

# Cisco Data Intelligence Platform with All NVMe Storage, Cisco Intersight, and Cloudera Data Platform

Deployment Guide for Cisco Data Intelligence Platform with All NVMe Storage, Cisco Intersight, and Cloudera Data Platform Private Cloud Base 7.1.1

Published: September 2020



In partnership with: CLOUDERA

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:

#### http://www.cisco.com/go/designzone.

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 CIS-CO 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 TECH-NICAL 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 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, Giga-Drive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, Power-Panels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Lisa.

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)

© 2020 Cisco Systems, Inc. All rights reserved.

## **Executive Summary**

In today's environment, datasets are growing with tremendous velocity and peta bytes of data are becoming norm. For instance, customers are dealing with huge influx of machine generated data from several new use cases such as IoT, autonomous driving, smart cities, genomics, and financials, to name a few. Exponential data growth and the need to analyze the exploding volume of data at higher rate has introduced several challenges such as IO bottlenecks, several management touchpoints, growing cluster complexity, performance degradation, and so on.

Amid those challenges, surge in Artificial Intelligence/Machine Learning (AI/ML) frameworks and its tremendous adoption across various industries have led enterprises to utilize advanced computing resources i.e. CPU, GPU, and FPGA to extract key insights and gain competitive edge. Since data lakes relies heavily on I/O bandwidth, given these ongoing enhancements, feature enrichments, and convergence of other open-source frameworks around Hadoop ecosystem, it is imperative to have compute intensive workloads to operate on the same data with high-performance, hence enabling parallel processing of data in real-time.

Data scientists are constantly searching for newer techniques and methodologies that can unlock the value of big data and distill this data further to identify additional insights which could transform productivity and provide business differentiation.

Given all those challenges, in this reference architecture, <u>Cisco Data Intelligence Platform</u> (CDIP) is thoughtfully designed with servers that support highest IO bandwidth with the inclusion of all NVMe.

All NVMe configuration provides accelerated IO bandwidth which is essential for Hadoop performance. NVMe provides high random read-write capabilities which makes it preferred choice for NoSQL or Data Warehousing applications running on top of Hadoop and helps improve GPU utilization instead of resting idle due to slow data access and faster parallel access of large datasets. IT can now seamlessly grow to cloud scale at a smaller datacenter footprint with higher storage density and performance.

This CVD extends the portfolio of the Cisco Data Intelligence Platform solutions and taking it to the next level of innovation by providing All NVMe to the Data Lake.

## Solution Overview

#### Introduction

Both Big Data and machine learning technology have progressed to the point where they are being implemented in production systems running 24x7. There exists a very clear need for a proven, dependable, high-performance platform for the ingestion, processing, storage, and analysis of the data, as well as the seamless dissemination of the output, results, and insights of the analysis.

This solution implements Cloudera Data Platform Private Cloud Base (CDP PvC Base) on Cisco UCS Integrated Infrastructure for Big Data and Analytics based on Cisco Data Intelligence Platform (CDIP) architecture, a worldclass platform specifically designed for demanding workloads that is both easy to scale and easy to manage, even as the requirements grow to thousands of servers and petabytes of storage.

Many companies, recognizing the immense potential of big data and machine learning technology, are gearing up to leverage these new capabilities, building out departments and increasing hiring. However, these efforts face a new set of challenges:

• Making the data available to the diverse set of people who need it

- Enabling access to high-performance computing resources, GPUs, that also scale with the data growth
- Allowing people to work with the data using the environments in which they are familiar
- Publishing their results so the organization can make use of it
- · Enabling the automated production of those results
- Managing the data for compliance and governance
- · Scaling the system as the data grows
- Managing and administering the system in an efficient, cost-effective way

This solution is based on the Cisco UCS Integrated Infrastructure for Big Data and Analytics and includes computing, storage, connectivity, and unified management capabilities to help companies manage the immense amount of data being collected. It is built on Cisco Unified Computing System (Cisco UCS) infrastructure, using Cisco UCS C-Series Rack Servers. This architecture is specifically designed for performance and linear scalability for big data and machine learning workload.

#### **Audience**

The intended audience of this document includes sales engineers, field consultants, professional services, IT managers, partner engineering and customers who want to deploy the Cloudera Data Platform Private Cloud Base on the Cisco UCS Integrated Infrastructure for Big Data and Analytics (Cisco UCS M5 Rack-Mount servers).

#### **Purpose of this Document**

This document describes the architecture, design choices, and deployment procedures for Cisco Data Intelligence Platform using Cloudera Data Platform Private Cloud Base on Cisco UCS C220 M5.

This document also serves as a step-by-step guide on how to deploy CDP PvC Base on a 16-node cluster of Cisco UCS C220 M5 Rack Server.

#### What's New in this Release?

This solution extends the portfolio of Cisco Data Intelligence Platform (CDIP) architecture with Cloudera Data Platform Private Cloud Base, a state-of-the-art platform, providing a data cloud for demanding workloads that is easy to deploy, scale and manage. Furthermore, as the enterprise's requirements and needs changes overtime, the platform can grow to thousands of servers, hence providing peta bytes of storage.

The following design consideration will be implemented in this validated design:

- NVMe based Cisco UCS Infrastructure for Big Data and Analytics
- Cisco Intersight deployed standalone C220 M5 Rack Server



#### What's Next?

This CVD showcases Cisco UCS Manager (UCSM). This solution can also be deployed using Cisco Intersight. Additional Cisco UCS features will be added to the Appendix in the following months. Some of these include the following:

Cloudera Data Platform Private Cloud

- Apache Ozone Object Storage
- A fully integrated CDP on CDIP with
- Data lake enabled through CDP PvC Base
- AI/ML enabled through CDP Private Cloud
- Exabyte storage enabled through Apache Ozone

#### **Solution Summary**

This CVD details the process of installing Cloudera Data Platform Private Cloud Base and the configuration details of the cluster. The current version of Cisco UCS Integrated Infrastructure for Big Data and Analytics offers the following configurations depending on the compute and storage requirements.

## **Cisco Data Intelligence Platform**

Cisco Data Intelligence Platform (CDIP) is a cloud scale architecture which brings together big data, Al/compute farm, and storage tiers to work together as a single entity while also being able to scale independently to address the IT issues in the modern data center. This architecture allows for:

- Extremely fast data ingest, and data engineering done at the data lake
- Al compute farm allowing for different types of Al frameworks and compute types (GPU, CPU, FPGA) to work on this data for further analytics
- A storage tier, allowing to gradually retire data which has been worked on to a storage dense system with a lower \$/TB providing a better TCO
- Seamlessly scale the architecture to thousands of nodes with a single pane of glass management using Cisco Application Centric Infrastructure (ACI)
- Cisco Data Intelligence Platform caters to the evolving architecture bringing together a fully scalable infrastructure with centralized management and fully supported software stack (in partnership with industry leaders in the space) to each of these three independently scalable components of the architecture including data lake, AI/ML and Object stores.

Figure 1 Cisco Data Intelligent Platform



Cisco has developed numerous industry leading Cisco Validated Designs (reference architectures) in the area of Big Data, compute farm with Kubernetes (CVD with RedHat OpenShift) and Object store (Scality, SwiftStack, Cloudian, and others).



Figure 2 Cisco Data Intelligence Platform with Hadoop, Kubernetes, and Object Store

This architecture can start from a single rack and scale to thousands of nodes with a single pane of glass management with Cisco Application Centric Infrastructure (ACI).

Figure 3 Cisco Data Intelligent Platform at Scale

## **Cisco Data Intelligence Platform**



## **CDP on CDIP**



A CDIP architecture can fully be enabled by Cloudera Data Platform with the following components:

- Data lake enabled through CDP PvC Base
- AI/ML enabled through CDP Private Cloud and
- Exabyte storage enabled through Apache Ozone

## **Reference Architecture**

#### **Data Lake Reference Architecture**

<u>Table 1</u> lists the data lake reference architecture configuration details for Cisco UCS Integrated Infrastructure for Big Data and Analytics.

	High Performance	Performance	Capacity	High Capacity
Servers	16 x Cisco UCS C220 M5SN Rack Serv- ers with small- form-factor (SFF) drives (UCSC- C220-M5SN)	16 x Cisco UCS C240 M5 Rack Servers with small-form- factor (SFF) drives	16 x Cisco UCS C240 M5 Rack Servers with large-form- factor (LFF) drives	8 x Cisco UCS S3260 Stor- age Servers
CPU	2 x 2nd Gen Intel® Xeon® Scalable	2 x 2nd Gen Intel® Xeon® Scalable	2 x 2nd Gen Intel Xeon Scalable Proces-	2 x 2nd Gen Intel Xeon Scalable

#### Table 1 Cisco UCS Integrated Infrastructure for Big Data and Analytics Configuration Options

	High Performance	Performance	Capacity	High Capacity
	Processors 6230R (2 x 26 cores, at 2.1 GHz)	Processors 5218R proces- sors (2 x 20 cores, at 2.1 GHz)	sors 5218R (2 x 20 cores, at 2.1 GHz)	Processors 6230R (2 x 26 cores, 2.1 GHz)
Memory	12 x 32GB DDR4 (384 GB)	12 x 32GB DDR4 (384 GB)	12 x 32GB DDR4 (384 GB)	12 x 32GB DDR4 (384 GB)
Boot	M.2 with 2 x 240-GB SSDs	M.2 with 2 x 240-GB SSDs	M.2 with 2 x 240-GB SSDs	2 x 240-GB SATA SSDs
Storage	10 x 8TB 2.5in U.2 Intel P4510 NVMe High Perf. Value Endurance	26 x 2.4TB 10K rpm SFF SAS HDDs or 12 x 1.6-TB Enterprise Value SATA SSDs	12 x 8-TB 7.2K rpm LFF SAS HDDs	28 x 6 TB 7.2K rpm LFF SAS HDDs per server node
Virtual in- terface card (VIC)	25 Gigabit Ethernet (Cisco UCS VIC 1457) or 40/100 Gigabit Ethernet (Cisco UCS VIC 1497)	25 Gigabit Ethernet (Cisco UCS VIC 1455) or 40/100 Gigabit Ethernet (Cisco UCS VIC 1497)	25 Gigabit Ethernet (Cisco UCS VIC 1455) or 40/100 Gigabit Ethernet (Cisco UCS VIC 1497)	40 Gigabit Ether- net (Cisco UCS VIC 1387) or 25 Gigabit Ether- net (Cisco UCS VIC 1455) or 40/100 Giga- bit Ethernet (Cisco UCS VIC 1495)
Storage con- troller	NVMe Switch included in the optimized server	Cisco 12-Gbps SAS modular RAID controller with 4- GB flash-based write cache (FBWC) or Cisco 12-Gbps modu- lar SAS host bus adapter (HBA)	Cisco 12-Gbps SAS modular RAID controller with 2- GB FBWC or Cisco 12-Gbps modular SAS host bus adapter (HBA)	Cisco 12-Gbps SAS Modular RAID Control- ler with 4-GB flash-based write cache (FBWC)
Network connec nec- tivity	Cisco UCS 6332 Fabric Interconnect or Cisco UCS 6454/64108 Fab- ric Interconnect	Cisco UCS 6332 Fab- ric Interconnect or Cisco UCS 6454/64108 Fabric Intercon- nect	Cisco UCS 6332 Fabric Interconnect or Cisco UCS 6454/64108 Fab- ric Interconnect	Cisco UCS 6332 Fabric Inter- connect or Cisco UCS 6454/64108 Fabric Inter- connect

	High Performance	Performance	Capacity	High Capacity
GPU (op- tional)	Up to 2 x NVIDIA Tesla T4 with 16 GB memory each	Up to 2 x NVIDIA Tesla V100 with 32 GB memory each Or Up to 6 x NVIDIA Tesla T4 with 16 GB memory each	2 x NVIDIA Tesla V100 with 32 GB memory each Or Up to 6 x NVIDIA Tesla T4 with 16 GB memory each	

As illustrated in <u>Figure 5</u>, a sixteen-node cluster with Rack#1 hosting sixteen Cisco UCS C220 M5 server (thirteen Data Node and three Name Node). Each link in the figure represents a 40 Gigabit Ethernet link from each of the sixteen-server connected to a pair of Cisco Nexus 9000 switch.

Figure 5 Cisco Data Intelligence Platform with Cloudera Data Platform Private Cloud Base - Data Lake





The Cisco UCS VIC 1387 provides 40Gbps, Cisco UCS VIC 1457 provides 10/25Gbps, and the Cisco UCS VIC 1497 provides 40/100Gbps connectivity for the Cisco UCS C-series rack server. For more information see, <u>Cisco UCS C-Series Servers Managing Network Adapters.</u>

## **Scaling the Solution**

Figure 6 illustrates how to scale the solution. Each pair of Cisco UCS 6332 Fabric Interconnects has 24 Cisco UCS C240 M5 servers connected to it. This allows for eight uplinks from each Fabric Interconnect to the Cisco Nexus 9332 switch. Six pairs of 6332 FI's can connect to a single switch with four uplink ports each. With 24 servers per FI, a total of 144 servers can be supported. Additionally, this solution can scale to thousands of nodes with the Cisco Nexus 9500 series family of switches.

In the reference architectures discussed here, each of the components is scaled separately, and for the purposes of this example, scaling is uniform. Two scale scenarios are as follows:

- Scaled architecture with 3:1 oversubscription with Cisco fabric interconnects and Cisco ACI
- Scaled architecture with 2:1 oversubscription with Cisco ACI

In the following scenarios, the goal is to populate up to a maximum of 200 leaf nodes in a Cisco ACI domain. Not all cases reach that number because they use the Cisco Nexus 9508 Switch for this sizing and not the Cisco Nexus 9516 Switch.

#### Scaled Architecture with 3:1 Oversubscription with Cisco Fabric Interconnects and Cisco ACI

The architecture discussed here and shown in <u>Figure 6</u> supports 3:1 network oversubscription from every node to every other node across a multidomain cluster (nodes in a single domain within a pair of Cisco fabric interconnects are locally switched and not oversubscribed).

From the viewpoint of the data lake, 24 Cisco UCS C240 M5 Rack Servers are connected to a pair of Cisco UCS 6332 Fabric Interconnects (with 24 x 40-Gbps throughput). From each fabric interconnect, 8 x 40-Gbps links connect to a pair of Cisco Nexus 9336 Switches. Three pairs of fabric interconnects can connect to a single pair of Cisco Nexus 9336 Switches (8 x 40-Gbps links per Fabric Interconnect to a pair of Nexus switch). Each of these Cisco Nexus 9336 Switches connects to a pair of Cisco Nexus 9508 Cisco ACI switches with 6 x 100-Gbps uplinks (connecting to a Cisco N9K-X9736C-FX line card). the Cisco Nexus 9508 Switch with the Cisco N9K-X9736C-FX line card can support up to 36 x 100-Gbps ports, each and 8 such line cards.



#### Scaled Architecture with 3:1 Oversubscription with Cisco Fabric Interconnects and Cisco ACI

## Scaled Architecture with 2:1 Oversubscription with Cisco ACI

In the scenario discussed here and shown in Figure 7, the Cisco Nexus 9508 Switch with the Cisco N9K-X9736C-FX line card can support up to 36 x 100-Gbps ports, each and 8 such line cards.

Here, for the 2:1 oversubscription, 30 Cisco UCS C240 M5 Rack Servers are connected to a pair of Cisco Nexus 9336 Switches, and each Cisco Nexus 9336 connects to a pair of Cisco Nexus 9508 Switches with three uplinks each. A pair of Cisco Nexus 9336 Switches can support 30 servers and connect to a spine with 6 x 100-Gbps links on each spine. This single pod (pair of Cisco Nexus 9336 Switches connecting to 30 Cisco UCS C240 M5 servers and 6 uplinks to each spine) can be repeated 48 times (288/6) for a given Cisco Nexus 9508 Switch and can support up to1440 servers.

To reduce the oversubscription ratio (to get 1:1 network subscription from any node to any node), you can use just 15 servers under a pair of Cisco Nexus 9336 Switches and then move to Cisco Nexus 9516 Switches (the number of leaf nodes would double).

To scale beyond this number, multiple spines can be aggregated.



#### Scaled Architecture with 2:1 Oversubscription with Cisco ACI

#### Sizing the Cluster Based on Network Bandwidth

Figure 8 Cisco Data Intelligence Platform - 16 Data node Configuration with CDP PvC Base



Cisco UCS C220 M5 Rack Server

When sizing the cluster network bandwidth across multiple domains, this could impact over performance of the cluster. The following section provides a few sample calculations for active-standby and active-active connection from Cisco UCS dual port 40G VIC connected to Cisco Nexus 9000 switch achieved through a combination of switch and bonding configuration. For more information on various bonding modes and required switch configuration go to: <a href="https://access.redhat.com/documentation/en-">https://access.redhat.com/documentation/en-</a>

## us/red hat enterprise linux/7/html/networking guide/overview-of-bonding-modes-and-the-required-settings-on-the-switch.

#### **Active-Standby Link Connection**

Servers are configured in active-standby configuration with bonding mode 1 on OS and active links configured to one of the Nexus Switches (see Figure 1). <u>Table 2</u> lists sample network bandwidth calculation for node-node communication in multi domain environment.

Server Bandwidth – Downstream (No. of Servers x Bandwidth	Upstream Bandwidth (Number of ports used for uplink port-channel	Node-Node Network Bandwidth (due to Oversubscription - Cross Do- main)			
of VIC port) x Bandwidth of the Port)		2 Domains: Oversubscription ratio 50%1 across Domain (2 racks)	5 Domains: Oversubscription ratio 80%2 across Domain (5 racks)		
10 x 40 Gbps = 400 Gbps	10 x 40 Gbps = 400 Gbps	400:0.5 x 400 = 2:1 => <b>20 Gbps</b>	400:0.8 x 400 = 1.25:1 => <b>32 Gbps</b>		
12 x 40 Gbps = 480 Gbps	12 x 40 Gbps = 480 Gbps	480:0.5 x 480 = 2:1 => <b>20 Gbps</b>	480:0.8 x 480 = 1.25:1 => <b>32 Gbps</b>		
16 x 40 Gbps = 640 Gbps	12 x 40 Gbps = 480 Gbps	640:0.5 x 480 = 2.6:1 => <b>15.3 Gbps</b>	640:0.8 x 480 = 1.66:1 => <b>24.1</b> Gbps		
16 x 40 Gbps = 640 Gbps	14 x 40 Gbps = 560 Gbps	640:0.5 x 560 = 2.3:1 => <b>17.3 Gbps</b>	640:0.8 x 560 = 1.42:1 => <b>28.1</b> Gbps		
16 x 40 Gbps = 640 Gbps	8 x 40 Gbps = 320 Gbps	640:0.5 x 320 = 4:1 => <b>10 Gbps</b>	640:0.8 x 320 = 2.5:1 => <b>16 Gbps</b>		
18 x 40 Gbps = 720 Gbps	10 x 40 Gbps = 400 Gbps	720:0.5 x 400 = 3.6:1 => <b>11.1 Gbps</b>	720:0.8 x 400 = 2.25:1 => <b>17.7</b> Gbps		
18 x 40 Gbps = 720 Gbps	8 x 40 Gbps = 480 Gbps	720:0.5 x 480 = 3:1 => <b>13.3 Gbps</b>	720:0.8 x 480 = 1.87:1 => <b>21.3</b> Gbps		
18 x 40 Gbps = 720 Gbps	6 x 40 Gbps = 240 Gbps	720:0.5 x 240 = 6:1 => <b>6.65 Gbps</b>	720:0.8 x 240 = 3.75:1 => <b>10.6</b> Gbps		
20 x 40 Gbps = 800 Gbps	10 x 40 Gbps = 400 Gbps	800:0.5 x 400 = 4:1 => <b>10 Gbps</b>	800:0.8 x 400 = 2.5:1 => <b>16 Gbps</b>		
20 x 40 Gbps = 800 Gbps	8 x 40 Gbps = 480 Gbps	800:0.5 x 480 = 3.3:1 => <b>12.1 Gbps</b>	800:0.8 x 480 = 2:1 => <b>20 Gbps</b>		
22 x 40 Gbps = 880 Gbps	8 x 40 Gbps = 480 Gbps	880:0.5 x 480 = 3.6:1 => <b>11.1 Gbps</b>	880:0.8 x 480 = 2.3:1 => <b>17.3 Gbps</b>		

#### Table 2 Node to Node network across Domains (Active - standby)

Æ

In a 2-rack system, 50% of traffic is expected between nodes in a Domain.
 In a 2-rack system, 50% of traffic is expected to go across Domain.

#### **Active-Active Link Connection**

Servers are configured in active-active configuration with bonding mode 4 on OS and active links configured to both Nexus Switches in LACP mode (see Figure 1). Table 3, Table 4, and Table 5 represents sample network

bandwidth calculation for node-node communication in single domain, two rack and five rack environment respectively.



The Cisco Nexus configuration and OS level configuration for Active-Active link connection is in the Appendix, section <u>Configure Cisco Nexus and Host for Active-Active Connections</u>.

#### Single Rack Topology

<u>Table 3</u> lists a sample calculation for single rack topology.

Total Bandwidth - Serv- ers (No. of Servers1 x No. Of VICs x BW of VIC)	Total Upstream Band- width supported (No. of uplink ports x No. of Switches x BW of each port)	Upstream traffic gener- ated by each Node for within Domain. (75%)1	Node- Node network bandwidth Oversubscription ratio within Do- main
16 x 2 x 40 Gbps = 1280 Gbps	12 x 2 x 40 Gbps = 960 Gbps	0.75 x 1280 = 960 Gbps	960:960 = 1:1 => <b>80 Gbps</b>
16 x 2 x 40 Gbps = 1280 Gbps	8 x 2 x 40 Gbps = 640 Gbps	0.75 x 1280 = 960 Gbps	960:640 = 1.5:1 => <b>53.3 Gbps</b>
16 x 2 x 40 Gbps = 1280 Gbps	6 x 2 x 40 Gbps = 480 Gbps	0.75 x 1280 = 960 Gbps	960:480 = 2:1 => <b>40 Gbps</b>
18 x 2 x 40 Gbps = 1440 Gbps	12 x 2 x 40 Gbps = 960 Gbps	0.75 x 1440 = 1080 Gbps	1080:960 = 1.125:1 => <b>71.1 Gbps</b>
18 x 2 x 40 Gbps = 1440 Gbps	8 x 2 x 40 Gbps = 640 Gbps	0.75 x 1440 = 1080 Gbps	1080:640 = 1.68:1 => <b>47.6 Gbps</b>
18 x 2 x 40 Gbps = 1440 Gbps	6 x 2 x 40 Gbps = 480 Gbps	0.75 x 1440 = 1080 Gbps	1080:480 = 2.25:1 => <b>35.5 Gbps</b>
20 x 2 x 40 Gbps = 1600 Gbps	10 x 2 x 40 Gbps = 800 Gbps	0.75 x 1600 = 1200 Gbps	1200:800 = 1.5:1 => <b>53.3 Gbps</b>
20 x 2 x 40 Gbps = 1600 Gbps	6 x 2 x 40 Gbps = 480 Gbps	0.75 x 1600 = 1200 Gbps	1200:480 = 2.5:1 => <b>32 Gbps</b>
22 x 2 x 40 Gbps = 1760 Gbps	8 x 2 x 40 Gbps = 640 Gbps	0.75 x 1760 = 1320 Gbps	1320:640 = 2:1 => <b>40 Gbps</b>
24 x 2 x 40 Gbps = 1920 Gbps	6 x 2 x 40 Gbps = 480 Gbps	0.75 x 1920 = 1440 Gbps	1440:480 = 3:1 => <b>26.6 Gbps</b>

Table 3 Node-to-Node Network Bandwidth Across Domains (Active-Active) - Single Rack Topology

Theoretically, 50% goes across, but, considering the hashing algorithm, a much higher traffic is expected to go across and so math is calculated using 75%.

#### **Two Rack Topology**

<u>Table 4</u> lists a sample calculation for 2-rack topology.

Per Node Network Bandwidth (If no Oversubscription)	Within Domain traffic U (%): Across Domain at traffic (%) for each w Server		Up ate wit	Jpstream traffic gener- ted by each Node for vithin Domain traffic Domain t		n traffic d by each across raffic	Total upstream traffic generated per Node
2 x 40 = 80 Gbps	509	%:50%	<b>0.7</b> Gb	<b>5</b> <sup>1</sup> x 0.5 x 80 = 30 ps	<b>0.5</b> <sup>2</sup> x 80	= 40 Gbps	30 + 40 = 70 Gbps
Total upstream traffic generated by all Serve	rs	Total Upstream Band width (Number of Up link ports x Bandwid	d- )- th)	Oversubscription rati	0	Node to Noo width acros Oversubscr	de network Band- s Domain due to iption
16 Servers x 70 = 1120 Gbps	)	14 x 2 x 40 = 1120 Gbps		1120:1120 = 1:1		80 / 1 = <b>80</b> (	Gbps
16 Servers x 70 = 1120 Gbps		12 x 2 x 40 = 960 Gb	ps	1120:960 = 1.16:1		80 / 1.16 =	68.9 Gbps
16 Servers x 70 = 1120 Gbps	)	10 x 2 x 40 = 800 Gb	ps	1120:800 = 1.4:1		80 / 1.4 = 5	7.1 Gbps
18 Servers x 70 = 1260 Gbps	)	12 x 2 x 40 = 960 Gb	ps	1260:960 = 1.3:1		80 / 1.3 = <b>6</b>	1.5 Gbps
18 Servers x 70 = 1260 Gbps		10 x 2 x 40 = 800 Gb	ps	1260:800 = 1.57:1		80 / 1.57 =	50.9 Gbps
20 Servers x 70 = 1400 Gbps	)	10 x 2 x 40 = 800 Gb	ps	1400:800 = 1.75:1		80 / 1.75 =	45.7 Gbps
20 Servers x 70 = 1400 Gbps	)	8 x 2 x 40 = 640 Gbp	S	1400:640 = 2.2:1		80 / 2.2 = 3	6.3 Gbps
22 Servers x 70 = 1540 Gbps		8 x 2 x 40 = 640 Gbp	S	1540:640 = 2.4:1		80 / 2.4 = 3	3.33 Gbps
22 Servers x 70 = 1540 Gbps		6 x 2 x 40 = 480 Gbp	S	1540:480 = 3.2:1		80 / 3.2 = <b>2</b>	5 Gbps
24 Servers x 70 = 1680 Gbps		6 x 2 x 40 = 480 Gbp	S	1680:480 = 3.5:1		3.5 = <b>22.85</b>	Gbps

#### Table 4 Node to Node network across Domains (Active-Active) - 2 Rack Topology



1. In a 2-rack system, 50% of traffic is expected between nodes in a Domain, and 75% of that 50% is expected to go upstream.

2. In a 2-rack system, 50% of traffic is expected to go across Domain.

#### **Five Rack Topology**

<u>Table 5</u> lists a sample calculation for 2-rack topology.

Per Node Network Bandwidth (if no oversubscription)	Within Domain Traf- fic (%): Across Do- main Traffic (%) for Each Server	Upstream Traffic Generated by Each Node within Domain Traffic	Upstream Traffic Generated by Each Node for Across Do- main Traffic	Total Upstream Traf- fic Generated Per Node
2 x 40 = 80 Gbps	20%:80%	<b>0.75</b> <sup>1</sup> x 0.2 x 80 = 12 Gbps	<b>0.8</b> <sup>2</sup> x 80 = 64 Gbps	12 + 64 = 76 Gbps
Total Upstream Traf- fic Generated by All Servers	Total Upstream Bandwidth (Number of Uplink Ports x Bandwidth)	Oversubscription Ra- tio	Node-to-Node Bandwidth Across Domain Due to Over- subscription	
16 Servers x 76 = 1216 Gbps	14 x 2 x 40 = 1120 Gbps	1216:1120 = 1.08:1	80 / 1.08 = <b>74 Gbps</b>	
16 Servers x 76 = 1216 Gbps	12 x 2 x 40 = 960 Gbps	1216:960 = 1.26:1	80 / 1.26 = <b>63.5 Gbps</b>	
16 Servers x 76 = 1216 Gbps	10 x 2 x 40 = 800 Gbps	1216:800 = 1.52:1	80 / 1.52 = <b>52.63</b> Gbps	
18 Servers x 76 = 1368 Gbps	12 x 2 x 40 = 960 Gbps	1368:960 = 1.42:1	80 / 1.42 = <b>56.33</b> Gbps	
18 Servers x 76 = 1368 Gbps	10 x 2 x 40 = 800 Gbps	1368:800 = 1.71:1	80 / 1.71 = <b>46.78</b> Gbps	
20 Servers x 76 = 1520 Gbps	10 x 2 x 40 = 800 Gbps	1520 800 = 1.9:1	80 / 1.9 = <b>42.1 Gbps</b>	
20 Servers x 76 = 1520 Gbps	8 x 2 x 40 = 640 Gbps	1520:640 = 2.37:1	80 / 2.37 = <b>33.7 Gbps</b>	
22 Servers x 76 = 1672 Gbps	8 x 2 x 40 = 640 Gbps	1672:640 = 2.6:1	80 / 2.6 = <b>30.7 Gbps</b>	
22 Servers x 76 = 1672 Gbps	6 x 2 x 40 = 480 Gbps	1672:480 = 3.48:1	80 / 3.48 = <b>23 Gbps</b>	
24 Servers x 76 = 1824 Gbps	6 x 2 x 40 = 480 Gbps	1824:480 = 3.8:1	80 / 3.8 = <b>21 Gbps</b>	

Tahla 5	Node-to-Node Network Across Domains (	Active-Active	) - 5 Rack Topology
	Node to Node Network Across Domains		



1. In a 5-rack system, 20% of traffic is expected between nodes in a Domain. And 75% of that 20% is expected to go upstream.

2. In a 5-rack system, 80% of traffic is expected to go upstream.

## **Technology** Overview

## **Cisco UCS Integrated Infrastructure for Big Data and Analytics**

Cisco Data Intelligence Platform for Cloudera is based on <u>Cisco UCS Integrated Infrastructure for Big Data and</u> <u>Analytics</u>, a highly scalable architecture designed to meet a variety of scale-out application demands with seamless data integration and management integration capabilities built using the components described in this section.

## Cisco UCS

Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that unites computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce Total Cost of Ownership (TCO) and increase business agility. The system integrates a low-latency, lossless 10/25/40/100 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain (Figure 9).





#### **Cisco Intersight**

Cisco Intersight is Cisco's systems management platform that delivers intuitive computing through cloudpowered intelligence. This platform offers a more intelligent level of management that enables IT organizations to analyze, simplify, and automate their environments in ways that were not possible with prior generations of tools. This capability empowers organizations to achieve significant savings in Total Cost of Ownership (TCO) and to deliver applications faster, so they can support new business initiatives.

Cisco Intersight is a Software as a Service (SaaS) infrastructure management which provides a single pane of glass management of CDIP infrastructure in the data center. Cisco Intersight scales easily, and frequent updates are implemented without impact to operations. Cisco Intersight Essentials enables customers to centralize con-

figuration management through a unified policy engine, determine compliance with the Cisco UCS Hardware Compatibility List (HCL), and initiate firmware updates. Enhanced capabilities and tight integration with Cisco TAC enables more efficient support. Cisco Intersight automates uploading files to speed troubleshooting. The Intersight recommendation engine provides actionable intelligence for IT operations management. The insights are driven by expert systems and best practices from Cisco.

Cisco Intersight offers flexible deployment either as Software as a Service (SaaS) on Intersight.com or running on your premises with the Cisco Intersight virtual appliance. The virtual appliance provides users with the benefits of Cisco Intersight while allowing more flexibility for those with additional data locality and security requirements.



Cisco Intersight has the following:

- Connected TAC
- Security Advisories
- Hardware Compatibility List (HCL) and much more

To learn more about all the features of Intersight go to:

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

To view current Intersight Infrastructure Service licensing, see

https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-infrastructure-service/licensing.html

#### **Cisco UCS C-Series Rack-Mount Servers**

Cisco UCS C-Series Rack-Mount Servers keep pace with Intel Xeon processor innovation by offering the latest processors with increased processor frequency and improved security and availability features. With the increased performance provided by the Intel Xeon Scalable Family Processors, Cisco UCS C-Series servers offer an improved price-to-performance ratio. They also extend Cisco UCS innovations to an industry-standard rack-mount form factor, including a standards-based unified network fabric, Cisco VN-Link virtualization support, and Cisco Extended Memory Technology.

It is designed to operate both in standalone environments and as part of Cisco UCS managed configuration, these servers enable organizations to deploy systems incrementally–using as many or as few servers as needed–on a schedule that best meets the organization's timing and budget. Cisco UCS C-Series servers offer investment protection through the capability to deploy them either as standalone servers or as part of Cisco UCS. One compelling reason that many organizations prefer rack-mount servers is the wide range of I/O options available in the form of PCIe adapters. Cisco UCS C-Series servers support a broad range of I/O options, including interfaces supported by Cisco and adapters from third parties.

#### Cisco UCS C220 M5 Rack-Mount Server

The Cisco UCS C220 M5 Rack-Mount Server (Figure 11) is a 2-socket, 1-Rack-Unit (1RU) rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, from big data and analytics to collaboration. Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of a Cisco Unified Computing System (Cisco UCS) managed environment to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' Total Cost of Ownership (TCO) and increase their business agility.

The latest update includes support for 2<sup>nd</sup> Generation Intel Xeon Scalable Processors, 2933-MHz DDR4 memory, and the new 512GB Intel OptaneTM DC Persistent Memory Modules (DCPMMs). With this combination of features, up to 9 TB of memory is possible (using 12 x 256 GB DDR4 DIMMs and 12 x 512 GB DCPMMs).

The Cisco UCS C220 M5 Rack-Mount Server has the following features:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Up to 10 hot-swappable Small-Form-Factor (SFF) 2.5-inch drives, (up to 10 NVMe PCIe SSDs on the NVMe-optimized chassis version), or 4 Large-Form- Factor (LFF) 3.5-inch drives
- Support for 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot, supporting dual 10/25/40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports
- Modular M.2 or Secure Digital (SD) cards that can be used for boot

#### Figure 11 Cisco UCS C220 M5 Rack-Mount Server

#### Cisco UCS C220 M5 Front View



Cisco UCS C220 M5 Rear View

#### **Cisco UCS Virtual Interface Cards (VICs)**

#### Cisco UCS VIC 1387

Cisco UCS Virtual Interface Cards (VIC) are unique to Cisco. Cisco UCS Virtual Interface Cards incorporate nextgeneration converged network adapter (CNA) technology from Cisco and offer dual 10- and 40-Gbps ports designed for use with Cisco UCS servers. Optimized for virtualized networking, these cards deliver high performance and bandwidth utilization, and support up to 256 virtual devices.

The Cisco UCS Virtual Interface Card 1387 (Figure 12) offers dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP+) 40 Gigabit Ethernet and Fiber Channel over Ethernet (FCoE) in a modular-LAN-on-motherboard (mLOM) form factor. The mLOM slot can be used to install a Cisco VIC without consuming a PCle slot providing greater I/O expandability.

Figure 12 Cisco UCS VIC 1387



#### Cisco UCS VIC 1457

The Cisco UCS VIC 1457 (Figure 13) is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.





## Cisco UCS VIC 1497

The Cisco VIC 1497 (Figure 14) is a dual-port Small Form-Factor (QSFP28) mLOM card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 40/100-Gbps Ethernet and FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as NICs and HBAs.

#### Figure 14 Cisco UCS VIC 1497



#### Cisco Nexus 9332C Switch

The Cisco Nexus 9332C is a compact form-factor 1-Rack-Unit (1RU) spine switch that supports 6.4 Tbps of bandwidth and 2.3 bpps across 32 fixed 40/100G QSFP28 ports and 2 fixed 1/10G SFP+ ports (Figure 15). Breakout cables are not supported. The last 8 ports marked in green are capable of wire-rate MACsec encryption. The switch can operate in Cisco ACI Spine or NX-OS mode.

Cisco Nexus 9300 ACI Spine Switch specifications are listed below:

- 32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports
- Buffer: 40MB
- System memory: 16 GB
- SSD: 128GB
- USB: 1 port
- RS-232 serial console ports: 1
- Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP)
- Broadwell-DE CPU: 4 cores

#### Figure 15 Cisco Nexus 9332C Switch



#### Intel P4510 Series Data Center NVMe

The Intel SSD DC P4510 Series drives built on NVMe specification 1.2 PCIe with the increased density of Intel 64-layer 3D NAND and enhanced firmware features. The 8TB DC P4510 part of the reference architecture as shown in Figure 3, is built to handle read-intensive workloads and beyond which supports optimized storage efficiency while enabling data center to do more per server and minimize service disruptions. The DC P4510 creates greater Quality of Service, bandwidth, and Performance. It significantly increases server agility and utilization and accelerates applications across a wide range of workloads to lead data centers through their evolving transformation.

Some of the key benefits are:

- · Optimized for storage efficiency across a range of workloads
- Manageability to maximize IT efficiency
- Industry-leading reliability and security
- Designed for today's modern data centers

## **Cloudera Data Platform Private Cloud Base (CDP PvC Base)**

CDP is an integrated data platform that is easy to deploy, manage, and use. By simplifying operations, CDP reduces the time to onboard new use cases across the organization. It uses machine learning to intelligently auto scale workloads up and down for more cost-effective use of cloud infrastructure.

Cloudera Data Platform Private Cloud Base (CDP PvC Base) is the on-premises version of Cloudera Data Platform. This new product combines the best of both world, Cloudera Enterprise Data Hub and Hortonworks Data Platform Enterprise along with new features and enhancements across the stack. This unified distribution is a scalable and customizable platform where you can securely run many types of workloads.

#### Figure 16 Cloudera Data Platform - Unity Release



Cloudera Data Platform provides:

- Unified Distribution: Whether you are coming from CDH or HDP, CDP caters both. It offers richer feature sets and bug fixes with concentrated development and higher velocity.
- Hybrid and On-prem: Hybrid and multi-cloud experience, on-prem it offers best performance, cost, and security. It is designed for data centers with optimal infrastructure.
- Management: It provides consistent management and control points for deployments.
- Consistency: Security and governance policies can be configured once and applied across all data and workloads.
- Portability: Policies stickiness with data, even if it moves across all supported infrastructure.

## Apache Ozone

Ozone is a scalable, redundant, and distributed object store optimized for big data workloads. Apart from scaling to billions of objects of varying sizes, Ozone can function effectively in containerized environments such as Kubernetes and YARN.

Ozone consists of three important storage elements: volumes, buckets, and keys. Each key is part of a bucket, which, in turn, belongs to a volume. Only an administrator can create volumes. Depending on their requirements, users can create buckets in volumes. Ozone stores data as keys inside these buckets.

When a key is written to Ozone, the associated data is stored on the DataNodes in chunks called blocks. Therefore, each key is associated with one or more blocks. Within the DataNodes, a series of unrelated blocks is stored in a container, allowing many blocks to be managed as a single entity.

Ozone separates management of namespaces and storage, helping it to scale effectively. Ozone Manager manages the namespaces while Storage Container Manager handles the containers.





Ozone is only available as a Technical Preview in Cloudera Runtime 7.1.2 and lower.

## **Red Hat Ansible Automation**

This solution uses Red Hat Ansible Automation for all pre and post deployment steps for automating repeatable tasks to maintain consistency.

Red Hat Ansible Automation is a powerful IT automation tool. It is capable of provisioning numerous types of resources and deploying applications. It can configure and manage devices and operating system components. Due to its simplicity, extensibility, and portability, this solution extensively utilizes Ansible for performing repetitive deployment steps across the nodes.

For more information about Ansible, go to: <a href="https://www.redhat.com/en/technologies/management/ansible">https://www.redhat.com/en/technologies/management/ansible</a>

## Solution Design

2

## Requirements

This CVD explains the architecture and deployment procedures for Cloudera Data Platform Private Cloud Base on a 16-node cluster using Cisco UCS Integrated Infrastructure for Big Data and Analytics. The solution provides the details to configure CDP PvC Base on the infrastructure.

The cluster configuration consists of the following:

- 16 Cisco UCS C220 M5 Rack-Mount servers
- 2 Cisco UCS Nexus 9000 series switch
- 1 Cisco R42610 standard racks
- 2 Vertical Power distribution units (PDUs) (Country Specific)

#### **Physical Topology**

Single rack consists of two vertical PDUs and two Cisco UCS Nexus 9000 series switch with sixteen Cisco UCS C220 M5 Rack Servers connected to each of the vertical PDUs for redundancy; thereby, ensuring availability during power source failure. Figure 18 represents a 40 Gigabit Ethernet link from each server is connected to both Fabric Interconnects



Please contact your Cisco representative for country-specific information.





Cisco UCS C220 M5 Rack Server

Cisco UCS VIC ports connected to each Nexus switch in active-standby configuration with active links configured on switch A with pinning recovery to switch A in case of link failure in RHEL OS bond configuration to keep traffic locally on leaf switch.



Virtual port-channel to Northbound/Spine switch consumes only cross domain traffic meaning server to server communication which are connected to two separate pair of leaf switch.

The same architecture can be implemented with Active/Active LACP (mode 4) or balanced-alb (mode 6) based configuration. A pair of Cisco Nexus switch (A/B) are configured with vPC domain and vPC peerlink with LACP configuration as per the Cisco Nexus switch configuration best practice.

**Logical Topology** 

#### Port Configuration on Cisco Nexus 9332C

Table 6 lists the port configuration on Cisco UCS Nexus 9000 series switch.

#### Table 6 Port Configuration on Cisco UCS Nexus Switch

Port Type	Port Number
Network Uplink from Cisco UCS C220 M5 to Nexus 9332C Switch	9-24

#### Server Configuration and Cabling for Cisco UCS C220 M5

The Cisco UCS C220 M5 Rack Server is equipped with 2 x  $2^{nd}$  Gen Intel Xeon Scalable Family Processor 6230R (2 x 26 cores, 2.1 GHz), 384 GB of memory (12 x 32GB @ 2933MHz), Cisco UCS Virtual Interface Card 1387, 10 x 8TB 2.5in U.2 Intel P4510 NVMe High Perf. Value Endurance, M.2 with 2 x 240-GB SSDs for Boot.

Figure 19 illustrates the port connectivity between the Cisco UCS Nexus switch and Cisco UCS C220 M5 Rack Server. Sixteen Cisco UCS C220 M5 servers are installed in this configuration.

For information on physical connectivity and single-wire management, go to: <u>https://www.cisco.com/c/en/us/td/docs/unified computing/ucs/c-series integration/ucsm4-0/b C-Series-Integration UCSM4-0/b C-Series-Integration UCSM4-0 chapter 01.html</u>

#### Figure 19 Network Connectivity for Cisco UCS C220 M5 Rack Server

VIC 1300/1400 Connec	cted to Pair of Nexus 9000 S	Switch	
		(9) 3%	

With Cisco UCS VIC 1455 and 1457, by default a port-channel is turned on between port 1-2 and portchannel between port 3-4. Up to 14 additional vHBAs or vNICs can be created.

When port-channel mode is set to enabled, the ports on the Cisco Nexus switch should be configured as channel group members.

The Cisco UCS 1455 and 1457 Virtual Interface Cards, in non-port channel mode, provide four vHBAs and four vNICs by default. Up to 10 additional vHBAs or vNICs can be created.

As a best practice, select port 1 and 3 to connect to a pair of Cisco Nexus switch, port 2 and 4 can be added without the need for any additional changes if desired.



Switching between port-channel mode on/off requires server reboot.

For detailed configuration through Intersight see <a href="https://www.intersight.com/help/resources/creating\_network\_policies">https://www.intersight.com/help/resources/creating\_network\_policies</a>

#### **Software Distributions and Firmware Versions**

The software distributions required versions are listed in Table 7.

Table 7	Software	Distribution	and	Version
	Juliance	Distribution	ana	10131011

Layer	Component	Version or Release
Compute	Cisco UCS C220 M5	4.1(1f)
Network	Cisco UCS VIC1387 Firmware	4.4(1c)
Storage	PCIe-Switch	1.8.0.58-22d9
Software	Red Hat Enterprise Linux Server	7.7
	Cisco Integrated Management Controller (CIMC)	4.1(1f)
	Cloudera CDP PvC Base	7.1.1
	Hadoop	3.1
	Spark	2.4



The latest drivers can be downloaded here:

https://software.cisco.com/download/home/283862063/type/283853158/release/4.0(4)

#### **Cisco Intersight**

Cisco Intersight provides the following features for ease of operations and administrator to the IT staff.

#### **Connected TAC**

Connected TAC is an automated transmission of technical support files to the Cisco Technical Assistance Center (TAC) for accelerated troubleshooting.

Cisco Intersight enables Cisco TAC to automatically generate and upload Tech Support Diagnostic files when a Service Request is opened. If you have devices that are connected to Intersight but not claimed, Cisco TAC can only check the connection status and will not be permitted to generate Tech Support files. When enabled, this feature works in conjunction with the Smart Call Home service and with an appropriate service contract. Devices that are configured with Smart Call Home and claimed in Intersight can use Smart Call Home to open a Service Request and have Intersight collect Tech Support diagnostic files.

Figure 20 Cisco Intersight: Connected TAC

## Cisco Intersight + Cisco TAC + Smart Call Home = Proactive resolution



#### To enable Connected TAC, follow these steps:

- 1. Log into Intersight.com
- 2. Click the Servers tab. Select Server > Actions tab. From the drop-down list, click Open TAC Case.
- 3. Clicking "Open TAC Case" launches Cisco URL for Support case manager where associated service contracts for Server or Fabric Interconnect is displayed.

=	andre Intersight	Servers > J14-Bigdate-TPC-M5-1						Q 🔺 2	8	FI 2	۹ ا	0	Sarath Gonsganta 🚊
۱Ŀ		General Inventory											Actions
				Properties							Alarms		
II.			O Hestby	Cisco UCSC C240 M55X								A1 (0)	Cnt Launch KVM
\$			J14-Bigdete-TPC-MS-1		व स्थ छ। छ।		9 69 69 69 69 69		e ma				Launch UCSM
÷			NameNode01-Admin										Open TAC Case
lê.		Serial	WZP21400000					Lunary Lunary	Law I	2			
a			Cisco Systems inc		8888	8 8 8 8 8 8 8							
<u></u>	Software Repository				-1								
				Power Dictor LED	I.				Health Overlay	-			
*			Essentials										
			IS Not Covered	Threads		Adapters							
			10 13 1 11										
				Memory Capacity (GB)	384.0		012fe6f6-f297-11	e9-0000-000aa1400	101				
			4.6(4)										
			D Incomplete)								Security Advi	sories (D)	
		Taga											

4. Click Continue.

Ceneral Inventor	γ HCL			Actions .
				UCS-F1236 Det 12. systrack.unt Schoath led shouse arron M002_FANT_SPEHD Sensor 1 breakail     UCS-F0317 Det 7, Server 3 (censice profile: orginatul/arg/ IDP/is2US-624CM-500) health impai
		Power U Open TAC Case OPUs Citck Continue to open Cisco Scoport Case Manager(SCM) with details	Health Overlay 🌑	
		Thusaids about your selection from Intersight. IPUI Coms Selected Server, J 14-Blugdsta-TPC-M5-3 CPUI Coms Hy Serial Number: WZP21400006		▲ UCS-F0480 Dec 17. Fan module 1-2 in server 3 operability
		Memory Dop. CPU Casesh	297 - 1 - 88 DUDO DODaa14D0D038	

5. Follow the procedure to Open TAC Case.

CISCO Products & Services Support How to Buy	Training & Events Partners	Hardik Patel 🥥					
Support Case Manager       Image: Comparison of the state of the stat							
CCM Home		Need help with your case? 🧖 Chat Now					
1 Check Entitlement	2 Describe Problem	3 Review & Submit					
Request Type <ul> <li>Diagnose and Fix</li> <li>Request RMA</li> <li>Ask a Question</li> </ul>							
∧ Find Product by Serial Number							
WZP21400006	Search						
Search for other Open cases for this Serial Number							
✓ Find Product by Service Agreement	✓ Find Product by Service Agreement						
Bypass Entitlement							
Select one	$\checkmark$						
Next Save draft and exit							

### **Cisco Intersight Integration for HCL**

Cisco Intersight evaluates the compatibility of your Cisco UCS and Cisco HyperFlex systems 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).

You can use Cisco UCS Tools, a host utility vSphere Installation Bundle (VIB), or OS Discovery Tool, an open source script to collect OS and driver information to evaluate HCL compliance.

In Intersight, you can view the HCL compliance status in the dashboard (as a widget), the Servers table view, and the Server details page.





Figure 21 Example of HCL Status and Driver Recommendation for RHEL 7.6

## Advisories (PSIRTs)

Cisco Intersight sources critical security advisories from the Cisco Security Advisory service to alert users about the endpoint devices that are impacted by the advisories and deferrals. These alerts are displayed as Advisories in Intersight. The Cisco Security Advisory service identifies and monitors and updates the status of the advisories to provide the latest information on the impacted devices, the severity of the advisory, the impacted products, and any available workarounds. If there are no known workarounds, you can open a support case with Cisco TAC for further assistance. A select list of the security advisories is shown in Intersight under Advisories.



#### Figure 22 Intersight Dashboard

#### Figure 23 Example: List of PSIRTs Associated with Sample Intersight Account

œ	cisco Intersight	Adviso	ies					[] 50199   87583	Q 1 9		Jay Torasa	ker &
.2.		New Kestures have recently been added! Learn More										
010		Active	Acknowledged									
-		-		200								
	Chassis	-	This is a feature proview for testing and feedback purposes or	iy.								
	HyperFlex Clusters		Q. Search							10 v per page		
朢	Fabric Interconnects											
۵					V High	CVE-2018-15382		Oct 3, 2018 9:00 AM				
ଜ					Medium	CVE-2017-5715, CV	6593 🚟	Jul 6, 2018 2:11 PM				
ſ					Medium	CVE-2018-15407		Oct 3, 2018 9:00 AM				
3	Workflows				O Medium	CVE-2018-15429		Oct 3, 2016 9:00 AM				
P	Administration				Medium	CVE-2017-6604	1562 📰	Apr 5, 2018 9:00 AM				
	Devices											
	UCS Director											
	Software Repository											

=	alada cisco Intersight	- Security Antoniaes -> canceae 2018/064 quasi landam nel						0	Handik Pasel 🚊		
<u>10</u> 2		Details	General								
III		Severity 💽 Medium	CPU Side-Channel Information Disclo	sure Vulnerabilities						(	Acknowledge
副 副 命 本 約 日 己 命	Servers Chassis Hypor Para Custors Fabrics Interconnector Service Hoffles Potaces Software Repository Owices	Evening         Model           ID         000000000000000000000000000000000000	CPU Side-Channel Information Disclo and the Theorem Side Side Side Side Side Side Side Side	sure Vulnerabilities incrososses are addited uses to a figure incrososses are addited uses to a series incrososses are addited uses to a series incrososses are addited uses and addited uses are UNLEGATION/OF/LA are collected used at a series and a series and addited uses are addited uses addited	side ename information dis in ancharose, to read provide kernel. win as the same at a kind of in an affected 'books' that and that in an affected 'books' that and in a soft of the same at a set of the interval of the same at a set of the interval of the same at a set of the same at a same at a set of the same at a set	ecosure far far phi blass of de that ensure focund 19	per page 💽 Firmener / 1 200 TAG.	C 9 of 9 () Version	2   ¢	Suma Stabili Affects Viorko	Ack conversely

## Deployment Hardware and Software

This section details the Cisco UCS C220 M5 Rack Servers with Cisco Intersight and Cisco Nexus 9000 switch configuration that was done as part of the infrastructure build out. The racking, power, and installation of the Cisco UCS Rack Server is described in the physical topology section earlier in this document. Please refer to the <u>Cisco Integrated Management Controller Configuration Guide</u> for more information about each step.

## **Configure Cisco Nexus 9000 Switch for a Cluster Setup**

To configure the Cisco Nexus 9000 switch, follow this step:

- 1. Verify the following physical connections to Cisco Nexus 9332C:
  - a. The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.
  - b. The Ethernet ports 1/1 through 1/6 and 1/27 through 1/32 on both Nexus are directly connected to ToR switch.
  - c. The Ethernet ports 1/9 through 1/24 on both Nexus are directly connected to VIC interfaces of Data nodes.

#### **Configure Nexus**

To configure Nexus A, follow these steps:

1. Cisco UCS C220 M5 server VIC interface connected to each Nexus switch. Port 9-24 is configured. Configure the ethernet interfaces on both Nexus switches.

```
# interface Ethernet1/9
# description Connected to Server rhel01
# switchport access vlan 14
# mtu 9216
```

```
# interface Ethernet1/10
# description Connected to Server rhel02
# switchport access vlan 14
# mtu 9216
```

2. Cisco Nexus 9332C ports 1 through 6 and 27 through 32 connected to upstream switch. Configure ethernet interfaces on both Cisco Nexus switch connected to upstream switch.

```
interface port-channel50
  description NB ToR N9K
  switchport mode trunk
  switchport trunk allowed vlan 14
  spanning-tree port type network
  mtu 9216
interface Ethernet1/27
  description K14-N9K-P19-24
  switchport mode trunk
  switchport trunk allowed vlan 14
  spanning-tree port type network
 mtu 9216
  channel-group 50 mode active
interface Ethernet1/28
  description K14-N9K-P19-24
  switchport mode trunk
  switchport trunk allowed vlan 14
  spanning-tree port type network
  mtu 9216
  channel-group 50 mode active
```

For more information about configuring Cisco Nexus 9000 Series, go to:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/interfaces/configuration/guid e/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-93x.html

Go to the <u>Appendix</u> to configure active-active (balance-alb/mod 6 or 802.3ad/mod 4) based deployment.

#### **Configure Cisco Integrated Management Controller**

To configure the on-board Cisco IMC, first connect a KVM console to the server, and follow these steps:

- 1. In the BIOS POST screen, press F8 to display the CIMC configuration screen.
- 2. A prompt displays to enter the default password and provide the user password (only first time).
- 3. Select Dedicated NIC mode.

B

- 4. Select Static or DHCP assignment.
- 5. For Static mode, configure the IP address, Netmask and Gateway for the IPv4 setting of the CIMC.
- 6. Select None for NIC redundancy.

- 7. Press F10 to save the configuration and exit the utility.
- 8. Open a web browser on a computer on the same network.
- 9. Enter the IMC IP address of the Cisco UCS C220 M5 Server: http://<<var cimc ip address>.
- 10. Enter the login credentials as updated in the IMC configuration.

Figure 24	Cisco IMC Login
	aftafta cisco
	C220-WZP23420UK9
	Cisco Integrated Management Controller
	Uberrarie III in the second
	Prazeovra Larquage : Englah ▼
	© 2010 Cesos Systems, Inc. Cesos, Second Systems and Cesos Systems ingo area ingidiment linatematics of Cesos Systems, Inc. and/or its allikation in this U.S. and outpart of the U.S.

cisco Cisco	a Integrated Management Controlli				🐥 🗹 0 admin@10.14.1.8 - C220-WZP23420UK8 4
Chassis / Sum	imary 🖈				Refresh   Host Power   Launch KVM   Ping   CIMC Reboot   Locator LED   🕘 🌘
Server Proper	rties	Cisco Integrated M	lanagement Controller (Cisc	o IMC) Information	n
Product Name:	UCS C220 M5SN	Hostname:	C220-WZP23420UK9		
Serial Number:	WZP23420UK9	IP Address:	10.14.1.201		
PID:	UCSC-C220-M5SN	MAC Address:	5C:71:0D:49:4D:78		
UUID:	848D666F-A416-4AE0-A7A8-054F5A81BFB4	Firmware Version:	4.0(4h)		
BIOS Version:	C220M5.4.0.4L0.0831191119	Current Time (UTC):	Thu Fab 13 20:56:09 2020		
Description:		Local Time:	Thu Feb 13 20 56:09 2020 UTC +0000		
Asset Tag:	Unknown	Timezone:	UTC	Select Timezone	
Chassis Statu Power Overall Berver Tempe	IS r State: Con Status: Cod erature: Cod	Server Utilization		Concel (Microson (%) CPU (Microson (%)	
Overall DIMM	Status: Will Good	.nu -		10 Usization (%)	
Power Su	ipplies: Second	60 -			
	Fans: M Good	50 - 40 -			
	or LED: VA	30			
Locate Overall Storage	Status: 🖾 Good	20 -			

## **Cisco Intersight and IMC Configuration**

This section details the Cisco Intersight configuration and Cisco IMC (Integrated Management Controller) configuration that was done as part of the infrastructure build out. The racking, power, and installation of the Cisco UCS Rack Server is described in the physical topology section earlier in this document.

### Integrate Cisco IMC with Intersight

To register Cisco IMC to Intersight, follow these steps:

1. From the Cisco IMC, go to Admin > Device connector.

	Se vinde Cisco Integrated Management Controller	÷ 🗹
	A / Admin / Device Connector 🗰	Refresh   Host Power   Launch
Chassis •	The Device Cannector is an embedded management controller that enables the capabilities of Cisce Intersight, a cleud based management platform. For detailed information about configuring the device connector, plas	ase visit Help Center
Compute	Device Connector	
Networking +	ACCELES HOLE. ALLOW COM HEL	
Storage +		
Admin 🔹		•••• 🛆
User Management	Device Connector Internet Hetry Connection	Intersight
Networking		
Communication Services		
Security Management	imersign Uxis Hesove Error	
Event Management	DNS appears to be configured, but unable to resolve the DNS name of Intensight. Intensight may be in maintenance	
Firmware Management	Remediators	
Utilities	verny me uno server m asanesses configures are vario. Open settings	
Device Connector	veriny the units servers are reachable from Device Connector.	
Derive Connector	1.0.4025	

2. On the right side of the screen, click Settings.

🗲 🧃 💼 Cisco Integrated Management Controller	÷ 🗹 0
Admin / Device Connector ★	Retreah   Host Power   Launch KVM   Ping   CIMC Reboot   Locator LED   🕹
The Device Connector is an embedded management controller that enables the capabilities of Cloco Intersight, a cloud-based management platform. For	detailed information about configuring the device connector, please visit Help Center
Device Connector	③ Settings ↓ ○ Refresh
ADDESS MODEL ALLEM CONTINUE	Device ID
	ß
Device Connector	Note: Section         Intersight
Intersight DNS Resolve Error	
DNS appears to be configured, but unable to resolve the DNS name of Intersight. Intersight may be in maintanance	
Remediations	
Verify the DNS server IP addresses configured are valid. Open Settings	
Verify the DNS servers are reachable from Device Connector.	
1.0.9428	

3. In the Settings screen, go to the General tab and enable the "Device connector." For the Access Mode, select "Allow control" and enable "Tunneled vKVM."

Tunneled vKVM is supported only for Cisco UCS C-Series servers with an Advantage or Premier license.


## We enabled and launched Tunneled vKVM to complete OS Installation from Cisco Intersight.

4. Configure DNS, NTP, Proxy as required for reachability to Intersight.

Admin / Device C	onnector *	Refresh   Host Power   Launch KVM   Ping   CIMC Reboot   Locator LED   🔞										
The Device Connector is an embed	a 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											
Settings		×										
General												
DNS Configuration	When this option is ON, you can claim this system and leverage the capabilities of Disco Intersight. If it Is DFF, no communication will be allowed to Disco Intersight. Leven More											
NTP Configuration	Device Connector											
Proxy Configuration	Access Mode											
Geroncave Manager	Read only     Allow descent											
	Longiguration from Intersight only											
	C Tunneled vKVM											
		Cancel Save										
1.0.9-1172												

5. Verify reachability to Cisco Intersight is updated after configuring Settings.

😸 📲 Cisco Integrated Management Controller	🕂 🗹 🕇 admi
I / Admin / Device Connector 🛣	resh   Host Power   Launch KVM   Ping
The Device Connector is an embedded management controller that enables the capabilities of Claco intersight, a cloud-based management platform. For detailed information about configuring the device connector, please v	sit Help Center
Device Connector	Settings C Refresh
Device Connector	E E
Not Claimed The connection to the Claco Intersight Portal is successful, but device is still not claimed. To claim the device open Claco Intersight, create a new account and follow the guidance or go to the Devices page and click Claim a New Device for existing account. Open Intersight 18.9428	

6. Log into Cisco Intersight with your credentials.



7. Click Continue to create a new Account or new devices can be registered in existing account. We created a new Account.

۱۱۱۱۱۱۱ cisco	
INTERSIGHT	
Create an Account To create an account you should sign in with Cisco	
Continue	
Already have an Intersight Account? Sign In	

8. Provide Device ID and Claim code to create an account for the cluster.

uluulu cisco
INTERSIGHT
Account Creation ①
To complete account creation, you must claim a device to Intersight. Enter the Account Name, Device ID, and Claim Code from the device.
Account Name *
UCSC-C220-M5SN
Device ID *
Claim Code *
Cancel Create
Learn more about Cisco Intersight at Help Center

9. Verify the account is created successfully.

יוןויוןוי cisco
INTERSIGHT
$\bigotimes$
Your account has been successfully created. For future logins, use your custom account URL:
https:// .intersight.com/ Log me in
Learn more about Cisco Intersight at Help Center

10. After logging in, verify the device added is listed under Administration > Devices.

=	-ili-ili- cisco Intersight	Devices		\$ B @	<   @   @   H	iardik Patel 🚊		
ıb	Dashboards	📉 New features have recently been added! Le	arn More					×
в							Claim a	New Device
	Chassis							
69	HyperFlex Clusters	(i) Types	ap Connection e= Ac	ocess Modes				
코	Fabric Interconnects							
6								
ន	Policies						16 ∨ perpage K < 1 of 1 ≥	
ģ	Administration ^							
	Devices		Connected	Standalone M5 Server		WZP23361125	hardipat@ciaco.com	
	Software Repository							

11. Click Claim a New Device to claim all remaining servers.

=	dtalls cisco Intersight	Device Claim	φ	Ø	¢\$	٩,	٢	0
<u>11</u>	Dashboards	寐 New features have recently been added: Learn More						
88	Servers							
	Chassis	Claim a New Device						
ŝ	HyperFlex Clusters							
Ŧ	Fabric Interconnects							
6	Profiles	Direct Claim Claim Claim Through Intersight Assist						
Ē	Policies	To claim your device, you must have the Device ID and Claim Code						
ģ	Administration ^	Device ID * Claim Code *						
	Devices							
	Software Repository							

12. Make sure all servers are claimed (the servers that are part of the cluster configuration).

≡	cisco Intersight	Serv	ars										(	0   D	ç1	Q,	۲	⊙ Hare	fik Patel <u>ட</u>
Dla	Dashboards																		
=	Servers			Health		Power On 16	HCL Status	16	Hodels		Cont	tract Status	📰 Server Pi	rofiles		3 Tasks	; (Last 24h)		X
	Chassis		(	16) • Headli	hy 16		- Internet			<ul> <li>c270 mssn 16</li> </ul>									
\$	HyperFlex Clusters																		
Ŧ	Fabric Interconnects			<i>ି</i> ା ପ୍ରେଲ	arch									16 items fou		per pag			$\odot$
3	Profiles			Name		Health	: Contract Sta		Manag :	Model :		Memor :					Jtility Storage		Ģ
Ē	Policies					Healthy	E Not Cox	ered	10.14.1.216	UCSC-C220		384.D						4.0(4h)	
ē	Administration ^					O Healthy		vered		UCSC-C220		384.0						4.0(4h)	
	Devices					Healthy		ered	10.14.1.213	UCSC-C220		384.0						4.0(4h)	
	Software Repository					Healthy			10.14.1.214	UCSC-C220	91.2	384.0						4.0(4h)	
						Healthy			10.14.1.212	UCSC-C220		384.0						4.0(4h)	
						Healthy				UCSC-C220		384.D						4.0(4h)	
						<ul> <li>Healthy</li> </ul>	Not Cov	ered		UCSC-C220		384.0						4.0(4h)	
						Healthy		ered	10.14.1.209	UCSC-C220	91.2	384.0						4.0(4h)	
						Healthy			10.14.1.208	UCSC-C220		384.0						4.0(4h)	
						O Healthy			10.14.1.207	UCSC-C220		384.D						4.0(4h)	
						© Healthy	Not Cov	ered	10.14.1.206	UCSC-C220		384.0						4.0(4h)	
						<ul> <li>Healthy</li> </ul>	Not Cov	rered	10.14.1.205	UCSC-C220	91.2	384.0						4.0(4h)	
						Healthy			10.14.1.204	UCSC-C220		384.0						4.0(4h)	
		C		() C220-WZP23	1260054	Healthy	I Not Cov	ered	10.14.1.203	UCSC-C220	91.2	384.D						4.0(4h)	

13. Click Settings, then select Licensing.

=	الالالالالالالالالالالالالالالالالالال	Servers			₽ <b></b>	Ø	Q,	۲	0
<u>00o</u>	Dashboards						Audit Logs		
	Servers	4 Health	() Power 🗮 () On 19 💿 1	HCL Status	Models		Sessions		at 19
	Chassis	(19) = Healthy 19			(19) C220 M5SI C220 M5SI	C220 M5SN 16 C220 M5SX 3	Licensing		
60 60	HyperFlex Clusters				$\smile$		Settings		

14. Click Register License to assign Essential, Advanced. or Premier License for Cisco Intersight. For more information about the different license tiers for Cisco Intersight, see: <u>https://www.intersight.com/help/getting\_started#licensing\_requirements</u>

By default, the claimed devices in Cisco Intersight are allocated Base License Tier.

15. Enter Product Registration Token for Cisco Intersight. Click Register.

Smart Software Licen	Sing Product R	egistration
If you do not have a Product Insta a new token within the specific vi Cisco Smart Software Manager	ance Registration Toke irtual account in the	n, you can generat
Product Instance Registration To	ken *	
	Cancel	Register

16. Click Set Default Tier. Assign the desired Default Tier.

≡	cisco Intersight	Licensing		C & 4 <	🚯 🕜 Hardik Patel 🖉
<u>00o</u>	Dashboards	enses			
	Servers				Set Default Tier
	Chassis				
<b>\$</b>	HyperFlex Clusters	Base ⊚	Essentials o	Advantage ©	
	Fabric Interconnects				
6	Profiles	Status • Not Used	Status O Not Used	Status • Not Used	Status In Compliance
í	Policies				Usage 19 Servers
~	Orchestration				

17. To assign a new license tier to existing server, click the Servers tab in Cisco Intersight. Select the server(s). Select Set License Tier.



18. Select License Tier from the drop-down list.

Tier		
Premier	 	✓ ①

19. From the Servers tab, check the checkbox to select all servers. Click the ellipses to view the drop-down list. Click Upgrade firmware.



20. Clicking the firmware upgrade provides the option to choose the location of the firmware iso. We configured the NFS share for remote ISO repository. Provide the information for Remote IP, Remote Share and Remote File. Click Upgrade Firmware.



The storage utility-based firmware upgrade steps are described in the Appendix.

Upgrade Firmw	are		×
Network Sha	ire	Utility Storage ①	
<ul> <li>Firmware will be reboot immediat corresponding or</li> </ul>	e installed on the tely after clicking option below.	next device reboot. To J Upgrade, enable the	
NFS	CIFS	HTTP/S	
Remote IP *			0
Remote Share *			ũ
/ISO			
Remote File *			-
ucs-c220m5-huu-4.	0.4i.iso		•
C Reboot Immed	iately to Begin U	ograde	
	Cancel	Upgrade Firmw	are

21. Click Upgrade Immediately.



≡	altala cisco	Intersight	Servers										٩	ß	ç) (	રે ⊚	©	Hardi	k Patel ,
ılı III III III III		Health 16 + Health	v 16		Power On 16	<ul> <li>HCL Status</li> <li>Incomplete 16</li> </ul>	Models	• C22D1455N 16	Con	tract Status Covered 16	Server F	<b>Profiles</b> A AVAILAB		asks (Last 24h) 4 Rannin • Falwel :	16 48				ХК
T.		୍ ପ୍ୟୁ												16 items found		page K K			٢
6		Name			Health	Contract Status	Manag :	Model :	CP ⊙ :	Memor 0	UCS Domain	HX Cluster		Utility Storage	Firmware				ş
目					Healthy	E Not Covered	10.14.1.216	UCSC-C220		384.0					4.0(4h)				
Ģ					Healthy	E Not Covered	10.14.1.215	UCSC-C220		384.0					4.0(4h)				
					Healthy	5 Not Covered	10.14.1.213	UCSC-C220		384.0					4.0(4h)				
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.214	UCSC-C220		384.0					4.0(4h)				•••
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.212	UCSC-C220		384.0					4.0(4h)				
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.211	UCSC-C220		384.0					4.0(4h)				
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.210	UCSC-C220		384.0					4.0(4h)				•••
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.209	UCSC-C220		384.0					4.0(4h)				•••
					<ul> <li>Healthy</li> </ul>	E Not Covered	10.14.1.208	UCSC-C220		384.0					4.0(4h)				
					Healthy	E Not Covered	10.14.1.207	UCSC-C220		384.0					4.0(4h)				••••
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.206	UCSC C220		384.0					4.0(4h)				•••
					<ul> <li>Healthy</li> </ul>	Not Covered	10.14.1.205	UCSC-C220		384.0					4.0(4h)				•••
					<ul> <li>Healthy</li> </ul>		10.14.1.204	UCSC-C220		384.0					4.0(dh)				
	0	O C220-WZP23	260354	0	<ul> <li>Healthy</li> </ul>	E Not Covered	10.14.1.203	UCSC-C220	91.2	384.0					4.0(4h)			0	

22. The progress indicator is displayed next to the server being upgraded in the Servers menu.

23. Click an individual server to display the status of the update.

<u>t0</u> ;	General Inventory	Server Profile HCL									Action	5 V
			Properties							Alama		
	Health	O Healthy	Cisco UCSC-C228-M55N			Fron	nt View	Rear View	Top View	AII (0)	Critical (0)	Warning (0)
	Namo	C220-WZP23361125						aille				
	User Label		the I	-		<u>↓</u>						
	Management IP			ŀ		->						
	Serial	WZP23361125	Power 🕐 Locator LED 🚺					Health	Overlay 🌉			
		UCSC-C220-MSSN										
		Claco Systems Inc	CPUs									
	Revision				Adaptera							
	Asset Tag	Unknown		48	NIC Interfaces							
		Essentials	CPU Cores Enabled	48	HBA Interfaces							
	Contract Status	EI Not Covered	Memory Capacity (GB)	384.0		F05503F2-015D-4883-9A7D-80	DSF089C994	в				
	Firmware Version	4.0(4h)	CPU Capacity (GHz)	91.2								
	Firmware Status	O Upgrading								Security Advisories (0)		
	Organizations											
	Tags											

24. The updated version can be verified from the Servers tab.

≡	cisco Intersight	Servers								٥		60   <i>C</i>   Ø	⊘ на	ardik Patel <u>"Q.</u>
16 11 11 10	() Health (16) * Healty 1	() Power () On 16 6	III HCL Status	Models	<ul> <li>czzowech 16</li> </ul>	Cont	ract Status Rovered 10	Server F	<b>rofiles</b> A AVAILABLI		Tasks (Last 24h) 64 Bongle Failed 4	lad 16 18		
8 19	J Q Search											<mark>16 ∨</mark> perpage K <		
E	C220-WZP2336	: Health	Contract Status	Manag : 10:14.1.216	Model :		Memor : 384.0	UCS Domain	HX Cluster	Server 0	Utility Storage	Firmware Version		
ē		12W © Healthy	E Not Covered	10.14.1.215	UCSC-C220	91.2	384.0					4.0(4i)		
		120 © Healthy	Not Covered	10.14.1.214	UCSC-C220		384.0					4.0(4i)		
		0 Healthy			UCSC-C220		384.0					4.0(4i)		
	CZ20-WZP2342	O Healthy	Not Covered	10.14.1.211	UCSC-C220	91.2	384.0					4.0(4i)		



More information about the firmware upgrade can be found here: <u>https://intersight.com/help/features#firmware\_upgrade</u>

## **Configure Policies to Create Server Profile**

To create policies for Server Profiles creation, follow these steps. These steps can also be completed at the time of the Server Profile creation.

1. On Cisco Intersight WebUI, select the Policies tab. Click Create Server Policy. Create Server Policy provides an option to create different policies.

	Select Policy Type			
	Q, Search	*		
	Adapter Configuration			
	) BIOS			
	O Boot Order	_		
	O Device Connector			
	O Disk Group			
	<ul> <li>Ethernet Adapter</li> </ul>			
	C Ethernet Network			
	Ethernet QoS			
	Fibre Channel Adapter			
	Fibre Channel Network			

- 2. Select Adapter Configuration from the list of policies, then click Next.
- 3. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

Olo Dashboards			
Servers	General	Organization *	
	General	CDIP-C220M5SN ~	
E Chassis			
씛 HyperFlex Clusters	<ul> <li>Policy Details</li> </ul>	Name *	
		CDIP-AdapterConfig	
Fabric Interconnects			
🕞 Profiles		Description	
0		Adapter Configuration Policy for CDIP setup v	
Policies			
별 Administration ^		Add Tag	
		CDIP UCSC-C220-M5SN × ×	
Uevices			
Software Repository			
			Next

4. Click Add VIC Adapter Configuration.

000 Dashboards					
E Servers	General	The Adapter Configuration	will be applied only on next host r	eboot.	
🧱 Chassis		Adapter Configurations			
器 HyperFlex Clusters	Policy Details				
👳 Fabric Interconnects					
👸 Profiles		PCI Slot			Port Channel
Policies					
Administration					
Devices					
Software Repository					
					Previous

5. Select PCI Slot and required setting for the Adapter Configuration.

<u>00o</u>	Dashboards			Add VIC Adapter Config	uration	
	Servers		General	PCI Slot * MLOM		0
000	Chassis					
୍ କୁଜି	HyperFlex Clusters		Policy Details	Ethernet Settings		
P	Fabric Interconnects			C Enable LLDP 🛛		
6	Profiles			Fibre Channel Settings		
1	Policies			Enable FIP 🛛		
Ō	Administration			Port Channel Settings		
	Devices			Enable Port Channel 🛛		
	Software Repository			DCE Interface Settings		
				DCE Interface 1	DCE Interface 2	
				FEC Mode	FEC Mode	
				Auto 🗸 🛈	Auto	<u> </u>
						· · · ·
		ŕ			Cancel	Add

6. Click Create.

<u>00o</u>	Dashboards							
	Servers	• General	🔥 The Adapter Co	nfiguration will be applied onl	y on next host reboot.			
	Chassis		Adapter Configuration	IS				
÷	HyperFlex Clusters	Policy Details	Add VIC Adapter C	onfiguration				
	Fabric Interconnects							
6	Profiles		PCI Slot				Port Channel	
í	Policies			Enabled		Enabled	Enabled	
ē	Administration							
	Devices							
	Software Repository							
							Previous	te

7. Select BIOS configuration in Create Server Policy options.

<u>00o</u>	Dashboards	HyperFlex Policies Server Pol	Select Policy Type ×	
			୍କ Search	
			Adapter Configuration	l
			• BIOS	
			O Boot Order	L
<u>ئ</u>			<ul> <li>Device Connector</li> </ul>	
			O Disk Group	
			C Ethernet Adapter	
			C Ethernet Network	l
			C Ethernet QoS	
			Fibre Channel Adapter	
			Fibre Channel Network	-
			Cancel	

0]0	Dashboards		
	Servers	General	0rganization * CDIP-C220M5SN v
	Chassis		
	HyperFlex Clusters	<ul> <li>Policy Details</li> </ul>	Name* CDIP-C220M5SN-BIOS
	Fabric Interconnects		
	Profiles		Description BIOS configuration for Class LICE C120 LICES
	Policies		
٩	Administration ^		Add Tag
	Devices		
	Software Repository		
			Net

9. Configure the BIOS policy.

## Error! No text of specified style in document.

• General	A The BIOS settings will be applied only on next host reboot.			
Policy Dataile	+ LOM And PCIe Slots			
	- Processor			
	Adjacent Cache Line Prefetcher		Altitude	
	enabled	× 0	platform-default	<u>~ 0</u>
	Autonomous Core C-state		CPU Autonomous Cstate	
	platform-default	× 0	platform-default	× 0
	Boot Performance Mode		Downcore control	
	platform-default		platform-default	
	Channel Interleaving		Closed Loop Therm Throt	
	auto		nlatform-default	
		<u>`</u>		
	Processor CMCI		Config TDP	
		~ 0	platform-default	¥ 0
	Core MultiProcessing		Energy Performance	
	all	× 0	performance	<u>~ 0</u>
	Farmer Flags Annalda		0011 Df	
	Frequency Floor Override		CPU Performance	
General	Frequency Floor Override platform-default	~ 0	CPU Performance platform-default	~ 0
General	Frequency Floor Override platform-default	<u>~ ©</u>	CPU Performance platform-default	<u>v 0</u>
General	Frequency Floor Override platform-default Power Technology	<u>~ ©</u>	CPU Performance platform-default	<u>~ 0</u>
<ul> <li>General</li> <li>Policy Details</li> </ul>	Frequency Floor Override platform-default Power Technology performance	<u>~ 0</u> ~ 0	CPU Performance platform-default Demand Scrub enabled	× 0 × 0
General     Policy Details	Frequency Floor Override platform-default Power Technology performance	<u>~ 0</u> ~ 0	CPU Performance platform-default Demand Scrub enabled	<u> </u>
General     Policy Details	Frequency Floor Override Platform-default Power Technology performance	× 0 × 0	CPU Performance platform-default Demand Scrub enabled	<u>~ 0</u> ~ 0
General     Policy Details	Frequency Floor Override  Frequency Floor Override  platform-default  Power Technology  performance  Direct Cache Access Support  enabled	× 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance	× 0 × 0
General     Policy Details	Frequency Floor Override  Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled	× 0 × 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance	× 0 × 0 × 0
General     Policy Details	Frequency Floor Override  Frequency Floor Override  platform-default  Power Technology  performance  Direct Cache Access Support  enabled	~ © ~ ©	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance	× 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo	× © × © × ©	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance Energy Performance Tuning http://www.communice.c	× 0 × 0 × 0
General     Policy Details	Frequency Floor Override  Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default	× 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default	~ 0 ~ 0 ~ 0
General     Policy Details	Frequency Floor Override platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default	× 0 × 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance Energy Performance Tuning platform-default	~ 0 ~ 0 ~ 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology	× 0 × 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance Energy Performance Tuning platform-default EPP Profile	× 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance Energy Performance Tuning platform-default EPP Profile platform-default	× 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override platform-default Power Technology performance Direct Cache Access Support enabled Energy Efficient Turbo platform-default Enhanced Intel Speedstep(R) Technology enabled	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default Demand Scrub enabled DRAM Clock Throttling Performance Energy Performance Tuning platform-default EPP Profile platform-default	× 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  EPP Profile platform-default  Local X2 Apic	× 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  Local X2 Apic platform-default	× 0 × 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance Energy Performance Tuning platform-default  EPP Profile platform-default Local X2 Apic platform-default	× 0 × 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default  Hardware Prefetcher	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  EPP Profile platform-default  Local X2 Apic platform-default  CPU Hardware Power Management	× 0 × 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default  Hardware Prefetcher enabled	× 0 × 0 × 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  Demand Scrub enabled  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  Local X2 Apic platform-default  CPU Hardware Power Management platform-default	× 0 × 0 × 0 × 0 × 0 × 0
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default  Hardware Prefetcher enabled	× 0 × 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  CPU Performance  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  Local X2 Apic platform-default  CPU Hardware Power Management platform-default	<ul> <li>• •</li> </ul>
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default  Hardware Prefetcher enabled  MC Interdesting	× 0 × 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  CPU Performance  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  Local X2 Apic platform-default  CPU Hardware Power Management platform-default	<ul> <li>• •</li> <li>• •</li></ul>
General     Policy Details	Frequency Floor Override  platform-default  Power Technology performance  Direct Cache Access Support enabled  Energy Efficient Turbo platform-default  Enhanced Intel Speedstep(R) Technology enabled  Execute Disable Bit platform-default  Hardware Prefetcher enabled  IMC Interleaving platform-default	× 0 × 0 × 0 × 0 × 0	CPU Performance platform-default  CPU Performance  DRAM Clock Throttling Performance  Energy Performance Tuning platform-default  Local X2 Apic platform-default  CPU Hardware Power Management platform-default  Intel HyperThreading Tech enabled	

## Error! No text of specified style in document.

Intel Turbo Boost Tech ✓ ○ enabled platform-default 📍 General Policy Details disabled v 
o platform-default ✓ ○ enabled enabled platform-default v O platform-default platform-default v 
o enabled ~ © platform-default ✓ ⊙ disabled disabled ✓ ⊙ disabled disabled ✓ ◎ HW ALL × 0

• C	Power Performance Tuning		Rank Interleaving	
General	platform-default		platform-default	
Policy Details				
	Single POTE		SMTMODE	
	platform-default	× ©	platform-default	<u> </u>
	Sub Numa Clustering		DCU Streamer Prefetch	
	platform-default		enabled	
	SVM Mode		Workload Configuration	
	platform-default		platform-default	
	XPT Prefetch			
	platform-default	× 0		
	+ USB			

• General	— RASMemory			
	CKE Low Policy		DRAM Refresh Rate	
Policy Details	platform-default	<u> </u>	platform-default	<u> </u>
	Low Voltage DDR Mode		Mirroring Mode	
	platform-default	× @	platform-default	<u>~ 0</u>
	NUMA optimized		SelectMemory RAS configuration	
	platform-default	<u>~ @</u>	maximum-performance	~ 0
	Sparing Mode			
	platform-default	<u>~ 0</u>		



Cisco recommends that you upgrade to Cisco UCS Manager Release 4.0(4h) or Release 4.1(1c) or later to expand memory fault coverage. ADDDC Sparing will be enabled and configured as "Platform Default" for Memory RAS configuration. For more information, refer to <u>Performance Tuning Guide for Cisco UCS</u> <u>M5 Servers.</u>

10. Select Boot order in Create Server Profile.

$\equiv$	cisco Intersight	Policies	n
		HyperFlex Policies Server Pol Select Policy Type	×
		Q Search	^
	Chassis	Adapter Configuration	
	HyperFlex Clusters	Name     BIOS	
		CDIP-C220M5SN-BIOS	
6		CDIP-AdapterConfig	
		C Ethernet Adapter	
			=
	Software Repository	C Ethernet OoS	=:::
			-
			-
		Cancel Next	

11. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

<u>00a</u>	Dashboards			
	Servers	eneral	Organization *	
	Chassis			
- 699 699	HyperFlex Clusters	Policy Details	Name * CDIP-C220M5SN-Boot	
<u></u>	Fabric Interconnects			
3	Profiles		Description Boot Policy for C220 M5SN nodes	
訚	Policies			
ছ	Administration ^		Add Tag CDIP UCSC-C220 MSSN × × ×	
	Devices			
	Software Repository			
			Next	

12. Select the boot mode.

<u>00o</u>	Dashboards		
38	Servers	General	Boot Mode
8	Chassis		Configured Boot Made ⊙ ⊙ Legacy ◯ Unified Extensible Firmware Interface (UEFI)
\$	HyperFlex Clusters	Policy Details	Add Boot Device v
₽	Fabric Interconnects		iSCSI Boot
6	Profiles		Local CDO
6	Policies		Local Disk
ē	Administration /		NVMe:
	Devices		PCH Storage
	Software Repository		PXE Boot
			SAN Boot
			SD Card
			UEFI Shell
			USB
			Virtual Media
			Previous Create

13. From the list of Boot Device select Virtual Media (vMedia-KVM) and select KVM mapped DVD as Sub-Type.

≡	alada cisco Intersight	Create Boot Order Policy		Δ.	2 .	2	ęt	Q,	۲	0	Hardik Pate
<u>00o</u>	Dashboards										
	Servers	• General	Boot Mode								
	Chaseis		Legacy      Unified Extensible Firmware Interface (UEFI)								
80	HyperFlex Clusters	Policy Details	Add Boot Device								
	Fabric Interconnects										
6	Profiles		- Virtual Media (vMedia-KVM)						Enabled		
A	Policies		Device Name *		Sub-Type						
ē	Administration ^				None						
	Devices				CIMC	MAPPED	DVD				
	Software Repository				CIMC	MAPPED	HDD				
	contraine responsibly				KVM N	MAPPED	DVD				
					KVM	MAPPED	HDD				
					KVM	MAPPED	FDD				
								Previou			Create

14. From the Add Boot Device list, select Local Disk and enter the name for the device and slot as MSTOR-RAID for M2 boot drives.

000	Dashboards		<b>.</b>				
	Servers	General	Boot Mode				
	Chassis		Legacy      Unified Extensible Firmware Interface (UEFI)				
	HyperFlex Clusters	Policy Details					
	Fabric Interconnects						
	Profiles		Virtual Media (vMedia-KVM)		Enabled	Û	
í	Policies		Device Name * vMedia-KVM	Sub-Type KVM MAPPED DVD			
	Administration						
	Devices		— Local Disk (M2-Boot)		Enabled		
	Software Repository		Device Name *	Slot			
			M2-Boot	MSTOR RAID			

15. Select Boot order in Create Server Profile.

Ξ	uludu cisco Intersight	Policies	o
		HyperFlex Policies Server Pol Select Policy Type	×
		Q, Search	-
	Chassis	Adapter Configuration	
	HyperFlex Clusters	Name     BIOS	
		CDIP-C220M5SN-BIOS	
6		CDIP-AdapterConfig	
		Disk Group	
		C Ethernet Adapter	
		C Ethernet Network	=
		C Ethernet QoS	
		Fibre Channel Adapter	
		Fibre Channel Network	
			1
		Cancel	

<u>oDo</u>	Dashboards		
	Servers	eneral	Organization * CDIP-C220M5SN
	Chassis		
889 899	HyperFlex Clusters	Policy Details	Name* CDIP-C220MSSN-Boot
	Fabric Interconnects		
ි	Profiles		Description
圁	Policies		Duck Pulicy in 1220 milan rides
ş	Administration ^		Add Tag
	Devices		
	Software Repository		
			Med.

17. Select the boot mode.

000	Dashboards		
	Servers	• General	Boot Mode
<b>8</b>	Chassis		Configured Boot Mode ⊙ ● Legacy ─ Unified Extensible Firmware Interface (UEFI)
\$	HyperFlex Clusters	Policy Details	Add Boot Device
₽	Fabric Interconnects		iSCSI Boot
6	Profiles		Local CDD
1	Policies		Local Disk
٩	Administration ^		NVMe
	Devices		PCH Storage
	Software Repository		PXE Boot
			SAN Boot
			SD Card
			UEFI Shell
			U\$8
			Virtual Media
		Cancel	Previous Dreate

18. From the list of Boot Device select Virtual Media (vMedia-KVM) and select KVM mapped DVD as Sub-Type.

cisco Intersight	Create Boot Order Policy		۵ م							Hardik Patel
Dashboards										
Servers	General	Boot Mode								
Chassis		Legacy Unified Extensible Firmware Interface (UEFI)								
HyperFlex Clusters	Policy Details	Add Boot Device								
Fabric Interconnects										
Profiles		— Virtual Media (vMedia-KVM)						Enabled	Û	
Policies		vMedia-KVM	0	Nor	-Type ne					~ 0
Administration ^				N	lone					
Devices					IMC MAPPED	) DVD				
Software Repository					IMC MAPPED	HDD				
					VM MAPPED	DVD				
				к	VM MAPPED	HDD				
					VM MAPPED	FDD				
							Previou		C	eate

19. From the Add Boot Device list, select Local Disk and enter the name for the device and slot as MSTOR-RAID for M2 boot drives.

0월 Dashboards 플 Servers Chasels 값 HyperFlex Clusters 약 Fabric Interconnects	General     General     Policy Details	Boot Mode Configured Boot Mode O • Legacy Unified Extensible Firmware Interface (UEFI) Add Boot Device V	
🔀 Profiles		- Virtual Media (vMedia KVM) Device Name * vMedia KVM 00000000000000000000000000000000000	Enabled      ^      Sub-Type     KVM MAPPED DVD
夏 Administration			
Devices Software Repository		— Local Disk (M2-Boot) Device Name *	C Enabled i 👔 🔺 🗸
		M2 Boot	MSTOR RAID O

20. Enable the option "Configuration from Intersight only" if you want to control only from Intersight.

≡	dialia Intersight	Create Device Connector Policy		🗘 🔺 2	ß	<del>ç.</del> ]	୍ତ	0	Hardik Patel
00.0	Dashboards								
	Servers	General	Configuration from Intersight only ③	Enables configuration lockout o	n the endpoint.				
	Chassis								
\$	HyperFlex Clusters	Policy Details							
52	Fabric Interconnects								
6	Profiles								
í	Policies								
ē	Administration ^								
	Devices								
	Software Repository								
								Cr	eate

21. Create Ethernet Adapter Policy in Create Server Policy.

≡	cisco Intersight	Policies	<u> </u>
<u>00a</u>		INew features have recently been a Select	Policy Type ×
		HyperFlex Policies Server Poli Q Se	arch
			dapter Configuration
60 (P)			os
			oot Order
6			evice Connector
Ē			sk Group
Ŷ			hernet Adapter
		CDIP-AdapterContig	hernet Network
			hernet QoS
		⊖ Fi	pre Channel Adapter
		🔿 Fil	ore Channel Network
			Cancel

≡	cisco Intersight	Create Ethernet Adapter Policy	L) 🖬 3 🗚 2				Hardik Patel
<u>00a</u>	Dashboards	E New features have recently been added! Learn More					
	Servers						
	Chassis	Organization *     Organization *     CDIP-C220M5SN					
ති	HyperFlex Clusters						
52	Fabric Interconnects	Policy Details     Name *     CDIP-EthAdapter					
6	Profiles						
1	Policies	Description Ethernet Adapter Policy for CDIP					
ð	Administration ^						
	Devices	Add Tag CDIP UCSC-C220-M5SN × ×					
	Software Repository						
		Cancel				Next	

23. Leave the default settings or set the custom value and click Create. For more information, see: <u>Tuning Guide-</u> <u>lines for Cisco UCS Virtual Interface Cards.</u>

		Enable Virtual Extensible LAN ©				<u>^</u>
🚟 Servers 📭 Ge	eneral		lation			
E Chassis						
ම් Po	olicy Details	Enable Accelerated Receive How Steering U				
Sabric Interconnects		Enable Advanced Filter ©				
🕞 Profiles	F	toCE Settings				
Policies						
⑨ Administration ^		nterrupt Settings				
Devices	lr c	nterrupts		Interrupt Mode		
Software Repository	-	5				<u>v v</u>
		nterrupt Timer, us		Interrupt Coalescing Type		
	1	125	_	Min		<u> </u>
	R	Receive				
	я	Receive Queue Count		Receive Ring Size		
	4	4		512		• •
	Cancel				Previous	Create
<u>01o</u> Dashboards	4	4	0	512		<u> </u>
📰 Servers 🛉 Ge	eneral					
		renemit				
E Chaseis	lieu Detaile T	Franceint		Tranomit Pina Siza		
📰 Chaseis	licy Details T −	Transmit Queue Count		Transmit Ring Size		<u>o</u>
표 Chasels	licy Details ⊤ 1	Transmit Queue Count		Transmit Ring Size		<u> </u>
Chassis Chass	Nicy Details T	Fransmit Queue Count		Transmit Ring Size 256		0
Chassis Chassis Chassis Chassis Profiles Profiles Profiles Chassis Ch	licy Details T 1 c 5	Fransmit Queue Count I Completion Completion Queue Count 5	0	Transmit Ring Size 256		<u>•</u>
<ul> <li>Chaseis</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Policies</li> <li>Administration</li> </ul>	licy Details T 1 C 5	Fransmit Queue Count I Completion Completion Queue Count 5		Tranamit Ring Size		•
Image: Chassis     Image: Chassis       Image: Chassis     Image: Chassi	Nicy Details T 1 c 5	Iransmit Queue Count I Completion Completion Queue Count 5 TCP Offload		Transmit Ring Size		<u> </u>
<ul> <li>Chassie</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Profiles</li> <li>Administration</li> <li>Devices</li> <li>Software Repository</li> </ul>	licy Details T 1 c 5 T	Iransmit Queue Count I Completion Completion Queue Count 5 TCP Offload TCP Offload		Transmit Ring Size 256		•
<ul> <li>Chassis</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Policies</li> <li>Administration ^</li> <li>Devices</li> <li>Software Repository</li> </ul>	licy Details T 1 C 5 T	Iransmit Queue Count I Completion Completion Queue Count 5 TCP Offload TCP Offload Tc Checksum Offload © Tc Checksum Offload ©		Transmit Ring Size 256		<u>.</u>
<ul> <li>Chaseis</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Politicise</li> <li>Administration</li> <li>Devices</li> <li>Software Repository</li> </ul>	Nicy Details T	Iransmit Queue Count I Completion Completion Queue Count 5 TCP Offload C Enable Tx Checksum Offload © C Enable Rx Checksum Offload ©		Transmit Ring Size		<u></u>
<ul> <li>Chassis</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Profiles</li> <li>Administration</li> <li>Devices</li> <li>Software Repository</li> </ul>	licy Details T 1 c 5	Iransmit Queue Count I Completion Completion Queue Count 5  (CP Offload  C Enable Tx Checksum Offload  Enable Rx Checksum Offload  Enable Large Send Offload		Transmit Ring Size		•
<ul> <li>Chassis</li> <li>HyperFlex Clusters</li> <li>Fabric Interconnects</li> <li>Profiles</li> <li>Administration ^</li> <li>Devices</li> <li>Software Repository</li> </ul>	Jicy Details T	Iransmit Queue Count I Completion Completion Queue Count 5 TCP Offload Enable Tx Checksum Offload  Enable Rx Checksum Offload  Enable Large Receive Offload  Enable Res  Enable Res Enable Res Enable Res Enable Res Enable Res Enable Large Receive Offload Enable Res Enabl		Transmit Ring Size		•

24. Create Ethernet Network Policy in Create Server Policy.

≡	الانتان cisco Intersight	Policies	
		HyperFlex Policies Server Poli Select Policy Type	×
		Q Search	^
	Chassis	Adapter Configuration	-
	HyperFlex Clusters	Name BIOS	-
		CDIP-EthAdapter	-
<u></u>		CDIP-DeviceConnect	
		CDIP-C220M5SN-Boot	
		CDIP-C220M5SN-BIOS	
	Devices	CDIP-AdapterConfig	
	Software Repository		
		Fibre Channel Adapter	
		Fibre Channel Network	-
		Cancel	

000	Dashboards			
88	Servers	General	Organization * CDIP-C220M5SN ✓	
-	Chassis			
60	HyperFlex Clusters	<ul> <li>Policy Details</li> </ul>	Name * CDIP-EthNetwork	
	Fabric Interconnects			
6	Profiles		Description	
8	Policies		Ehternet Network Policy	
Ō	Administration		Add Tag	
	Devices		COIP OCSC-C220-M5SN × ×	
	Software Repository			
		Cancel		Next

26. Select VLAN mode and Default VLAN. Click Create.

<u>00o</u>	Dashboards						
	Servers		General	VLAN Settings			
	Chassis			VLAN Mode	Default VLAN 14		
	HyperFlex Clusters		Policy Details		<u></u>		
<u> </u>	Fabric Interconnects						
6	Profiles						
Ē	Policies						
ę	Administration ^						
	Devices						
	Software Repository						
		(	Cancel			Previous	Create

27. Create Ethernet QoS Policy in Create Server Policy.

		HyperFlex Policies Server Pol	Select Policy Type ×	
			୍ଦ୍ Search	^
			Adapter Configuration	
	HyperFlex Clusters			
			○ Boot Order	
@]			Device Connector	
			O Disk Group	
			Fthernet Adapter	
			Ethernet Network	
	Software Repository			
			Eitre Channel Adapter	
			Fibre Channel Network	•
			Cancel Next	

28. Enter Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

Image: Dashboa       Image: D	ox Clusters terconnects tration ^ # Repository	General     Policy Details	Organization * CDIP-C220MSSN V Namo * CDIP-QOS Description QoS Policy for Ethernet Add Tag CDIP-UCSC-C220-MSSN × ×	
				Next

29. Select MTU 9000, Class of Service (CoS). Enable Trust Host CoS.

<u>000</u> C	Dashboards				
== s	Servers	• General	QoS Settings		
	Chassis		MTU, Bytes 9000	Rate Limit, Mbps	<u>•</u>
® ⊦	HyperFlex Clusters	Policy Details			
垔 F	Fabric Interconnects		Class of Service 5		
ិតៃ គ	Profiles				
Ē F	Policies		■ Enable Trust Host CoS ①		
<u>م</u> ۾	Administration ^				
	Devices				
s	Software Repository				
					Create

30. Create LAN Connectivity Policy in Create Server Policy.

Нур	erFlex Policies Server Policies		Select Policy Type	×
			O Disk Group	^
			C Ethernet Adapter	
			C Ethernet Network	
		IPMI Over LAN	C Ethernet QoS	
		Ethernet QoS	Fibre Channel Adapter	
		Ethernet Network	Fibre Channel Network	
		Ethernet Adapter	-	
		Adapter Configura		
				11
			() NTP	
			Network Connectivity	
			O SAN Connectivity	
			○ SD Card	
				*
			Cancel	

Conorol	Organization *	
General	CDIP-C220M5SN ×	
<ul> <li>Policy Details</li> </ul>	Name *	
	CDIP-LANConnect	
	Description	
	LAN Connection Policy for CDIP	
	Add Tag	
	CDIP UCSC-C220-M5SN × ×	
		Next

32. Add vNICs required and provide vNIC configuration details.

The following steps are for the Cisco VIC 1387. For more information, go to the Cisco Intersight section <u>Creating Network Policies</u>. For Cisco VIC 1400 series with four ports, the PCI order will be changed to 1 and 3 or 1,2,3 and 4 depends on how many ports are in use and whether port-channel mode is enabled/disabled.

• General	Add vNIC	
Policy Details	+ eth0 🖂	â ^ <del>`</del>
	+ eth1 🗵	<u> </u>

33. Provide input for eth0 as shown in the screenshot below for MLOM:

— eth0 (MLOM) 🗵	
Name * eth0 0	
Consistent Device Naming(CDN)	
Source vNIC Name v 0	
Placement	
Slot ID *	Uplink Port
MLOM ©	<u>0</u>
PCI Link	
0	
PCI Order	
<u>0</u>	
Ethernet Network *	
Select Policy	

34. Select the previously created Ethernet Network, Ethernet QoS, and Ethernet Adapter Policy.

General	Placement		Ethernet Network	
ochicita	Slot ID *	Uplink Port	Policies 1	
	MLOM	<u> </u>		
Policy Details				
	PCI Link		CDIP-EthNetwork	
	0	<u>)</u>		
	PCI Order			
	0	<u>)</u>		
	Ethernet Network *			
	Ethernet QoS *			
	Ethomat Adapter #			
	Connection			
	Disabled usNiC VM	1		
	+ eth1 🗵			

General	Placement			Ethernet QoS	×
General	Slot ID *		Uplink Port	Policies 1	Create New
	MLOM	٥	0		
Policy Details					200 - 20 - 21
	PCI Link			CDIP-QOS	Select ©
	0				
	PCI Order				
	0				
	Ethornet Network *				
	Selected Policy CDIP-EthNetwork (D)   X				
	Ethernet QoS *				
	Ethernet Adapter *				
	0				
	Connection				
	Disabled usNIC	VMQ			
	+ eth1 1				
				Ethernet Adanter	_ ~
• General	Placement				
	Slot ID *		Uplink Port	Policies 1	
	MLOM	©	0		
Policy Details					
	PCI Link			CDIP-EthAdapter	
	0				

	PCILink			CDIP-EthAdapter	
	0		<u> </u>		
	PCI Order				
	<u> </u>				
	Ethernet Network *				
	Selected Policy: CDIP-EthNetwork				
	Ethernet QoS *				
	Selected Policy: CDIP-QOS 💿   >				
	Ethernet Adapter *				
	Connection				
	Disabled	usNIC	VMQ		
	+ eth1 🗵				
Cancel				Previous	Create

35. Repeat steps 32-33 for eth1.

	Add vNIC	
General		
e Policy Details	+ eth0 (MLOM) ⊘	<u>n</u> ^ •
	— eth1 (MLOM) ⊘	ii <b>^ ~</b>
	Name *	
	eth1 ©	
	Consistent Device Naming(CDN)	
	Source	
	vNIC Name view view view view view view view vie	
	Placement	
	Slot ID *	Uplink Port
	PCI Link	
	<u>0                                    </u>	
	PCI Order	
	<u>1</u> ©	
	vNIC Name v ©	
• General		
Roliau Dataila	Placement	
	Slot ID * MLOM ©	Uplink Port 1 O
	PCI Link 0 0	
	PCI Order 1 00	
	Ethernet Network *	
	Ethernet QoS *	
	Ethernet Adapter *	
	Selected Policy: CDIP-EthAdapter 💿   ×	
	Connection	
	Disabled usNIC VMQ	

36. Select NTP in Create Server Policy.

HyperFlex Policies Server Policies		
		LAN Connectivity
		C Local User
	LAN Connectivity	• NTP
	IPMI Over LAN	Network Connectivity
		O SAN Connectivity
	Ethernet Network	○ SD Card
	Ethernet Adapter	○ SMTP
		○ SNMP
		⊖ ssн
		O Serial Over LAN
	Adapter Configurat	○ Storage
		⊖ Syslog
		Virtual KVM
		🔿 Virtual Media
		Cancel

	Organization *	
General	CDIP-C220M5SN	~
<ul> <li>Policy Details</li> </ul>	Name *	
	CDIP-NTP	
	Description	
	NTP Policy for CDIP setup	
	Add Tag	
	CDIP UCSC-C220-M5SN $\times$	×

38. Enable NTP server then Add NTP server.

• General	Enable NTP ①  NTP Server *
Policy Details	<u>©</u> +

39. Create Virtual KVM policy in Create Server Policy.

HyperFlex Policies Server Policies		Select Policy Type ×	
		C LAN Connectivity	<b>^</b>
		⊖ LDAP	
		🔿 Local User	
	LAN Connectivity	○ NTP	
	IPMI Over LAN	Network Connectivity	
		O SAN Connectivity	
	Ethernet Network	O SD Card	
	Ethernet Adapter	⊖ smtp	
		⊖ SNMP	
		<u>)</u> ssн	
		Serial Over LAN	
	Adapter Configurat	⊖ Storage	
		) Syslog	
		• Virtual KVM	
		🔿 Virtual Media	Ŧ
		Cancel	
General	Organization * CDIP-C220M5SN ✓		
------------------------------------	------------------------------------		
<ul> <li>Policy Details</li> </ul>	Name * CDIP-vKVM		
	Description Virtual KVM Policy		
	Add Tag CDIP UCSC-C220-M5SN × ×		

41. Configure the information related to the number of sessions and remote port.

🛉 General	Enable Virtual KVM 💿	
	Max Sessions *	
	4	<u>()</u>
Policy Details		
	Remote Port *	
	2068	0
	Enable Video Encryption 🛈	
	Enable Local Server Video 🛈	

42. Select Virtual Media in Create Server Policy.

HyperFlex Policies Server Policies		Select Policy Type ×
		C LAN Connectivity
		⊖ LDAP
	Virtual KVM	O Local User
		○ NTP
	LAN Connectivity	Network Connectivity
	IPMI Over LAN	SAN Connectivity
		O SD Card
	Ethernet Network	⊖ smtp
	Ethernet Adapter	○ SNMP
		O Serial Over LAN
		Cancel

43. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

General	Organization * <u>CDIP-C220M5SN</u> ✓
<ul> <li>Policy Details</li> </ul>	Name * CDIP-vMedia
	Description Virtual Media Policy
	Add Tag CDIP UCSC-C220-M5SN × ×

44. Enable Virtual Media, then enable either HDD or CDD Virtual Media. Select NFS/CIFS/HTTP/HTTPS. Enter input to access ISO image to install OS from.

<ul> <li>General</li> <li>Policy Details</li> </ul>	Enable Virtual Media ©     Enable Virtual Media Encryption ©     Enable Low Power USB ©	
	+ HDD Virtual Media	🔵 Enable
	— CDD Virtual Media	C Enable
	NFS CIFS HTTP HTTPS	
	Volume * Hostname/IP Address *	
	Remote Path * Remote File * /public/RHELISO/ <sup>©</sup> rhel-server-7.6-x86_64-dvd.iso	0
	Mount Options O	
	Previous	Create

45. Repeat steps 32-33 for eth1.

• General	Add vNIC	
Policy Details	+ eth0 (MLOM) ⊘	iii ^ ▼
	— eth1 (MLOM) ⊘	ii • •
	Name* eth1	
	Consistent Device Naming(CDN) Source	
	vNIC Name vo	
	Placement Slot ID *	Uplink Port
	MLOM O	<u>•</u>
	PCI Link 0	
	PCI Order 1 ©	
• General	vNIC Name v 0	
	Placement	
Policy Details	Slot ID * MLOM ©	Uplink Port 1
	PCI Link 0	
	PCI Order 1 ©	
	Ethernet Mehwork +	
	Selected Policy: CDIP-EthNetwork ③   ×	
	Ethernet QoS *	
	Ethernet Adapter *	
	Connection	
	Disabled usNIC VMQ	
		Direutour
Cancer		Previous

46. Select NTP in Create Server Policy.

HyperFlex Policies Server Policies		
		C LAN Connectivity
		O Local User
	LAN Connectivity	• NTP
	IPMI Over LAN	Network Connectivity
		SAN Connectivity
	Ethernet Network	O SD Card
	Ethernet Adapter	○ SMTP
		○ SNMP
		_ с ssн
		O Serial Over LAN
	Adapter Configurat	◯ Storage
		⊖ Syslog
		O Virtual KVM
		🔿 Virtual Media
		Cappel

47. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

	Organization *	
General	CDIP-C220M5SN	~
<ul> <li>Policy Details</li> </ul>	Name *	
	CDIP-NTP	
	Description	
	NTP Policy for CDIP setup	
	Add Tag	
	CDIP UCSC-C220-M5SN $\times$	×

48. Enable NTP server then Add NTP server.

• General	Enable NTP ①  NTP Server *
Policy Details	<u>©</u> +

49. Create Virtual KVM policy in Create Server Policy.

HyperFlex Policies Server Policies		Select Policy Type	×
		C LAN Connectivity	<b>^</b>
		O LDAP	
		🔿 Local User	
	LAN Connectivity	⊖ NTP	
	IPMI Over LAN	O Network Connectivity	
		SAN Connectivity	
	Ethernet Network	○ SD Card	
	Ethernet Adapter	⊖ smtp	
		⊖ SNMP	
		⊖ ssh	
		Serial Over LAN	
	Adapter Configural	○ Storage	
		⊖ Syslog	
		Virtual KVM	
		🔿 Virtual Media	-
		Cancel	xt

50. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

General	Organization * CDIP-C220M5SN ✓
<ul> <li>Policy Details</li> </ul>	Name * CDIP-vKVM
	Description Virtual KVM Policy
	Add Tag CDIP UCSC-C220-M5SN × ×

51. Configure the information related to the number of sessions and remote port.

🛉 General	Enable Virtual KVM 💿	
	Max Sessions *	
	4	<u>()</u>
Policy Details		
	Remote Port *	
	2068	0
	Enable Video Encryption 🛈	
	Enable Local Server Video 🛈	

52. Select Virtual Media in Create Server Policy.

HyperFlex Policies Server Policies		Select Policy Type ×
		LAN Connectivity
		○ LDAP
	Virtual KVM	O Local User
		○ NTP
	LAN Connectivity	Network Connectivity
	IPMI Over LAN	O SAN Connectivity
		○ SD Card
	Ethernet Network	⊖ SMTP
	Ethernet Adapter	○ SNMP
		<u>)</u> ssн
		Serial Over LAN
		⊖ Storage
		Cancel

53. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

General	Organization * <u>CDIP-C220M5SN ~</u>
<ul> <li>Policy Details</li> </ul>	Name * CDIP-vMedia
	Description Virtual Media Policy
	Add Tag CDIP UCSC-C220-M5SN × ×

54. Enable Virtual Media, then enable either HDD or CDD Virtual Media. Select NFS/CIFS/HTTP/HTTPS. Enter input to access ISO image to install OS from.

<ul> <li>General</li> <li>Policy Details</li> </ul>	Enable Virtual Media      Enable Virtual Media Encryption      Enable Low Power USB	
	+ HDD Virtual Media	Enable
	— CDD Virtual Media	C Enable
	NFS CIFS HTTP HTTPS	
	Volume * Hostname/IP Address *	
	Remote Path * Remote File *	
	Mount Options ©	
Cancel	Previous	Create

6

55. Select Storage policy in Create Server Policy

The Storage Policy is applied to Name nodes with HDD and UCSC-RAID-M5 storage controller. Cisco UCS C220 M5SN for Data Lake with NVMe disks were in JBOD.

HyperFlex Policies Server Policies		
		LAN Connectivity
		O Local User
	Virtual Media	○ NTP
	Virtual KVM	O Network Connectivity
		O SAN Connectivity
	LAN Connectivity	O SD Card
	IPMI Over LAN	О ѕмтр
		⊖ SNMP
	Ethernet Network	<u>О</u> ssн
	Ethernet Adapter	○ Serial Over LAN
		• Storage
		⊖ Syslog
		O Virtual KVM
		O Virtual Media
		Cancel

56. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

CDIP-C220M5SN	<u> </u>
Name *	
CDIP-DNStoragePolicy	
Description	
Storage Policy for Data Nodes	
Add Tag	
CDIP UCSC-C220-M5SN ×	×
	Name * CDIP-DNStoragePolicy Description Storage Policy for Data Nodes Add Tag CDIP UCSC-C220-M5SN ×

57. Configure the policy details required for Storage Policy.

• General	You must have an existing Disk Group Policy before you create a Storage Policy									
	Drive Configuration									
Policy Details	+ Global Hot Spares Enable									
	Unused Disks State ©									
	If the encryption is enabled in JBOD disks, the encryption will be disabled before they are moved to Unconfigured Good state									
	Retain Virtual Drives									
	▲ If you do not enable Retain Virte loss	ual Drives, all existing virtual dri	ves will be removed from the se	erver, and all configuration will t	be cleared. This may result in da	ata				
	Add Virtual Drives									
	Virtual Drive Name	Size (MB)	Disk Group	Expand to Available	Set as Boot Drive					
	NameNode-R1		CDIP-NN-DG	true						

58. Create Disk Group policy for Name Nodes.

I New features have recently been added! Learn More		Select Policy Type	×
HyperFlex Policies Server Policies		Q, Search	<b>^</b>
		Adapter Configuration	
		O BIOS	
	Virtual Media	O Boot Order	
		O Device Connector	
		Disk Group	
	LAN Connectivity	Ethernet Adapter	
	IPMI Over LAN	C Ethernet Network	
		C Ethernet QOS	
	Ethernet Network		
	Ethernet Adapter	Fibre Channel OoS	
		O IPMI Over LAN	
		C LAN Connectivity	
	BIOS	🔿 LDAP	
		Cancel	Next

59. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

● General	Organization * CDIP-C220M5SN  V
<ul> <li>Policy Details</li> </ul>	Name * CDIP-NN-DG
	Description Disk Group Policy for Name Node
	Add Tag CDIP UCSC-C220-M5SN × ×

## **Server Profile Creation**

To create the Server Profile for Name Node and Data Node with their corresponding policies configured in the Create Server Policies section, follow these steps:

- 1. Select the Profiles tab and click Create Server Profile.
- 2. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

≡	رابیان Intersight	Create Server Profile	
<u>00o</u>			
			Organization *
		General	CDIP-C220M5SN ×
000			
		Conver Configuration	Server Profile Name *
69 69		Server Configuration	CDIP-C220N-SP
Ģ			Description
-0-		<ul> <li>Server Assignment</li> </ul>	Cisco UCS C220 M5SN server profile CDIP Setup
6			
			Add Tag
í		Summary	CDIP UCSC-C220-M5SN × ×
িজ			
ц.			

3. Assign the Compute, Network, Storage and Management policies created on the Server Configuration tab.

≡	cisco Intersight	Create Server Profile		¢   B	<i>§</i> :}	Q,
						-
		General	Show Attached Policies (6)			
×.			Remains Lot J Deliving Conference			
		Server Configuration	Compare 4 of 4 Policies Computed			
		<ul> <li>Server Assignment</li> </ul>	V BIOS	CDIP-C220M5SN-BIOS		
			🗸 Boot Order	CDIP-C220M5SN-Boot	8	
		Summary	V NTP	CDIP-NTP	1	
ē			Virtual Media	CDIP-vMedia		
			Network 2 of 3 Policies Configured			~
			Storage () of 2 Policies Configured			~
			Management 0 of 11 Policies Configured			~

≡	cisco Intersight	Create Server Profile	۵	ß	¢1	9,
		General     Show Attached Policies (6)				
		Server Configuration     Compute 4 of 4 Policies Configured				~
		Network 2 of 3 Policies Configured				^
6		Server Assignment     Adapter Configuration	CDIP-Adapte	erConfig		
		Summary     LAN Connectivity	CDIP-LAN	Connect	1	
¢		SAN Connectivity				
		Storage 0 of 2 Policies Configured				~
		Management 0 of 11 Policies Configured				~
ļ	General	Show Attached Policies (9)				
	Server Configuration	Compute 4 of 5 Policies Configured				
•	Server Assignment	Network 2 of 3 Policies Configured				
		Storage 0 of 2 Policies Configured				
·	Summary	Management 3 of 11 Policies Configured				
		V Device Connector	CDIP-DeviceCo	nnect		
		SSH	CDIF	P-SSH		
		Virtual KVM	CDIP-	vKVM	1	

4. Select Assign Server.

	General   Assign Server Assign Server Later  Server Configuration											
		Q Search				19 items found   10 ∨ per page K < 1 of 2 >>> >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>						
	Server Assignment		Name ‡	User Label 🗘	Health 🌐	Model 🌐	Serial Number 🗘	Management IP 👙				
	Summary		C220-WZP23361125		Healthy	UCSC-C220-M5SN	WZP23361125	10.14.1.216				
•			C220-WZP2336112W		Healthy	UCSC-C220-M5SN	WZP2336112W	10.14.1.215				
			C220-WZP23420UL3		Healthy	UCSC-C220-M5SN	WZP23420UL3	10.14.1.213				
		0	C220-WZP2336112D		Healthy	UCSC-C220-M5SN	WZP2336112D	10.14.1.214				

5. Click Next to view the summary configuration. Click Deploy.

≡	cisco Intersight	Create Server Profile					Ŷ	C ¢‡	Q,	0
<u>00o</u>										
=		• General	General							
55			Server Profile Name	CDIP-C220N-SP	Assigned Server		Management IP	10.14.1.216		
÷		<ul> <li>Server Configuration</li> </ul>	Server Profile Status Organization	Not Deployed CDIP-C220M5SN	Management Platform	IMC				
272		0								
6		<ul> <li>Server Assignment</li> </ul>	Configuration Error	s (0)						
E		Summary	Adapter Configuration					CDIP-AdapterConfig		
			BIOS					CDIP-C220M5SN-BIOS		
-			Boot Order					CDIP-C220M5SN-Boot		
			Device Connector					CDIP-DeviceConnect		
			LAN Connectivity					CDIP-LANConnect		
			NTP					CDIP-NTP		
			SSH					CDIP-SSH		
			Virtual KVM					CDIP-vKVM		
			Virtual Media					CDIP-vMedia		
								s Depic	У	

6. Create Server Profile clone for multiple servers..

cisco Intersight	Profiles						dik Patel 요
HyperFlex Cluster Profile	s Server Profiles					Create Ser	ver Profile
	Q_Search			1 items found	I <u>16 ∨</u> per page ⊨ <		⊴   ©
			Server Health				: Ø
		Nat Assigned			a few seconds ago		
							Edit
							Clone

7. Select the Profiles tab and click Create Server Profile.

Summary

0	. Linter the Organ	lization, Name, Description and	i create a new tay of assign an existing tay. Click ne
≡	رابیان Intersight	Create Server Profile	
<u>00o</u>			
		Constal	Organization *
		General	CDIP-C220M5SN Y
000			Server Profile Name *
99 9		Server Configuration	CDIP-C220N-SP
			Description
		<ul> <li>Server Assignment</li> </ul>	Cisco UCS C220 M5SN server profile CDIP Setup
6			
			Add Tag

8. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

9. Assign the Compute, Network, Storage and Management policies created on the Server Configuration tab.

CDIP UCSC-C220-M5SN ×

≡	alada cisco Intersight	Create Server P	Profile		0 R 4	Q,	
			General Server Configuration Server Assignment Summary	Show Attached Policies (6)   Compute 4 of 4 Policies Configured <ul> <li>BIOS</li> <li>Boot Order</li> <li>NTP</li> <li>Virtual Media</li> </ul> Network: 2 of 3 Policies Configured   Storage 0 of 2 Policies Configured   Storage 0 of 2 Policies Configured	CDIP-C220M5SN-BIOS		
≡	cisco Intersight	Create S	Server Profile			¢ []	€1 0°
0 F & # # # #			General     Server Configuration     Server Assignment     Summary	<ul> <li>Show Attached Policies (6)</li> <li>Compute 4 of 4 Policies Configured</li> <li>Network 2 of 3 Policies Configured</li> <li>Adapter Configuration</li> <li>LAN Connectivity</li> <li>SAN Connectivity</li> <li>Storage 0 of 2 Policies Configured</li> <li>Management 0 of 11 Policies Configured</li> </ul>		CDIP-AdapterCon CDIP-LANConne	*           fig           tet           iii           *           *
I	General		Show Attached	Policies (9)			
¢	Server Configura	tion	Compute 4 of 5 Polic	ies Configured			Ý
	Server Assignme	nt	Network 2 of 3 Polici	es Configured			~
			Storage 0 of 2 Policie	es Configured			~
ė	Summary		Management 3 of 11	Policies Configured			^
			<ul> <li>✓ Device Con</li> <li>✓ SSH</li> <li>✓ Virtual KVM</li> </ul>	nector A	C	DIP-DeviceConnec CDIP-SS CDIP-vKVI	н () м ()

10. Select Assign Server.

General     Server Configuration	•	Assign Server O Assi Show Assigned	gn Server Later						
	٩,	Search			19 items found   10 v per page 🔣 < of 2 🔈 🕅 🤅				
Server Assignment		Name 🌐	User Label 🗘	Health 🗘	Model 🗘	Serial Number 🗘	Management IP 👙		
		C220-WZP23361125		Healthy	UCSC-C220-M5SN	WZP23361125	10.14.1.216		
<ul> <li>Summary</li> </ul>		C220-WZP2336112W		Healthy	UCSC-C220-M5SN	WZP2336112W	10.14.1.215		
		C220-WZP23420UL3		Healthy	UCSC-C220-M5SN	WZP23420UL3	10.14.1.213		
		C220-WZP2336112D		Healthy	UCSC-C220-M5SN	WZP2336112D	10.14.1.214		

11. Click Next to view the summary configuration. Click Deploy.

≡	cisco Intersight	Create Server Profile					¢	⊡ ¢ł	Q,	Θ
4 @ E II E		General     Server Configuration	General Server Profile Name Server Profile Status Organization	CDIP-C22DN-SP Not Deployed CDIP-C220M5SN	Assigned Server Management Platform	C220 W2P23361125	Management IP	10.14.1.216		
		<ul> <li>Server Assignment</li> </ul>	Configuration Errors							
		Summary	Adapter Configuration					CDIP-AdapterConfig	1	
ē			BIOS					CDIP-C220M5SN-BIO		
			Boot Order					CDIP-C220M5SN-Boo		
			Device Connector					CDIP-DeviceConnec		
			LAN Connectivity					CDIP-LANConnec		
			NTP					CDIP-NT		
			SSH					CDIP-SSI	1	
			Virtual KVM					CDIP-vKVN		
			Virtual Media					CDIP-vMedi		
								: Depl	ey 👘	

12. Create Server Profile clone for multiple servers.

≡	cisco Intersight Pro	files		ç	2   B	ମ   ୦,   ୦୦	③ Han	ik Patel 요
<u>01</u> e		Server Profiles					Create Ser	er Profile
8								
		Search			nt 1 items found	I <u>16 ∨</u> per page IC ⊂		
灥				Server Health				
			Not Assigned			a few seconds ago		
6	··· / 📋 🧷 🕬	ected 1 of 1 Unseld						
E								Clone
ø								

## **Install Red Hat Enterprise Linux 7.7**

This section provides detailed procedures for installing Red Hat Enterprise Linux Server using associated server profile on Cisco UCS C220 M5 servers. There are multiple ways to install the RHEL operating system. The instal-

lation procedure described in this deployment guide uses KVM console and virtual media from Cisco Intersight Server profile.



In this study, RHEL version 7.7 DVD/ISO was utilized for OS the installation on Cisco UCS C220 M5 Rack Servers.

To install the Red Hat Enterprise Linux 7.7 operating system, follow these steps:



We configured Tunneled vKVM and Launched Tunneled vKVM from Cisco Intersight.

2. Log into UCS KVM Direct with CIMC credential. Click Launch KVM.



## The KVM window will appear.

$\leftrightarrow$ $\rightarrow$ C <b>a</b> intersight.com/kvm/mux-0/ui/?sessionid=tlqCVRbuY1&mux=m	ux-0		☆ 😬 :
File View Macros Tools Power Virtual Media Help		A 1	s aludo UCS KVM
	No Signal		
3. Verify that Virtual Device is already mapp	ed in Virtual Media tab as per the Virtual	Media	Policy.
Policies   Intersight	disco UCS KVM Direct	×	+
$\leftrightarrow$ $\rightarrow$ C $rac{}$ intersight.com/kw	/m/mux-0/ui/?sessionid=2NHU0x	ogTE8	&mux=mux-0
File View Macros Tools Power	Virtual Media Help		
	Create Image		
Cisco Sy	Deactivate Virtual Devices		
Conf igur	rhel-server-7.7-x86_64-dvd.iso Ma	pped t	to CD/DVD
Conf igur	Map Removable Disk		
	Map Floppy Disk		

4. Select the Installation option from Red Hat Enterprise Linux 7.7.

intersight.com/kvm/mux-0/ui/?sessionid=2NHU0xogTE&mux=mux-0

Macros Tools Power Virtual Media Help



5. Select the language for the installation and click Continue.

	ntersight.com/	kvm/mux-1/ui/	?sessionid	=tAZ7rEzWNA&mux=mu	x-1			07	Å	0
acros	Tools Power	Virtual Media	Help				A I S	cisco.	UC	S KVM
						RED HAT ENTERPRISE LINUX 7.7	INSTALLATION			
		Rec	Hat			🕎 us	Help!			
				WELCOME TO RE	D HAT ENTERPRISE	LINUX 7.7.				
				What language would yo	u like to use during the insta	lation process?				
				English	English >	English (United States)				
				Afrikaans	Afrikaans	English (United Kingdom)				
				አማርኛ	Amharic	English (India)				
				العربية	Arabic	English (Australia)				
				অসমীয়া	Assamese	English (Canada)				
				Asturianu	Asturian	English (Denmark)				
				Беларуская	Belarusian	English (Ireland)				
				Български	Bulgarian	English (Nigeria)				
				বাংলা	Bengali	English (Hong Kong SAR China)				
				Bosanski	Bosnian	English (Philippines)				
				Català	Catalan	English (Singapore)				
				Čeština	Czech	English (South Africa)				
				Cymraeg	Welsh	English (Zambia)				
				Dansk	Danish	English (Zimbabwe)				
				Deutsch	German	English (Botswana)				
				beatsen	Gernan	English (Antiqua & Barbuda)				
				L	Ð					

6. Select the date and time, which pops up another window. Select the location on the map, set the time, and click Done.



7. Click Installation Destination.

Bed Hat	INSTALLATION S	UMMARY	REI	D HAT ENTERPRISE LINUX	7.7 INSTALLATION
Red nat			<b>#</b>	us	Help!
	LOCALIZA	TION			
	Θ	DATE & TIME Americas/Los Angeles timezone		KEYBOARD English (US)	
	á	LANGUAGE SUPPORT English (United States)			
	SOFTWAR	E			
	0	INSTALLATION SOURCE	4	SOFTWARE SELECTION	
	SYSTEM				
		INSTALLATION DESTINATION	Q	KDUMP Kdump is enabled	
	÷	NETV No disks selected ME Not connected		SECURITY POLICY No profile selected	
				Quit	Begin Installation
			V	Ve won't touch your disks until yo	u click 'Begin Installation'.
	A Please complete it				

8. This opens a new window with the boot disks. Select a device and choose "I will configure partitioning". Click Done. We selected two M.2 SATA SSDs.



- 9. This opens a window to create the partitions. Click the + sign to add a new partition as shown below with a boot partition size 2048 MB.
- 10. Click Add Mount Point to add the partition.

MANUAL PARTITIONING			RED HAT ENTERPRISE LINUX 7.7 INS	TALLATION
Done			🖽 us	Helpl
New Red Hat Enterprise Linux 7.7 Installation You haven't created any mount points for your Red Hat for 7.7 Installation yet. You can: <u>Click here to create them automatically</u> Create new mount points by clicking the '+' button. New mount points will use the following partitioning sch LVM	Enterprise Linux neme:			
AI	DD A NEW MOU	INT POINT		
	More customiza after creating th	tion options are available e mount point below.		
M	ount Point: /	boot 👻	nts for your Red Hat Enterprise Linux 7.7 ins etails here.	stallation,
De	esired Capacity: 2	048mb		
	Ca	Add mount point		
		R		
+ - C				
AVAILABLE SPACE 447.14 GIB TOTAL SPACE 447.14 GIB				
2 storage devices selected				Reset All

11. Change the device type to RAID and make sure the RAID level is RAID1 (redundancy) and click Update Settings to save the changes.

MANUAL PARTITIONING			RED HAT E	ENTERPRISE LINUX 7.7 I	NSTALLATION Helpi
▼ New Red Hat Enterprise Linux 7.7 Installation	n	sdal			
SYSTEM		Mount Point:		Device(s):	
sdal	1953 MiB >	/boot			
		Desired Capacity:		ATA Micron_5100_MTFD	(sda) and 1
		1953 MiB		other	
				Modify	
		Device Type:		RAID Level:	
		RAID 👻	Encrypt	RAID1 (Redundancy)	-
		File System:		-	
		xfs 🔹 Refo	rmat		
		Label:		Name:	
				boot	
				Upd	ate Settings
+ - C			Note: Ti be appl	he settings you make on this ied until you click on the main Inst	screen will not n menu's 'Begin allation' button.
AVAILABLE SPACETOTAL SPACE445.23 GiB447.14 GiB					
2 storage devices selected					Reset All

12. Click the + sign to create the swap partition of size 2048 MB. Click Add Mount Point.

MANUAL PARTITIONING		RED HAT	ENTERPRISE LINUX 7.7 INS	Help!
New Red Hat Enterprise Linux 7.7 Installation     SYSTEM     /boot     1953 MiB     boot	> Mount Point: /boot Desired Capacity: 1953 MIB		Device(s): ATA Micron_5100_MTFD (sd other	a) and 1
ADD A NEW More cust after creat Mount Point: Desired Capacit	MOUNT POINT omization options are available ing the mount point below. swap ty: 2048mb I	) Encrypt at	Modify RAID Level: RAID1 (Redundancy)	×
+ - C AVAILABLE SPACE TOTAL SPACE	Cancel Add mount point	Note: 1 be app	Name: Update Update The settings you make on this scr bied until you click on the main m Installa	Settings een will not enu's 'Begin tion' button.
443.33 GiB 447.14 GiB				Reset All

13. Change the Device type to RAID and RAID level to RAID1 (Redundancy) and click Update Settings.

MANUAL PARTITIONING		RED HAT	ENTERPRISE LINUX 7.7 INS	TALLATION Help!
<ul> <li>New Red Hat Enterprise Linux 7.7 Installation</li> <li>SYSTEM</li> <li>/boot</li> <li>boot</li> </ul>	1953 MiB	rhel-swap Mount Point:	Device(s):	
swap rhel-swap	1952 MiB >	Desired Capacity: 1952 MiB	ATA Micron_5100_MTFD (sda other Modify	a) and 1
		Device Type: RAID   Encrypt  File System:  swap  Reformat	RAID Level: RAID1 (Redundancy)	•
		Label:	Name: swap	
+ - C AVAILABLE SPACE 441.41 GIB 447.14 GIB		Note: 1 be app	Update The settings you make on this scro lied until you click on the main me Installat	Settings een will not enu's 'Begin ion' button.
2 storage devices selected				Reset All

14. Click + to add the / partition. The size can be left empty so it will use the remaining capacity. Click Add Mountpoint.

MANUAL PARTITIONING			RED HAT	ENTERPRISE LINUX 7.7 INSTALLAT	
▼ New Red Hat Enterprise Linux 7.7 In	nstallation	swap	in the second se		
SYSTEM /boot boot	1953 MiB	Mount Point:		Device(s):	
swap swap	1952 MiB 义	Desired Capacity: 1952 MiB		ATA Micron_5100_MTFD (sda) and 1 other	
	ADD A NEW MOU	JNT POINT		Modify	
	More customiza after creating th Mount Point:	ation options are available ne mount point below.	) Encrypt	RAID Level: RAID1 (Redundancy)	
	Desired Capacity:		at		
	C	ancel Add mount point		Name:	
				swap	
+ - C			Note: 1 be app	Update Settings The settings you make on this screen will n lied until you click on the main menu's 'Beg	ot
AVAILABLE SPACE TOTAL SPACE 439.51 GIB 447.14 GIB				Installation' butto	n.
2 storage devices selected				Reset	All

15. Change the Device type to RAID and RAID level to RAID1 (Redundancy). Click Update Settings.

MANUAL PARTITIONING		RED HA	NT ENTERPRISE LINUX 7.7 INSTALLATION
New Red Hat Enterprise Linux 7.7 In SYSTEM /boot boot	stallation 1953 MiB	root Mount Point:	Device(s):
/ root	219.63 GiB >	Desired Capacity:	ATA Micron_5100_MTFD (sda) and 1 other
SWap swap	1952 MiB	Device Type: RAID  Encryp File System: xfs  Reformat Label: Note be a	Modify RAID Level: RAID1 (Redundancy)  Name: Toot Upigte Settings  set The settings you make on this screen will not applied until you click on the main menu's 'Begin Installation' button.
2 storage devices selected			Reset All

16. Click Done.

New Red Ha SYSTEM /boot	at Enterp	rise Linux 7.7	Installation	1953 MiB	root Mount Point:		Device(s):	
boot	_				1			
root	SUMMA	ARY OF CHANGE	s					TFD (sda) and 1
swap	Your cu	stomizations will	result in the follo	wing changes t	aking effect after you	return to the main men	nu and begin installatior	n:
swap	Order	Action	Туре	Devi	ce Name	Mount point		
	1	Destroy Format	swap	cimc7	.cdip.cisco.local:swap			
	2	Destroy Device	mdarray	cimc7	.cdip.cisco.local:swap			
	3	Destroy Format	software RAID	sdb2				
	4	Destroy Format	software RAID	sda2				
	5	Destroy Format	xfs	cimc7	.cdip.cisco.local:root			
	6	Destroy Device	mdarray	cimc7	.cdip.cisco.local:root			
	7	Destroy Format	software RAID	sdb3				
	8	Destroy Device	partition	sdb3				
	9	Destroy Device	partition	sdb2				
	10	Destroy Format	software RAID	sda3				
	11	Destroy Device	partition	sda3				
	12	Destroy Device	partition	sda2				
					Cancel & Return to	Custom Partitioning	Accept Changes	
	_	_	_					Update Setting
						Note:	The settings you make	on this screen will
+ -	C					be app	olied until you click on t	he main menu's 'Be
		_						Installation' but
	TOTAL S	PACE						

17. Click Accept changes and continue the Installation.

18. Click Software Selection.

<mark>ط</mark> Red Hat	INSTALLATION S	UMMARY	RE	D HAT ENTERPRISE LINUX	7.7 INSTALLATION Help!
	LOCALIZA	TION			
	Θ	DATE & TIME Americas/Los Angeles timezone	Ē	<b>KEYBOARD</b> English (US)	
	á	LANGUAGE SUPPORT English (United States)			
	SOFTWAR	E			
	0	INSTALLATION SOURCE		SOFTWARE SELECTION Minimal Install	<b>b</b>
	SYSTEM			Minimal Install	
	9	INSTALLATION DESTINATION No disks selected	Q	KDUMP Kdump is enabled	
	¢ →	NETWORK & HOST NAME Not connected		SECURITY POLICY No profile selected	
				Quit	Begin Installation
			V	Ve won't touch your disks until yo	ou click 'Begin Installation'.
	A Please complete i	tems marked with this icon before continuing	to the next step.		

- 19. Select Infrastructure Server and select the Add-Ons as noted below, then click Done:
  - Network File System Client
  - Performance Tools
  - Compatibility Libraries
  - Development Tools
  - Security Tools

	RED HAT ENTERPRISE LINUX 7.7 INSTALLATION
Base Environment  Minimal Install Basic functionality.  Infrastructure Server Server for operating network infrastructure services.  File, print, and storage server for enterprises. Basic Web Server Server for serving static and dynamic internet content. Virtualization Host Minimal virtualization host. Server with GUI Server for operating network infrastructure services, with a GUI.	Add-Ons for Selected Environment          Java support for the Red Hat Enterprise Linux Server and Desktop Platforms.         Large Systems Performance         Performance support tools for large systems.         Load Balancer         Load Balancing support for network traffic.         MariaDB Database Server         The MariaDB SQL database server, and associated packages.         Network File System Client         Enables the system to attach to network storage.         Performance Tools         Tools for diagnosing system and application-level performance problems.         PostgreSQL Database Server         The PostgreSQL SQL database server, and associated packages.         Print Server         Allows the system to act as a print server.         Remote Management for Linux         Remote management interface for Red Hat Enterprise Linux, including
	<ul> <li>OpenLovi and Store.</li> <li>Virtualization Hypervisor Smallest possible virtualization host installation.</li> <li>Compatibility Libraries Compatibility Libraries for applications built on previous versions of Red Hat Enterprise Linux.</li> <li>Development Tools A basic development environment.</li> <li>Security Tools Security tools for integrity and trust verification.</li> <li>Smart Card Support Support for using smart card authentication.</li> <li>System Administration Tools Utilities useful in system administration.</li> </ul>

20. Click Network and Hostname and configure Hostname and Networking for the Host.



21. Type in the hostname as shown below.

NETWORK & HOST NAME	RED HAT ENTERPRISE LINUX 7.7 INSTALLATION
Ethernet (eno1, unplugged)         Intel Corporation Ethernet Controller 10G X550T         Intel Corporation Ethernet NIC (VIC 1387 MLOM Ethernet NIC)         Ethernet (eno6)         Cisco Systems Inc VIC Ethernet NIC (VIC 1387 MLOM Ethernet NIC)	Ethernet (eno1)         Unavailable    Hardware Address 5C:71:0D:49:50:26
+     -     Set as current syste       Host name:     rhel07.cdip.cisco.local     Apply	Configure Current host name: localhost

## The network configuration is configured at a later time after the installation.

- 22. Click Save, update the hostname, and turn Ethernet ON. Click Done to return to the main menu.
- 23. Click Begin Installation in the main menu.

么

- 24. Select Root Password in the User Settings.
- 25. Enter the Root Password and click Done.

		RED HAT ENTERPR	ISE LINUX 7.7 INSTALLATION
The root account is used f	for administering the system. Enter a par	ssword for the root user.	
Root Password:	•••••		
		Strong	
Confirm:	•••••		

26. Once the installation is complete, reboot the system.

<mark>-</mark> Red Hat	CONFIGURATION	RED HAT ENTERPRISE LINUX 7.7 INSTALLATION
	USER SETTINGS	
	ROOT PASSWORD Root password is set	USER CREATION No user will be created
	Complete!	
	Red Hat E	nterprise Linux is now successfully installed and ready for you to use! Go ahead and reboot to start using it!
		REDOUL
	A Use of this product is subject to the license agreement found at /use	/share/redhat-release/EULA

27. Repeat steps 1 to 26 to install Red Hat Enterprise Linux 7.7 on Servers 2 through 30.

The OS installation and configuration of the nodes that is mentioned above can be automated through PXE boot or third-party tools.
See the Appendix, section **Error! Reference source not found.** for Installation steps for Cisco Boot Optimized M.2 RAID Controller.

The hostnames and their corresponding IP addresses are shown in Table 8.

Table 8 Hostname and IP addr	ess
Hostname	Bond0
rhelnn01	10.14.1.45
rhelnn02	10.14.1.46
rhelnn03	10.14.1.47
rhel01	10.14.1.51
rhel02	10.14.1.52
rhel03	10.14.1.53
rhel04	10.14.1.54
rhel05	10.14.1.55
Rhel15	10.14.1.65
Rhel16	10.14.1.66

Multi-homing configuration is not recommended in this design, so assign only one network interface on each host.



For simplicity, outbound NATing is configured for internet access when desired, such as accessing public repos and/or accessing Red Hat Content Delivery Network. However, configuring outbound NAT is beyond the scope of this document.

Table 9	Hostname	and IP	address
	nostname	and n	auur 033

Hostname	Bond0
rhelnn01	10.14.1.45
rhelnn02	10.14.1.46
rhelnn03	10.14.1.47
rhel01	10.14.1.51

Hostname	Bond0
rhel02	10.14.1.52
rhel03	10.14.1.53
rhel04	10.14.1.54
rhel05	10.14.1.55
Rhel15	10.14.1.65
Rhel16	10.14.1.66

Multi-homing configuration is not recommended in this design, so assign only one network interface on each host.



For simplicity, outbound NATing is configured for internet access when desired, such as accessing public repos and/or accessing Red Hat Content Delivery Network. However, configuring outbound NAT is beyond the scope of this document.

# **Post OS Install Configuration**

Choose one of the nodes of the cluster or a separate node as the Admin Node for management, such as CDP PvC Base installation, Ansible, creating a local Red Hat repo, and others. In this document, we used rhelnn01 for this purpose.

# **Configure Network and Bond Interfaces**

To configure the network and bond interfaces, follow these steps:



The following section captures configuration details for active-standby network bond configuration. See the <u>Appendix</u> to configure active-active (balance-alb/mod 6 or 802.3ad/mod 4).

# Based on RHEL the bond mod configuration requires a corresponding configuration on the Cisco Nexus switch.

- 1. Setup /etc/sysconfig/ifcfg-bond0. Configure the two VNIC interfaces as slave interfaces to the bond interface.
- 2. Run the following to configure bond on for each Name Node and Data Node:

```
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-bond0
DEVICE=bond0
```

NAME=bond0 TYPE=Bond BONDING MASTER=yes IPADDR=10.14.1.45 NETMASK=255.255.255.0 ONBOOT=yes HOTPLUG=no BOOTPROTO=none USERCTL=no BONDING OPTS="miimon=100 mode=1 primary=eno5 primary reselect=0" NM CONTROLLED=no MTU="9000" [root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno5 TYPE=Ethernet BOOTPROTO=none NAME=bond0-slave1 DEVICE=eno5 ONBOOT=no MASTER=bond0 SLAVE=ves NM CONTROLLED=no HOTPLUG=no USERCTL=no MTU="9000" [root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno6 TYPE=Ethernet BOOTPROTO=none NAME=bond0-slave6 DEVICE=eno6 ONBOOT=no MASTER=bond0 SLAVE=yes NM CONTROLLED=no HOTPLUG=no USERCTL=no MTU="9000" [root@rhelnn01 ~]# ip addr 1: lo: <LOOPBACK, UP, LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default glen 1000 link/loopback 00:00:00:00:00 brd 00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid lft forever preferred lft forever 2: eno5: <BROADCAST, MULTICAST, SLAVE, UP, LOWER UP> mtu 9000 qdisc mq master bond0 state UP group default qlen 1000 link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff 3: eno6: <BROADCAST,MULTICAST,SLAVE,UP,LOWER UP> mtu 9000 qdisc mq master bond0 state UP group default glen 1000 link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff:ff 4: eno1: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 gdisc mg state DOWN group default glen 1000 link/ether 38:0e:4d:7d:b7:f2 brd ff:ff:ff:ff:ff:ff 5: eno2: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc mq state DOWN group default glen 1000

link/ether 38:0e:4d:7d:b7:f3 brd ff:ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER\_UP> mtu 9000 qdisc noqueue state UP
group default qlen 1000
link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff
inet 10.14.1.45/24 brd 10.14.1.255 scope global bond0
valid\_lft forever preferred\_lft forever

BONDING\_OPTS=" miimon=100 mode=1 primary=<Interface Name> primary\_reselect=0" - primary re-select default value is 0.

## **Configure /etc/hosts**

2

Prior to setting up DNS, configure /etc/hosts on the Admin node.

For the purpose of simplicity, /etc/hosts file is configured with hostnames in all the nodes. However, in large scale production grade deployment, DNS server setup is highly recommended. Furthermore, /etc/hosts file is not copied into containers running on the platform.

Below are the sample A records for DNS configuration within Linux environment:

```
ORIGIN cdip.cisco.local
rhelnn01 A 10.14.1.45
rhelnn02 A 10.14.1.46
rhelnn03 A 10.14.1.47
rhel01 A 10.14.1.51
rhel02 A 10.14.1.52
rhel03 A 10.14.1.53
...
Rhel15 A 10.14.1.65
Rhel16 A 10.14.1.66
```

To create the host file on the admin node, follow these steps:

1. Log into the Admin Node (rhelnn01).

```
#ssh 10.14.1.46
```

2. Populate the host file with IP addresses and corresponding hostnames on the Admin node (rhelnn01) and other nodes as follows:

On Admin Node (rhelnn01):

```
[root@rhelnn01 ~]# cat /etc/hosts
          localhost localhost.localdomain localhost4 localhost4.localdomain4
127.0.0.1
::1
            localhost localhost.localdomain localhost6 localhost6.localdomain6
# Name nodes
10.14.1.45
               rhelnn01.cdip.cisco.local
                                             rhelnn01
10.14.1.46
               rhelnn02.cdip.cisco.local
                                             rhelnn02
10.14.1.47
               rhelnn03.cdip.cisco.local
                                             rhelnn03
# Data nodes
10.14.1.51
               rhel01.cdip.cisco.local rhel01
10.14.1.52
               rhel02.cdip.cisco.local rhel02
10.14.1.53
               rhel03.cdip.cisco.local rhel03
```

10.14.1.54	rhel04.cdip.cisco.local	rhel04
10.14.1.55	rhel05.cdip.cisco.local	rhel05
10.14.1.56	rhel06.cdip.cisco.local	rhel06
10.14.1.57	rhel07.cdip.cisco.local	rhel07
10.14.1.58	rhel08.cdip.cisco.local	rhel08
10.14.1.59	rhel09.cdip.cisco.local	rhel09
10.14.1.60	rhel10.cdip.cisco.local	rhel10
10.14.1.61	rhel11.cdip.cisco.local	rhel11
10.14.1.62	rhel12.cdip.cisco.local	rhel12
10.14.1.63	rhel13.cdip.cisco.local	rhel13
10.14.1.64	rhel14.cdip.cisco.local	rhel14
10.14.1.65	rhel15.cdip.cisco.local	rhel15
10.14.1.66	rhel16.cdip.cisco.local	rhel16

## Set Up Passwordless Login

To manage all the nodes in a cluster from the admin node password-less login needs to be setup. It assists in automating common tasks with Ansible, and shell-scripts without having to use passwords.

To enable password-less login across all the nodes when Red Hat Linux is installed across all the nodes in the cluster, follow these steps:

- 1. Log into the Admin Node (rhelnn01).
- 2. Run the ssh-keygen command to create both public and private keys on the admin node.

```
# ssh-keygen -N '' -f ~/.ssh/id rsa
```



3. Run the following command from the admin node to copy the public key id\_rsa.pub to all the nodes of the cluster. ssh-copy-id appends the keys to the remote-hosts .ssh/authorized\_keys.

```
# for i in {01..03}; do echo "copying rhelnn$i.cdip.cisco.local"; ssh-copy-id -i
~/.ssh/id_rsa.pub root@rhelnn$i.cdip.cisco.local; done;
# for i in {01..16}; do echo "copying rhel$i.cdip.cisco.local"; ssh-copy-id -i
~/.ssh/id_rsa.pub root@rhel$i.cdip.cisco.local; done;
```

- 4. Enter yes for Are you sure you want to continue connecting (yes/no)?
- 5. Enter the password of the remote host.

# Create a Red Hat Enterprise Linux (RHEL) 7.7 Local Repository

To create a repository using RHEL DVD or ISO on the admin node (in this deployment rhelnn01 is used for this purpose), create a directory with all the required RPMs, run the "createrepo" command and then publish the resulting repository.

To create a RHEL 7.7 local repository, follow these steps:

1. Log into rhelnn01. Create a directory that would contain the repository.

# # mkdir -p /var/www/html/rhelrepo

- 2. Copy the contents of the Red Hat DVD to /var/www/html/rhelrepo
- 3. Alternatively, if you have access to a Red Hat ISO Image, Copy the ISO file to rheInn01.
- 4. Log back into rheInn01 and create the mount directory.

```
# scp rhel-server-7.7-x86_64-dvd.iso rhelnn01:/root/
# mkdir -p /mnt/rheliso
# mount -t iso9660 -o loop /root/rhel-server-7.7-x86 64-dvd.iso /mnt/rheliso/
```

5. Copy the contents of the ISO to the /var/www/html/rhelrepo directory.

# cp -r /mnt/rheliso/\* /var/www/html/rhelrepo

6. On rhelnn01 create a .repo file to enable the use of the yum command.

```
# vi /var/www/html/rhelrepo/rheliso.repo
[rhel7.7]
name=Red Hat Enterprise Linux 7.7
baseurl=http://10.14.1.46/rhelrepo
gpgcheck=0
enabled=1
```

7. Copy rheliso.repo file from /var/www/html/rhelrepo to /etc/yum.repos.d on rhelnn01.

# cp /var/www/html/rhelrepo/rheliso.repo /etc/yum.repos.d/

Based on this repository file, yum requires httpd to be running on rhelnn01 for other nodes to access the repository.

8. To make use of repository files on rhelnn01 without httpd, edit the baseurl of repo file /etc/yum.repos.d/rheliso.repo to point repository location in the file system.

This step is needed to install software on Admin Node (rhelnn01) using the repo (such as httpd, create-repo, and so on.)

```
# vi /etc/yum.repos.d/rheliso.repo
[rhel7.7]
name=Red Hat Enterprise Linux 7.7
baseurl=file:///var/www/html/rhelrepo
```

gı	pgcheck=0		
e	nabled=1		

#### **Create the Red Hat Repository Database**

To create the Red Hat repository database, follow these steps:

1. Install the "createrepo" package on admin node (rhelnn01). Use it to regenerate the repository database(s) for the local copy of the RHEL DVD contents.

# yum -y install createrepo

2. Run "createrepo" on the RHEL repository to create the repo database on admin node

```
# cd /var/www/html/rhelrepo
# createrepo .
```

Figure 27 createrepo

```
[root@rhel01 rhelrepo]# createrepo
```

#### Set Up Ansible

To set up Ansible, follow these steps:

1. Download Ansible rpm from the this link: <u>https://releases.ansible.com/ansible/rpm/release/epel-7-x86\_64/ansible-2.9.6-1.el7.ans.noarch.rpm</u>

```
# wget https://releases.ansible.com/ansible/rpm/release/epel-7-x86 64/ansible-2.9.6-
1.el7.ans.noarch.rpm
```

2. Run the following command to install ansible:

# yum localinstall -y ansible-2.9.6-1.el7.ans.noarch.rpm

3. Verify Ansible installation by running the following commands:

```
# ansible --version
ansible 2.9.6
config file = /etc/ansible/ansible.cfg
configured module search path = [u'/root/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
ansible python module location = /usr/lib/python2.7/site-packages/ansible
executable location = /usr/bin/ansible
python version = 2.7.5 (default, Jun 11 2019, 14:33:56) [GCC 4.8.5 20150623 (Red
Hat 4.8.5-39)]
# ansible localhost -m ping
localhost | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

4. Prepare the host inventory file for Ansible as shown below. Various host groups have been created based on any specific installation requirements of certain hosts.

```
[root@rhelnn01 ~]# cat /etc/ansible/hosts
[admin]
rhelnn01.cdip.cisco.local
[namenodes]
rhelnn01.cdip.cisco.local
rhelnn02.cdip.cisco.local
rhelnn03.cdip.cisco.local
[datanodes]
rhel01.cdip.cisco.local
rhel02.cdip.cisco.local
rhel03.cdip.cisco.local
rhel04.cdip.cisco.local
rhel05.cdip.cisco.local
rhel06.cdip.cisco.local
rhel07.cdip.cisco.local
rhel08.cdip.cisco.local
rhel09.cdip.cisco.local
rhel10.cdip.cisco.local
rhel11.cdip.cisco.local
rhel12.cdip.cisco.local
rhel13.cdip.cisco.local
rhel14.cdip.cisco.local
rhel15.cdip.cisco.local
rhel16.cdip.cisco.local
[nodes]
rhelnn01.cdip.cisco.local
rhelnn02.cdip.cisco.local
rhelnn03.cdip.cisco.local
rhel01.cdip.cisco.local
rhel02.cdip.cisco.local
rhel03.cdip.cisco.local
rhel04.cdip.cisco.local
rhel05.cdip.cisco.local
rhel06.cdip.cisco.local
rhel07.cdip.cisco.local
rhel08.cdip.cisco.local
rhel09.cdip.cisco.local
rhel10.cdip.cisco.local
rhel11.cdip.cisco.local
rhel12.cdip.cisco.local
rhel13.cdip.cisco.local
rhel14.cdip.cisco.local
rhel15.cdip.cisco.local
rhel16.cdip.cisco.local
```

5. Verify host group by running the following command.

```
# ansible datanodes -m ping
```

# Install httpd

Setting up the RHEL repository on the admin node requires httpd. To set up RHEL repository on the admin node, follow these steps:

1. Install httpd on the admin node to host repositories:



The Red Hat repository is hosted using HTTP on the admin node; this machine is accessible by all the hosts in the cluster.

# yum -y install httpd

2. Add ServerName and make the necessary changes to the server configuration file:

```
# vi /etc/httpd/conf/httpd.conf
ServerName 10.14.1.46:80
```

3. Start httpd:

```
# service httpd start
# chkconfig httpd on
```

#### **Disable the Linux Firewall**

The default Linux firewall settings are too restrictive for any Hadoop deployment. Since the Cisco UCS Big Data deployment will be in its own isolated network there is no need for that additional firewall.

To disable the Linux firewall, run the following:

```
# ansible all -m command -a "firewall-cmd --zone=public --add-port=80/tcp --
permanent"
# ansible all -m command -a "firewall-cmd --reload"
# ansible all -m command -a "systemctl disable firewalld"
```

**Disable SELinux** 

SELinux must be disabled during the install procedure and cluster setup. SELinux can be enabled after installation and while the cluster is running.

SELinux can be disabled by editing /etc/selinux/config and changing the SELINUX line to SELI-NUX=disabled.

To disable SELinux, follow these steps:

1. The following command will disable SELINUX on all nodes:

This command may fail if SELinux is already disabled. This requires reboot to take effect.

```
# ansible nodes -m shell -a "sed -i 's/SELINUX=enforcing/SELINUX=disabled/g'
/etc/selinux/config"
# ansible nodes -m shell -a "setenforce 0"
```

2. Reboot the machine, if needed for SELinux to be disabled in case it does not take effect. It can be checked using the following command:

## Set Up All Nodes to use the RHEL Repository

To set up all noes to use the RHEL repository, follow these steps:



Based on this repository file, yum requires httpd to be running on rhel1 for other nodes to access the repository.

1. Copy the rheliso.repo to all the nodes of the cluster:

```
# ansible nodes -m copy -a "src=/var/www/html/rhelrepo/rheliso.repo
dest=/etc/yum.repos.d/."
```

2. Copy the /etc/hosts file to all nodes:

```
# ansible nodes -m copy -a "src=/etc/hosts dest=/etc/hosts"
```

3. Purge the yum caches:

```
# ansible nodes -a "yum clean all"
# ansible nodes -a "yum repolist"
```

While the suggested configuration is to disable SELinux, if for any reason SELinux needs to be enabled on the cluster, run the following command to make sure that the httpd can read the Yum repofiles.

#chcon -R -t httpd\_sys\_content\_t /var/www/html/

#### Upgrade the Cisco Network Driver for VIC1387

The latest Cisco Network driver is required for performance and updates. The latest drivers can be downloaded from the link below:

https://software.cisco.com/download/home/283862063/type/283853158/release/4.1(1a)

In the ISO image, the required driver kmod-enic-4.0.0.8-802.24.rhel7u7.x86\_64.rpm can be located at \Network\Cisco\VIC\RHEL\RHEL7.7\.

To upgrade the Cisco Network Driver for VIC1387, follow these steps:

1. From a node connected to the Internet, download, extract, and transfer kmod-enic-.rpm to rhelnn01 (admin node).

2. Copy the rpm on all nodes of the cluster using the following Ansible commands. For this example, the rpm is assumed to be in present working directory of rhelnn01:

[root@rhelnn01 ~]# ansible all -m copy -a "src=/root/kmod-enic-4.0.0.8-802.24.rhel7u7.x86 64.rpm dest=/root/."

3. Use the yum module to install the enic driver rpm file on all the nodes through Ansible:

```
[root@rhelnn01 ~]# ansible all -m yum -a "name=/root/ kmod-enic-4.0.0.8-
802.24.rhel7u7.x86_64.rpm state=present"
Make sure that the above installed version of kmod-enic driver is being used on all
nodes by running the command "modinfo enic" on all nodes:
[root@rhel02 ~]# ansible all -m shell -a "modinfo enic | head -5"
```

- It is recommended to download the kmod-megaraid driver for higher performance on Name nodes. The RPM can be found in the same package at: \Storage\LSI\Cisco\_Storage\_12G\_SAS\_RAID\_controller\RHEL\RHEL7.7\kmod-megaraid\_sas-07.710.06.00\_el7.7-1.x86\_64.rpm:
- 5. Copy the rpm on all Name nodes of the cluster using the following Ansible commands. For this example, the rpm is assumed to be in present working directory of rhelnn01:

[root@rhelnn01 ~]# ansible namenodes -m copy -a "src=/root/kmod-megaraid\_sas-07.710.06.00 el7.7-1.x86 64.rpm dest=/root/."

6. Use the yum module to install the megaraid driver rpm file on all the Name nodes using Ansible:

```
[root@rhelnn01 ~]# ansible namenodes -m yum -a "name=/root kmod-megaraid_sas-
07.710.06.00_el7.7-1.x86_64.rpm state=present"
Make sure that the above installed version of kmod-megaraid driver is being used on
all nodes by running the command "modinfo megaraid_sas" on all nodes:
[root@rhelnn01 ~]# ansible all -m shell -a "modinfo megaraid_sas | head -5"
```

# Intel SPDK

The SPDK NVMe device driver is a user space, polled-mode, asynchronous, lockless NVMe driver. This driver provides zero-copy, highly parallel access directly to an SSD from a user space application. The driver runs in userspace, which avoids syscalls and enables zero-copy access from the application using the driver. The SPDK NVMe driver addresses the issue of interrupt latency by polling the storage device for completions instead of relying on interrupts, which effectively lowers both total latency and latency variance. Finally, the driver avoids all locks in the I/O path for maximum scalability.

SPDK provides a block stack with a unified API for talking to different storage backend devices(NVMe SSDs, PMEM, ramdisk, Ceph RBD, virtio-scsi/blk and so on).

SPDK provides an NVMe-oF target application that is capable of serving disks over the network via different transports; RDMA (iWARP, RoCE), InfiniBand<sup>™</sup>, Intel<sup>®</sup> Omni-Path Architecture. SPDK provide a unified interface for the NVMe driver and the NVMe-oF Initiator, so whether you're talking to locally PCIe-attached NVMe devices or remote NVMe devices over a Fabric you can use the same API in your application. SPDK is an open-source project under the BSD license which allows users to integrate any or all of the components under the most permissive licensing terms.

The total time it takes to read/write a block of data from/to an NVMe SSD is a function of the NVMe device latency and the NVMe driver latency. The device latency depends on the block size of the workload. NVMe SSDs can read/write a small block (4KiB) in less than 100 microseconds and have IOPS throughput of over 500K I/O per second. Therefore, even a small improvement of a few microseconds in the transaction time of a single I/O translates into huge saving in CPU cycles when building systems with many SSDs.

The SPDK open-source community redesigned storage software to highlight the outstanding efficiency enabled by running software optimized for NVMe SSDs. The SPDK NVMe driver has demonstrated that millions of I/Os per second per CPU core are easily attainable with no additional offload hardware for small block work-loads(4KiB). For large block workloads (> 1MB) the device latency is much higher com-pared to the NVMe driver latency and the I/O per second are much lower, so savings of a few microseconds will not reduce the total transaction time significantly or improve the IOPS throughput noticeably.

Intel SPDK driver requires RHEL version 8.1 and later which reduces latency and required number of cores. Intel SPDK driver requires kernel version 5.7 and later.

For more information on SPDK, go to: <u>https://spdk.io/</u>.

# Set Up JAVA

To setup JAVA, follow these steps:

# CDP PvC Base 7 requires JAVA 8.

- 1. Download jdk-8u241-linux-x64.rpm and src the rpm to admin node (rhelnn01) from the link: https://www.oracle.com/technetwork/iava/iavase/downloads/idk8-downloads-2133151.html
- 2. Copy JDK rpm to all nodes:

```
# ansible nodes -m copy -a "src=/root/jdk-8u241-linux-x64.rpm dest=/root/."
```

3. Extract and Install JDK all nodes:

# ansible all -m command -a "rpm -ivh jdk-8u241-linux-x64.rpm "

4. Create the following files java-set-alternatives.sh and java-home.sh on admin node (rhelnn01):

```
# vi java-set-alternatives.sh
#!/bin/bash
for item in java javac javaws jar jps javah javap jcontrol jconsole jdb; do
rm -f /var/lib/alternatives/$item
alternatives --install /usr/bin/$item $item /usr/java/jdk1.8.0_241-amd64/bin/$item
9
alternatives --set $item /usr/java/jdk1.8.0_241-amd64/bin/$item
done
# vi java-home.sh
export JAVA HOME=/usr/java/jdk1.8.0_241-amd64
```

5. Make the two java scripts created above executable:

chmod 755 ./java-set-alternatives.sh ./java-home.sh

6. Copying java-set-alternatives.sh to all nodes:

```
ansible nodes -m copy -a "src=/root/java-set-alternatives.sh dest=/root/."
ansible nodes -m file -a "dest=/root/java-set-alternatives.sh mode=755"
ansible nodes -m copy -a "src=/root/java-home.sh dest=/root/."
ansible nodes -m file -a "dest=/root/java-home.sh mode=755"
```

7. Setup Java Alternatives:

[root@rhelnn01 ~]# ansible all -m shell -a "/root/java-set-alternatives.sh"

8. Make sure correct java is setup on all nodes (should point to newly installed java path):

```
# ansible all -m shell -a "alternatives --display java | head -2"
rhelnn01.cdip.cisco.local | CHANGED | rc=0 >>
java - status is manual.
link currently points to /usr/java/jdk1.8.0 241-amd64/bin/java
rhelnn02.cdip.cisco.local | CHANGED | rc=0 >>
java - status is manual.
link currently points to /usr/java/jdk1.8.0 241-amd64/bin/java
rhelnn03.cdip.cisco.local | CHANGED | rc=0 >>
java - status is manual.
link currently points to /usr/java/jdk1.8.0 241-amd64/bin/java
rhel02.cdip.cisco.local | CHANGED | rc=0 >>
java - status is manual.
link currently points to /usr/java/jdk1.8.0 241-amd64/bin/java
rhel01.cdip.cisco.local | CHANGED | rc=0 >>
java - status is manual.
 link currently points to /usr/java/jdk1.8.0 241-amd64/bin/java
```

9. Setup JAVA\_HOME on all nodes:

# ansible all -m copy -a "src=/root/java-home.sh dest=/etc/profile.d"

10. Display JAVA\_HOME on all nodes:

# ansible all -m command -a "echo \$JAVA\_HOME"
rhelnn01.cdip.cisco.local | CHANGED | rc=0 >>
/usr/java/jdk1.8.0 241-amd64

11. Display current java -version:

# ansible all -m command -a "java -version"
rhelnn01.cdip.cisco.local | CHANGED | rc=0 >>
java version "1.8.0\_241"
Java(TM) SE Runtime Environment (build 1.8.0\_241-b07)
Java HotSpot(TM) 64-Bit Server VM (build 25.241-b07, mixed mode)

# **Enable Syslog**

Syslog must be enabled on each node to preserve logs regarding killed processes or failed jobs. Modern versions such as syslog-ng and rsyslog are possible, making it more difficult to be sure that a syslog daemon is present.

Use one of the following commands to confirm that the service is properly configured:

```
# ansible all -m command -a "rsyslogd -v"
# ansible all -m command -a "service rsyslog status"
```

#### Set the ulimit

On each node, ulimit -n specifies the number of inodes that can be opened simultaneously. With the default value of 1024, the system appears to be out of disk space and shows no inodes available. This value should be set to 64000 on every node.



To set ulimit, follow these steps:

- 1. For setting the ulimit on Redhat, edit "/etc/security/limits.conf" on admin node rhelnn01 and add the following lines:
- # vi /etc/security/limits.conf
- \* soft nofile 1048576
- \* hard nofile 1048576
- Copy the /etc/security/limits.conf file from admin node (rhelnn01) to all the nodes using the following command:

# ansible nodes -m copy -a "src=/etc/security/limits.conf
dest=/etc/security/limits.conf"

3. Make sure that the /etc/pam.d/su file contains the following settings:

```
# cat /etc/pam.d/su
#%PAM-1.0
auth
               sufficient
                           pam rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth
               sufficient pam wheel.so trust use uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth
               required
                         pam wheel.so use uid
                              system-auth
auth
               include
               include
                              postlogin
auth
                              pam succeed if.so uid = 0 use uid quiet
               sufficient
account
account
               include
                              system-auth
password
               include
                              system-auth
               include
                              system-auth
session
               include
session
                              postlogin
session
               optional
                              pam xauth.so
```

4. Copy the /etc/pam.d/su file from admin node (rhelnn01) to all the nodes using the following command:

# ansible nodes -m copy -a "src=/etc/pam.d/su dest/etc/pam.d/su"



The ulimit values are applied on a new shell, running the command on a node on an earlier instance of a shell will show old values.

## **Set TCP Retries**

Adjusting the tcp\_retries parameter for the system network enables faster detection of failed nodes. Given the advanced networking features of Cisco UCS, this is a safe and recommended change (failures observed at the operating system layer are most likely serious rather than transitory).

To set TCP retries, follow these steps:

#### On each node, set the number of TCP retries to 5 can help detect unreachable nodes with less latency.

1. Edit the file /etc/sysctl.conf and on admin node rhelnn01 and add the following:

net.ipv4.tcp retries2=5

2. Copy the /etc/sysctl.conf file from admin node (rhelnn01) to all the nodes using the following command:

# ansible nodes -m copy -a "src=/etc/sysctl.conf dest=/etc/sysctl.conf"

3. Load the settings from default sysctl file /etc/sysctl.conf by running the following command:

```
# ansible nodes -m command -a "sysctl -p"
```

## **Disable IPv6 Defaults**

To disable IPv6 defaults, follow these steps:

1. Run the following command:

```
# ansible all -m shell -a "echo 'net.ipv6.conf.all.disable_ipv6 = 1' >>
/etc/sysctl.conf"
# ansible all -m shell -a "echo 'net.ipv6.conf.default.disable_ipv6 = 1' >>
/etc/sysctl.conf"
# ansible all -m shell -a "echo 'net.ipv6.conf.lo.disable_ipv6 = 1' >>
/etc/sysctl.conf"
Load the settings from default sysctl file /etc/sysctl.conf:
# ansible all -m shell -a "sysctl -p"
```

#### **Disable Swapping**

To disable swapping, follow these steps:

1. Run the following on all nodes. Variable vm.swappiness defines how often swap should be used, 60 is default:

# ansible all -m shell -a "echo 'vm.swappiness=0' >> /etc/sysctl.conf"

2. Load the settings from default sysctl file /etc/sysctl.conf and verify the content of sysctl.conf:

# ansible all -m shell -a "sysctl -p"
# ansible all -m shell -a "cat /etc/sysctl.conf"

#### **Disable Memory Overcommit**

To disable Memory Overcommit, follow these steps:

1. Run the following on all nodes. Variable vm.overcommit memory=0

# ansible all -m shell -a "echo 'vm.overcommit memory=0' >> /etc/sysctl.conf"

2. Load the settings from default sysctl file /etc/sysctl.conf and verify the content of sysctl.conf:

```
# ansible all -m shell -a "sysctl -p"
# ansible all -m shell -a "cat /etc/sysctl.conf"
rhelnn01.cdip.cisco.local | CHANGED | rc=0 >>
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.tcp retries2=5
net.ipv6.conf.all.disable ipv6 = 1
net.ipv6.conf.default.disable ipv6 = 1
net.ipv6.conf.lo.disable ipv6 = 1
vm.swappiness=0
vm.overcommit memory=0
```

#### **Disable Transparent Huge Pages**

Disabling Transparent Huge Pages (THP) reduces elevated CPU usage caused by THP.

To disable Transparent Huge Pages, follow these steps:

1. You must run the following commands for every reboot; copy this command to /etc/rc.d/rc.local so they are executed automatically for every reboot:

# ansible all -m shell -a "echo never > /sys/kernel/mm/transparent\_hugepage/enabled"
# ansible all -m shell -a "echo never > /sys/kernel/mm/transparent hugepage/defrag"

2. On the Admin node, run the following commands:

```
#rm -f /root/thp_disable
#echo "echo never > /sys/kernel/mm/transparent_hugepage/enabled" >>
/root/thp_disable
#echo "echo never > /sys/kernel/mm/transparent_hugepage/defrag " >>
/root/thp_disable
```

3. Copy file to each node:

# ansible nodes -m copy -a "src=/root/thp\_disable dest=/root/thp\_disable"

4. Append the content of file thp\_disable to /etc/rc.local:

# ansible nodes -m shell -a "cat /root/thp\_disable >> /etc/rc.d/rc.local"
# ansible nodes -m shell -a "chmod +x /etc/rc.d/rc.local"

#### **NTP Configuration**

The Network Time Protocol (NTP) is used to synchronize the time of all the nodes within the cluster. The Network Time Protocol daemon (ntpd) sets and maintains the system time of day in synchronism with the timeserver located in the admin node (rhelnn01). Configuring NTP is critical for any Hadoop Cluster. If server clocks in the cluster drift out of sync, serious problems will occur with HBase and other services.

To configure NTP, follow these steps:

1. Run the following:

```
# ansible all -m yum -a "name=ntp state=present"
```

Installing an internal NTP server keeps your cluster synchronized even when an outside NTP server is inaccessible.

2. Configure /etc/ntp.conf on the admin node only with the following contents:

```
# vi /etc/ntp.conf
driftfile /var/lib/ntp/drift
restrict 127.0.0.1
restrict -6 ::1
server 127.127.1.0
fudge 127.127.1.0 stratum 10
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys
```

3. Create /root/ntp.conf on the admin node and copy it to all nodes:

# vi /root/ntp.conf
server 10.14.1.46
driftfile /var/lib/ntp/drift
restrict 127.0.0.1
restrict -6 ::1
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys

4. Copy ntp.conf file from the admin node to /etc of all the data nodes and two other name nodes by executing the following commands in the admin node (rhelnn01):

```
# ansible datanodes -m copy -a "src=/root/ntp.conf dest=/etc/ntp.conf"
# ansible rhelnn01 -m copy -a "src=/root/ntp.conf dest=/etc/ntp.conf"
# ansible rhelnn03 -m copy -a "src=/root/ntp.conf dest=/etc/ntp.conf"
Run the following to syncronize the time and restart NTP daemon on all nodes:
# ansible all -m service -a "name=ntpd state=stopped"
# systemctl start ntpd (On admin node)
```

# ansible all -m command -a "ntpdate rhelnn01.cdip.cisco.local" # ansible all -m service -a "name=ntpd state=started"

5. Make sure to restart of NTP daemon across reboots:

```
# ansible all -a "systemctl enable ntpd"
```

6. Verify NTP is up and running in all nodes by running the following commands:

# ansible all -a "systemctl status ntpd"

Alternatively, the new Chrony service can be installed, which is quicker to synchronize clocks in mobile and virtual systems.

7. Install the Chrony service:

```
# ansible all -m yum -a "name=chrony state=present"
```

8. Activate the Chrony service at boot:

# ansible all -a "systemctl enable chronyd"

9. Start the Chrony service:

```
# ansible all -m service -a "name=chronyd state=started"
# systemctl start chronyd
```

The Chrony configuration is in the /etc/chrony.conf file, configured similar to /etc/ntp.conf.

#### Configure the Filesystem for NameNodes and DataNodes

The following script formats and mounts the available volumes on each node whether it is NameNode or Data node. OS boot partition will be skipped. All drives are mounted based on their UUID as /data/disk1, /data/disk2, and so on.

To configure the filesystem for NameNodes and DataNodes, follow these steps:

1. On the Admin node, create a file containing the following script:

#vi /root/driveconf.sh

2. To create partition tables and file systems on the local disks supplied to each of the nodes, run the following script as the root user on each node:

This script assumes there are no partitions already existing on the data volumes. If there are partitions, delete them before running the script. For detailed information, go to section <u>Delete Partitions</u>.

```
#vi /root/driveconf.sh
#!/bin/bash
#disks_count=`lsblk -id | grep sd | wc -l`
#if [ $disks_count -eq 24 ]; then
# echo "Found 24 disks"
```

```
#else
# echo "Found $disks count disks. Expecting 24. Exiting.."
# exit 1
#fi
[[ "-x" == "${1}" ]] && set -x && set -v && shift 1
count=1
for X in /sys/class/scsi host/host?/scan
do
echo '- - -' > \{X\}
done
for X in /dev/sd?
do
echo "======"
echo $X
echo "======"
if [[ -b ${X} && `/sbin/parted -s ${X} print quit |/bin/grep -c boot` -ne 0
]]
then
echo "$X bootable - skipping."
continue
else
Y = \{X # # * / \} 1
echo "Formatting and Mounting Drive => ${X}"
/sbin/mkfs.xfs -f ${X}
(( $? )) && continue
#Identify UUID
UUID=`blkid ${X} | cut -d " " -f2 | cut -d "=" -f2 | sed 's/"//q'`
/bin/mkdir -p /data/disk${count}
(( $? )) && continue
echo "UUID of ${X} = ${UUID}, mounting ${X} using UUID on /data/disk${count}"
/bin/mount -t xfs -o inode64, noatime -U ${UUID} /data/disk${count}
(( $? )) && continue
echo "UUID=${UUID} /data/disk${count} xfs inode64, noatime 0 0" >> /etc/fstab
((count++))
fi
done
```

3. Run the following command to copy driveconf.sh to all the nodes:

```
# chmod 755 /root/driveconf.sh
# ansible namenodes -m copy -a "src=/root/driveconf.sh dest=/root/."
# ansible namenodes -m file -a "dest=/root/driveconf.sh mode=755"
```

4. Run the following command from the admin node to run the script across all name nodes:

# ansible namenodes -m shell -a "/root/driveconf.sh"

5. Run the following from the admin node to list the partitions and mount points:

```
# ansible namenodes -m shell -a "df -h"
# ansible namenodes -m shell -a "mount"
# ansible namenodes -m shell -a "cat /etc/fstab"
```

6. On the Admin node, create a file containing the following script for data nodes:

#vi /root/driveconf\_nvme.sh

2

7. To create partition tables and file systems on the local disks supplied to each of the nodes, run the following script as the root user on each node:

This script assumes there are no partitions already existing on the data volumes. If there are partitions, delete them before running the script. For detailed information, go to section Delete Partitions.

```
#vi /root/driveconf nvme.sh
#!/bin/bash
#disks count=`lsblk -id | grep sd | wc -l`
#if [ $disks count -eq 24 ]; then
# echo "Found 24 disks"
#else
# echo "Found $disks count disks. Expecting 24. Exiting.."
# exit 1
#fi
[[ "-x" == "${1}" ]] && set -x && set -v && shift 1
count=1
for X in /sys/class/scsi host/host?/scan
do
echo '- - -' > \${X}
done
for X in /dev/nvme?n1
do
echo "======"
echo $X
echo "======"
if [[ -b ${X} && `/sbin/parted -s ${X} print quit |/bin/grep -c boot` -ne 0
]]
then
echo "$X bootable - skipping."
continue
else
Y = \{X # # * / \} 1
echo "Formatting and Mounting Drive => \{X\}"
/sbin/mkfs.xfs -f ${X}
(( $? )) && continue
#Identify UUID
UUID=`blkid ${X} | cut -d " " -f2 | cut -d "=" -f2 | sed 's/"//g'`
/bin/mkdir -p /data/disk${count}
(( $? )) && continue
echo "UUID of ${X} = ${UUID}, mounting ${X} using UUID on /data/disk${count}"
/bin/mount -t xfs -o inode64, noatime -U ${UUID} /data/disk${count}
(( $? )) && continue
echo "UUID=${UUID} /data/disk${count} xfs inode64, noatime 0 0" >> /etc/fstab
((count++))
fi
done
```

8. Run the following command to copy driveconf.sh to all the nodes:

```
# chmod 755 /root/driveconf_nvme.sh
# ansible datanodes -m copy -a ``src=/root/driveconf nvme.sh dest=/root/."
```

# ansible datanodes -m file -a "dest=/root/driveconf\_nvme.sh mode=755"

9. Run the following command from the admin node to run the script across all data nodes:

# ansible datanodes -m shell -a "/root/driveconf\_nvme.sh"

10. Run the following from the admin node to list the partitions and mount points:

```
# ansible datanodes -m shell -a "df -h"
# ansible datanodes -m shell -a "mount"
# ansible datanodes -m shell -a "cat /etc/fstab"
```

# **Delete Partitions**

To delete a partition, follow these steps:

- 1. Run the mount command ('mount') to identify which drive is mounted to which device /dev/sd<?>
- 2. Umount the drive for the partition that needs to be deleted and run fdisk to delete as shown below.

## Do not delete the OS partition since this will wipe out the OS.

```
# mount
```

# umount /data/disk1 & (disk1 shown as example)
#(echo d; echo w;) | sudo fdisk /dev/sd<?>

#### **Cluster Verification**

This section explains the steps to create the script cluster\_verification.sh that helps to verify the CPU, memory, NIC, and storage adapter settings across the cluster on all nodes. This script also checks additional prerequisites such as NTP status, SELinux status, ulimit settings, JAVA\_HOME settings and JDK version, IP address and hostname resolution, Linux version and firewall settings.

To verify a cluster, follow these steps:

```
The following script uses cluster shell (clush) which needs to be installed and configured.
```

1. Create the script cluster\_verification.sh as shown, on the Admin node (rhelnn01).

```
#vi cluster_verification.sh
#!/bin/bash
shopt -s expand_aliases,
# Setting Color codes
green='\e[0;32m'
red='\e[0;31m'
NC='\e[0m' # No Color
echo -e "${green} === Cisco UCS Integrated Infrastructure for Big Data and Analytics
\ Cluster Verification === ${NC}"
echo ""
echo ""
echo ""
echo -e "${green} ==== System Information ==== ${NC}"
```

```
echo -e "${green}System ${NC}"
clush -a -B " `which dmidecode` |grep -A2 '^System Information'"
echo ""
echo ""
echo -e "${green}BIOS ${NC}"
clush -a -B " `which dmidecode` | grep -A3 '^BIOS I'"
echo ""
echo ""
echo -e "${green}Memory ${NC}"
clush -a -B "cat /proc/meminfo | grep -i ^memt | uniq"
echo ""
echo ""
echo -e "${green}Number of Dimms ${NC}"
clush -a -B "echo -n 'DIMM slots: '; `which dmidecode` |grep -c \
'^[[:space:]]*Locator:'"
clush -a -B "echo -n 'DIMM count is: '; `which dmidecode` | grep \ "Size" | grep -c
"MB""
clush -a -B "`which dmidecode` | awk '/Memory Device$/,/^$/ {print}' |\ grep -e
'^Mem' -e Size: -e Speed: -e Part | sort -u | grep -v -e 'NO \ DIMM' -e 'No Module
Installed' -e Unknown"
echo ""
echo ""
# probe for cpu info #
echo -e "${green}CPU ${NC}"
clush -a -B "grep '^model name' /proc/cpuinfo | sort -u"
echo ""
clush -a -B "`which lscpu` | grep -v -e op-mode -e ^Vendor -e family -e\ Model: -e
Stepping: -e BogoMIPS -e Virtual -e ^Byte -e '^NUMA node(s)'"
echo ""
echo ""
# probe for nic info #
echo -e "${green}NIC ${NC}"
clush -a -B "`which if config` | egrep ((^e)^p)' | awk \{print \ \$1\}' | \ xargs -l
`which ethtool` | grep -e ^Settings -e Speed"
echo ""
clush -a -B "`which lspci` | grep -i ether"
echo ""
echo ""
# probe for disk info #
echo -e "${green}Storage ${NC}"
clush -a -B "echo 'Storage Controller: '; `which lspci` | grep -i -e \ raid -e
storage -e lsi"
echo ""
clush -a -B "dmesg | grep -i raid | grep -i scsi"
echo ""
clush -a -B "lsblk -id | awk '{print \$1, \$4}'|sort | nl"
echo ""
echo ""
echo ""
echo ""
echo -e "${green}Linux Release ${NC}"
clush -a -B "cat /etc/*release | unig"
echo ""
echo ""
echo -e "${green}Linux Version ${NC}"
```

```
clush -a -B "uname -srvm | fmt"
echo ""
echo ""
echo -e "${green}Date ${NC}"
clush -a -B date
echo ""
echo ""
echo -e "${green}NTP Status ${NC}"
clush -a -B "ntpstat 2>&1 | head -1"
echo ""
echo ""
echo -e "${green}SELINUX ${NC}"
clush -a -B "echo -n 'SElinux status: '; grep ^SELINUX= \ /etc/selinux/config 2>&1"
echo ""
echo ""
clush -a -B "echo -n 'CPUspeed Service: '; `which service` cpuspeed \ status 2>&1"
clush -a -B "echo -n 'CPUspeed Service: '; `which chkconfig` --list \ cpuspeed 2>&1"
echo ""
echo ""
echo -e "${green}Java Version${NC}"
clush -a -B 'java -version 2>&1; echo JAVA HOME is ${JAVA HOME:-Not \ Defined!}'
echo ""
echo ""
echo -e "${green}Hostname LoOKup${NC}"
clush -a -B " ip addr show"
echo ""
echo ""
echo -e "${green}Open File Limit${NC}"
clush -a -B 'echo -n "Open file limit(should be >32K): "; ulimit -n'
```

2. Change permissions to executable:

# chmod 755 cluster\_verification.sh

 Run the Cluster Verification tool from the admin node. This can be run before starting Hadoop to identify any discrepancies in Post OS Configuration between the servers or during troubleshooting of any cluster / Hadoop issues:

#./cluster\_verification.sh

# **Install Cloudera Data Platform**

This section provides instructions for installing Cloudera software, including Cloudera Manager, Cloudera Runtime, and other managed services, in a production environment.

Review the <u>Cloudera Production Installation: Before You Install</u> steps prior to the production installation of Cloudera Manager, Cloudera Runtime, and other managed services, review the Cloudera Data Platform 7 Requirements and Supported Versions, in addition to the Cloudera Data Platform Release Notes.

# Prerequisites for CDP PvC Base Installation

This section details the prerequisites for the CDP PvC Base installation, such as setting up Cloudera Repo.

# **Cloudera Manager Repository**

To setup the Cloudera Manager Repository, follow these steps:

1. From a host connected to the Internet, download the Cloudera's repositories as shown below and transfer it to the admin node:

#mkdir -p /tmp/cloudera-repos/

2. Download Cloudera Manager Repository:

```
#cd /tmp/cloudera-repos/
# wget <u>https://archive.cloudera.com/cm7/7.1.1/redhat7/yum/cloudera-manager-
trial.repo
# reposync --config=./cloudera-manager-trial.repo --repoid=cloudera-manager
# wget <u>https://archive.cloudera.com/cm7/7.1.1/allkeys.asc</u></u>
```

# This downloads the Cloudera Manager RPMs needed for the Cloudera repository.

- 3. Run the following command to move the RPMs:
- 4. Copy the repository directory to the admin node (rhelnn01):

```
# scp -r /tmp/cloudera-repos/ rhelnn01:/var/www/html/
# mkdir -p /var/www/html/cloudera-repos/cloudera-manager (On admin node rhelnn01)
# scp allkeys.asc rhelnn01:/var/www/html/cloudera-repos/cloudera-manager/
```

5. On admin node (rhelnn01) run create repo command:

```
#cd /var/www/html/cloudera-repos/
#createrepo --baseurl <u>http://10.14.1.46/cloudera-repos/cloudera-manager/</u>
/var/www/html/cloudera-repos/cloudera-manager/
```



6. Create the Cloudera Manager repo file with following contents:

```
# vi /var/www/html/cloudera-repos/cloudera-manager/cloudera-manager.repo
# cat /var/www/html/cloudera-repos/cloudera-manager/cloudera-manager.repo
[cloudera-manager]
name=Cloudera Manager 7.1.1
baseurl=http://10.14.1.46/cloudera-repos/cloudera-manager/
gpgcheck=0
enabled=1
```

Copy the file cloudera-manager.repo into /etc/yum.repos.d/ on the admin node to enable it to find the packages that are locally hosted:

```
#cp /var/www/html/cloudera-repos/cloudera-manager/cloudera-manager.repo
/etc/yum.repos.d/
From the admin node copy the repo files to /etc/yum.repos.d/ of all the nodes of the
cluster:
# ansible all -m copy -a "src=/etc/yum.repos.d/cloudera-manager.repo
dest=/etc/yum.repos.d/."
```

# Set Up the Local Parcels for CDP PvC Base 7.1.1

From a host connected the internet, download CDP PvC Base 7.1.1 parcels that are meant for RHEL7.7 from the URL: <u>https://archive.cloudera.com/cdh7/7.1.1.0/parcels/</u> and place them in the directory /var/www/html/cloudera-repos/ " of the Admin node.

The following are the required files for RHEL7.7:

- CDH-7.1.1-1.cdh7.1.1.p0.3266817-el7.parcel
- CDH-7.1.1-1.cdh7.1.1.p0.3266817-el7.parcel.sha256
- manifest.json

# **Download Parcels**

To download parcels, follow these steps:

1. From a host connected to the Internet, download the Cloudera's parcels as shown below and transfer it to the admin node:

#mkdir -p /tmp/cloudera-repos/CDH7.1.1.0parcels

2. Download parcels:

```
#cd /tmp/cloudera-repos/CDH7.1.1.0parcels
# wget https://archive.cloudera.com/cdh7/7.1.1.0/parcels/CDH-7.1.1-
1.cdh7.1.1.p0.3266817-el7.parcel
# wget https://archive.cloudera.com/cdh7/7.1.1.0/parcels/CDH-7.1.1-
1.cdh7.1.1.p0.3266817-el7.parcel.sha256
# wget https://archive.cloudera.com/cdh7/7.1.1.0/parcels/manifest.json
```

3. Copy /tmp/cloudera-repos/CDH7.1.1.0parcels to the admin node (rhelnn01):

```
# mkdir -p /var/www/html/cloudera-repos/cdh7/7.1.1.0/parcels/ (on rhelnn01)
# scp -r /tmp/cloudera-repos/CDH7.1.1.0parcels/ rhelnn01:/var/www/html/cloudera-
repos/cdh7/7.1.1.0/parcels/
# chmod -R ugo+rX /var/www/html/cloudera-repos/cdh7
```

- 4. Verify that these files are accessible by using the URL <u>http://10.14.1.46/cloudera-repos/cdh7/7.1.1.0/parcels/</u> in admin node.
- 5. Download Sqoop Connectors.

```
# mkdir -p /tmp/cloudera-repos/sqoop-connectors
# wget --recursive --no-parent --no-host-directories
http://archive.cloudera.com/sqoop-connectors/parcels/latest/ -P /tmp/cloudera-repos/
```

6. Copy /tmp/cloudera-repos/sqoop-connectors to the admin node (rhelnn01).

```
# scp -r /tmp/cloudera-repos/sqoop-connectors rhelnn01:/var/www/html/cloudera-repos/
# sudo chmod -R ugo+rX /var/www/html/cloudera-repos/sqoop-connectors
```

# Install and Configure Database for Cloudera Manager

This section provides the steps to install and configure the database for Cloudera Manager.

## Install PostgreSQL Server

To install the PostgreSQL packages on the PostgreSQL server, follow these steps:

1. In the admin node where Cloudera Manager will be installed, use the following command to install PostgreSQL server.

```
# yum install postgresql10-server postgresql10
```

2. Install psycopg2 Python package 2.7.5 or higher if lower version is installed.

```
# yum install -y python-pip
# pip install psycopg2==2.7.5 --ignore-installed
```

Check installing dependencies for hue: https://docs.cloudera.com/documentation/enterprise/upgrade/topics/ug\_cdh\_upgrade\_hue\_psycopg2. html

# Configure and Start PostgreSQL Server

To configure and start the PostgreSQL server, follow these steps:

1. To configure and start the PostgreSQL Server, stop PostgreSQL server if it is running.

# systemctl stop postgresql-10.service



By default, PostgreSQL only accepts connections on the loopback interface. You must reconfigure PostgreSQL to accept connections from the fully qualified domain names (FQDN) of the hosts host-ing the services for which you are configuring databases. If you do not make these changes, the services cannot connect to and use the database on which they depend.

2. Make sure that LC\_ALL is set to en\_US.UTF-8 and initialize the database as follows:

```
# echo 'LC_ALL="en_US.UTF-8"' >> /etc/locale.conf
# sudo /usr/pgsql-10/bin/postgresql-10-setup initdb
```

3. # To enable MD5 authentication, edit /var/lib/pgsql/10/data/pg\_hba.conf by adding the following line:

# host all all 127.0.0.1/32 md5



The host line specifying md5 authentication shown above must be inserted before this ident line:

# host all 127.0.0.1/32 ident

Failure to do so may cause an authentication error when running the scm\_prepare\_database.sh script. You can modify the contents of the md5 line shown above to support different configurations.

For example, if you want to access PostgreSQL from a different host, replace 127.0.0.1 with your IP address and update postgresql.conf, which is typically found in the same place as pg\_hba.conf, to include:

#### # listen\_addresses = '\*'

4. Configure settings to ensure your system performs as expected. Update these settings in the /var/lib/pgsql/10/data/postgresql.conf file. Settings vary based on cluster size and resources as follows:

```
max_connection - 500
shared_buffers - 1024 MB
wal_buffers - 16 MB
max_wal_size - 6GB (checkpoint_segments=128)
checkpoint_completion_target - 0.9
```

Refer to section Install and Configure PostgreSQL for CDP, in the Cloudera Data Platform Private Cloud Base Installation guide.

5. Start the PostgreSQL Server and configure to start at boot.

```
# systemctl start postgresql-10.service
# systemctl enable postgresql-10.service
```

#### **Databases for CDP**

Create databases and service accounts for components that require a database.

Create databases for the following components:

- Cloudera Manager Server
- Cloudera Management Service Roles: Activity Monitor, Reports Manager, Hive Metastore Server, Data Analytics Studio, Ranger, hue, and oozie.

The databases must be configured to support the PostgreSQL UTF8 character set encoding.

Record the values you enter for database names, usernames, and passwords. The Cloudera Manager installation wizard requires this information to correctly connect to these databases.

To create databases for CDP, follow these steps:

1. In the admin node, connect to PostgreSQL:

# sudo -u postgres psql

2. Create databases using the following command:

```
CREATE ROLE scm LOGIN PASSWORD 'password';
CREATE DATABASE scm OWNER scm ENCODING 'UTF8';
CREATE ROLE amon LOGIN PASSWORD 'password';
CREATE DATABASE amon OWNER amon ENCODING 'UTF8';
CREATE ROLE rman LOGIN PASSWORD 'password';
CREATE DATABASE rman OWNER rman ENCODING 'UTF8';
```

```
CREATE ROLE hue LOGIN PASSWORD 'password';
CREATE DATABASE hue OWNER hue ENCODING 'UTF8';
CREATE ROLE hive LOGIN PASSWORD 'password';
CREATE DATABASE metastore OWNER hive ENCODING 'UTF8';
CREATE ROLE nav LOGIN PASSWORD 'password';
CREATE DATABASE nav OWNER nav ENCODING 'UTF8';
CREATE ROLE navms LOGIN PASSWORD 'password';
CREATE DATABASE navms OWNER navms ENCODING 'UTF8';
CREATE ROLE oozie LOGIN PASSWORD 'password';
CREATE DATABASE oozie OWNER oozie ENCODING 'UTF8';
CREATE ROLE rangeradmin LOGIN PASSWORD 'password';
CREATE DATABASE ranger OWNER rangeradmin ENCODING 'UTF8';
CREATE ROLE das LOGIN PASSWORD 'password';
CREATE DATABASE das OWNER das ENCODING 'UTF8';
ALTER DATABASE metastore SET standard conforming strings=off;
ALTER DATABASE oozie SET standard conforming strings=off;
```



For Apache Ranger specific configuration for PostgreSQL, see: <u>Configuring a PostgreSQL Database for</u> <u>Ranger</u>

# **Cloudera Manager Installation**

The following sections describe how to install Cloudera Manager and then using Cloudera Manager to install CDP PvC Base 7.1.1.

# Install Cloudera Manager

Cloudera Manager, an end-to-end management application, is used to install and configure CDP PvC Base. During CDP Installation, Cloudera Manager's Wizard will help to install Hadoop services and any other role(s)/service(s) on all nodes using the following procedure:

- Discovery of the cluster nodes
- Configure the Cloudera parcel or package repositories
- Install Hadoop, Cloudera Manager Agent (CMA) and Impala on all the cluster nodes.
- Install the Oracle JDK or Open JDK if it is not already installed across all the cluster nodes.
- Assign various services to nodes.
- Start the Hadoop services

# Please see the <u>JAVA requirements</u> for CDP PvC Base.

To install Cloudera Manager, follow these steps:

1. Update the repo files to point to local repository.

#rm -f /var/www/html/cloudera-repos/cloudera-manager/\*.repo
#cp /etc/yum.repos.d/cloudera-manager.repo /var/www/html/cloudera-repos/

2. Install the Oracle Java Development Kit on the Cloudera Manager Server host.

# ansible nodes -m shell -a "yum install -y java-1.8.0-openjdk-devel"



3. Install the Cloudera Manager Server packages either on the host where the database is installed, or on a host that has access to the database:

```
#yum install -y cloudera-manager-agent cloudera-manager-daemons cloudera-manager-
server
```

#### Set Up the Cloudera Manager Server Database

The Cloudera Manager Server Database includes a script that can create and configure a database for itself.

The script can:

- Create the Cloudera Manager Server database configuration file.
- (PostgreSQL) Create and configure a database for Cloudera Manager Server to use.
- (PostgreSQL) Create and configure a user account for Cloudera Manager Server.

The following sections describe the syntax for the script and demonstrate how to use it.

#### Prepare a Cloudera Manager Server External Database

To prepare a Cloudera Manager Server external database, follow this step:

1. Run the <u>scm\_prepare\_database.sh</u> script on the host where the Cloudera Manager Server package is installed (rheInn01) admin node:

```
# cd /opt/cloudera/cm/schema/
```

```
# ./scm_prepare_database.sh postgresql scm scm <password>
# ./scm_prepare_database.sh postgresql amon amon <password>
# ./scm_prepare_database.sh postgresql rman rman <password>
# ./scm_prepare_database.sh postgresql hue hue <password>
# ./scm_prepare_database.sh postgresql metastore hive <password>
# ./scm_prepare_database.sh postgresql oozie oozie<password>
# ./scm_prepare_database.sh postgresql das das <password>
# ./scm_prepare_database.sh postgresql ranger rangeradmin <password>
```

#### Start the Cloudera Manager Server

To start the Cloudera Manager Server, follow these steps:

1. Start the Cloudera Manager Server:

#systemctl start cloudera-scm-server

2. Access the Cloudera Manager using the URL, <u>http://10.14.1.46:7180/</u> to verify that the server is up.

3. Once the installation of Cloudera Manager is complete, install CDP PvC Base 7 using the Cloudera Manager Web interface.

# Install Cloudera Data Platform Private Cloud Base (CDP PvC Base)

To install the Cloudera Data Platform Private Cloud Base, follow these steps:

1. Log into the Cloudera Manager. Enter "admin" for both the Username and Password fields.

C CLOUDERA Manager	
	Automatic Sign Out Due to
	Inactivity
	You are now signed out of your account.
	We have not heard from you for about 30 minute(s), so for your security, Clouders Manager automatically signed you out of your account. Sign in below to continue.
	admin
	Remember me
	Sign In
(2) Support Portal	
12 Help	

2. Upload license file. Click Continue after successfully uploading license for CDP PvC Base.



3. Click Continue on the Welcome screen.



4. Enter name for the Cluster.

CLOUDERA Manager	Add Cluster - Installation			
<ul> <li>Parcels</li> <li>Running Commands</li> <li>Support</li> <li>Support</li> <li>admin</li> </ul>	<ul> <li>Welcome</li> <li>Cluster Basics</li> <li>Specify Hosts</li> <li>Select Rpository</li> <li>Select JDK</li> <li>Enter Login Credentials</li> <li>Install Agents</li> <li>Install Parcels</li> <li>brancels</li> <li>brancels</li> <li>cluster Cluster</li> </ul>	M ains storage nodes, compute nodes, and other services such as metadata and security collocated in a single cluster.		
«			Back	Continue

5. Specify the hosts that are part of the cluster using their IP addresses or hostname. The figure below shows a pattern that specifies the IP addresses range.

```
10.14.1.[45-47] or rhelnn[01-03].cdip.cisco.local
10.14.1.[51-66] or rhel[01-16].cdip.cisco.local
```

6. After the IP addresses or hostnames are entered, click Search.

	Welcome     Cluster Basics     Ssecify Hosts	Specify Hosts Hosts should be specified using the monitoring for that host.	same hostname (FQDN) that they will ide	entify themselves with. Clo	udera recommends including Cl	oudera Manager Server's host. This also enables
	(4) Select Repository	Hostname	eine(01-03).cdip.cisco.local.the((01-16).cd	fip.cisco.local		
	(5) Select JDK	Hin	t: Search for hostnames or IP addresses	using patterns 🗖		
	6 Enter Login Credentials	SSH Port:	22 Search			
	🕖 Install Agents	19 hosts scanned, 19 running SSH. Click the first checkbox hold down	the Shift key and click the last checkboy to	o select a cappe		
	8 Install Parcels	Expanded Query 1	Hostname (FQDN)	IP Address	Currently Managed	Result
	9 Inspect Cluster	rhel01.cdip.cisco.local	rhel01.cdip.cisco.local	10.14.1.51	No	Host was successfully scanned.
		rhel02.cdip.cisco.local	rhel02.cdip.cisco.local	10.14.1.52	No	Host was successfully scanned.
		rhel03.cdip.cisco.local	rhel03.cdip.cisco.local	10.14.1.53	No	Host was successfully scanned.
		fhel04.cdip.cisco.local	rhel04.cdip.cisco.local	10.14.1.54	No	Host was successfully scanned.
		rhel05.cdip.cisco.local	rhel05.cdip.cisco.local	10.14.1.55	No	Host was successfully scanned.
		rhel06.cdip.cisco.local	rhel06.odip.cisco.local	10.14.1.56	No	Host was successfully scanned.
		rhel07.cdip.cisco.local	rhel07.cdip.cisco.local	10.14.1.57	No	Host was successfully scanned.
		rhel08.cdip.cisco.local	rhei08.odip.cisco.local	10.14.1.58	No	Host was successfully scanned.
		rhel09.cdip.cisco.local	rhel09.cdip.cisco.local	10.14.1.59	No	Host was successfully scanned.
		rhel10.cdip.cisco.local	rhel10.odip.cisco.local	10.14.1.60	No	Host was successfully scanned.
		rhel11.cdip.cisco.local	rhel11.odip.cisco.local	10.14.1.61	No	Host was successfully scanned.
a statement of the		rhel12.cdip.cisco.local	rhel12.odip.cisco.local	10.14.1.62	No	Host was successfully scanned.
Commands		rhel13.cdip.cisco.local	rhel13.odip.cisco.local	10.14.1.63	No	Host was successfully scanned.
		rhel14.cdip.cisco.local	rhel14 odip cisco local	10.14.1.64	No	Host was successfully scanned.

7. Cloudera Manager will "discover" the nodes in the cluster. Verify that all desired nodes have been found and selected for installation.

#### Edit the Cloudera Data Platform Private Cloud Base Parcel Settings to use the CDP 7.1.1 Parcels

#### To edit the CDP PvC Base Parcel settings, follow these steps:

- 1. Add custom repository path for Cloudera Manager local repository created.
- 2. On the Cloudera Manager installation wizard, click Parcels.
- 3. Click Parcel Repositories and Network Settings.

#### CDH and other software

```
Cloudera recommends the use of parcels for installation over packages, because parcels enable Cloudera Manager to easily manage the software on your cluster, automating the deployment and upgrade of service binaries. Electing not to use parcels will require you to manually upgrade packages on all hosts in your cluster when software updates are available, and will prevent you from using Cloudera Manager's rolling upgrade capabilities.
```

4. Click to remove the entire remote repository URLs and add the URL to the location where we kept the CDP PvC Base 7.1.1 parcels, such as <a href="http://10.14.1.46/cloudera-repos/cdh7/7.1.1.0/parcels/">http://10.14.1.46/cloudera-repos/cdh7/7.1.1.0/parcels/</a>

CLOUDER Managar	RA	Add Cluster -	Installation	
_		🔗 Welcome		
F	Parcel Reposit	ory & Network Settin	38	×
	Cloudera Manager o	hecks the connection to the o	enfigured parcel reportiony URLs. A valid license is recurred to access most Clouders parcel reportionies.	
>	> 🗢 1/1 URL(s) - Th	e repository was successfull	accessed and the manifest downloaded and validated. (HTTP Status: 200)	
F	Remote Parcel Repo	sitory URLs	http://10.14.1.46/doudersreppos/adh777.11.0/percels/	• •
			•	
E	Enable Automatic A Repositories	uthentication for Cloudera	2	0
H	HTTP authentication Cloudera Repositori	i usemame override for es		
H	HTTP authentication Cloudera Repositori	1 password override for as		
F	Proxy Server			0
F	Praxy Port			
F	Prexy User			0
F	Proxy Pasaword			0
			2	
🚔 Parcels			Clove Siver & Verily Cot	figuration.
🖧 Running Dam	mmands			
ga support				
			Back Continue	

- 5. Click Save Changes to finish the configuration.
- 6. Click Continue on the confirmation page.
- 7. For the method of installation, select the Use Parcels (Recommended) radio button.
- 8. For the CDP PvC Base 7 version, select the Cloudera Runtime 7.1.1–1.cdh7.1.1.p0.3266817 radio button.
- 9. For the specific release of Cloudera Manager, select the Custom Repository radio button.
- 10. Enter the URL for the repository within the admin node. http://10.14.1.46/cloudera-repos/cm7 and click Continue.



11. Select appropriate option for JDK.

C CLOUDERA Manager	Add Cluster - Inst	tallation	
	Welcome     Cluster Basics     Specify Hosts     Select Repository     Select JDK     Enter Login Credentials	Select JDK         Selected Version         Supported JDK         Supported JDK         Version         More details on supported J         More details on supported J         If you plan to use JDK 11, you will need to install it manually on all hosts and then select the Manually manage JDK option below.         @ Manually manage JDK	DK version. C*
Parcels Running Commands Support Support a admin	<ul> <li>7 Install Agents</li> <li>(8) Inspect Cluster</li> <li>(9) Inspect Cluster</li> </ul>	Please ensure that a supported JDK is already installed on all hosts. You will need to manage installing the unlimited strength JCE policy file, if necessary. Install a Cloudera will install a supported version of OpenJDK version 8. Install a system provided version of OpenJDK By proceeding. Cloudera will install the default version of OpenJDK version 8 provided by the Operating System.	
«		Back	Continue



We selected the Manually Manager JDK option as shown in the screenshot (above).

12. Provide SSH login credentials for the cluster and click Continue.

CLOUDERA Manager	Add Cluster - Insta	allation	
	Velcome	Enter Login Credentials	
	Specify Hosts	Root access to your hosts is required to install the Cloudera packages. This installer will connect to your hosts via SSH and log in either directly as root or as another user with pass less sudo/phrun privileges to become root.	word-
	Select Repository	Login To All Hosts As:   root  Another user	
	Select JDK	You may connect via password or public-key authentication for the user selected above. Authentication Method: • All hosts accept same password	
	6 Enter Login Credentials	<ul> <li>All hosts accept same private key</li> </ul>	
	(7) Install Agents	Enter Password:	
	(8) Install Parcels	Confirm Password:	
	9 Inspect Cluster	Number of Simultaneous         10           Installations:         (Running a large number of installations at once can consume large amounts of network bandwidth and other system resources)	
		Þ	
Parcels     G Running Commands     Support     admin			
«		Back	Continue

The installation of the local Cloudera repository and using parcels begins.

CLOUDERA Manager	Add Cluster - Installation					
	<ul> <li>Welcome</li> <li>Cluster Basics</li> <li>Specify Hosts</li> </ul>	Install Agents Installation in progress.				
	Select Repository	0 of 19 host(s) completed successfull	y. Abort Installation			
	Select JDK	Hostname	IP Address	Progress	Status	
	C Enter Login Credentials	rhei01.cdip.cisco.local	10.14.1.51		<ul> <li>Refreshing package metadata</li> </ul>	Details
	7 Install Agents	rhel02.cdip.cisco.local	10.14.1.52		O Refreshing package metadata	Details 🗖
	(8) Install Parcels	rhel03 cdip.cisco.local	10.14.1.53		O Refreshing package metadata	Details 🗖
	9 Inspect Cluster	rhel04.cdip.cisco.local	10.14.1.54		○ Refreshing package metadata	Details 🗖
		rhel05.cdip.cisco.local	10.14.1.55		○ Refreshing package metadata	Details 🗖
		rhel06.cdip.cisco.local	10.14.1.56		∪ Refreshing package metadata	Details 🗖
		rhel07.cdip.cisco.local	10.14.1.57		O Refreshing package metadata	Details 🗖
		rhel08.cdip.cisco.local	10.14.1.58		O Refreshing package metadata	Details 🗖
		rhel09.cdip.cisco.local	10.14.1,59		U Refreshing package metadata	Details 🗖
		rhel10.cdip.cisco.local	10.14.1.60		U Refreshing package metadata	Details 🗖
Running Commands		rhel11.cdip.cisco.local	10.14.1.61	1	O Pending	Details 🗖
<ul> <li>Support</li> <li>admin</li> </ul>		rhel12.cdip.cisco.local	10.14.1.62	1	U Pending	Details 🗖
«						Back Continue



- 13. Run the inspect the hosts and network performance test through Cloudera Manager on which it has just performed the installation.
- 14. Review and verify the summary. Click Continue.
| C CLOUDERA<br>Manager   | Add Cluster - Insta  | allation   |
|---|--|--|
| <ul> <li>Parcels</li> <li>42 Running Commands</li> <li>(*) Support</li> </ul> | <ul> <li>Welcome</li> <li>Cluster Basics</li> <li>Specify Hosts</li> <li>Select Repository</li> <li>Select JDK</li> <li>Enter Login Credentials</li> <li>Install Agents</li> <li>Install Parcels</li> <li>Inspect Cluster</li> </ul> | Instruction of the second seco |
| C CLOUDERA<br>Manager   | Add Cluster - Insta  | allation   |
|   | <ul> <li>Welcome</li> <li>Cluater Basics</li> <li>Specify Hosts</li> <li>Select Repository</li> <li>Select JDK</li> <li>Enter Login Credentials</li> <li>Install Agents</li> <li>Install Parcels</li> <li>Inspect Cluster</li> </ul> | Index of the series of the ser |
| Parcels  Running Commands  Support  admin                                     |  | Back Continue  |

15. Select services that need to be started on the cluster.



We selected Custom Services for this study.

- 16. This is a critical step in the installation: Inspect and customize the role assignments of all the nodes based on your requirements and click Continue.
- 17. Reconfigure the service assignment to match Table 10.

Table 10 Service/Role Assign	ment
------------------------------	------

Service Name	Host
NameNode	Rhelnn01, rhelnn02, rhelnn03 (HA)
HistoryServer	rhelnn01
JournalNodes	rhelnn01, rhelnn02, rhelnn03
ResourceManager	rhelnn02, rhelnn03 (HA)
Hue Server	rhelnn02
HiveMetastore Server	rhelnn01
HiveServer2	rhelnn02

Service Name	Host
HBase Master	rhelnn02
Oozie Server	rhelnn01
ZooKeeper	rhelnn01, rhelnn02, rhelnn03
DataNode	rhel01 to rhel16
NodeManager	rhel01 to rhel16
RegionServer	rhel01 to rhel16
Sqoop Server	rhelnn01
Impala Catalog Server Daemon	rhelnn01
Impala State Store	rhelnn02
Impala Daemon	rhel01 to rhel16
Solr Server	rhel01 (can be installed on all hosts if needed if there is a search use case)
Spark History Server	rhelnn01
Spark Executors	rhel01 to rhel16

CLOUDERA Manager	Add Cluster - Configuration					
	<ul> <li>Select Services</li> <li>Assign Roles</li> <li>Setup Database</li> <li>Enter Required Parameters</li> <li>Review Changes</li> </ul>	Assign Roles You can customize the role assignments for your new cluster here; but if assignments are made incorrectly, such as assigning too many roles to a single host; this can impact the performance of your services. Cloudera does not recommend altering assignments unless you have specific requirements, such as having pre-selected a specific host for a specific role. You can also view the role assignments by host. View by Host © Data Analytics Studio				
	6 Command Details	rheinn02.cdip.cisco.local 🕶	rheinn02.odip.cisco.local 🕶			
	(7) Summary	▶ HBase				
		Master × 1 New rheinn02.cdip.clsco.local  RegionServer × 16 New	HBsse REST Server × 1 New rheinn01.cdip.oisco.local +	HBase Thrift Server × 1 New     rheinn03.cdip.clsco.local		
		Same As DataNode +				
		HDFS				
		NameNode × 1 New rheim02.cdip.cisco.local -	SecondaryNameNode × 1 New rhelm01.cdip.cisco.local	Balancer × 1 New rheimi03.cdip.cisco.local +		
		HttoFS	NFS Geteway	DataNode × 16 New		
		Select hosta	Select hosts	rhel[01:16].cdip.cisco.local +		
		😺 Hive				
m∎ Parcels L& Running Commands		Cateway × 19 New  rhel[01-16].odip.oisco.local; rheim[01-03].odip.oisco.l  HiveServer2  Catewat mate	Hive Metastore Server × 1 New rheinn02.odip.oisoo.local -	¥ WebHCat Server × 1 New rheinn03.odip.cisco.local +		
🕫 Support		Derect fibera				
CLOUDERA Manager		😵 Hive on Tez				
		Gateway × 19 New	WhiteServer2 × 2 New			
		ab Hus	mennio-ostorporocional -			
		en nue				
		rheinn02.cdip.cisco.local +	rheinn[01, 03].cdip.cisco.local +			
		9 Impala				
		9 Impala StateStore × 1 New	9 Impala Catalog Server × 1 New	9 Impala Daemon × 16 New		
		rheinn01.cdip.cisco.local	rhefnn03.cdip.cisco.local +	Same As DataNode +		
		😤 Key-Value Store Indexer				
		Lily HBase Indexer × 1 New     rheInn01.cdip.cisco.local				
		O Cloudera Management Service				
		G Service Monitor × 1 New	G Activity Monitor × 1 New	G Host Monitor × 1 New		
		rheinn02.cdip.cisco.local +	rheinn02.cdip.cisco.local +	rhelnn02.cdip.cisco.local +		
		Reports Manager × 1 New  rheinp02 cdip cisco local +	event Server × 1 New rheinn82 cdip cisco local +	Alert Publisher × 1 New     theim 02 cdip cisco local +		
		The second se		The second state state and a second sec		

# Figure 28 Assign Roles in Cloudera Manager, Cluster Creation Wizard Example

	C Llive on Ten		
C Manager	• Hive on Tez		
	😵 Gateway × 19 New	FliveServer2 × 2 New	
	rhel[01-16].cdip.cisco.local; rhelnn[01-03].cdip.cisco.local	rhelnn[02-03].cdip.cisco.local +	
	+ Hue		
	H Hue Server × 1 New	H Load Balancer × 2 New	
	rhelnn02.cdip.cisco.local +	rhelnn[01, 03].cdip.cisco.local +	
	9 Impala		
	9 Impala StateStore × 1 New	9 Impala Catalog Server × 1 New	9 Impala Daemon × 16 New
	rhelnn01.edip.cisco.local	rhefnn03.cdip.cisco.local +	Same As DataNode -
	🔆 Key-Value Store Indexer		
	ALIII HBase Indexer × 1 New		
	rhelnn01.cdip.cisco.local		
	G Cloudera Management Service		
	Service Monitor × 1 New	G Activity Monitor × 1 New	(e) Host Monitor × 1 New
	rhelnn02.odip.cisco.local +	rhelnn02.cdip.cisco.local +	rhelnn02.cdip.cisco.local +
	Reports Manager × 1 New	G Event Server × 1 New	G Alert Publisher × 1 New
	rhelnn02.cdip.cisco.local +	rhelnn02.odip.cisco.local +	rheinn02.cdip.cisco.local +

#### Set Up the Database

The role assignment recommendation above is for clusters of up to 64 servers. For clusters larger than 64 nodes, use the high availability recommendation defined in <u>Table 9</u>.

To set up the database, follow these steps:

- 1. In the Database Host Name sections use port 3306 for TCP/IP because connection to the remote server always uses TCP/IP.
- 2. Enter the Database Name, username and password that were used during the database creation stage earlier in this document.
- 3. Click Test Connection to verify the connection and click Continue.

CLOUDERA Manager	Add Cluster - Configuration				
	<ul> <li>Select Services</li> <li>Assign Roles</li> <li>Setup Database</li> </ul>	Setup Database Configure and test database connections. If Installation Guide C.	using custom databases, create the databases	first according to the Installing and Configuring	an External Database section of the
	(4) Enter Required Parameters	Currently assigned to run on rheinn02.cdip.c	isco.local. Database Hostname	Database Name	✓ Successful Username
	<ul><li>(5) Review Changes</li><li>(6) Command Details</li></ul>	PostgreSQL ~	localhost	amon	amon
	(Z) Summary	Reports Manager	ices level		✓ Successful
		Type PostgreSQL	Database Hostname	Database Name	Username man
		Password Oozie Server			e Durante de la
		Currently assigned to run on rhelnn02.cdip.c	isco.local. Database Hostname	Database Name	Usemame
		PostgreSQL ~	localhost	oozie	oozie
		Hive Type	Use JDBC URL Override	Database Hostname	✓ Successful Database Name
Parcels Running Commands		PostgreSQL ~	No ~ Password	localhost	metastore
③ Support					
	₿.	Hue Type PostoreSOL	Database Hostname	Database Name	✓ Successful Username
		Password			

4. Enter required parameters for Data Analytics Studio.

CLOUDERA Manager	<ul> <li>Select Services</li> <li>Assian Roles</li> </ul>	Enter Required Pa	rameters	
	Setup Database	DAS Database Hostname data_analytics_studio_database_h ost	Data Analytics Studio (Service-Wide) 🔊 Undo rheInn01.cdip.cisco.local	0
	Enter Required Parameters     Review Changes	DAS Database Name data_analytics_studio_database_n ame	Data Analytics Studio (Service-Wide) das	0
	6 Command Details	DAS Database Username data_analytics_studio_database_u semame	Data Analytics Studio (Service-Wide) das	0
	7 Summary	DAS Database Password data_analytics_studio_database_p assword	Data Analytics Studio (Service-Wide) 🧿 Undo	0
		Existing Cloudera Manager API Client Username queuemanager_em_api_client_logi n_name	YARN Queue Manager Webapp Default Group 🕤 Undo admin	0
Parcels  C Recent Commands  Support  admin		Existing Cloudera Manager API Client Password queuemanager_om_api_client_logi n_password	YARN Queue Manager Webapp Default Group 🕤 Undo	0
«			Back Co	ontinue

5. Review Data Analytics Studio (DAS) configuration.

CLOUDERA Manager	Add Cluster - Conf	iguration		
	Select Services	Review Changes		
	<ul> <li>Assign Roles</li> <li>Setup Database</li> </ul>	DAS Database Hostname	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0
	C Enter Required Parameters	ost DAS Database Name	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0
	5 Review Changes	data_analytics_studio_database_n ame	das	
	6 Command Details	DAS Database Username data_analytics_studio_database_u semame	CDIP-NVMe > Data Analytics Studio (Service-Wide) das	0
	7 Summary	DAS Database Password data_analytics_studio_database_p	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0
Parcels		Hive Session Parameters	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0
Recent Commands Support		Hive Secure Session	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0
🔥 admin 兴		Parameters	Back	ontinue

6. Review Data Analytics Studio (DAS) configuration.

CLOUDERA Manager	Add Cluster - Configuration				
	Select Services	Review Changes			
	Setup Database	DAS Database Hostname data_analytics_studio_database_h ost	CDIP-NVMe > Data Analytics Studio (Service-Wide) Service-Wide)	0	
	Enter Required Parameters	DAS Database Name data_analytics_studio_database_n ame	CDIP-NVMe > Data Analytics Studio (Service-Wide) das	0	
	6 Command Details	DAS Database Username data_analytics_studio_database_u	CDIP-NVMe > Data Analytics Studio (Service-Wide) das	0	
	7 Summary	semame DAS Database Password data_analytics_studio_database_p	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0	
Parcels		assword Hive Session Parameters das_hive_session_params	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0	
Recent Commands     Support     admin		Hive Secure Session Parameters	CDIP-NVMe > Data Analytics Studio (Service-Wide)	0	
«			Back Con	tinue	

7. Review and customize the configuration changes based on your requirements.

CLOUDERA Manager	Add Cluster - Cont	figuration		
	<ul> <li>Select Services</li> <li>Assign Roles</li> <li>Setup Database</li> </ul>	Review Changes HDFS Root Directory hbsse.rootdir	HBase (Service-Wide)	0
	C Enter Required Parameters	Enable Indexing	🗹 HBase (Service-Wide) 🥎	0
	5 Review Changes	Enable Replication	Z HBase (Service-Wide) ち	?
	<ol> <li>Command Details</li> <li>Summary</li> </ol>	HDFS Block Size	HDFS (Service-Wide)	۲
		DataNode Failed Volumes Tolerated dfs.datanode failtd.volumes.leterated Edit Individual Values	DataNode Group 2 • 4 DataNode Default Groupand 1 other • 5	٢
		DataNode Data Directory dfs.datanode.data.dir	DataNode Default Group 🜨 /data/disk1/dfs/dn	(? □ ⊕
🆀 Parcels			/data/disk2/dfs/dn	Ð₽
Running Commands			/data/disk3/dfs/dn	Ѐ
(9) Support (A) admin			/data/disk4/dfs/dn	⊡⊕

8. Click Continue to start running the cluster services.

C CLOUDERA Manager	Add Cluster - Configuration					
	<ul> <li>Select Services</li> <li>Assign Roles</li> <li>Setup Database</li> <li>Enter Required Parameters</li> <li>Review Chances</li> </ul>	First Run Command         Status       Finished       Context       CDIP-NVMe [2]				
	6 Command Details	<ul> <li>✓ ● Run a set of services for the first time Successfully completed 13 steps.</li> <li>&gt; ● Execute 9 steps in sequence</li> </ul>	Jun 12, 8:36:37 PM Jun 12, 8:36:42 PM	3.4m 3.3m		
Parcels	7 Summary					
Running Commands						
🚯 admin 🔇			Back	Continue		

9. Hadoop services are installed, configured, and now running on all the nodes of the cluster. Click Finish to complete the installation.

CLOUDERA Manager	Add Cluster - Configuration		
<ul> <li>Parcels</li> <li>Running Commands</li> <li>Support</li> <li>admin</li> </ul>	<ul> <li>Select Services</li> <li>Assign Roles</li> <li>Setup Database</li> <li>Enter Required Parameters</li> <li>Review Changes</li> <li>Command Details</li> <li>Summary</li> </ul>		
"		Back	Finish

Cloudera Manager now displays the status of all Hadoop services running on the cluster.

C CLOUDERA Manager	Home					Switch to Table View     Add +
Search	Status All Health Issues Configuration - All Recen	t Command	8			
& Clusters	CDIP-NVMe	i.	Charts			20m 1h 2h 6h 12h 1d 7d 30d 🖉 -
Diagnostics     Audits	Cloudera Runtime 7.1.1 (Parcels)		Chaster CPU	Cluster Disk 10	Cluster Network 10	
M Charts	Il 19 Hosts		1070	872M/a 881M/s	2 05.414/a	
2 Replication	HBase	1	50%	191M/s	10 F07294/18	
Administration	O B HOFS	1	28x45 DV PM	C8-13 D9 PM		
	🗢 😵 Hive	1	<ul> <li>COIP-NVMe, Host CPU Usage Across Hosts 0.38%</li> </ul>	<ul> <li>Total Disk Byte., \$.3M/s = Total Disk Byt., 13.6M/s</li> </ul>	<ul> <li>Total Bytes Rec. 12M/s = Total Bytes Tr. 17.8M/s</li> </ul>	
	Hive on Tez	1	HDFS IO	Completed Impela Queries		
	O Eb Hue	1				
	♥ Impala	1	19.15016	/ says are		
	Key-Value Store Inde	1	D8-45 09 PM	D* (8-45 00 PM		
	🛇 📓 Cozle	1	<ul> <li>Total Bytes Read SM/s = Total Bytes Wit 4.3M/s</li> </ul>	<ul> <li>Impala, Total Queries Across Impala Baemons 0</li> </ul>		
	O 🤊 Solr	1				
	O 🛷 Spark	1				
	tez	1				
	O III YARN	1				
	C 3: YARN Queue Manager	1				
	C 🔮 ZooKeeper	-				
	Cloudera Management Service					
Parces     Running Commands	<ul> <li>Cloudera Manageme</li> </ul>	1				
(9) Support 👧 admin						

## **Configure NVMe as YARN Local Directory**

To configure YARN local directory on separate NVMe disks, follow these steps:

- 1. Click cluster > YARN > Configuration tab, filter properties for dirs.
- 2. Modify disk labels specific to NVMe as per the format and partition performed earlier for following properties:

#### yarn.nodemanager.local-dir

yarn.nodemanager.log-dirs

CLOUDERA Monager	CDIP-NVMe				
Search	🗢 🏭 YARN 🛛 🗛 🖉	<del>ሀ</del> 🗟		Jun 15, 7.1	13 PM PDT
<ul> <li>Clusters</li> <li>Hosts</li> <li>Clagnostics</li> <li>Audits</li> </ul>	Status instances <u>Configuration</u>	) Commonde Applications Chartellionry Audio	c Web III + Quick Linice +		
l <u>at</u> , Charts 🕲 Replication 🛛 Administration	Filters MapReduce ApplicationMaster Staging Root SCOPF Directory		Jootfisiary Server Deles // Group	Show All Decon	islione D
	YARN (Service-Wide) 4 Gatavary 0 JobHistory Server 1 Nockelfarrager 5	yam app mepredizes an stuging-tir NodeManager Local Directories yam.notemanager/local dirs	risaan Noderbarager Gefault Group: 🕲 lineta Izerapitnemaät zyomutan	3 Dæ	Ð
	✓ CATEGORY		/temp/nema02/yam/nm	ÐŒ	
	Advanced 1 Compression 0 Docker on VARN 0	NodeManager Container Log Directories yaminofemanagorlog-dirs	NodeManager Defaalt Droop 10 toels //temp/invmtil/ syon/centurerHogs		D
	FPGA Management 0 GPU Management 0 Log Aggregation 6		/temp/mvms/2/yom/cantorer-logs	ÐÆ	

#### **Scale the Cluster**

The role assignment recommendation above is for cluster with at least 64 servers and in High Availability. For smaller cluster running without High Availability the recommendation is to dedicate one server for NameNode and a second server for secondary name node and YARN Resource Manager. For larger clusters larger than 28 nodes the recommendation is to dedicate one server each for name node, YARN Resource Manager and one more for running both NameNode (High Availability) and Resource Manager (High Availability) as in the table (no Secondary NameNode when in High Availability).

# For production clusters, it is recommended to set up NameNode and Resource manager in High Availability mode.

This implies that there will be at least 3 master nodes, running the NameNode, YARN Resource manager, the failover counterpart being designated to run on another node and a third node that would have similar capacity as the other two nodes.

All the three nodes will also need to run zookeeper and quorum journal node services. It is also recommended to have a minimum of 7 DataNodes in a cluster. Please refer to the next section for details on how to enable HA.

#### **Enable High Availability**

Setting up high availability is done after the Cloudera Installation is completed.

#### **HDFS High Availability**

The HDFS High Availability feature provides the option of running two NameNodes in the same cluster, in an Active/standby configuration. These are referred to as the Active NameNode and the Standby NameNode. Unlike the Secondary NameNode, the Standby NameNode is a hot standby, allowing a fast failover to a new NameNode in case that a machine crashes, or a graceful administrator-initiated failover for the purpose of planned maintenance. There cannot be more than two NameNodes.

For more information go to: <u>https://docs.cloudera.com/cdp-private-cloud-base/7.1.3/fault-tolerance/topics/cr-</u> <u>configuring-namenode-high-availability.html</u>

# Set Up HDFS High Availability

The Enable High Availability workflow leads through adding a second (standby) NameNode and configuring JournalNodes. During the workflow, Cloudera Manager creates a federated namespace. To set up HDFS High Availability, follow these steps:

1. Log into the admin node (rheInn01) and create the Edit directory for the JournalNode:

```
# ansible namenodes -m shell -a "mkdir -p /data/disk1/namenode-edits"
# ansible namenodes -m shell -a "chmod 77 /data/disk1/namenode-edits"
```

- 2. Log into the Cloudera manager and go to the HDFS service.
- 3. Select Actions> Enable High Availability. The hosts that are eligible to run a standby NameNode and the JournalNodes displays.



4. Specify a name for the nameservice or accept the default name nameservice1 and click Continue.

CLOUDERA Manager	Enable High Availability for HDFS							
	<ol> <li>Getting Started</li> <li>Assign Roles</li> <li>Review Changes</li> <li>Command Details</li> <li>Final Steps</li> </ol>	Getting Started         This wizard leads you through adding a standby NameNode, restarting this HDPS service and any dependent services, and then re-deploying client configurations.         Nameservice Name       nameservice1         Enabling High Availability creates a new nameservice. Accept the default name nameservice1 or provide another name in Nameservice Name.						

- 5. In the NameNode Hosts field, click Select a host. The host selection dialog displays.
- 6. Check the checkbox next to the hosts (rhelnn01) where the standby NameNode is to be set up and click OK.

- 7. In the JournalNode Hosts field, click Select hosts. The host selection dialog displays.
- 8. Check the checkboxes next to an odd number of hosts (a minimum of three) to act as JournalNodes and click OK. We used the same nodes for the Zookeeper nodes.
- 9. Click Continue.

<u>e</u>>

The standby NameNode cannot be on the same host as the active NameNode, and the host that is chosen should have the same hardware configuration (RAM, disk space, number of cores, and so on) as the active NameNode.

C CLOUDERA Manager	Enable High Availa	Enable High Availability for HDFS								
	Getting Started     Assign Roles	Assign Roles								
	3 Review Changes	NameNode Hosts	rhelnn02.cdip.cisco.local rhelnn03.cdip.cisco.local							
	4 Command Details	JournalNode Hosts	rhelm/01-03].cdip.cisco.l							
	5 Final Steps		We recommend that JournalNodes be hosted on machines of similar hardware specifications as the NameNodes. The hosts of NameNodes and the ResourceManager are generally good options. You must have a minimum of three and an odd number of JournalNodes.							

10. In the JournalNode Edits Directory property, enter a directory location created earlier in step 1 for the Journal-Node edits directory into the fields for each JournalNode host.

	Assign Roles	Review Changes							
	3 Review Changes	Des tre rollowing conliguration values for your new role(s), kequired values are marked with ".							
	④ Command Details	Parameter	Group 😡	Value	Description				
		Service HDFS							
(§) Final Steps	(5) Final Steps	NameNode Data Directories* dfs.namenode.name.dir	rheinn02	/data/disk1/dfs/nn Inherited from: NameNode Default Group	Determines where on the local file system the NameNode should store the name table (faimage). For redundancy, enter a comma-delimited list				
			rheinn03	/data/disk1/dfs/nn Inherited from: NameNode Default Group	or directories to replicate the name table in all of the directories. Typical values are /data/N/dfs/nn where N=1_3.				
	JournalNode Edits Directory* dfs.journalnode.edits.dir	rheinn01	/data/disk1/namenode-e Reset to empty default value**	Directory on the local file system where NameNode edits are written.					
			rheinn02	/data/disk1/namenode-e Reset to empty default value*					
			rheinn03	/data/disk1/namenode-e Reset to empty default value					
	Q.	Extra Options							
		S Force initialize the ZooKeepe	er ZNode for auto	failover. Any previous ZNode used for this name	service will be overwritten.				
		Clear any existing data prese Make sure you have backed up	ent in name direct any existing data	tories of Standby NameNode. in the name directories of Standby NameNode.					
		Clear any existing data prese	int in the Journal	Node edits directory for this nameservice.					
		Make sure you have backed up	any existing data	in the edits directory on <b>all</b> hosts running Journ	alNodes.				
Parcels									
🔏 Running Commands									
Support									
🚷 admin									

The directories specified should be empty and must have the appropriate permissions.

- 11. Extra Options: Decide whether Cloudera Manager should clear existing data in ZooKeeper, Standby NameNode, and JournalNodes. If the directories are not empty (for example, re-enabling a previous HA configuration), Cloudera Manager will not automatically delete the contents—select to delete the contents by keeping the default checkbox selection. The recommended default is to clear the directories.
- 12. If you choose not to configure any of the extra options, the data should be in sync across the edits directories of the JournalNodes and should have the same version data as the NameNodes.
- 13. Click Continue.

Cloudera Manager executes a set of commands that will stop the dependent services, delete, create, and configure roles and directories as appropriate, create a nameservice and failover controller, and restart the dependent services and deploy the new client configuration.

C CLOUDERA Manager	Enable High Availa	ability for HDFS				
	Getting Started     Assign Roles     Review Changes     Gommand Details	Enable High Availability Command Status © Finished Context HDFS @				
	(5) Final Steps	Check that name directories for the new Standby NameNode either do not exist or are writable and empty. Can optionally clear directories.		rheinn03.odip.cisco.local C <sup>#</sup>	Jun 15, 6:24:05 PM	1.8s
		Check that edits directories for the nameservice either do not exist or are writable and empty. Can optionally clear directories.			Jun 15, 6:24:07 PM	1.87s
		> O Stop hdfs and its dependent services	S.	CDIP-NVMe IS	Jun 15, 6:24:09 PM	2.6m
		> O Creating roles to enable High Availability.			Jun 15, 6:26:46 PM	34ms
		Deleting the SecondaryNameNode role. The checkpoint directories of the SecondaryNameNode will not be deleted.			Jun 15, 6:26:46 PM	37ms
		Configuring NameNodes and the HDFS service to enable High Availability.			Jun 15, 6:26:46 PM	1ms
	Þ	> O Initializing High Availability state in ZooKeeper.	(S	Failover Controller (rheinn02) (3*	Jun 15, 6:26:46 PM	16.23s
		> O Starting the JournalNodes			Jun 15, 6:27:03 PM	22.85s
		Formatting the name directories of the current NameNode. If the name directories are not empty, this is expected to fail. Failed to format NameNode.	ଙ	NameNode (rheinn02)	Jun 15, 6:27:26 PM	19.02s
- Oscarla		> O Initializing shared edits directory of NameNodes.	ď	NameNode (rheinn02)	Jun 15, 6:27:45 PM	20.15s
Running Commands		<ul> <li>Starting the NameNode that will be transitioned to active mode NameNode (htelnn02).</li> </ul>	Ø	NameNode (rheinn02)	Jun 15, 6:28:05 PM	22.36s
(admin		> O Waiting for the Active NameNode to start up.	C.	NameNode (rheinn02)	Jun 15, 6:28:27 PM	4.27s
«					Ba	Continue

- Formatting the name directory is expected to fail if the directories are not empty.
- 14. In the next screen additional steps are suggested by the Cloudera Manager to update the Hue and Hive metastore. Click Finish.

CLOUDERA Manager	Enable High Availa	nable High Availability for HDFS							
	<ul> <li>Getting Started</li> <li>Assign Roles</li> <li>Review Changes</li> <li>Command Details</li> <li>Final Steps</li> </ul>	Final Steps Successfully enabled High Availability. The following manual steps must be performed after completing this wizard:  Configure the HDFS Web Interface Role of Hue service(s) Hue to be an HTTPFS role instead of a NameNode. Documentation ?  For each of the Hive service(s) Hive, stop the Hive service, back up the Hive Metastore Database to a persistent store, run the service command "Update Hive Metastore NameNodes", then restart the Hive services.							

The following sections explain configuring Hue and Hive for high availability as needed.

#### Configure Hive Metastore to use HDFS High Availability

To configure the Hive Megastore to use HDFS High Availability, follow these steps:

- 1. Go the Hive service.
- 2. Select Actions > Stop.



- 3. Click Stop to confirm the command.
- 4. Back up the Hive Metastore Database (if any existing data is present).
- 5. Select Actions > Update Hive Metastore NameNodes and confirm the command.

CLOUDERA Manager	CDIP-NVMe							
Search	n 😵 Hive 🚺	Actions -						
& Clusters	e mive	Start						
Hosts	Status Instances	Stop	Audits Quick Links +					
Contraction Diagnostics	Health Tests	Restart	Create Trigger	Charts				
Litt. Charts	2 Show 2 Disabled	Add Role Instances		CPU Cores Used @	Health @			
අු Replication		Rename		0.01	100			
Administration	Status Summ	Enter Maintenance Mode		80 0.01	50			
	Gateway			06:15 06:30	06:15 06:30			
	Hive Metastore Server	Deploy Client Configuration Create Hive User Directory		-Hive Metastore 0.0044 -WebHCat Ser 0.00083	bad health 0 -concerning health 0     disabled health 0 -good health 100			
	WebHCat Server	Create Hive Warehouse Directory		Important Events and Alerts @	Critical Events and Alerts @			
	Hosts	Create Hive Warehouse External Directory			23			
		Create Hive Metastore database tables		event	even			
	Health History	Create Hive Sys database Validate Hive Metastore schema		06:15 06:30	06:15 06:30			
	> 2 Became Good	Update Hive Metastore NameNodes	6:31:30 PM 🚦	=Alerts 0 =Critical Events 0 = Important Events 0	WebHCat Server (rhe 0 WebHCat Server (rhe 0			
	Ø > 2 Became Disal	Upgrade Hive Metastore Database Schema	6:26:37 PM	Hive Metastore Server Canary Duration				
	2 Became Good	Create Ranger Plugin Audit Directory	Jun 12 9:13:24 PM 🚦	1.58				
	> 2 Became Disal	Download Client Configuration	Jun 12 9:11:48 PM	8 500ms				
	O > 2 Became Good		Jun 12 8:39:07 PM	06:15 06:30				
	🖉 🕤 2 Recame Disah	led	hin 12 6/46/36 DM :	- Hive Metastore Server (rheinn02.cdip.cisco.io 498ms				
Update Are you su the service	Update Hive Metastore NameNodes × Are you sure you want to run the <b>Update Hive Metastore NameNodes</b> command on the service <b>Hive</b> ?							
A Back up the Hive Metastore Database before running this command. If using Impala, after running this command you must either restart Impala or execute an 'invalidate metadata' query.								
Impala, af 'invalidate	o the Hive ter running metadata	Metastore Databa y this command y ' query.	ase before r ou must eit	unning this commar her restart Impala or	nd. If using rexecute an			

- 6. Select Actions > Start.
- 7. Restart the Hue and Impala services if stopped prior to updating the Metastore.

# Configure Hue to Work with HDFS High Availability

To configure Hue to work with HDFS High Availability, follow these steps:

- 1. Go to the HDFS service.
- 2. Click the Instances tab.
- 3. Click Add Role Instances.

C CLOUDIRA Manager	CDIP-NVMe										
Search	🗢 🖥 HDFS 🛛 Actions 🗸	B HDFS Actions -									
& Clusters	Status Instances Configuration	Commands	File Browser	Charts Library Cache Statistics	Audits Web	h III z Ouick Links z					
III Hosts	Anna manaces oringation outriants the construction outriance pages into or - QUEX ENS +										
I Diagnostics											
Audits	Q Search					C Filters		Last Updated: Jun 15, 6:45:52 PM PDT			
Let Charts	Eltoro	Action	ns for Selected -				Migrate Roles Add Role I	nstances Federation and High Availability Role Groups			
2 Replication	Filters		Chaban	Dala Tuna	Plate	Hasterne	Commission State	Bala Casua			
Administration	V STATUS		Status	ноге туре	otate	Hosiname	commission state	Kole Group			
	None 1		•	Balancer	N/A	rheinn01.cdip.cisco.local	Commissioned	Balancer Default Group			
	Good Health 23		٥	DataNode	Started	rhel06.cdip.cisco.local	Commissioned	DataNode Default Group			
	COMMISSION STATE		٥	DataNode	Started	rhel15.cdip.cisco.local	Commissioned	DataNode Default Group			
	> MAINTENANCE MODE		٥	DataNode	Started	rhel03.cdip.cisco.local	Commissioned	DataNode Default Group			
	> RACK ID		•	DataNeda	Startad	the MR or in cases	Commissioned	Datablada Dafault Group			
	> ROLE GROUP		, in the second	Datantue	otanieu	The second concerned	Commastered	betariote betaut oroup			
	> ROLE TYPE		0	DataNode	Started	rhel01.cdip.cisco.local	Commissioned	DataNode Default Group			
	> STATE		۲	DataNode	Started	rhel10.cdip.cisco.local	Commissioned	DataNode Default Group			
	> HEALTH TEST		۰	DataNode	Started	rhe109.cdip.cisco.local	Commissioned	DataNode Default Group			
			۲	DataNode	Started	rhel13.cdip.cisco.local	Commissioned	DataNode Default Group			

- 4. Select the text box below the HttpFS field. The Select Hosts dialog displays.
- 5. Select the host on which to run the role and click OK.
- 6. Click Continue.
- 7. Check the checkbox next to the HttpFS role and select Actions for Selected > Start.

C CLOUDERA Manager	Add Role Instance	Add Role Instances to HDFS							
	Assign Roles     Review Changes	Assign Roles You can specify the role assignments for your new roles here. You can also view the role assignments by host. View By Host & Gateway Select hosts & NFS Gateway	G HttpFS × 1 New rhelm03.cdip.cisco.local + G JournalNode × 3	SecondaryNameNode Select hosts					
		Select hosts Select hosts Select hosts	Select hosts DataNode × 16 Select hosts +	Select hosts					

C CLOUDIRA Manager	CDIP-NVMe									
Search	Status Instances Configuration Commands File Browser Charts Library Cache Statistics Audits Web UI • Quick Links •									
<ul> <li>Diagnostics</li> <li>Audits</li> <li>Lat. Charts</li> </ul>	Q Search	Actions for Selected (1) •			<ul> <li>Filters</li> <li>Migrate Roles</li> <li>Add Role In</li> </ul>		Last Updated: Jun 15, 6:49:08 PM PDT C Instances Federation and High Availability Role Groups			
C Replication	~ STATUS	Start by stop		State	Hostname	Commission State	Role Group			
	None 1 Good Health 23 Stopped 1	Restart Rolling Restart	•	N/A Started	rhelm01.cdip.cisco.local	Commissioned Commissioned	Balancer Default Group DataNode Default Group			
	> COMMISSION STATE	Decommission de	e	Started	rhel15.odip.cisco.local	Commissioned	DataNode Default Group			
	> MAINTENANCE MODE	Recommission	0	Started	rhel03.cdip.cisco.local	Commissioned	DataNode Default Group			
	> RACK ID	Regenerate missing Keytab	•	Started	rhel08.cdip.cisco.local	Commissioned	DataNode Default Group			
	> ROLE GROUP	Enter Maintenance Mode de	•	Started	rhel01.cdip.cisco.local	Commissioned	DataNode Default Group			
	STATE	Exit Maintenance Mode de	e	Started	rhel10.odip.cisco.local	Commissioned	DataNode Default Group			
	> HEALTH TEST	Delete #	0	Started	rhel09.odip.cisco.local	Commissioned	DataNode Default Group			
		DataNode	e	Started	rhel13.odip.cisco.local	Commissioned	DataNode Default Group			

- 8. After the command has completed, go to the Hue service.
- 9. Click the Configuration tab.
- 10. Locate the HDFS Web Interface Role property or search for it by typing its name in the Search box.
- 11. Select the HttpFS role that was just created instead of the NameNode role and save your changes.
- 12. Restart the Hue service.

C CLOUDERA Manager	CDIP-NVMe				
Search	🛇 🚯 Hue 🛛 Actions 🗸				Jun 15, 6:54 PM PDT
III Hosts ♥ Diagnostics	Q Search	commands Charts Library Audits	Web UI + Quick Links +	C Filters Role Groups History and Rollback	
Left Charts & Replication • Administration	Filters ~ SCOPE Hun (Gervice-Wide) 60 Hun Server 40	HDFS Web Interface Role webhdfa_uri	Hue (Service-Wide) 🗩 Undo 🐵 HttpFS (rheInn03) NameNode (rheInn03) NameNode (rheInn02)		Show All Descriptions
	Kerberos Ticket Renewer 30		C minerove (mining)		

Refer to the high availability section in the Cloudera Management document: <u>https://www.cloudera.com/documentation/enterprise/6/6.2/topics/admin\_ha.html</u> for more information on setting up high availability for other components like Impala, Oozie, and so on.

#### YARN High Availability

The YARN Resource Manager (RM) is responsible for tracking the resources in a cluster and scheduling applications (for example, MapReduce jobs). Before CDH 5, the RM was a single point of failure in a YARN cluster. The RM high availability (HA) feature adds redundancy in the form of an Active/Standby RM pair to remove this single point of failure. Furthermore, upon failover from the Standby RM to the Active, the applications can resume from their last check-pointed state; for example, completed map tasks in a MapReduce job are not re-run on a subsequent attempt. This allows events such the following to be handled without any significant performance effect on running applications.

• Unplanned events such as machine crashes.

 Planned maintenance events such as software or hardware upgrades on the machine running the ResourceManager.

For more information, go to: <u>https://docs.cloudera.com/cdp-private-cloud-base/7.1.3/yarn-high-availability/topics/yarn-configuring-resourcemanager-ha.html</u>

#### Set Up YARN High Availability

To set up YARN high availability, follow these steps:

- 1. Log into the Cloudera manager and go to the YARN service.
- 2. Select Actions > Enable High Availability.

CLOUDERA Manager	CDIP-NVMe					
Search	Status Instances C	Actions - Start Step	Audits W	eb Ul + Quick Links +		4 30 minutes preceding Jun 15, 6:56 PM PDT (# 19)
Disgnostics     Audits     Id Charts	Health Tests	Restart Rolling Restart	Create Trigger	Charts		30m 1h 2h 0h 12h 1d 7d 30d 🖍-
2 Replication Administration	Show 3 Good VARN Container Usage This health test is disat	Add Role Instances Rename	Rappress	Sector a second formation of	Abbitrations Lands (Cramination), An	
	Status Summar	Enter Maintenance Mode		8 (6.30 00-45 wroot (VARN), Applications Running (Currulative) 0	06:30 06:45 =root (CMRN), Applications Failed (Cumulative) 0	-F
	JobHistory Server	Create Job History Dir		Applications Killed (Cumulative) ©	Total Containers Running Across NodeManag	
	ResourceManager	Create NodeManager Remote Application Log Directory		flore /	1	
	Hosta	Create CM Container Usage Metrics Dr Install YARN MapReduce Framework JARa		06.45	06.00 00.45	
	Health History	Install YARN Services Dependencies		= root (YARN), Applications Killed (Cumulative) 0	vARM, Total Containers Running Across NodeMana	
	3 Became Good	Create Ranger Plugin Audit Directory	:05 PM 1	Penang comuners (cumulative) (p	soul containers raised Across Nooelinanager	
	<ul> <li>3 Became Disable</li> <li>JobHistory Server</li> </ul>	Reset ACLs on YARN Zookeeper nodes	k37 PM 1	contribut	Containers	
	<ul> <li>1 Became Bad</li> <li>3 Became Good</li> </ul>	Enable High dyalability	04 PM 1	05.30 06-45 wroot (YARN), Pending Containers (Cumulative) 0	00.30 00.45 ••• YABN, Total Contarives Pailed Across NodeManagers @	
Parcels  Running Commands  Support	3 Became Disabled	Jun 12 9.1	1:48 PM	Health @	Important Events and Alerts @	
ladmin (K				Objige Column Colu	Otal     Otal	

The hosts that are eligible to run a standby ResourceManager displays.

The host where the current ResourceManager is running is not available as a choice.

3. Select the host (rhelnn03) where the standby ResourceManager is to be installed and click Continue.

CLOUDERA Manager	Enable High Avail	ability for YARN
	Getting Started     Review Changes     Command Details	Getting Started This wizard leads you through adding a standby ResourceManager, restarting this YARN service and any dependent services, and then re-deploying client configurations. ResourceManager Hosts thehn02.cdip cisco.local thehn03.cdip cisco.local

Cloudera Manager proceeds to execute a set of commands that stop the YARN service, add a standby ResourceManager, initialize the ResourceManager high availability state in ZooKeeper, restart YARN, and rede-ploy the relevant client configurations. 4. Click Finish when the installation is completed successfully.

#### Configure Yarn (MR2 Included) and HDFS Services

The parameters in <u>Table 11</u> and <u>Table 12</u> are used for Cisco UCS Integrated Infrastructure for Big Data and Analytics Performance Optimized cluster configuration described in this document. These parameters are to be changed based on the cluster configuration, number of nodes and specific workload.

Table 11 YARN	
Service	Value
mapreduce.output.fileoutputformat.compress.type	BLOCK
mapreduce.output.fileoutputformat.compress.codec	org.apache.hadoop.io.compress.DefaultCodec
mapreduce.map.output.compress.codec	org.apache.hadoop.io.compress.SnappyCodec
mapreduce.map.output.compress	True
zlib.compress.level	BEST_SPEED
mapreduce.task.io.sort.factor	64
mapreduce.map.sort.spill.percent	0.9
mapreduce.reduce.shuffle.parallelcopies	20
yarn.nodemanager.resource.memory-mb	320GB
yarn.nodemanager.resource.cpu-vcores	64
yarn.scheduler.maximum-allocation-vcores	64
yarn.scheduler.maximum-allocation-mb	320GB
mapreduce.task.io.sort.mb	2047
mapreduce.job.reduce.slowstart.completedmap	0.8
yarn.app.mapreduce.am.resource.cpu-vcores	1
mapreduce.map.memory.mb	5G
mapreduce.reduce.memory.mb	5G
mapreduce.job.heap.memory-mb.ratio	0.8
mapreduce.job.shuffle.merge.percent	0.95

Service	Value
mapreduce.job.shuffle.input.buffer.percent	0.7
mapreduce.job.reduce.input.buffer.percent	0.7
mapreduce.input.fileinputformat.split.minsize	409600000
mapreduce.ifile.readahead.bytes	16777216
mapreduce.inmem.merge.threshold	0
Enable Optimized Map-side Output Collector	Enable - Gateway Default Group

#### Table 12 HDFS

Service	Value
dfs.datanode.failed.volumes.tolerated	4
dfs.datanode.du.reserved	50 GiB
dfs.datanode.data.dir.perm	755
Java Heap Size of Namenode in Bytes	4096 MiB (Could not change since minimum 1GB rec- ommended)
Java Heap Size of Secondary namenode in Bytes	4096 MiB (Could not change since minimum 1GB rec- ommended)
dfs.namenode.handler.count	55
dfs.namenode.service.handler.count	55

# **Configure Spark**

The two main resources that Spark (and YARN) are dependent on are CPU and memory. Disk and network I/O play a part in Spark performance as well, but neither Spark nor YARN currently can actively manage them. Every Spark executor in any application has the same fixed number of cores and same fixed heap size. The number of cores can be specified with the executor-cores flag when invoking spark-submit, spark-shell, and pyspark from the command line, or by setting the spark.executor.cores property in the spark-defaults.conf file or in the SparkConf object.

The heap size can be controlled with the executor-memory flag or the spark.executor.memory property. The cores property controls the number of concurrent tasks an executor can run, executor-cores = 5 mean that each executor can run a maximum of five tasks at the same time. The memory property impacts the amount of data Spark can cache, as well as the maximum sizes of the shuffle data structures used for grouping, aggregations, and joins.

The num-executors command-line flag or spark.executor.instances configuration property control the number of executors requested. Dynamic Allocation can be enabled from CDH5.4 instead setting the spark.dynamicAllocation.enabled to true. Dynamic allocation enables a Spark application to request executors when there is a backlog of pending tasks and free up executors when idle.

Asking for five executor cores will result in a request to YARN for five virtual cores. The memory requested from YARN is a little more complex for the following reasons:

- executor-memory/spark.executor.memory controls the executor heap size, but JVMs can also use some memory off heap, for example for VM overhead, interned Strings and direct byte buffers. The value of the spark.yarn.executor.memoryOverhead property is added to the executor memory to determine the full memory request to YARN for each executor. It defaults to max (384, 0.10 \* spark.executor.memory).
- YARN may round the requested memory up a little. YARN's yarn.scheduler.minimum-allocation-mb and yarn.scheduler.increment-allocation-mb properties control the minimum and increment request values respectively.

The application master is a non-executor container with the special capability of requesting containers from YARN, takes up resources of its own that must be budgeted in. In *yarn-client* mode, it defaults to a 1024MB and one vcore. In *yarn-cluster* mode, the application master runs the driver, so it's often useful to add its resources with the -driver-memory and -driver-cores properties.

Running executors with too much memory often results in excessive garbage collection delays. 64GB is a rough guess at a good upper limit for a single executor.

A good estimate is that at most five tasks per executor can achieve full write throughput, so it's good to keep the number of cores per executor around that number.

Running tiny executors (with a single core and just enough memory needed to run a single task, for example) throws away the benefits that come from running multiple tasks in a single JVM. For example, broadcast variables need to be replicated once on each executor, so many small executors will result in many more copies of the data.

#### **Tune Resource Allocation for Spark**

 Below is an example of configuring a Spark application to use as much of the cluster as possible, we are using an example cluster with 16 nodes running NodeManagers, each equipped with 56 cores and 256GB of memory. yarn.nodemanager.resource.memory-mb and yarn.nodemanager. resource.cpu-vcores should be set to 180 \* 1024 = 184320 (megabytes) and 48 respectively.

```
spark.default.parallelism=10000
spark.driver.memoryOverhead=4096
spark.executor.memoryOverhead=4096
spark.executor.extraJavaOptions=-XX:+UseParallelGC -XX:ParallelGCThreads=4
spark.shuffle.file.buffer=1024k
spark.broadcast.compress=true
spark.shuffle.compress=true
spark.io.compression.codec=org.apache.spark.io.SnappyCompressionCodec
spark.io.compression.snappy.blockSize=512k
```

• This configuration results in four executors on all nodes except for the one with the AM, which will have three executors.

```
executor-memory is derived as (180/4 \text{ executors per node}) = 45; 45 * 0.10 = 4.5 45 - 4.5 ~ 40.
For taking care of long running processes use 2G for the spark driver spark.driver.memory = 2G
```

Submit a Job

--driver -memory 2G -executor -memory 40G --num-executors 63 --executor-cores 5 -properties-file /opt/cloudera/parcels/CDH/etc/spark/conf.dist/spark-defaults.conf

In yarn-cluster mode, the local directories used by the Spark executors and the Spark driver will be the local directories configured for YARN (Hadoop YARN config yarn.nodemanager.local-dirs). If the user specifies spark.local.dir, it will be ignored.

In yarn-client mode, the Spark executors will use the local directories configured for YARN while the Spark driver will use those defined in spark.local.dir. The Spark driver does not run on the YARN cluster in yarn-client mode, only the Spark executors do.

```
spark.local.dir /tmp (Directory to use for "scratch" space in Spark, including map output files and RDDs that get stored on disk. This should be on a fast, local disk in your system).
```

Every Spark stage has several tasks, each of which processes data sequentially. In tuning Spark jobs, this parallelism number is the most important parameter in determining performance. The number of tasks in a stage is the same as the number of partitions in the last RDD in the stage. The number of partitions in an RDD is the same as the number of partitions in the RDD on which it depends, with a couple exceptions: the coalesce transformation allows creating an RDD with fewer partitions than its parent RDD, the union transformation creates an RDD with the sum of its parents' number of partitions, and Cartesian creates an RDD with their product.

RDDs produced by a file have their partitions determined by the underlying MapReduce InputFormat that's used. Typically there will be a partition for each HDFS block being read. Partitions for RDDs produced by parallelize come from the parameter given by the user, or spark.default.parallelism if none is given.

The primary concern is that the number of tasks will be too small. If there are fewer tasks than slots available to run them in, the stage won't be taking advantage of all the CPU available.

If the stage in question is reading from Hadoop, your options are:

- Use the repartition transformation, which will trigger a shuffle.
- Configure your InputFormat to create more splits.
- Write the input data out to HDFS with a smaller block size.

If the stage is getting its input from another stage, the transformation that triggered the stage boundary will accept a numPartitions argument.

The most straightforward way to tune the number of partitions is experimentation: Look at the number of partitions in the parent RDD and then keep multiplying that by 1.5 until performance stops improving.

In contrast with MapReduce for Spark when in doubt, it is almost always better to be on the side of a larger number of tasks (and thus partitions).

#### **Shuffle Performance Improvement**

spark.shuffle.compress true (compress map output files)

spark.broadcast.compress true (compress broadcast variables before sending them)

spark.io.compression.codec org.apache.spark.io.SnappyCompressionCodec (codec used to compress internal data such as RDD partitions, broadcast variables and shuffle outputs)

spark.shuffle.spill.compress true (Whether to compress data spilled during shuffles.)

spark.shuffle.io.numConnectionsPerPeer 4 (Connections between hosts are reused in order to reduce connection buildup for large clusters. For clusters with many hard disks and few hosts, this may result in insufficient concurrency to saturate all disks, and so users may consider increasing this value.)

spark.shuffle.file.buffer 64K (Size of the in-memory buffer for each shuffle file output stream. These buffers reduce the number of disk seeks and system calls made in creating intermediate shuffle file)

#### **Improve Serialization Performance**

Serialization plays an important role in the performance of any distributed application. Often, this will be the first thing that should be tuned to optimize a Spark application.

spark.serializer org.apache.spark.serializer.KryoSerializer (when speed is necessary)

spark.kryo.referenceTracking false

spark.kryoserializer.buffer 2000 (If the objects are large, may need to increase the size further to fit the size of the object being deserialized).

SparkSQL is ideally suited for mixed procedure jobs where SQL code is combined with Scala, Java, or Python programs. In general, the SparkSQL command line interface is used for single user operations and ad hoc queries.

For multi-user SparkSQL environments, it is recommended to use a Thrift server connected via JDBC.

#### Spark SQL Tuning

The guidelines for Spark SQL tuning are as follows:

 To compile each query to Java bytecode on the fly, turn on sql.codegen. This can improve performance for large queries but can slow down very short queries: spark.sql.codegen true

```
spark.sql.unsafe.enabled true
```

- Configuration of in-memory caching can be done using the setConf method on SQLContext or by running SET key=value commands using SQL.
- spark.sql.inMemoryColumnarStorage.compressed true (will automatically select a compression codec for each column based on statistics of the data)
- spark.sql.inMemoryColumnarStorage.batchSize 5000 (Controls the size of batches for columnar caching. Larger batch sizes can improve memory utilization and compression, but risk OOMs when caching data)
- The columnar nature of the ORC format helps avoid reading unnecessary columns, but it is still possible to
  read unnecessary rows. ORC avoids this type of overhead by using predicate push-down with three levels
  of built-in indexes within each file: file level, stripe level, and row level. This combination of indexed data
  and columnar storage reduces disk I/O significantly, especially for larger datasets where I/O bandwidth
  becomes the main bottleneck for performance.

• By default, ORC predicate push-down is disabled in Spark SQL. To obtain performance benefits from predicate push-down, enable it explicitly, as follows:

spark.sql.orc.filterPushdown=true

In SparkSQL to automatically determine the number of reducers for joins and groupbys, use the parameter:

spark.sql.shuffle.partitions 200, (default value is 200)

- This property can be put into hive-site.xml to override the default value.
- Set log to WARN in log4j.properties to reduce log level.

Running the Thrift server and connecting to spark-sql through beeline is the recommended option for multi-session testing.

#### **Compression for Hive**

Set the following Hive parameters to compress the Hive output files using Snappy compression:

```
hive.exec.compress.output=true
hive.exec.orc.default.compress=SNAPPY
```

#### **Change the Log Directory for All Applications**

To change the default log from the /var prefix to /data/disk1, follow these steps:

- 1. Log into the cloudera home page and click My Clusters.
- 2. From the configuration drop-down list select "All Log Directories."
- 3. Click Save.

#### Summary

All NVMe PCIe based storage for Big Data and Analytics solution for various AI/ML workload and multiple applications which could scale to thousands of nodes and operational efficiency can't be an afterthought.

NVMe storage helps us achieve fast and parallel access to data reducing idle time for GPU and able to utilize resource in much more efficient way while reducing TCO by minimizing required hardware which saves in overall rack space, power, and cooling in the datacenter.

To achieve a seamless operation of the application at this scale, you need the following:

- Infrastructure automation of Cisco UCS servers with service profiles and Cisco Data Center network automation with application profiles with Cisco ACI.
- Centralized Management and Deep telemetry and Simplified granular trouble-shooting capabilities and 
  Multi-tenancy allowing application workloads including containers, micro-services, with the right level of
  security and SLA for each workload.
- Cisco UCS with Cisco Intersight and Cisco ACI can enable this cloud scale architecture deployed and managed with ease.
- CDP on CIDP delivers new approach to data where machine learning intelligently auto scale workloads up and down for more cost-effective use of private cloud infrastructure.

# **For More Information**

For additional information, see the following resources:

- To find out more about Cisco UCS big data solutions, see http://www.cisco.com/go/bigdata.
- To find out more about Cisco Data Intelligence Platform, see https://www.cisco.com/c/dam/en/us/products/servers-unified-computing/ucs-c-series-rackservers/solution-overview-c22-742432.pdf
- To find out more about Cisco UCS big data validated designs, see http://www.cisco.com/go/bigdata\_design
- To find out more about Cisco UCS AI/ML solutions, see http://www.cisco.com/go/ai-compute
- To find out more about Cisco ACI solutions, see http://www.cisco.com/go/aci
- To find out more about Cisco validated solutions based on Software Defined Storage, see https://www.cisco.com/c/en/us/solutions/data-center-virtualization/software-defined-storagesolutions/index.html
- Cloudera Data Platform Private Cloud Base 7.1.1 release note, see https://docs.cloudera.com/runtime/7.1.1/release-notes/index.html
- CDP Private Cloud Base Requirements and Supported Versions, see <a href="https://docs.cloudera.com/cdp-private-cloud-base/7.1.3/installation/topics/cdpdc-requirements-supported-versions.html">https://docs.cloudera.com/cdp-private-cloud-base/7.1.3/installation/topics/cdpdc-requirements-supported-versions.html</a>

# **Bill of Materials**

This section provides the bill of materials for the 28 Nodes Hadoop Base Rack. See <u>Table 13</u> for the bill of materials for the Hadoop Base rack and <u>Table 14</u> for Red Hat Enterprise Linux License.

Part Number	Description	Quantity
UCSC-C220-M5SN	Cisco UCS C220 M5 SFF 10 NVMe w/o CPU, mem, HD, PCIe, PSU	16
CON-SNT-C220M5SN	SNTC 8X5XNBD UCS C220 M5 SFF NVMe 10 HD w/o CPU, mem, HD, PC	16
UCS-MR-X32G2RT-H	32GB DDR4-2933-MHz RDIMM/2Rx4/1.2v	192
UCSC-NVMEHW-I8000	8TB 2.5in U.2 Intel P4510 NVMe High Perf. Value Endurance	160
UCSC-MLOM-C40Q-03	Cisco VIC 1387 Dual Port 40Gb QSFP CNA MLOM	16
UCS-M2-240GB	240GB SATA M.2	32
UCS-M2-HWRAID	Cisco Boot optimized M.2 Raid controller	16
CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	16
UCSC-PSU1-1050W	Cisco UCS 1050W AC Power Supply for Rack Server	32

Table 13Bill of Materials for Cisco UCS C240 M5SX Hadoop Nodes Base Rack

Part Number	Description	Quantity
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	32
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 & C240 M4 & M5 rack servers	16
UCS-SID-INFR-BD	Big Data and Analytics Platform (Hadoop/IoT/ITOA/AI/ML)	16
UCS-SID-WKL-BD	Big Data and Analytics (Hadoop/IoT/ITOA)	16
UCSC-HS-C220M5	Heat sink for UCS C220 M5 rack servers 150W CPUs & below	32
UCS-CPU-I6230R	Intel 6230R 2.1GHz/150W 26C/ 35MB DCP DDR4 2933 MHz	32
RHEL-2S2V-3A	Red Hat Enterprise Linux (1-2 CPU,1-2 VN); 3-Yr Support Req	16
CON-ISV1-EL2S2V3A	ISV 24X7 RHEL Server 2Socket-OR-2Virtual; ANNUAL List Price	16
RACK2-UCS2	Cisco R42612 standard rack, w/side panels	2
CON-SNT-RCK2UCS2	SNTC 8X5XNBD, Cisco R42612 standard rack, w side panels	2

# Å

### For NameNode, we configured ten 1.8TB 10K RPM SAS HDD.

#### Table 14 Red Hat Enterprise Linux License

Part Number	Description	Quantity
RHEL-2S2V-3A	Red Hat Enterprise Linux	30
CON-ISV1-EL2S2V3A	3-year Support for Red Hat Enterprise Linux	30

Æ

For Cloudera Data Platform Private Cloud Base (CDP PvC Base) software licensing requirement, contact <u>Cloudera Data Platform software - Sales</u>

# Appendix

# **Storage Policy in Intersight for Data Nodes**

To create a storage policy and server policy for a data node with RAID Controller (UCSC-RAID-M5 or UCSC-RAID-M5HD) with each disk configured in RAID 0, follow these steps:

1. In Cisco Intersight, click Policies. Select Disk Group.

	cisco Intersight	Policies		
<u>allo</u>		New features have recently been added! Learn More	Select Policy Type	×
			Q Search	
			Adapter Configuration	
6 <u>0</u>			O BIOS	
52				
			O Boot Order	
L©		CDID.BIOSDalles.Tematate	O Device Connector	
e			Oisk Group	
ास्त				
ा स्वत्र ()				
			Ethernet Network	
			C Ethernet QoS	

2. Enter the Organization, Name, Description and create a new tag or assign an existing tag. Click Next.

General	Organization * CDIP-C220M5SN ~
<ul> <li>Policy Details</li> </ul>	Name * R0-DG0
	Description RAID 0 policy for disk group 0
	Add Tag CDIP UCSC-C220-M5SN × ×

3. Select RAID Level as RAID0. In Local Disk Configuration for Disk Group (Span 0) and enter Slot Number 1.

Create Disk Group Policy		Q 🖬 1 🖸   🕫   Q,   🥸
	General     Policy Details	Virtual Drive Configuration RAID Level RAID0 v © Local Disk Configuration
		- Disk Group (Span 0) Slot Number * 1+
		Set Disks in JBCD state to Unconfigured Good <sup>©</sup>

- 4. Repeat steps 1–3 to create Disk Group for disks installed in slot 1–10, for example C240 M5 with 26 disks will require creation of 26 Disk groups and associate disk to each Disk Group.
- 5. Select Storage in Create Server Policy.

=		
<u>00o</u>	E New features have recently been added! Learn More	Select Policy Type
==		
æ		Fibre Channel QoS
- aia		O IPMI Over LAN
		O LAN Connectivity
6		O LDAP
1		O Local User
¢		
		Network Connectivity
		SAN Connectivity
		○ SD Card
		⊖ SMTP
		○ SNMP
		⊖ ssh
		O Serial Over LAN
		• Storage
		⊖ Syslog
		O Virtual KVM
	R0-DG5 Disk	

General	Organization * CDIP-C220M5SN ~
<ul> <li>Policy Details</li> </ul>	Name * R0-DG0
	Description RAID 0 policy for disk group 0
	Add Tag CDIP UCSC-C220-M5SN × ×

6. Select RAID Level as RAIDO. In Local Disk Configuration for Disk Group (Span 0) and enter Slot Number 1.

Create Disk Group Polic		Q∎1 [2] ¢\$   \$\$   \$\$   \$\$
	General     Policy Details	Virtual Drive Configuration RAID Level RAIDD v 0 Local Disk Configuration Disk Group (Span 0) Stot Number *
		Set Disks in JBCD state to Unconfigured Good <sup>©</sup> A. If the encryption is enabled in JBCD disks, the encryption will be disabled before they are used in virtual drive creation

- 7. Repeat steps 1–3 to create Disk Group for disks installed in slot 1–10, for example C240 M5 with 26 disks will require creation of 26 Disk groups and associate disk to each Disk Group.
- 8. Select Storage in Create Server Policy.

$\equiv$		
000	New features have recently been added! Learn More	Select Policy Type
		C Eikra Channal Natwark
##		
÷		O Fibre Channel QoS
F		O IPMI Over LAN
5		LAN Connectivity
a		
a		C Local User
ų reguli		○ NTP
		Network Connectivity
		O Persistent Memory
		O SAN Connectivity
		○ SD Card
		⊖ SMTP
		O SNMP
		⊖ ssh
		O Serial Over LAN
		Storage
		Svslog
		O Virtual KVM
	R0-DG5 Disk	

9. Click Create to complete Storage Policy creation for Data Nodes with each disk as RAID0.

# **Cisco UCS Rack Server Firmware Upgrade from Intersight**

A firmware upgrade can be performed via remote HUU (Host Upgrade Utility) ISO file mounted to Cisco IMC via NFS/CIFS/HTTP/HTTPS protocols or the server firmware can be upgraded through Utility Storage.

# Booting HUU from Cisco FlexUtil on Cisco UCS M5 servers and Cisco FlexFlash in Util mode on Cisco UCS M4 servers.

To upgrade from Intersight, follow these steps:

∕⊳⊾

1. From Intersight web UI console, go to Servers tab. Select server(s). Right-click and select Upgrade Firmware.

≡	ոկովս cisco Intersight	Servers							0   B	¢٦	Q,	© \$	Hardik P	Patel <u>&amp;</u>
<u>00</u> 0	Dashboards													
	Servers			0 Off 1 0 0n 3	Inco	status mplete 4		s		<ul> <li>Contract S</li> <li>Not Covere</li> </ul>	atus d 4	Server Prof	nies	
	Chassis	4 • Healthy	•					<ul> <li>C220 MS.</li> <li>C240 M5L</li> </ul>	2				Not Assig 2     Failed 1	
8	HyperFlex Clusters													
Ŧ	Fabric Interconnects	🧷 🔍 Search									I ∨ perpage			
6	Profiles	Power On		Contract Status	Man 🗘	Model 🗧		Mem 0	UCS Doma	HX Cluster	Serv C	Utility Stor	Firm	
e	Policies	Power Off	althy	Not Covered	10.1.9.30	UCSC-C2	89.6	192.0					4.1(1f)	
8	Orchestration	Power Cycle	althy		10.1.9.31	UCSC-C2	89.6	192.0					4.0(4h)	
٢	Administration ^	Shut Down OS		Not Covered	10.1.9.32	UCSC-C2	89.6	384.0					4.0(4h)	
	Devices	Reboot IMC	althy	Not Covered	10.1.9.33	UCSC-C2	89.6	384.0					4.0(4h)	
	Software Repository NEW	"Turn On Locator												
		Turn Off Locator												
		Upgrade Firmware												
		Install Operating System												

2. Select the Utility Storage tab and from the drop-down list select the firmware version. Click Upgrade Firmware.



3. Monitor upgrade process from the active list of task.

≡	الدان. cisco Intersight	Requests > Firmware upgrade - utility storage(upgrade on re	tooot)	(3) ⑦ Hardik Patel 요
<u>000</u>	Dashboards	Details	Execution Flow	
	Servers	Status 📀 Success	⊘ Update Inventory	
RR	Chassis	Name Firmware upgrade - utility storage(upgrade on re		
60	HyperFlex Clusters	ID 5eeb3e88696f6e2d30fb3db2 Target Type Rack Server	<ul> <li>Initiating Rimware Upgrade</li> <li>Upgrade on next reboot request placed successfully. Image-from: microsd</li> </ul>	Apr 30, 2020 2:37 PM
8	Fabric Interconnects	Target Name Truist-Intersight-C240-M5-1-CIMC	Monitoring and Waiting for Image Download to Complete in Endpoint     Download completed successfully	Apr 30, 2020 2:37 PM
@ []	Policies	Source Truist-intersignt-C240-MS-1-CIMC (Himware Up., Start Time Apr 30, 2020 2:09 PM	<ul> <li>Initiate Image Download to Endpoint</li> </ul>	Apr 30, 2020 2:09 PM
~	Orchestration	End Time Apr 30, 2020 2:38 PM Duration 28 m 39 s		
ē	Administration ^	Organization Truist		
	Devices			
	Software Repository <b>NEW</b>			

Once HUU ISO image is downloaded to local endpoint, the upgrade process starts after performing a Power Cycle or Host Reboot on the server, HUU is booted and upgrade begins on the server.

≡	cisco Intersight	Requests > Firmware upgrad	le monitor - server boot detected	û 🔺 3 💿 1 q⊄1 🔍 💿 💮 Hardik Patel &
<u>000</u>	Dashboards	Details		Execution Flow
36	Servers	Status	<ul> <li>In Progress</li> </ul>	Progress 0%
	Chassis	Name Firmware upgrade m	onitor - server boot detected	<ul> <li>Monitoring and Watting for Firmware Upgrade to Complete</li> <li>Apr 30, 2020 2:52 PM</li> <li>Update in progress BIOS IniProgress, CIMC IniProgress, UCS VIC 1457 IniProgress, UCSC-RAID-M5 Completed, X550-L0M IniProgress, UCS-M2-</li> </ul>
88	HyperFlex Clusters	Target Type	Rack Server	nwawu iiriugasa,

Upgrade process can be monitor from the list of active task.

≡	վիկին Intersight	Requests > Firmware upgrade monitor - server boot detected	a Û	ę1		Hardik Patel 🚊
<u>00</u> 0	Dashboards	Details	Execution Flow			
88	Servers	Status 📀 Success	Update Inventory			
	Chassis	Name Firmware upgrade monitor - server boot detected				
\$	HyperFlex Clusters	ID 5eab4615696f6e2d30fb4405	<ul> <li>Monitoring and Waiting for Firmware Upgrade to Complete</li> </ul>			
_		Target Type Rack Server				

# **Configure Cisco Nexus and Host for Active-Active Connections**

#### Port Configuration on Cisco Nexus 9332C

Table 15 lists the port configuration on Cisco UCS Nexus 9000 series switch.

Table 15 Port Configuration on Cisco UCS Nexus Switch						
Port Type	Port Number					
vPC Peer-Link	1-4 (for LACP)					
Network Uplink from C220 M5 to Nexus 9332C Switch	5-20					
Network Uplink from Cisco Nexus 9332C to Nexus 9504	21-32					

#### Configure vPC Domain and vPC Peer-Link on Pair of Cisco Nexus Switch

To configure Nexus A, follow these steps:

1. Connect to the console port or management port on the first Cisco Nexus 9332C-A. Complete the initial setup. 2. Enable feature VPC and configure VPC domain.

```
# config terminal
# feature vpc
# feature lacp
# vpc domain 100
# peer-keepalive destination 173.37.52.67 source 173.37.52.66
# exit
```

#### Enable feature lacp for mode 4 based bond configuration.

- 3. Connect to the console port or management port on the second Cisco Nexus 9332C-B.
- 4. Enable feature VPC and configure VPC domain. Configure peer nexus for keep alive.

```
# config terminal
# feature vpc
# feature lacp
# vpc domain 100
# peer-keepalive destination 173.37.52.66 source 173.37.52.67
# exit
```

5. On both Nexus Switch, create interface port channel (we use 100 here for example), for VPC peer link. Configure the port channel for allowed VLAN (VLAN 14 in the example below).

```
# interface port-channel100
# description vpc-peerlink
# switchport mode trunk
# switchport trunk allowed vlan 14
# spanning-tree port type network
# vpc-peer-link
```

6. Configure the interconnected ports on both Nexus switches and add them in port-channel 100 created for vPC-peerlink.

```
# interface Ethernet1/1
# switchport mode trunk
# switchport trunk allowed vlan 14
# spanning-tree port type network
# channel-group 100
# no shutdown
# interface Ethernet1/2
# switchport mode trunk
# switchport trunk allowed vlan 14
# spanning-tree port type network
# channel-group 100
# no shutdown
# interface Ethernet1/3
# switchport mode trunk
# switchport trunk allowed vlan 14
```

```
# spanning-tree port type network
# channel-group 100
# no shutdown
# interface Ethernet1/4
# switchport mode trunk
# switchport trunk allowed vlan 14
# spanning-tree port type network
# channel-group 100
# no shutdown
```

7. Configure the ethernet interfaces on both Nexus switches to be part of port channels connected to northbound switch in spine-leaf architecture or ToR switch. Ports 1 through 6 and 27 through 32 were configured part of interface port-channel 50.

```
interface port-channel50
 description NB_TOR_N9K
 switchport mode trunk
 switchport trunk allowed vlan 14
 spanning-tree port type network
 mtu 9216
interface Ethernet1/27
 description K14-N9K-P19-24
 switchport mode trunk
 switchport trunk allowed vlan 14
 spanning-tree port type network
 mtu 9216
 channel-group 50 mode active
interface Ethernet1/28
 description K14-N9K-P19-24
```

```
switchport mode trunk
switchport trunk allowed vlan 14
spanning-tree port type network
mtu 9216
channel-group 50 mode active
```

8. Create the port-channel between Cisco UCS C220 M5 server VIC interface connected to each Nexus switch. Port 9-24 is configured in the port-channel with the corresponding vpc id for mod 4.

```
interface port-channel51
  description DataNode01
  switchport access vlan 14
  spanning-tree port type edge
  mtu 9216
  vpc 51
interface port-channel52
  description DataNode02
  switchport access vlan 14
  spanning-tree port type edge
  mtu 9216
  vpc 52
interface Ethernet1/9
```

```
description Connected to Server DataNode01
switchport access vlan 14
spanning-tree port type edge
mtu 9216
channel-group 51 mode active
interface Ethernet1/10
description Connected to Server DataNode02
switchport access vlan 14
spanning-tree port type edge
mtu 9216
channnel-group 52 mode active
```

9. Create the port-channel between Cisco UCS C220 M5 server VIC interface connected to each Nexus switch. Port 9-24 is configured in the port-channel.

```
interface port-channel51
  description DataNode01
  switchport access vlan 14
 spanning-tree port type edge
 mtu 9216
 vpc 51
interface port-channel52
  description DataNode02
 switchport access vlan 14
 spanning-tree port type edge
 mtu 9216
 vpc 52
interface Ethernet1/9
  description Connected to Server rhel01
  switchport access vlan 14
  spanning-tree port type edge
 mtu 9216
interface Ethernet1/10
  description Connected to Server rhel02
  switchport access vlan 14
  spanning-tree port type edge
 mtu 9216
```

#### **Configure Network and Bond Interfaces for Mode 4**

To configure the network and bond interfaces, follow these steps:

- 1. Setup /etc/sysconfig/ifcfg-bond0. Configure the two VNIC interfaces as slave interfaces to the bond interface.
- 2. Run the following to configure bond on for each Name Node and Data Node:

```
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-bond0
DEVICE=bond0
NAME=bond0
TYPE=Bond
BONDING_MASTER=yes
IPADDR=10.14.1.45
```

```
NETMASK=255.255.255.0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
USERCTL=no
BONDING OPTS="miimon=100 mode=4"
NM CONTROLLED=no
MTU="9000"
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno5
TYPE=Ethernet
BOOTPROTO=none
NAME=bond0-slave1
DEVICE=eno5
ONBOOT=no
MASTER=bond0
SLAVE=yes
NM CONTROLLED=no
HOTPLUG=no
USERCTL=no
MTU="9000"
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno6
TYPE=Ethernet
BOOTPROTO=none
NAME=bond0-slave6
DEVICE=eno6
ONBOOT=no
MASTER=bond0
SLAVE=yes
NM CONTROLLED=no
HOTPLUG=no
USERCTL=no
MTU="9000"
[root@rhelnn01 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default
glen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid lft forever preferred lft forever
2: eno5: <BROADCAST,MULTICAST,SLAVE,UP,LOWER UP> mtu 9000 qdisc mq master bond0
state UP group default glen 1000
    link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff
3: eno6: <BROADCAST,MULTICAST,SLAVE,UP,LOWER UP> mtu 9000 qdisc mq master bond0
state UP group default glen 1000
    link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff:ff
4: eno1: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc mq state DOWN group
default glen 1000
    link/ether 38:0e:4d:7d:b7:f2 brd ff:ff:ff:ff:ff
5: eno2: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc mq state DOWN group
default glen 1000
    link/ether 38:0e:4d:7d:b7:f3 brd ff:ff:ff:ff:ff
6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER UP> mtu 9000 gdisc noqueue state UP
group default glen 1000
    link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff
```
inet 10.14.1.45/24 brd 10.14.1.255 scope global bond0
 valid\_lft forever preferred\_lft forever



#### BONDING\_OPTS="miimon=100 mode=4" for link aggregated bond configuration.

#### **Configure Network and Bond Interfaces for mode 6**

To configure the network and bond interfaces, follow these steps:

- 1. Setup /etc/sysconfig/ifcfg-bond0. Configure the two VNIC interfaces as slave interfaces to the bond interface.
- 2. Run the following to configure bond on for each Name Node and Data Node:

```
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-bond0
DEVICE=bond0
NAME=bond0
TYPE=Bond
BONDING MASTER=yes
IPADDR=10.14.1.45
NETMASK=255.255.255.0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
USERCTL=no
BONDING OPTS="miimon=100 mode=6"
NM CONTROLLED=no
MTU="9000"
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno5
TYPE=Ethernet
BOOTPROTO=none
NAME=bond0-slave1
DEVICE=eno5
ONBOOT=no
MASTER=bond0
SLAVE=yes
NM CONTROLLED=no
HOTPLUG=no
USERCTL=no
MTU="9000"
[root@rhelnn01 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eno6
TYPE=Ethernet
BOOTPROTO=none
NAME=bond0-slave6
DEVICE=eno6
ONBOOT=no
MASTER=bond0
SLAVE=yes
NM CONTROLLED=no
HOTPLUG=no
USERCTL=no
MTU="9000"
[root@rhelnn01 ~]# ip addr
```

1: lo: <LOOPBACK,UP,LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid lft forever preferred lft forever 2: eno5: <BROADCAST,MULTICAST,SLAVE,UP,LOWER UP> mtu 9000 qdisc mq master bond0 state UP group default glen 1000 link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff 3: eno6: <BROADCAST,MULTICAST,SLAVE,UP,LOWER UP> mtu 9000 qdisc mq master bond0 state UP group default glen 1000 link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff:ff 4: eno1: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc mq state DOWN group default glen 1000 link/ether 38:0e:4d:7d:b7:f2 brd ff:ff:ff:ff:ff:ff 5: eno2: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc mq state DOWN group default qlen 1000 link/ether 38:0e:4d:7d:b7:f3 brd ff:ff:ff:ff:ff:ff 6: bond0: <BROADCAST,MULTICAST,MASTER,UP,LOWER UP> mtu 9000 qdisc noqueue state UP group default glen 1000 link/ether 38:0e:4d:b5:49:d6 brd ff:ff:ff:ff:ff:ff inet 10.14.1.45/24 brd 10.14.1.255 scope global bond0 valid lft forever preferred lft forever

### BONDING\_OPTS="miimon=100 mode=6" for balanced-alb bond configuration.

# About the Authors

Sarath Gonugunta, Technical Marketing Engineer, Computing Systems Product Group, Cisco Systems, Inc.

Sarath Gonugunta is a Technical Marketing Engineer in the Cisco Computing Systems Product Group. He is part of the Cisco UCS Solutions Engineering team currently focusing on Big Data infrastructure, solutions, and performance.

Hardik Patel, Technical Marketing Engineer, Computing Systems Product Group, Cisco Systems, Inc.

Hardik Patel is a Big Data Solutions Architect in the Computing Systems Product Group. He is part of the Cisco UCS Solution Engineering team focusing on Big Data infrastructure, solutions, and performance.

## **Acknowledgements**

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Karthik Kulkarni, Architect, Computing Systems Product Group, Cisco Systems, Inc.
- Muhammad Afzal, Architect, Computing Systems Product Group, Cisco Systems, Inc.