			

**Step 5.** Review the summary within Ready to complete and click **FINISH**.

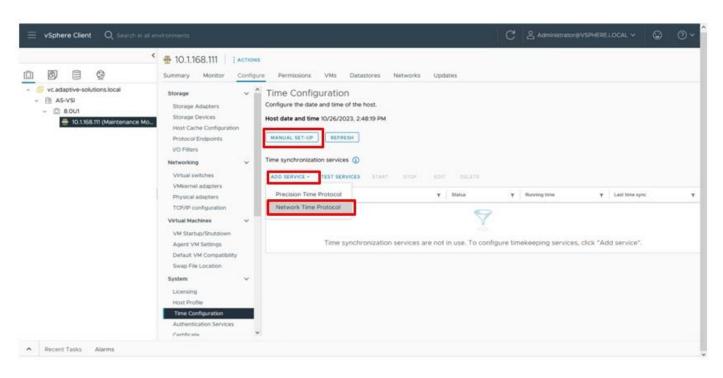


## Procedure 6. Configure settings on the ESXi host

**Step 1.** Select the **Hosts and Clusters** icon, expand the datacenter and cluster to find the first ESXi host. Select **Configure > System > Time Configuration**.

19162	Summary Monitor Confi				
<ul> <li>vc adaptive-solutions.local</li> <li> <sup>™</sup> AS-VSI         <sup>™</sup> 8.0U1         <sup>₩</sup> 10.1368.TH (Maintenance Mo         <sup>₩</sup> 10.1368.TH (Maintenance Mo         <sup>™</sup> 10.1368.TH (Maintenance Mo)         <sup>™</sup> 10.1368.TH (Maintenance Mo)</li></ul>	Storage Adapters Storage Adapters Storage Devices Host Cache Configuration Protocol Endpoints VO Fitters Networking v Vortual switches VMiserrot adapters TCP/AP configuration Verbual Machines v VM Startup/Shutdown Agent VM Settings Default VM Compatibility Swap File Location System v Licensing Host Profile Tme Configuration	Configure the date and time of the host. Host date and time 10/26/2023, 2:42:39 PM MANUAL SET-UP REFRESH Time synchronization services ① ADD SERVICE TEST SERVICES START STOP CDI DELETE	Petere) –	Running time <b>y</b> Last time a ekseeping services, click *Add service	

**Step 2.** Select **MANUAL SET-UP** if the time is not correct and adjust it. From the **ADD SERVICE** drop-down list and select the **Network Time Protocol** option.





Specify the appropriate IP/FQDN(s) for NTP server(s). Click OK.

vSphere Client Q, takenty in M e					
, 00000	♣ 10.1.168.111   Actions Summary Montor Contigues P	ermasione : VHa Dislastores : Networks : I	Updates		
voladapive-solutional Bi AS-VB Di ECUI     TO X 561 TH (Maintenance Mo:	Storage Association Storage Devices Host Cache Cantiguistics Protocol Endpoints VO Filters Notworking	e Configuration were the date and time of the host Ork Time Protocol (NTP) to synchronize the sy- monitoring events () even void 1088/254/10.1588/258 · governter multiple server hames and P addresses. We cancel	e contras to	<ul> <li>Let two ayot</li> <li>rvices, clock "Add Service"</li> </ul>	•
<ul> <li>Recent Tasks</li> <li>Alarma</li> </ul>					

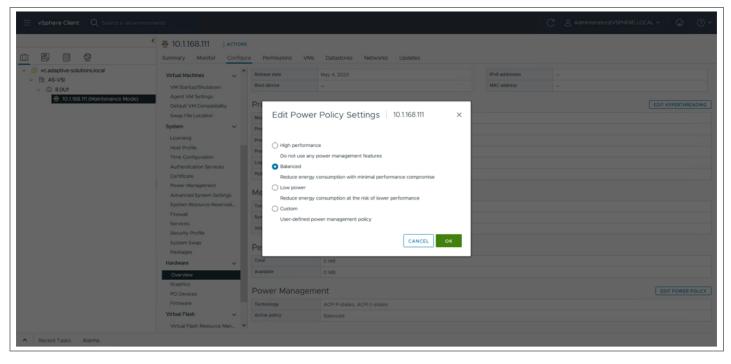
#### Procedure 7. Configure Host Power Policy

**Note:** Implementing this policy is recommended in the Performance Tuning Guide for Cisco UCS M7 Servers:

https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-server

<u>s/ucs-m7-platforms-wp.html#AdditionalBIOSrecommendationsforenterpriseworkloads</u> for maximum VMware ESXi performance. This policy can be adjusted based on your requirements.

**Step 1.** Within the first ESXi host, select **Configure > Hardware > Overview** and find Power Management at the bottom of the **Overview** section. Click **EDIT POWER POLICY**.



Step 2. Select Balanced from the options and click OK.

## vSphere Cluster Image Update

**Procedure 1.** UCS Tools Update

The UCS Tools VIB for ESXi allows IPMI communication over the CISCO IMC of the underlying Cisco UCS server to communicate vSphere relevant host information to Intersight and UCSM managed placements.

**Step 1.** Download the UCS Tools VIB for ESXi 8.0 from https://software.cisco.com/download/home/286305108/type/286323573/release/1.3.3

**Step 2.** Go to **Lifecycle Manager** from the main vCenter left-hand menu, click **ACTIONS** and choose the **Import Updates** option.

ifec	ycle Manager	ACTIONS -						
nage	Depot Updates	Updates Sync Updates	Settings					
sxi v	ERSIONS VENDOR A	import Updates						Lad Sync 17 hours ago. Next Sync in 6 ho
530 Ve	irsions	Hardware Compatibility List						
	Version	Sync HCL	•	Release Date		•	Category	Ť
0	ESKI 8 0 U2 - 22380479			09/20/2023			Enhancement	
0	ESKI 8 0 UK - 22088125			07/26/2023			Enhancement	
0	E5Xi 8.0 Ulsc - 22082334			07/26/2023			Enhancement	
0	ESKI 8.0 Uta - 21813344			05/31/2023			Enhancement	
0	E5Xi 8.0 UT - 21495797			04/17/2023			Enhancement.	
0	ESXI 8.0c - 21493926			03/29/2023			Enhancement	
0	ESX/ E 06 - 21203435			02/13/2023			Enhancement	
0	ESXI 8.01b - 21203431			02/13/2023			Enhancement	
0	ESXI 8 0a - 20842819			12/07/2022			Enhancement	
0	ESKI 8.0 GA - 20513097			0%/23/2022			Enhancement	
								R € 1/8 > N
ndor	Addons							
	Name	2	r Version		+ Release Date		T Category	• 1

**Step 3.** Click **Browse** within the pop-up window and navigate to the downloaded location of the UCS Tools VIB package.

The uploaded VIB is now available from **Edit Image** for the cluster within the **ADD COMPONENTS** within the Independent components and Vendor Addon Components selection.

1 67 8 2	Add Components		5	×
<ul> <li>Vecadaptive-solutions.local</li> <li>AS-VSI</li> <li>AS-VSI</li> <li>10.1/68.111</li> </ul>	Search for components by filtering on the "Co Show: Independent components and Vendor Ad			ently to all these hosts.
	Component Name Cisco VIC Ethernet Driver Cisco VIC Ethernet Driver Out-of-band host inventory and network Cout-of-band most inventory and network Cout-of-band host inventory Cout-of	Version         F           2.0.11.0 ~         1           1.3.3-10EM ~         1	Out-of-band host inventory and network configuration X using Cisco CIMC, v 1.3.3-IOEM Cisco + 10/17/2023	
	Cisco VIC Ethernet ENS Driver  DeliEMC utility VIB setting OS Name and Version in iDRAC  A DeliEMC component which provides custom DCUI screen for Factory installed PowerEdge servers and UWare ESXI  Dell OSName component for VMware ESXI 8.x  Dell ESXI FIST Installer for VMware ESXI	1060-         (           Version 7.0 GA-         (           Version 7.0 Update 3 -         (           8.0.0-         (           5.2.3-2023.03.20 -         (	(Important) Enhancement : [Fling] Cisco Out-of-band Host Inventory and Network Configuration https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes /UCS-Tools-ESXI-RN html	
		к с [2]/7 > Э	CANCEL SELECT	

Procedure 2. Hardware Support Manager Configuration

**Step 1.** Select the cluster for the VSI servers and click the **Updates** tab, then click **EDIT** within the **Image** section.

	8.0U1 ACTIONS mary Monitor Configure Permissions Hosts V	is Datastores Networks Updates
10.1.168.111	Image Hots in this cluster are managed colle tardware Compatibility M Hardware M Hard	

**Step 2.** Select the ESXi Version from the drop-down list and select the 8.0 U1c version that will reflect the addition of the vSphere 8.0U1c patch.

vSphere Client Q, Search in et er			C & Administration SVSPHERELOCAL V 😡 🔿 V
C cataptive-solutions.local  C cataptive-sol	Hosts 🗸 Edit Image	B O UB4 - 29813344         Enhancement           B O UB4 - 29813344         Enhancement           B O UB4 - 29813344         Enhancement           B O UB - 29813345         Enhancement           B O C - 29409926         Enhancement           B O C - 29409926         Enhancement           B O C - 29409926         Enhancement           B O C - 29429345         Enhancement           B O C - 2942916         Enhancement           B O C - 2063097         Enhancement	e will be applied consistently to all these hosts.
Y Recent Tasks Alarms			
Tail None * Tarpet	V Status V Details V	<b>9</b>	Comparison Time T Server
m Al - More Tasks		No items found	.00

**Step 3.** Click **SELECT** from Firmware and Drivers Addon. From the Select the hardware support manager drop-down list, select the **Cisco Intersight HSM @[the deployed Intersight Assist name]**.

😑 Inspende Client 🗌 🔍 Scores in a ser	ayaan			C Same	anarysistem (Construction of the Construction
	S ID 8:001 TATION				
S      S     S     S     S     S	Select Firmware and I vSphere integrates with hardware chuter. Select the hardware support manu Select Cisco Intensight HBM @as-assist at	support managers to install the selected firmware a	nd shiver addion on hosts in your cluster as part of applys	X a pu	ne horts
	Addon neme	T Addon version	+ Supported ESII) versions		
		Select hardware vendor to see availa	ble firmware and driver addons.		Anna e Composition see: 10 = Composition - e
Persent Tanker Alarma					
Tarthon Targe				ANCEL	300

**Step 4.** Find the desired firmware to set for the servers and click **SELECT**.

$\equiv$ violater Clerk $Q_i$ South is denoted		C & American Street & O ×
	C BOUT (Active	
C B B C C C C C C C C C C C C C C C C C	Select Firmware and Drivers Addon Select the hardware support manager Osco Intersight HSM @is-assist and/ot-isolation.local ~ () Hardware Support Manager Select a firmware and driver addon	× Allman Acats
	Addam name         Addam version         Suggested ESX versions           CR-3.0(4q)         30(4q)         200,2.03,170,2.70,3,800,80         CR-5.1(1,220052) 5.1(1320052)           CR-4.1(2P)         4.1(3P)         700,7.01,70,2.70,3,800,80         CR-5.1(1,220052) 5.1(1320052)           CR-5.2(0,230061)         5.2(0,230061)         700,7.01,70,2.70,3,800,80         CR-5.1(1,220052) 5.1(1320052)           CR-5.2(2)         5.2(0,230061)         700,7.01,70,2.70,3,800,80         CR-5.1(1,220052)           CR-5.2(2)         5.2(0,230061)         700,7.01,70,2.70,3,800,80         Supported ESX Versions           CR-5.2(2)         3.2(2)         700,7.01,70,2.70,3,800,80         TO,0,7.01,70,2,7.03,800,80           CR-5.2(2)         3.2(2)         700,7.01,70,2,7.03,800,80         TO,0,7.01,70,2,7.03,800,80           CR-5.2(2)         3.2(2)         700,7.01,70,2,7.03,800,80         TO,0,7.01,70,2,7.03,800,80           CR-5.2(2)         5.2(2)         700,7.01,70,2,7.03,800,80         TO,0,7	
w <u>Annen Tabl</u> Alarm Das New * Tarps	CP-5 (1220052)         5 (1220052)         7 (0, 7 (0, 7 (0, 2 (0, 3, 10 (0, 10) (0, 10) (0, 10)(0, 1	С
g ar _ Monitans		

Step 5. Click Show Details from Components.

🚊 vSphere Client 🛛 Q, Bearth in at set	inservents	C & Administratives/VSPAGAELOCAL ~ @ @ ~
	Cil B.OU1 Exchoes	
0 8 8 8	Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates	
<ul> <li>Vic adaptive-solutions local</li> <li>AS-VS</li> <li>ISOUT</li> </ul>	Inside       Cold: Image         Hardware Compatibility       Select the version of ESXI and other components that you want for the hosts in this cluster. The same image         Version       ESX Version         Version       EQUE_22088055_ (newsion) 01/26/20030         Version and Drivers Addon ()       Clust-VC5 Addon ESXI 4316 d/ ()         Components ()       No additional component Final Adds         Not Subscription       Version ()         Version       EQUE_22088055_ (newsion) 01/26/20030         Version       EQUE_2001052 ()         Version       Components ()         No additional component Final Adds       ()         Values Addon ()       Version ()         Version       Version ()         Version       No additional component Final Adds         Nove ()       Version ()         Values Adds       Version ()         Version       Version ()         Version ()       Version ()	e will be applied consistently to all these hosts.
♥ Recent Tasks Atems		
Tasi Name Y Target	T Status T Details T bilinter T Owned T Start True i T C	Completion Time T Server
	No items found	
II Al - More Tasks		- Dar



E vSphere Client Q, Search in all environments			C		9 0
	Monitor Configure Permissions Hosts VMs. Configure Permissions 19535 and other component sets Compatibility e floors traineer BSX Version B ESX Version B Pirmware and Drivers Addon C Components C	Datastores     Networks     Updates       ents that you want for the hosts in this cluster. The sate       0/Mc-22088025~     pressed 07/26/0228       100-105-Associ-2514 431-06     Image: Composer 14 400 estats       000-00407046/155     Show Additional components       000-00407046/155     Show Additional components       000-00407046/155     Show Additional components       00-00407046/155     Show Additional components       00-00407046/155     Show Additional components	Ine image will be applied consiste versus.	edy to al these hosts Notes	
Recent Tasks Alarms					
Name Y Tarpet Y Status	<ul> <li>Tetals</li> <li>Tetals</li> </ul>	Queued      V     Start Time	Completion Time	Server	
		No items found			
AL - More Tasks					

Step 7. Find the Cisco Native Ethernet Driver, the Cisco UCS VIC Native fNIC Driver, and the **Out-of-band host inventory and network configuration** using Cisco CIMC (UCS Tools for ESXi) selections and from the drop-down list for each to select the recommended drivers (nenic 2.0.11.0, nfnic 5.0.0.41, 1.3.3-10EM).

	C B.OUI Actions Summary Monitor C	i Configure Permissionis Hosts	VMs Datastores Networks Updates		
<ul> <li>vc.adaptive-solutions.local</li> <li>B AS-VSI</li> </ul>	Hosts 🗸		Congenient Name	• Version	Notes
D BOUT	Hardware Compatibility		Broadcom 120bps SAS HBA Driver	17.00.13.00-2vmw -	ESN component
	VMware Tools		Broadcom 120bbs SAS/PCIe HBA Driver	26.00.00.00-3vmw -	ES0 component
	VM Hardware		Broadcom LSI NATIVE DRIVERS LSU Management Plugin v2	10.2-hmw -	ESH component
1			Broadcom NetXtheme I ESX VMXAPI ethemet driver	4110-0-5vmw	ESN component
			Out-of-band host inventory and network configuration using Clico CMC	133-10EM -	Vendor addon component
			Osco Ethernet relive other	201010350-5uma	Ventor addon component
			Caco VC Ethemet ENS Driver	1060-	Vendor addon component
			Claco UCS VIC Netwer IVIC driver	50041Ctco - 600354vmw	Vendor addon component.
			ESR	8.0.1 Buld - 22088125 -	ESR component
			HPE HPSA LSU V2 Management Plugin	100-####	ESH component
Recent Tasks Alarms					
is Netw * Target	T lists T	Details * Initiatur	Ψ Queued Ψ Start Time ± Ψ Campletion Time	er * beer	
			8		
			No items found		

**Step 8.** With the appropriate drivers selected, click **VALIDATE** and then click **SAVE**.

	C III 8.0U1 Actions				
Ø Ø Ø	Summary Monitor G	onfigure Permissions Hosts VM	As Datastones Networks Updates		
<ul> <li>vc.adaptive-solutions.local</li> <li>III AS-VSI</li> </ul>	Hosts 🗸		Broadcom LSI NATIVE DRIVERS LSU Management Plugin v2	10.2-hmw -	ESN component
E sout	Hardware Compatibility		Broadcom Necktreme I ESX VMXAPI etternet driver	4110.0-5vmw -	ESN component
	VMware Tools		Out-of-cent host invertiny and retwork configuration using Cocil CMC	13.3.40EM-	Venitor addon component
	VM Hardware		Clico-Ethernet habive driver	2010 - 10250 Sime	Vendor addon
	1		Opco VIC Ethernet ENS Driver	1060-	Vendor addon component
			Osco-UCS VIC Native fNIC driver	500.41-Osco 500-35.4-mw	Vendor addon O
			2530	8.0.1 (build - 22088125	ESD component
			HE'S HPSA LSU V2 Management Plugin.	10.0-4vmw -	ESK component
Recent Tables Alarma		SAVE VALIDATE CANCEL	]	Contractivents per page <u>un v</u> 75 company	
a Nere * Tarpet	T Inte T	Details * Instatur	Ψ Quantit Ψ Start Time ± Ψ Completion The Compl	ine * Server	
			8		

Step 9. Select the added host and go to **Updates > Hosts > Image** and then click **View Image**.

Image     Host Version     Image Version       EDD Version     B.O. Ula - 2003044     B.O. Ula - 2008005       Components     Mast Version     Image Version		< 💮 10.1.168.111	ICTIONS					
Components     C	9 8 8			Datastores Networks Updates				
Image:       Market Computations         VM-Read Computations       VM-Read Computations         VM-Read Computations       Read Computations         VM-Read Computations       Read Version         Image:       Read Version	AS-VS							
Image     Heat Version     Image Version       EDD Version     8.0 Ula - 2003244     8.0 Ula - 2208225       Components     Heat Version     Image Version		VMware Tools	Quark Boot is not supported on the host.					
EDI Version B.O.U.s2013344 B.O.U.s2208225 Components Most Version Image Version			Software compliance		9	ow. Only all't compare		
Components Most Version Image Version			inage .	Hast Version	Image Version			
Series Company			ESR Version	8.0 Uta - 21813344	B.O.UNc - 22088125			
			Components	Mast Version	Image Version			
				<b>Y</b>				
Firmware compliance					Camp	ponents per page 4		
Host firmware is in compliance with the cluster image			Fernware compliance Host firmware is in compliance with the	e cluster image				
(a) The "bistribulaser" Configured in intersight supports the model of the hist UCSX 20C-M7			The 'Distributable' Configured in Inte	enaget supports the model of the host UCSX-250C-M7				

**Step 10.** With the host selected in the **Image Compliance** section, click **RUN PRE-CHECK**.

	1 8.0U1   ACTIONS				
0 8 9	Summary Monitor C	onfigure Permissions Hosts	VMs Datastores Networks	Updates	
vc.adaptive-solutions.local A 5-VS	Hods v Herbare Competibility VMeans Tools VM Herbare	ESIX Version Vendor Addon ① Firmware and Drivers Addon ① Components ① Image hardware computability is / Image Compliance Unit remained on fyito 2000, 12/200 Mil 61 and and and fitted mit simpliced	Trish enabling these Solutions, visionere H	etails	
			Software compl	fance	Show Only drift comparison
					L annual territoria

Step 11. With the RUN PRE-CHECK, cleared, click REMEDIATE ALL.

e e	C I 8.0U1 Actions	onfigure Permissions Hosts VMs D	stastores Networks Updates					
vc.adaptive-solutions.local	Hosts v	The cluster needs remediation to finish enable		die 1				
10.1168.ITI (Maintenance Mode)	VMware Tools VM Hardware	HEMEDIATE ALL BUT PRE-CHECK STAGE AL Notes	Heats Y 10.1168.111 ACTIONS V					
			The host will be reloce     Q Cuck Boot is not supp     Benediating this host		plane 1			
	î l		Software compliance		Show Only an	nt companiion ~		
			anage	Hust Version	Image Version			
			ESR Version	8.0 (Jta - 21813344	8.0 UK - 22088125			
			Components	Nost Version	Image Version			
				2				
				Components per page - 4 - 14				
			Firmware compliance Host firmware is in complia					
			The 'Distributable' Con	figured in intersight supports the model of the	Fest UCSX-210C-M7			

**Step 12.** Review the Impact summary and click **START REMEDIATION**.

			. 2 Administrational VSPHERE LOCAL V 🕘 💮 V
3	IT 8.0U1 FACTIONS		
B     B     C adaptive-solutions.local	Review Remediation Impact		×
✓ III AS-VSI	Impact summary	Impact summary	
<ul> <li>III 168.111 (Maintenance Mode)</li> </ul>	Applicable remediation settings	Thost(s) are non-compliant with the image.	
a contraction of contraction of the contract	VMware General Terms	1 host(s) will be rebooted.     The cluster needs remediation to finish enabling these Solutions: vSphere HA 8.0 Update 1.	
	Impact to specific hosts		×
	10.1.168.111	Notes VM states honor remediation settings	
		Whit may be powered off, suspended or migrated to other hosts based on the applicable remediation set Pre-check will be run again as a part of the remediation process. This is to ensure that no new issues have arisen on the duster or hosts since the last pre-check (if any) that prevent remediation. Hosts are remediated one at a time Hosts will be remediated on eat a time. So hosts will not reboot/go into maintenance mode simultaneoush Order of host remediation is determined at runtime. Hence that order may not correspond to the in which they appear here. Outck Boot optimizes the reboot path to avoid the hardware full power cycle, saving considerable time fro the upgrade process.	Show Only diff comparison - Image Version II.0 UTc - 2205/125
	I accept VMware General Terms		Components per page <u>4 ~</u>
	EXPORT IMPACT DETAILS	CLOSE START REMEDIA	TION
A Recent Tasks Alarms			

The host will be patched to 8.0 U1c and the VIBs will be installed, after which the host will automatically reboot after remediation.

vSphere Client Q Search in all environ		L 🖣 Level	WBVSPHERELOCAL V 🙄 🕐 V
1) Ø E Ø		nfigure Permissions Hosts VMs Datastores Networks Updates	
<ul> <li>Source adaptive-solutions Jocal</li> <li></li></ul>	Hosts v Image Hardware Compatibility VMware Tools VM Hardware	Image Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.         ESXI Version       8.0 Ufc - 2208125         Vendor Addon ①       Cisco-UCS-Addon-ESXI 4.31-8         Firmware and Drivers Addon ①       Cisco-UCS-Addon-ESXI 4.31-8         Firmware and Drivers Addon ①       Cisco-UCS-Addon-ESXI 4.31-8         Mage hardware compatibility is not verified in non-vSAN clusters. See details         Image Compliance         Lust checked on 1M300203, 138.41 PM (9 days age)         Image All hosts in this cluster are compliant	EDIT ····
Recent Tasks Alarms			
ask Name T Target T	Status Y	Details         Y         Initiator         Y         Queued         Y         Start Time         Y         Completion Time         Y         Server	
		No items found	

## Add Remaining Hosts to vCenter

This procedure details the steps to add and configure an ESXi host in vCenter.

#### **Procedure 1.** Add the ESXi Hosts to vCenter

**Step 1.** From the Home screen in the VMware vCenter HTML5 Interface, select **Hosts and Clusters**.

Step 2. Right-click the cluster and click Add Hosts.

	9 0	D 8.0U1 : Actrioxa Summary Monitor Configure Permissions Hosts VMs Dat	tastores Networks Updates		
vc.adapt B AS-V - 0 80 -	Actions - 8.001     Add Hosts     Annov Virtual Machine     New Virtual Machine     New Resource Pool	SSUES and Alarms      (0) vibrare 205 functionality and instantial data to unhabity data vibrare Coder Services can	and by the unavailability of elignees Quales Service	VML stateme Cusher Service VML are regared to maintain the health of vilaneee DRE	fathera "
	Ist Depley OVE Tensele.	Cluster Deteils Sa Total Processors: Sa Total Veotom O Megrations: C Regulations: Sa Sa Sa Sa Sa Sa Sa Sa Sa Sa Sa Sa Sa S	Capacity and Usage II Last updated at 1123 AM CPU O date used Memory O dia used Storage O dia used	VSphere HA II Protected OFU reserved for fallower: 0% OFU reserved for fallower: 0% Hemory reserved for fallower: 0% Proactive HA Dualled Heat Mandaeng: Endent VM Montoring: Disabled	6
	Move To Rename Tags & Custom Attributes 1 Add Permission Atams 1 Bendue from Inventury C Delete	vSphere DRS         E           Custer DRS Score ()         VM DRS Score ()           0-20%         0-VMs           20-40%         0-VMs           40-40%         0-VMs           40-40%         0-VMs           40-40%         0-VMs           40-60%         0-VMs           40-60%         0-VMs	Related Objects II Datacenter III AS-VII	Ouster Services     II     Ouster Consumers     II       Ouster Service health     Besource pods     0       Unhealthy     vApps     0       Virbuil machines     1	

**Step 3.** In the IP address or FQDN field, enter either the IP address or the FQDN name of the configured VMware ESXi host. Enter the user id (root) and associated password. If more than one host is being added, add the corresponding host information, optionally selecting "Use the same credentials for all hosts." Click **NEXT**.

······································	inati i				C & Advention	nymmesticox	@ @~
	10 8.0U1   attenses						
	Add hosts	Add new and existing the series of the serie	Literate (0)		×	eri in	
	2 Hard Summary 3 Hardstimage 4 Reven	50.1 MBR IND           50.1 MBR IND           30.1 MBR IND           40.1 MBR IND           ADD HORT	Per Constantin	Autorite Paraceter		2 500 2 500 2 500 2 500 2 500	٥
· monting Ameri		CPU reserved for failurest Memory reserved for failurest	05 05	CANCEL	NEXT	N 0. 0-	

**Step 4.** Select all hosts being added and click **OK** to accept the thumbprint(s) when prompted with the Security Alert pop-up.

**Step 5.** Review the host details and click **NEXT** to continue.

Step 6. Leave Don't import an image selected and click NEXT.

**Step 7.** Review the configuration parameters and click **FINISH** to add the host(s).

**Note:** The added ESXi host(s) will be placed in Maintenance Mode and will have Warnings that the ESXi Shell and SSH have been enabled. These warnings can be suppressed. The TPM Encryption Recovery Key Backup Alarm can also be Reset to Green.

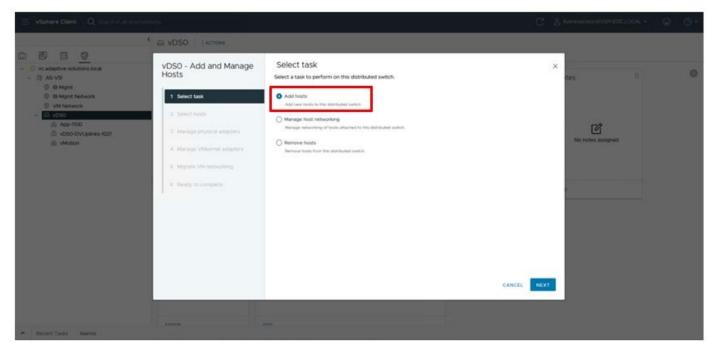
#### Procedure 2. Add additional hosts to vDS

The additional host will need to join the vDS for vMotion and application traffic.

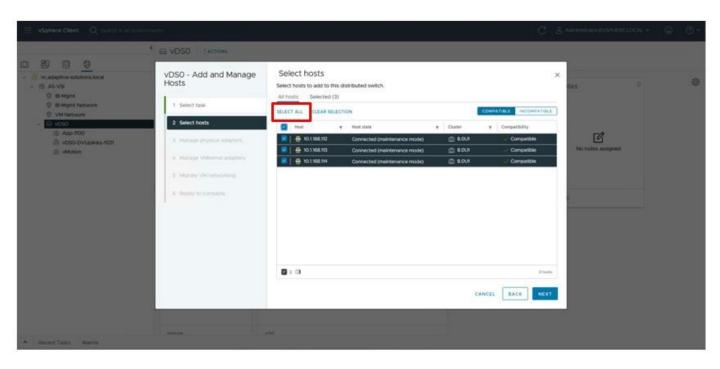
**Step 1.** Select the Network icon from the left side menu, right-click the created vDS and select the **Add and Manage Hosts...** option.

	<ul> <li>VDS0   ACTIONS</li> </ul>		
0 0 0	Summary Monitor Configure	Permissions Ports Hosts VMs Networks	
<ul> <li>Or categorie-solutions.local</li> <li>B. AS-VS</li> <li>B. Mymt</li> <li>B. Mymt</li> <li>B. Mymt Network</li> <li>VM Network</li> <li>M. Ase-100</li> <li>Ase-100</li> <li>VOSO 0VUplexis-1021</li> <li>VMotion</li> </ul>	Switch Details Manufacturer Version  Actions - V660 Distributed Port Group  Add and Manage Hosts.  Edit Notes.  Upgrade Settings P	VMware, Inc. 80.0 3 1 1 3 1 1 3 1 1 1 1 1 1 1 1 1 1 1 1	Notes II
	Move To Rename Tags & Custom Attributes Add Permission Alarms	Custom Attributes II	
	1 Delete		
	No tags assigned	Ko custom attributes assigned	
		100	

Step 2. With Add hosts selected click NEXT.



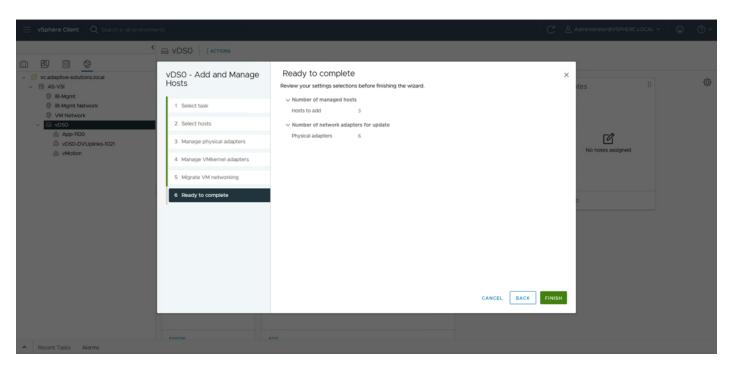
Step 3. Select all additional hosts and click **NEXT**.



Step 4. Assign Uplink 1 to vmnic2 and Uplink 2 to vmnic3 and then click NEXT.

🗇 vSphere Client 🔍 barmin a w			
	C El VDSO   (actions		
B     B     B     B     Advis     D     B     Advis     D     B     Advis      D     B     Advis      D	vDS0 - Add and Manage Hosts 1 Select task 2 Select hosts	Manage physical adapters Add or remove physical network adapters to this distributed switch. <u>Adapters on all hosts</u> Adapters per host To resolate a behavior adapter with an waiting, we "Assign spins". This assignment would be applied to all the to any explored reference adapter exercises.	x E Ø
- Are 100		Physical network adapters y In use by switch Assign spink	T <sup>2</sup>
C vDSO-DVUpress 1021	3 Manage physical adapters	3 vervic0 3 hosts / 3 switches None	- No Hotes assigned
	4. Manager VM amail adaptiers	36 smrith 3 hots / t switch None	
	5 Mphile Ministering	wmsc2     This switch     Uples 1     wmsc3     wmsc3     Inotes / 0 switches     None	
	\$ Rests to consists.	Adore Lights 1 Uptins 2 (Auto-assign) A (Pryonic CANCEL BAC	
· Record Table Alastia	anne		

**Step 5.** Click **NEXT** through Manage VMkernel adapters and Migrate VM networking.

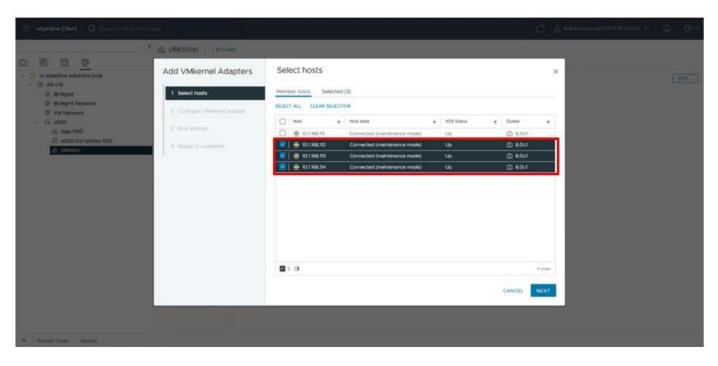


**Step 6.** Confirm the host addition numbers match and click **FINISH**.

**Step 7.** Right-click the **vMotion vDS** port group and click the **Add VMkernel Adapters...** option.

1 8 6 9	Summary Monitor Cont		arts Hosts VMs	
vc. adaptive-solutions.local     @ A5-v/s     @ B-Mgmt     @ B-Mg	Properties Protices Traffic titlering and marking Alarm Definitions I Mr Nr ther Nettwork	Properties General Name Port binding Port allocation Number of ports Natures resource pool Advanced Configure reset at discorreset Block ports Traffic shaping Vendor configuration VLAN Upliek teaming Security policy NetThow Traffic fibriefing and mailing	VAGION Stade Dividing Elucitic E Interface) Dividing Dividing Dividing Dividing Dividing Dividing Dividing Dividing Dividing	

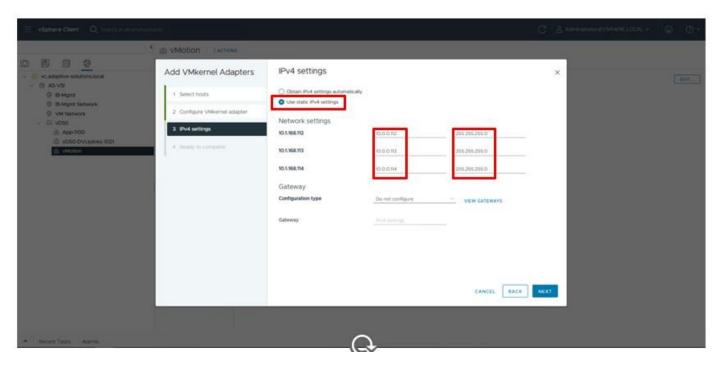
**Step 8.** Select the added hosts and click **NEXT**.



**Step 9.** From the drop-down list for TCP/IP stack, choose **vMotion** and click **NEXT**.

🚊 ASphare Client 🔍 Sparst tradisations							
	Add VMkernel Adapters Add VMkernel Adapters  Science Adapters  Configure VMeenel Adapters  Productions  Add VMkernel Adapters  Adapte	0,	VMotion (VDS0 Get MTU hom Default ops minor Porteauttors Provide Velacion	switch - 9000	NVMd over TOP NVMd over HDMA	×	
A Incentials Jame							

**Step 10.** Select the **Use static IPv4** settings option and provide **vMotion** IP and netmask information for each host. Click **NEXT**.





vSphere Client Q Search in all environment							© ~
	Add VMkernel Adapters	Ready to com	plete			×	EDIT
<ul> <li>III AS-VSI</li> <li>IB-Mgmt</li> <li>IB-Mgmt Network</li> <li>VM Network</li> <li>VM Network</li> <li>App-1100</li> <li>App-100</li> <li>VDSO-DVUplinks-1021</li> <li>MAddon</li> </ul>	Select hosts     Configure VMkernel adapter     I FV4 settings     Ready to complete	Network label MTU TCP/IP stack Enabled services No.1368.112 10.1368.113 10.1368.114 Gateway	vMotion (vDS0) 9000 vMotion IP Femily IPv4 IPv4 IPv4 not configured	IP Address 10.0.0.112 10.0.0.113 10.0.0.114	Subnet Mask/Prefix 255 255 255 0 255 255 255 0 255 255 255 0 255 255 255 0	K ENISH	
Recent Tasks Alarms							

## Procedure 3. Image Reconciliation

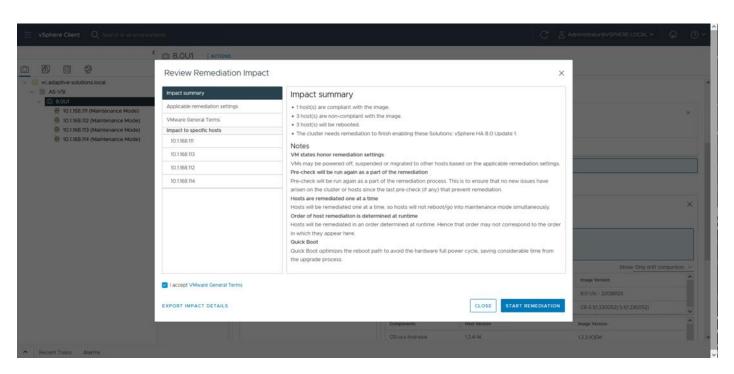
Step 1. Click Updates > Hosts > Image for the VSI cluster and select RUN PRE-CHECK.

	C 0 8.001   ACTION		
0 6 0	Summary Monitor C	onfigure Permissions Hosts VMs Datastores Networks Updates	
AS-VSI     COLT     B 10.166.01 (Maintenance Mode)     T0.166.01 (Maintenance Mode)     D1.168.01 (Maintenance Mode)     D1.168.01 (Maintenance Mode)     D1.168.01 (Maintenance Mode)	Harts v	Image         Hosts in this cluster are managed collectively. This image below will be applied to all hosts in this cluster.         ESD Westen       B.0 UK - 2008055         Windor Addon ()       Orce-UCS-Addon-KER 4.3.1-e         Permeare and Drivers Addon ()       CH-5 (1/230052) 5.1(1/230052)         Components ()       2 additional components Show setable         Image handware compatibility is not writified in non-vSAN clusters. See declate.         Image Compliance         Last memory in the cluster         Image Reset on the provide and the provide action of the pr	OHECK COMPLUNCE
		Number     The image of the entity '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance their for '8,000 has done of the host is added after checking compliance the host is added after checking compline of the host is added after checking compliance the ho	

Step 2. After the pre-check resolves, click **REMEDIATE ALL**.

	101 8.0U1 #ACTIONS					
8 8 8	Summary Monitor C	onfigure Permissions Hosts VMs Datastore	s Networks Updates			
vc.adaptive-solutions.local	Hosts v	Last channel on Antonio 2010 2010 Peri (1 disponente) A transit nel complete				
Image: 2014         Image: 2014 <thimage: 2014<="" th=""> <thimage: 2014<="" th=""></thimage:></thimage:>	Hardware Compatibility VMware Tools VM Hardware	Pre-check completed Completed 10/3/2023, 2:32 26 PM O No pre-check issues found				
The second second second second		4 hosts pre-checked: 10.1.168.111, 10.1.168.112, 10.1.168.1	13, 10.1.168.014			
		The cluster needs remediation to firsth enabling these	Solutions: vSphere HA 8:0 Update 1			
		REMEDIATE ALL BUN PRE-CHECK STAGE ALL				
		Hosts	10.1.168.113 ACTIONS ~			
		<u>▲</u> 10116E.H3	A Host is out of compliance w	with the image		
		A 10 1 166 T2	The host will be rebooted a	during remediation.		
		▲ 10.1 588 114	Guick Boot is not supporte     Gi Remediating this host will a	id on the host. Image these Solutions, vSphere HA & 0 Upo	ater 1	
			Software compliance		Show Only ant. co	mparison
			itrage	Hoxi Version	Image Version	
			ES0 Version	8.0 Uta - 21813344	0.0 U% - 22088125	
			Femware and Drivers Addon	None	(29-5-1(1.230052) (5-1(1.230052)	
			Congonanta	Hust Version	Image Version	
			CS-ucs-tool-exal	1244	13.3-10EM	

#### Step 3. Click START REMEDIATION.



**Step 4.** Confirm the remediation has completed successfully.

📃 vSphere Client	Q Search in all environ						C		ERELOCAL ~	@~
		< 1 8.001 ACTION	1							
	9	Summary Monitor	Configure Permissions I	iosts VMs Datastores	Networks	Updates				- 1
<ul> <li>vc.adaptive-solution</li> <li>AS-VSI</li> </ul>	ns.local	Hosts v	A Image hardware compa	ibility is not verified in non-vSAN o	lusters. See de	tais				^
H 10.1.168.11	(Maintenance Mode) 2 (Maintenance Mode) 3 (Maintenance Mode) 4 (Maintenance Mode)	Hardware Compatibility VMware Tools VM Hardware	Image Compliance Last checked on IVI3/2022, 3:03:25 P Al hosts in this cluster are compliance						HECK COMPLIANCE	
			Remediation completed successf Completed 10/5/2023, 3:05:12 PM						SKIP REMAINING HOSTS	×
			4 Hosts completed + 4 host	i wmediatael 10.1.168.07, 10.1.168.02, 10.1.168.02	id ties na					- 1
			Pre-check completed Completed 1/13/2023, 2:32:28 PM in pre-check issues found							×
			4 hosts pre-checked: 10.1.168.78, 3	0.1368.112, 30.5368.112, 10.5368.114						
← Recent Tasks A	larms									
Task Name T	Target T	Status o T	Details T	Initiator Y	Queued ¥ For	Start Time T	Completion Time Y	Server		
Remediate Cluster	(D) 8.0U1	Completed		Administrator@VSPHERELOCAL	11 ms	11/13/2023, 2:34:26 PM	11/13/2023; 3:05:12 PM	vc.adaptive-solutions.local		_
Check compliance of hos	10.1.168.114	@ Completed		Administrator@VSPHERE.LOCAL	13 ms	11/13/2023, 3:04:52 PM	11/13/2023, 3:05:12 PM	vc.adaptive-solutions.local		
DRS recommends hosts t_	(II) 8.0U1	O Completed		com.vmware.vcIntegrity	3 ms.	11/13/2023, 2:57:11 PM	11/13/2023, 2:57:11 PM	vc.adaptive-solutions.local		
Check compliance of clu	(D) 8.0U1	O Completed		Administrator@VSPHERE.LOCAL	29 ms	11/13/2023, 3:05:12 PM	11/13/2023, 3:05:34 PM	vc.adaptive-solutions.local		
Initiate host reboot	10.1.168.114	Completed		com, vmware.vcintegrity	4 ms	11/13/2023, 2:59:41 PM	11/13/2023, 2:59:41 PM	vc.adaptive-solutions.local		
DRS recommends hosts t_	(III) 8.0U1	@ Completed		com.vmware.vcintegrity	9 ms	11/13/2023, 2:58:11 PM	11/13/2023, 2:58:11 PM	vc.adaptive-solutions.local		-
Al More Ta	sks									6 dem 🗸

## Add VSP Storage to Hosts

#### Procedure 1. Add FC-SCSI Datastores

Step 1. Select the first ESXi host, right-click and select Storage > New Datastore... .

≣ vSphere Client Q	Actions - 10.1.168.111 (Maintenance Mode)	C & Ad	ministratoria/VSPHERELOCAL ~ 😨 💿
) B) 🗎 👲	12 Deploy OVF Templata 20 New Resource Paol 12 New vApp	Configure Permissions VMs Datastores Networks Updates	
<ul> <li>         → AS-VSI      </li> <li>         → B.OU1      </li> <li>         → 10.1168.111 (Mast      </li> </ul>	्री import VMs	TTS on this facet is disabled	
III W.L. IOC. III (MILLIN	Maintenance Mode >	and has been enabled	Actions *
	Connection	s been enabled	Actors "
	Power > Certificates >		
	Storage >	Capacity and Usage     Last sedand at 257 PM	6
	C Add Networking	Rescan Storage     VMware ESX, 8.0.1, 21813344     Det     UCSX-210C-M7	
	Export System Logs	recessor Type: Intel(R) Xeon(R) Gold 64387* Memory rglcal Processors: 128 6.21 GB used alocated	
	Reconfigure for «Sphere HA	Cs: 4 Storage	
	R Assign License	rtual Machines: 0 ate: Maintenance Mode O il used	
	Settings	Dome: 2 days	
	Move To	VIEW STATS	
	Tags & Custom Attributes 🗧		

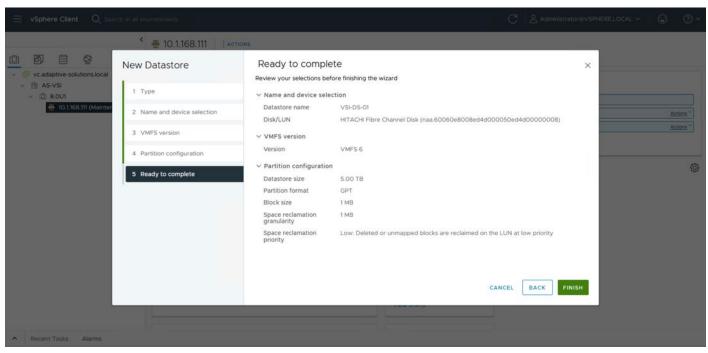
**Step 2.** Leave VMFS selected for the type and click **NEXT**.

**Step 3.** Select the allocated LUN and provide an appropriate name and click **NEXT**.

😑 vSphere Client: 🔍 🗤									
	* 番 10.1.168.111 EAction	6							
vc adaptive solutions.book     vc adaptive solutionsolutions.book     vc adaptive solutions.book     vc adaptive soluti	New Datastore 1. Type 2. Name and device selection	Name and device sel Specify datastore name and a de Name	k/LUN for prove	-	store.			×	
	.3 VMFS version	Narve	LUN	at local to prove the	Hardware T Acceleration	Туря	T Sector Format	Y QA V S	
	4. Partition configuration	HITACHI Fibre Channel Dis.		5.00 18	Supported.	HOD	51211	M	
	5 Ready to soriplete	HITACH Fibre Channel Dis.		5.00 TB	Supported	HOD	512n	Y	0
	a construction of the second second	O Local ATA Disk (110 ATA_		223.57 68	Not supported	Flash	512.0	- N	
		O Local ATA Disk (110.ATA	0	223.57.68	Not supported	Flash	512 e	Nu	
		CI EXPORT~				CANCEL	BACK	A bans	
A Rocant Tasks Alarma									

Step 4. Leave VMFS 6 selected and click NEXT.

Step 5.Leave the default options to use all storage within the Partition configuration screen and clickNEXT.



**Step 6.** Review the summary within the Ready to complete dialogue and click **FINISH**.

**Step 7.** Repeat steps 1–6 for any additional datastores.

#### Procedure 2. Configure FC-NVMe Datastores

Step 1. Select the first host added within the cluster and click **Configure > Storage > Storage Devices**.

Ø E &	Summary Monitor Configu								
Cradiadove-solutions local     As-vis     As-vis     As-vis     Ino.168.11     Do.168.12     Do.168.13     Do.168.14     Order Test-terness	Storage Adapters Storage Adapters Storage Adapters Host Cache Configuration Protocol Endpoints UO Filters Networking v Virtual switches Vingernel adapters TCP/IP configuration Virtual Machines v Virtual Machines v	Storage Devices           REFRESH         ATTACH         DETACH         ABNAME           Nome         Interactive Trace Comment Disk (mas/60060e80036ed4d0000050ed4d0000000018)         Interactive Trace Comment Disk (mas/60060e80036ed4d0000050ed4d0000000018)           Local ATA Disk (100.ATA         Microm_S300_MTTPDDAV240TDS         MES324450           Introduct Table (100.ATA         Microm_S300_MTTPDDAV240TDS         MES324450           Introduct Table (100.ATA         Microm_S300_MTTPDDAV240TDS         MES324450           Introduct Table (100.ATA         Microm_S300_MTTPDDAV240TDS         MES324450           NVMer Fiber Channel Disk (mas/60006e808000000000000000000000000000000		*	Type disk disk disk disk disk disk disk enclosure	▼ Capacity ▼ 46.88 MB 223.57 GB 5.00 TB 5.00 TB 32.00 GB 5.00 TB	Detectore         ▼           Not Consumed         Not Consumed           Not Consumed         Not Consumed           Not Consumed         Not Consumed           Not Consumed         Solo Consumed           Image: Solo Consumed         Solo Consumed           Not Consumed         Solo Consumed           Not Consumed         Not Consumed           Not Consumed         Not Consumed	Operational ¥ State Attached Attached Attached Attached Attached Attached Attached Attached Attached	Hardware Acceleration Supported Not supported Supported Supported Supported Not supported
	Agent VM Settings Default VM Compatibility Swap File Location System v Licensing Host Profile Time Configuration Authentication Services Certificate Power Management Advanced System Settings System Resource ReservatL. Firewal Services Security Profile System Swap	EXPORT  No items s	lected					fern per page	20 10 4

**Step 2.** Confirm that the NVMe Fibre Channel Disk devices are listed.

	10.1.168.111	ACTIONS								
B B B Sum	nwary Monitor O	Configu	Permissions VMs Datastones Networks Updates							
v: adaptive-iolution local a As-VB © 8000 ©	Israge Scorage Adapters Scorage Descers Next Carek Configuration Persisted Endoortis UD Pitters Isterations Without antiDes Vedermet adapters Physical adapters TOVP configuration	~	Storage Devices  EXTELL ATTRO POSITION	MSAZESHETMI MSV20450FD	0	T Type data data data data data data windbaure	<ul> <li>Casedy 7</li> <li>46.85 MB</li> <li>223.87 68</li> <li>223.87 68</li> <li>3.00 TB</li> <li>3.00 TB</li> <li>3.00 TB</li> </ul>	Delative Rat Consumed Rat Consumed Rat Consumed Rat Consumed Rat Consumed Rat Consumed	Sale Attached Attached Attached Attached Attached	<ul> <li>Notherst Antifestion</li> <li>Supported</li> <l< th=""></l<></ul>

Step 3. Select the first NVMe Fibre Channel Disk, then select Paths. Verify that all paths have a status of Active (I/O).

VSphere Client Q Search in all another variants										0 0
, 19 11 12 12 12 12 12 12 12 12 12 12 12 12	ID.1.168.111 Actor		ntores Networks Updates							
vc.adaptive-solutions.local           -         IB: AS-V/S           -         ID: BOUT           ID: 168.172         ID: 168.172           ID: 1588.173         ID: 1588.173           ID: 1588.174         ID: 1588.174           Yourget and the solution of the solution o	Europe v v Europe Adapters Europe Adapters Pred Cathe Configuration Produced Endpoints (2) Faires Visual adultins Visual adultins Visual adultins Visual adultins TCMP configuration TCMP configuration Visita Machines v Visita Machines v Visita Status(Chinastow) Agent Vil Status(Chinastow) Bank Pile Location	KOTECH ATTACH OTTACH     Figure     HTACH Files Outward Data ()     Local ATA Data (IDLATA)     Local ATA Data (IDLATA)     Kottel ATA Data (IDLATA)     MVMs Fibre Outward Data ()     HTACH Fibre Outward Data ()	ADMANE         Turns on US         Turns on US           wild 20050-80078-9400000-046-840000000- Winner, 5300, WTFD0AV240705,         Turns on US           Marrier, 5300, WTFD0AV240705,         Turns on US           Condensid/CondensionCondensis         Turns on US           Statum, 5300, WTFD0AV240705,         Turns on US           Statum, 5300, WTFD0AV2400005, Turns on US         Turns on US           Statum, 5300, WTFD0AV2400005, Turns on US         Turns on US           Statum, 5300, WTFD0AV2400005, Turns on US         Turns on US           Statum, 5300, WTFD0AV25, TURNs on US         Turns on US           Statum, 5300, WTFD0AV25, TURNs on US         Turns on US           Statum, 5400, TUR         Turns on US </th <th></th> <th>* LUN * 3 MI 0</th> <th>Type Type chain ch</th> <th><ul> <li>Capiting V</li> <li>Capiting V</li></ul></th> <th>Batastone Hell Consumed Hell Consumed Hell Consumed Hell Consumed Hell Consumed Hell VII-DD-DE Hell Consumed</th> <th>Sets Affactived Affactived Affactived Affactived Affactived Affactived Affactived Affactived</th> <th>Accesses Accesses Sequenced Not support Not support Seconted Secon</th>		* LUN * 3 MI 0	Type Type chain ch	<ul> <li>Capiting V</li> <li>Capiting V</li></ul>	Batastone Hell Consumed Hell Consumed Hell Consumed Hell Consumed Hell Consumed Hell VII-DD-DE Hell Consumed	Sets Affactived Affactived Affactived Affactived Affactived Affactived Affactived Affactived	Accesses Accesses Sequenced Not support Not support Seconted Secon
	System v Learning Host Profile Three Carlinguation Autorescation Services Carlifocation House Management Advanced System Settinge System Housecate Reservation Security Insuline Security Insuline	Intel3         DIANS           Retrie Non         unitsal CO TILLO           unitsal CO TILLO         unitsal CO TILLO           unitsal CO TILLO         unitsal CO TILLO           unitsal CO TILLO         unitsal CO TILLO	V         Status         Y         Ea           Accises (VO)         SO         Accises (VO)         SO           Accises (VO)         SO         Accises (VO)         SO	06-0x30-08-x0-48-21 %. 08-06-80-08-x0-48-31 %. 06-0x30-08-x0-48-01 %.	Transport Pitro Olamad Pitro Olamad Pitro Olamad Pitro Olamad Pitro Olamad	Y	Name vertilika30011L0 vertilika30011L0 vertilika30011L0 vertilika30010L0	Y.	Patiental Hito No Hito	44

Step 4. Repeat Step 3 for any additional NVMe Fibre Channel Disks that have been provisioned.

Step 5. Click ACTIONS for the host and choose Storage > New Datastore... from the drop-down list.

Sphere Client Q. Search in all another								18.		MINE-SOLUTIX			* U	Γ
	10.1.168.111	ACTIONS												
Catagolive solutions local	Summary Monitor	C Actions - 10.1568.111		Datastores Networks Updates										
- B AS-VS - D BOUT	Storage Adapters Storage Eevices	6 <sup>8</sup> Deploy OVF Template (2) Item Resource Post.	14	die PERSONE										
0 10.1368.02 0 10.1368.02	Host Cache Configurat	12 New years.		Ť	LIN		Type	* Ce	-ity *	Datastore		Operational y State	Hardware Acceleration	i
D 101168.113	Protocol Endpoints VO Filters	(2 import VMs	15	044 (144 600604800844600005044460000018)	3		308	- 40	10.440	Not Consult	est (	Attached -	Supported	ł
30.1.968.314		Mantenance Mode	. 24	More-3300_MIPDGAV3401DSMGA3634E9M	6		dik	323	37.68	Not Consum	est -	Attached	Not suppo	ł
) G Test-Harness	Networking		7.4	MEY36450FQ.	0		396	321	37.08	Not Consum	ed. S	Attached	fect suppo	é
	Virtual switches	Connection	1.24	a (eu 0050es4400000000000060e808es4a0012)	0		0.0	5.0	5.18	hast Corouty	est -	Attached	Supported	ł
	Wheensi adapters	Power	1.24	# (%4.0050%94000000000000000000000000000000000			1004	5.0	2.78	Not Consum	est -	Attached	Supported	ł
	Physical adapters TCH/IP confeguration	Certificates	1 12	348 (144.60060e8008e848000050e84800000048	0		004	32.	0.00	Not Consum	ed.	Attached	Suportes	ł
	Virtual Machines	111.14M.1958	10	000 (100 000000000000000000000000000000	- 2		1910	5.0	5.78	VSICE	02	Attached	Supported	ļ
		Storage		Trew Datastore	0		endowe			Not Consum	ed .	Attuched	Not suppo	ł
	VM Shartus/Shutdowi Agent VM Settings	@ Add Networking		Q, Rescan Storage							-	in segn ( )		
	Default VM Compatibil Swep File Location	Host Profiles	2	And a second										
	System	Export System Logi												
	Literaing Hast Profile Time Configuration	Reconfigure for vSphere HA Ct: Assign License												
	Authentication Service Certificate	Settings		No itema sele										
	Power Management Advanced System Set System Besource Hea	Move To Tags & Custom Attributes												
	Frenad	Remove from Inventory												
	Services Security Profile	Add Permission												
	System Swap	Alarmis	3											

Step 6. Leave VMFS selected and click NEXT.

**Step 7.** Provide a name for the new datastore and select the LUN to use and click **NEXT**.

😑 Victore Client 🛛 🔘 (Serie) in America			
	€ g 10.1168.111   (scross)		
C BU G G · C Antonio catal · C Antonio ·	New Datastore 1. Turk 2. Kom and divide selection 3. Vold Summary 4. Parties and divide selection 4. Parties and divide selection	Name and device selection Series datasets are and a disk LIN for provisioning the datastore. Name            Name              view 0.001            Name	LUCE Di Ant Lanacetti Handred Samered Rull Di Igo Canacetti Handred Ramered Rull Di Igo Canacetti Handred Ramered Rectare page <u>20 c.</u> 100mm
	Second States		
A Deces Taxes Aleres			

- Step 8. Leave VMFS 6 selected and click NEXT.
- **Step 9.** Leave the Partition configuration with the default values and click **NEXT**.
- **Step 10.** Review the summary from Ready to complete and click **FINISH**.

#### **Step 11.** Repeat steps 5-10 for any additional LUNs provisioned.

## Hitachi Storage Provider for VMware vCenter Initial Configuration

To prepare the VSP storage system for vVols, the storage administrator must configure a custom resource group. Within the resource group, admins must map the appropriate LDEVs that support the vVol pool, as well as a range of LDEVs IDs which are reserved for vVols creation. Additionally, you must map a single protocol endpoint (PE) to each ESXi server within the cluster.

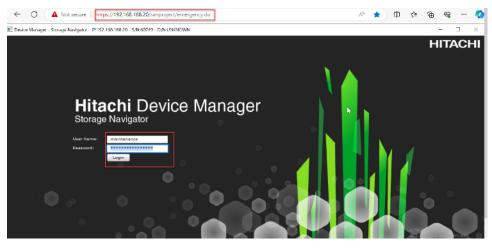
#### Procedure 1. Access Hitachi Storage Navigator

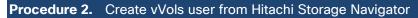
You can access the storage system using the Hitachi Storage Navigator web user interface, which runs on the SVP. To connect to the SVP, ensure that Adobe AIR from HARMAN needs to be installed and configured on your machine, For more information, see the section Installing Storage Device Launcher on the management client here: <a href="https://knowledge.hitachivantara.com/Documents/Storage/VSP">https://knowledge.hitachivantara.com/Documents/Storage/VSP</a> 5000 Series/90-07-0x/System Configuration/ 01 Accessing the storage system

After Adobe AIR from HARMAN is installed, you can proceed with the following steps to access Hitachi Storage Navigator.

Note: VSP E1090 will require an SVP to access Storage Navigator.

- **Step 1.** Using a web browser, navigate to https://[SVP-IP-ADDRESS]/sanproject/emergency.do.
- **Step 2.** Use the following credentials for the first-time login.
  - a. Username: maintenance
  - b. Password: raid-maintenance





**Step 1.** From the Hitachi Storage Navigator web user interface, select **Administration**.

Step 2.Expand Administrator User Group under the Users tab, and then click Create User under the<br/>Users tab.

								-
litachi Device Manager Storage Navigi				New Inc.	udelog RP-D	peration unlocked	Logged in as: mi	HITAC
Explorer	Administrator User Grou							/11/23 13:54 70 3
Storage Systems	User Groups > Administrate					1.12		
Analytics		- che orong	2					
isolation in the second s	Number of Roles				8			
Administration	Number of Resource Grou	<b>P</b> 4			2			
* 😽 User Groups	Number of Users				1 Built-in			
Administrator User Group	User Group Type All Resource Groups Assig	and .			Yes .			
Audit Log Administrator (View & Modify) U	All Resource Groups Assig	nieu.			145			
Audit Log Administrator (View Only) User	Users Roles Resou	rce Groups						
Security Administrator (View & Modify) Use								
Security Administrator (View Only) User O				tions *				Selected: 0 of 1
Storage Administrator (View& Modify) Use	& Filter ON CLE S	elect All Page	Column Settings			0	ptions w 10- 0-	1 71 (+ (+)
Storage Administrator (View Only) User G	User Name	1.4	Account Statue	Authentication	User Type	Number of User Groups	Account Version	Require Password C First Login
Support Personnel Group	a maintenance		Enabled	Local	Built-in		Ver.2	No
System User Group	i a maintenance		Enabled	LOCBI	Built-in		ver.z	NO NO
* Resource Groups								
* Cache Partitiona								
Sencryption Keys								
🔀 License Keys								
	1.5							
· · · · · · · · · · · · · · · · · · ·								
General Tasks								
General Tasks								
Create Host Groups								Windows

**Step 3.** Provide the following information:

- a. Enter the Username.
- b. Select the **Enable** option to activate the **Account Status**.
- c. Select Authentication as the Local option.
- d. Enter the Password and Re-enter Password.

Step 4. Click Finish.

Create User	TOX
1.Create User > 2	2.Confirm
Set values for the ne	ew user account and click Finish to confirm.
User Name:	vVols-user (Max 256 Characters)
Account Status:	💿 Enable 🔘 Disable
Authentication:	<ul> <li>Local</li> <li>External</li> </ul>
	Password: ******
	(8 - 256 Characters) Re-enter Password: *******
	Require Password Change on First Login: 💽 Yes 🔘 No
E-mail Address:	
	4 Back Next ▶ Finish Cancel ?

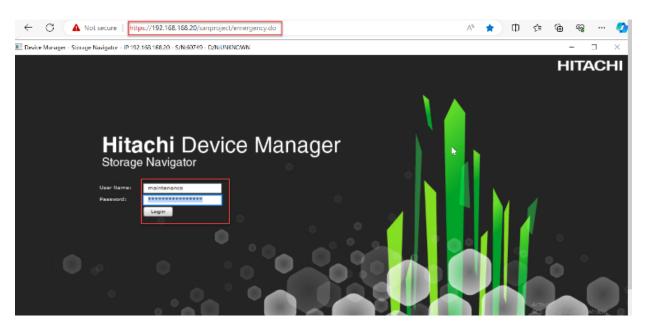
**Step 5.** Click **Apply** to create the Administrator User Account.

Create User	TOX
1.Create User > 2.Confirm	
Task Name: 231123-CreateUser (Max. 32 Characters)	click Apply to add task in Tasks queue for execution.
Selected User	
Item	Value
User Name	vVols-user
Account Status	Enabled
Authentication	Local
Password	•••••
User Group Name	Administrator User Group
Require Password Change on First Login	Yes
E-mail Address	•
Go to tasks window f	for status ( Back Next ) Apply Cancel ?

**Note:** If multiple Storage Providers for VMware vCenters are connecting to the storage, create a separate user account for each instance.

**Procedure 3.** Configure a Protocol Endpoint (PE) from Hitachi Device Manager - Storage Navigator

**Step 1.** Log in to **Hitachi Storage Navigator**.



Step 2. From the Navigation pane, select the General Tasks panel. Click Create LDEVs.

	VSP5500_NVMe ASE-47.11	2 G10(S/N:30595)	
Storage Systems	VSP5500_NVMe ASE-47.112 G10(	S/N:30595)	
* 🗊 VSP5500_NVMe ASE-47.112	Edit Storage System		
Masks 👔	Storage System Name	VSP5500_N	VMe ASE-47.112 G10
Reports	Storage System Type	VSP 5500H	
Components	Serial Number	30595	
🐕 Parity Groups	IP Address	172.25.47.	112
🌈 Logical Devices	Contact		
Pools	Location	G10	
Ports/Host Groups/iSCS			
' 🎆 External Storage	Allocation Summary		
Replication	Internal/External : Total	+ Open/Mainfrar	ne: Total 🛛 🗸
	Physical Summary		
		Allocated	
		Reserved	B Used DP Pool
	<		Unused DP Por
	F		D Other
		Available Space	Unallocated
			Unallocated
		Available Space Physical Total	
Analytics	Virtual Summary	Physical Total	
		Physical Total DP Allocated	
Analytics Administration ~		Physical Total DP Allocated DP Unallocated	
Analytics		Physical Total DP Allocated	

#### **Step 3.** Provide the following details:

- a. Select ALU from the Provisioning Type drop-down list.
- b. Enter the value **1** in the **Number of LDEVs** field. **Note**: You only need one ALU.
- c. Enter the LDEV name in the LDEV Name Prefix field.
- d. Click Add.

te LDEVs										TE
eate LDEVs > 2.Cor	firm									
s wizard lets you create k Finish to confirm the	and provision LDEVs enter creation, or click Next if you	the information for LDEVs you wa want to add LUN paths for the Li	int to create, and then clic DEVs.	k Add.	Click Options t	o expand the	LDEV setting	s.		
Provisioning Type:	ALU		-	s	elected LDE\	/s				
	Contraction			Se	lect All Pages					Options w
Number of LDEVs:	1 (1*60)				LDEV ID	LDEV Name	SSID	CLPR	MP Unit ID	Resource G Name (ID)
LDEV Name:	Prefix	Initial Number								
	VVOL-ALU									
	(Max. 32 characters t or blank)	otal including max. 9-digit numb	ar,							
¥ Options										
			Add 🕨				No	Data		
				< (		Change LDEV !	Settings	Remove	Salacta	d: 0 of 0

Step 4. The Selected LDEVs pane shows the PE created. Click Next to continue.

ate LDEVs > 2.Conf										
								_		
		er the information for LDEVs you wa ou want to add LUN paths for the LD		Add.	Click Options t	o expand the LD	EV setting	B.		
Provisioning Type:	ALU		(w)	s	elected LDEV	ls				
	Contraction of the second			Se	lect All Pages					Options
Number of LDEVs:	(1-59)			2	LDEV ID	LDEV Name	SSID	CLPR	MP Unit ID	Resource ( Name (ID)
	(1.00)				00:00:22	WOL-ALU	0004	0:CLPR0	Auto	meta_reso
LDEV Name:	Prefix	Initial Number								
	(Max. 32 character or blank)	s total including max. 9-digit numbe	r.							
S Options										
			Add 🕨	]						
				< 6		Change LDEV Se		Remove		d: 1 of 1

**Step 5.** Select the checkboxes for the available VSI **Host Groups** created from the Ops Center Administrator for the cluster.

Step 6. Click Add to move host groups to Selected Host Groups.

	5									T
Create LDEVs	> 2.Select LDEVs > 3.Sele	ct Host Groups / ISCSI Targets	> 4.View/Chang	e LUN Paths >	5.Confirm					
		roups list, and then click Add. If ost groups or ISCSI Targets to LU		SCSI targets, se	elect iSCSI from	Selection Object, select	ISCSI targets fro	m the Available	e iSCSI Target	s list,
Selection Obj Host Groups:		251								
Available	Host Groups				Selected I	lost Groups				
☆Filter Of	OFF Select All Pages	Options 🗸 📧 🐔 1	/1 > -1		Select All Pa	ges				_
Port ID	Priority order for provisioning	Host Group Name	Host Mode		Port ID	Host Group Name	Host Mode	Port Attribute	Port Security	Numb Hosts
CL1-A		VSI_x210_M7_01_Fab_A (	21 [VMware							
CL1-A		VSI_x210_M7_02_Fab_A (	21 [VMware							
CL1-A	1	VSI_x210_M7_03_Fab_A (	21 [VMware							
CL1-A		VSI_x210_M7_04_Fab_A (	21 [VHware							
CL3-A		VSI_x210_M7_01_Fab_B (	21 [VMware							
CL3-A		VSI_x210_M7_02_Fab_B (	21 [VMware	-						
CL3-A		VSI_x210_M7_03_Fab_B (	21 [VMware							
SL3-A	1	VSI_x210_M7_04_Fab_B (	21 [VMware	Add 🕨						
CL2-A	2	VSI_x210_M7_01_Fab_A (	21 [VMware		1					
CL2-A		VSI_x210_M7_02_Fab_A (	21 [VMware	4 Remove		1	Jo Dat			
CL2-A	2	VSI_x210_M7_03_Fab_A (	21 [VMware	-		1	NO Dat	.cl		
CL2-A		VSI_x210_M7_04_Fab_A (	21 [VMware							
CL4-A	2	VSI_x210_M7_01_Fab_B (	21 [VMware							
CL4-A	2	VS1_x210_M7_02_Fab_B (	21 [VMware							
SL4-A	2	VSI_x210_M7_03_Fab_B (	21 [VMware							
CL-I-A		VSI_x210_M7_04_Fab_8 (	21 [VMware	1						

Step 7. Click Next.

Valiable Host Groups   Riter Groups   Priority order for and the st Mode   A A A VSI_v210_M7 21 [VMware Target Enabled Mr.   V C1.1-A VSI_v210_M7 21 [VMware <		ti 🛞 Fibre 🔘 ISC	51									
Alter       Options       I <th< th=""><th>st Groups:</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>	st Groups:											
Port ID       Priority order for provisioning       Host Group Name       Host Mode       Port Mode		and the second se						the boltomer to first an article	_	_	_	_
Port ID       Port ID       Mat Group Name       Hoat Mode       Attribut       Security       Mit         Port ID       Port ID       Mat Group Name       Hoat Mode       Attribut       Security       Mit         Port ID       Mat Group Name       Hoat Mode       Victor       Target       Enabled       Port ID       Mat Group Name       Hoat Mode       Attribut       Security       Mit         Port ID       Mat Group Name       Mode       Victor       Target       Enabled       Forbled	Critter Territ		opuons + (reject +	X * [52](20)		Sel	ect All Page	15			11.000	
Image: Section of the section of th	Port ID		Host Group Name	Host Mode		1	Port ID	Host Group Name	Host Mode			Numb
Image: Second							CL1-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Adb       V       CL1-A       VST_x210_M7       21 [VMware       Target       Enabled       Image: Classical State						~	CL1-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Add       V       CL3-A       VSL_S210_M7       21 [VMware       Target       Enabled       Image: Classical State						~	CL1-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Add       V       CL3-A       VSI_x210_M7       21 [VMware       Target       Enabled       Image: Classical Science Scie						~	CL1-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Add >       V       CL3-A       VST_x210_M7       21 [VMware       Target       Enabled       I         Add >       V       CL3-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL3-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL3-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL2-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL4-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL4-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V       CL4-A       VST_x210_M7       21 [VMware       Target       Enabled       I         V <td></td> <td></td> <td></td> <td></td> <td></td> <td>~</td> <td>CL3-A</td> <td>VSI_x210_M7</td> <td>21 [VMware</td> <td>Target</td> <td>Enabled</td> <td></td>						~	CL3-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Add       V       CL3-A       VS1_x210_M7       21 [VMware       Target       Enabled         NO Data       V       CL2-A       VS1_x210_M7       21 [VMware       Target       Enabled         V       CL4-A       VS1_x210_M7       21 [VMware       Target       Enabled						~	CL3-A	V51_x210_M7	21 [VMware	Target	Enabled	
Image: Constraint of the second se						$\checkmark$	CL3+A	VSI_x210_M7	21 [VMware	Target	Enabled	
Image: Second					-00 F	$\checkmark$	CL3-A	VSI_x210_M7	21 [VMware	Target	Enabled	
Volume						$\checkmark$	CL2-A	VSI_x210_M7	21 [VMware	Target	Enabled	
CL2-A       VSI_SZ10_M7       Z1 [VMware       Target       Enabled         CL4-A       VSI_SZ10_M7       Z1 [VMware       Target       Enabled         CL4-A       VSI_SZ10_M7       Z1 [VMware       Target       Enabled		No	Data		Remove	~	CL2-A	VSI_x210_M7	21 [VMware	Target	Enabled	
V     CL4-A     VST_x210_M7     21 [VMware     Target     Enabled		NO	Data			$\checkmark$	CL2-A	VSI_x210_M7	21 [VMware	Target	Enabled	
V         CL4-A         VSI_x210_M7         21         Target         Enabled           V         CL4-A         VSI_x210_M7         21         IVMware         Target         Enabled						$\checkmark$	CL2-A	VSI_x210_M7	21 [VMware	Target	Enabled	
CL4-A VSI_v210_M7 21 [VMware Target Enabled						$\checkmark$	CL4-A	VSI_x210_M7	21 [VMware	Target	Enabled	
						~	CL4-A	VSI_x210_M7	21 [VMware	Target	Enabled	
V CLAR WIT-COOLUT OF DURING THESE TRANSPORT						$\checkmark$	CL4-A	VSI_x210_M7	21 [VMware	Target	Enabled	
CLE-X VSI_XZIO_M/ ZI_LYMWare larget Enabled						$\checkmark$	CL4-A	VSI_x210_M7	21 [VMware	Target	Enabled	
				-								

**Step 8.** (Optional) Ensure you use the scrollbar at the bottom of the dialog to double-check that all **Host LUN IDs** are set consistently across all paths. To do this, select the **checkbox for all ports/paths listed**, select **the checkbox for the LDEV ID**, and then click **Change LUN IDs** to make changes.

reate LDEVs	-										TO
Create LDEVs > 2.5	elect LDEVs	> 3.Select Hor	it Groups / ISCSI	Targets > 4.Vie	w/Change LU	N Paths > 5.C					
The LUN IDs are auto and select LDEVs you							check box fo	r the host grou	p (in the table subheadin	g) you want to chang	e.
JUNs:											
Added LUNs			_	_	_	_	_	_			
&Filter ON OFF	Select All I	Pages	1						Townshit Reads	ons <b>y</b>   €   €   1	/1 + 91
	LDEV	Parity	Pool Name	Emulation		Deputation from			LUN ID(16 Sets of I		
LDEV ID	Name	Group ID	(ID)	Type	Capacity	Provisioning Type	Attribute	T10 P1	CL1- A/VSI_x210_M 7 01 Fab A	CL1- A/VSI_x210_M 7.02 Eab A	CL1- A/VSI_x210 7.03 Fab.
00:00:22	WOL-ALU		1	OPEN-V CVS	1	ALU	ALU		4	4	4
					-						
							-				
			1		k.	_					>
Change LDEV Sett	ings Char	nge LUN IDs								Select	ed: 1 of 1
				_	_	_	_	_	_		
									( Back	Next ) Finish	Cancel ?

### Step 9. Click OK.

Change LUN ID	5	TOX
Set the initial LU	N ID.	
Initial LUN ID:	4	
	(0-4095, Decimal input)	
	OK (	Cancel ?
	ок	Cancel ?



			t Groups / iSCSI 1								
			k Change LUN by cli ck Change LUN ID:				check box for	the host group	p (in the table subheadin	g) you want to change	≥,
Ns: Added LUNs											
Filter ON OF	Select All F	ages							Optic	ons 🔻 🗲 1	/1 → →
									LUN ID(16 Sets of F	Paths)	
LDEV ID	LDEV Name	Parity Group ID	Pool Name (ID)	Emulation Type	Capacity	Provisioning Type	Attribute	T10 PI	CL1- A/VSI_×210_M 7_01_Fab_A	CL1- A/VSI_×210_M 7_02_Fab_A	CL1- A/VSI_x21 7_03_Fab
00:00:22	VVOL-ALU	-	-	OPEN-V CVS		ALU	ALU	-	4	4	4
						_					
Change LDEV S	attings I Chan	ge LUN IDs				-				Select	ed: 1 of 1

**Step 11.** Click **Apply** to create the LDEV and add paths to the UCS servers.

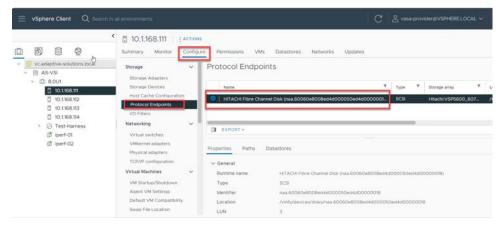
	231221	CreateLDEVs											
	(Max. 3	2 Characters)											
Selected	LDEVs												
LDEV ID	LDEV Name	Provisio Type	ning SSID	MP Unit ID	Resource Grou Name (ID)	P Virtual Sto	orage Machine				CLPR		
00:00:22	VVOL-	ALU ALU	0004	Auto	meta_resource	(0) VSP 5200.	5600 / 60749				0:CLPR0	1	
	_			-		-							
												Total	
							_		_			Totalı	
Added L	depend of		LDEV	Host Group	Parity	Pool Name	Emulation		Provisioning				
Added L	JNS LUN ID	LDEV 1D	LDEV Name	Host Group Name	Parity Group ID	Pool Name (ID)	Emulation Type	Capacity	Provisioning Type	Attribute	ALUA Mode	Totalı Asymm Access	
Port ID CL1-A	LUN ID	00:00:22	Name VVOL-ALU	Name VSI_x210	Group ID		Type OPEN-V CVS	Capacity	Type	ALU	Disabled	Asymm	
Port ID CL1-A CL1-A	LUN ID 4 4	00:00:22	Name VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210	Group ID - -	(ID) - -	Type OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU	ALU	Disabled Disabled	Asymm	
Port ID CL1-A CL1-A CL1-A	LUN ID 4 4 4	00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210 VSI_x210	Group 1D - -	(ID) - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU	ALU ALU ALU	Disabled Disabled Disabled	Asymm	
Port ID CL1-A CL1-A CL1-A CL1-A	LUN ID 4 4 4 4	00:00:22 00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210 VSI_x210 VSI_x210	Group 10	(ID) - - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU ALU	ALU ALU ALU ALU	Disabled Disabled Disabled Disabled	Asymm	n
Port ID CL1-A CL1-A CL1-A CL1-A CL1-A	LUN ID 4 4 4 4 4 4	00:00:22 00:00:22 00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210 VSI_x210 VSI_x210 VSI_x210	Group 1D - -	(ID) - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU ALU ALU	ALU ALU ALU ALU ALU	Disabled Disabled Disabled Disabled Disabled	Asymm	
Port ID CL1-A CL1-A CL1-A CL1-A	LUN ID 4 4 4 4	00:00:22 00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210 VSI_x210 VSI_x210	Group 10	(ID) - - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU ALU	ALU ALU ALU ALU	Disabled Disabled Disabled Disabled	Asymm	n
Port ID CL1-A CL1-A CL1-A CL1-A CL1-A	LUN ID 4 4 4 4 4 4	00:00:22 00:00:22 00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU	Name VSI_x210 VSI_x210 VSI_x210 VSI_x210 VSI_x210	Group 1D - - - - -	(10) - - - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU ALU ALU	ALU ALU ALU ALU ALU	Disabled Disabled Disabled Disabled Disabled	Asymm	
Port ID CL1-A CL1-A CL1-A CL1-A CL1-A CL3-A	LUN ID 4 4 4 4 4 4 4	00:00:22 00:00:22 00:00:22 00:00:22 00:00:22 00:00:22	Name VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU VVOL-ALU	Name           VSI_x210           VSI_x210           VSI_x210           VSI_x210           VSI_x210           VSI_x210           VSI_x210	Group 1D - - - - - - - -	(ID) - - - -	Type OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS OPEN-V CVS	Capacity	Type ALU ALU ALU ALU ALU ALU ALU	ALU ALU ALU ALU ALU ALU	Disabled Disabled Disabled Disabled Disabled Disabled	Asymm	

#### Procedure 4. Verify that the PE is Available and Visible

Verify that the protocol endpoint (PE) is visible in vSphere. On the storage system, the PE is the administrative logical unit (ALU) that the storage administrator presented to vSphere Cluster/ESXi hosts in the prior procedure.

Step 1. Log in to the vSphere Client, select Inventory from Home tab, and then select an ESXi host.

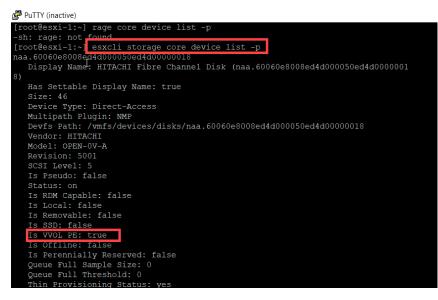
Step 2. Select Protocol Endpoints under the Configure tab.



**Step 3.** (Optional), Using the ESXi host root console, you can view the protocol endpoints (PEs) by running the following command from the esxcli command line.

#esxcli storage core device list -p

This will display the devices that are recognized as PEs. Note the Is VVOL PE=True value.



Procedure 5. Initialize Parity Groups with Hitachi Ops Center Administrator

Configuration steps in this section assume that Parity Groups have already been created by Hitachi professional services or using Hitachi Storage Navigator. For initializing Parity Groups from Hitachi Ops Center Administrator, proceed with the following steps:

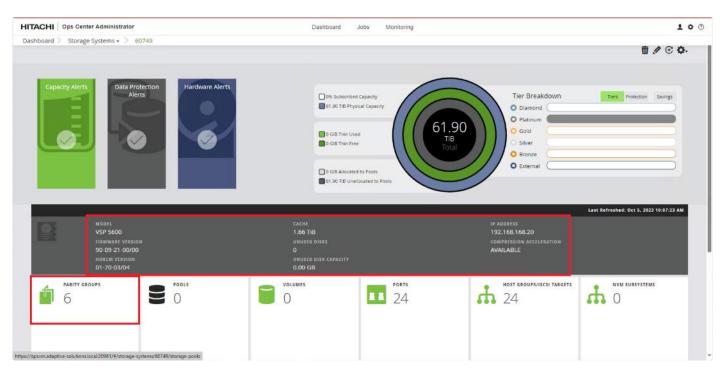
# Step 1.Log in to Hitachi Ops Center Administrator and select Storage Systems from the navigationpane.





5								
5								
a Protection Alerts	Hardware Alerts	C G/B Thin	Physical Capacity Used Free ated to Pools	61.90 TB Total	Tier Breakdowr O Diamond P Flaenum G Gold Silver B Bronze External S SDS	1 Twy	Protection Savings	
								4
IP ADDRESS	MODEL	TOTAL	THIN FREE	THIN USED	USAGE	INCOMPLETE HA ARRA	Y MIGRATION TA	ASK COUN
192.168.168.20	VSP 5600	61.90 TIB	0.00 GIB	0.00 GIB	0.96		0	
						show 20	0 🕶 items	- 11
	Alerts	Alerts Alerts Alerts Alerts Alerts MOEL MOEL	Merts         0% 54bsc           0% 54bsc         0% 54bsc           0 G 8 Han         0 G 8 Han           0 G 8 Han         0 G 8 Han <tr< td=""><td>Nerts CONS Subscribed Capacity CONS Subscr</td><td>Alerts         Image: Constraint of the state of th</td><td>Alerts</td><td>Merts       Image: Construction of Capacity       Image: Construle of Capacity       Image: Construction of</td><td>Merts       Oth Subscribed Capacity       Ter Breakdown       Ter S Protector       Scores         0 06 Subscribed Capacity       0 68 Thin Used       0 68 Thin Used       0 68 Thin Used       0 68 Allocated to Pools       0 68 Allocated to Pools       0 50 S         10 068 Allocated to Pools       0 68 Allocated to Pools       0 50 S       50 S       0 50 S         12 ADDREss       MODEL       TOTAL       THIN FREE       THIN USED       USAGE       INCOMPLETE HA ABBAY       MIGRATION 1/2         192.168.168.20       VSP 5600       61.90 TIB       0.00 GIB       0.00 GIB       0 %        0</td></tr<>	Nerts CONS Subscribed Capacity CONS Subscr	Alerts         Image: Constraint of the state of th	Alerts	Merts       Image: Construction of Capacity       Image: Construle of Capacity       Image: Construction of	Merts       Oth Subscribed Capacity       Ter Breakdown       Ter S Protector       Scores         0 06 Subscribed Capacity       0 68 Thin Used       0 68 Thin Used       0 68 Thin Used       0 68 Allocated to Pools       0 68 Allocated to Pools       0 50 S         10 068 Allocated to Pools       0 68 Allocated to Pools       0 50 S       50 S       0 50 S         12 ADDREss       MODEL       TOTAL       THIN FREE       THIN USED       USAGE       INCOMPLETE HA ABBAY       MIGRATION 1/2         192.168.168.20       VSP 5600       61.90 TIB       0.00 GIB       0.00 GIB       0 %        0

**Step 3.** Click the **PARITY GROUPS** icon under the selected storage system to view parity groups.



**Step 4.** Click any **Parity Group ID** to initialize it as parity for creating the vVol volume pool. From the **Ac-tions** pane click **Initialize Parity Groups.** 

HITACHI	Ops Center Administrator			Dashboard	d Jobs Monitoring				10
Dashboard )	Storage Systems + > 6	0749 👌 Parity Groups 👻							
Parity	/ Groups								Ģ
Summary									
Actions									
Initialize Par	ity Groups								
	pression on Parity Groups	RAID TYPE	DISK TYPE	TOTAL CAPACITY	UNINITIALIZED CAPACITY	INITIALIZED	USED	COMPRESSION	USAGE
0 1-1	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB	-	100%
D 1-2	IN_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 TIB		100%
) 1-3	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		095
O 1-4	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB	-	095
O 1-5	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
) 1-6	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB	0.00 GIB	0.00 GIB		0%
5 items 1 selec	cted								show 200 🗸 items »

Step 5. Click OK.

Dashboard	Storage Systems + ) 6	0749 ) Parity Groups -							
Parit	ly Groups						×		ţ
			🔒 In	tialize Parity	Groups Confir	mation			
Summary				he selected 1 parity gro	ups in the current storage s	vstem will be			
Actions				itialized. Do you want					
Initialize P	arity Groups								
Enable Co	mpression on Parity Groups	RAID TYPE	DISK TYPE		Cancel OK •		USED	COMPRESSION	USAGE
34	IN_USE	RAID6 6D+28	S5D NVMc 1.90 T6	10/32 116	3.00 MIB	0.00 616	10.92 116	24	10096
142	(N_USE	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	3.00 MIB	0.00 GIB	10.32 718		100%
1-3	LININITIALIZED	RAID6 6D 2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 110	0.00 G/B			096
1.4	UNINITIALIZED	RAID6 6D+2P	SSO NVMe 1.90 TB	10.32 118	10.32 118	0.00 618	0.00 GIB		0%
	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 78	10.32 TIB	10.32 TIB	0.00 GIB	0.00 G/B		C%
	UNINITIALIZED	RAID6 6D+2P	SSD NVMe 1.90 TB	10.32 TIB	10.32 TIB				0%

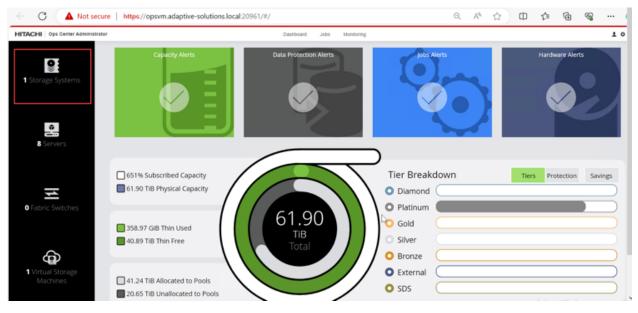
**Note:** Created Parity Groups have status as UNINITIALIZED and after it gets initialized completely, the status should change to IN\_USE.

#### Procedure 6. Create a Dynamic Provisioning Pool for vVols

When creating a pool, use the Basic option to take advantage of tiers of storage available on the VSP that are based on best practices. By default, the basic option will create a Hitachi Dynamic Provisioning Pool.

If you want more flexibility and do not need to take advantage of best practices, you can use the advanced option to select specific Parity Groups and define your pool types as either Tiered, Thin, or Snap.

**Step 1.** On the **Ops Center Administrator dashboard**, click **Storage Systems** to see the inventory of registered storage systems.



Step 2. Click the S/N listing of the Storage System.

Storage Systems     Submitted     Image: Storage Systems     Ima	HITACHI Ops Center Administrator	Dashboard Jobs Montoring		100
	Storage Systems			
	Fsammary			
Q. D name sine ipadoress woons, total. Their been their used brace incomplete ha areay wickation laye co		61.50 TB Physick Capacity     214.50 GB Thin laived     2041 TB Thin have     2062 TB Allocated to Prote	Diamond     Triatnum     Gold     Silver     Otrone     trone     trone     trone	Ters Prosection Survey
) NAME 5/% IP ADDRESS ANDORL TOTAL THIN FRED THIN USED WAACE INCOMPLETE HA ARBAY MICRATION JASH CO	T D Actors			3
	2			
	) NAME S/W IP ADDRESS MODEL	TOTAL THIN FREE THIN USED	USAGE INCOMPLETE	NA ARRAY NIGRATION TASK COUNT
10/19 132-168-168-20 139-5000 01-30 110 21-139 dib 0-14 - 0		61.90 TIB 20.41 TIB 214.39 GIB	0.% -	0

Step 3. From the storage system, click Pools.

HITACHI Ops Center Administrator	Dashboard Jobs Monitoring	100
Dashboard > Storage Systems + > 60749		
AA22-5600		± 1 € \$-
Copacity Alerts Alerts	S27% Subcorbed Capacity G 150 TIR Physical Capacity C 214,39 Gill Thin Used 20.41 TiB Thin Free C 20.62 TIB Allocated to Pools G 41.27 TIB Unaflocated to Pools	1.90     Diamond       0 Diamond     Oild Control       0 Gold     Silver       0 Bronze     External
AA22-5600		Lust Refreshed: Nov 16, 2023 2:02:51 AM
морт. VSP 5600 Frankwait vy isson 99 09 21 100/00 ноокск и указол 01-70 03/04	c cami 1.66 TIB umusto acsks 0 umusto acsk canacity 0.00 G8	IF ADDRESS 192,188,168,20 COMPRESSION ACCELERATION AVAILABLE
6 PARITY GROUPS POOLS 2	6 PORTS 24	Host Groupsrisch Targetts       NVM SUBSYSTEMS         40       0         Activate Windows       Go to Settings to activate Windows.

**Step 4.** Click the plus sign (+) to open the **Create Storage Pool** window.

#### HITACHI Ops Center Administrator

Dashboard	> Storage Systems • > 60749	> Pools +	
Pool	S		
▼ Summary	Capacity Alerts		
+ 🗊 🤈	Actions		
Q Create	Storage Pool		
O 10	NAME	TYPE	ACTIVE FLASH
0 0	UCS_Boot_Pool	Thin	No
0 1	UCS Application Pool	Thin	No

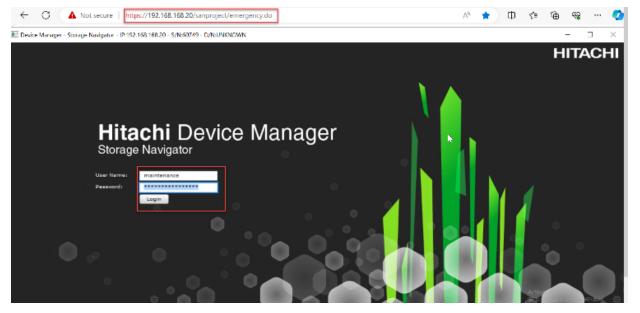
Step 5. Enter the following details and click Submit.

- a. Enter **POOL NAME** as vVOL\_Dynamic\_Pool (Pool names can contain alphanumeric characters, hyphens, and underscores only. Initial hyphens are not allowed.)
- b. Click an available Tier to view the available storage capacity and select the available capacity.
- c. Review the **high and low pool utilization thresholds**. By default, the utilization threshold low is set to 70% and high respectively at 80%. If required, you can modify thresholds to receive notifications for the thresholds that meet your environment needs.
- d. To specify over allocation, you can set the limit to Unlimited.
- e. Click Submit.

HITACHI Ops Center Administrator		Jobs Monitoring	
Dashboard > Storage Systems -> 60749 > Pools -> Cr       Create Pool	eate Pool		
	Basic	Ad	vanced
POOL NAME WOL_Dynamic_Pool STORAGE SYSTEM 60749	Select capacity from Tiers to alloca DIAMOND 0.00 GIB	ate to Pool	Tier Management 0.00 GiB Available ~
USE FOR SNAP?	10.32 TIB		10.32 TiB Available
Yes No BREAKDOWN OF DISKS Total: 10.32 TiB Platinum: 10.32 TiB (100.00 %)	GOLD 0.00 GIB SILVER 0.00 GIB		0.00 GIB Available 0.00 GIB Available
	0.00 GIB		0.00 GiB Available V
	UTILIZATION THRESHOLD (LOW) %	UTILIZATION THRESHOLD (HIGH) % 80 If this threshold is exceeded, snapshots will be disabled to ensure there is enough capacity for user data.	SUBSCRIPTION LIMIT
			Cancel Submit Tor

Procedure 7. Create vVols Resource Group from Hitachi Storage Navigator

Step 1. Log in to Hitachi Device Manager- Storage Navigator.



Step 2. Expand Administration, select Resource Groups, and click Create Resource Groups.

#### E Device Manager - Storage Navigator - IP:192.168.168.20 - 5/N:60749 - D/N:AA22-5600

xplorer	Re	source Groups							Last Update
Storage Systems	Re	source Groups							
Analytics		Number of Resource Gro	NIPS			1	(Max Allowed: 10	24)	
Administration	R	esource Groups							
1 . Resource Groups		Create Resource Group	Edit Resourc	e Group Delet	e Resource Gr	oups Export	1		
Cache Partitions		AFilter ON CT	Select All Pages	Column Settings					Options w
Cherryption Keys		Resource Group	Number of User Groups	Number of Parity Groups	Number of LDEVs	Number of Porta	Number of Host Groups	Number of (SCSI Targets	
		A meta mainum	9	6	65280	24	5100	3	

**Step 3.** Enter the Resource Group Name and click **Select LDEVs**.

Devic	Manager - Storage Navigator - IP:192.168.168.20 - S/N:60749 - D/N:AA22-5600
Hit o	eate Resource Groups
	Seate Resource Groups > 2.Confirm
	his wizard lets you create resource groups. Click each button to select parity groups, LDEVs, p
-	Resource Group Name: VVols-RG (Max. 32 Characters)
	Parity Group Selection:
	Select Parity Groups
	Total Selected Parity Groups: 0
	LDEV Selection:
	Select LDEVs
	Total Selected LDEVs: 0
	Port Selection:
	Select Ports
	Total Selected Ports: 0
	Host Group Selection:
	Select Host Groups
	Total Selected Host Groups: 0
	ISCSI Target Selection:
G	Select iSCSI Targets
1	Total Selected ISCSI Tamets: 0
9.000	

**Step 4.** Select an available range of **LDEV IDs for reservation** from the **Available LDEVs** tab, including the LDEVs created in the prior vVol pool step. Click **Add**.

Available LDEV	s			1	Selected LDE	Vs	_			
RFilter ON OFF	Select All Pages	Options 👻 😥 🗧	1 / 66 🌶 🖻		Select All Pages					Options 👻
LDEV ID	LDEV Name	Parity Group ID	Pool Name(ID)		LDEV ID	LDEV Name	Parity Group ID	Pool Name(ID)	Capacity	Namesp ID
00:00:20	vVol_Pool_LDEV0	1-6	vVol_Application							
00:00:21	vVol_Pool_LDEV1	1-6	vVol_Applicatio							
00:00:22		-	-							
00:00:23										
00:00:24	2									
00:00:25	1									
00:00:26		-	1.							
00:00:27			021.							
00:00:28		-								
00:00:29		-		-						
00:00:2A	19 (B)	1		Add )	1					
00:00:28	1. C.	2								
00:00:2C				Pressential			No D	ata		
00:00:20			and the second s	< Remove			110 0	547. 54 547		
00:00:2E			-2							
0010012F		2	1.42							
00:00:30										
00:00:31	÷:									
00:00:32										
00:00:33			1.20							
00:00:34			-							
00:00:35										
00:00:36										
00:00:37										
00:00:38										
00:00:39	÷.									
1			,		<		1			
		Selec	ted: 26 of 65246		11517				Selected	0 of 0



Click **OK** to reserve the selected LDEVs to the **Resource Group**.

Avallable	LDEVs				s	elected LDEV	ls				
R Filter 0	N OFF Select All Pages	Options 👻 😥 🗧 1	1 / 66 🤿 🔿		Se	lect All Pages				Option	5 W
LDEV 10	LDEV Name	Parity Group ID	Pool Name(ID)		⊻	LDEV ID	LDEV Name	Parity Group ID	Pool Name(ID)	Capacity	Na ID
00:00:3	IA -	20	. 0			00:00:20	vVol_Pool_LDEV0	1-6	vVol_Applic	500.00 GB	-
00:00:3	- 18	-	14		~	00:00:21	vVol_Pool_LDEV1	1-6	vVol_Applic	500.00 GB	
00:00:2	ic +	*	()e		$\checkmark$	00:00:22		-		0	-
00:00:3	- G	•	-		$\checkmark$	00:00:23		-		1	-
00:00:3	ie -	-1	27		$\checkmark$	00:00:24					
00:00:3	IF -	•	-		~	00:00:25					
00:00:4		20	52			00:00:26	12	-			
00:00:4	-	*	- C4		$\checkmark$	00:00:27		-	1.0	-	
00:00:4		÷)	9		$\checkmark$	00:00:28		-		-	-
00:00:4	-	*	•	-	$\checkmark$	00:00:29			-		
00:00:4	14 -	5	67	Add )	$\checkmark$	0010012A	1				
00:00:4	-	*:		ADD F	$\checkmark$	00:00:28	1	-	10		
00:00:4				-	$\checkmark$	00:00:2C	14	-	24 - C	-	-
00:00:4	17 -		-	Remove	1	00:00:20	3	6	14		
00:00:4	- 18	-2	32		$\checkmark$	00:00:2E					
00:00:4	19 -				$\checkmark$	00:00:2F					
00:00:4	iA t	10	13		$\checkmark$	00:00:30	i Per	2			
00:00:4		•			$\checkmark$	00:00:31		-			-
00:00:4	ic -				~	00:00:32	(e)				
00:00:4	iD -	-	-		~	00:00:33					
00:00:4	е -	2	3 <b>4</b>		$\checkmark$	00:00:34	1	1		353	
00:00:4	ιF -	*	÷		$\checkmark$	00:00:35		-			-
00:00:5	io -	<del>,</del> 23	÷		$\checkmark$	00:00:36					
00:00:		-			$\mathbf{\mathbf{v}}$	00:00:37	-				
00:00:5	52 -	-				00:00:38					
00:00:5	i3 •				V	00:00:39		3		j j	
	*		, v		4.6						

Step 6. After the LDEVs selection is completed, click Add.

ite Resource Groups								
eate Resource Groups > 2.Confirm								
s wizard lets you create resource groups. Click each button to select parity groups. LDEVs.	ports, host group	and	ISCSI targets to be	added to the resou	irce group an	d click Add. Click	c Finish to confirm.	
Resource Group Name: vVols-RG		s	elected Resource	Groups				
(Max. 32 Characters)		Se	lect All Pages					Ļ
Parity Group Selection:			Resource Group Name (ID)	Number of Parity Groups	Number of LDEVs	Number of Ports	Number of Host Groups	
Select Parity Groups         0								
LDEV Selection:								
Total Select LDEVs: 26								
Port Selection:								
Select Ports         0	Add 🕽	1		No	Data	a		
Host Group Selection:	-				000			
Select Host Groups Total Selected Host Groups: 0								
ISCSI Target Selection:								
Select iSCSI Targets: 0								
		< 6						
			Detail Remove				Selected: 0 of	D.

**Step 7.** The created **Resource Group** is visible under the **Selected Resource Groups** pane, and the **Number of LDEVs** are presented as selected. Click **Finish.** 

Resource Group Name: vVols_RG	1	S	elected Resource	Groups			
(Max. 32 Characters)		Se	lect All Pages				
Parity Group Selection:		2	Resource Group Name (ID)	Number of Parity Groups	Number of LDEVs	Number of Ports	Number of Host Groups
Select Parity Groups: 0	- H		vVols_RG (-)	0	26	U	
DEV Selection:	 						
Select LDEVs Total Selected LDEVs: 0							
Port Selection:	-						
Select Ports Total Selected Ports 0	Add 🕨	1					
Host Group Selection:	7						
Select Host Groups: 0	3						
SCSI Target Selection:	-						
Total Selected ISCSI Targets: 0							

Step 8. Click Apply.

ate Resource							
eate Resource	Groups > 2.Conf						
ter a name for	the task. Confirm t	he settings ir	n the list ar	nd click Apply to a	dd task in Tasks (	queue for execution	to.
sk Name:	231221-Create	ResourceGrou	aps				
	(Max. 32 Chara	cters)					
Create Re	source Groups		_				
Resource Name (1			lumber of LDEVs	Number of Ports	Number of Host Groups	Number of ISCSI Targets	
VVols_R	G (-)	0	26	0	0	0	
Detail							Totali 1
Detail							Totai: 1

#### **Procedure 8.** Deploy Storage Provider for VMware vCenter

Storage Provider for VMware vCenter is deployed using an OVF template. You can obtain the binaries from your Hitachi representative or download the latest OVF file from - <u>Support | Hitachi Vantara</u>.

This virtual machine is typically deployed into the vSphere management cluster where the vCenter Appliance (VCSA) is deployed. You can also deploy this virtual machine to any vSphere environment if it has network access to the VSP storage.

Step 1. Log in to VMware vSphere web client.

VMware <sup>®</sup> vSphere	
Administrator@vsphere.local	
Use Windows session authentication	
LOGIN	

Step 2. From the vCenter Dashboard, right-click Management Cluster and select Deploy OVF Template.

$\equiv$ vSphere Client $$ Q Search in all environme	[]] Actions - 8.0U1 ]* Add Hosts	
	🗟 New Virtual Machine 🥭 New Resource Pool	
✓	🤃 Deploy OVF Template	
<ul> <li>✓ III AS-VSI</li> <li>→ III 8.0U1</li> </ul>	문 <mark>.</mark> New vApp	
	댭 Import VMs	
	Storage >	
	Host Profiles >	
	Edit Default VM Compatibility	

#### Step 3.

Select the Local File, click UPLOAD FILES, and then select the respective OVA. Click Next.

Deploy OVF Template	Select an OVF template Select an OVF template from remote URL or local file system	×
1 Select an OVF template	Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
2 Select a name and folder	O URL http://remoteserver-address/filetodeploy.ovf  _ova	
3 Select a compute resource	http://temateserver-adoress/tiletodeploy.ov/1.jova	-
4 Review details	Local file     UPLOAD FILES     HitachiStorageProvider_3.7.3-00.ova	
5 Select storage		
6 Ready to complete		
	CANCEL	

**Step 4.** Provide the name of the virtual machine and select the management cluster. Click **NEXT**.

Deploy OVF Template	Select a name and folder ×
1 Select an OVF template	Specify a unique name and target location Virtual machine name: Http://storageProvider_3.7.3-00
2 Select a name and folder	Select a location for the virtual machine.
3 Select a compute resource	vc.adaptive-solutions.local     BI AS-VS
4 Review details	
5 Select storage	
6 Ready to complete	
	CANCEL BACK NEXT

**Step 5.** Select the Compute Resource and click Next.

.

Deploy OVF Template	Select a compute resource	×
1 Select an OVF template	Select the destination compute resource for this operation	
2 Select a name and folder		
3 Select a compute resource		
4 Review details		
5 Select storage		
6 Ready to complete		
	Compatibility	
	Compatibility checks succeeded.	
	CANCEL BACK NEX	т

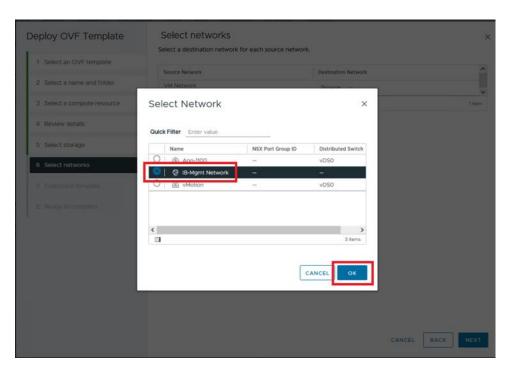
Step 6. Verify the template details and click Next.

<ol> <li>Select an OVF template</li> <li>Select a name and folder</li> <li>Select a compute resource</li> <li>Review details</li> <li>Select storage</li> </ol>	configuration options below. Publisher Product	dvanced configuration options, which might pose a security risk. Review the advanced Click next to accept the advanced configuration options. No certificate present Hitachi Storage Provider for VMware vCenter -b
3 Select a compute resource 4 Review details	Publisher Product	No certificate present
4 Review details	Product	
		Hitachi Storage Provider for VMware vCenter -b
5 Select storage	Version	3.7.3
	Vendor	Hitachi
6 Select networks	Download size	2.1 GB
7 Customize template	Size on disk	Unknown (thin provisioned) 200.0 GB (thick provisioned)
8 Ready to complete	Advanced configuration	nvram = ovf:/file/file3

### Step 7. Select the compatible Datastore and click Next.

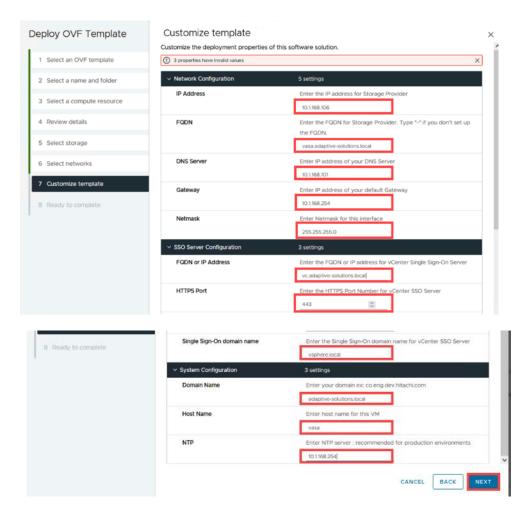
Deploy OVF Template	Select storage ×
	Select the storage for the configuration and disk files
1 Select an OVF template	Encrypt this virtual machine (Requires Key Management Server)
2 Select a name and folder	Select virtual disk format Thick Provision Lazy Zeroed  VM Storage Policy Datastore Default  Disable Storage DRS for this virtual machine
3 Select a compute resource	Name T Storage Compatibility, T Capacity T Provisioned T Free T Type T Ouster
4 Review details	I I VS⊩DS-01 5 TB 1.58 TB 3.54 TB VMFS 6
5 Select storage	○         □         VSI-DS         -         5 TB         438.92 GB         4.68 TB         VMPS 6           ✓
6 Select networks	Berns per page 10 v 2 items
7 Customize template	
8 Ready to complete	
	Compatibility
	✓ Compatibility checks succeeded.
	CANCEL BACK NEXT





**Step 9.** Provide the following details:

- Network Configuration
  - IP Address
  - FQDN
  - DNS
  - Gateway
  - Netmask
- SSO Server Configuration
  - FQDN or IP Address: Enter the FQDN or IP address for the vCenter Single Sign-On Server.
  - HTTPS Port: Enter the HTTPS Port Number 443 for vCenter SSO Server.
  - Single Sign-On domain name: Enter the domain name for the vCenter SSO Server as vSphere.local
- System Configuration
  - Domain Name
  - Host Name
  - NTP
- Step 10. Click Next.



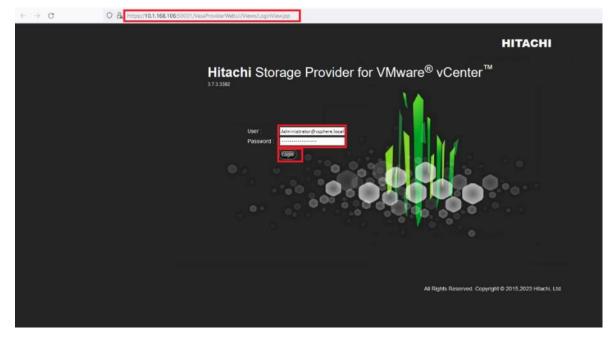
**Step 11.** Validate the details and click **Finish.** 

Deploy OVF Template	Ready to comple ~ Select a compute reso			×
1 Select an OVF template	Resource	8.0U1		
2 Select a name and folder	✓ Review details Download size	2.1 GB		
3 Select a compute resource	✓ Select storage			
4 Review details	Size on disk Storage mapping	200.0 GB 1		
5 Select storage	All disks	Datastore: VSI-DS-01; Format: Thick provision lazy zeroed		
6 Select networks	<ul> <li>Select networks</li> <li>Network mapping</li> </ul>	1		
7 Customize template	VM Network	IB-Mgmt Network		
	IP allocation settings			
8 Ready to complete	IP protocol	IPv4		
	IP allocation	Static - Manual		
	Customize template			
	Properties	IP Address = 10.1168.106 FQDN = vasa adaptive-solutions.local DNS Server = 10.1168.00 Getmask = 255.255.05 FQDN or IP Address = vc.adaptive-solutions.local HTTPS Port = 443 Single Sign-On domain name = vsphere.local Domain Name = adaptive-solutions.local Host Name = vasa NTP = 10.1168.254		2
		CANCEL	BACK	ISH

**Step 12.** Once the Storage Provider OVA has been deployed, **Power On** the virtual machine.

**Step 13.** In the browser, enter the IP Address or FQDN of Storage Provider for VMware vCenter with the following port number 50001. https://[Storage-Provider-IP-Address or FQDN]:50001/

**Step 14.** Enter the administrator SSO credentials for logging in to the **VMware vCenter**. Click **Login**.



#### Procedure 9. Onboard Hitachi VSP to Storage Provider for VMware vCenter

**Step 1.** In the **Storage Provider for VMware vCenter** console, from the Management pane, select **Manage Storage Systems**, and then click **Add Storage Systems**.

Management	Manage Storage Systems				
Manage Storage Systems	Physical Storage Virtual Storage				
Manage Storage Containers	Storage Systems - contains -	GO CH	30 V H 4 p	age[ 1/1] G0 ▶	Reload
Capability Schema	Physical Storage Systems	80 011			T THEFE TY ALL
Replication Groups	Storage Systems	Model Type SVP IP Address Configuration Ma	nager RESTAPI Server IP Address Serial Numbe	er Microcode Status	Last Update
Maintenance			Add Storage Systems Refresh Storage Systems	Edit Storage Systems (Ren	move Storage Systems)
General Settings					
Download Logs					
Update Certificate					
Change Credentials					
Restart Service					
Resolve and Troubleshoot					
Update Software					

Step 2. Select a Storage System Type and enter the SVP IP address. Enter the vVols User ID and Password that you created earlier. Click OK.

Management	Add Storage System		
	Storage System Type : VSP 5100/5200/5600/5600/51~		
Manage Storage Systems	SVP IP address : 192.168.168.20		
Manage Storage Containers	User ID : Wals-user		
Capability Schema	Password :		
Replication Groups			OK Cancel
Maintenance			
Ceneral Settings			
Download Logs			
Update Certificate		k.	
Change Credentials			
Restart Service			
Resolve and Troubleshoot			
Update Software			

Note: Click Reload to update the progress until the storage system is added successfully.

Management	Manage Storage Systems		
Manage Storage Systems	Physical Storage Virtual Storage		
Manage Storage Containers	Storage Systems	GD OIT	30 V H 4 page   1 / 1   SU F H Hittered: 1 / Alt1
Capability Schema Replication Groups	Physical Storage Systems	del Type SVP IP Address Configuration Manag	
		P 5600 192.168.168.20 -	Bit Process         Server in- Address         Server in- Add
Maintenance		Add	f Storage Systems Refresh Storage Systems Edit Storage Systems Remove Storage Systems
General Settings			
Update Certificate			
Change Credentials			
Restart Service Resolve and Troubleshoot			
Update Software			

**Procedure 10.** Register Storage Provider for VMware vCenter in VMware vSphere

Step 1. Log in to the vSphere Client.



Step 2.

Select vCenter. Click the Configure tab and select Storage Providers, and then click ADD.

	🕑 vc.adaptive-s	
	Summary Monitor	Configure Permissions Datacenters Hosts
<ul> <li>vc.adaptive-solutions.local</li> <li>AS-VSI</li> <li>8.0U1</li> <li>10.1.168.111</li> </ul>	Settings V General Licensing	Storage Providers STORAGE PROVIDERS PROVIDERS ARRAYS ADD SYNCHRONIZE STORAGE PROVIDERS RE-AU
<ul> <li>☐ 10.1.168.112</li> <li>☐ 10.1.168.113</li> <li>☐ 10.1.168.114</li> <li>&gt; → Test-Harness</li> </ul>	Message of the Day Advanced Settings vCenter HA Security ~ Trust Authority Key Providers Alarm Definitions Scheduled Tasks Storage Providers vSphere Zones vSAN >	Storage Provider       Status         IOFILTER Provider 10.1.168       Online         IOFILTER Provider 10.1.168       Online

- **Step 3.** Enter the following information:
  - a. Enter the Name for the New Storage Provider.
  - b. In the URL field, enter https://[Storage-Provider-FQDN]:50001/version.xml
  - c. In the Username field, enter the vCenter username in the format shown in the following figure.
  - d. In the Password field, enter the vCenter password.
  - e. Click OK.

New Storage	Provider vc.adaptive-solutions.loc x
Name	vasa
URL	https://Storage-Provider-FQDN:50001/
User name	vsphere.local\administrator
Password	
Use storage provide	er certificate
Certificate location	BROWSE
	CANCEL

Step 4. In the Security Alert prompt, click YES.



**Step 5.** After successful onboarding, the Storage Provider for VMware vCenter displays an **Online** status.

	600	figure	Permissions Datacenters	FROS	is & Clusters VMs [	Datastores Networks	Linked vCenter Server Systems
Settings 🗸 🗸	Sto	rag	e Providers				
General	STO	RAGE	PROVIDERS PROVIDERS ARRAYS				
Licensing Message of the Day	AL	do	SYNCHRONIZE STORAGE PROVIDERS	RE-	AUTHENTICATE HOST VASA C	LIENTS	
Advanced Settings			Storage Provider 🛛 🔻				
vCenter HA	:	>>>	IOFILTER Provider 10.1,168				
ecurity 🗸	:	>>	IOFILTER Provider 10.1.168		General Supported	Vendor IDs Certificate	Info Arrays
Trust Authority	:	>>>	IOFILTER Provider 10.1.168		Provider name	Vasa	
Key Providers	:	>>	IOFILTER Provider 10.1.168		Provider status	Online	
darm Definitions		~	vasa		Activation	Explicit	
cheduled Tasks	-	»	VMware vSAN		URL		olutions.local:50001/version.xml
itorage Providers	-	- 20-			Provider version	3.7.3	
Sphere Zones					VASA API version	3.0	
SAN >					Default namespace	Hitachi	
					Provider ID	ecbf2413 bbbf 4554 bb	xc3-bab5c2b3ff68
					Supported profiles	Storage Profile Based Mention Replication Profile	Management

**Procedure 11.** Create a Storage Container for vVols and Define a Capability Profile from Storage Provider for VMware vCenter

**Step 1.** Log in to Storage Provider for VMware vCenter, from the Management pane select **Manage Storage Containers**, and then click **Create Storage Container**.

27										
Hitachi Storage Provider for VMware vCer	ter - block component 3.7	3.3382 Welcome to	vasa-provider@vspher	e local						Help About Logout
Management	Manage Storage Cor	tainers								
1977 - SS	Name	✓ contains ✓	P 00				30	~	pege[ 1/1] 0	0 . Filtered: 0/All 0
Marage Storage Systems			00				30	·	bage ( i ) i ] [0	o ritered of ALO
Marage Storage Cortainers	Storage Contain		10XX 6010	Capacity	Logical	Capacity	Snapshot C	aparity		
(Capability Schema	Name	Description	Storage System	Total Free	Total	Free	Total	Free	Resource Group	Dummy Host Group
Replication Groups					-0.26		_		-	23
- majar and the set							Create S	Storage Conta	inter (Established) for the	
							-			
Maintenance										
General Settings										
Download Logs										
Update Dertificate										
Change Destentials										
Restart Service										
Resolve and Troubleshoot										
Update Software										

**Step 2.** Enter the following details:

- a. Provide a Name for vVols Storage Container.
- b. Select a Storage System.
- c. Select the vVols Resource Group.
- Step 3. Select the undefined Capability Profiles and click Define Profile.

tachi Storage Provider for VMware vCer	ter - block component 3.7.3.3382 Welcome to vasa-providen@	vsphere.local					bout Logout
Management	Create Storage Container						
	Specify information about the storage container.						
Manage Storage Systems	Step1 Specify information about the storage contain	er and resource group.					
Manage Storage Containers	Name :	fols Storage Container					
Capability Schema	Description :	put storage container description.					
Replication Groups	Storage System :	SP 5600 #60749 🗸					
	Resource Group :	/ols-RG 🗸					
	Step2 Specifies whether to use a storage container	for raplication If used specify the part for the du	mmy hast aroun				
Maintenance	Shup2 Specifies whether to use a storage container     Not used in Replication	for replication. If used, specify the port for the do	miny nost group.				
	Used in Replication Port for Dummy Host Grou	o: CL1-A 🗸					
General Settings							
Download Logs	Stop3 Specify a capability profile for the DP pool th	it exists in the storage container. 0MB /	0MB				
Updale Certificate	Capacity(Free/Total) : Logical Capacity(Free/Total) :	OMB /	OMB				
Change Credentials	Snapshot Capacity(Free/Total) :	5.15TB /	5.15TB				
Restart Service	Capability Profiles						
Resolve and Troubleshoot	Name	Description	Pool Pool Name	Pool Type	Capacity	Logical Capacity	1
Update Software					Total Free	Total Free	4
Updake Somware	(undefined)	DP 3	vVOL_Dynamic_Pool	HDT	5.15TB 5.15TB	N N	
					De	fine Profile Delete Profile Definition	2
	Advanced Options						
						Subr	Cancel

**Step 4.** Select the parameters for **Managed Capabilities** based on your environment and click **OK.** In the context of this guide, the following capabilities were selected.

- a. Performance IOPS class Tier1\_IOPS
- b. Performance Latency class Tier1\_Latency
- c. Availability class Tier1

Define Capability P			
Specify the na	me and provide a description of the capability profile,	, and then select the cap	abilities to be registered .
Name :	Capability Profile		
Description : [	input profile description.		
Managed Cap	pabilities User Defined		
Performa	nce IOPS - class		Tier1_IOPS V
Performa	nce Latency - class		Tier1_Latency V 🖓
🖾 Availabilit	ty - class		Tier1 V
Cost - clas	55		10
Recovery b	y Virtual Infrastructure Integrator.		
	Snapshot Backup Importance - Class	Select a ba	chap patry v D
-Auto-general	ted Capabilities		
Drive Typ	pe/Drive Speed	NVMe SSD (2)	
Pool Type	•	HDT 🔊	
RAID Let	vel	RAID6(6D+2P) D	
Encryptic	n	No 💬	
Snapsho	e de la companya de la	Yes 💬	
C Storage	Efficiency	• 💬	
SPBM tag(V	MFS)		
Deduplic	cation and Compression		
Compres	ssion		

Step 5. Click Submit.

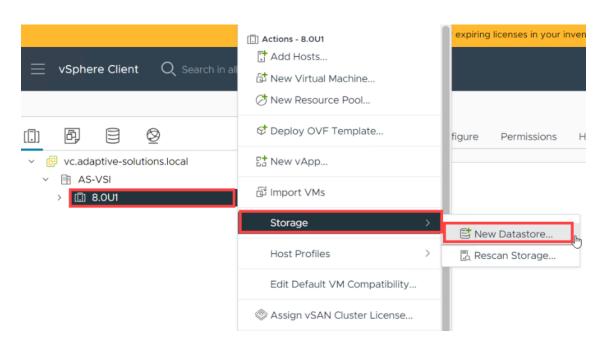
							/		•
k component 3.7.3.3382 Welcome to vasa-provider	@vsphere.local								Help About Log
·····									
e Storage Container									
Specify information about the storage container.									
Step1 Specify information about the storage cont	aloar and resource aroun								
	vVols Storage Container								
	input storage container description.								
Storage System :	VSP 5600 #60749								
Resource Group :	vVols-RG 🗸								
Step2 Specifies whether to use a storage contain	er for replication. If used, specify the port f	for the dummy host gro	up.						
Not used in Replication		, ,							
Oused in Replication Port for Dummy Host G	oup: CL1-A 🗸								
Step3 Specify a capability profile for the DP pool									
Capacity(Free/Total) :	5.151	B/ 5.1 ∞/	5TB						
Logical Capacity(Free/Total) : Snapshot Capacity(Free/Total) :	5.1570		5TB						
onaparior capacity (riee/10tal) :	5.1510	5.1	510						
Capability Profiles									
Name	Description	Pool	Pool Nar	ne	Pool Type	Cap	acity Free	Logical C Total	apacity Free
Capability Profile		DP 3	vVOL Dynamic Po	ol HDT		5.15TB	5.15TB	*	×
	1	0.0				0.1010	Dofer	Profile Delete P	rofile Definition
							Comme	Denote	Tome Demission
Advanced Options									
									Submit Car

# vVols Storage Configuration

Procedure 1.	Deploy vVols Datastore
Step 1.	Log in to VMware vSphere client.

VMware <sup>®</sup> vSphere	
Administrator@vsphere.local	
Use Windows session authentication	
LOGIN	

Step 2. Right-click the Cluster, select Storage, and then click New Datastore.



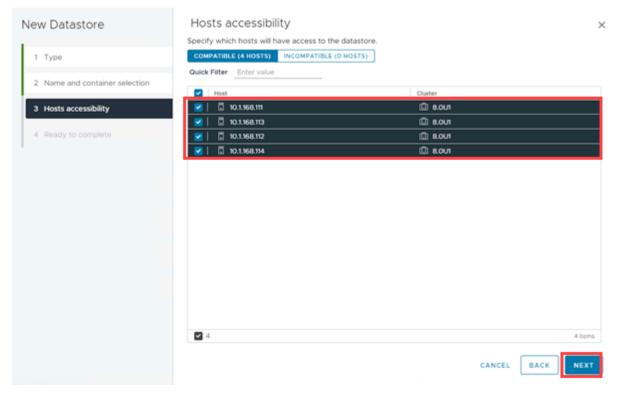


New Datastore	Type Specify datastore type.	×
1 Type 2 Name and container selection	VMFS Create a VMFS datastore on a disk/LUN. NFS Create an NFS datastore on an NFS share over the network.	
3 Hosts accessibility 4 Ready to complete	<ul> <li>VVol</li> <li>Create a Virtual Volumes datastore on a storage container connected to a storage provider.</li> </ul>	]
	CA	NCEL

#### Step 4. Enter the Name for the datastore and select the Storage Container. Click Next.

New Datastore	Name and cont	tainer selection		×
	Specify datastore name	and backing storage container.		
1 Type	Name VSI-	-vVols-01		
2 Name and container selection	Backing Storage Contain	ner		
3 Hosts accessibility	Name ¥	Identifier	¥ Maximum Disk Size	Y Existing Datastore Y
4 Ready to complete	VVois Storag_	vvot51c50c9c51474d96-87561e891f5	ie06e9 60 TB	-
1				
				1 item
		tastores, PE LUNs need to be configured ma out configuring PE LUNs, the ESXi host mark		
	Backing Storage Contain	ner Details		
	Storage array(s)	VSP 5600_60749		
	Storage provider(s)	VASA Provider		
			CAN	ICEL BACK NEXT

#### Step 5. Select all the Hosts that will be included in the vVols Datastore. Click Next.



**Step 6.** Click **Finish** to create a vVols Datastore.

New Datastore	Ready to comple	ete ×
1	Review your selections be	Hore finishing the wizard
1 Туре	✓ Name and container s	selection
2 Name and container selection	Datastore name	VSI-vVols-01
	Datastore type	VVor
3 Hosts accessibility	Storage container name:	vVols Storage Container
4 Ready to complete	Storage container UUID:	vvot5lc50c9c5f474d96-87561e89ff5e06e9
· · · · · · · · · · · · · · · · · · ·	Storage array(s):	VSP 5600_60749
	Storage provider(s):	VASA Provider
	✓ Hosts accessibility	
	Hosts	10.1.168.111
		<ul> <li>10.1168.03</li> <li>10.1168.012</li> </ul>
		10.1168.114
		CANCEL BACK FINISH
Procedure 2. Defin	e a Virtual Ma	chine Storage Profile
Step 1. Log i	n to VMware v	vSphere Client.
0		
VMware <sup>®</sup> \	/Sphere	
Administrator@vsphere	local	
Use Windows session	n authentication	
	LOGIN	

**Step 2.** Navigate to Policies and Profiles under vSphere Client Home tab.

$\equiv$ vSphere Client ${f Q}$ Search in all environmen	ts
☆ Home Shortcuts	VM Storage Policies
品 Inventory 同 Content Libraries	CREATE Quick Filter Enter value
↔ Workload Management ᠍ Global Inventory Lists	Name       VM Encryption Policy
Policies and Profiles 入 Auto Deploy	VSAN Default Storage Policy       VVol No Requirements Policy
<ul> <li>Hybrid Cloud Services</li> <li>Developer Center</li> </ul>	Management Storage Policy - F
ll Tasks	

**Step 3.** Select the VM storage Policies and click **Create**.

≡ v\$phere Client Q Search )		C & Administrator@VSPHERELOCAL + 😧 🔿 +
Policies and Profiles	VM Storage Policies     CREATE CHECK REAPPLY EDIT CLONE DELETE     Ouck FEter Enter value	
Rb Compute Policies	D Norma	VE
15 Storage Policy Components	Management Storage policy - Encryption	g vc.adaptive-solutions.local
	Host-local PMem Default Storage Policy	😰 vc.adaptive-solutions.local
	VSAN ESA Default Policy - RAIDS	() vc.adaptive-solutions.local
	SAN ESA Detault Policy - RAIDG	💋 vc.adaptive-solutions.local

Step 4. Enter the Name and click Next.

Create VM Storage Policy	Name and desc	cription	×
Name and description     Policy structure     Storage compatibility	vCenter Server: Name:	@VC.ADAPTIVE-SOLUTIONS.LOCAL ~	
4 Review and finish	Description:		
			CANCEL

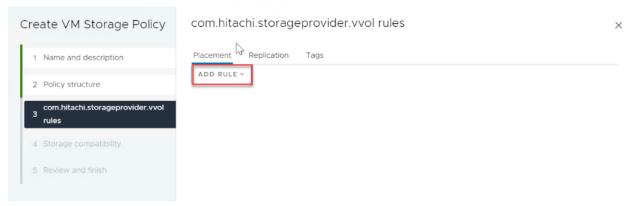


Select the Datastore specific rules for Hitachi Storage provider and click Next.

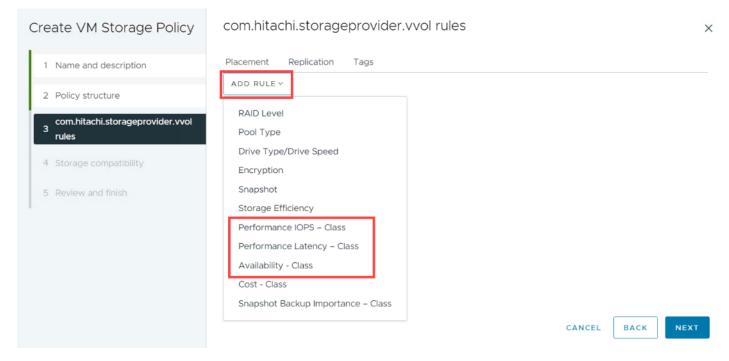
Name and description	Host based services
Policy structure	Create rules for data services provided by hosts. Available data services could include encryption, I/O control,
com hitachi storageprovider vvol rulei	caching, etc. Host based services will be applied in addition to any datastore specific rules.
Storage compatibility	Datastore specific rules
5 Review and finish	Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
	Enable rules for "vSANDirect" storage
	Enable rules for "VMFS" storage
	Enable rules for "com.hitachi.storageprovider.vvol" storage
	Enable tag based placement rules
	Passes as shows
	CANCEL. BACK NEXT

#### Step 6.

Click **ADD RULE** for com.hitachi.storageprovider.vvol.



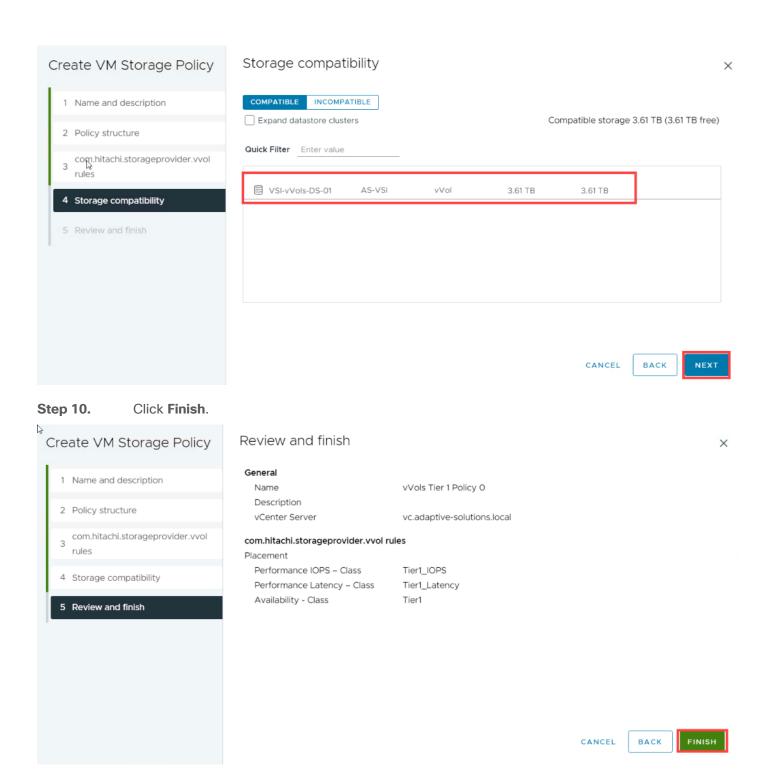
**Step 7.** Add the capabilities profiles as shown below:



**Step 8.** Select the capabilities based on environment requirements. In the context of this document Tier1\_IOPS, Tier1\_Latency, and Tier1 Availability are selected. Click **Next.** 

reate VM Storage Policy	com.hitachi.storageprovic	ler.vvol rules		
1 Name and description	Placement Replication Tags			
	Performance IOPS – Class (1)	✓ Tier1_IOPS		REMOVE
2 Policy structure		Tier2_IOPS		
com.hitachi.storageprovider.vvol 3 rules		Tier3_IOPS		
4 Storage compatibility	Performance Latency – Class (i)	✓ Tier1_Latency		REMOVE
		Tier2_Latency		
5 Review and finish		Tier3_Latency		
	Availability - Class (1)	Tier1		REMOVE
		Tier2		
		Tier3		
			CANCEL	CK NEX

Step 9. Select the compatible datastore. Click Next.

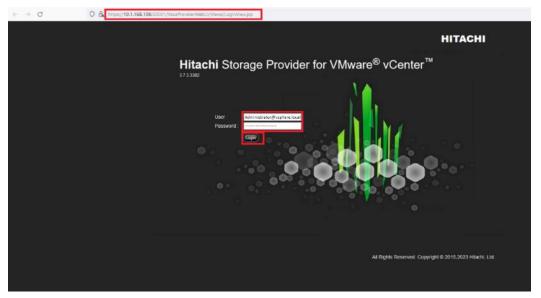


## Storage Policy Based Management (SPBM) for VMFS LDEVs

**Procedure 1.** Storage Policy Based Management (SPBM) for VMFS LDEVs from Storage Provider for VMware vCenter

SPBM provides capabilities of applicable storage resources to VMware vCenter.

From the Hitachi Storage Provider for VMware vCenter, you define an LDEV profile to pass storage characteristics to VMware vCenter, such as IOPS, Latency, Availability, Drive RPM, and even storage location. To create an LDEV profile from Hitachi Storage Provider, follow these steps:



Step 1. Log in to Hitachi Storage Provider.

Step 2. Select Manage Storage Systems. Click LDEVs.

nagement	Manage Storage Systems		
Manage Storage Systems	Physical Storage Virtual Storage		
Manage Storage Containers	Storage System: V contains V	GO OFF	30 🗸 н (4
Capability Schema	Physical Storage Systems		
Replication Groups	Storage Systems	Model Type SVP IP Address Configuration Ma	nager REST API Server IP Address Serial Nu
	AA22-5600 Cool's CLDEV's	VSP 5600 192.168.168.20 -	60749
ntenance General Settings			Add Storage Systems
Download Logs			
Update Certificate			
Change Credentials	)		
Restart Service			

**Step 3.** Select the VMFS LDEV to provide capabilities for and click **Define Profile**.

Management	Man	age Volun	nes - AA22-5600					
Manage Storage Systems							No. of Volu	imes
Manage Storage Containers	D	atastore N:	ame 🗸 🛛 contains 🗸	Ĩ	-1	GO OFF		
Capability Schema			e and click Define F			00		
Replication Groups		efine Profil		TOTIle.				
		umn Settings						
		ume's						
laintenance	_	Volume	Datastore Name	Profile Status	Pool	Resource Group	Label	Device ID
		00-00-00	VSI-DS-01	Custom	DP 1	meta resource	VSI-VMFS-DS-01	naa 60060e8008ed4d000050ed4d000000
Ourseal Outlines		00.00.00			1000			
General Settings		Statement and strength of the	VSI-DS-02	Disable		meta_resource	VSI-VMFS-DS-02	naa.60060e8008ed4d000050ed4d000000
General Settings Download Logs		Statement and strength of the	VSI-DS-02		DP 1			
		00:00:09	VSI-DS-02 -	Disable	DP 1 DP 0	meta_resource	ESXi1_Boot_Vol	naa.60060e8008ed4d000050ed4d000000
Download Logs		00:00:09	VSI-DS-02 -	Disable Disable	DP 1 DP 0 DP 0	meta_resource meta_resource	ESXi1_Boot_Vol ESXi2_Boot_Vol	naa.60060e8008ed4d000050ed4d000000 naa.60060e8008ed4d000050ed4d000000
Download Logs Update Certificate		00:00:09 00:00:04 00:00:05	VSI-DS-02 - -	Disable Disable Disable	DP 1 DP 0 DP 0 DP 0	meta_resource meta_resource meta_resource	ESXi1_Boot_Vol ESXi2_Boot_Vol	naa.60060e8008ed4d000050ed4d0000000 naa.60060e8008ed4d000050ed4d000000 naa.60060e8008ed4d000050ed4d0000000 naa.60060e8008ed4d000050ed4d0000000 naa.60060e8008ed4d000050ed4d0000000

**Step 4.** Select the parameters for **Managed Capabilities** based on your environment and click **OK.** In the context of this guide the following capabilities were selected.

- a. Performance IOPS Class Tier2\_IOPS
- b. Performance Latency Class Tier2\_Latency
- c. Availability Class Tier2

#### Step 5. Click Submit.

pecify select the capability tags to be re-	gistered.		
DEV ID: 00:00:08			
Managed Capabilities - Per Device Us	er Defined		
Performance IOPS - Class		Tier2_IOPS	
Performance Latency - Class		Tier2_Latency ✓	
🖾 Availability - Class		Tier2	
Cost - Class		Contract of the same state party of the	
Becovery by Victual Infrastructure Integra	stor		
Recovery by Virtual Infrastructure Integra Snapshot Backup Important		i w backup policy w P	
Snapshot Backup Important		Deduplication and Compression	Yes @
Auto-define Capabilities	ce - Class		Yes ⊚ Normal ⊚
Auto-define Capabilities     Drive Type/Drive Speed	ce - Class SSD Ø	Deduplication and Compression     Compression	
Snepshot Backup Important     Auto-define Capabilities     Drive Type/Drive Speed     Pool Type	ce - Class SSD @ HDP @	Deduplication and Compression     Compression	



Step 1. Log in to VMware vSphere Client.

VMware <sup>®</sup> vSphere	
Administrator@vsphere.local	
Use Windows session authentication	
LOGIN	



From vCenter, navigate to Inventory.

📃 vSphere Client	Q Search in all environments
☆ Home ♦ Shortcuts	<
몹 Inventory	
🗐 Content Libraries	
% Workload Management	
🗟 Global Inventory Lists	
🖫 Policies and Profiles	
☐ Auto Deploy	
lightarri	
V> Developer Center	

Step 3. Navigate to the Datastore section and select the VMFS Datastore.

📃 vSpl	nere Client Q Search in all	envilionmen
		<
() B		
vc.a	daptive-solutions.local	
~ 🖻 A	AS-VSI	
	VSI-DS-01	
	VSI-DS-02	
	VSI-NVMe-DS-01	
	VSI-NVMe-DS-02	
	VSI-vVols-DS-01	

Step 4.After you have selected the Datastore, click Summary and view Storage Capabilities in the Tagspane.

ts	
Summary Monitor Configure	Permissions Files Hosts VMs
Related Objects	Tags    Availability : Tier2    Performance IOPS : Tier    2
(i) None	Performance Latency : T SPB X

## Host Image and vSphere Configuration Profiles

Procedure 1. Image Remediation

**Step 1.** From the **Cluster** view, select **Updates** > **Hosts** > **Image**, and select the first added host, and from **ACTIONS**, select **Run pre-check**.

00 8 0	Summary Monitor C		atastores Networks	Updates			
Vsc.adaptive-solutions.local     AS-VSI     SOUT     10.1568.112     10.1568.112     10.1568.113     10.1168.114     3 as-assist	Hosts V Image Hardware Compatibility VMware Tools VM Hardware				CHECK COMPLIANCE	MPLIANCE	
		A 10 1 168 114	Oulck Boot i     Software compliance	tage	host.	Show Only drift con	u analana
			inage		Heat Version	Image Version	
			Femware and Drivers	Addon	None	CR-5.1(1230052) 5.1(1230052)	
			Components	Host Version		Image Version	^
			CS-ucs-tool-eski	12.4-14		1.3.3-10EM	
			Osco-nenic	20100.005	M 700 1 0 15843807	2 0 11 C-10EM 800 1 0 20143090	

#### **Step 2.** With the pre-check run, re-select the added host and select **Remediate** from the ACTIONS menu.

vSphere Client Q. Search in all	eméconments		C &*	ministrator@VSPHERELOCAL ~	9 0
Contractions     Contrel     Contraction     Contraction     Contraction     Contracti	Hosts Ynope Mardware Compatability VM Hardware 10ols VM Hardware 1	found	rom the houls in the ck	aster during remediation.	×
ම to constant ලී as-assest	Houts ▲ 10.1 168: THA ▲ 10.1 568: THA ▲ 10.1 568: THA		nage ediation. Fost	×	
	IT SHELLOF	Software compliance Image Ferriware and Drivers Addon	Host Version	Show Only drift of Image Version CR-5 1(1.230052) 5.1(1.230052)	î
		Companents Hest Version OS-ucs-tool-ecs) 12 8-14 Osco-nenic 2.0.10.0-10	е ЭЕМ 700 1.0.15843807	13.3-10EM 2.0110-10EM.80010.201430	90
Recent Tasks Alarms					

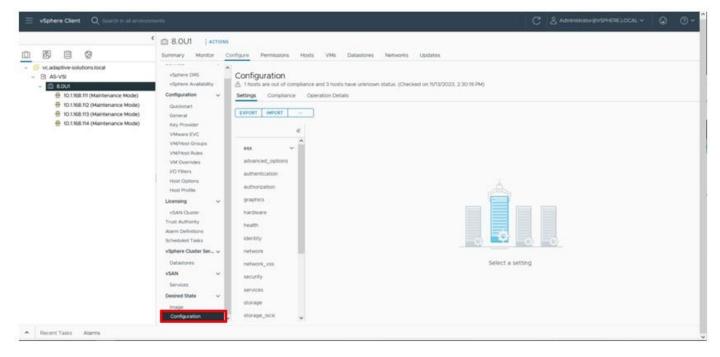
#### **Step 3.** Within the pop-up, click **START REMEDIATION**.

0 8 9	<b>Review Remediation Impact</b>		×		
vc adaptive-solutions.local	Impact summary Applicable remediation settings VMware General Terms Impact to specific hosts 10.1.168.112	Impact summary         • 1 host(s) are non-compliant with the image.         • 1 host(s) will be rebooted.         • Solution components of disabled Solutions vSphere MA 8.0 Update 1 will be removed from the hosts in the cluster during remediation.         Notes         VMs states honor remediation settings         VMs may be powered off, suspended or migrated to other hosts based on the applicable remediation settings.         Pre-check will be run again as a part of the remediation process. This is to ensure that no new issues have arisen on the cluster or hosts since the last pre-check (if any) that prevent remediation.         Hosts are remediated one at a time. so hosts will not reboot/go into maintenance mode simultaneously.         Order of host remediated in a order determined at runtime.         Hosts will be remediated in an order determined at runtime. Hence that order may not correspond to the order in which they appear here.	*	toe.	×
	I accept VMware General Terms	Quick Boot	×	052) 5.1(1.230052)	
	EXPORT IMPACT DETAILS	CLOSE START REMEDIATION	N	en	

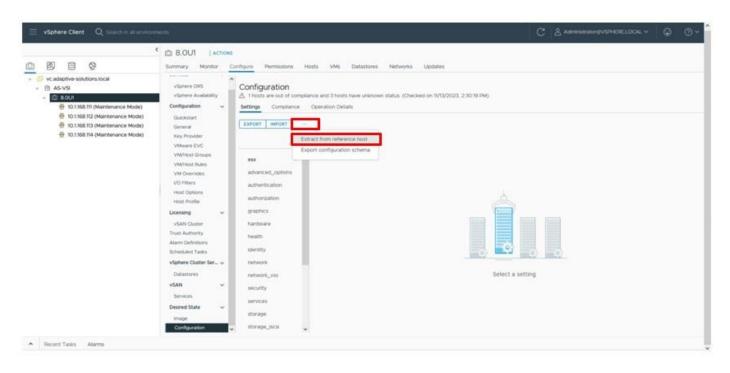
**Step 4.** Repeat steps 1 – 3 for each of the remaining hosts.

#### Procedure 2. Create Reference Configuration

**Step 1.** From the VSI cluster, click **Configure > Desired State > Configuration**.

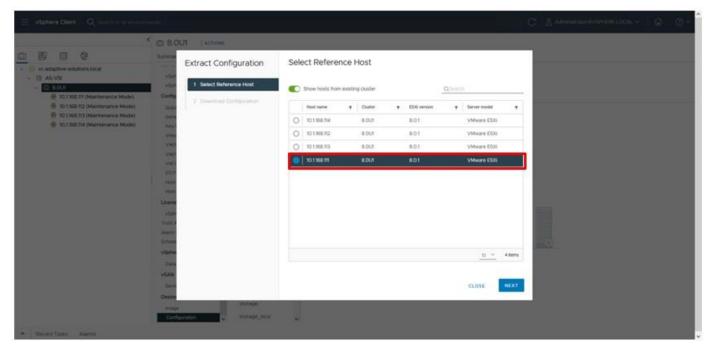


Step 2. Click the ... box and select Extract from reference host.





Select the first ESXi host that has been manually configured and click **NEXT**.



Step 4. Click DOWNLOAD.

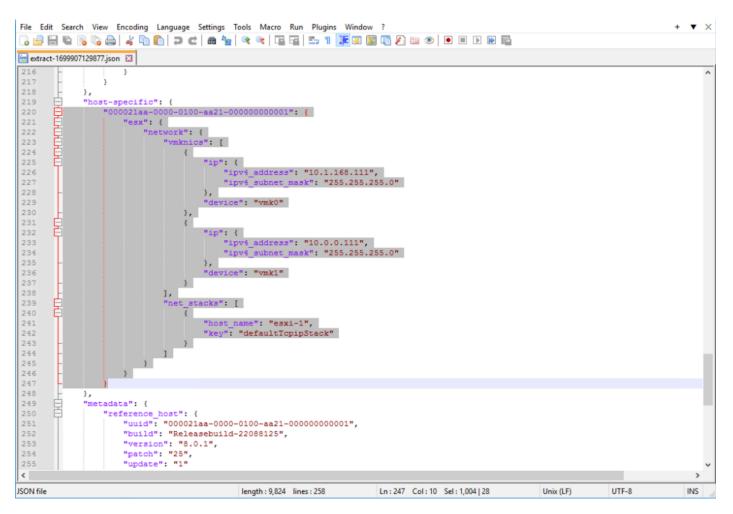
Sphere Client Q Search in all environme	ints		C & Administrator@VSPHERELOCAL ~ ③ ⑦ ~
		Download Configuration © Configuration file is ready to download.	
<ul> <li>Recent Tasks Alarms</li> </ul>	Alarmi I Schedu VSphen Data VSAN Servi Desite Image storage_jscsl	CLOSE BACK DOWNLOA	

### Procedure 3. Add Additional Hosts

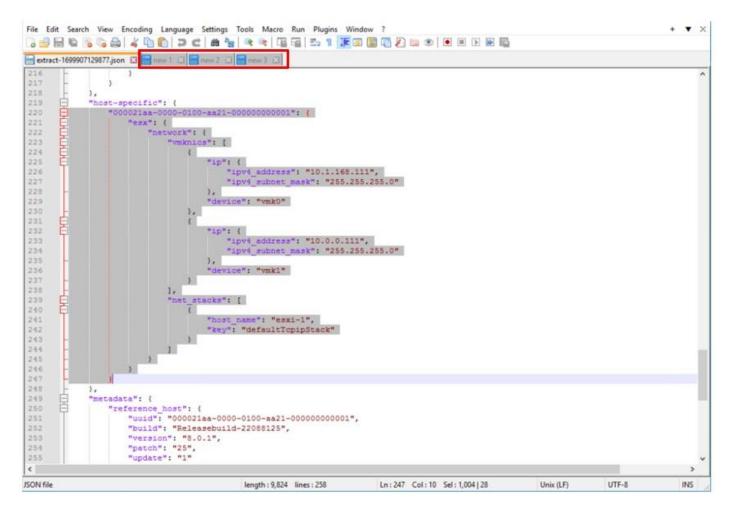
 Step 1.
 Open the downloaded JSON file in an editor. Notepad++ is used in our example.

 Step 1.
 Step 1.

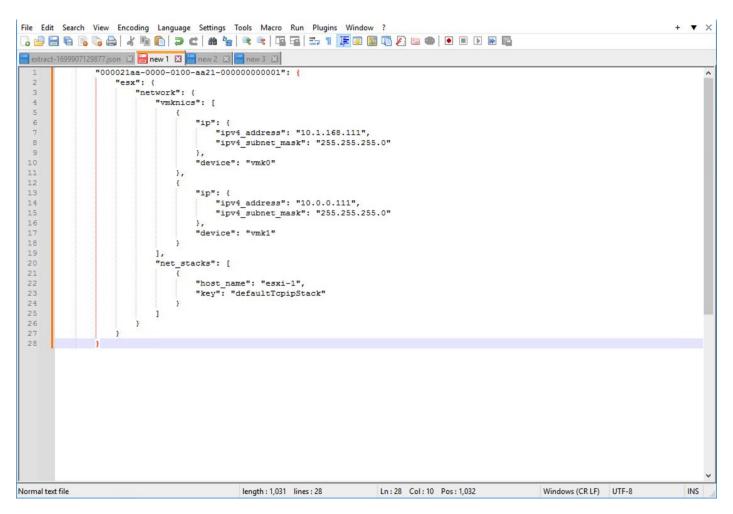
**Step 2.** Find the **host-specific** section within the JSON file, highlight the **UUID bracket** section and copy it.



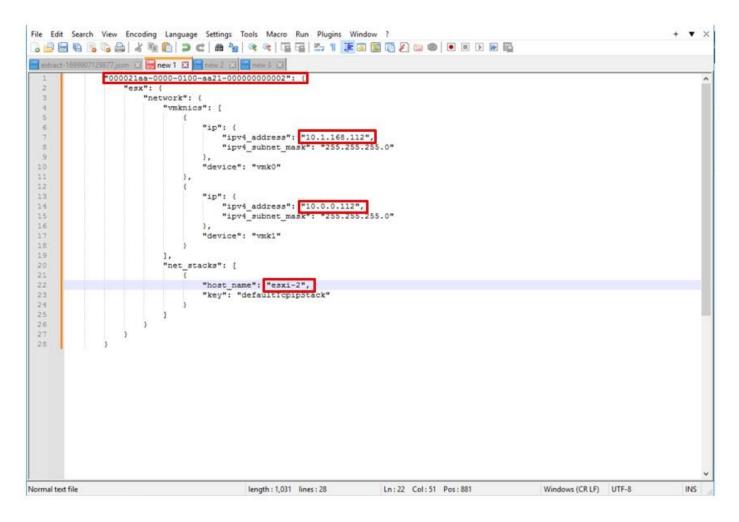
**Step 3.** Create additional tabs or files for each host to be configured and copy the host-specific JSON text.



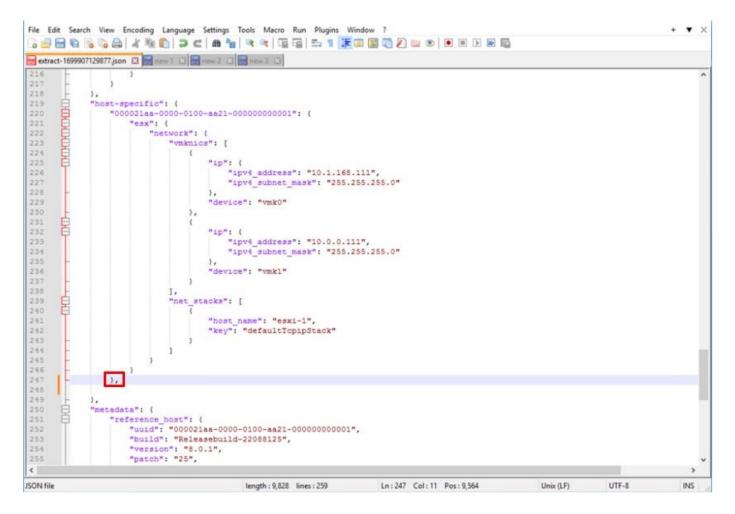
**Step 4.** Paste this copied host-specific JSON section into each tab.



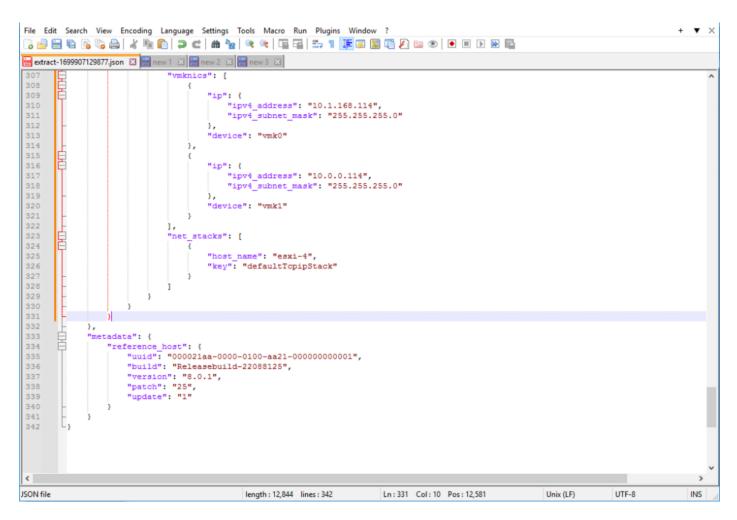
**Step 5.** Adjust the UUID (top alpha-numeric sequence above the "esx": line) with the UUID values for each additional host, along with adjustments for their respective VMkernel IPs and host names.



**Step 6.** Add a comma after the first UUID block in the original JSON file.

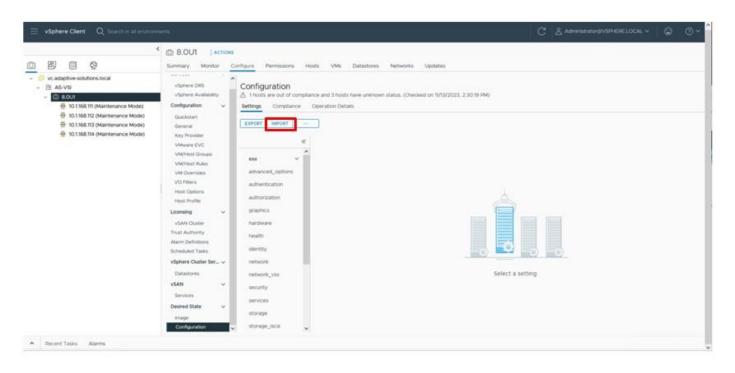


**Step 7.** Insert each additional host UUID block segments into the file after the comma, with commas separating each additional host, and then save the file.



Note: The last host block inserted will not have a comma added to it.

**Step 8.** From vCenter, return to the cluster **Configure > Configuration**, and click **IMPORT**.





$\equiv$ vSphere Client $Q_i$ boards in all resources				C & Administrational VSP-IERE LOCAL Y Q O Y
	In 8.0U1 Summary More	Import Configuration from File	×	
	VSphere DRS	The imported configuration will overwrite and replace the current desired configuration.		
<ul> <li>①1160.116(Maintenance Mode)</li> <li>①1168.112 (Maintenance Mode)</li> <li>①1168.113 (Maintenance Mode)</li> <li>①1169.114 (Maintenance Mode)</li> </ul>	Calactorat General Key Ploateder VMArbert Group VMArbert Group VMArbert Group VD Filters Hos Potion Hos Potion Hos Potion Licensing VSAN Classer Trust Authority Alarm Oxfontions Scheduled Talan VSAN Datastons Desired State Image	Select a JSON file with the configuration that you want to use as the new desired state. Select a JSON file	CLOSE IMPORT	ttng
Recent Tasks Alarms	Configuration	storage_Hctli		

Step 10. Click CLOSE after the import completes.

Procedure 4. Remediate Hosts

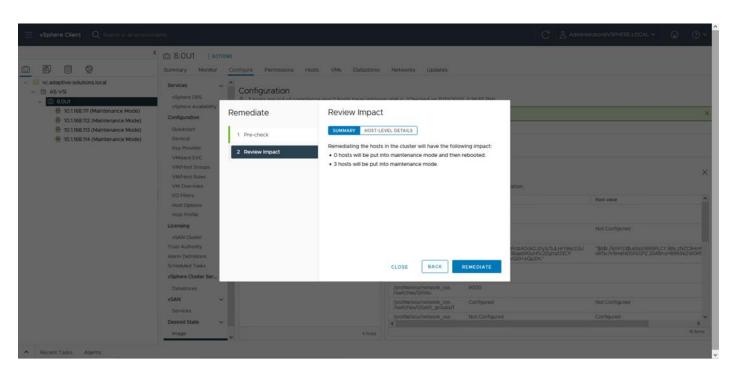
**Step 1.** Click the **Compliance** tab of **Configure > Desired State > Configuration** of the VSI cluster, select a non-compliant host, and click **RUN PRE-CHECK**.

	ments				
	6 1 8.0U1 EACTIONS				
Constructions.local     As-vs     Constructions.local     As-vs     Constructions.local     To1.168.112 (Maintenance Mode)     Ho1.168.113 (Maintenance Mode)     Ho1.168.113 (Maintenance Mode)     Ho1.168.114 (Maintenance Mode)	Surrerary Monitor C orightere DRS orightere DRS	Integrate Permissions Hosts VMs Datatores Configuration  (a) Thoots are out of compliance and 0 hosts have unline Settings Compliance Operation Details COECX COMPLIANCE TWA PRE-CHECX TEMEDIATE  Math TO 1566 TD  (a) TO 1566 TD  (b) TO 1566 TD  (c) TO 1568		vith desired configuration.	Heat value Not Configured Not Configured Not Configured Configured
	Desired State ~		/profile/ess/petwork /saf_cfure/cfu	Configured	Not Configured
	Configuration	4 hosts			

**Step 2.** With the pre-check completed, click **REMEDIATE**.

	6 10 8.0U1 EACTION				
8 8	Summary Monitor C	Configure Permissions Hosts VMs Datastores	Networks Updates		
vc.adaptive-solutions.local AS-VR C BLOUT	Services v	Configuration	in status. (Checked on 11/13/202	3, 3 36 55 PM)	
# 10.1368.111 (Maintenance Mode)	Configuration v	Remediation pre-check completed. No errors found.			
<ul> <li>10.1.168.112 (Maintenance Mode)</li> <li>10.1.168.113 (Maintenance Mode)</li> </ul>	Quickstart	Settings Compliance Operation Details			
H 10.1168.114 (Maintenance Mode)	General Key Provider				
	VM/Host Groups VM/Host Bules	Hada T	10.1.168.112		
	VM Overrides	() IO X MALTIT	A Host is out of compliance w	vith desired configuration.	
	VO Filters	A 10.1168.1D	Setting T	Civitar value	Hist value
	Host Options Host Profile	101366.02	/profile /etx/advancest_options	"Balanced"	
	Licensing v	A 10.1368.04	/power/cpu_pokcy		
	vSAN Ousler		/profile /esx/advanced_options /user_yars/1	Configured	Not Configured
	Trust Authority Alarm Definitions		/profile/esx/authentication /user_accounts /0/password_bash	*\$650KYuuqMx5GPctp40ck0.pyx/5JUHY8Hc03J M/2ouab0a64MHt6ox6R0uH5c22gHqd5CY /m3kyK2FP0KT7WQ0Hx6p2m*	16647/5mP015v6ep08899,CY385392C9 dotw3v6m930592692,2548mp4896962W
	Scheduled Tasks vSphere Cluster Ser v		/profile/esc/hetwork_vsa /switches/0/bridge /beacon_internal	L.	
	Datastores		/profile/esk/network_ysa /switches/0/mtu	9000	
	vsan v		/profile/esx/hetwork_vsa /switches/0/port_groups/1	Configured	Not Configured
	Services Desired State		/profile/etx/network_vss	Not Configured	Configured
	image	4 hody	¢		

**Step 3.** Click **NEXT** after the PRE-CHECK and then click **REMEDIATE** on the Review Impact screen.



Step 4.

With remediation complete, remove all hosts from Maintenance Mode.

Summary Summary <th></th> <th></th> <th></th> <th></th>				
vSphere Cluster Ser v	Image: Second	Services       ✓         vSphere DRS       ✓         vSphere Availability       △         Cenfiguration       ✓         Calcidstart       ✓         General       ✓         Key Provider       ✓         VM-Host Groups       ✓         VM-Host Rines       ✓         VO Prens       ✓         Host Options       ✓         Host Options       ✓         Most Profile       ✓         VSAN Cluster       ✓         Trust Authority       ✓         Alam Definitions       ✓         Schuled Tasks       ✓	07.05 PM)	

## vSphere Additional Finishing Steps

#### Procedure 5. VMware ESXi 8.0 U1 TPM Attestation

**Note:** If your Cisco UCS servers have Trusted Platform Module (TPM) 2.0 modules installed, the TPM can provide assurance that ESXi has booted with UEFI Secure Boot enabled and using only digitally signed code. In the <u>Cisco UCS Configuration</u> section of this document, UEFI secure boot was enabled in the boot order

policy. A server can boot with UEFI Secure Boot with or without a TPM 2.0 module. If it has a TPM, VMware vCenter can attest that the server booted with UEFI Secure Boot. To verify the VMware ESXi 8.0 U1 TPM Attestation, follow these steps:

**Step 1.** For Cisco UCS servers that have TPM 2.0 modules installed, TPM Attestation can be verified within vCenter.

Step 2. In the vCenter under Hosts and Clusters select the cluster.

Step 3. In the center pane, choose the Monitor tab.

**Step 4.** Click **Monitor > Security**. The Attestation status will show the status of the TPM:

	ID 8.0U1	are Permissions Hosts	VMs Datastrows	Networks Linds	sters			
vc.adaptive-solutions.local     vc.adaptive-solutions.local     with AS-VS     vo.adaptive-solutions.local     vo.adaptiv	Summary Monitor Config Events A VSphere DRS V Reconstructedors Fauts Hattory VM DRS Score CRU Utilization Network Utilization Network Utilization Sphere HA V Summary Heartbeat			Attended by vCenter Server vCenter Server vCenter Server	194 oerman 2.0 2.0 2.0	TXT + Folice Folice Folice	Messeji	
	Configuration Issues Datastores under APO or . Besource Allocation v Org Memory Partistiert Memory Browaw URituation Storage Overview Security Volpere Overview							

**Note:** It may be necessary to disconnect and reconnect or reboot a host from vCenter to get it to pass attestation the first time.

#### **Procedure 6.** (Optional) Configure Distributed Power Management (DPM)

This procedure configures the host to be able to be shut down during low cluster utilization times to reduce power.

The CIMC Management interface associated with the DPM BMC MAC address will need to be gathered from the Fabric Interconnect Device Console CLI, either from direct console connection, or via ssh.

To gather the CIMC Management interface MAC addresses, perform the following steps:

**Step 1.** Connect to either Fabric Interconnect Device Console as admin.

```
% ssh admin@192.168.168.11
Cisco UCS 6500 Series Fabric Interconnect
admin@192.168.168.12's password:
UCS Intersight Management
```

AA21-6536-A#

**Step 2.** Connect to the CIMC Debug Firmware Utility Shell of the first server (*connect cimc <chas-sis>/<blade slot>*) from which to collect information.

```
AA21-6536-B# connect cimc 1/1
Entering character mode
Escape character is '^]'.
CIMC Debug Firmware Utility Shell [ ]
[ help ]#
```

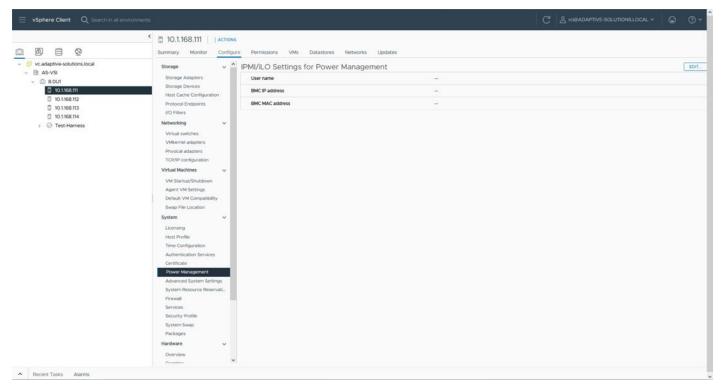
**Step 3.** Run the network command and identify the first server MAC (HWaddr) address for the eth0 value from the top of the output that returns.

```
[ help ]# network
eth0 Link encap:Ethernet HWaddr 56:51:DE:D5:87:E9
inet6 addr: fe80::5451:deff:fed5:87e9/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:48387344 errors:0 dropped:0 overruns:0 frame:0
TX packets:37023312 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:18446744071908661842 (16777215.9 TiB) TX bytes:1097208517 (1.0 GiB)
Interrupt:50
```

**Step 4.** Type **exit** and repeat steps 2 and 3 for each server.

**Note:** With the information gathered for each server to configure, continue with the following steps:

**Step 5.** From the first host that has been added, go to **Configure > System > Power Management** and click **EDIT...**.



**Step 6.** Provide the credentials for a local user with admin privileges within the UCS domain, the assigned KVM mgmt IP from Intersight, and the CIMC MAC address previously collected from the Fabric Interconnect Device Console.

$\equiv$ vSohere Client $Q_i$ South and estimated					
	10.1.168.111				
• • • •	Summary Monitor Configure	Permissions VMs Datastores N	tworks Updates		
Vic.adaptive-solutions.local     H AS-VS     B BOUT	Storage	IPMI/ILO Settings for Power Ma User name	nagement		
10.1168.112	Storage Devices Host Cache Configuration	BMC IP address			
0 10.1168.113 10.1168.114	Protocol Enderoints VD Filters	EMC MAC address			
) G Test-Harness	Networking v Virtual switches Virkernel adapters Physical adapters TCP/RF configuration	IPMI/iLO Settings fo Management	r Power   10.1.168.111	×	
	Virtual Machines 🗸 🗸	User name	vskuser		
	VM Stamus/Shutoown Agent VM Settings	Password	•••••		
	Default VM Computibility Swap File Location	BMC IP address	192.168.168.101		
	System v Licensing Host Proble	BMC MAC address	56:51DED5.87:E9		
	Tané Configuration Authentication Services		CANCEL		
	Certificate Poliver Managements Advanced System Settings				
	System Resource Reservati.				
	Services Security Profile				
	System Swep Packages				
	Hardware 🗸				
	Overview				
<ul> <li>Recent Tasks Alarms</li> </ul>					

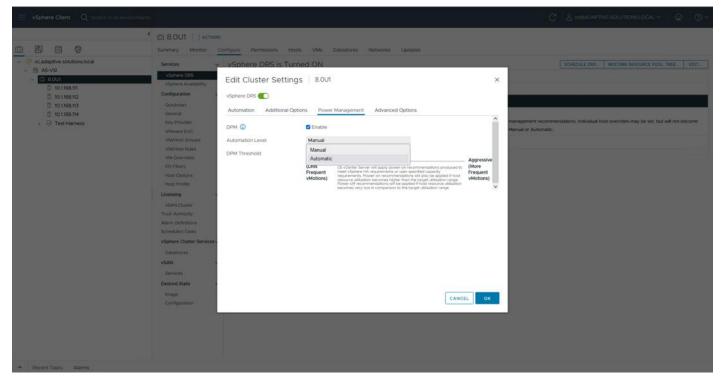
**Step 7.** Repeat **Step 2** for each additional host in the cluster.

**Note:** The MAC addresses used in this configuration are associated with the physical hardware of the server and will need to be re-entered if the server profiles associated with these hosts are deployed to different servers.

Step 8. Go to Configure > Services > vSphere DRS for the cluster and click EDIT....

	(1) 8.0U1 ; ACTIONS		
1 8 6 2		onfigure Permissions Hosts VMs Datastores Network	ks Updates.
Image: Construction of the construction of		vrfgure Permissions Hosts VMs Dutastores Network VSphere DRS is Turned ON  DRS Automation  Additional Options  Power Munagement Automation Level  DPM Threshold  Advanced Options	

**Step 9.** Select the **Power Management** tab within the **Edit Cluster Settings** window, click the **Enable** checkbox for DPM, and select the **Automatic** option from the Automation Level drop-down list.



**Step 10.** Click **OK** to apply the changes.

**Step 11.** Click **OK** past any warnings about the standby functionality of certain hosts, or alternately test each host for standby now that it has been configured and repeat <u>Step 5</u>.

# About the Authors

#### Ramesh Isaac, Technical Marketing Engineer, Cisco Systems, Inc.

Ramesh Isaac is a Technical Marketing Engineer in the Cisco UCS Data Center Solutions Group. Ramesh has worked in the data center and mixed-use lab settings for over 25 years. He started in information technology supporting UNIX environments and focused on designing and implementing multi-tenant virtualization solutions in Cisco labs before entering Technical Marketing where he has supported converged infrastructure and virtual services as part of solution offerings as Cisco. Ramesh has held certifications from Cisco, VMware, and Red Hat.

#### Ramakrishna Manupuri, Senior Software Development Engineer, Hitachi Vantara

Ramakrishna Manupuri is a Senior Software Development Engineer, in the Solutions Engineering team of Converged UCP group. He has worked as a Solution engineer with mainly experience in UCP products, Cloud services, SAN Storage solutions and Virtualization technologies with expertise in VMware products such as VMware Cloud Foundation (Hyperconverged infrastructure solution), vCloud Director, vSphere, vSAN, VMware Site Recovery Manager (SRM). Ramakrishna has held certifications from VMware (VCP), AWS Solutions Architect - Associate and Fortinet (NSE4).

#### Sandeep Rakshe, Senior Software Development Engineer, Hitachi Vantara

Sandeep Rakshe is a Senior Software Development Engineer in the Hitachi Engineering Converged UCP group. Sandeep has worked as QA and Solutions group with mainly experience in disaster recovery solutions. He started in information technology with different FC and NAS Storages with expertise in products such as Symantec NetBackup, Veritas Storage foundation, Hitachi Ops Center Protector and Unified compute advisor (Hyperconverged infrastructure solutions), IBM IP flash system IP replication, VMware vSAN. Sandeep has held certifications from Cisco and Red Hat

### **Acknowledgements**

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- John George, Technical Marketing Engineer, Cisco Systems, Inc.
- Archana Sharma, Engineering Technical Leader, Cisco Systems, Inc.
- Arvin Jami, Solutions Architect, Hitachi Vantara

# Appendix

This appendix contains the following:

- Allocate a VMFS Datastore with Cisco Intersight Cloud Orchestrator using Hitachi VSP
- MDS Configurations used in this validation
- Nexus Configurations used in this validation

**Note:** The features and functionality explained in this Appendix are optional configurations that can be helpful in configuring and managing the Adaptive Solutions deployment.

### Allocate a VMFS Datastore with Cisco Intersight Cloud Orchestrator using Hitachi VSP

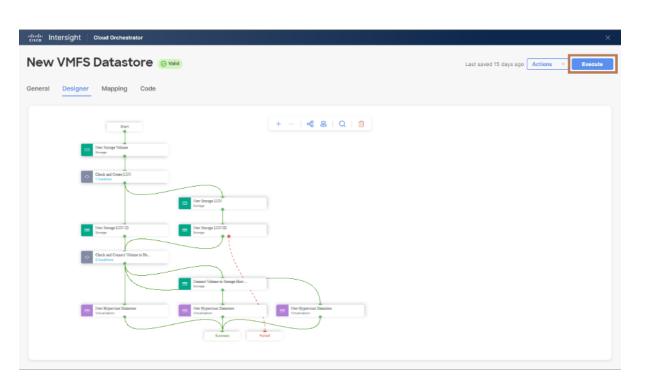
Intersight Cloud Orchestrator (ICO) enables administrators to allocate a VMFS datastore from system-defined workflow New VMFS Datastore, this single workflow is a combination of tasks that carves the virtual volume from an existing pool, adds LUN paths to a single host in a cluster with an associated LUN ID, and then onboards the datastore within VMware vCenter to the selected host. After the initial datastore has been mounted, administrators can use the ICO workflow output logs to identify the volume backing the datastore, after identified administrators must use ICO task New Storage LUN ID to allocate to other hosts within the desired cluster and any other multipaths required. A storage rescan from the ESXi host will be required.

#### Procedure 1. Use the New VMFS Datastore from the system-defined workflow

Step 1.Select Cloud Orchestrator from the system drop-down list, click Workflows, and click SampleWorkflows tab.

Configure A	Workflows						Imp	port Crea	ste Worl
Workflows Tasks Data Types	My Workflows Sample Workflows a				- 28 item	s found 10	I – perpage [	र्डि <u>२</u> of ३ (	IN
Command Palette * allo intersight with Ctrl+K or go tp > Command Palette	Top 5 Workflow Categorie (23) Borage 9 Writedization 7 Writedization 7 Compute 1	(32)	tribution by Targets NetApp Active IO U						н
	Display Name	22223142241544	aul: Executions			Failed/	Validat	Last Update	9
	New VMFS Datastore	Create a st		-		Disabled	© Valid	Dec 7, 2023	
	New Virtual Machine	Create a ne	1 0	-		Disabled	@ Valid	Dec 7, 2023	
	New Storage Virtual Machine	Create a st	1 0	+	(#)	Disabled	I Valid	Dec 7, 2023	- 92
		Create a st	1 0	(1.5.) (1.5.)	852 3	Disabled	Valid	Dec 7, 2023	
	New Storage Interface						A CONTRACTOR OF CARD	Dec 7, 2023	
	New Storage Interface     New Storage Host Group	Create a ne	2 0	-	-	Disabled	@ Valid	0007,2023	
		Create a ne Create a ne		-		Disabled Disabled	<ul><li>Valid</li><li>Valid</li></ul>	Dec 7, 2023	199
	New Storage Host Group		4 0		*				
	New Storage Host Group     New Storage Host	Create a ne	4 0 1 0	-	•	Disabled	<ul> <li>Valid</li> </ul>	Dec 7, 2023	
	New Storage Host Group     New Storage Host     New NAS Datastore	Create a ne Create a NF	4 0 1 0	-	•	Disabled Disabled	<ul> <li>Valid</li> <li>Valid</li> </ul>	Dec 7, 2023 Dec 7, 2023	

#### Step 2. From the predefined list, select New VMFS Datastore. Click Execute.



Step 3. From the Workflow Input wizard, select the Storage Device, LUN ID, Volume Label, Data Reduction Mode, Volume Size and Unit, Storage Host (Host Group), Port ID, Host Group Number, Hypervisor Manager, Data Center, Cluster, Host, Datastore Name, and Datastore Type. Click Execute. cloud Orchestrator

## Execute Workflow: NewVmfsDatastore

#### **Execute Workflow**

Hitachi volume option.

Volume Label VMFS-DS_Prod_Intersight	0	
Data Reduction Mode disabled	~ 0_	
Volume Capacity		
Size * 200	٥	
Unit * GiB	× 0	
Storage Host Selected Storage Host_VSI_x210_M7_01_Fab_A 🖉 ×		
Hitachi Host Group Parameter		
Port Id * ⊙ Selected Port Id CL1-A 🖉 X		
Host Group Number * ◎ Selected Host Group Number 1 🖉   ×		
Hypervisor Manager * ⊙ Selected Hypervisor Manager _vc.adaptive-solutions.local / ×		
atacenter *		
vlected Datacenter AS-VSI 🥒 🛛 ×		
elected Cluster 8.0U1 / ×		
elected Host 10.1.168.111 🕜 🛛 ×		
MFS-DS_Intersight	٥	
atastore Type *		

If input parameters are correct, ICO displays Success after the task is complete:

"loade Intersight Could Orchestrator	×
New VMFS Datastore 💿 🗤 📾	Last saved 15 days ago Executa
General Designer Mapping Code History	
Rollback Cione Execution	Execution Netw VMI S Datastore - Dec 12, 2023 9.80 MM V Organization Status
	default (0 Stateme)
Contract Contrac	(3) New Storage LUN ID Doc 22, 2023 09:50:45 AM ✓ Logs ✓ Inputs ✓ Outputs
	Check and Connect Volume to Host Gr Dec 22, 2023 09:50:45 AM     Logo     Outputs
Control Canada Tarabase	5 New Hypervisor Datastore Dec 22, 2023 09:51:04 AM V Logs V Inges V Ingets V Consults
See Reported Denses     O     Terrer and     T	Success         Dec 22, 2023 09:51:04 AM

**Step 4.** After the task is complete, expand **New Storage Volume Task > Outputs** to view the created LDEV ID in decimal:

anization ult		Status @ Success	
Vorkflow Inputs			
Start		Dec 22, 2023 09:50:33 AM	
New Storage	Volume	Dec 22, 2023 09:50:41 AM	
✓ Logs			
✓ Inputs			
∧ Outputs			
		1 } iow.ApiTask	
	Message: Volume cr	eated successfully.	
	State: Ok		
	Type: Config		
	olume Capacity: { 2 }		
-	Size: 200		
	Unit: G		

If multipathing or any other pathing to additional hosts is required, administrators are required to use New Storage LUN ID as explained in the VSP with Cisco Intersight Cloud Orchestrator best practices guide: <u>https://www.hitachivantara.com/en-us/pdfd/architecture-guide/vsp-with-cisco-intersight-cloud-orchestrator.p</u> <u>df</u> to allocate the volume to other hosts. A manual HBA rescan from the host is required to discover VMFS datastore after allocation is complete.

### **MDS Configurations used in this validation**

MDS A Configuration

```
version 9.3(2)
power redundancy-mode redundant
license smart transport smart
system default switchport mode F
feature fport-channel-trunk
feature nxapi
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
 rule 3 permit show feature module
  rule 2 permit show feature snmp
 rule 1 permit show feature system
username admin password 5 $5$Wor/sHUt$qlWc3XEUwEufzrMpHVwPdQdWeOgOmlBQ0aoP0sAPE61 role network-admin
username svc-nxcloud password 5 ! role network-admin
username svc-nxcloud passphrase lifetime 99999 warntime 14 gracetime 3
username snmpadmin password 5 $5$187vpH8F$Nxo6Ss6qcqiq2Yt5nwjsdydxgV3KBdrKY12et7wTro. role network-admin
username snmpadmin passphrase lifetime 99999 warntime 14 gracetime 3
ip domain-lookup
ip domain-name adaptive-solutions.local
ip name-server 192.168.160.53
ip host AA21-9124V-1 192.168.168.15
aaa group server radius radius
snmp-server contact vsiuser@adaptive-solutions.local
snmp-server user admin network-admin auth md5 0xe4c3b09168f2dc77ecb2ee99b1425233 priv aes-128 0xe4c3b09168
f2dc77ecb2ee99b1425233 localizedkey
snmp-server user snmpadmin network-admin auth sha 0x257e997f8e55f3c21deab856dc2bdc7bf6a7fa36 priv aes-128
0x257e997f8e55f3c21deab856dc2bdc7bf6a7fa36 localizedkey
snmp-server host 192.168.168.92 traps version 2c public udp-port 2162
snmp-server host 192.168.168.94 traps version 2c public udp-port 2162
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
port-monitor name fabricmon_edge_policy
  logical-type edge
  counter link-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts s
yslog rmon portguard FPIN
  counter sync-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts s
vslog rmon portguard FPIN
 counter signal-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts
 syslog rmon portguard FPIN
  counter invalid-words poll-interval 30 delta rising-threshold 1 event 4 falling-threshold 0 event 4 aler
ts syslog rmon portguard FPIN
 counter invalid-crc poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts
 syslog rmon portguard FPIN
  counter state-change poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4 alert
s syslog rmon
  counter tx-discards poll-interval 60 delta rising-threshold 200 event 4 falling-threshold 10 event 4 ale
rts syslog rmon
  counter lr-rx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslo
g rmon
  counter lr-tx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslo
g rmon
```

```
counter timeout-discards poll-interval 60 delta rising-threshold 200 event 4 falling-threshold 10 event
4 alerts syslog rmon
 counter credit-loss-reco poll-interval 1 delta rising-threshold 1 event 4 falling-threshold 0 event 4 al
erts syslog rmon
  counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 ev
ent 4 alerts syslog rmon
 counter rx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 70 event 4 aler
ts syslog rmon obfl
 counter tx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 70 event 4 aler
ts syslog rmon obfl
 no monitor counter err-pkt-from-port
  no monitor counter err-pkt-to-xbar
 no monitor counter err-pkt-from-xbar
  counter tx-slowport-oper-delay poll-interval 1 absolute rising-threshold 50 event 4 falling-threshold 0
event 4 alerts syslog rmon
 counter txwait poll-interval 1 delta rising-threshold 30 event 4 falling-threshold 10 event 4 alerts sys
log rmon portguard FPIN
 counter txwait warning-signal-threshold 40 alarm-signal-threshold 60 portguard congestion-signals
  no monitor counter sfp-tx-power-low-warn
 no monitor counter sfp-rx-power-low-warn
  counter rx-datarate-burst poll-interval 10 delta rising-threshold 5 event 4 falling-threshold 1 event 4
alerts syslog rmon obfl datarate 90
 counter tx-datarate-burst poll-interval 10 delta rising-threshold 5 event 4 falling-threshold 1 event 4
alerts syslog rmon obfl datarate 90
 counter input-errors poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alert
s syslog rmon
callhome
  email-contact rci@cisco.com
  destination-profile xml transport-method http
  destination-profile xml email-addr sl-sch-test@cisco.com
 destination-profile xml email-addr rci@cisco.com
 destination-profile xml http://tools.cisco.com/its/service/oddce/services/DDCEService
  enable
ntp_server_192.168.168.254
vsan database
 vsan 101 name "Fabric-A"
device-alias database
 device-alias name AA21-esxi-1 pwwn 20:00:00:25:b5:21:0a:00
  device-alias name AA21-esxi-2 pwwn 20:00:00:25:b5:21:0a:02
  device-alias name AA21-esxi-3 pwwn 20:00:00:25:b5:21:0a:04
 device-alias name AA21-esxi-4 pwwn 20:00:00:25:b5:21:0a:06
 device-alias name AA21-esxi-5 pwwn 20:00:00:25:b5:21:0a:08
  device-alias name AA21-esxi-6 pwwn 20:00:00:25:b5:21:0a:0a
  device-alias name AA22-5600-0-1a pwwn 50:06:0e:80:08:ed:4d:00
 device-alias name AA22-5600-1-2a pwwn 50:06:0e:80:08:ed:4d:10
  device-alias name AA21-esxi-1-fc-nvme pwwn 20:00:00:25:b5:21:0a:01
 device-alias name AA21-esxi-2-fc-nvme pwwn 20:00:00:25:b5:21:0a:03
 device-alias name AA21-esxi-3-fc-nvme pwwn 20:00:00:25:b5:21:0a:05
  device-alias name AA21-esxi-4-fc-nvme pwwn 20:00:00:25:b5:21:0a:07
  device-alias name AA21-esxi-5-fc-nvme pwwn 20:00:25:b5:21:0a:09
  device-alias name AA21-esxi-6-fc-nvme pwwn 20:00:00:25:b5:21:0a:0b
  device-alias name AA22-5600-0-1b-fc-nvme pwwn 50:06:0e:80:08:ed:4d:01
  device-alias name AA22-5600-1-2b-fc-nvme pwwn 50:06:0e:80:08:ed:4d:11
device-alias commit
fcdomain fcid database
  vsan 1 wwn 50:06:0e:80:08:ed:4d:10 fcid 0x0e0000 dynamic
            [AA22-5600-1-2a]
   1
 vsan 1 wwn 50:06:0e:80:08:ed:4d:11 fcid 0x0e0020 dynamic
   1
             [AA22-5600-1-2b-fc-nvme]
  vsan 1 wwn 50:06:0e:80:08:ed:4d:00 fcid 0x0e0040 dynamic
             [AA22-5600-0-1a]
   !
  vsan 1 wwn 50:06:0e:80:08:ed:4d:01 fcid 0x0e0060 dynamic
             [AA22-5600-0-1b-fc-nvme]
   1
  vsan 101 wwn 50:06:0e:80:08:ed:4d:10 fcid 0xcc0000 dynamic
               [AA22-5600-1-2a]
   1
  vsan 101 wwn 50:06:0e:80:08:ed:4d:11 fcid 0xcc0020 dynamic
               [AA22-5600-1-2b-fc-nvme]
   1
```

```
vsan 101 wwn 50:06:0e:80:08:ed:4d:00 fcid 0xcc0040 dynamic
               [AA22-5600-0-1a]
   1
  vsan 101 wwn 50:06:0e:80:08:ed:4d:01 fcid 0xcc0060 dynamic
               [AA22-5600-0-1b-fc-nvme]
   1
  vsan 101 wwn 24:01:00:08:31:33:76:7c fcid 0xcc0080 dynamic
  vsan 101 wwn 20:00:00:25:b5:21:0a:00 fcid 0xcc0081 dynamic
   !
               [AA21-esxi-1]
  vsan 101 wwn 20:00:00:25:b5:21:0a:02 fcid 0xcc0082 dynamic
   1
               [AA21-esxi-2]
  vsan 101 wwn 20:00:00:25:b5:21:0a:04 fcid 0xcc0083 dynamic
   1
               [AA21-esxi-3]
  vsan 101 wwn 20:00:00:25:b5:21:0a:06 fcid 0xcc0084 dynamic
               [AA21-esxi-4]
   1
  vsan 101 wwn 24:65:00:08:31:33:76:7c fcid 0xcc0085 dynamic
  vsan 101 wwn 20:00:00:25:b5:21:0a:01 fcid 0xcc0086 dynamic
   1
               [AA21-esxi-1-fc-nvme]
  vsan 101 wwn 20:00:00:25:b5:21:0a:03 fcid 0xcc0087 dynamic
               [AA21-esxi-2-fc-nvme]
   1
  vsan 101 wwn 20:00:00:25:b5:21:0a:05 fcid 0xcc0088 dynamic
               [AA21-esxi-3-fc-nvme]
   1
  vsan 101 wwn 20:00:00:25:b5:21:0a:07 fcid 0xcc0089 dynamic
               [AA21-esxi-4-fc-nvme]
   1
  vsan 101 wwn 20:00:00:25:b5:21:0a:0a fcid 0xcc008a dynamic
   1
              [AA21-esxi-6]
  vsan 101 wwn 20:00:00:25:b5:21:0a:08 fcid 0xcc008b dynamic
               [AA21-esxi-5]
   1
  vsan 101 wwn 20:00:00:25:b5:21:0a:09 fcid 0xcc008c dynamic
   1
               [AA21-esxi-5-fc-nvme]
  vsan 101 wwn 20:00:00:25:b5:21:0a:0b fcid 0xcc008d dynamic
   1
              [AA21-esxi-6-fc-nvme]
system default zone distribute full
zone smart-zoning enable vsan 101
zoneset distribute full vsan 101
!Active Zone Database Section for vsan 101
zone name FC-AA22-5600 vsan 101
   member device-alias AA21-esxi-1 init
   member device-alias AA21-esxi-2 init
   member device-alias AA21-esxi-3 init
   member device-alias AA21-esxi-4 init
   member device-alias AA22-5600-0-1a target
   member device-alias AA22-5600-1-2a target
   member device-alias AA21-esxi-5 init
   member device-alias AA21-esxi-6 init
zone name FC-NVMe-AA22-5600 vsan 101
   member device-alias AA21-esxi-1-fc-nvme init
    member device-alias AA21-esxi-2-fc-nvme init
   member device-alias AA21-esxi-3-fc-nyme init
    member device-alias AA21-esxi-4-fc-nvme init
   member device-alias AA22-5600-0-1b-fc-nvme target
   member device-alias AA22-5600-1-2b-fc-nvme target
   member device-alias AA21-esxi-5-fc-nvme init
   member device-alias AA21-esxi-6-fc-nvme init
zoneset name Fabric-A vsan 101
   member FC-AA22-5600
   member FC-NVMe-AA22-5600
zoneset activate name Fabric-A vsan 101
do clear zone database vsan 101
!Full Zone Database Section for vsan 101
zone name FC-AA22-5600 vsan 101
   member device-alias AA21-esxi-1 init
   member device-alias AA21-esxi-2 init
   member device-alias AA21-esxi-3 init
   member device-alias AA21-esxi-4 init
   member device-alias AA22-5600-0-1a target
    member device-alias AA22-5600-1-2a target
   member device-alias AA21-esxi-5 init
```

```
member device-alias AA21-esxi-6 init
zone name FC-NVMe-AA22-5600 vsan 101
   member device-alias AA21-esxi-1-fc-nyme init
   member device-alias AA21-esxi-2-fc-nvme init
   member device-alias AA21-esxi-3-fc-nvme init
   member device-alias AA21-esxi-4-fc-nvme init
   member device-alias AA22-5600-0-1b-fc-nvme target
   member device-alias AA22-5600-1-2b-fc-nvme target
    member device-alias AA21-esxi-5-fc-nvme init
   member device-alias AA21-esxi-6-fc-nvme init
zoneset name Fabric-A vsan 101
   member FC-AA22-5600
   member FC-NVMe-AA22-5600
interface mgmt0
  ip address 192.168.168.15 255.255.255.0
interface port-channel101
 switchport trunk allowed vsan 101
  switchport description AA21-6536-A
  switchport speed 32000
  switchport rate-mode dedicated
vsan database
 vsan 101 interface port-channel101
 vsan 101 interface fc1/5
  vsan 101 interface fc1/6
 vsan 101 interface fc1/7
 vsan 101 interface fc1/8
clock timezone EST -5 0
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60
switchname AA21-9124V-1
no terminal log-all
line console
line vty
boot kickstart bootflash:/m9124v-s8ek9-kickstart-mz-npe.9.3.2.bin
boot system bootflash:/m9124v-s8ek9-mz-npe.9.3.2.bin
interface fc1/5
  switchport speed 32000
interface fc1/6
  switchport speed 32000
interface fc1/7
  switchport speed 32000
interface fc1/8
 switchport speed 32000
interface fc1/1
 switchport speed 32000
interface fc1/2
 switchport speed 32000
interface fc1/3
 switchport speed 32000
interface fc1/4
  switchport speed 32000
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
```

interface fc1/22 interface fc1/23 interface fc1/24 interface fc1/5 interface fc1/6 interface fc1/7 interface fc1/8 interface fc1/1 switchport mode auto interface fc1/2 switchport mode auto interface fc1/3 switchport mode auto interface fc1/4 switchport mode auto interface fc1/1 switchport description AA21-6536-A:1/35/1 port-license acquire channel-group 101 force no shutdown interface fc1/2 switchport description AA21-6536-A:1/35/2 port-license acquire channel-group 101 force no shutdown interface fc1/3 switchport description AA21-6536-A:1/35/3 port-license acquire channel-group 101 force no shutdown interface fc1/4 switchport description AA21-6536-A:1/35/4 port-license acquire channel-group 101 force no shutdown interface fc1/5 switchport description AA22-5600-0:1a switchport trunk mode off port-license acquire no shutdown interface fc1/6 switchport description AA22-5600-0:1b switchport trunk mode off port-license acquire no shutdown interface fc1/7 switchport description AA22-5600-1:2a switchport trunk mode off port-license acquire no shutdown interface fc1/8 switchport description AA22-5600-1:2b switchport trunk mode off port-license acquire no shutdown interface fc1/9 interface fc1/10 interface fc1/11

interface fc1/12		
interface fc1/13		
interface fc1/14		
interface fc1/15		
interface fc1/16		
interface fc1/17		
interface fc1/18		
interface fc1/19		
interface fc1/20		
interface fc1/21		
interface fc1/22		
interface fc1/23		
interface fc1/24 ip default-gateway 192.168.168.254		

#### MDS B Configuration

```
version 9.3(2)
power redundancy-mode redundant
license smart transport smart
system default switchport mode F
feature fport-channel-trunk
feature nxapi
role name default-role
 description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
 rule 3 permit show feature module
 rule 2 permit show feature snmp
 rule 1 permit show feature system
username admin password 5 $5$xpHyz.ti$lUhjNr3J4er5pJ4jx16B2hfmMV/LMGNByCUqPfu76I7 role network-admin
username svc-nxcloud password 5 ! role network-admin
username svc-nxcloud passphrase lifetime 99999 warntime 14 gracetime 3
username snmpadmin password 5 $5$eEEDJ3ip$JCExf.xkI1G0.BN.KiM12kaRnFFpNeOeyHVUop7clC/ role network-admin
username snmpadmin passphrase lifetime 99999 warntime 14 gracetime 3
ip domain-lookup
ip domain-name adaptive-solutions.local
ip name-server 192.168.160.53
ip host AA21-9124V-2 192.168.168.16
aaa group server radius radius
snmp-server contact vsiuser@adaptive-solutions.local
snmp-server user admin network-admin auth md5 0x7232ee5c6e9db49adebf4c33a8afd5f6 priv aes-128 0x7232ee5c6e
9db49adebf4c33a8afd5f6 localizedkey
snmp-server user snmpadmin network-admin auth sha 0x45459c8d1d3ff0ec5c89cfd138e792b8ff48967a priv aes-128
0x45459c8d1d3ff0ec5c89cfd138e792b8ff48967a localizedkey
snmp-server host 192.168.168.92 traps version 2c public udp-port 2162
snmp-server host 192.168.168.94 traps version 2c public udp-port 2162
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
port-monitor name fabricmon_edge_policy
 logical-type edge
```

counter link-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts s yslog rmon portguard FPIN counter sync-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts s yslog rmon portguard FPIN counter signal-loss poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslog rmon portguard FPIN counter invalid-words poll-interval 30 delta rising-threshold 1 event 4 falling-threshold 0 event 4 aler ts syslog rmon portguard FPIN counter invalid-crc poll-interval 30 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslog rmon portguard FPIN counter state-change poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4 alert s syslog rmon counter tx-discards poll-interval 60 delta rising-threshold 200 event 4 falling-threshold 10 event 4 ale rts syslog rmon counter lr-rx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslo g rmon counter lr-tx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslo g rmon counter timeout-discards poll-interval 60 delta rising-threshold 200 event 4 falling-threshold 10 event 4 alerts syslog rmon counter credit-loss-reco poll-interval 1 delta rising-threshold 1 event 4 falling-threshold 0 event 4 al erts syslog rmon counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 ev ent 4 alerts syslog rmon counter rx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 70 event 4 aler ts syslog rmon obfl counter tx-datarate poll-interval 10 delta rising-threshold 80 event 4 falling-threshold 70 event 4 aler ts syslog rmon obfl no monitor counter err-pkt-from-port no monitor counter err-pkt-to-xbar no monitor counter err-pkt-from-xbar counter tx-slowport-oper-delay poll-interval 1 absolute rising-threshold 50 event 4 falling-threshold 0 event 4 alerts syslog rmon counter txwait poll-interval 1 delta rising-threshold 30 event 4 falling-threshold 10 event 4 alerts sys log rmon portguard FPIN counter txwait warning-signal-threshold 40 alarm-signal-threshold 60 portguard congestion-signals no monitor counter sfp-tx-power-low-warn no monitor counter sfp-rx-power-low-warn counter rx-datarate-burst poll-interval 10 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslog rmon obfl datarate 90 counter tx-datarate-burst poll-interval 10 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alerts syslog rmon obfl datarate 90 counter input-errors poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 1 event 4 alert s syslog rmon callhome email-contact rci@cisco.com destination-profile xml transport-method http destination-profile xml email-addr sl-sch-test@cisco.com destination-profile xml email-addr rci@cisco.com destination-profile xml http://tools.cisco.com/its/service/oddce/services/DDCEService enable ntp server 192.168.168.254 vsan database vsan 102 name "Fabric-B" cfs ipv4 distribute device-alias database device-alias name AA21-esxi-1 pwwn 20:00:00:25:b5:21:0b:00 device-alias name AA21-esxi-2 pwwn 20:00:00:25:b5:21:0b:02 device-alias name AA21-esxi-3 pwwn 20:00:00:25:b5:21:0b:04 device-alias name AA21-esxi-4 pwwn 20:00:00:25:b5:21:0b:06 device-alias name AA21-esxi-5 pwwn 20:00:00:25:b5:21:0b:08 device-alias name AA21-esxi-6 pwwn 20:00:00:25:b5:21:0b:0a device-alias name AA22-5600-0-3a pwwn 50:06:0e:80:08:ed:4d:20 device-alias name AA22-5600-1-4a pwwn 50:06:0e:80:08:ed:4d:30 device-alias name AA21-esxi-1-fc-nvme pwwn 20:00:00:25:b5:21:0b:01 device-alias name AA21-esxi-2-fc-nvme pwwn 20:00:00:25:b5:21:0b:03 device-alias name AA21-esxi-3-fc-nvme pwwn 20:00:00:25:b5:21:0b:05 device-alias name AA21-esxi-4-fc-nvme pwwn 20:00:25:b5:21:0b:07 device-alias name AA21-esxi-5-fc-nvme pwwn 20:00:00:25:b5:21:0b:09

```
device-alias name AA21-esxi-6-fc-nvme pwwn 20:00:00:25:b5:21:0b:0b
 device-alias name AA22-5600-0-3b-fc-nvme pwwn 50:06:0e:80:08:ed:4d:21
 device-alias name AA22-5600-1-4b-fc-nvme pwwn 50:06:0e:80:08:ed:4d:31
device-alias commit
fcdomain fcid database
 vsan 1 wwn 50:06:0e:80:08:ed:4d:20 fcid 0x340000 dynamic
   1
            [AA22-5600-0-3a]
 vsan 1 wwn 50:06:0e:80:08:ed:4d:31 fcid 0x340020 dynamic
            [AA22-5600-1-4b-fc-nvme]
   1
 vsan 1 wwn 50:06:0e:80:08:ed:4d:30 fcid 0x340040 dynamic
           [AA22-5600-1-4a]
  1
 vsan 1 wwn 50:06:0e:80:08:ed:4d:21 fcid 0x340060 dynamic
            [AA22-5600-0-3b-fc-nvme]
   1
 vsan 102 wwn 50:06:0e:80:08:ed:4d:30 fcid 0xdd0000 dynamic
   1
              [AA22-5600-1-4a]
 vsan 102 wwn 50:06:0e:80:08:ed:4d:31 fcid 0xdd0020 dynamic
              [AA22-5600-1-4b-fc-nvme]
   !
 vsan 102 wwn 50:06:0e:80:08:ed:4d:20 fcid 0xdd0040 dynamic
              [AA22-5600-0-3a]
   !
 vsan 102 wwn 50:06:0e:80:08:ed:4d:21 fcid 0xdd0060 dynamic
   1
              [AA22-5600-0-3b-fc-nvme]
 vsan 102 wwn 24:02:00:08:31:33:75:24 fcid 0xdd0080 dynamic
 vsan 102 wwn 20:00:00:25:b5:21:0b:00 fcid 0xdd0081 dynamic
               [AA21-esxi-1]
   1
 vsan 102 wwn 20:00:00:25:b5:21:0b:02 fcid 0xdd0082 dynamic
   1
              [AA21-esxi-2]
 vsan 102 wwn 20:00:00:25:b5:21:0b:04 fcid 0xdd0083 dynamic
   1
              [AA21-esxi-3]
 vsan 102 wwn 20:00:00:25:b5:21:0b:06 fcid 0xdd0084 dynamic
   1
              [AA21-esxi-4]
 vsan 102 wwn 24:66:00:08:31:33:75:24 fcid 0xdd0085 dynamic
 vsan 102 wwn 20:00:00:25:b5:21:0b:01 fcid 0xdd0086 dynamic
   !
              [AA21-esxi-1-fc-nvme]
 vsan 102 wwn 20:00:00:25:b5:21:0b:03 fcid 0xdd0087 dynamic
              [AA21-esxi-2-fc-nvme]
   1
 vsan 102 wwn 20:00:00:25:b5:21:0b:05 fcid 0xdd0088 dynamic
              [AA21-esxi-3-fc-nvme]
   1
 vsan 102 wwn 20:00:00:25:b5:21:0b:07 fcid 0xdd0089 dynamic
              [AA21-esxi-4-fc-nvme]
  - I
 vsan 102 wwn 20:00:00:25:b5:21:0b:0a fcid 0xdd008a dynamic
              [AA21-esxi-6]
   1
 vsan 102 wwn 20:00:00:25:b5:21:0b:08 fcid 0xdd008b dynamic
   1
             [AA21-esxi-5]
 vsan 102 wwn 20:00:00:25:b5:21:0b:09 fcid 0xdd008c dynamic
              [AA21-esxi-5-fc-nvme]
   !
 vsan 102 wwn 20:00:00:25:b5:21:0b:0b fcid 0xdd008d dynamic
              [AA21-esxi-6-fc-nvme]
   !
system default zone distribute full
zone smart-zoning enable vsan 102
zoneset distribute full vsan 102
!Active Zone Database Section for vsan 102
zone name FC-AA22-5600 vsan 102
   member device-alias AA21-esxi-1 init
   member device-alias AA21-esxi-2 init
   member device-alias AA21-esxi-3 init
   member device-alias AA21-esxi-4 init
   member device-alias AA22-5600-0-3a target
   member device-alias AA22-5600-1-4a target
   member device-alias AA21-esxi-5 init
   member device-alias AA21-esxi-6 init
zone name FC-NVMe-AA22-5600 vsan 102
   member device-alias AA21-esxi-1-fc-nvme init
   member device-alias AA21-esxi-2-fc-nvme init
   member device-alias AA21-esxi-3-fc-nvme init
   member device-alias AA21-esxi-4-fc-nvme init
   member device-alias AA22-5600-0-3b-fc-nvme target
```

```
member device-alias AA22-5600-1-4b-fc-nvme target
    member device-alias AA21-esxi-5-fc-nvme init
    member device-alias AA21-esxi-6-fc-nvme init
zoneset name Fabric-B vsan 102
   member FC-AA22-5600
   member FC-NVMe-AA22-5600
zoneset activate name Fabric-B vsan 102
do clear zone database vsan 102
!Full Zone Database Section for vsan 102
zone name FC-AA22-5600 vsan 102
   member device-alias AA21-esxi-1 init
   member device-alias AA21-esxi-2 init
    member device-alias AA21-esxi-3 init
   member device-alias AA21-esxi-4 init
   member device-alias AA22-5600-0-3a target
   member device-alias AA22-5600-1-4a target
    member device-alias AA21-esxi-5 init
   member device-alias AA21-esxi-6 init
zone name FC-NVMe-AA22-5600 vsan 102
   member device-alias AA21-esxi-1-fc-nvme init
   member device-alias AA21-esxi-2-fc-nvme init
   member device-alias AA21-esxi-3-fc-nvme init
    member device-alias AA21-esxi-4-fc-nvme init
   member device-alias AA22-5600-0-3b-fc-nvme target
    member device-alias AA22-5600-1-4b-fc-nvme target
    member device-alias AA21-esxi-5-fc-nvme init
   member device-alias AA21-esxi-6-fc-nvme init
zoneset name Fabric-B vsan 102
   member FC-AA22-5600
   member FC-NVMe-AA22-5600
interface mgmt0
 ip address 192.168.168.16 255.255.255.0
interface port-channel102
  switchport trunk allowed vsan 102
  switchport description AA21-6536-B
  switchport speed 32000
  switchport rate-mode dedicated
vsan database
  vsan 102 interface port-channel102
 vsan 102 interface fc1/5
 vsan 102 interface fc1/6
 vsan 102 interface fc1/7
  vsan 102 interface fc1/8
clock timezone EST -5 0
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60
switchname AA21-9124V-2
no terminal log-all
line console
line vty
boot kickstart bootflash:/m9124v-s8ek9-kickstart-mz-npe.9.3.2.bin
boot system bootflash:/m9124v-s8ek9-mz-npe.9.3.2.bin
interface fc1/8
  switchport speed 32000
interface fc1/1
  switchport speed 32000
interface fc1/2
  switchport speed 32000
interface fc1/3
  switchport speed 32000
interface fc1/4
  switchport speed 32000
```

```
interface fc1/5
 switchport speed 32000
interface fc1/6
 switchport speed 32000
interface fc1/7
 switchport speed 32000
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/8
interface fc1/1
  switchport mode auto
interface fc1/2
 switchport mode auto
interface fc1/3
 switchport mode auto
interface fc1/4
 switchport mode auto
interface fc1/5
 switchport mode auto
interface fc1/6
 switchport mode auto
interface fc1/7
 switchport mode auto
interface fc1/1
 switchport description AA21-6536-B:1/35/1
 port-license acquire
 channel-group 102 force
 no shutdown
interface fc1/2
 switchport description AA21-6536-B:1/35/2
  port-license acquire
 channel-group 102 force
 no shutdown
interface fc1/3
 switchport description AA21-6536-B:1/35/3
  port-license acquire
  channel-group 102 force
  no shutdown
interface fc1/4
  switchport description AA21-6536-B:1/35/4
  port-license acquire
  channel-group 102 force
 no shutdown
interface fc1/5
 switchport trunk allowed vsan 102
  switchport description AA22-5600-0:3a
 switchport trunk mode off
 port-license acquire
 no shutdown
```

```
interface fc1/6
 switchport trunk allowed vsan 102
  switchport description AA22-5600-0:3b
 switchport trunk mode off
 port-license acquire
 no shutdown
interface fc1/7
 switchport trunk allowed vsan 102
 switchport description AA22-5600-1:4a
 switchport trunk mode off
 port-license acquire
 no shutdown
interface fc1/8
 switchport description AA22-5600-1:4b
 switchport trunk mode off
 port-license acquire
 no shutdown
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
ip default-gateway 192.168.168.254
```

### Nexus Configurations used in this validation

Nexus A Configuration

```
version 10.2(5) Bios:version 05.47
switchname AA21-93600-1
vdc AA21-93600-1 id 1
limit-resource vlan minimum 16 maximum 4094
limit-resource vrf minimum 2 maximum 4096
limit-resource port-channel minimum 0 maximum 511
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
feature nxapi
```

```
© 2024 Cisco and/or its affiliates. All rights reserved.
```

```
feature bash-shell
cfs eth distribute
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60
feature telemetry
username admin password 5 $5$LPEEDD$18n0a/ovGkzLCgIq.OQgVrhrRa5QY0xLAddG.nrCxR4 role network-admin
ip domain-lookup
ip domain-name adaptive-solutions.local
ip name-server 10.1.168.101
crypto key generate rsa label AA21-93600-1 modulus 1024
copp profile strict
snmp-server user admin network-admin auth md5 3746D2E94FC8C30BAA3BC4F3699B8E0055C6 priv aes-128 5236DEF202
969C02A212A8AE7ED6934D5F8C localizedV2key
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp peer 192.168.168.14 use-vrf management
ntp server 10.81.254.202 use-vrf management
ntp master 3
system default switchport
ip route 0.0.0.0/0 10.1.168.254
vlan 1-2,119,1000,1100-1102
vlan 2
  name native-vlan
vlan 119
  name ib-mgmt
vlan 1000
 name vmotion
vlan 1100
 name vm-traffic
vlan 1101
 name vm-traffic-a
vlan 1102
 name vm-traffic-b
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 192.168.168.254
port-channel load-balance src-dst l4port
vpc domain 10
 peer-switch
 role priority 10
  peer-keepalive destination 192.168.168.14 source 192.168.168.13
 delay restore 150
 peer-gateway
  auto-recovery
  ip arp synchronize
interface Vlan1
 no ip redirects
 no ipv6 redirects
interface Vlan119
 no shutdown
  no ip redirects
  ip address 10.1.168.13/24
  no ipv6 redirects
```

```
interface Vlan1100
 no shutdown
 no ip redirects
 ip address 10.1.100.252/24
 no ipv6 redirects
 hsrp 100
   preempt
   ip 10.1.100.254
interface Vlan1101
  no shutdown
  ip address 10.1.101.252/24
 hsrp 101
   preempt
   priority 105
   ip 10.1.101.254
interface Vlan1102
 no shutdown
  ip address 10.1.102.252/24
 hsrp 102
   preempt
    ip 10.1.102.254
interface port-channel10
 description vPC peer-link
  switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type network
 speed 100000
 duplex full
 no negotiate auto
 vpc peer-link
interface port-channel11
 description AA21-6536-A:Eth1/35
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 11
interface port-channel12
 description AA21-6536-B:Eth1/35
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 12
interface port-channel13
 switchport mode trunk
 switchport trunk native vlan 2
  switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 13
interface port-channel14
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 14
```

```
interface port-channel136
 description MGMT-Uplink
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119
  spanning-tree port type network
  mtu 9216
  vpc 136
interface Ethernet1/1
 description <ucs-domainname>-a:Eth1/35
 switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
 channel-group 11 mode active
 no shutdown
interface Ethernet1/2
  description <ucs-domainname>-b:Eth1/35
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
  channel-group 12 mode active
 no shutdown
interface Ethernet1/3
 description C220-M6-1 mLOM1
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
 channel-group 13
 no shutdown
interface Ethernet1/4
 description C220-M6-2 mLOM1
  switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
  channel-group 14
 no shutdown
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
```

```
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
 description <nexus-b-hostname>:Eth1/29
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 119,1000,1100-1102
 speed 100000
  duplex full
 no negotiate auto
 channel-group 10 mode active
 no shutdown
interface Ethernet1/30
 description <nexus-b-hostname>:Eth1/30
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 speed 100000
 duplex full
  no negotiate auto
 channel-group 10 mode active
 no shutdown
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
interface Ethernet1/34
interface Ethernet1/35
interface Ethernet1/36
 description <mgmt-uplink-switch-a-hostname>:<port>
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119
 mtu 9216
  channel-group 136 mode active
  no shutdown
interface mgmt0
  vrf member management
  ip address 192.168.168.13/24
```

icam monitor scale line console line vty boot nxos bootflash:/nxos64-cs.10.2.5.M.bin telemetry certificate /bootflash/home/admin/telemetry-cert.pem localhost destination-profile destination-group timba-653bf02b6f726134012b59a2-0 ip address 10.1.168.99 port 443 protocol HTTP encoding JSON sensor-group timba-653bf02b6f726134012b59a2-0 data-source NX-API path "show system resources all-modules" sensor-group timba-653bf02b6f726134012b59a2-1 data-source NX-API path "show module" sensor-group timba-653bf02b6f726134012b59a2-2 data-source NX-APT path "show environment power" sensor-group timba-653bf02b6f726134012b59a2-3 data-source NX-API path "show interface fc regex \*" sensor-group timba-653bf02b6f726134012b59a2-4 data-source DME path sys/ch depth 1 query-condition query-target=subtree&target-subtree-class=eqptSensor sensor-group timba-653bf02b6f726134012b59a2-5 data-source DME path sys/ch query-condition query-target=subtree&target-subtree-class=eqptSupC sensor-group timba-653bf02b6f726134012b59a2-6 data-source DME path sys/ch query-condition query-target=subtree&target-subtree-class=eqptFt sensor-group timba-653bf02b6f726134012b59a2-7 data-source DME path sys/intf query-condition query-target=subtree&target-subtree-class=ethpmPhysIf filter-condition u pdated(ethpmPhysIf.operSt) subscription 884 dst-grp timba-653bf02b6f726134012b59a2-0 snsr-grp timba-653bf02b6f726134012b59a2-0 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-1 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-2 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-3 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-4 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-5 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-6 sample-interval 300000 snsr-grp timba-653bf02b6f726134012b59a2-7 sample-interval 0

Nexus B Configuration

```
version 10.2(5) Bios:version 05.47
switchname AA21-93600-2
vdc AA21-93600-2 id 1
  limit-resource vlan minimum 16 maximum 4094
 limit-resource vrf minimum 2 maximum 4096
 limit-resource port-channel minimum 0 maximum 511
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
feature nxapi
feature bash-shell
cfs eth distribute
feature udld
feature interface-vlan
feature hsrp
feature lacp
feature vpc
feature lldp
```

```
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60
feature telemetry
username admin password 5 $5$FFMNLD$jleNSaBR4dYYXNIU2WFfs.2BCl8tY3v/KsG.255JE5/ role network-admin
ip domain-lookup
ip domain-name adaptive-solutions.local
ip name-server 10.1.168.101
crypto key generate rsa label AA21-93600-2 modulus 2048
copp profile strict
snmp-server user admin network-admin auth md5 3777EB3A39B7335F9884B2EB1D3FC5E6D259 priv aes-128 4962845B19
D763649384E2E05F5CDCA4DB3A localizedV2key
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 10.81.254.202 use-vrf management
ntp peer 192.168.168.13 use-vrf management
ntp master 3
system default switchport
ip route 0.0.0.0/0 10.1.168.254
vlan 1-2,119,1000,1100-1102
vlan 2
  name native-vlan
vlan 119
 name ib-mgmt
vlan 1000
 name vmotion
vlan 1100
 name vm-traffic
vlan 1101
  name vm-traffic-a
vlan 1102
 name vm-traffic-b
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
 ip route 0.0.0.0/0 192.168.168.254
port-channel load-balance src-dst l4port
vpc domain 10
  peer-switch
  role priority 20
 peer-keepalive destination 192.168.168.13 source 192.168.168.14
 delay restore 150
 peer-gateway
 auto-recovery
 ip arp synchronize
interface Vlan1
 no ip redirects
 no ipv6 redirects
interface Vlan119
 no shutdown
  no ip redirects
 ip address 10.1.168.14/24
 no ipv6 redirects
interface Vlan1100
 no shutdown
  no ip redirects
  ip address 10.1.100.253/24
  no ipv6 redirects
  hsrp 100
    preempt
```

```
priority 105
    ip 10.1.100.254
interface Vlan1101
 no shutdown
  ip address 10.1.101.253/24
 hsrp 101
   preempt
   ip 10.1.101.254
interface Vlan1102
 no shutdown
  ip address 10.1.102.253/24
 hsrp 102
   preempt
   priority 105
   ip 10.1.102.254
interface port-channel10
 description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type network
 speed 100000
 duplex full
 no negotiate auto
 vpc peer-link
interface port-channel11
 description AA21-6536-A:Eth1/36
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 11
interface port-channel12
 description AA21-6536-B:Eth1/36
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 12
interface port-channel13
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 13
interface port-channel14
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 spanning-tree port type edge trunk
 mtu 9216
 vpc 14
interface port-channel136
 description MGMT-Uplink
 switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 119
 spanning-tree port type network
```

```
mtu 9216
  vpc 136
interface Ethernet1/1
 description <ucs-domainname>-a:Eth1/36
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
 channel-group 11 mode active
 no shutdown
interface Ethernet1/2
  description <ucs-domainname>-b:Eth1/36
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
  channel-group 12 mode active
 no shutdown
interface Ethernet1/3
 description C220-M6-1 mLOM2
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
  channel-group 13
 no shutdown
interface Ethernet1/4
 description C220-M6-2 mLOM2
  switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
 mtu 9216
 channel-group 14
 no shutdown
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
```

```
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
 description <nexus-a-hostname>:Eth1/29
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 119,1000,1100-1102
 speed 100000
  duplex full
  no negotiate auto
 channel-group 10 mode active
 no shutdown
interface Ethernet1/30
 description <nexus-a-hostname>:Eth1/30
  switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119,1000,1100-1102
  speed 100000
 duplex full
 no negotiate auto
 channel-group 10 mode active
 no shutdown
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
interface Ethernet1/34
interface Ethernet1/35
interface Ethernet1/36
 description <mgmt-uplink-switch-a-hostname>:<port>
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 119
 mtu 9216
 channel-group 136 mode active
 no shutdown
interface mgmt0
 vrf member management
  ip address 192.168.168.14/24
icam monitor scale
line console
line vtv
boot nxos bootflash:/nxos64-cs.10.2.5.M.bin
```

telemetry destination-profile destination-group timba-653bf38b6f726134012b8087-0 ip address 10.1.168.99 port 443 protocol HTTP encoding JSON sensor-group timba-653bf38b6f726134012b8087-0 data-source NX-APT path "show system resources all-modules" sensor-group timba-653bf38b6f726134012b8087-1 data-source NX-API path "show module" sensor-group timba-653bf38b6f726134012b8087-2 data-source NX-API path "show environment power" sensor-group timba-653bf38b6f726134012b8087-3 data-source NX-API path "show interface fc regex \*" sensor-group timba-653bf38b6f726134012b8087-4 data-source DME path sys/ch depth 1 query-condition query-target=subtree&target-subtree-class=eqptSensor sensor-group timba-653bf38b6f726134012b8087-5 data-source DME path sys/ch query-condition query-target=subtree&target-subtree-class=eqptSupC sensor-group timba-653bf38b6f726134012b8087-6 data-source DME path sys/ch query-condition query-target=subtree&target-subtree-class=eqptFt sensor-group timba-653bf38b6f726134012b8087-7 data-source DME path sys/intf query-condition query-target=subtree&target-subtree-class=ethpmPhysIf filter-condition u pdated(ethpmPhysIf.operSt) subscription 2779 dst-grp timba-653bf38b6f726134012b8087-0 snsr-grp timba-653bf38b6f726134012b8087-0 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-1 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-2 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-3 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-4 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-5 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-6 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-7 sample-interval 0 subscription 3357 dst-grp timba-653bf38b6f726134012b8087-0 snsr-grp timba-653bf38b6f726134012b8087-0 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-1 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-2 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-3 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-4 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-5 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-6 sample-interval 300000 snsr-grp timba-653bf38b6f726134012b8087-7 sample-interval 0

# Feedback

For comments and suggestions about this guide and related guides, join the discussion on <u>Cisco Community</u> at <u>https://cs.co/en-cvds</u>.

## **CVD Program**

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DIS-CLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FIT-NESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFES-SIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS X-Series, Cisco VCS Manager, Cisco UCS Management Software, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trade-marks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW\_P5)

All other trademarks mentioned in this document or website 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. (0809R)

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)

© 2024 Cisco and/or its affiliates. All rights reserved.

Page 367 of 367