

Design and Deployment Guide Cisco Public

Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Mode

Design and Deployment Guide

Published: May 2024



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: <u>http://www.cisco.com/go/designzone</u>.

Executive Summary

Application modernization is the foundation for digital transformation, enabling organizations to integrate advanced technologies. The key technologies include AI, IoT, cloud computing, and data analytics. Once integrated, these technologies enable businesses take advantage of digital innovations and identify opportunities for growth. These applications are diverse, distributed across geographies and deployed across data centers, edge and remote sites. For instance, new AI workloads, demand modern infrastructure to make inferences in branch offices, in retail locations, or at the network edge. The key challenge for IT Administrators is how to quickly deploy and manage infrastructure at scale, whether with many servers at a core data center or with many dispersed locations.

Hyperconverged Infrastructure (HCI) is the solution to many of today's challenges because it offers built-in data redundancy and a smooth path to scaling up computing and storage resources as your needs grow.

The Cisco Compute Hyperconverged (CCHC) with Nutanix (Cisco HCI with Nutanix) solution helps you overcome the challenge of deploying on a global scale with an integrated workflow. The solution uses Cisco Intersight[®] to deploy and manage physical infrastructure, and Nutanix Prism Central to manage your hyperconverged environment. Cisco and Nutanix engineers have tightly integrated our tools through APIs, establishing a joint cloud-operating model.

Whether it is at the core, edge or remote site, Cisco HCI with Nutanix provides you with a best in class solution, enabling zero touch accelerated deployment through automated workflows, simplified operations with an enhanced solution-support model combined with proactive, automated resiliency, secure cloud-based management and deployment through Cisco Intersight and enhanced flexibility with choice of compute and network infrastructure

This Cisco Validated Design and Deployment Guide provides prescriptive guidance for the design, setup, and configuration to deploy Cisco Compute Hyperconverged with Nutanix in Intersight Standalone mode allowing nodes to be connected to a pair of Top-of-Rack (ToR) switches and servers are centrally managed using Cisco Intersight[®].

For more information on Cisco Compute for Hyperconverged with Nutanix, go to: https://www.cisco.com/go/hci

Solution Overview

This chapter contains the following:

- <u>Audience</u>
- Purpose of this Document
- Solution Summary

Audience

The intended audience for this document includes sales engineers, field consultants, professional services, IT managers, partner engineering staff, and customers deploying Cisco Compute Hyperconverged Solution with Nutanix. External references are provided wherever applicable, but readers are expected to be familiar with Cisco Compute, Nutanix, plus infrastructure concepts, network switching and connectivity, and the security policies of the customer installation.

Purpose of this Document

This document describes the design, configuration, deployment steps for Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Mode (ISM)

Solution Summary

The Cisco Compute Hyperconverged with Nutanix family of appliances delivers pre-configured UCS servers that are ready to be deployed as nodes to form Nutanix clusters in a variety of configurations. Each server appliance contains three software layers: UCS server firmware, hypervisor (Nutanix AHV), and hyperconverged storage software (Nutanix AOS).

Physically, nodes are deployed into clusters, with a cluster consisting of Cisco Compute Hyperconverged All-Flash Servers. Clusters support a variety of workloads like virtual desktops, general-purpose server virtual machines in edge, data center and mission-critical high-performance environments. Nutanix clusters can be scaled out to the max cluster server limit documented by Nutanix. The minimum depends on the management mode. These servers can be interconnected and managed in two different ways:

UCS Managed mode: The nodes are connected to a pair of Cisco UCS[®] 6400 Series or a pair of Cisco UCS 6500 Series fabric interconnects and managed as a single system using UCS Manager. The minimum number of nodes in such a cluster is three. These clusters can support both general-purpose deployments and mission-critical high-performance environments.

Intersight Standalone mode: The nodes are connected to a pair of Top-of-Rack (ToR) switches and servers are centrally managed using Cisco Intersight[®]. While a minimum of three nodes are required to deploy a standard Nutanix cluster, we also offer an option to deploy a single node cluster and a two-node cluster for Edge and branch locations and situations that already have a high-performance network fabric installed.

The present solution elaborates on design and deployment details to deploy Cisco C-Series nodes for Nutanix configured in Intersight Standalone Mode.

Technology Overview

This chapter contains the following:

- <u>Cisco Intersight Platform</u>
- <u>Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers</u>

The components deployed in this solution are configured using best practices from both Cisco and Nutanix to deliver an enterprise-class data protection solution deployed on Cisco UCS C-Series Rack Servers. The following sections provide a summary of the key features and capabilities available in these components.

Cisco Intersight Platform

As applications and data become more distributed from core data center and edge locations to public clouds, a centralized management platform is essential. IT agility will be a struggle without a consolidated view of the infrastructure resources and centralized operations. Cisco Intersight provides a cloud-hosted, management and analytics platform for all Cisco Compute for Hyperconverged, Cisco UCS, and other supported third-party infrastructure deployed across the globe. It provides an efficient way of deploying, managing, and upgrading infrastructure in the data center, ROBO, edge, and co-location environments.



Cisco Intersight provides:

- No Impact Transition: Embedded connector (Cisco HyperFlex, Cisco UCS) will allow you to start consuming benefits without forklift upgrade.
- SaaS/Subscription Model: SaaS model provides for centralized, cloud-scale management and operations across hundreds of sites around the globe without the administrative overhead of managing the platform.
- Enhanced Support Experience: A hosted platform allows Cisco to address issues platform-wide with the experience extending into TAC supported platforms.
- Unified Management: Single pane of glass, consistent operations model, and experience for managing all systems and solutions.
- Programmability: End to end programmability with native API, SDK's and popular DevOps toolsets will enable you to deploy and manage the infrastructure quickly and easily.

- Single point of automation: Automation using Ansible, Terraform, and other tools can be done through Intersight for all systems it manages.
- Recommendation Engine: Our approach of visibility, insight and action powered by machine intelligence and analytics provide real-time recommendations with agility and scale. Embedded recommendation platform with insights sourced from across Cisco install base and tailored to each customer.

For more information, go to the Cisco Intersight product page on cisco.com.

Cisco Intersight Virtual Appliance and Private Virtual Appliance

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

Licensing Requirements

The Cisco Intersight platform uses a subscription-based license with multiple tiers. You can purchase a subscription duration of 1, 3, or 5 years and choose the required Cisco UCS server volume tier for the selected subscription duration. Each Cisco endpoint automatically includes a Cisco Intersight Base license at no additional cost when you access the Cisco Intersight portal and claim a device. You can purchase any of the following higher-tier Cisco Intersight licenses using the Cisco ordering tool:

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

Servers in the Cisco Intersight managed mode require at least the Essentials license. For more information about the features provided in the various licensing tiers, go to:

https://www.intersight.com/help/saas/getting_started/licensing_requirements

Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers

The Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers extends the capabilities of Cisco's Compute Hyperconverged portfolio in a 2U form factor with the addition of the 4th Gen Intel[®] Xeon[®] Scalable Processors (codenamed Sapphire Rapids), 16 DIMM slots per CPU for DDR5-4800 DIMMs with DIMM capacity points up to 256GB.

The All-NVMe/all-Flash Server supports 2x 4th Gen Intel[®] Xeon[®] Scalable Processors (codenamed Sapphire Rapids) with up to 60 cores per processor. With memory up to 8TB with 32 x 256GB DDR5-4800 DIMMs, in a 2-socket configuration. There are two servers to choose from:

- HCIAF240C-M7SN with up to 24 front facing SFF NVMe SSDs (drives are direct-attach to PCIe Gen4 x2)
- HCIAF240C-M7SX with up to 24 front facing SFF SAS/SATA SSDs

For more details, go to: HCIAF240C M7 All-NVMe/All-Flash Server specification sheet

cisco	ADD GR	Host Can	001.00	Sid CF	PEO LA	100.00	310 60	BOD GB	010 68	100 64	400.68	820 GB	HOD GB	B20 GB	101.09	100108	tot Ga	ENT GR		HON CA	BOD DR	UCS C240 MP

Figure 1. Front View: HCIAF240C M7 All-NVMe/All-Flash Servers

Reference Architecture

This chapter contains the following:

- Deployment Architecture
- Licensing
- Software Components

Deployment Architecture

The deployment architecture for Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Mode (ISM) is detailed in <u>Figure 2</u>. The entire Day0 deployment is managed through Cisco Intersight and Nutanix Foundation Central enabled through Prism Central.

Each C240 M7 All NVMe server is configured with the following:

- 2x Intel(R) Xeon(R) Gold I6448H
- 384 GB DDR5 memory
- 2x 240GB M.2 card managed through M.2 RAID controller
- 24x 1.9 TB NVMe
- 1x Cisco VIC 15425 4x 10/25/50G PCIe C-Series w/Secure Boot

Note: This document illustrates the Cisco HCIAF240C M7 All-NVMe/All-Flash Servers specifications as validated in this document. You have several options to configure CPU, Memory, Network cards, GPUs and storage as detailed in this spec sheet: <u>Cisco Compute Hyperconverged with Nutanix</u>

Figure 2. High-level Deployment Architecture



Figure 3 illustrates the cabling diagram for CCHC with Nutanix in ISM mode.





Licensing

Cisco Intersight Licensing

Cisco Intersight uses a subscription-based license with multiple tiers. Each Cisco automatically includes a Cisco Intersight Essential trial license when you access the Cisco Intersight portal and claim a device.

More information about Cisco Intersight Licensing and the features supported in each license can be found here: <u>https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-infrastructure-service/licensing.html</u>

In this solution, using Cisco Intersight Advantage License Tier enables the following:

- Configuration of Server Profiles for Nutanix on Cisco UCS C-Series Rack Servers
- Integration of Cisco Intersight with Foundation Central for Day 0 to Day N operations

Software Components

<u>Table 1</u> lists the software components and the versions validated for the Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Software Components.

Table 1. Software components and versions

Component	Version
Foundation Central	1.6

Component	Version
Prism Central deployed on ESXi cluster	pc.2022.6.0.10
AOS and AHV bundled	nutanix_installer_package-release-fraser-6.5.5.6
Cisco C240 M7 All NVMe server	4.3(3.240043)

Solution Deployment

This chapter contains the following:

- Prerequisites
- <u>Cisco IMC configuration</u>
- <u>Cisco Intersight Configuration and Keys</u>
- <u>Claim Servers on Cisco Intersight</u>
- Configure Foundation Central
- Nutanix Cluster Creation
- Post Cluster Creation Task

This chapter describes the solution deployment for Nutanix on Cisco UCS C-Series Rack Servers in Intersight Standalone Mode (ISM), with step-by-step procedures for implementing and managing the deployment. The Intersight Standalone Mode requires the Cisco UCS C-Series Rack Servers to be directly connected to a ethernet switches and the servers are claimed through Cisco Intersight.

Note: If you are deploying a Nutanix ISM cluster, refer to the <u>Nutanix ISM Field Install Guide</u> for step-bystep guidance. This guide explains the installation and initial configuration of Cisco Compute Hyperconverged with Nutanix systems using Standalone Cisco UCS C-Series servers managed by Cisco Intersight. This guide is intended for technical training and educational purposes, for all who wish to install Nutanix on Cisco UCS based hardware following our supported hardware and software integrations and compatibility lists. This document presents our best practices and recommendations as of the time of publishing and will be updated periodically. Please refer to the document history to ensure you are using the most current version available

<u>Figure 4</u> shows the high-level configuration of Cisco UCS C-Series nodes in Intersight Standalone Mode for Nutanix.



Figure 4. Cisco UCS C-Series Nodes configured in Intersight Standalone Mode for Nutanix

Prerequisites

Prior to beginning the installation of Nutanix Cluster on Cisco UCS C-Series servers in Intersight Standalone Mode, you should ensure they have deployed Nutanix Prism Central and enabled Nutanix Foundation Central

through Nutanix marketplace available through Prism Central. Foundation Central can create clusters from factory-imaged nodes and reimage existing nodes that are already registered with Foundation Central from Prism Central. This provides benefits such as creating and deploying several clusters on remote sites, such as ROBO, without requiring onsite visits

At a high level, to continue with the deployment of Nutanix on Cisco UCS C-Series servers in Intersight standalone mode (ISM), ensure the following:

- Prism Central is deployed on either a Nutanix Cluster or on ESXi cluster
- Foundation Central 1.6 or later is enabled on Prism Central
- · A local webserver is available hosting Nutanix AOS image

Note: Either deploy Prism Central 2023.4 or newer on Nutanix Cluster or deploy Prism Central 2022.6.x available as OVA on ESXi cluster

Prism Central Installation

The following high-level steps describe the process to deploy Prism Central either on a Nutanix Cluster or on an ESXi cluster. You should follow either of the procedures for PC installation.

Procedure 1. Deploy PC 2023.4.x on Nutanix Cluster

Note: Skip this step if you already have PC 2023.4 or newer.

Step 1. Login to Prism Element on Nutanix Cluster and navigate to Settings -> Prism Central Registration.

🗙 ntnx-ism-trunk-1 Settings 🔹 😻 🌲 🔕 🚥 🔿 🗸	
Settings	Prism Central
Setup Connect to Citrix Cloud	Not registered Register or create new
Prism Central Registration Pulse	
Rack Configuration	
Network	
Name Servers	
Network Configuration Network Switch	
NTP Servers	
SNMP	

Step 2. Select the option to deploy a new Prism Central instance.



Step 3. Prism Central binaries are available here: <u>https://portal.nutanix.com/page/downloads?product=prism</u>, download PC version 2023.4.x or upload to the library.

Prism Central Deployment X							
1 2 3 4	PC version Scale type Configuration Summary	Select an image to install, download the latest version from the Internet or upload one from your computer. Available versions Show compatible version pc.2022.6.0.10 You can upload the Prism Central binary instead of downloading from the Internet.	ons				
<	Back	Cancel	t				



	Select an image to install, download the latest version from
Scale type	the Internet or upload one from your computer.
Configuration	Available versions Show compatible versions
conngulation	pc.2023.4 × •
Microservices	
	downloading from the Internet.

Step 4. Select the appropriate Prism Central deployment option as per your resiliency requirement.



Step 5. Enter valid network details and IP addressing for Prism Central. Even though DNS is optional, ensure a valid DNS is defined for successful discovery of Cisco Intersight domain name.

	Prism Central Deployment	×
 PC version Scale type Configuration Summary 	Select a PC size and provide your Network details. Small (6 vCPUs and 26 GB Memory) For managing up to 2,500 VMs Large (10 vCPUs and 44 GB Memory) For managing up to 12,500 VMs X-Large (14 vCPUs and 60 GB Memory) For managing up to 12,500 VMs Resources included for all optional services Network VMNetwork	•
	Subnet Mask Gateway 255.255.255.0 10.108.1.254 DNS Address(es) Opt 10.108.1.6,172.20.4.53,172.20.4.54 0	ional
	Select a Container SelfServiceContainer VM Name PC-NameOption-1	•
< Back	Cancel	Next

Step 6. Deploy Prism Central on Nutanix Cluster.

		Prism Central Deploym	nent
1	PC version	PC version	pc.2023.4
2	Scale type	Scale type	Single-VM PC
3	Configuration	Added resiliency:	-
4	Microservices	Configuration	
5	Summary	VM Size	Small (up to 2,500 VMs)
		vCPUs	6
		Memory	26 GiB
		Storage	500 GiB
		Network	VMNetwork
		Subnet Mask	255.255.255.0
		Gateway	10.108.1.254
		DNS Address(es)	10.108.1.6,172.20.4.53,172.20.4.54
		NTP Address(es)	172.20.10.18,172.20.10.15
		Container	SelfServiceContainer
		VM Name	PC-NameOption-1
		IP	10.108.1.230
		Microservices	
		Prism Central Service Do Name	prism-central.cluster.local
		Internal Network	Private Network [default]
		Subnet Mask	255.255.255.0
<	Back		Cancel

Procedure 2. Deploy PC 2022.6.x on ESXi Cluster

Note: Skip this step if you already have a Prism Central Instance.

Step 1. Download Prism Central 2022.6.x OVA here: <u>https://portal.nutanix.com/page/downloads?product=prism</u>

Step 2. Identify an ESXi host and deploy OVF template.

eploy 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	Ourl	
3 Select a compute resource		
4 Review details	Local file	
5 Select storage	UPLOAD FILES pc 2022.6.0.10.ova	
6 Ready to complete		
	CANCEL N	XT

Step 3. Identify compute, storage, and network resource on ESXi Cluster and deploy the OVF template.

Deploy OVF Template	Ready to comp Click Finish to start creat	plete tion.	×
1 Select an OVF template			
2 Select a name and folder	Name	prismcentral.2022.6.0.10	
	Template name	pc.2022.6.0.10	
3 Select a compute resource	Download size	5.5 GB	
4 Review details	Size on disk	8.4 GB	
	Folder	DC1	
5 Select storage	Resource	10.108.1.7	
6 Select networks	Storage mapping	1	
7 Ready to complete	All disks	Datastore: ds1-ssd; Format: Thin provision	
	Network mapping	1	
	VM Network	VM Network	
	IP allocation settings		
	IP protocol	IPV4	
	IP allocation	Static - Manual	
		CANCEL BACK	FINISH

Step 4. Once the OVA is deployed, power ON the VM. Post installation steps for Prism Central on ESXi are detailed here: <u>https://portal.nutanix.com/page/documents/details?targetId=Acropolis-Upgrade-Guide-v6_5:upg-vm-install-wc-t.html</u>.

Note: Please wait at least 20-25 minutes before you login to PC instance through ESXi web console.

- Step 5. Launch VM web console and login with login: Nutanix password: nutanix/4u.
- **Step 6.** Edit the ifcfg-eth0 with the following settings (/etc/sysconfig/network-scripts/ifcfg-eth0):

NETMASK="xxx.xxx.xxx.xxx"

IPADDR="xxx.xxx.xxx.xxx" BOOTPROTO="none" GATEWAY="xxx.xxx.xxx.xxx.

DEVICE=eth0 BOOTPROTO=none ONBOOT=yes NETMASK=255.255.255.0 GATEWAY=10.108.1.254 IPADDR=10.108.1.230_

Step 7. Restart the Prism Central VM and login with username Nutanix.

Step 8. Create a Prism Central cluster with the following command:

cluster --cluster_function_list="multicluster" -s static_ip_address create

** SSH to PCVM via 'nutanix' user will be restricted in coming releases. ** ** Please consider using the 'admin' user for basic workflows. ** nutanix@NTNX-10-108-1-230-A-PCVM:~\$ cluster --cluster_function_list="multicluster" -s 10.108.1.230<mark>|</mark>create

Step 9. Once completed, login to Prism Central 2022.6.x.

= Q Dashboard			👌 Prism			🚺 🔿 🔕 ? 🌣 admin '
Main Dashboard 🌣 Manag	ge Dashboards				Reset Dashboard + A	Add Widgets Data Density :
Alerts	Last 24 hours :	Cluster Quick Access	Cluster Storage		Cluster Latency	Last Hour =
1 2 1 Critical Warning Info		Click on any line to open a Prism Element Instance in a new tab.			No clusters	were found.
		No clusters were found.	No clusters were found.			
		churte contraction and the state	Contrall of DEC	1	Churter Daman	
Cluster Memory Usage Last Hour : No clusters were found.		No clusters were found.	No clusters were found.		No data	avallable
VM Efficiency		Plays	Tasks		Reports	
			View All Task(s)	Details		
0 Overprovisioned	O	Plays Completed	Create report config	Succeeded		
		in the last 24 hours	Create report config	Succeeded	3	0
0	0	Failed	Create report config: Cluster Efficiency Summary	Succeeded	Total Reports	Scheduled Reports

Enable and Upgrade Foundation Central

This section provides the process to enable and upgrade Foundation Central on Prism Central 2022.6.x and 2023.4.x.

Procedure 1. Enable and Upgrade Foundation Central (FC) on PC 2022.6.x

Note: Ensure the DNS (name server) and NTP settings are updated in Prism Central.

Step 1. Go to Services > Foundation Central and enable Foundation Central.

E Q. Foundation Central	💩 Prism	🐥 🚺 🔾 🗿 🤶 🗘 admin 🗸
Dashboard		
Compute & Storage v		
Data Protection ~		
Activity ~ Operations ~		
Administration ~		
Calm O	Foundation Central	
Foundation Central	Foundation Central can manage several Foundation instances from a single pane of glass, allowing you to create clusters of remote nodes without needing to configure each of them individually.	
Objects 🕆	Enable Foundation Central	
Prism Central Settings		

Step 2. Download FC 1.6 from: https://portal.nutanix.com/page/downloads?product=foundationcentral

Step 3. Upgrade FC to 1.6 as described here: <u>https://portal.nutanix.com/page/documents/details?targetId=Foundation-Central-v1_6:v1-upgrade-fc-cli-</u>t.html.

Step 4. SSH into Prism Central VM with user name nutanix.

Step 5. Stop Foundation Central service 'genesis stop foundation_central.'

Step 6. Remove existing Foundation Central files, if exists 'sudo rm -rf /home/docker/foundation_central/*'

Step 7. Extract Foundation Central tar file 'sudo tar -xf foundation-central-installer.tar.xz -C /home/docker/foundation_central/'

Step 8. Change the directory permission to nutanix:Nutanix 'sudo chown -R nutanix:nutanix /home/docker/foundation_central/*'

Step 9. Restart Foundation Central service 'genesis restart.'

Step 10. Foundation Central service will display after some time. You can validate service status by running "genesis status" command on your PC VM.

Procedure 2. Enable and Upgrade Foundation Central (FC) on PC 2023.4.x

Note: Ensure the DNS (name server) and NTP settings are updated in Prism Central.

Note: To enable marketplace on Prism Central 2023.4, the Nutanix cluster hosting PC 2023.4 should be registered to Prism Central.

Step 1. Enable marketplace on Prism Central 2023.4.

Step 2. Go to marketplace and get Foundation Central Application.



Step 3. Once deployed, upgrade Foundation Central to latest version (1.6) by performing Inventory on LCM.

≡	X Admin Center				Q. Lon	n J	. 8	0	?	🗘 admir	~
My A Mark	pps stplace	LCM	Best Practices In	iventory	Updates	Settings	ø Co	nnected	- Portal	Version 2.7.	
Proje			Overall Progress May 30, 2024		0	Performing Inventory This can take several minutes depending on the size of your cluster. Once completed, you can view available updates for the cluster.			55%		
LCM						Stage 1/1: Auto Update					
¢s			Stage 1/1: Auto Update 1:32:11 PM	te	0	Auto Update Restarting genesis service on CVM: 10308.1340			•		

Step 4. Go to marketplace and get Foundation Central Application.

≡ × Admin Center		Q. Lom			4 💷 O 💿 ? 🌣	admin
My Apps	LCM Best Practices Inventory	Updates 5 Settings			S Connected - Portal Ver	rsion 3.0
Marketplace Projecta	The latest available versions have been aut cannot update AOS or AHV from Prism Cer general settings menu.	to populated. If available, you may select other stral. To update these components, switch to Pr	versions, LCM will auto-select the entity version ism Element and use LCM from there. Automat	n to resolve any dependencies. Please review al ic updates for the NCC module can now be enal	I selections before continuing, LCM sled via Auto Inventory in the	×
IAM	View Upgrade Plan Pre-Upgrade	. w			Ŧ	Filter
Licensing	Viewing all 5 Software Updates					
	Software	Available Version	Current Version	Last Updated	Release Notes	
Settings	Epsilon	3.7.2.1 1 version updato	372			
	Foundation Central	1.6 1 version update	1.5		View Release Notes	
	Network Controller - 406b0698-0ddc- 4248-9934-2c236b1217d0	3.0.2 1 version update	3.01			
	Nutanix Kubernetes Engine	2.10.0 t version update	2.9.0		View Release Notes	
	Self Service	3.7.2.1 1 version update	3.7.2			

Step 5. Once Foundation Central is upgraded to 1.6, proceed to the subsequent sections.

Create IMC Configuration (CIMC)

Procedure 1. Configure CIMC

Note: This step has to be completed for all the Cisco UCS C-Series nodes configured for Nutanix cluster.

This procedure provides a Management IP to each of the node enabling connection to Cisco Intersight.

Step 1. Attach a keyboard and monitor to the USB ports on the rear panel of the Cisco UCS C240 Rack Server or by using a KVM cable (Cisco PID N20-BKVM) and connector to access the appliance console.

Step 2. During bootup, press F8 when prompted to open the Cisco IMC Configuration Utility.

Step 3. When prompted enter the default CIMC username (admin) and password (password).

Step 4. When prompted, change the default CIMC (IPMI) username and password. You must enter a strong password.

Step 5. Enable the NIC mode Dedicated field by entering a space.

Step 6. Enable either the IP (Basic) IPV4 field or the IP (Basic) IPV6 field to reflect your networking environment.

Step 7. Arrow down to the IP (Basic) DHCP enabled field and enter a space to disable it.

Step 8. Arrow down to the NIC redundancy None field and enter a space to enable it.

Step 9. Enter appropriate values for your network in the following fields:

- CIMC IP–Specify the IP address to access the Cisco Integrated Management Controller (CIMC) which is similar to IPMI.
- Prefix/Subnet-Specify the Subnet Mask for the CIMC (IPMI) Subnet.
- Gateway–Specify the IP address of the Subnet Gateway for the CIMC (IPMI) network interfaces.
- Pref DNS Server–Specify the IP Addresses of the preferred Domain Name System (DNS) Server.

The details for the CIMC settings for the Cisco UCS C240 Rack Servers are shown below:

		117.0				
1 -4		NIG	reoundancy		0-2	
ц <u>а</u> ј		Noni			23	
[]		Act.	ive-standby	-	[]	
		Act.	ive-active:		[]	
[]		VLAN	(Advanced)			
[]		VLA	N enabled:		[]	
[]		VLA				
[]		Pri	ority:			
DCI	IPV6:	[]				
[]						
10.1.0.1						
10.1.0.1						
20121012						
r 1						
	20 () () () () () () () ()	20 [] [] [] [] [] [] [] [] [] []	NIC 1 [2] Hone [] Act Act Act I VLAN [] VLAN [] VLAN [] Prio [] [] 10.1.0.1 10.1.0.1 10.1.0.1	NIC redundancy [2] None: [] Active-standby Active-standby Active-active [] VLAN (Advanced) [] VLAN (Advanced) [] VLAN ID: [] Priority: [] IPV6: [] IPV6:	NIC redundancy [2] None: [1] Active-standby: [2] VLAW (Rdvanced) [1] VLAW (Rdvanced) [2] VLAW enabled: [3] VLAW enabled: [4] VLAW enabled: [5] VLAW enabled: [6] VLAW enabled: [7] Priority: [8] 1946: [9] 1946: [1] 10.1.0.1	NIC redundancy [2] None: [2] Active-standby: [] Active-active: [] VLAN (Advanced) [] [] VLAN mobiled: [] [] VLAN ID: 1 [] Priority: 0 [] IPV6: [] [] IPV6: [] [] IPV6: []

Step 10. Enter F10 to save the settings.

Step 11. Repeats steps 1-10 for all the nodes deployed for Nutanix Cluster in ISM mode.

Cisco Intersight Configuration and Keys

Procedure 1. Enable Intersight software download permission

This option allows Cisco Intersight to download recommend firmware from cisco.com using the user account for cisco.com

Step 1. Login to Cisco Intersight, go to System > Settings > Cisco ID and from the Cisco software download option click Activate.



Step 2. Once activated, the login screen displays. Login with your CEC or Cisco ID.

Gen	erate Security Token
i	To upgrade firmware from Cisco Repository, Intersight must be enabled for Cisco Software Download Services. Learn more at Help Center.
Provide you to d The sec account	your user credentials to generate the security token that enables lownload firmware images from the cloud. urity token expires if there has been no upgrade activity in the for 30 days.
Cisco I andh	D*
Passw	ord *
	Cancel Generate

Step 3. Once the user is authenticated, the software download access status will change to the active state.



Procedure 2. Generate Cisco Intersight API keys

The Cisco Intersight API keys allows authentication and communication of Nutanix Foundation Central with Cisco Intersight. Further, once the communication channel is setup, Nutanix Foundation Central can identify the Cisco C-Series nodes claimed in Intersight and configure Server profile and upgrade firmware of Cisco UCS C-Series Rack Servers in ISM mode.

Step 1. Login to Cisco Intersight, go to System > Settings > API keys.



Step 2. Click Generate API Keys.

= "linelin Intersight	System V			Q Search	C @	D 43	Q 💿 🚮	0	ዾ
Settings	A There are 1 Warning, 1 Info alerts. Exp								~
Admin Targets	Settings								
Tech Support Bundles Audit Logs Sessions Licensing	GENERAL Account Details Access Details Notifications AUTHENTICATION	API Keys * All API Keys © + @ @ @ Mod Filter Descript : API K	Gay ID	O items four S. : Purp Cr :	id 13 E. :	∽ per L. :	Generate A page « < 0 of 0 Email Role	PI Key)
New Command Palette Nuvigate Intensight with CMI-K or go to Help > Command Palette	Single Sign-On Domain Names Cisco ID Trusted Certificates	/ 6	N	IO ITEMS AVAILABLE			≪ < 0 of 0		

Step 3. Select the API key for OpenAPI schema version 3, add a description and key expiration date and click Generate.

Generate API Key	×
Generate API key to auther requests with Intersight ac	nticate and authorize API acount.
Description* (j)	
ISM Key	
API Key Purpose 🕦	
API key for OpenAPI schema ver	ersion 3 🛈
API key for OpenAPI schema ve	ersion 2 (deprecated) 🛈
Expiration Time* ()	
Nov 23, 2024 02:46 PM	
	Close Generate

Step 4. Once generated, save the API key ID and Secret Key at a secure place. This will be subsequently added in Nutanix Foundation Central.



Claim Servers on Cisco Intersight

The following high-level steps describe the process to claim servers on Cisco Intersight. Ensure CIMC of all servers have been configured with proper DNS for Cisco Intersight reachability

Procedure 1. Claim servers on Cisco Intersight

Step 1. Open a web browser and type in Cisco IMC IP, login with the username: admin and the password as configured during CIMC configuration.

	Please note: Intersight In	frastructure Services license	is required with this server. Learn M	More.
hassis / Summary 🖈				Refresh Host Power Launch vKVM Ping CIMC Reboot Locator LED
erver Properties	Cisco Integrated M	lanagement Controller	(Cisco IMC) Information	
Product Name: UCS C240 M7SN	Hostname:	C240-WZP2736045T		
Serial Number: WZP2736045T	IP Address:	10.108.0.113		
PID: UCSC-C240-M7SN	MAC Address:	EC:F4:0C:61:21:C0		
UUID: 4E4E4208-8464-4006-80A3-8AA411965B8F	Firmware Version:	4.3(3.240043)		
BIOS Version: C240M7.4.3.3a.0.0118241337	Current Time (UTC):	Tue May 07 15:07:10 2024		
Description:	Local Time:	Tue May 7 15:07:10 2024 UTC +0	1000 (Local)	
Asset Tag: Unknown	Timezone:	UTC	Select Timezone	
Personality: Nutanix HCI Node				
hassis Status	Server Utilization			
Power State: Off	Overall Utilizat	ion (%): N/A		
Post Completion Status: Not-Completed	CPU Utilizat	ion (%): N/A		
Overall Server Status: 🧖 Good	Memory Utilizat	ion (%): N/A		
Temperature: 🧖 Good	IO Utilizat	ion (%): N/A		
Overall DIMM Status: 🖾 Good				
Power Supplies: 🧖 Good				
Fans: 🧖 Good				
Locator LED: Off				

Step 2. From the left navigation pane, go to Admin > Device Connector.

	Cisco Integrated Management Control	lier	united with this server Law Nov
Chassis	A / Chassis / Summary *	initiastractore dervices license is re	quires that street, contratore.
Compute	Server Properties	Cisco Integrated N	Management Controller (Cisco IMC) Information
	Product Name: UCS C240 M7SN	Hostname:	C240-WZP2736045T
Networking	Serial Number: WZP2736045T	IP Address:	10.108.0.113
0	PID: UCSC-C240-M7SN	MAC Address:	EC:F4:0C:61:21:C0
Storage	UUID: 4E4E4208-8464-4006-80A3-8AA411965B8F	Firmware Version:	4.3(3.240043)
Admin	BIOS Version: C240M7.4.3.3a.0.0118241337	Current Time (UTC):	Tue May 07 15:07:10 2024
Admin	Description:	Local Time:	Tue May 7 15:07:10 2024 UTC +0000 (Local)
User Management	Asset Tag: Unknown	Timezone:	UTC Select Timezone
Networking	Personality: Nutanix HCI Node		
Communication Services			
Security Management	Chassis Status	Server Utilization	
Event Management	Power State: Off	Overall Utilizat	tion (%): N/A
	Post Completion Status: Not-Completed	CPU Utilizat	tion (%): N/A
Firmware Management	Overall Server Status: Sood	Memory Utilizat	tion (%): N/A
Utilities	Temperature: 🥙 Good	IO Utilizat	tion (%): N/A
Davies Connector	Overall DIMM Status: Sood		
Device Connector	Power Supplies: Sood		
	Fans: Good		
	Locator LED: Off		
	Overall Storage Status: 🖾 Good		

Step 3. From the Device Connector page, ensure the server is not connected to Intersight and identify the Device ID and Claim Code. This will be utilized to claim the server on Cisco Intersight.

😸 📲 Cisco Integrated Management Controller 🗧 🗧	admin@10.108.1.2 - C240-WZP2736045T 🄅
Please note: Intersight Infrastructure Services license is required with this server. Learn More.	
A / Admin / Device Connector 🖈 Patresh Host Power Laur	ch vKVM Ping CIMC Reboot Locator LED @
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center	
Device Connector	⊙ Settings │ ⊖ Refresh
ACCESS MORE ALLOW CONTROL Device Connector Device Connector Mersign	Device ID WZP2736045T
Not Claimed	
The connection to the Clisco Intersight Portal is successful, but device is still not claimed. To claim the device open Clisco Intersight, create a new account and follow the guidance or go to the Targets page and click. Claim a New Device for Open Intersight 1.0.11-3233	



Step 4. Login to Cisco Intersight and navigate to System > Targets.





Step 6. Enter the Device ID and Claim code as copied from the Cisco IMC device connector page.

≡ diada Intersight] System ∨	Q Search	C © 4	Q 📵 🔺	ک ®
Ø Settings	There are 1 Warning, 1 Info alerts. Expand All				~
Admin Admin Targets Tach Support Bundles	- _{Targets} Claim a New Target				
Audit Logs Sessions Licensing	Claim Cisco UCS Server (Standalone) Target To claim your target, provide the Device ID, Claim Code and select the appropriate Resource Groups. General Device ID * 0 Claim Code * 0 WZP27360451				
New Command Palette × Navigate Intersight with Ctri+K or go to Help > Command Palette	Resource Groups Select resource groups, if required. This is not mandatory, since by default, the claimed targe	t will be added to "All" type resource groups.			
	Name Usage	0 items found 10 \sim per page \ll < 0 Description	0 of 0 > > ③		
	NO ITEMS AVAILABLE				
			≪ < 0 of 0 > ≫		
					Claim

Step 7. Ensure the server is successfully claimed on Cisco Intersight.

= the Intersight	a System ∨	Q Search C O A Q @ (1) (9)	R
	A There are 1 Warning, 1 Info alerts. Expand All		
Admin ^ Targets	Targets	Claim a New Tar	get
Tech Support Bundles	★ All Targets ⊕ +		
Audit Logs	C D Add Filter	C Export 1 items found 10 → per page ≪ < 1 of 1 > ≫	
Sessions	Health Connection Top Targets by Types	Vendor	
Licensing	• Healthy 1 • Standalone M6/M7_ 1	1 * Cisco Systems, Inc. 1	
New Command Palette			
Navigate Intersight with Ctrl+K or go to Help > Command Palette	C240-WZP2736045T C240-WZP2736045T C4ealthy Connected Standalo	lone M7 Server a few seconds ago andhiman@cisco.com ···	

Step 8. Repeat Steps 1-7 and claim the remaining servers provisioned for Nutanix cluster with Cisco UCS C240 M7 in ISM mode.

≡ diada Intersight	📲 System 🗸		Q Search	C © 4 0 0 01	ଡ
Ø Settings	A There are 1 Warning, 1 Info alerts. Expand All				~
🚺 Admin ^	Targets			Clair	m a New Target
Targets					
Tech Support Bundles	★ All Targets ◎ +				
Audit Logs	🖉 📋 🔍 Add Filter		Export 4 items found	i 10 v per page « < 1	of 1 $> \gg$
Sessions	Health Connectio	n Top Targets by Types	Vendor		XX
Licensing	4 • Healthy 4	• Standalone M8/M7 4	4 • Cisco Systems, Inc. 4		
New Command Palette					
Navigate Intersight with Ctrl+K or	Name : Health	: Status : Type	Claimed Time	: Claimed By	: Ø
go to Help > Command Palette	C240-WZP2736044T C2 Healthy	Connected Stands	alone M7 Server a few seconds ago	andhiman@cisco.com	***
	C240-WZP2737078Q C Healthy	Connected Stands	alone M7 Server 2 minutes ago	andhiman@cisco.com	
	C240-WZP2736045M C Healthy	Connected Stands	alone M7 Server 6 minutes ago	andhiman@cisco.com	***
	C240-WZP2736045T C Healthy	Connected Stands	alone M7 Server 13 minutes ago	andhiman@cisco.com	***
				« < 1	of 1 > >>

Configure Foundation Central

This procedure describes the Foundation Central configuration required for a successful Nutanix cluster creation with Cisco UCS C-Series nodes in ISM mode.

Procedure 1. Generate API key

Note: API key authenticates API communication between the Nutanix node and Foundation Central. It is recommended that you create a unique key for each remote site.

Step 1. Login to Prism Central and navigate to Foundation Central.

Step 2. Click Generate API key.



The API key displays. It will be added during the Nutanix cluster creation through Foundation Central.

≡	Q. Foundation Central	۵	Prism			• •	0	? 🌣	admin Y
Foun	dation Central Version 1.6								
Nodes	odes Deployment History API Keys Management Foundation Central Settings								
API K	API Keys Management								
+ G	enerate API Key								
Found	tion Central requires some additional configuration in your D	DHCP server, such as applying one of the API keys below. See node of	discovery setup guide	i					
API Ke	VPI Keys Last ando spekind at 3.55.24 PM								
Alias	0	Created Time 🖕	Actions		Registered Nodes				
ntnx	ism-api-1	4/10/2024, 5:39:45 PM	View Delete		3 Nodes				۲

Procedure 2. Cisco intersight connection to Foundation Central

This procedure allows the connection of Foundation Central to Cisco Intersight through the Cisco Intersight API key created in the Intersight configuration. This allows Foundation Central to discover nodes claimed on Cisco Intersight.

Step 1. From Foundation Central, navigate to Foundation Central Settings. Click Connect Hardware Provider.

⊒ Q. Foundation Central ☆	A Prism	🗍 🗿 📀 🔅 💠 admir
Foundation Central Version 1.6		
Nodes Deployment History API Keys Management	oundation Central Settings	
Foundation Central Settings		
	Connect Hardware Provider	
	Connect a Hardware Provider to onboard nodes to Foundation Central. Enter a unique name for each connection and provide the hardware provider details.	

Step 2. From Connect Hardware Provider, enter a Connection Name and select the Hardware Provider as 'Cisco Intersight' and select the option as 'SaaS'. Intersight URL is automatically displayed as per the region configured in Foundation Central.

Connect Hardware Prov	vider >	<
Connection Details		
Connection Name		1
intersight		1
Only the special characters are allowed		1
Hardware Provider		1
Cisco Intersight	\$	1
Intersight Deployment Type		1
 SaaS Connected/Private Virtual Applia 	ance	1
Intersight Region & URL		1
North America + https://us-east-1.intersight.	.com	I

Step 3. From Connection Credential, enter the Intersight API key ID and secret Key generated in the previous section through Cisco Intersight. Click Connect.

Connection Credentials
You can find the API key ID and secret key on the Cisco Intersight Settings page. Currently, only Open API schema version 3 is supported.
Intersight API Key ID
66394bec756461330122766d/66394bec7564613301227671/663a4c
Intersight Secret Key Show
·
Cancel

Step 4. Once the authentication to Intersight succeeds, the connection displays under FC settings.

	Q Foundation Central			👌 Prism				
Found	dation Central	sion 1.6						
Nodes	Nodes Deployment History API Keys Management Foundation Central Settings							
Found	dation Central Setting	S						
			Connect Hardware Provider Connect a Hardware Provider only a single connection is allo Connection Name intersight	to onboard nodes to Foundation Central. wed at a time. To add a new connection, r Hardware Provider Cisco Intersight	Currently, only Cisco Intersight is supported a emove the existing one. URL https://us-east-1.intersight.com	nd		

Nutanix Cluster Creation

This procedure describes the process to onboard the nodes on Foundation Central and thereafter create the cluster for Cisco UCS C-Series nodes managed in Intersight Standalone Mode (ISM).

Procedure 1.	Onboard	nodes on	Foundation	Central
--------------	---------	----------	------------	---------

Step 1. Go to Foundation Central, select the Nodes tab and select the Manually Onboarded tab. Click Onboard Nodes.

E Q Foundation Central		A Prism	🐥 🚺 💿 ? 🌣 admin Y
Foundation Central Version 1.6			
Nodes Deployment History API Keys	Management Foundation Central Settings		
Nodes Auto Discovered Manually	Onboarded		
Foundation Central now supports the o	nboarding of only Cisco nodes via Cisco Intersight. Connect Cisco Intersigh	t to onboard nodes on Foundation Central.	
	Constant Hardware Devidents From	Onboard Nodes	
	Connect a Hardware Provider to Found	aton Central, and you can directly onboard into Houndation Central.	

Step 2. The screen displays the connection details configured for Cisco Intersight. Click Next.

Ξ Q Foundation Central ☆		\land Prtsm		🐥 🚺 🔿 📍 🌣 admin 🛩		
Onboard Nodes				×		
	0	Select Hardware Provider 2	Select Nodes			
	Select a Hardware Provider to onboard single connection is allowed at a time. To	Net a Hardware Provider to onboard nodes to Foundation Central. Currently, only Cisco Intersight is supported and only a ngle connection is allowed at a time. To add a new connection, remove the existing one.				
	Connection Name	Hardware Provider	URL.			
	 intersight 	Cisco Intersight	https://us-east-1.intersight.com :			
				Cancel		

Step 3. Foundation Central connects to Cisco Intersight and displays all the unconfigured nodes existing in Intersight. Select the nodes provisioned for Nutanix and click Onboard.

E Q Foundation Central			\land Prism			A 🚺 😐 ?	🌣 admin Y
Onboard Nodes							×
			 Select Hardware Provider S 	elect Nodes			
You are currently viewing the nodes connect	ted to Cisco Intersight for the connection n	ame 'intersight' and	d there are no server profiles attached. To u	pdate the node list, plea	ase click on <u>Refresh</u> ,		
Type in a query						₹ M	Addify Filters
3 selected out of 4 Cisco Nodes						3 1-4 of 4 3	20 rows =
Node Serial †	Name :	Classification :	Model 1	Organizations :	Tags :	Memory (GB)	CPU (Core)
WZP2736044T	C240-WZP2736044T	Unknown	UCSC-C240-M7SN	default		384	64
WZP2736045M	C240-WZP2736045M	Nutanix	UCSC-C240-M7SN	default		384	64
WZP2736045T	C240-WZP2736045T	Nutanix	UCSC-C240-M7SN	default		384	64
WZP2737078Q	C240-WZP2737078Q	Nutanix	UCSC-C240-M7SN	default	-	384	64
							,
< Back						Cancel	Onboard

Three Nutanix nodes are onboarded on Foundation Central as shown below:

E Q. Foundation Central				\land Prtsm			4 0		🗘 admin
Foundation Central Version	1.6								
Nodes Deployment History A	PI Keys Management Found	ation Central Settings							
Nodes Auto Discovered N	Nodes Auto Discovered Manually Onboarded								
Onboard Nodes Create Clust	ter Actions +						View by	Group	by ÷
Type In a query								₹ Modi	fy Filters
3 selected out of 3 Cisco Nodes							0 1	-3 of 3 🕖 🗌	20 rows
Node Serial *	Name :	Node Status :	Model :	Organizations :	Tags :	Classification :	Onboarded On ÷	Last Refreshe	d :
WZP2736045M	C240-WZP2736045M	Onboarded	UCSC-C240-M7SN	default		Nutanix	May 7, 2024, 11:59 AM	May 7, 2024	, 11:59 AM
WZP2736045T	C240-WZP2736045T	Onboarded	UCSC-C240-M7SN	default	-	Nutanix	May 7, 2024, 11:59 AM	May 7, 2024	, 11:59 AM
☑ WZP2737078Q	C240-WZP2737078Q	Onboarded	UCSC-C240-M7SN	default		Nutanix	May 7, 2024, 11:59 AM	May 7, 2024	, 11:59 AM

Procedure 2. Setup Nutanix Cluster

Step 1. Go to Foundation Central, select the Nodes tab and select the Manually Onboarded tab. Select Onboard Nodes. The Cisco UCS C-Series nodes onboarded for Nutanix Cluster creation display.

				Prism			A ()	🔿 ? 🌣 admin
Foundation Central Version	1.6							
Nodes Deployment History A	PI Keys Management Found	lation Central Settings						
Nodes Auto Discovered	Manually Onboarded							
Onboard Nodes Create Clust	ter Actions ~						View by	Group by
Type In a query								
3 selected out of 3 Cisco Nodes							G 1	-3 of 3 💿 20 rows 🤊
Node Serial *	Name :	Node Status	Model :	Organizations ÷	Tags ÷	Classification :	Onboarded On ÷	Last Refreshed ÷
WZP2736045M	C240-WZP2736045M	Onboarded	UCSC-C240-M7SN	default		Nutanix	May 7, 2024, 11:59 AM	May 7, 2024, 11:59 AM
WZP2736045T	C240-WZP2736045T	Onboarded	UCSC-C240-M7SN	default		Nutanix	May 7, 2024, 11:59 AM	May 7, 2024, 11:59 AM
WZP2737078Q	C240-WZP2737078Q	Onboarded	UCSC-C240-M7SN	default		Nutanix	May 7, 2024, 11:59 AM	May 7, 2024, 11:59 AM

Step 2. Click Create Cluster under the Actions tab.

Step 3. Enter a cluster name, since there are three nodes, the replication factor (RF) of cluster would be RF2, select the Intersight organization in which the servers had been claimed. Click Next.

	\$	A Prism
Create Deployment		
	1 Cluster Details	2 Hypervlsor / AOS 3 Network Settings 4 CVM Settings 5 Configure Nodes 6 Security
		Cluster Configuration The following settings affect the entire cluster as a single entity. Cluster Name Ism-Cluster Allowed characters: alphanumerics, dots, hyphens, underscores. Cluster Replication Factor Image: Replication Factor Image: Replication Factor Intersight Organization The organization is required to apply server profiles to nodes. Only nodes within the sense organization can create a cluster. If the selected nodes currently belong in multiple organizations, you can choose any one organization to apply to the policy. Idefault :

Step 4. Enter the AOS download URL. You are required to host the Nutanix AOS on a http/https web server. The web server should be reachable from Cisco IMC network. Select hypervisor as AHV and check the option to use the AHV version bundled with AOS package. This option is required if AHV is not imaged from the factory, or the nodes are reimaged. Click Next.

E Q Foundation Central		Ptsm	🐥 🚺 🔿 ? 🌣 admin v
Create Deployment			×
	1 Cluster Det	alls 2 Hypervisor / AOS 3 Network Settings 4 CVM Settings 5 Configure Nodes 6 Security	
		I want to image all nodes with custom AOS and hypervisor installers. AOS Download UR. Intps://to.108.16/nutanix_installer_package-release-fraser-6.7.15-stable AOS package will be downloaded from this location during the imaging process of each node. Procemputed SHA256 Checksum of AOS Installer (Optional) Providel the checksum it you word Frandation Central to not a checksum text of the.	
		Hypervisor ArV Choose the hypervisor type that you want to install on each node.	
		Hypervisor Deventional URL. Hypervisor Installer will be downloaded from this location during the imaging process of each node. Pre-computed SHA256 Checksum of Hypervisor Installer (Optional)	
		Provide the checksum if you want Foundation Cantal to run a checksum test of the downloaded testable before starting the imaging process. This checksum ideo tests foundation cleans the starting test analysis of the starting test and the starting of the starting of the starting test analysis of the starting test and the starting cleans of the starting test and the starting test and the starting test and and sperivice. We are responsible for emanary test regulatement before starting tim.	

- **Step 5.** Enter the enter subnet, gateway, and Cluster Virtual IP.
 - Enter VLAN ID to enable trunk mode on the Cisco VIC ports.
 - In the event customers need access ports , leave the VLAN ID blank. The port type on the uplink switch should be configured as 'access' with VLAN defined in the switch

- You have a choice to enable LACP with AHV. Default mode is active-backup. Go to: <u>https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2071-AHV-</u> <u>Networking:bp-ahv-networking-best-practices.html</u>. Enable LACP after cluster configuration and is supported only during re-imaging of nodes.
- In the event of LACP configuration failure wherein cluster creation fails with error as "Failed to receive the first heart beat of the node," go to <u>https://portal.nutanix.com/page/documents/kbs/details?targetId=kA0VO000001w0L0AQ</u> for resolution
- The default FEC setting is CL91 or AUTO (RS-FEC) applicable for 10/40/50/100 GbE cables and optics. Some models of 25GbE cables and optics require CL74 (FC-FEC) for links to be active. Configure appropriate FEC mode both on the Cisco VIC port configuration and uplink switch configuration.

Create Deployment	 Cluster Details Hype Hoto Nu Gat 1 Th Mu 1 	ervisor / AOS Network Settings CVM Settings CVM Settings Configure Nodes Configure Nod
Q Foundation Central Create Deployment	Cluster Details 2 Hype Ho Nu u arr	ervisor / AOS Network Settings CVM Settings Configure Nodes Generative set and CVM Network tank requires all hosts and CVMs of a cluster to have static IP addresses in the me subnet. Reuse Existing to 108.1.254 Reuse Existing to 108.1.254 Reuse Existing to 108.1.254 Reuse Existing to 108.1.27 Reuse Existing to 108.1.37 Reuse Existing to 10.108.1.37 Reuse Existing to 10.108.1.37 Reuse for a node failure. Reuse for a node failure. Reuse Reus
Q Foundation Central Create Deployment	Ho Nu sa Ga 1 Ne 2 Ch 1 Ti Mu 1	est and CVM Network tanix requires all hosts and CVMs of a cluster to have static IP addresses in the me subnet. toway of Every Host and CVM Rouse Existing 10.108.1.254 totak of Every Host and CVM Es5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host CVM Se5 255 255 0 totak of Every Host CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host CVM Se5 255 255 0 totak of Every Host CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 0 totak of Every Host and CVM Se5 255 255 255 0 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 totak of Every Host and CVM Se5 255 255 2 tot
Q Foundation Central Create Deployment	ά	Prism
		Cluster Virtual IP (Optional)
		10.108.1.137 This IP will always point to an online node, even in case of a node failure. Must be in the host-CVM subnet. Your subnet range is: 10.108.1.0 - 10.108.1.255 I If you plan to deploy Nutanix Objects, click here to learn about important network requirements.
		Host and CVM VLAN If your host-CVM subnet has a VLAN configuration, enter the tag below. All packets leaving the hosts and the CVMs will be wrapped with this VLAN tag. VLAN Tag of Every Host and CVM (Optional) ULAN Tag of Every Host and CVM (Optional) Minimum 1, maximum 4094. If left blank, VLAN 0 will be used. Hypervisor LACP Configuration Enable LACP
		FEC Mode for VIC Adapter The FEC mode on the VIC adapter must match what is configured on the ports on the unlink switch. Setting the EEC mode to all the switch le for most acces, but a cl91 cl cl91 :

Note: In this deployment, the VLAN tag was not defined (trunk mode) and FEC Mode was selected as CL91. The servers were connected to 25G ports on Nexus 93180YC-FX. The port configuration is detailed below.



Step 6. Enter the Timezone, DNS and NTP server configuration.

⊒ Q. Foundation Central ☆	💩 Prism
Create Deployment	
	The following amount of vRAM will be allocated for each CVM. vRAM Allocation for Every CVM (Optional) • • Unit Is Gigabytes. Minimum 12, no maximum. Leave blank to use recommended defaults. Time Configuration Time settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. Timezone IntercalLos_Angeles • Only available when you choose to form a cluster, because of technical reasons. NTP Servers (Optional) T2.20.10.18, 172.20.10.15 Porter a comma-separated list of IPs or domain names. Applies to hosts to fifthe oratio ArM? Port Settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. DNS settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. DNS settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. DNS settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. DNS settings apply to every CVM, and also apply to hosts depending on the hypervisor you chose. DNS servers (Optional) 10.108.1.6 Externational apply the proversion adomain name, or if ADS/hypervisor package download affer and

Step 7. Enter the Host IP, CVM IP, and hostnames for all the nodes configured for cluster and click Next.

reate Deployment						
	1 Cluster Det	tails (2) Hypervisor / AOS (3) 1	Network Settings (4) C	VM Settings 5	Set up Hostname Range Set up an incremental hostname for the entire column in the input below.	
	Enter the IP/hostnames you w	ant each node to have.			ntnx-ism	Clea
	Node Serial	Node Name	Host IP Set Range	CVM IP Set Range	Set Range	
	WZP2736045M	C240-WZP2736045M	10.108.1.131	10.108.1.134	ntnx-ism1	
	WZP2736045T	C240-WZP2736045T	10.108.1.132	10.108.1.135	ntnx-ism2	
	W7P27370780	C240-WZP2737078Q	10.108.1.133	10.108.1.136	ntnx-ism3	

Step 8. Select the Foundation Central API key as created under FC configuration. Click Submit.

E Q. Foundation Central			A Prism	
Create Deployment				
	1 Cluster Det	alls 2 Hypervisor / AOS 3 Networ	k Settings 4 CVM Settings 5 Configure No	odes 🟮 Security
		Foundation Central API Key Foundation Central provides an A recommended that a distinct API is create a new key or select from th Foundation Central API Key Intrx-ism-api-1	PI key to authenticate the remote nodes. It is key be created for each remote site. You can se existing ones.	

Step 9. Monitor the cluster creation process.

E Q Foundation Cen	ntral			Prtsm		A 0	○ ? ✿	admi
Foundation Central	Version 1.6							
Nodes Deployment His	story API Keys Manageme	nt Foundation	Central Settings					
Deployment History								
It may take up to 15 minute	s for a deployment progress to	start being reporte	ed. Why?		Viewing 8 d	eployments Sho	w Only Non-archive	d :
ism-cluster Deplo	ryment in progress Start	Date and Time:	5/7/2024, 12:09 PM					
Phase 1A: Node Preparation	progress	Phase 1B: Node Ima	iging started	Phase 2: Cluster Formation 0 0% Waiting for Phase 1 to finish				
Cluster Details								
Redundancy Factor 2	Host-CVM Subnet 10.108.1.254 / 255.255.2	255.0	CVM NTP Servers 172.20.10.18, 172.20.10.15	AOS Installer URL https://10.108.1.6/nutanix_installer_package-release-fraser-6.71.5-st	table-ac4cf514dc7d54742dfeadd98	ca39fcb7bb8a477-x8	6_64.tar.gz	
Cluster External IP 10.108.1.137	Intensight Organization default		CVM DNS Servers 10.108.1.6	Hypervisor Installer URL Not provided				
CVM VLAN Tag Not provided	Deployment UUID d5c5f915-2312-4e44-6d	lce-ea32fc63683f	LACP No					
3 Nodes In This Deploy	ment 🛓					View	original Configurati	ion
Block Serial ^	Node Serial	Position	Progress of Phase 1	Status	Host IP	CVM IP	Host Type	
WZP2736045M	WZP2736045M	А	. 2%	[NodeConfiguration] Waiting for the node to power on	10.108.1.131	10.108.1.134	AHV	
WZP2736045T	WZP2736045T	А	• 4%	[NodeConfiguration] Deploying and activating the profile of the Node	10.108.1.132	10.108.1.135	AHV	
WZP2737078Q	WZP2737078Q	А	. 2%	[NodeConfiguration] Waiting for the node to power on	10.108.1.133	10.108.1.136	AHV	

Step 10. Once the cluster is created successfully, go to the cluster VIP, and complete the post cluster creation task such as configuration of Storage containers, High availability reservation, iSCSI Data IP configuration, VM network configuration, and address any warnings displayed during NCC checks.

E Q. Foundation Central	tion Central					▲ ① ⊂			admin			
Foundation Central	Version 1.6											
Nodes Deployment Histor	y API Keys Management Found	ation Central Setting	js									
Deployment History												
It may take up to 15 minutes for	r a deployment progress to start being re	eported. Why?					Vie	wing 9 deployments	Show Or	ly Non-a	irchived	•
ism-cluster Deployme	ent complete Start Date and Time:	5/7/2024, 12:37 P	м					c)pen Prism E	lement	Archiv	re .
Phase 1A: Node Preparation O 100% 3 nodes prep	Phase 18: Nor 0 100%	de Imaging 3 nodes finished		Phase 2: Cluster	Formation All operations completed successfully							
Cluster Details												
Redundancy Factor 2	Host-CVM Subnet 10.108.1.254 / 255.255.255.0	17	/M NTP Servers 2.20.10.8, 172.20.10.15	AOS http	6 Installer URL ps://10.108.1.8/nutanix_installer_package-re	elease-fraser-	6.7.1.5-stable-ac4cf514dc7d54742	dfeadd98ca39fcb7bb8	a477-x86_6	4.tar.gz		
Cluster External IP 10.108.1.137	Intersight Organization default	10	/M DNS Servers 108.1.6, 172.20.4.53	Hyp	ervisor Installer URL c provided							
CVM VLAN Tag Not provided	Deployment UUID 49129eef-c297-4b5e-722e-d018a04a	6566 No	CP D									
3 Nodes In This Deploymen	nt 土								View Orig	inal Conf	figuratio	m
Block Serial 🔿	Node Serial	Position 🔿	Progress of Phase 1		Status 🕚		Host IP	CVM IP 🔅	Hos	Type		
WZP2736045M	WZP2736045M	Α		Done	All operations completed successfully		10.108.1.132	10.108.1.135	AH	/		
WZP2736045T	WZP2736045T	А		Done	All operations completed successfully		10.108.1.131	10.108.1.134	AH	/		
WZP2737078Q	WZP2737078Q	А		- Done	All operations completed successfully	,	10.108.1.133	10.108.1.136	AH	/		

Step 11. Go to Cisco Intersight to view the Server Profile created as part of Day 0 deployment.

≡	diale Intersight	2 Infrastructure Service V	Q Search C ⓒ 쉮 1 Q @ 41 ⑦ 오
:0:	Overview	Servers	
	Operate ^		G Export 4 items found 10 → per page ≪ < 1 of 1 > ≫.
	Chassis Fabric Interconnects	Health Power HCL Status Bunc (4) • Healthy 4 0 063 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	He Version Firmware Version Models # • 4.3(3.240043) 3 • 4.3(2.200270) 1 • 4.3(3.240043) 3 • 4.3(2.200270) 1 • C240 M75N 4 •
	HyperFiex Clusters	Name : Health : Model : □ □ C240-WZP2737078Q © Healthy UCSC-C240-M7SN	CPU Ca © : Memory Ca : UCS Domain : Server Profile : Bundle Ver ∮ 256.0 384.0 ntmx_W2P2737 ⊙ 4.3(3.2400 n
Ð,	Analyze ^ Explorer New	• • C240-WZP2738045T • Healthy UCSC-C240-M7SN • • C240-WZP2736045M • Healthy UCSC-C240-M7SN • • C240-WZP2736045M • Healthy UCSC-C240-M7SN	256.0 384.0 ntmx_WZP2736 4.3(3.2400
ş	Configure ^ Profiles Templates Policies		((1) of 1 >)>
Ne	Pools		

Post Cluster Creation Task

This procedure describes the recommended post cluster creation steps.

Procedure 1. Post Cluster Creation task

Step 1. Login to Cluster VIP with admin - Nutanix/4u and change the password.

PRISM	
· Create a new password for the cluster admin.	
admin .	
••••••	
••••••	
Note: When you change the admin user password, update any applications and scripts using the admin user credentials for authentication. Nutanix	
recommends that you create a user assigned with the admin role instead of	
using the admin user for authentication. The Prism Web Console Guide describes authentication and roles.	
Having issues logging in?	

Step 2. Go to the to Storage tab and create the storage container. Click Save.

Create Storage Container ? X
Name
ds1
Storage Pool
default-storage-pool-12494355784072 🗸
Max Capacity
115.14 TiB (Physical) Based on storage pool free unreserved capacity
Advanced Settings
Replication Factor ③
2
Reserved Capacity
0 GiB
Advertised Capacity
Total GiB GiB
Advanced Settings Cancel Save

Step 3. Enable Rebuild Capacity Reservation for cluster self-healing from failures.

Ism-cluster Settings - 😻 🐥 🔕 + • O 🗷 -	
ettings	Rebuild Capacity Reservation
	Reserve Rebuild Capacity
ta-at-rest Encryption	Enable this option to reserve the Rebuild Capacity required for the
rsystem allowiists	cluster to self-heal from failures.
L Certificate	
	Save
ins and Roles	
thentication	
al User Management	
• Mapping	
rts and Notifications	
rt Email Configuration	
TP Server	
Resiliency	
figure Witness	
aded Node Settings	
age VM High Availability	
build Capacity Reservation	
Jundancy State	
arance	
Jage Settings	
ettings	

Step 4. Go to Cluster details and enter iSCSI data services IP and enable Retain Deleted VMs for 1 day. Click Save.

Cluster Details ?
Cluster Name ism-cluster
FQDN
Virtual IP
Virtual IPv6
ISCSI Data Services IP
10.108.1.138
VMs when deleted will be retained in the Recycle Bin for 1d after which the used space is purged
Not encrypted
Save

Step 5. Go to Settings > Manage VM High Availability and select Enable HA Reservation. Click Save.



Step 6. Go to the VM tab and create a VM network subnet.

X Ism-cluster		0		Q, ? × 🎝 admin •	
Overview - Table				+ Create VM Network Config	
Hypervisor Summary		p Guest VMs by Controller IOPS VM Critical Alerts	VM Events		
AHV	20230302.2008 VERSION	No data available			
VMs 3	HA - sk	Top Guest VMs by Controller IO Latency			
On Unknown	3 • Off 0	Network Configuration ? x			
		Subnets Internal Interfaces Virtual Switch			
CPU		No subnets have been configured.		Antes	
48 PROVISIONED VCPUS	3.23% CPU USAGE		reate Subnet	No Events	
Memory		THE AVERT THE OF ST & VIEW			

Step 7. Run a NCC check and address warnings such as changing AHV and CVM default passwords.

Appendix

This appendix contains the following:

- Appendix A Bill of Materials
- Appendix B References used in this guide

Appendix A - Bill of Materials

<u>Table 2</u> provides an example the Bill of Materials used for one (3) node cluster deployed, used in the testing and reference design described in this document.

Part Number	Description	Quantity
HCIAF240C-M7SN	Cisco Compute Hyperconverged HCIAF240cM7 All Flash NVMe Node	3
HCI-IS-MANAGED	Deployment mode for Standalone Server Managed by Intersight	3
HCI-NVME4-1920	1.9TB 2.5in U.2 15mm P5520 Hg Perf Med End NVMe	72
HCI-M2-I240GB	240GB M.2 Boot SATA Intel SSD	6
HCI-M2-HWRAID	Cisco Boot optimized M.2 Raid controller	3
HCI-RAIL-M7	Ball Bearing Rail Kit for C220 & C240 M7 rack servers	3
HCI-TPM-002C	TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, for servers	3
HCI-AOSAHV-67-SWK9	HCI AOS AHV 6.7 SW	3
UCSC-HSHP-C240M7	UCS C240 M7 Heatsink	6
UCS-DDR5-BLK	UCS DDR5 DIMM Blanks	60
UCSC-M2EXT-240-D	C240M7 2U M.2 Extender board	3
UCSC-FBRS2-C240-D	C240 M7/M8 2U Riser2 Filler Blank	3
UCSC-FBRS3-C240-D	C240 M7/M8 2U Riser3 Filler Blank	3
HCI-CPU-I6448H	Intel I6448H 2.4GHz/250W 32C/60MB DDR5 4800MT/s	6
HCI-MRX32G1RE1	32GB DDR5-4800 RDIMM 1Rx4 (16Gb)	36
HCI-RIS1A-24XM7	C240 M7 Riser1A; (x8;x16x, x8); StBkt; (CPU1)	3
HCI-MLOM	Cisco VIC Connectivity	3
HCI-M-V5Q50G	Cisco VIC 15428 4x 10/25/50G mLOM C-Series	3
HCI-PSU1-1200W	1200W Titanium power supply for C-Series Servers	6
NO-POWER-CORD	ECO friendly green option, no power cable will be shipped	6

Table 2. Bill of Materials

Appendix B - References use in this guide

Cisco Compute Hyperconverged with Nutanix: <u>https://www.cisco.com/c/en/us/products/hyperconverged-infrastructure/compute-hyperconverged/index.html</u>

Cisco Intersight: https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html

HCIAF240C M7 All-NVMe/All-Flash Server: https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hc-240m7specsheet.pdf

Nutanix reference documentation: <u>https://portal.nutanix.com/</u>

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 DISCLAIM ALL WAR-RANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS 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 APPLICA-TION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLE-MENTING 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 UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. 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_P11)

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)