Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub
With optional guidelines for Scaling with Cisco Application Centric Infrastructure (ACI)

Last Updated: May 22, 2015
About the Authors

**Raghunath Nambiar, Distinguished Engineer, Data Center Business Group (Cisco Systems)**

Raghunath Nambiar is a Distinguished Engineer at Cisco's Data Center Business Group. His current responsibilities include emerging technologies and big data strategy.

**Karthik Kulkarni, Technical Marketing Engineer, Data Center Solutions Group (Cisco Systems)**

Karthik Kulkarni is a Technical Marketing Engineer in the Data Center Solutions Group at Cisco Systems. He is part of solution engineering team focusing on big data infrastructure and performance.

**Manankumar Trivedi, Technical Marketing Engineer, Data Center Solutions Group (Cisco Systems)**

Manankumar Trivedi is a Technical Marketing Engineer in the Data Center Solutions Group at Cisco Systems. He is part of solution engineering team focusing on big data infrastructure and performance.
About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit 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 DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.
Acknowledgment

The authors acknowledge the contributions of Amrit Kharel, Ashwin Manjunatha, and Sindhu Sudhir in developing this document.
Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub

Audience

This document describes the architecture and deployment procedures of Cloudera on Cisco UCS Integrated Infrastructure for Big Data with Application Centric Infrastructure (ACI). The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering and customers who want to deploy Cloudera on Cisco UCS Integrated Infrastructure for Big Data with Application Centric Infrastructure (ACI).

Introduction

Hadoop has become a strategic data platform embraced by mainstream enterprises as it offers the fastest path for businesses to unlock value in big data while maximizing existing investments. Cloudera is the leading provider of enterprise-grade Hadoop infrastructure software and services, and the leading contributor to the Apache Hadoop project overall. Cloudera provides an enterprise-ready Hadoop-based solution known as Cloudera Enterprise, which includes their market leading open source Hadoop distribution (CDH), their comprehensive management system (Cloudera Manager), and technical support. The combination of Cisco UCS Servers along with Application Centric Infrastructure (ACI) provides an industry-leading platform for Hadoop based applications.

This solution is based on Cisco UCS Integrated Infrastructure for Big Data with Application Centric Infrastructure (ACI), with multiple Cisco UCS Fabric Interconnect domains. Each Fabric Interconnect domain consists of 5 racks of servers (total of 80 Cisco UCS C240 M4 servers) along with a pair of Fabric Interconnect. These domains are inter-connected through ACI.

Cisco UCS Integrated Infrastructure for Big Data

The Cisco UCS solution for Cloudera is based on Cisco UCS Integrated Infrastructure for Big Data, 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 following components:
Cisco UCS 6200 Series Fabric Interconnects

Cisco UCS 6200 Series Fabric Interconnects provide high-bandwidth, low-latency connectivity for servers, with integrated, unified management provided for all connected devices by Cisco UCS Manager. Deployed in redundant pairs, Cisco fabric interconnects offer the full active-active redundancy, performance, and exceptional scalability needed to support the large number of nodes that are typical in clusters serving big data applications. Cisco UCS Manager enables rapid and consistent server configuration using service profiles, automating ongoing system maintenance activities such as firmware updates across the entire cluster as a single operation. Cisco UCS Manager also offers advanced monitoring with options to raise alarms and send notifications about the health of the entire cluster.

Figure 1  Cisco UCS 6296UP 96-Port Fabric Interconnect

Cisco UCS C-Series Rack Mount Servers

Cisco UCS C-Series Rack Mount C220 M4 High-Density Rack servers (Small Form Factor Disk Drive Model) and Cisco UCS C240 M4 High-Density Rack servers (Small Form Factor Disk Drive Model) are enterprise-class systems that support a wide range of computing, I/O, and storage-capacity demands in compact designs. Cisco UCS C-Series Rack-Mount Servers are based on Intel Xeon E5-2600 v3 product family and 12-Gbps SAS throughput, delivering significant performance and efficiency gains over the previous generation of servers. The servers use dual Intel Xeon processor E5-2600 v3 series CPUs and support up to 768 GB of main memory (128 or 256 GB is typical for big data applications) and a range of disk drive and SSD options. 24 Small Form Factor (SFF) disk drives are supported in performance-optimized option and 12 Large Form Factor (LFF) disk drives are supported in capacity-optimized option, along with 4 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Cisco UCS virtual interface cards 1227 (VICs) designed for the M4 generation of Cisco UCS C-Series Rack Servers are optimized for high-bandwidth and low-latency cluster connectivity, with support for up to 256 virtual devices that are configured on demand through Cisco UCS Manager.
Cisco UCS Virtual Interface Cards (VICs)

Cisco UCS Virtual Interface Cards (VICs), unique to Cisco, incorporate next-generation converged network adapter (CNA) technology from Cisco, and offer dual 10-Gbps ports designed for use with Cisco UCS C-Series Rack-Mount 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 (VIC) 1227 is a dual-port, Enhanced Small Form-Factor Pluggable (SFP+), 10 Gigabit Ethernet and Fiber Channel over Ethernet (FCoE)-capable, PCI Express (PCIe) modular LAN on motherboard (mLOM) adapter. It is designed exclusively for the M4 generation of Cisco UCS C-Series Rack Servers and the C3160 dense storage servers.

Cisco UCS Manager

Cisco UCS Manager resides within the Cisco UCS 6200 Series Fabric Interconnects. It makes the system self-aware and self-integrating, managing all of the system components as a single logical entity. Cisco UCS Manager can be accessed through an intuitive graphical user interface (GUI), a command-line interface (CLI), or an XML application-programming interface (API). Cisco UCS Manager uses service profiles to define the personality, configuration, and connectivity of all resources within Cisco UCS,
radically simplifying provisioning of resources so that the process takes minutes instead of days. This simplification allows IT departments to shift their focus from constant maintenance to strategic business initiatives.

Cloudera’s Distribution Including Apache Hadoop (CDH) 5.3.2

Built on the transformative Apache Hadoop open source software project, Cloudera Enterprise is an hardened distribution of Apache Hadoop and related projects that are designed to meet the demanding needs of enterprise customers. Cloudera is one of the largest contributors to the Hadoop ecosystem, and has created a rich suite of complementary open source projects that are included in Cloudera Enterprise.
All the facets of integration and the entire solution is thoroughly tested and documented. The readily available pre-integrated solution in CDH helps in building your Hadoop deployment model with ease. CDH provides a coherent and practical solution to solve real business problems.

Cloudera Enterprise, with Apache Hadoop at the core, is:

- **Unified** – one integrated system, bringing diverse users and application workloads to one pool of data on common infrastructure; no data movement required
- **Secure** – perimeter security, authentication, granular authorization, and data protection
- **Governed** – enterprise-grade data auditing, data lineage, and data discovery
- **Managed** – native high-availability, fault-tolerance and self-healing storage, automated backup and disaster recovery, and advanced system and data management
- **Open** – Apache-licensed open source to ensure your data and applications remain yours, and an open platform to connect with all of your existing investments in technology and skills

Figure 5  Enterprise Data Hub Architecture by Cloudera

Cloudera provides a scalable, flexible, integrated platform that makes it easy to manage rapidly increasing volumes and varieties of data in your enterprise. Industry-leading Cloudera products and solutions enable you to deploy and manage Apache Hadoop and related projects, manipulate and analyze your data, and keep that data secure and protected.

Cloudera provides the following products and tools:

- **CDH**—The Cloudera distribution of Apache Hadoop and other related open-source projects, including Cloudera Impala and Cloudera Search. CDH also provides security and integration with numerous hardware and software solutions.
  - **Cloudera Impala**—A massively parallel processing SQL engine for interactive analytics and business intelligence. Its highly optimized architecture makes it ideally suited for traditional BI-style queries with joins, aggregations, and subqueries. It can query Hadoop data files from a variety of sources, including those produced by MapReduce jobs or loaded into Hive tables. The YARN and Llama resource management components let Impala coexist on clusters running batch workloads concurrently with Impala SQL queries. You can manage Impala alongside other Hadoop components through the Cloudera Manager user interface, and secure its data through the Sentry authorization framework.
  - **Cloudera Search**—Provides near real-time access to data stored in or ingested into Hadoop and HBase. Search provides near real-time indexing, batch indexing, full-text exploration and navigated drill-down, as well as a simple, full-text interface that requires no SQL or
programming skills. Fully integrated in the data-processing platform, Search uses the flexible, scalable, and robust storage system included with CDH. This eliminates the need to move large data sets across infrastructures to perform business tasks.

- **Cloudera Manager**—A sophisticated application used to deploy, manage, monitor, and diagnose issues with your CDH deployments. Cloudera Manager provides the Admin Console, a web-based user interface that makes administration of your enterprise data simple and straightforward. It also includes the Cloudera Manager API, which you can use to obtain cluster health information and metrics, as well as configure Cloudera Manager.

- **Cloudera Navigator**—An end-to-end data management tool for the CDH platform. Cloudera Navigator enables administrators, data managers, and analysts to explore the large amounts of data in Hadoop. The robust auditing, data management, lineage management, and life cycle management in Cloudera Navigator allow enterprises to adhere to stringent compliance and regulatory requirements.

## Cisco Application Centric Infrastructure (ACI) Overview

ACI provides network the ability to deploy and respond to the needs of applications, both in the data center and in the cloud. The network must be able to deliver the right levels of connectivity, security, compliance, firewalls, and load balancing, and it must be able to do this dynamically and on-demand. This is accomplished through centrally defined policies and application profiles. The profiles are managed by new Application Policy Infrastructure Controller (APIC) and distributed to switches like the Cisco Nexus 9000 Series. Cisco Nexus 9000 Series Switches and the Cisco Application Policy Infrastructure Controller (APIC) are the building blocks for ACI.

ACI is software-defined networking (SDN) plus a whole lot more. Most SDN models stop at the network. ACI extends the promise of SDN—namely agility and automation—to the applications themselves. Through a policy-driven model, the network can cater to the needs of each application, with security, network segmentation, and automation at scale. And it can do so across physical and virtual environments, with a single pane of management.

The ACI fabric supports more than 64,000 dedicated tenant networks. A single fabric can support more than one million IPv4/IPv6 endpoints, more than 64,000 tenants, and more than 200,000 10G ports. The ACI fabric enables any service (physical or virtual) anywhere with no need for additional software or hardware gateways to connect between the physical and virtual services and normalizes encapsulations for Virtual Extensible Local Area Network (VXLAN) / VLAN / Network Virtualization using Generic Routing Encapsulation (NVGRE).

The ACI fabric decouples the endpoint identity and associated policy from the underlying forwarding graph. It provides a distributed Layer 3 gateway that ensures optimal Layer 3 and Layer 2 forwarding. The fabric supports standard bridging and routing semantics without standard location constraints (any IP address anywhere), and removes flooding requirements for the IP control plane Address Resolution Protocol (ARP) / Generic Attribute Registration Protocol (GARP). All traffic within the fabric is encapsulated within VXLAN.
Architectural Benefits of using Fabric Interconnect with Cisco ACI

UCS Servers are connected directly to Fabric Interconnect (FI) which in-turn connects to ACI (N9K switches). This mode allows using the UCS Manager capabilities in FI for provisioning the servers within a domain. This topology can scale up to 5760 servers for a fully populated pair of Nexus 9508s with all the eight linecards; details of which are discussed in “Scaling section”. Benefits of ACI architecture are discussed in the next section.

Centralized Management for the Entire Network

Cisco ACI treats the network as a single entity rather than a collection of switches. It uses a central controller to implicitly automate common practices such as Cisco ACI fabric startup, upgrades, and individual element configuration. The Cisco Application Policy Infrastructure Controller (Cisco APIC) is this unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric. This architectural approach dramatically increases the operational efficiency of networks, by reducing the time and effort needed to make modifications to the network and, also, for root cause analysis and issue resolution.

Performance Oriented Fabric

The Cisco ACI Fabric incorporates numerous capabilities that can help provide performance improvements to applications.

Dynamic Load Balancing (DLB): The ACI fabric provides several load balancing options for balancing the traffic among the available uplinks. Static hash load balancing is the traditional load balancing mechanism used in networks where each flow is allocated to an uplink based on a hash of its 5-tuple. This load balancing gives a distribution of flows across the available links that is roughly even. Usually, with a large number of flows, the even distribution of flows results in an even distribution of bandwidth as well. However, if a few flows are much larger than the rest, static load balancing might give suboptimal results. Dynamic load balancing (DLB) adjusts the traffic allocations according to congestion levels. It measures the congestion across the available paths and places the flows on the least congested paths, which results in an optimal or near optimal placement of the data.

Dynamic Packet Prioritization (DPP), while not a load balancing technology, uses some of the same mechanisms as DLB in the switch. DPP configuration is exclusive of DLB. DPP prioritizes short flows higher than long flows; a short flow is less than approximately 15 packets. Short flows are more sensitive to latency than long ones. DPP can improve overall application performance.

Together these technologies enable performance enhancements to applications, including Big Data workloads. More information on these technologies and results associated with performance analysis can be found in the following paper that recently won the best paper award at ACM SIGCOMM 2014:
Application-Centric Policy Model

The Cisco ACI policy model is designed top down using a promise theory model to control a scalable architecture of defined network and service objects. This model provides robust repeatable controls, multitenancy, and minimal requirements for detailed knowledge by the control system known as the Cisco APIC. The model is designed to scale beyond current needs to the needs of private clouds, public clouds, and software-defined data centers.

The policy enforcement model within the fabric is built from the ground up in an application-centric object model. This provides a logical model for laying out applications, which will then be applied to the fabric by the Cisco APIC. This helps to bridge the gaps in communication between application requirements and the network constructs that enforce them. The Cisco APIC model is designed for rapid provisioning of applications on the network that can be tied to robust policy enforcement while maintaining a workload anywhere approach.

Multi-Tenant and Mixed Workload Support

Cisco ACI is built to incorporate secure multi-tenancy capabilities. The fabric enables customers to host multiple concurrent Big Data workloads on a shared infrastructure. ACI provides the capability to enforce proper isolation and SLA’s for workloads of different tenants. These benefits extend beyond multiple Big Data workloads – Cisco ACI allows the same cluster to run a variety of different application workloads, not just Big Data, with the right level of security and SLA for each workload.

Extensibility and Openness

ACI supports an open ecosystem embracing open APIs, open source, and open standards. This provides the broadest choice in data center management and infrastructure. ACI supports embracing open APIs, open source, and open standards. This provides the broadest choice in data center management and infrastructure.

Easy Migration to 40Gbps in the Network

Cisco QSFP BiDi technology removes 40-Gbps cabling cost barriers for migration from 10-Gbps to 40-Gbps connectivity in data center networks. Cisco QSFP BiDi transceivers provide 40-Gbps connectivity with immense savings and simplicity compared to other 40-Gbps QSFP transceivers. The Cisco QSFP BiDi transceiver allows organizations to migrate the existing 10-Gbps cabling infrastructure to 40 Gbps at no cost and to expand the infrastructure with low capital investment. Together with Cisco Nexus 9000 Series Switches, which introduce attractive pricing for networking devices, Cisco QSFP BiDi technology provides a cost-effective solution for migration from 10-Gbps to 40-Gbps infrastructure.

Cisco ACI Building blocks

Cisco ACI consists of:

- The Cisco Nexus 9000 Series Switches.
- A centralized policy management and Cisco Application Policy Infrastructure Controller (APIC).
Cisco Nexus 9000 Series Switches

The 9000 Series Switches offer both modular (9500 switches) and fixed (9300 switches) 1/10/40/100 Gigabit Ethernet switch configurations designed to operate in one of two modes:

- Cisco NX-OS mode for traditional architectures and consistency across the Cisco Nexus portfolio.
- ACI mode to take full advantage of the policy-driven services and infrastructure automation features of ACI.

The ACI-Ready Cisco Nexus 9000 Series provides:

- Accelerated migration to 40G: zero cabling upgrade cost with Cisco QSFP+ BiDi Transceiver Module innovation.
- Switching platform integration: Nexus 9000 Series enables a highly scalable architecture and is software upgradable to ACI.
- Streamline Application Management: Drastically reduce application deployment time and get end to end application visibility.

This architecture consists of Cisco Nexus 9500 series switches acting as the spine and Cisco Nexus 9300 series switches as leaves.

Cisco Nexus 9508 Spine Switch

The Cisco Nexus 9508 Switch offers a comprehensive feature set, high resiliency, and a broad range of 1/10/40 Gigabit Ethernet line cards to meet the most demanding requirements of enterprise, service provider, and cloud data centers. The Cisco Nexus 9508 Switch is an ACI modular spine device enabled by a non-blocking 40 Gigabit Ethernet line card, supervisors, system controllers, and power supplies.

The Cisco Nexus 9500 platform internally uses a Clos fabric design that interconnects the line cards with rear-mounted fabric modules. The Cisco Nexus 9500 platform supports up to six fabric modules, each of which provides up to 10.24-Tbps line-rate packet forwarding capacity. All fabric cards are directly connected to all line cards. With load balancing across fabric cards, the architecture achieves optimal bandwidth distribution within the chassis.
ACI Spine Line Card for Cisco Nexus 9508

There are multiple spine line cards supported on Nexus 9508. This architecture uses N9K-X9736PQ: 40 Gigabit Ethernet ACI Spine Line Card.

- 36-port 40 Gigabit Ethernet QSFP+ line card
- Non-blocking
- Designed for use in an ACI spine switch role
- Works only in ACI mode
- Cannot mix with non-spine line cards
- Supported in 8-slot chassis

Cisco Nexus 9396 Leaf Switch

The Cisco Nexus 9396PX Switch delivers comprehensive line-rate layer 2 and layer 3 features in a two-rack-unit (2RU) form factor. It supports line rate 1/10/40 GE with 960 Gbps of switching capacity. It is ideal for top-of-rack and middle-of-row deployments in both traditional and Cisco Application Centric Infrastructure (ACI)–enabled enterprise, service provider, and cloud environments.
Cisco ACI Building blocks

Cisco Application Policy Infrastructure Controller (APIC)

The Application Centric Infrastructure is a distributed, scalable, multitenant infrastructure with external end-point connectivity controlled and grouped through application-centric policies. The APIC is the unified point of automation, management, monitoring, and programmability for the Cisco Application Centric Infrastructure. The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for physical and virtual components of the infrastructure. The APIC programmatically automates network provisioning and Control that is based on the application requirements and policies. It is the central control engine for the broader cloud network; it simplifies management and allows flexibility in how application networks are defined and automated. It also provides northbound REST APIs. The APIC is a distributed system that is implemented as a cluster of many controller instances.

ACI Topology

ACI topology is spine-leaf architecture. Each leaf is connected to each spine. It uses internal routing protocol; Intermediate System to Intermediate System (IS-IS) to establish IP connectivity throughout the fabric among all the nodes including spine and leaf. To transport tenant traffic across the IP fabric, integrated VxLAN overlay is used. The broadcast ARP traffic coming from the end point or hosts to the leaf are translated to unicast ARP in the fabric.

The forwarding is done as a host based forwarding. In the leaf layer the user information such as username, IP address, locations, policy groups etc., are decoupled from the actual forwarding path and encode them into the fabric VxLAN header and is forwarded to the desired destination.

Each spine has the complete forwarding information about the end hosts that are connected to the fabric and on every leaf have the cached forwarding information. The leaf only needs to know the hosts it needs to talk to. For example if Server Rack-1 has to send some information to Server Rack-2, When packet comes in the ingress leaf (LEAF_1) it will encapsulate the information into the VxLAN header and
forward that information to LEAF_2. If the LEAF_1 does not have information about the LEAF_2, it uses Spine as a proxy and since Spine has all the complete information about the entire end host connected to the fabric, it will resolve the egress leaf and forward the packet to the destination.

To the outside world, routing protocols can be used to learn outside prefixes or static routing can be used instead. The outside learned routes will be populated into the fabric or to the other leaves with Multiprotocol BGP (M-BGP). In M-BGP topology the spine nodes acts as route reflectors.

The Network topology of ACI is as depicted below:

The Cisco ACI infrastructure incorporates the following components:

- Two Cisco Nexus 9508 Spine Switch
  - ACI Spine Line Card for Nexus 9508
- Cisco Nexus 9396 Leaf Switch for Data Traffic
- Cisco APIC-L1-Cluster with three APIC-L1 appliances

**Solution Overview**

This CVD describes architecture and deployment procedures for Cloudera (CDH 5.3.2) on 160 Cisco UCS C240 M4 server based on Cisco UCS Integrated Infrastructure for Big Data with two domains (each Fabric-Interconnect domain has 80 servers under a pair of Fabric Interconnect) interconnected through ACI. The Cisco UCS Integrated Infrastructure with ACI brings together a highly scalable architecture designed to meet a variety of scale-out application demands with seamless data integration and management integration capabilities.

**Note**

System Architecture and Scaling sections discussed below describe three Cisco UCS Fabric Interconnect domains under a pair for Cisco Nexus 9396.

Further, the CVD describes in detail the process of creating the Application Network Profile in the ACI for Big Data application. Application Network Profiles (Application Network Profile is a collection of EPGs, their connections, and the policies that define those connections described in detail later) are the logical representation of an application (here Big Data) and its interdependencies in the network fabric.
Application Network Profiles are designed to be modeled in a logical way that matches the way that applications are designed and deployed. The configuration and enforcement of policies and connectivity is handled by the system rather than manually by an administrator.

The current version of the Cisco UCS Integrated Infrastructure for Big Data offers the following configuration depending on the compute and storage requirements:

This CVD uses Performance Optimized configuration.

This CVD describes the install process of CDH 5.3.2 for a 160 node (3 Master nodes in High Availability + 157 Data node) of Performance Optimized Cluster configuration.

The Performance cluster configuration consists of the following:

- Four Cisco UCS 6296UP Fabric Interconnects
- 160 UCS C240 M4 Rack-Mount servers (16 per rack)
- Ten Cisco R42610 standard racks
- Eighteen Vertical Power distribution units (PDUs) (Country Specific)
- Two Cisco Nexus 9508 Spine Switch
  - ACI Spine Line Card for Nexus 9508
- Cisco Nexus 9396 Leaf Switch for Data Traffic
- Cisco APIC-L1-Cluster with three APIC-L1 appliances

### Table 1  Compute Nodes used for the Big Data Cluster with ACI

<table>
<thead>
<tr>
<th>Performance Optimized</th>
<th>Capacity Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 Cisco UCS C240 M4 Rack Servers (SFF), each with:</td>
<td>16 Cisco UCS C240 M4 Rack Servers (LFF), each with:</td>
</tr>
<tr>
<td>2 Intel Xeon processors E5-2680 v3 CPUs</td>
<td>2 Intel Xeon processors E5-2620 v3 CPUs</td>
</tr>
<tr>
<td>256 GB of memory</td>
<td>128 GB of memory</td>
</tr>
<tr>
<td>Cisco 12-Gbps SAS Modular Raid Controller with 2-GB flash-based write cache (FBWC)</td>
<td>Cisco 12-Gbps SAS Modular Raid Controller with 2-GB FBWC</td>
</tr>
<tr>
<td>24 1.2-TB 10K SFF SAS drives (460 TB total)</td>
<td>12 4-TB 7.2K LFF SAS drives (768 TB total)</td>
</tr>
<tr>
<td>2 120-GB 6-Gbps 2.5-inch Enterprise Value SATA SSDs for Boot</td>
<td>2 120-GB 6-Gbps 2.5-inch Enterprise Value SATA SSDs for Boot</td>
</tr>
<tr>
<td>Cisco UCS VIC 1227 (with 2 10 GE SFP+ ports)</td>
<td>Cisco UCS VIC 1227 (with 2 10 GE SFP+ ports)</td>
</tr>
</tbody>
</table>

### Table 2  Hardware Component Details

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Role</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NK-C9508</td>
<td>Spine</td>
<td>2</td>
</tr>
</tbody>
</table>

Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub
Physical Layout for the Solution

Physical Layout for the solution is as shown in the following table. Each rack consists of two vertical PDUs. The solution consists of 5 Cisco R42610 racks. The Nexus 9396 leaf switch and the Fabric Interconnect is distributed across rack1 and rack2, the APIC appliances are distributed across rack2 to rack4. Similarly, Nexus 9508 Spine switch is mounted in rack2 for easier cabling between the spine and leaf switches. The rest of the spaces in the 5 racks are used for mounting 80 servers. All the Switches and UCS Servers are dual connected to vertical PDUs for redundancy; thereby, ensuring availability during power source failure.

For second pod, only two FI’s are required in this domain because the uplink from the FI is connected to the leaf switches in pod1 and rest of the space is used to mount another 80 servers.

Table 3  Rack 1-5

<table>
<thead>
<tr>
<th>Slot</th>
<th>Rack 1</th>
<th>Rack 2</th>
<th>Rack 3</th>
<th>Rack 4</th>
<th>Rack 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N9K-C9396PX</td>
<td>N9K-C9396PX</td>
<td>APIC-L1</td>
<td>APIC-L1</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>FI-A</td>
<td>FI-B</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>UCS C240M4</td>
<td></td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td>UC C240M4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>UCS C240M4</td>
<td></td>
<td>UC C240M4</td>
<td>UC C240M4</td>
<td>UC C240M4</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note

For more details on Connecting Application Centric Infrastructure (ACI) to Outside Layer 2 and 3 Networks can be found at:
### Table 3  Rack 1-5

<table>
<thead>
<tr>
<th></th>
<th>UCS C240M4</th>
<th>UCS C240M4</th>
<th>UCS C240M4</th>
<th>UCS C240M4</th>
<th>UCS C240M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>UCS C240M4</td>
<td>N9k-C9508</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>UCS C240M4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4  Rack 1-5

<table>
<thead>
<tr>
<th>Slot</th>
<th>Rack 1</th>
<th>Rack 2</th>
<th>Rack 3</th>
<th>Rack 4</th>
<th>Rack 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FI-C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>FI-D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
<td>UCS C240M4</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Software Distributions and Versions

The software distribution’s required versions are listed below.

### Cloudera Enterprise

The Cloudera software for Cloudera Distribution for Apache Hadoop is version 5.3.2. For more information on CDH, visit: [www.cloudera.com](http://www.cloudera.com)

### Red Hat Enterprise Linux (RHEL)

The operating system supported is Red Hat Enterprise Linux 6.5. For more information on RHEL, visit: [http://www.redhat.com](http://www.redhat.com)

### Software Versions

The software versions tested and validated in this document are shown in Table 5.
System Architecture

The ACI fabric consists of three major components: the Application Policy Infrastructure Controller (APIC), spine switches, and leaf switches. These three components handle both the application of network policy and the delivery of packets.

The system architecture consists of 3 domains (3 pair of FIs) connecting to ACI having two Cisco Nexus 9508 switches acting as a Spine and two Cisco Nexus 9396 as the leaf switches and three APIC-L1 as an APIC appliance.

System architecture can be explained as:

- The 80 server are rack mounted and are connected to a pair of Cisco UCS FIs representing a domain through 10GE link (dual 10GE link to a pair of FI).
- 3 such domains are connected to a pair of Nexus 9396 which is the ACI Fabric leaf nodes. Here 10GEx14 links from each FI are connected to Nexus 9396. This is done through a port-channel of 7 ports connected to each of the Nexus 9396.

Table 5   Software Component Details

<table>
<thead>
<tr>
<th>Layer</th>
<th>Component</th>
<th>Version or Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Cisco ACI OS</td>
<td>11.0 (2m)</td>
</tr>
<tr>
<td></td>
<td>APIC OS</td>
<td>1.0 (1e)</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS 6296UP</td>
<td>UCS 2.2(3d)A</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS VIC1227 Firmware</td>
<td>4.0(1d)</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS VIC1227 Driver</td>
<td>2.1.1.66</td>
</tr>
<tr>
<td>Compute</td>
<td>Cisco UCS C240-M4</td>
<td>C240M4.2.0.3d</td>
</tr>
<tr>
<td>Storage</td>
<td>LSI SAS 3108</td>
<td>24.5.0-0020</td>
</tr>
<tr>
<td>Software</td>
<td>Red Hat Enterprise Linux Server</td>
<td>6.5 (x86_64)</td>
</tr>
<tr>
<td></td>
<td>CDH</td>
<td>5.3.2</td>
</tr>
<tr>
<td></td>
<td>UCS Manager</td>
<td>2.2(3d)</td>
</tr>
</tbody>
</table>

Note

- The latest drivers can be downloaded from the link below: [https://software.cisco.com/download/release.html?mdfid=283862063&flowid=25886&softwareid=283853158&release=1.5.7d&relind=AVAILABLE&rellifecycle=&reltype=latest](https://software.cisco.com/download/release.html?mdfid=283862063&flowid=25886&softwareid=283853158&release=1.5.7d&relind=AVAILABLE&rellifecycle=&reltype=latest)
- The Latest Supported RAID controller Driver is already included with the RHEL 6.5 operating system.
- C240/C220 M4 Rack Servers are supported from UCS firmware 2.2(3d) onwards.
- Nexus 9396 receives the 14x10GE from each pair of FI as a vPC (Virtual Port-Channel), that is, all the 7 ports set from each of the FIs as an uplink to the leaf. There are 6 vPC for the 3 domains in each of 9396 connecting to the 3 pair of FIs.
- Each leaf is connected to Spines via 12 x 40 Gig connectivity cables.
- The three APIC’s are connected to two leaves (Nexus 9396) via 10 Gig SFP cable.

The figure below shows the overall system architecture and physical layout of the solution.
**Figure 12** Fabric Interconnect Connectivity

The figure below shows the connectivity between the leaf switches and fabric interconnect, where vPC has been configured on leaf switches through the APIC. These vPC ports are the same ports that were configured as port-channel in fabric interconnect.

**Figure 13** vPC Connectivity

The figure below shows the connectivity between the one C240 M4 servers and two Fabric Interconnects.
Scaling the Architecture

Here the UCS Servers are directly connected to Cisco UCS Fabric Interconnect (FI) which in-turn connects to leaf switches (Nexus 9396). This mode allows using the UCS Manager capabilities in FI for provisioning the servers. Up to 5 Racks (each with 16 servers) are connected to a Pair of FI forming a single domain and three such domains are connected to a pair of Leaf 9396 (every domain or pair of Cisco FI has 14 uplinks to Nexus 9396). This topology has no network over-subscription within a domain (80 servers under a pair of FI). The over-subscription ratio between domains is 5.7:1 and can scale up to 5760 servers for a fully populated pair of Nexus 9508 with all the 8 line cards in use.
Figure 15  Scaling Architecture

Scaling Architecture

ACI Scaling with F1: Servers connect directly to F1

36 Ports 40 Gig QSFP+ Line card

40 Gig

10 Gig

Rack 1  Rack 2  Rack 3  Rack 4  Rack 5  Rack 1  Rack 2  Rack 3  Rack 4  Rack 5
## Scaling the Architecture

### Table 6  
*Cisco Nexus 9508 – Cisco Nexus 9396PX Connectivity*

<table>
<thead>
<tr>
<th>SPINE</th>
<th>Line Card Pair</th>
<th>Ports Used</th>
<th>POD</th>
<th>Servers</th>
<th>LEAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9508_A</td>
<td>Line Card 1</td>
<td>1-6</td>
<td></td>
<td></td>
<td>3936_1A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>7-12</td>
<td>1</td>
<td>240</td>
<td>3936_1B</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>13-18</td>
<td></td>
<td></td>
<td>3936_2A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>19-24</td>
<td>2</td>
<td>480</td>
<td>3936_2B</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>25-30</td>
<td></td>
<td></td>
<td>3936_3A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>31-36</td>
<td>3</td>
<td>720</td>
<td>3936_3B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>1-6</td>
<td></td>
<td></td>
<td>3936_22A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>7-12</td>
<td>22</td>
<td>5280</td>
<td>3936_22B</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>13-18</td>
<td></td>
<td></td>
<td>3936_23A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>19-24</td>
<td>23</td>
<td>5520</td>
<td>3936_23B</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>25-30</td>
<td></td>
<td></td>
<td>3936_24A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>31-36</td>
<td>24</td>
<td>5760</td>
<td>3936_24B</td>
</tr>
<tr>
<td>N9508_B</td>
<td>Line Card 1</td>
<td>1-6</td>
<td></td>
<td></td>
<td>3936_1A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>7-12</td>
<td>1</td>
<td>240</td>
<td>3936_1B</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>13-18</td>
<td></td>
<td></td>
<td>3936_2A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>19-24</td>
<td>2</td>
<td>480</td>
<td>3936_2B</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>25-30</td>
<td></td>
<td></td>
<td>3936_3A</td>
</tr>
<tr>
<td></td>
<td>Line Card 1</td>
<td>31-36</td>
<td>3</td>
<td>720</td>
<td>3936_3B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>1-6</td>
<td></td>
<td></td>
<td>3936_22A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>7-12</td>
<td>22</td>
<td>5280</td>
<td>3936_22B</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>13-18</td>
<td></td>
<td></td>
<td>3936_23A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>19-24</td>
<td>23</td>
<td>5520</td>
<td>3936_23B</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>25-30</td>
<td></td>
<td></td>
<td>3936_24A</td>
</tr>
<tr>
<td></td>
<td>Line Card 8</td>
<td>31-36</td>
<td>24</td>
<td>5760</td>
<td>3936_24B</td>
</tr>
</tbody>
</table>
Scaling the Architecture Further with Additional Spines Switches

The physical network of the Cisco Application Centric Infrastructure is built around leaf-spine architecture. It is possible to scale this infrastructure, immensely, by adding additional Spine switches. The ACI infrastructure supports up to 12 spine switches.

Table 7  
Cisco Nexus 9396 - Cisco Fabric Interconnect Connectivity

<table>
<thead>
<tr>
<th>LEAF</th>
<th>Ports Used</th>
<th>FI</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>9396_1A</td>
<td>1-14</td>
<td>FI_1A</td>
<td>1-80</td>
</tr>
<tr>
<td>9396_1A</td>
<td>15-28</td>
<td>FI_2A</td>
<td>81-160</td>
</tr>
<tr>
<td>9396_1A</td>
<td>29-42</td>
<td>FI_3A</td>
<td>161-240</td>
</tr>
<tr>
<td>9396_1A</td>
<td>43</td>
<td>APIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44-48</td>
<td>Unused</td>
<td></td>
</tr>
<tr>
<td>9396_1B</td>
<td>1-14</td>
<td>FI_1B</td>
<td>1-80</td>
</tr>
<tr>
<td>9396_1B</td>
<td>15-28</td>
<td>FI_2B</td>
<td>81-160</td>
</tr>
<tr>
<td>9396_1B</td>
<td>29-42</td>
<td>FI_3B</td>
<td>161-240</td>
</tr>
<tr>
<td>9396_1B</td>
<td>43</td>
<td>APIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44-48</td>
<td>Unused</td>
<td></td>
</tr>
</tbody>
</table>

Scaling the Architecture Further with Additional Spines Switches

The physical network of the Cisco Application Centric Infrastructure is built around leaf-spine architecture. It is possible to scale this infrastructure, immensely, by adding additional Spine switches. The ACI infrastructure supports up to 12 spine switches.

Figure 16  Cisco ACI Fabric with Multiple Spine Switches

With a 12-spine design, each leaf switch can be connected up to 12 spine switches. Allowing for tens of thousands of servers to be part of this infrastructure – being interconnected by a non-blocking fabric.
Network Configuration

The network configuration includes configuring the APIC, leaf, spine switches and Fabric Interconnect and deploying various application profiles and policies. In order to achieve this we first need to register the connected Nexus 9K switches to the APIC so that these switches become the part of the ACI fabric. Once the switch is registered the communication between the spine and leaf are completed.

The admin is the only account enabled by default after the APIC is configured and it is always a good practice to create other user accounts with different privilege levels to make the APIC and the network secure. For this purpose we create a local or remote user depending on requirement.

Adding a management access is required in the ACI to let ACI know about any physical or virtual domain that is connected to it. By adding management access, APIC will control the physical interface and assign the policies to this interface. This is achieved by configuring Attachable Access Entity Profile (AEP). AEP requires having the domain and vlan pool that the ACI fabric will be using to communicate with various devices attached to it.

Note
For more detail on AEP please refer “Adding Management Access” section.

Figure 17  Attachable Access Entity Profile for Communication with Other Devices

AEP: Represents a group of external entities with similar infrastructure policy

Domain: VM Management, Physical Or External Associated To Interfaces.

VLAN: Define VLANs for the infrastructure.

In this CVD, two pair of FIs representing two domains are connected to the pair of leaf switch. The uplink in the FIs is connected to the leaf via the port channeling (created in FI) and vPC is created at the leaf switches. The vPC allows single device to use a PortChannel across two upstream devices, eliminating Spanning Tree Protocol blocked ports which in turns provides a loop-free topology. With the use of vPC provides high availability and link-level resiliency.

Depending on the number of VLANs created in the FI, to trunk these vlans across the ACI fabric an Attachable Entity Profile (AEP) is required. An AEP provisions the VLAN pool (and associated VLANs) on the leaf, these VLAN pools are defined under the domain created within the AEP. A domain could be various external entities such as bare metal servers, hypervisors, VM management, Layer 2 or Layer 3 domains. The VLANs are not actually enabled on the port. No traffic flows unless an EPG is deployed on the port. An EPG acts as a separate entity which is analogous to VLAN. A tenant needs to be created before an EPG is defined.

A tenant contains policies that enable qualified users domain-based access control. Application profile, security policies and network are the elements of Tenants. An EPG for each VLAN is created under the application profile. Since EPG represent VLANs, a switch virtual interface (SVI) is needed to provide the Layer 3 processing for packets from all switch ports associated with the VLAN. A bridge domain
needs to be created which acts as switch virtual interface (SVI) for this purpose. Now, for the inter-Vlan communication, contracts need to be created to achieve communication among each EPG. Contracts are policies that enable inter-End Point Group (inter-EPG) communication. These policies are the rules that specify communication between application tiers.

**Note**

For more details on Tenant please refer to the “Adding Tenant” section.

The relationship between the AEP, its elements and tenants is show in the flowchart below.

### Figure 18 Flowchart Showing AEP, AEP Elements and Tenants

**IP Address Assignment**

The IP address schemes of UCS and ACI management are configured as out of band management access through the management switch.

**APIC** 10.0.130.71/24

<table>
<thead>
<tr>
<th>Address 1</th>
<th>Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN - 1</td>
<td>DOMAIN - 2</td>
</tr>
<tr>
<td>UCSM 10.0.141.5/24</td>
<td>UCSM 10.0.141.10/24</td>
</tr>
<tr>
<td>FI-A 10.0.141.6/24</td>
<td>FI-C 10.0.141.8/24</td>
</tr>
</tbody>
</table>
Configuration of APIC

This section describes loading and configuring the APIC.

Once the APIC appliance is booted for the first time, the APIC console presents a series of initial setup options. For many options, you can press Enter to choose the default setting that is displayed in brackets. At any point in the setup dialog, you can restart the dialog from the beginning by pressing Ctrl-C.

Shown below is the initial configuration of the APIC.

Enter the fabric name [ACI Fabric1]:
Enter the number of controllers in the fabric (1-9) [3]:3
Enter the controller ID (1-3) [1]:1
Enter the controller name [apic1]:APIC_1
Enter address pool for TEP addresses [10.0.0.0/16]:
Enter the VLAN ID for infra network (1-4094) [4]: 130

Out-of-band management configuration...
Enter the IP address for out-of-band management: 10.0.130.71/24
Enter the IP address of the default gateway [None]: 10.0.130.1
Administrator user configuration...
Enable strong passwords? [Y]
Enter the password for admin:

Below is the screenshot of the configuration

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Domain - 1</th>
<th>Domain - 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>10.0.145.45 - 124/24</td>
<td>10.0.145.125 - 204/24</td>
</tr>
<tr>
<td>11</td>
<td>10.0.146.45 - 124/24</td>
<td>10.0.146.125 - 204/24</td>
</tr>
<tr>
<td>12</td>
<td>10.0.147.45 - 124/24</td>
<td>10.0.147.125 - 204/24</td>
</tr>
</tbody>
</table>

Table 8: IP Address Assignment for Domain 1 and 2

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Domain - 1</th>
<th>Domain - 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>10.0.145.45 - 124/24</td>
<td>10.0.145.125 - 204/24</td>
</tr>
<tr>
<td>11</td>
<td>10.0.146.45 - 124/24</td>
<td>10.0.146.125 - 204/24</td>
</tr>
<tr>
<td>12</td>
<td>10.0.147.45 - 124/24</td>
<td>10.0.147.125 - 204/24</td>
</tr>
</tbody>
</table>
Figure 19 APIC Initial Configuration

Once the configuration is completed, the APIC will boot its APIC IOS Image and will ask for the login information. The default username is “admin” and the password is the one that was set during the initial configuration.
Switch Discovery with the APIC

The APIC is a central point of automated provisioning and management for all the switches that are part of the ACI fabric. A single data center might include multiple ACI fabrics, each with their own APIC cluster and Cisco Nexus 9000 Series switches that are part of the fabric. To ensure that a switch is managed only by a single APIC cluster, each switch must be registered with that specific APIC cluster that manages the fabric. The APIC discovers new switches that are directly connected to any switch it currently manages. Each APIC instance in the cluster first discovers only the leaf switch to which it is directly connected. After the leaf switch is registered with the APIC, the APIC discovers all spine switches that are directly connected to the leaf switch. As each spine switch is registered, that APIC discovers all the leaf switches that are connected to that spine switch. This cascaded discovery allows the APIC to discover the entire fabric topology in a few simple steps.

Switch Registration with the APIC Cluster

Once the switch is discovered by the APIC cluster it needs to be registered in the APIC to make it as a part of the fabric.

**Prerequisite:** All switches must be physically connected and booted with the correct ACI Image.

Using a web browser connect to the out-of-band management ip address [10.0.130.71] configured in the initial configuration.

1. On the menu bar, choose **FABRIC > INVENTORY**. In the Navigation pane, choose the appropriate pod.
2. In the Navigation pane, expand the pod, and click **Fabric Membership**. In the Work pane, in the Fabric Membership table, a single leaf switch is displayed with an ID of 0. It is the leaf switch that is connected to APIC.
3. To configure the ID, double-click the leaf switch row, and perform the following actions:
   a. In the ID field, add the appropriate ID (leaf1 is ID 101, leaf2 is ID 102 and leaf3 is ID 103). The ID must be a number that is greater than 100 because the first 100 IDs are for APIC appliance nodes.
   b. In the Switch Name field, add the name of the switch, and click Update. After an ID is assigned, it cannot be updated. The switch name can be updated by double-clicking the name and updating the Switch Name field.

   **Note** The Success dialog box is displayed. An IP address gets assigned to the switch, and in the Navigation pane, the switch is displayed under the pod.

4. Monitor the Work pane until one or more spine switches appear.
5. To configure the ID, double-click the spine switch row and perform the following actions:
   a. In the ID field, add the appropriate ID (spine1 is ID 201 and spine 2 is ID 202). The ID must be a number that is greater than 100.
b. In the Switch Name field, add the name of the switch, and click **Update**.

The Success dialog box is displayed. An IP address gets assigned to the switch, and in the Navigation pane, the switch is displayed under the pod. Wait until all remaining switches appear in the Node Configurations table.

6. For each switch listed in the Fabric Membership table, perform the following steps:
   a. Double-click the switch, enter an ID and a Name, and click **Update**.
   b. Repeat for the next switch in the list.

**Validating the Switches**

1. On the menu bar, choose **FABRIC > INVENTORY**, and in the Navigation pane, under Pod 1, expand Fabric Membership.

2. The switches in the fabric are displayed with their node IDs. In the Work pane, all the registered switches are displayed with the IP addresses that are assigned to them.

**Figure 23 Switch Validation**

### Fabric Membership

<table>
<thead>
<tr>
<th>SERIAL NUMBER</th>
<th>NODE ID</th>
<th>NODE NAME</th>
<th>RACK NAME</th>
<th>MODEL</th>
<th>ROLE</th>
<th>IP</th>
<th>REDEPLOYED</th>
<th>SUPPLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGE1820WWF00</td>
<td>201</td>
<td>SPINE_1</td>
<td>B12_DATA</td>
<td>N8K-C9308</td>
<td>spine</td>
<td>10.0.168.94/32</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>FGE1820WWF01</td>
<td>202</td>
<td>SPINE_2</td>
<td>B12_DATA</td>
<td>N8K-C9308</td>
<td>spine</td>
<td>10.0.168.64/32</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>SAL1816WPA</td>
<td>203</td>
<td>LEAF_3</td>
<td>B12_DATA</td>
<td>N8K-C9312T4</td>
<td>leaf</td>
<td>10.0.168.64/32</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>SAL1819COMI</td>
<td>202</td>
<td>LEAF_2</td>
<td>U12_DATA</td>
<td>N8K-C939KFX</td>
<td>leaf</td>
<td>10.0.168.93/32</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>SAL1819COMY</td>
<td>201</td>
<td>LEAF_1</td>
<td>U12_DATA</td>
<td>N8K-C939KFX</td>
<td>leaf</td>
<td>10.0.168.95/32</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>

**Validating the Fabric Topology**

1. On the menu bar, choose **FABRIC > INVENTORY**.

2. In the Navigation pane, choose the pod that you want to view.

3. In the Work pane, click the **TOPOLOGY** tab.

   The displayed diagram shows all attached switches, APIC instances, and links.

4. (Optional) To view the port-level connectivity of a leaf switch or spine switch, double-click its icon in the topology diagram.

   To return to the topology diagram, in the upper left corner of the Work pane click the **Previous View** icon.

5. (Optional) To refresh the topology diagram, in the upper left corner of the Work pane, click the **Refresh** icon.
Creating User Accounts

The admin is the only user when the system starts. The APIC supports a granular, role-based access control system where user accounts can be created with various roles including non-admin users with fewer privileges.

1. On the menu bar, choose **ADMIN > AAA**.
2. In the Navigation pane, click **AAA Authentication**.
   
   In the Work pane, the AAA Authentication dialog box is displayed.
3. Verify that in the default Authentication field, the Realm field displays as Local.

4. In the Navigation pane, expand **Security Management > Local Users**.
   
   The admin user is present by default.
5. In the Navigation pane, right-click Create Local User.
   The Create Local User dialog box opens.

6. Under the Security dialog box, choose the desired security domain for the user, and click **Next**.

   *Figure 26  Creating Local User*

   ![Creating Local User](image)

   The Roles dialog box opens.

7. In the Roles dialog box, click the radio buttons to choose the roles for your user, and click **Next**.
   You can provide read-only or read/write privileges.

8. In the User Identity dialog box, perform the following actions:
   a. In the Login ID field, add an ID.
   b. In the Password field, type the password.
   c. In the Confirm Password field, confirm the password.
   d. Click **Finish**.
   e. Type other parameters if desired.
9. In the Navigation pane, click the name of the user that you created. In the Work pane, expand the + sign next to your user in the Security Domains area.

The access privileges for your user are displayed.

Adding Management Access

Attach Entity Profiles (AEP)

The ACI fabric provides multiple attachment points that connect through leaf ports to various external entities such as baremetal servers, hypervisors, Layer 2 switches (for example, the Cisco UCS fabric interconnect), and Layer 3 routers (for example Cisco Nexus 7000 Series switches). These attachment points can be physical ports, port channels, or a virtual port channel (vPC) on the leaf switches.

An attachable entity profile (AEP) represents a group of external entities with similar infrastructure policy requirements. The infrastructure policies consist of physical interface policies, for example, Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), maximum transmission unit (MTU), and Link Aggregation Control Protocol (LACP).

An AEP is required to deploy any VLAN pools on the leaf switches. It is possible to reuse the encapsulation pools (for example, VLAN) across different leaf switches. An AEP implicitly provides the scope of the VLAN pool (associated to the VMM domain) to the physical infrastructure.

Note

- An AEP provisions the VLAN pool (and associated VLANs) on the leaf. The VLANs are not actually enabled on the port. No traffic flows unless an EPG is deployed on the port.
• Without VLAN pool deployment using an AEP, a VLAN is not enabled on the leaf port even if an EPG is provisioned.
• A particular VLAN is provisioned or enabled on the leaf port based on EPG events either statically binding on a leaf port or based on VM events from external controllers such as VMware vCenter.
• A leaf switch does not support overlapping VLAN pools. Different overlapping VLAN pools must not be associated with the same AEP.

Configuring In-Band Management Access Using the GUI

The In-Band management access is required to establish the communication between the APIC and the ACI fabric.

1. On the menu bar, choose FABRIC > Access Policies. In the Work pane, click Configure an Interface, PC and VPC.
2. In the Configure Interface, PC, and VPC dialog box, click the large + icon next to the switch diagram to create a new profile and configure VLANs for the APIC.
   In the Switches field, from drop-down list, check the check boxes for the switches to which the APICs are connected. (leaf1 and leaf2).

   ![Figure 28 Configuring Interface, PC, and VPC](image)

3. In the Switch Profile Name field, enter a name for the profile (Apic_Connected_Leaf).
4. Click the + icon to configure the ports.
5. Verify that in the Interface Type area, the Individual radio button is selected.
6. In the Interfaces field, enter the ports to which APICs are connected (1/48).
7. In the Interface Selector Name field, enter the name of the port profile (Apic_Connected_Port).
8. In the Interface Policy Group field, from drop-down list, choose Create Interface Policy Group.
9. In the Create Access Port Policy Group dialog box, perform the following actions:
   a. In the Name field, enter the name of the policy group (INBAND).
      You can leave the default values in the rest of the fields as they are.
   b. In the Attached Entity Profile field, choose create Attachable Access Entity Profile.
10. In the Create Attachable Access Entity Profile dialog box, perform the following actions:

   a. In the Name field, enter a name (INBAND).

   b. Expand Domains to be Associated to Interfaces field. In the Domain Profile field, from the drop-down list, choose Create Physical Domain.
c. In the Create Physical Domain dialog box, in the Name field, enter the name (INBAND).

d. In the VLAN Pool field, from the drop-down list, choose Create VLAN Pool.

**Figure 32 Creating Physical Domain**

```
CREATE PHYSICAL DOMAIN

Specify the domain name and the VLAN Pool

Name: INBAND
VLAN Pool: select an option
   Create VLAN Pool

SUBMIT CANCEL
```

e. In the Create VLAN Pool dialog box, in the Name field, enter the pool name (INBAND).

f. In the Allocation Mode area, click the Static Allocation radio button.

**Figure 33 Creating Vlan Pool**

```
CREATE VLAN POOL

Specify the Pool identity

Name: INBAND
Description: optional
Allocation Mode: Dynamic Allocation
Static Allocation
Encap Blocks: +  X

VLAN Range

SUBMIT CANCEL
```

g. Expand Encap Blocks. In the Create Ranges dialog box, in the Range fields, add a VLAN range (145-145).
Figure 34  Creating VLAN Range

h. In the Create VLAN Pool dialog box, click Submit.
i. In the Create Physical Domain dialog box, click Submit.
j. In the Create Attachable Access Entity Profile dialog box, click Update and then Submit.
k. In the Create Access Port Policy Group dialog box, click Submit.
l. In the Configure Interface, PC, and VPC dialog box, click Save.

Figure 35  Saving the Configuration

The VLAN and the ports to which the APIC is connected are now configured.

Configuring VPC Ports for Fabric Interconnect

In order to configure vPC we need to create CDP Policy, LLDP Policy and LACP Policy that can be applied to the vPC ports.

- The APIC does not manage fabric interconnects and the rack servers, so these services must be configured from UCSM
• Create VLAN pools that are associated on the fabric interconnect uplink to the leaf switch on the fabric interconnect.

• Cisco UCS C-series server when used along with ACI, Link Layer Discovery Protocol (LLDP) is not supported and must be disabled.

• Cisco Discovery Protocol (CDP) is disabled by default in the Cisco UCS Manager Fabric interconnects. In the Cisco UCS Manager, you must enable CDP by creating a policy under Network Control Policies > CDP.

The above steps are explained in detail further below

Creating CDP Policy group

1. On the menu bar, choose FABRIC > ACCESS POLICIES.
2. In the Navigation pane, expand the Interface Policies and expand the Policies again.
3. Right-click the CDP Interface and select Create CDP Interface Policy.

![Create CDP Interface Policy](image)

4. In the Create CDP Interface Policy dialogue box, enter “FI_CDP” as the policy name, set Admin State “Enabled” and click submit.
5. This will create the CDP policy group.
Creating LLDP Policy group

1. On the menu bar, choose **FABRIC > ACCESS POLICIES**.
2. In the Navigation pane, expand the Interface Policies and expand the Policies again.
3. Right-click the LLDP Interface and select **Create LLDP Interface Policy**.

4. In the Create LLDP Interface Policy dialogue box, enter “FI_LLDP” as the policy name, set both the Receive and Transmit State “Disabled” and click **submit**.
5. This will create the LLDP policy group.
Creating LACP Policy

1. On the menu bar, choose FABRIC > ACCESS POLICIES.
2. In the Navigation pane, expand the Interface Policies and expand the Policies again.
3. Right-click the LACP and select Create LACP Policy.

4. In Create LACP Policy window, enter the name “LACP_Active”. In the mode select the “Active” radio button and click submit.
Creating vPC

1. Expand the Configured Switch Interfaces area to configure the VPCs for the server ports, and perform the following actions:
   a. In the Switches drop-down list, check the check boxes for the switches that you want to connect to the Fabric Inteconnect. (LEAF_1 & LEAF_2).
   b. In the Switch Profile Name field, enter a name for the profile (FI_Connected_Leaves).
e. Click the + icon to configure the ports.

d. In the Interface Type area, verify the VPC radio button is selected.

e. In the Interfaces field, enter the ports to which the servers are connected.

f. In the Interface Selector Name field, enter the name of the port profile (VPC_1).

g. In the VPC Policy Group field, from the drop-down list, choose **Create VPC Interface Policy Group**.

h. In Create VPC Interface Policy Group window, enter the name “VPC1”.

---

**Note**: Create separate VPC interface policy group for each VPC link.
i. In the CDP Policy field, from the drop-down list, choose “FI_CDP”.

j. In the LLDP Policy field, from the drop-down list, choose “FI_LLDP”.

k. In the LACP policy field, from the drop-down list choose “LACP_Active” and click Submit.

l. In the Create VPC Interface Policy Group window click Submit.

m. In the Configure Interface, PC, and VPC dialog box, click Save and click Save again.

n. In the Configure Interface, PC, and VPC dialog box, click Submit.

o. Repeat step “C” to “M” to create VPC port for all the Fabric Interconnects connected to the ACI fabric. Once all the FI vPC port is configured, the configured switch interface window should look like fig below.

**Configuring vPC Leaf Pairing**

1. In the Configure Interface, PC, and VPC dialog box, click on the “+” on VPC DOMAIN ID.
2. In the VPC Domain ID field, enter “145”.
3. In the “Switch A” drop down box, select node “101”.
4. In the “Switch B” drop down box, select node “102” and click Save and Submit.

**Creating Attachable Entity Profile**

2. Select Attachable Access Entity Profile and right-click on it and select **Create Attachable Access Entity Profile**.

**Figure 46 Fabric Window**

3. Create Attachable Access Entity Profile window opens, in the name field enter FI_AEP and click + Domains (VMM, Physical Or External) To Be Associated To Interfaces.
4. In the Domain Profile field, from the drop-down list, choose **Create Physical Domain**.
5. In the Create Physical Domain dialog box, in the Name field, enter the name (UCS_FI).

6. In the VLAN Pool field, from the drop-down list, choose **Create VLAN Pool**.
7. In the Create VLAN Pool dialog box, in the Name field, enter the pool name (UCS_FI).
8. In the Allocation Mode area, click the **Static Allocation** radio button.

**Figure 49 Creating VLAN Pool**

```
CREATE VLAN POOL

Specify the Pool identity
Name: UCS_R
Description: optional
Allocation Mode: Static Allocation
Encap Blocks:
   VLAN Range

SUBMIT CANCEL
```

9. Expand Encap Blocks. In the Create Ranges dialog box, in the Range fields, add a VLAN range (11-12) and click **OK**.

**Figure 50 Assigning VLAN Range**

```
CREATE RANGES

Specify the Encap Block Range
Type: VLAN
Range: [11-12]

OK CANCEL
```

10. Repeat step 9 again to create VLAN 160.

   VLAN Assignments are as follows:
   - Vlan 160 for Management
   - Vlan 11 for HDFS
   - Vlan 12 for DATA

   More detail is provided in the FI configuration section.
11. In the Create VLAN Pool dialog box, click Submit.
12. In the Create Physical Domain dialog box, click Submit.
13. In the Create Attachable Access Entity Profile dialog box, click Update.
14. Create Attachable Access Entity Profile window opens, in the name field enter FI_AEP and click “+” Domains (VMM, Physical Or External) To Be Associated To Interfaces.
15. In the Domain Profile field, from the drop-down list, choose Create Layer 2 Domain.
16. In the Create Layer 2 Domain dialog box, in the Name field, enter the name (FI).
17. From the VLAN Pool drop-down list choose “UCS_FI” and click Submit.
18. In Create Attachable Access Entity Profile window click Next.

19. In each of the “Interface Policies” that was created for the vPC, select the radio button All and click Finish.
Creating Tenants, Private Network, and Bridge Domains

Tenants Overview

- A tenant contains policies that enable qualified users domain-based access control. Qualified users can access privileges such as tenant administration and networking administration.
- A user requires read/write privileges for accessing and configuring policies in a domain. A tenant user can have specific privileges into one or more domains.
- In a multi-tenancy environment, a tenant provides group user access privileges so that resources are isolated from one another (such as for endpoint groups and networking). These privileges also enable different users to manage different tenants.

Creating a Tenant, Private Network, and Bridge Domain Using the GUI

Create and specify a network and a bridge domain for the tenant. The defined bridge domain element subnets reference a corresponding Layer 3 context.

1. On the menu bar, choose TENANTS, and perform the following actions:
   a. Click Add Tenant.
   b. The Create Tenant dialog box opens.
   c. In the Name field, add the tenant name (Big_Data), and click Next.

2. Create a security domain so that it allows only users in that security domain to have access.
   Click the + sign next to Security Domains to open the Create Security Domain dialog box, and perform the following actions:
   a. In the Name field, specify the security domain name. (Big_Data)
   b. Click Submit. In the Create Tenant dialog box, check the check box for the security domain that you created, and click Next.
3. In the Network window, perform the following actions:
   a. Click the + sign to add the network.
   b. In the Create New Network area, specify the private tenant network name (PVN_1) and click Next.
4. Specify the bridge domain in the Name field (BD_1), click **OK**. Click **Next**, and perform the following actions:
a. Confirm that the private network (PVN_1) is created and is associated with the bridge domain (BD_1).

b. In the Application Profile window, click Finish.
5. To validate that the tenant has a private network and bridge domain, in the submenu bar under the Tenants tab, click the new tenant name that was created earlier. In the Navigation pane, expand the tenant name. Under Bridge Domains, the new bridge domain is displayed. Under Private Networks, the new network is displayed.
6. Select the bridge domain created earlier (BD_1) and check the L2 Unknown Unicast to Flood, and check the ARP Flooding checkbox and click **Submit**.
7. Expand the Bridge Domain and BD_1, right-click on the Subnets and select **Create Subnet**.

8. In the Create Subnet dialogue box, enter the gateway IP 10.0.145.1/24 and click **Submit**.

This IP address (10.0.145.1/24) is assigned to the bridge domain that typically is used as the switch virtual interface (SVI) in a traditional switch configuration.
Repeat step 7 again to create two more subnets for other two VLANS.

Creating an Application Profile Using the GUI

1. On the menu bar, choose TENANTS. In the Navigation pane, expand the tenant, right-click Application Profiles, and click Create Application Profile.

2. In the Create Application Profile dialog box, in the Name field, add the application profile name (CLOUDERA).
Creating EPGs Using the GUI

1. Expand Tenant BIG_DATA > Application Profiles > CLOUDERA, right-click on the Application EPGs and select Create Application EPG. In the Create Application EPG dialog box, perform the following actions:
   a. In the Name field, add the EPG name (Mgmt).
   b. In the Bridge Domain field, choose the bridge domain from the drop-down list (BD_1).
   c. Expand Associated Domain Profiles and from the drop-down list, choose the Domain Profile name (Mgmt).
   d. From the Deployment Immediacy and Resolution Immediacy drop-down list select Immediate.
   e. Click Update, and click Finish.
2. Repeat step 1 to create two more EPGs named DATA and HDFS.

Note: On Cloudera Security: When deploying Cloudera with Security only one VLAN on one vNIC is supported at the UCS Manager and UCS Server level. Under this scenario, there is no need to create EPGs DATA and HDFS at the ACI level. If already created, there is no problem. This could be left as is as from the downstream, only data from mgmt VLAN will be forwarded upstream.

3. Once all three EPGs are created, these EPGs are associated with the Application Profile CLOUDERA.
Configuring EPGs

1. Expand Tenant BIG_DATA > Application Profiles > CLOUDERA > Application EPGs > EPG Mgmt.
2. Right-click the Subnets and select Create EPG Subnet.
3. In the Create EPG Subnet dialogue box, enter the Default Gateway IP as 10.0.145.1/24 and click Submit.

4. Similarly configure subnet for other EPGs with appropriate subnet address. For more detail, navigate to the IP Address Assignment section.

Creating the Static Binding for the Leaves and Paths

The static binding for the leaves are required to associate the physical interfaces with the EPGs.
No traffic flows unless an EPG is deployed on the port. Without VLAN pool deployment using an AEP, a VLAN is not enabled on the leaf port even if an EPG is provisioned. A particular VLAN is provisioned or enabled on the leaf port based on EPG events by statically binding on a leaf port.

1. On the menu bar, choose TENANTS and the tenant name on which you want to operate. In the Navigation pane, expand the Tenants > Application Profiles > CLOUDERA > Application EPGs > EPG Mgmt and select Static Bindings (Paths).

2. Right-click the Static Bindings (paths) and select Deploy Static EPG on PC, VPC, or Interface.
3. In the Path Type: select the Virtual Port Channel radio button.
4. From the Path: drop down list select the appropriate nodes and port where the FI’s are connected. On Encap field use vlan-160, on Deployment Immediacy select the Immediate radio button and on Mode select the Untagged and click Submit.
5. Repeat step 2, 3 & 4 for all the vPC ports created.

6. Similarly, statically bind the ports in other EPGs created using the appropriate VLAN numbers (12 for HDFS and 11 for DATA).

7. Once the Static binding for all the EPG is configured properly, verify that the VPC ports created earlier are trunking the appropriate VLANS. This can be verified by the following steps:
   a. On the menu bar, choose **FABRIC > Access Policies**.
   b. Expand **Pod 1 > LEAF_1 (Node-101) > Interfaces > VPC Interfaces > 1** (This number might be different in different setups). Select any of the Interfaces to view the properties.
Creating Contracts

Contracts are policies that enable inter-End Point Group (inter-EPG) communication. These policies are the rules that specify communication between application tiers. If no contract is attached to the EPG, inter-EPG communication is disabled by default. No contract is required for intra-EPG communication because intra-EPG communication is always allowed.

1. On the menu bar, choose TENANTS and the tenant name on which you want to operate. In the Navigation pane, expand the Tenant > Security Policies.
   a. Right-click Contracts > Create Contract.
b. In the Create Contract dialog box, in the Name field, enter the contract name (Mgmt) and click Submit.

2. Create two more contracts for Data and for HDFS following the same steps in this procedure.

3. On the menu bar, choose TENANTS and the tenant name on which you want to operate. In the Navigation pane, expand the Tenant > Application Profiles > CLOUDERA > Application EPGs > EPG Mgmt.

4. Right-click the contract and select Add Provided Contract.
5. In the add provided contract dialogue box, from the contract drop-down list choose BIG_DATA/Mgmt and click Submit.

6. Right-click the contract and select Add Consumed Contract.

7. In the add consumed contract dialogue box, from the contract drop-down list choose BIG_DATA/DATA and click Submit.

8. Right-click the contract and select Add Consumed Contract.

9. In the add consumed contract dialogue box, from the contract drop-down list choose BIG_DATA/HDFS and click Submit.
10. For EPG DATA, add provided contract BIG_DATA/Data and consumed contract BIG_DATA/Mgmt and BIG_DATA/HDFS.

11. For EPG HDFS, add provided contract BIG_DATA/HDFS and consumed contract BIG_DATA/Mgmt and BIG_DATA/Data.

12. Once all the contract is configured, in the Navigation pane, expand the tenant BIG_DATA > Application Profiles > CLOUDEERA and select Application EPGs, the window should appear as follows.

This will complete the Network configuration with three EPGs for each VLANs, a Private Network and a Bridge Domain.
Fabric Configuration

This section provides details for configuring a fully redundant, highly available Cisco UCS 6296 fabric configuration.

1. Initial setup of the Fabric Interconnect A and B.
2. Connect to UCS Manager using virtual IP address of using the web browser.
3. Launch UCS Manager.
4. Enable server, uplink and appliance ports.
5. Start discovery process.
6. Create pools and polices for Service profile template.
7. Create Service Profile template and 64 Service profiles.
8. Associate Service Profiles to servers.

Performing Initial Setup of Cisco UCS 6296 Fabric Interconnects

This section describes the steps to perform initial setup of the Cisco UCS 6296 Fabric Interconnects A and B.

Configure Fabric Interconnect A

1. Connect to the console port on the first Cisco UCS 6296 Fabric Interconnect.
2. At the prompt to enter the configuration method, enter console to continue.
3. If asked to either perform a new setup or restore from backup, enter setup to continue.
4. Enter y to continue to set up a new Fabric Interconnect.
5. Enter y to enforce strong passwords.
6. Enter the password for the admin user.
7. Enter the same password again to confirm the password for the admin user.
8. When asked if this fabric interconnect is part of a cluster, answer y to continue.
10. Enter the cluster name for the system name.
11. Enter the Mgmt0 IPv4 address.
12. Enter the Mgmt0 IPv4 netmask.
13. Enter the IPv4 address of the default gateway.
14. Enter the cluster IPv4 address.
15. To configure DNS, answer y.
16. Enter the DNS IPv4 address.
17. Answer y to set up the default domain name.
18. Enter the default domain name.
19. Review the settings that were printed to the console, and if they are correct, answer yes to save the configuration.
20. Wait for the login prompt to make sure the configuration has been saved.
Configure Fabric Interconnect B
1. Connect to the console port on the second Cisco UCS 6296 Fabric Interconnect.
2. When prompted to enter the configuration method, enter console to continue.
3. The installer detects the presence of the partner Fabric Interconnect and adds this fabric interconnect to the cluster. Enter y to continue the installation.
4. Enter the admin password that was configured for the first Fabric Interconnect.
5. Enter the Mgmt0 IPv4 address.
6. Answer yes to save the configuration.
7. Wait for the login prompt to confirm that the configuration has been saved.

For more information on configuring Cisco UCS 6200 Series Fabric Interconnect, see:

Logging Into Cisco UCS Manager
Follow these steps to login to Cisco UCS Manager.
1. Open a web browser and navigate to the Cisco UCS 6296 Fabric Interconnect cluster address.
2. Click the Launch link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin for the user-name and enter the administrative password.
5. Click Login to log in to the Cisco UCS Manager.

Upgrading Cisco UCS Manager Software to Version 2.2(3d)
This document assumes the use of UCS 2.2(3d). Refer to Upgrading between Cisco UCS 2.0 Releases to upgrade the Cisco UCS Manager software and UCS 6296 Fabric Interconnect software to version 2.2(3d). Also, make sure the UCS C-Series version 2.2(3d) software bundles is installed on the Fabric Interconnects.

Adding Block of IP Addresses for KVM Access
These steps provide details for creating a block of KVM IP addresses for server access in the Cisco UCS environment.
1. Select the LAN tab at the top of the left window.
3. Right-click IP Pool ext-mgmt
4. Select Create Block of IPv4 Addresses.
5. Enter the starting IP address of the block and number of IPs needed, as well as the subnet and gateway information.

6. Click **OK** to create the IP block.

7. Click **OK** in the message box.

**Enabling Uplink Port**

These steps provide details for enabling uplinks ports.

1. Select the **Equipment** tab on the top left of the window.

2. Select **Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module > Ethernet Ports.**
3. On the Right window select all the ports that are connected to the Nexus 9396 leaf switch (14 per FI), right-click them, and select **Configure as uplink Port**.

4. Select **Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module**.
5. Expand the UnConfigured Ethernet Ports section.
6. Select all the ports that are connected to the Nexus 9396 leaf switch (14 per FI), right-click them, and select **Configure as uplink Port**.

**Note**  The ports that are configured as uplink port should appear as Network under IF role.

### Enabling Server Ports

These steps provide details for enabling server ports.

7. Select the **Equipment** tab on the top left of the window.
8. Select **Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module > Ethernet Ports**.

9. On the Right window select all the ports that are connected to the UCS C240 server (1 per Server), right-click them, and select **Configure as Server Port**.
Figure 81  Showing Servers Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC Address</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>00:2A:6A:CD:46:95</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>15</td>
<td>00:2A:6A:CD:46:96</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>16</td>
<td>00:2A:6A:CD:46:97</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>17</td>
<td>00:2A:6A:CD:46:98</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>18</td>
<td>00:2A:6A:CD:46:99</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>19</td>
<td>00:2A:6A:CD:46:9A</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>20</td>
<td>00:2A:6A:CD:46:9B</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>21</td>
<td>00:2A:6A:CD:46:9C</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>22</td>
<td>00:2A:6A:CD:46:9D</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>23</td>
<td>00:2A:6A:CD:46:9E</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>24</td>
<td>00:2A:6A:CD:46:9F</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>26</td>
<td>00:2A:6A:CD:46:9H</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>28</td>
<td>00:2A:6A:CD:46:A2</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>29</td>
<td>00:2A:6A:CD:46:A3</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>30</td>
<td>00:2A:6A:CD:46:A4</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>31</td>
<td>00:2A:6A:CD:46:A5</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
<tr>
<td>32</td>
<td>00:2A:6A:CD:46:A6</td>
<td>Unconfigured</td>
<td>Physical</td>
</tr>
</tbody>
</table>

Configuring Port-Channels

1. Click the LAN tab on top left window.
2. Expand the LAN Cloud > Fabric A.
3. On the right window select Create Port Channel.

Figure 82  Creating Port Channel

4. On Set Port Channel Name window, perform the following actions:
a. In the ID field, specify the ID “01” as the first port channel

b. In Name field, type P01 as Port-channel01 and click **Next**.

*Figure 83 Setting Port-Channel ID and Name*

5. In Add Ports window select all the ports that is connected to the Nexus 9396 Leaf Switch and click **>>**. This will add all the ports in the port channel created earlier.
Figure 84 Adding Ports to the Port Channel
6. Similarly for Fabric Interconnect B, click the **LAN** tab on top left window.
7. Expand the **LAN Cloud > Fabric B**.
8. In the right pane of the window select **Create Port Channel**.
Fabric Configuration

Figure 86  Creating Port Channel

9. On Set Port Channel Name window, perform the following actions:
   a. In the ID field, specify the ID “02” as the second port channel
   b. In Name field, type P02 as Port-channel01 and click Next.
10. In Add Ports window select all the ports that is connected to the Nexus 9396 Leaf Switch and click `>>`. This will add all the ports in the port channel created earlier.
Figure 88  Adding Ports to the Port Channel
11. The configured port channels and vPC can be verified by logging in to the APIC.
Creating Pools for Service Profile Templates

Creating an Organization

Organizations are used as a means to arrange and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources. This document does not assume the use of Organizations; however the necessary steps are provided for future reference.

Follow these steps to configure an organization within the Cisco UCS Manager GUI:

1. Click New on the top left corner in the right pane in the UCS Manager GUI.
2. Select Create Organization from the options
3. Enter a name for the organization.
4. (Optional) Enter a description for the organization.
5. Click OK.
6. Click OK in the success message box.

Creating MAC Address Pools

Follow these steps to create MAC address pools:

1. Select the LAN tab on the left of the window.
2. Select Pools > root.
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool. Enter ucs for the name of the MAC pool.
5. (Optional) Enter a description of the MAC pool.
6. Select Assignment Order Sequential.
7. Click Next.
8. Click Add.
9. Specify a starting MAC address.
10. Specify a size of the MAC address pool, which is sufficient to support the available server resources.
11. Click OK.
12. Click Finish.
Figure 94 Confirming Newly Added MAC Pool

13. When the message box displays, click **OK**.

**Configuring VLANs**

VLANs are configured as shown in Table 6.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Fabric</th>
<th>NIC Port</th>
<th>Function</th>
<th>Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan160_mgmt</td>
<td>A</td>
<td>eth0</td>
<td>Management, User connectivity</td>
<td>Fabric Failover to B</td>
</tr>
<tr>
<td>vlan12_HDFS</td>
<td>B</td>
<td>eth1</td>
<td>Hadoop</td>
<td>Fabric Failover to A</td>
</tr>
<tr>
<td>vlan11_DATA</td>
<td>A</td>
<td>eth2</td>
<td>Hadoop with multiple NICs support</td>
<td>Fabric Failover to B</td>
</tr>
</tbody>
</table>

All the VLANs created need to be trunked to the upstream distribution switch connecting the fabric interconnects. For this deployment VLAN160 is configured for management access (Installing and configuring OS, clustershell commands, setup NTP, user connectivity, etc) and vlan12_HDFS is configured for Hadoop Data traffic.

With some Hadoop distributions supporting multiple NICs, where Hadoop uses multiple IP subnets for its data traffic, vlan11_DATA can be configured to carry Hadoop Data traffic allowing use of both the Fabrics (10 GigE on each Fabric allowing 20Gbps active-active connectivity).

Further, if there are other distributed applications co-existing in the same Hadoop cluster, then these applications could use vlan11_DATA providing full 10GigE connectivity to this application on a different fabric without affecting Hadoop Data traffic (here Hadoop is not enabled for multi-NIC).

**Note**

- **On Cloudera Security**: When deploying Cloudera with Security only one VLAN on one vNIC is supported. If the Cloudera install is going to have Security features enabled at a later stage, then use or create only single VLAN/vNIC in UCS Manager (could be name VLAN160_mgmt or VLAN12_HDFS) which will carry both management traffic and HDFS traffic. Ensure the MTU is set to 9000 and QoS policy is set to Platinum.

- If all the three VLANs are already created, and Cloudera Security needs to be enabled, then keep only one vNIC, VLAN160_Mgmt and delete rest of the vNICs from UCS Manager Service Profile Template. Modify the vNIC connected to VLAN160_Mgmt and update the MTU to 9000 and QoS Policy and before re-acknowledging the changes (this will lead to server reboot), on the servers.
remove the configuration files for the vNICs
/etc/sysconfig/network-scripts/<ifcfg-deleted-NICs> and re-acknowledge on the UCS Manager.
This will restart the servers with only one vNIC/VLAN enabled.

Follow these steps to configure the VLANs in the Cisco UCS Manager GUI:
1. Select the **LAN** tab in the left pane in the UCS Manager GUI.
2. Select **LAN > VLANs**.
3. Right-click the **VLANs** under the root organization.
4. Select **Create VLANs** to create the VLAN.

5. Enter vlan160_mgmt for the VLAN Name.
6. Click the **Common/Global** radio button for the vlan160_mgmt.
7. Enter 160 on VLAN IDs of the Create VLAN IDs.
8. Click **OK** and then, click **Finish**.
9. Click **OK** in the success message box.
10. Select the **LAN** tab in the left pane again.
11. Select **LAN > VLANs**.
12. Right-click the **VLANs** under the root organization.
13. Select Create **VLANs** to create the VLAN.
14. Enter `vlan11_DATA` for the VLAN Name.
15. Click the **Common/Global** radio button for the `vlan11_DATA`.
16. Enter `11` on VLAN IDs of the Create VLAN IDs.
17. Click **OK** and then, click **Finish**.
18. Click **OK** in the success message box.
19. Click the LAN tab in the left pane again
20. Select LAN > VLANs.
21. Right-click the VLANs under the root organization.
22. Select Create VLANs to create the VLAN.
23. Enter vlan12_HDFS for the VLAN Name.
24. Select Common/Global for the vlan12_HDFS.
25. Enter 12 on VLAN IDs of the Create VLAN IDs.
26. Click OK and then, click Finish.
Creating Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

Follow these steps to configure the server pool within the Cisco UCS Manager GUI:

1. Select the Servers tab in the left pane in the UCS Manager GUI.
2. Select Pools > root.
3. Right-click the Server Pools.
4. Select Create Server Pool.
5. Enter your required name (ucs) for the Server Pool in the name text box.
6. (Optional) enter a description for the organization
7. Click Next to add the servers.
8. Select all the Cisco UCS C240M4SX servers to be added to the server pool you previously created (ucs), then Click >> to add them to the pool.

9. Click Finish.

10. Click OK, and then click Finish.
Creating Policies for Service Profile Templates

Creating Host Firmware Package Policy

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These include adapters, BIOS, board controllers, FC adapters, HBA options, ROM and storage controller properties as applicable.

Follow these steps to create a firmware management policy for a given server configuration using the Cisco UCS Manager GUI:

1. Select the Servers tab in the left pane in the UCS Manager GUI.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter your required Host Firmware package name (ucs).
6. Click the Simple radio button to configure the Host Firmware package.
7. Select the appropriate Rack package that you have.
8. Click OK to complete creating the management firmware package.
9. Click OK.

Figure 101  Creating Host Firmware Package

Creating QoS Policies

Follow these steps to create the QoS policy for a given server configuration using the Cisco UCS Manager GUI:

Best Effort Policy

1. Select the LAN tab in the left pane in the UCS Manager GUI.
2. Select Policies > root.
4. Select Create QoS Policy.

![Creating QoS Policy](image)

5. Enter BestEffort as the name of the policy.
6. Select BestEffort from the drop down menu.
7. Keep the Burst (Bytes) field as default (10240).
8. Keep the Rate (Kbps) field as default (line-rate).
9. Keep Host Control radio button as default (none).
10. Once the pop-up window appears, click OK to complete the creation of the Policy.
Platinum Policy

1. Select the LAN tab in the left pane in the UCS Manager GUI.
2. Select Policies > root.
4. Select Create QoS Policy.
5. Enter Platinum as the name of the policy.
6. Select Platinum from the drop down menu.
7. Keep the Burst (Bytes) field as default (10240).
8. Keep the Rate (Kbps) field as default (line-rate).
9. Keep Host Control radio button as default (none).
10. Once the pop-up window appears, click OK to complete the creation of the Policy.
Creating Policies for Service Profile Templates

Figure 104 Creating Platinum QoS Policy

![Creating Platinum QoS Policy](image)

Setting Jumbo Frames

Follow these steps for setting up the Jumbo frames and enabling QoS:

1. Select the LAN tab in the left pane in the UCS Manager GUI.
2. Select LAN Cloud > QoS System Class.
3. In the right pane, select the General tab.
4. Check the Enabled Check box next to Platinum.
5. In the Best Effort row, select best-effort for weight.
6. In the Fiber Channel row, select none for weight.
7. Click Save Changes.
8. Click OK.

![Setting Jumbo Frames](image)

Creating Local Disk Configuration Policy

Follow these steps to create local disk configuration in the Cisco UCS Manager GUI:

1. Select the Servers tab on the left pane in the UCS Manager GUI.
2. Go to Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter ucs as the local disk configuration policy name.
6. Change the Mode to Any Configuration. Check the **Protect Configuration** box.
7. Keep the FlexFlash State field as default (Disable).
8. Keep the FlexFlash RAID Reporting State field as default (Disable).
9. Click **OK** to complete the creation of the Local Disk Configuration Policy.
10. Click **OK**.

**Figure 106 Configuring Local Disk Policy**

Creating Server BIOS Policy

The BIOS policy feature in Cisco UCS automates the BIOS configuration process. The traditional method of setting the BIOS is done manually and is often error-prone. By creating a BIOS policy and assigning the policy to a server or group of servers, you can enable transparency within the BIOS settings configuration.
Note

BIOS settings can have a significant performance impact, depending on the workload and the applications. The BIOS settings listed in this section is for configurations optimized for best performance which can be adjusted based on the application, performance and energy efficiency requirements.

Follow these steps to create a server BIOS policy using the Cisco UCS Manager GUI:

1. Select the **Servers** tab in the left pane in the UCS Manager GUI.
2. Select **Policies > root**.
3. Right-click **BIOS Policies**.
4. Select **Create BIOS Policy**.
5. Enter your preferred BIOS policy name (ucs).
6. Change the BIOS settings as per the following figures:

**Figure 107 Creating Server BIOS Policy**
Figure 108  Creating Server BIOS Policy for Processor
7. Click **Finish** to complete creating the BIOS policy.

8. Click **OK**.
Creating Boot Policy

Follow these steps to create boot policies within the Cisco UCS Manager GUI:

1. Select the Servers tab in the left pane in the UCS Manager GUI.
2. Select Policies > root.
3. Right-click the Boot Policies.
4. Select Create Boot Policy.
5. Enter ucs as the boot policy name.
6. (Optional) enter a description for the boot policy.
7. Keep the Reboot on Boot Order Change check box unchecked.
8. Keep Enforce vNIC/vHBA/iSCSI Name check box checked.
10. Expand Local Devices > Add CD/DVD and select Add Local CD/DVD.
11. Expand Local Devices and select Add Local Disk.
12. Expand vNICs and select Add LAN Boot and enter eth0.
13. Click OK to add the Boot Policy.
14. Click OK.
Creating Power Control Policy

Follow these steps to create the Power Control policies within the Cisco UCS Manager GUI:

15. Select the Servers tab in the left pane in the UCS Manager GUI.
17. Right-click the Power Control Policies.
18. Select Create Power Control Policy.
19. Enter ucs as the Power Control policy name.
20. (Optional) enter a description for the boot policy.
21. Select **No cap** for Power Capping selection.
22. Click **OK** to the Power Control Policy.
23. Click **OK**.
Creating Service Profile Template

To create a service profile template, follow these steps:

1. Select the Servers tab in the left pane in the UCS Manager GUI.
2. Right-click Service Profile Templates.
3. Select Create Service Profile Template.

4. The Create Service Profile Template window appears.
   These steps below provide a detailed configuration procedure to identify the service profile template:
   a. Name the service profile template as ucs. Click the Updating Template radio button.
b. In the UUID section, select **Hardware Default** as the UUID pool.

c. Click **Next** to continue to the next section.

**Figure 116 Identify Service Profile Template**

**Configuring Network Settings for the Template**

1. Keep the Dynamic vNIC Connection Policy field at the default.
2. Click the **Expert** radio button for the option, **how would you like to configure LAN connectivity?**
3. Click **Add** to add a vNIC to the template.
4. The Create vNIC window displays. Name the vNIC as eth0.
5. Select UCS in the Mac Address Assignment pool.
6. Click the Fabric A radio button and Check the Enable failover check box for the Fabric ID.
7. Check the vlan160_mgmt check box for VLANs and select the Native VLAN default radio button.
8. Select MTU size as 1500.
9. Select adapter policy as Linux
10. Select QoS Policy as BestEffort.
11. Keep the Network Control Policy as Default.
12. Keep the Connection Policies as Dynamic vNIC.
13. Keep the Dynamic vNIC Connection Policy as <not set>.
14. Click OK.
15. The Create vNIC window appears. Name the vNIC eth1.
16. Select ucs in the Mac Address Assignment pool.
17. Click the Fabric B radio button and Check the Enable failover check box for the Fabric ID.
18. Check the vlan12_HDFS check box for VLANs and select the Native VLAN default radio button.
19. Select MTU size as 1500.
20. Select adapter policy as Linux.
22. Keep the Network Control Policy as Default.
23. Keep the Connection Policies as Dynamic vNIC.
24. Keep the Dynamic vNIC Connection Policy as <not set>.
25. Click OK.
The Create vNIC window appears. Name the vNIC eth2.

27. Select ucs in the Mac Address Assignment pool.

28. Click the Fabric A radio button, and then Check the Enable failover check box for the Fabric ID.

29. Check the vlan11_DATA check box for VLANs and select the Native VLAN default radio button.

30. Select MTU size as 1500.

31. Select adapter policy as Linux.

32. Select QoS Policy as Platinum.

33. Keep the Network Control Policy as Default.

34. Keep the Connection Policies as Dynamic vNIC.

35. Keep the Dynamic vNIC Connection Policy as <not set>.

36. Click OK.
Configuring Storage Policy for the Template

Follow these steps to configure storage policies:

1. Select ucs for the local disk configuration policy.
2. Click the No vHBAs radio button for the option, **How would you like to configure SAN connectivity?**
3. Click **Next** to continue to the next section.
4. Click **Next** once the zoning window appears to go to the next section.
Configuring vNIC/vHBA Placement for the Template

Follow these steps to configure vNIC/vHBA placement policy:

1. Select the Default Placement Policy option for the Select Placement field.
2. Select eth0, eth1 and eth2 assign the vNICs in the following order:
   a. eth0
   b. eth1
   c. eth2
3. Review to make sure that all of the vNICs were assigned in the appropriate order.
4. Click **Next** to continue to the next section.
Configuring vMedia Policy for the Template

1. Click **Next** once the vMedia Policy window appears to go to the next section.
Configuring Server Boot Order for the Template

Follow these steps to set the boot order for servers:

1. Select ucs in the Boot Policy name field.
2. Review to make sure that all of the boot devices were created and identified.
3. Verify that the boot devices are in the correct boot sequence.
4. Click OK.
5. Click Next to continue to the next section.
In the Maintenance Policy window, follow these steps to apply the maintenance policy:

1. Keep the Maintenance policy at no policy used by default.
2. Click Next to continue to the next section.

Configuring Server Assignment for the Template

In the Server Assignment window, follow these steps to assign the servers to the pool:

3. Select ucs for the Pool Assignment field.
4. Keep the Server Pool Qualification field at default.
5. Select ucs in Host Firmware Package.
Configuring Operational Policies for the Template

In the Operational Policies Window, follow these steps:

7. Select ucs in the Power Control Policy field.
8. Click Finish to create the Service Profile template.
9. Click OK in the pop-up window to proceed.
Select the **Servers** tab in the left pane of the UCS Manager GUI.

1. Go to Service Profile **Templates** > **root**.
2. Right-click Service Profile Templates ucs.
3. Select Create Service Profiles From Template.
4. The Create Service Profile from Template window appears.

Association of the Service Profiles will take place automatically.

The Final Cisco UCS Manager window is shown in Figure 131.
Installing Redhat Enterprise Linux 6.5 software RAID on Cisco UCS C240M4 Servers

The following section provides detailed procedure for installing Red Hat Linux 6.5 using Software RAID (OS Based Mirroring) on cisco UCS C240 M4 Servers.

There are multiple methods to install Red Hat Linux operating system. The installation procedure described in this deployment guide uses KVM console and virtual media from Cisco UCS Manager.

1. Log in to the Cisco UCS 6296 Fabric Interconnect and launch the Cisco UCS Manager application.
2. Select the Equipment tab.
3. In the navigation pane expand Rack-mounts and Servers.
4. Right-click the server and select KVM Console.
1. In the KVM window, select the Virtual Media tab.
2. Click the Activate Virtual Devices found under Virtual Media tab.
3. In the KVM window, select the Virtual Media tab and Click the **Map CD/DVD**.

The Red Hat Enterprise Linux 6.5 DVD is assumed to be on the client machine.

5. Click **Open** to add the image to the list of virtual media.

**Figure 134** Browse to Red Hat Enterprise Linux ISO Image

6. In the KVM window, select the **KVM** tab to monitor during boot.
7. In the KVM window, select the **Macros > Static Macros > Ctrl-Alt-Del** button in the upper left corner.
8. Click **OK**.
9. Click **OK** to reboot the system.
10. On reboot, the machine detects the presence of the Red Hat Enterprise Linux Server 6.5 install media.
11. Select the **Install or upgrade an existing system**.
12. Skip the Media test and start the installation

13. Click Next
14. Select language of installation, and then Click Next
15. Select Basic Storage Devices and Click **Next**.
16. Provide hostname and configure Network for the host.
17. Select System eth0 and click **Edit**.

18. In the “Editing System eth0” window select the **IPv4 Settings** tab, from the Method drop-down list choose **Manual** and click **Add** to assign the IP address.
Installing Redhat Enterprise Linux 6.5 software RAID on Cisco UCS C240M4 Servers

Figure 141  RHEL Installation: IPv4 Settings for eth0
Installing Redhat Enterprise Linux 6.5 software RAID on Cisco UCS C240M4 Servers

Figure 142  RHEL Installation: Location Selection
19. Choose **Create Custom Layout** for Installation type.
20. Following steps can be used to create two software RAID 1 partitions for boot and, or (root) partitions.
a. Choose free volume and click on **Create** and choose **RAID Partition**.

**Figure 145  RHEL Installation: Create RAID Partition**

b. Choose “Software RAID” for File system Type and set size for Boot volume
21. Similarly, do the RAID configuration for the other free volume.
Figure 147  RHEL Installation: Create RAID Partition
22. Now similarly create RAID partitions for root (/) partition on both the devices and use rest of the available space.
**Figure 149  RHEL Installation: Create RAID Partition**

![Screenshot of RHEL installation process showing RAID partition creation](image_url)
Figure 150  RHEL Installation: Add RAID Partition
Figure 151  RHEL Installation: Create RAID Partition

![RHEL Installation: Create RAID Partition](image-url)
The above steps created 2 boot and 2 root (/) partitions. Following steps will RAID1 Devices
24. Choose one of the boot partitions and click on **Create > RAID Device**.
25. Choose this as /boot (boot device) and in RAID members, choose all the boot partitions created above in order to create a software RAID 1 for boot.
26. Similarly repeat for / partitions created above choosing both members with mount point as “/”. 
Figure 156  
**RHEL Installation: Select RAID Device**

![RHEL Installation: Select RAID Device](image-url)
Figure 157  RHEL Installation: Make RAID Device
27. Click on **Next**.
Installing Redhat Enterprise Linux 6.5 software RAID on Cisco UCS C240M4 Servers

Note
Swap partition can be created using the similar steps, however, since these systems are high in memory, this step is skipped (click Yes).

28. Click Next, and then click Format.
29. Select default settings and click Next.
30. Continue with RHEL Installation as shown below.
31. Once the installation is complete reboot the system. 

Repeat the steps 1 through 40 to install Red Hat Linux 6.5 on Servers 2 through 160.

**Note**
The OS installation and configuration of the nodes that is mentioned above can be automated through PXE boot or third party tools.

<table>
<thead>
<tr>
<th>Table 10</th>
<th>Host Names and IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>ETH 0</td>
</tr>
<tr>
<td>rhel 1</td>
<td>10.0.145.45</td>
</tr>
<tr>
<td>rhel 2</td>
<td>10.0.145.46</td>
</tr>
<tr>
<td>rhel 3</td>
<td>10.0.145.47</td>
</tr>
</tbody>
</table>
Post OS Install Configuration

Choose one of the nodes of the cluster as Admin Node for management such as CDH installation, parallel shell, creating a local Red Hat repo and others. This CVD uses rhel1 for this purpose.

**Note**
rhel1 is admin node for the entire Hadoop cluster spawning across two different FI domains

Setting Up Password-less Login

To manage all of the clusters nodes from the admin node we need to setup password-less login. It assists in automating common tasks with cluster-shell (clush, a cluster wide parallel shell), and shell-scripts without having to use passwords.

Once Red Hat Linux is installed across all the nodes in the cluster, follow these steps in order to enable password-less login across all the nodes.

1. Login to the Admin Node (rhel1)

```
ssh 10.0.145.45
```
2. Run the ssh-keygen command to create both public and private keys on the admin node.

```
[root@rhel1 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
ab:4e:78:10:54:81:4e:04:3d:af:4f:a1:b2:04:bb:88 root@rhel1
The key's randomart image is:
```

3. Then 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-host’s .ssh/authorized_key.

```
for IP in {101..168}; do echo -n "$IP -> "; ssh-copy-id -i ~/.ssh/id_rsa.pub 10.29.160.$IP; done
```

Enter yes for Are you sure you want to continue connecting (yes/no)?

Enter the password of the remote host.

## Configuring /etc/hosts

Setup /etc/hosts on the Admin node and other nodes as follows; this is a pre-configuration to setup DNS
as shown in the further section.

Follow these steps to create the host file across all the nodes in the cluster:

1. Populate the host file with IP addresses and corresponding hostnames on the Admin node (rhel1)
and other nodes as follows

**On Admin Node (rhel1)**

```
vi /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.0.145.45 rhel1.mgmt
10.0.145.46 rhel2.mgmt
10.0.145.47 rhel3.mgmt
10.0.145.48 rhel4.mgmt
10.0.145.49 rhel5.mgmt
10.0.145.50 rhel6.mgmt
10.0.145.51 rhel7.mgmt
10.0.145.52 rhel8.mgmt
10.0.145.53 rhel9.mgmt
10.0.145.54 rhel10.mgmt
10.0.145.55 rhel11.mgmt
```
Setup ClusterShell

ClusterShell (or clush) is cluster wide shell to run commands on several hosts in parallel.

From the system connected to the Internet download Cluster shell (clush) and install it on rhel1. Cluster shell is available from EPEL (Extra Packages for Enterprise Linux) repository.

```
wget http://dl.fedoraproject.org/pub/epel/6/x86_64/clustershell-1.6-1.el6.noarch.rpm

scp clustershell-1.6-1.el6.noarch.rpm rhel1:/root/
```

Login to rhel1 and install cluster shell

```
yum -y install clustershell-1.6-1.el6.noarch.rpm
```

Edit `/etc/clustershell/groups` file to include host-names for all the nodes of the cluster. These set of hosts are taken when running clush with `-a` option

For 68 node cluster as in our CVD, set groups file as follows,

```
vi /etc/clustershell/groups
all: rhel[1-160]
```

For more information and documentation on ClusterShell, visit


Note

Clustershell will not work if not ssh to the machine earlier (as it requires to be in known_hosts file), for instance, as in the case below.
Creating Red Hat Enterprise Linux (RHEL) 6.5 Local Repo

To create a repository using RHEL DVD or ISO on the admin node (in this deployment rhel1 is used for this purpose), create a directory with all the required RPMs, run the createrepo command and then publish the resulting repository.

1. Log on to rhel1. Create a directory that would contain the repository.

   ```bash
   mkdir -p /var/www/html/rhelrepo
   ```


3. Alternatively, if you have access to a Red Hat ISO Image, Copy the ISO file to rhel1.

   ```bash
   scp rhel-server-6.5-x86_64-dvd.iso rhel1:/root/
   ```

   Here we assume you have the Red Hat ISO file located in your present working directory.

   ```bash
   mkdir -p /mnt/rheliso
   mount -t iso9660 -o loop /root/rhel-server-6.5-x86_64-dvd.iso /mnt/rheliso/
   ```

4. Next, copy the contents of the ISO to the `/var/www/html/rhelrepo` directory

   ```bash
   cp -r /mnt/rheliso/* /var/www/html/rhelrepo
   ```

5. Now on rhel1 create a.repo file to enable the use of the yum command.

   ```bash
   vi /var/www/html/rhelrepo/rheliso.repo
   [rhel6.5]
   name=Red Hat Enterprise Linux 6.5
   baseurl=http://10.29.160.101/rhelrepo
   gpgcheck=0
   enabled=1
   ```

6. Now copy rheliso.repo file from `/var/www/html/rhelrepo` to `/etc/yum.repos.d` on rhel1

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

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

7. Copy the `rheliso.repo` to all the nodes of the cluster.

   ```bash
   clush -a -b -c /etc/yum.repos.d/rheliso.repo --dest=/etc/yum.repos.d/
   ```
8. To make use of repository files on rhel1 without httpd, edit the baseurl of repo file /etc/yum.repos.d/rheliso.repo to point repository location in the file system.

```
vi /etc/yum.repos.d/rheliso.repo
[rhel6.5]
name=Red Hat Enterprise Linux 6.5
baseurl=file:///var/www/html/rhelrepo
gpgcheck=0
enabled=1
```

**Note** This step is needed to install software on Admin Node (rhel1) using the repo (such as httpd, createrepo, etc).

9. Creating the Red Hat Repository Database.

Install the createrepo package on admin node (rhel1). Use it to regenerate the repository database(s) for the local copy of the RHEL DVD contents.

```
yum -y install createrepo
```

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

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

11. Finally, purge the yum caches after httpd is installed (steps in section “Install Httpd”).
Configuring DNS

This section details setting up DNS using dnsmasq as an example based on the /etc/hosts configuration setup in the earlier section.

Follow these steps to create the host file across all the nodes in the cluster:

1. Disable Network manager on all nodes
   - `clush -a -b service NetworkManager stop`
   - `clush -a -b chkconfig NetworkManager off`

2. Update /etc/resolv.conf file to point to Admin Node
   - `vi /etc/resolv.conf`
   - `nameserver 10.0.146.45`
   
   **Note**
   - This step is needed if setting up dnsmasq on Admin node. Else this file should be updated with the correct nameserver.

3. Install and Start dnsmasq on Admin node
   - `yum -y install dnsmasq`
   - `service dnsmasq start`
   - `chkconfig dnsmasq on`

4. Deploy /etc/resolv.conf from the admin node (rhel1) to all the nodes via the following clush command:
   - `clush -a -B -c /etc/resolv.conf`
   
   **Note**
   - A clush copy without - –dest copies to the same directory location as the source-file directory.

5. Ensure DNS is working fine by running the following command on Admin node and any datanode
   - `[root@rhel2 ~]# nslookup rhel1`
     Server: 10.0.146.45
     Address: 10.0.146.45#53
     Name: rhel1
     Address: 10.0.146.45

   - `[root@rhel2 ~]# nslookup rhel1.mgmt`
     Server: 10.0.146.45
     Address: 10.0.146.45#53
     45.146.0.10.in-addr.arpa name = rhel1.mgmt

   - `[root@rhel2 ~]# nslookup rhel1.mgmt`
     Server: 10.0.146.45
     Address: 10.0.146.45#53
     Name: rhel1.mgmt
     Address: 10.0.145.45
Installing httpd

Setting up RHEL repo on the admin node requires httpd. This section describes the process of setting up one.

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 10.0.145.45:80
   ```

3. Start httpd
   ```
   service httpd start
   chkconfig httpd on
   ```

4. Purge the yum caches after httpd is installed (step followed from section Setup Red Hat Repo)
   ```
   clush -a -B yum clean all
   clush -a -B yum repolist
   ```

   ![Output Image]

   **Note**
   While suggested configuration is to disable SELinux as shown below, if for any reason SELinux needs to be enabled on the cluster, then ensure to run the following to make sure that the httpd is able to read the Yum repos files:
   ```
   chcon -R -t httpd_sys_content_t /var/www/html/
   ```

Upgrading Cisco Network driver for VIC1227

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/release.html?mdfid=283862063&flowid=25886&softwareid=283853158&release=1.5.7d&relind=AVAILABLE&rellifecycle=&reltype=latest

In the ISO image, the required driver `kmod-enic-2.1.1.66-rhel6u5.el6.x86_64.rpm` can be located at `\Linux\Network\Cisco\12x5x\RHEL\RHEL6.5`

From a node connected to the Internet, download, extract and transfer `kmod-enic-2.1.1.66-rhel6u5.el6.x86_64.rpm` to rhel1 (admin node).

Install the rpm on all nodes of the cluster using the following clush commands. For this example the rpm is assumed to be in present working directory of rhel1.

```
[root@rhel1 ~]# clush -a -b -c kmod-enic-2.1.1.66-rhel6u5.el6.x86_64.rpm
[root@rhel1 ~]# clush -a -b "rpm -ivh kmod-enic-2.1.1.66-rhel6u5.el6.x86_64.rpm"
```
Ensure 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@rhel1 ~]# clush -a -B "modinfo enic | head -5"
```

<table>
<thead>
<tr>
<th>filename:</th>
<th>/lib/modules/2.6.32-431.el6.x86_64/extra/enic/enic.ko</th>
</tr>
</thead>
<tbody>
<tr>
<td>version:</td>
<td>2.1.1.66</td>
</tr>
<tr>
<td>license:</td>
<td>GPL v2</td>
</tr>
<tr>
<td>author:</td>
<td>Scott Feldman <a href="mailto:scofeldm@cisco.com">scofeldm@cisco.com</a></td>
</tr>
<tr>
<td>description:</td>
<td>Cisco VIC Ethernet NIC Driver</td>
</tr>
</tbody>
</table>

**Installing xfsprogs**

From the admin node rhel1 run the command below to install `xfsprogs` on all the nodes for xfs filesystem.

```
clush -a -B yum -y install xfsprogs
```

```
[root@rhel1 ~]# Clush -a -B yum -y install xfsprogs

```

---

**Package**   | **Arch**   | **Version**   | **Repository** | **Size**
---|---|---|---|---
**Installing:**
- xfsprogs  | x86_64    | 3.1.1-14.el6  | rhe16.5        | 724 k

**Transaction Summary**

- Install 1 Package(s)
- Total download size: 724 k
- Installed size: 3.2 M
- Downloading Packages:
  - Running xps_check_debug
  - Running Transaction Test
  - Transaction Test Succeeded
- Running Transaction
  - Installing: xfsprogs-3.1.1-14.el6.x86_64
  - Verifying: xfsprogs-3.1.1-14.el6.x86_64
- Installed: xfsprogs.x86_64 0:3.1.1-14.el6

Complete!
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 (rhel1). 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.

Configure `/etc/ntp.conf` on the admin node 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
```

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

```
vi /root/ntp.conf
server 10.29.160.101
driftfile /var/lib/ntp/drift
restrict 127.0.0.1
restrict -6 ::1
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys
```

Copy ntp.conf file from the admin node to `/etc` of all the data nodes (except rhel1) by executing the following command in the admin node (rhel1)

```
for SERVER in {46..204}; do scp /root/ntp.conf 10.0.145.$SERVER:/etc/ntp.conf; done
```

Note

To run the above in clush use `-w` option:

```
clush -w rhel[2-160].mgmt -b -c /root/ntp.conf --dest=/etc
```

Do not use `clush -a -b -c /root/ntp.conf --dest=/etc` command as it overwrites `/etc/ntp.conf` on the admin node.
Run the following to synchronize the time and restart NTP daemon on all nodes

```bash
clush -a -B "yum install -y ntpdate"
clush -a -b "service ntpd stop"
clush -a -b "ntpd rhel1"
clush -a -b "service ntpd start"
```

Ensure restart of NTP daemon across reboots

```bash
clush -a -b "chkconfig ntpd on"
```

### Enabling 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. One of the following commands should suffice to confirm that the service is properly configured:

```bash
clush -B -a rsyslogd -v
clush -B -a service rsyslog status
```

![Syslog Configuration](image)

See [http://www.rsyslog.com](http://www.rsyslog.com) for more information.

```bash
clush -B -a service rsyslog status
```

### Setting 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.

Higher values are unlikely to result in an appreciable performance gain.

For setting ulimit on Redhat, edit `/etc/security/limits.conf` on admin node rhel1 and add the following lines:

```bash
vim /etc/security/limits.conf
root soft nofile 64000
root hard nofile 64000
```
Copy the `/etc/security/limits.conf` file from admin node (rhel1) to all the nodes using the following command.

```
clush -a -b -c /etc/security/limits.conf --dest=/etc/security/
```

Verify the `ulimit` setting with the following steps:

```
Note
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
```

Run the following command at a command line. The command should report 64000.

```
clush -B -a ulimit -n
```

**Disabling 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 SELINUX=disabled. The following command will disable SELINUX on all nodes.

```
clush -a -b "sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config ">
clush -a -b "setenforce 0"
```

```
Note
The above command may fail if SELinux is already disabled.
```

**VM.Swapping**

Lowering vm.swappiness reduces anonymous paging and minimizes OOM killer invocations. Run the following on all nodes. Variable vm.swappiness defines how often swap should be used. 0 is No Swapping, 60 default. With vm.swappiness set to 1, the kernel will try to reclaim from the page cache instead of application (anonymous) pages.

```
clush -a -b "echo 'vm.swappiness=1' >> /etc/sysctl.conf"
```

Load the settings from default sysctl file `/etc/sysctl.conf`

```
clush -a -b "sysctl -p"
```
Disable Transparent Huge Pages

Disabling Transparent Huge Pages (THP) reduces elevated CPU usage caused by THP. From the admin node, run the following commands:

```
clush -a -b "echo never > /sys/kernel/mm/redhat_transparent_hugepage/enabled"
clush -a -b "echo never > /sys/kernel/mm/redhat_transparent_hugepage/defrag"
```

The above command needs to be run for every reboot, hence, copy this command to /etc/rc.local so they are executed automatically for every reboot.

On Admin node, run the following commands:

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

Copy file to each node:

```
clush -a -b -c /root/thp_disable
```

Append the content of file thp_disable to /etc/rc.local

```
clush -a -b "cat /root/thp_disable >> /etc/rc.local"
```

Set TCP Retries

Adjusting the tcp_retries parameter for the system network enables faster detection of failed nodes. Given the advanced networking features of UCS, this is a safe and recommended change (failures observed at the operating system layer are most likely serious rather than transitory). 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 rhel1 and add the following lines:

```
net.ipv4.tcp_retries2=5
```

Copy the /etc/sysctl.conf file from admin node (rhel1) to all the nodes using the following command.

```
clush -a -b -c /etc/sysctl.conf --dest=/etc/
```

2. Load the settings from default sysctl file /etc/sysctl.conf by running the below command.

```
clush -B -a sysctl -p
```

Disabling the Linux Firewall

The default Linux firewall settings are far too restrictive for any Hadoop deployment. Since the UCS Big Data deployment will be in its own isolated network, there’s no need to leave the IP tables service running.

```
clush -a -b "service iptables stop"
clush -a -b "chkconfig iptables off"
```

```
[root@rhel1 ~]# clush -a -b "service iptables stop"
[root@rhel1 ~]# clush -a -b "chkconfig iptables off"
```
Disable IPv6 Defaults

Disable IPv6 as the addresses used are IPv4.

```bash
clush -a -b "echo 'net.ipv6.conf.all.disable_ipv6 = 1' >> /etc/sysctl.conf"
clush -a -b "echo 'net.ipv6.conf.default.disable_ipv6 = 1' >> /etc/sysctl.conf"
clush -a -b "echo 'net.ipv6.conf.lo.disable_ipv6 = 1' >> /etc/sysctl.conf"
```

Load the settings from default sysctl file /etc/sysctl.conf

```bash
clush -a -b "sysctl -p"
```

Disable IPv6 Defaults

Disable IPv6 as the addresses used are IPv4.

```bash
clush -a -b "echo 'net.ipv6.conf.all.disable_ipv6 = 1' >> /etc/sysctl.conf"
clush -a -b "echo 'net.ipv6.conf.default.disable_ipv6 = 1' >> /etc/sysctl.conf"
clush -a -b "echo 'net.ipv6.conf.lo.disable_ipv6 = 1' >> /etc/sysctl.conf"
```

Load the settings from default sysctl file /etc/sysctl.conf

```bash
clush -a -b "sysctl -p"
```

Configuring Data Drives on Name Node

This section describes steps to configure non-OS disk drives as RAID1 using StorCli command as described below. All the drives are going to be part of a single RAID1 volume. This volume can be used for Staging any client data to be loaded to HDFS. This volume won’t be used for HDFS data.

From the website download storcli:

Extract the zip file and copy storcli-1.14.12-1.noarch.rpm from the linux directory.

1. Download storcli and its dependencies and transfer to Admin node.

   ```bash
   scp storcli-1.14.12-1.noarch.rpm rhel1:/root/
   ```

2. Copy storcli rpm to all the nodes using the following commands:

   ```bash
clush -a -b -c /root/storcli-1.14.12-1.noarch.rpm --dest=/root/
   ```

3. Run the below command to install storcli on all the nodes

   ```bash
clush -a -b rpm -ivh storcli-1.14.12-1.noarch.rpm
   ```

4. Run the below command to copy storcli64 to root directory.

   ```bash
   cd /opt/MegaRAID/storcli/
   cp storcli64 /root/
   ```

   ```bash
   [root@rhel ~]# cd /opt/MegaRAID/storcli/
   [root@rhel storcli]# ls
   install.log  libstorelibir-2.so  libstorelibir-2.so.14.07-0  storcli64
   [root@rhel storcli]# cp storcli64 /root/
   ```

5. Copy storcli64 to all the nodes using the following commands:

   ```bash
clush -a -b -c /root/storcli64 --dest=/root/
   ```

6. Run the following script as root user on NameNode and Secondary NameNode to create the virtual drives.
Configuring Data Drives on Data Nodes

This section describes steps to configure non-OS disk drives as individual RAID0 volumes using StorCli command as described below. These volumes are going to be used for HDFS Data.

Issue the following command from the admin node to create the virtual drives with individual RAID 0 configurations on all the datanodes.

```
clish -w rhel[3-64] -B ./storcli64 -cfg eachdskraid0 WB RA direct NoCachedBadBBU Strpsz1024 -a0
```

WB: Write back  
RA: Read Ahead  
NoCachedBadBBU: Do not write cache when the BBU is bad.  
Strpsz1024: Strip Size of 1024K

**Note**  
The command above will not override any existing configuration. To clear and reconfigure existing configurations refer to Embedded MegaRAID Software Users Guide available at [www.lsi.com](http://www.lsi.com)

Configuring the Filesystem for NameNodes and DataNodes

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

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

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.
168

Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub

Configuring the Filesystem for NameNodes and DataNodes

Note

The script assumes there are no partitions already existing on the data volumes. If there are partitions, then they have to be deleted first before running this script. This process is documented in the “Note” section at the end of the section.

```bash
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 $X
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 "Setting up Drive => ${X}"
/sbin/parted -s ${X} mklabel gpt quit
/sbin/parted -s ${X} mkpart 1 6144s 100% quit
/sbin/mkfs.xfs -f -q -l size=65536b,lazy-count=1,su=256k -d sunit=1024,swidth=6144 -r
extsize=256k -L ${Y} ${X}1
(( $? )) && continue
#Identify UUID
UUID=`blkid ${X}1 | cut -d " " -f3 | cut -d '=' -f2 | sed 's//g'`
/bin/mkfs.xfs -f -q -l size=65536b,lazy-count=1,su=256k -d sunit=1024,swidth=6144 -r
extsize=256k -L ${Y} ${X}1
(( $? )) && continue
echo "UUID of ${X}1 = ${UUID}, mounting ${X}1 as UUID on /data/disk${count}"
/bin/mount -t xfs -o allocsize=128m,noatime,nobarrier,nodiratime -U ${UUID} /data/disk${count}
(( $? )) && continue
echo "UUID=${UUID} /data/disk${count} xfs allocsize=128m,noatime,nobarrier,nodiratime
0 0" >> /etc/fstab
((count++))
fi
done

2. Run the following command to copy driveconf.sh to all the nodes
   chmod 755 /root/driveconf.sh
   clush –a -B /root/driveconf.sh

3. Run the following command from the admin node to run the script across all data nodes
   clush –a -B /root/driveconf.sh

4. Run the following from the admin node to list the partitions and mount points
   clush –a -B df -h
   clush –a -B mount
```
Cluster Verification

clush –a -B cat /etc/fstab

Note

In-case there is need to delete any partitions, it can be done so using the following. Run command
‘mount’ to identify which drive is mounted to which device /dev/sd<?> umount the drive for which
partition is to be deleted and run fdisk to delete as shown below.
Care to be taken not to delete OS partition as this will wipe out OS
mount
umount /data/disk1 # <-- disk1 shown as example
(echo d; echo w;) | sudo fdisk /dev/sd<?>

Cluster Verification
The section describes the steps to create the script cluster_verification.sh that helps to verify CPU,
memory, NIC, 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.
Create script cluster_verification.sh as follows on the Admin node (rhel1).
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 \ Cluster
Verification === ${NC}"
echo ""
echo ""
echo -e "${green} ==== System Information ==== ${NC}"
echo ""
echo ""
echo -e "${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"

Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub

169


# Cluster Verification

echo **
clush -a -B "\`which lscpu\` | grep -v -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 ifconfig\` | grep -e (^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 "$\{green\}Storage \{NC\}"
clush -a -B "\`echo `Storage Controller:` ; `which lspci` | grep -i -e raid -e storage -e lsi"**
echo **
clush -a -B "dmesg | grep -i raid | grep -i scsi"
echo **
clush -a -B "lsblk -id | awk '{print \$1,\$4}'|sort | nl"
echo **
echo **
echo -e "$\{green\} ================ Software ================ \{NC\}*
echo **
echo **

echo -e "$\{green\}Linux Release \{NC\}"
clush -a -B "\`cat /etc/*release | uniq\``
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 -e "$\{green\}NTP Status \{NC\}"
clush -a -B "\`ntpstat 2>&1 | head -1\``
echo **

echo -e "$\{green\}SELINUX \{NC\}"
clush -a -B "\`echo -n `SELinux status:` ; grep `SELINUX= \ `/etc/selinux/config 2>&1\``
echo **

echo **

echo -e "$\{green\}IPTables \{NC\}"
clush -a -B "\`which chkconfig --list iptables 2>&1\``
echo **

clush -a -B "\`which service` iptables status 2>&1 | head -10"
echo **

echo -e "$\{green\}Transparent Huge Pages \{NC\}"
clush -a -B "\`cat /sys/kernel/mm/*/transparent_hugepage/enabled\``
echo **

echo -e "$\{green\}CPU Speed\{NC\}"
clush -a -B "\`which service` cpuspeed | status 2>&1"
clush -a -B "\`which service` cpuspeed | status 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 **
Installing Cloudera

Cloudera’s Distribution including Apache Hadoop (CDH) is an enterprise grade, hardened Hadoop distribution. CDH offers Apache Hadoop and several related projects into a single tested and certified product. It offers the latest innovations from the open source community with the testing and quality you expect from enterprise quality software.

Pre-Requisites for CDH Installation

This section details the pre-requisites for CDH Installation such as setting up of CDH Repo.

Cloudera Repo

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

```bash
mkdir -p /tmp/clouderarepo/
1. Download Cloudera Manager Repo
   cd /tmp/clouderarepo/
   wget http://archive.cloudera.com/cm5/redhat/6/x86_64/cm/cloudera-manager.repo
```

```bash
Connecting to archive.cloudera.com|184.73.217.71|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 289 [text/plain]
Saving to: cloudera-manager.repo
100%[============================================================================] 204839 bytes received in 1.02s (24.4 MB/s)

reposync --config=/tmp/clouderarepo/cm/cloudera-manager.repo --repoid=cloudera-manager
Installing Cloudera

2. Download Cloudera Manager Installer.

```
cd /tmp/clouderarepo/
```

3. Copy the repository directory to the admin (rhel1) node.

```
scp -r /tmp/clouderarepo/ rhel1:/var/www/html
```

4. On admin node (rhel1) run create repo command.

```
cd /var/www/html/clouderarepo/
```
Installing Cloudera

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

```
vim /var/www/html/clouderarepo/cloudera-manager/cloudera-manager.repo
[cloudera-manager]
name=Cloudera Manager
baseurl=http://10.0.145.45/clouderarepo/cloudera-manager/
gpgcheck = 0
```

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.

```
```

From the admin node copy the repo files to /etc/yum.repos.d/ of all the nodes of the cluster.

```
crush -a -B -c /etc/yum.repos.d/cloudera-manager.repo
```

Setup the Local Parcels for CDH 5.3.2

From a host that’s connected the internet, download the appropriate CDH 5.3.2 parcels that are meant for RHEL6.5 from the URL: http://archive.cloudera.com/cdh5/parcels/ and place them in the directory “/var/www/html/CDH5.3parcels” of the Admin node.

The following screenshot shows the files relevant for RHEL6.5. They are,

- CDH-5.3.2-1.cdh5.3.2.p0.10-el6.parcel
- CDH-5.3.2-1.cdh5.3.2.p0.10-el6.parcel.sha1
- manifest.json
Installing Cloudera

1. `mkdir -p /tmp/clouderarepo/CDH5.3parcels`
2. `cd /tmp/clouderarepo/CDH5.3parcels`
3. Download Parcels

```
wget http://archive.cloudera.com/cdh5/parcels/5.3.2/CDH-5.3.2-1.cdh5.3.2.p0.10-el6.parcel
wget http://archive.cloudera.com/cdh5/parcels/5.3.2/CDH-5.3.2-1.cdh5.3.2.p0.10-el6.parcel.sha1
wget http://archive.cloudera.com/cdh5/parcels/5.3.2/manifest.json
```
4. Now edit the manifest.json file and remove the scripts that are not meant for RHEL6.5. Below is that script which you can copy and paste.

```json
{  
  "lastUpdated": 14248220420000,  
  "parcels": [  
    {  
      "parcelName": "CDH-5.3.2-1.cdh5.3.2.p0.10-el6.parcel",  
      "components": [  
        {  
          "pkg_version": "0.7.0+cdh5.3.2+0",  
          "pkg_release": "1.cdh5.3.2.p0.17",  
          "name": "bigtop-tomcat",  
          "version": "6.0.41-cdh5.3.2"
        },  
        {  
          "pkg_version": "0.11.0+cdh5.3.2+18",  
          "pkg_release": "1.cdh5.3.2.p0.17",  
          "name": "crunch",  
          "version": "0.11.0-cdh5.3.2"
        },  
        {  
          "pkg_version": "1.5.0+cdh5.3.2+84",  
          "pkg_release": "1.cdh5.3.2.p0.17",  
          "name": "flume-ng",  
          "version": "1.5.0-cdh5.3.2"
        },  
        {  
          "pkg_version": "2.5.0+cdh5.3.2+813",  
          "pkg_release": "1.cdh5.3.2.p0.17",  
          "name": "hadoop-0.20-mapreduce",  
          "version": "2.5.0-cdh5.3.2"
        },  
        {  
          "pkg_version": "2.5.0+cdh5.3.2+813",  
          "pkg_release": "1.cdh5.3.2.p0.17"
        }
      ]
    }
  ]
}
```

**Note**  
Make sure the script starts and end with initial additional braces.
Installing Cloudera

```
{"name": "hadoop",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "2.5.0+cdh5.3.2+813",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hadoop-hdfs",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "2.5.0+cdh5.3.2+813",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hadoop-httpfs",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "2.5.0+cdh5.3.2+813",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hadoop-kms",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "2.5.0+cdh5.3.2+813",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hadoop-mapreduce",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "2.5.0+cdh5.3.2+813",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hadoop-yarn",
"version": "2.5.0-cdh5.3.2" },
{"pkg_version": "0.98.6+cdh5.3.2+83",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hbase",
"version": "0.98.6-cdh5.3.2" },
{"pkg_version": "1.5+cdh5.3.2+25",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hbase-solr",
"version": "1.5-cdh5.3.2" },
{"pkg_version": "0.13.1+cdh5.3.2+330",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hive",
"version": "0.13.1-cdh5.3.2" },
{"pkg_version": "0.13.1+cdh5.3.2+330",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hive-hcatalog",
"version": "0.13.1-cdh5.3.2" },
{"pkg_version": "3.7.0+cdh5.3.2+163",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "hue",
"version": "3.7.0-cdh5.3.2" }
```
"pkg_version": "2.1.2+cdh5.3.2+0",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "impala",
"version": "2.1.2-cdh5.3.2"
},

"pkg_version": "0.15.0+cdh5.3.2+193",
"pkg_release": "1.cdh5.3.2.p0.18",
"name": "kite",
"version": "0.15.0-cdh5.3.2"
},

"pkg_version": "1.0.0+cdh5.3.2+0",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "llama",
"version": "1.0.0-cdh5.3.2"
},

"pkg_version": "0.9+cdh5.3.2+19",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "mahout",
"version": "0.9-cdh5.3.2"
},

"pkg_version": "4.0.0+cdh5.3.2+339",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "oozie",
"version": "4.0.0-cdh5.3.2"
},

"pkg_version": "1.5.0+cdh5.3.2+62",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "parquet",
"version": "1.5.0-cdh5.3.2"
},

"pkg_version": "0.12.0+cdh5.3.2+51",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "pig",
"version": "0.12.0-cdh5.3.2"
},

"pkg_version": "1.4.0+cdh5.3.2+128",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "sentry",
"version": "1.4.0-cdh5.3.2"
},

"pkg_version": "4.4.0+cdh5.3.2+326",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "solr",
"version": "4.4.0-cdh5.3.2"
},

"pkg_version": "1.2.0+cdh5.3.2+369",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "spark",
"version": "1.2.0-cdh5.3.2"
},

"pkg_version": "1.99.4+cdh5.3.2+21",
"pkg_release": "1.cdh5.3.2.p0.17",
"name": "sqoop2",
"version": "1.99.4-cdh5.3.2"
5. scp/tmp/clouderarepo/CDH5.3parcels to the /var/www/html directory of Admin node (rhel1).
   
   scp -r /tmp/clouderarepo/CDH5.3parcels/ rhel1:/var/www/html/

6. Verify that these files are accessible by visiting the URL http://10.0.145.45/CDH5.3parcels/ in admin node.

   ![Index of /CDH5.3parcels]

   **Index of /CDH5.3parcels**

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDH-5.3.2-1.cdh5.3.2.p0.10.parcel</td>
<td>18-Mar-2015 18:56</td>
<td>1.5G</td>
<td></td>
</tr>
<tr>
<td>CDH-5.3.2-1.cdh5.3.2.p0.10.parcel.gz</td>
<td>18-Mar-2015 18:56</td>
<td>1.6K</td>
<td></td>
</tr>
<tr>
<td>manifest.json</td>
<td>18-Mar-2015 18:37</td>
<td>6.9K</td>
<td></td>
</tr>
</tbody>
</table>

   Apache/2.2.15 (Red Hat) Server at 10.0.145.45 Port 80

### Setting MySQL Database for Cloudera manager

To use a MySQL database, follow these procedures:

1. Installing the MySQL Server
2. Configuring and Starting the MySQL Server
3. Installing the MySQL JDBC Driver

Following steps provide details of the above procedure for setting MySQL database for Cloudera Manager:

1. Installing the mysql server

   In the admin node where Cloudera manager will be installed, use the following command to install mysql server.

   ```
   [root@rhel1 ]# yum -y install mysql-server
   ```

2. Configuring and starting the MySQL Server

   a. Stop the MySQL server if it is running.

   ```
   [root@rhel1 ]# service mysqld stop
   ```

   b. Move old InnoDB log if exists.

   Move files `/var/lib/mysql/ib_logfile0` and `/var/lib/mysql/ib_logfile1` out of `/var/lib/mysql/` to a backup location.

   ```
   mv /var/lib/mysql/ib_logfile0 /root/ib_logfile0.bkp
   mv /var/lib/mysql/ib_logfile1 /root/ib_logfile1.bkp
   ```

   c. Determine the location of the option file, `my.cnf` and edit/add following lines

   ```
   vim /etc/my.cnf
   [mysqld]
   transaction-isolation = READ-COMMITTED

   # InnoDB settings
   innodb_flush_method = O_DIRECT

   max_connections = 550
   ```
Installing Cloudera

Note: max_connections need to be increased based on number of nodes and applications. Please follow the recommendations as mentioned in Cloudera document:
http://www.cloudera.com/content/cloudera/en/documentation/core/v5-3-x/topics/cm_ig_mysql.html

d. Ensure MySQL Server starts at boot
   
   chkconfig mysqld on

   [root@rhel1 ]# chkconfig --list mysqld
   mysqld 0:off 1:off 2:on 3:on 4:on 5:on 6:off

e. Start the MySQL Server
   
   service mysqld start

   [root@rhel1 -]# chkconfig --list mysqld
   mysqld 0:off 1:off 2:on 3:on 4:on 5:on 6:off
   [root@rhel1 -]# service mysqld start
   Initializing MySQL database: Installing MySQL system tables...
   OK
   Filling help tables...
   OK
   To start mysql at boot time you have to copy support-files/mysql.server to the right place for your system
   PLEASE REMEMBER TO SET A PASSWORD FOR THE MYSQL root USER!
   To do so, start the server, then issue the following commands:
   /usr/bin/mysqladmin -u root password 'new-password'
   /usr/bin/mysqladmin -u root -h rhel1 password 'new-password'
   Alternatively you can run:
   /usr/bin/mysql_secure_installation
   which will also give you the option of removing the test databases and anonymous user created by default. This is strongly recommended for production servers.
   See the manual for more instructions.
   You can start the MySQL daemon with:
   cd /usr ; /usr/bin/mysqld_safe &
   You can test the MySQL daemon with mysql-test-run.pl
   cd /usr/mysql-test ; perl mysql-test-run.pl
   Please report any problems with the /usr/bin/mysqlbug script!

   Starting mysqld: [ OK ]

   f. set the MySQL root password
      
      In the admin node (rhel1) run the mysql_secure_installation to set MySQL root password. The file is located at /usr/bin directory.
[root@rhel1 ]# cd /usr/bin/
[root@rhel1 bin]# mysql_secure_installation

************************OUTPUT**************************
[root@rhel1 bin]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current
password for the root user. If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorization.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
... skipping.

By default, MySQL comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MySQL
3. Installing the MySQL JDBC Driver

Install the JDBC driver on the Cloudera Manager Server host, as well as hosts which run the Activity Monitor, Reports Manager, Hive Metastore Server, Sentry Server, Cloudera Navigator Audit Server, and Cloudera Navigator Metadata Server roles.

**a.** From the host connected to the internet, download the MySQL JDBC driver from: [http://www.mysql.com/downloads/connector/j/5.1.html](http://www.mysql.com/downloads/connector/j/5.1.html).

**Note** select the platform independent from the drop down list and download mysql-connector-java-5.1.34.tar.gz file

**b.** Copy the downloaded file to the admin (rhel1) node, log in to the admin node and extract the file.

```bash
scp mysql-connector-java-5.1.34.tar.gz rhel1:/root/
```

c. Login to the admin (rhel1) node and extract the file.

```bash
tar xzvf mysql-connector-java-5.1.34.tar.gz
```

d. Create `/usr/share/java/` directory in the admin node.

```bash
mkdir -p /usr/share/java/
```

e. Go the mysql-connector-java-5.1.34 directory and copy the mysql-connector-java-5.1.35-bin.jar and rename it to the folder created above as shown in the command below:

```bash
cd mysql-connector-java-5.1.34
cp mysql-connector-java-5.1.34/mysql-connector-java-5.1.34-bin.jar
/usr/share/java/mysql-connector-java.jar
```


**a.** In the admin node (rhel1) Log into MySQL as the root user:

```bash
mysql -u root -p
```

Enter the password that was supplied in step 2.f above

Enter password:

**b.** Create databases for the Activity Monitor, Reports Manager and Hive Metastore Server using the command below:

```bash
Mysql> create database amon DEFAULT CHARACTER SET utf8;
Mysql> create database rman DEFAULT CHARACTER SET utf8;
Mysql> create database metastore DEFAULT CHARACTER SET utf8;
```
Cloudera Installation

The following section describes installation of Cloudera Manager first and then using Cloudera Manager to install CDH 5.3

Installing Cloudera Manager

Cloudera Manager, an end to end management application, is used to install and configure CDH. During CDH Installation, Cloudera Manager’s Wizard will help to install Hadoop services 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 if it is not already installed across all the cluster nodes.
- Assign various services to nodes.
- Start the Hadoop services.

Follow the steps below to install Cloudera Manager.

Update the repo files to point to local repository.

```bash
rm -f /var/www/html/clouderarepo/*.repo
cp /etc/yum.repos.d/c*.repo /var/www/html/clouderarepo/
```
1. Change the permission of Cloudera Manager Installer on the admin node.
   
   ```bash
   cd /var/www/html/clouderarepo
   chmod +x cloudera-manager-installer.bin
   ```

2. Execute the following command in the admin node (rhel1) to start Cloudera Manager Installer.
   
   ```bash
   cd /var/www/html/clouderarepo/
   ./cloudera-manager-installer.bin --skip_repo_package=1
   ```

3. This displays the Cloudera Manager Read Me file. Click Next.

   ![Cloudera Manager README](image)

   Cloudera Manager 5

   The Cloudera Manager Installer enables you to install Cloudera Manager and bootstrap an entire CDH cluster, requiring only that you have SSH access to your cluster’s machines, and that those machines have Internet access.

   This installer is only recommended for demonstration and proof of concept deployments, but is not recommended for production deployments because it is not intended to scale and may require database migration as your cluster grows.

   The Cloudera Manager Installer will automatically:

   * Detect the operating system on the Cloudera Manager host
   * Install the package repository for Cloudera Manager and the Java Runtime Environment (JRE)
   * Install the JRE if it’s not already installed
   * Install and configure an embedded PostgreSQL database
   * Install and run the Cloudera Manager Server

   Once server installation is complete, you can browse to Cloudera Manager’s web interface and use the cluster installation wizard to set up your CDH cluster.

   Cloudera Manager supports the following 64-bit operating systems:

   * Red Hat Enterprise Linux 5 (Update 7 or later recommended)
   * Red Hat Enterprise Linux 6 (Update 4 or later recommended)
   * Oracle Enterprise Linux 5 (Update 6 or later recommended)
   * Oracle Enterprise Linux 6 (Update 4 or later recommended)
   * CentOS 5 (Update 7 or later recommended)
   * CentOS 6 (Update 4 or later recommended)
   * SUSE Linux Enterprise Server 11 (Service Pack 2 or later recommended)

   ![Progress Bar](image)

   < Cancel > < Next >

4. Click Next in the End User License agreement page.
Installing Cloudera

5. Click Yes in the license agreement confirmation page.

6. Click Next in Oracle Binary Code License Agreement and Yes in the Oracle Binary Code License Agreement for the Java SE Platform Products page.
7. Wait for the installer to install the packages needed for Cloudera Manager.
8. Save the url displayed http://10.0.145.45:7180. You will need this url to access Cloudera Manager. If you are unable to connect to the server, check to see if iptables and SELinux are disabled.

9. Click OK.

10. Once the installation of Cloudera Manager is complete. Install CDH5 using the Cloudera Manager web interface.

**Setting up the Cloudera Manager Server Database**

The Cloudera Manager Server database stores information about service and host configurations.

**Preparing a Cloudera Manager Server External Database**

1. Run the scm_prepare_database.sh script on the host where the Cloudera Manager Server package is installed:
   
   ```bash
   [root@rhel1 ~]# cd /usr/share/cmf/schema
   [root@rhel1 schema]# ./scm_prepare_database.sh mysql amon root <password>
   [root@rhel1 schema]# ./scm_prepare_database.sh mysql rman root <password>
   [root@rhel1 schema]# ./scm_prepare_database.sh mysql metastore root <password>
   ```

2. Verify the database connectivity using the following command.

   ```bash
   [root@rhel1 ~]# mysql -u root -p
   Mysql> connect amon
   Mysql> connect rman
   Mysql> connect metastore
   ```
The MySQL External database setup is complete.

## Installing Cloudera Enterprise Data Hub Edition (CDH5)

### Role Assignment

This is one of the critical considerations for the installation. Inspect and customize the role assignments of all the nodes based on your requirements.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>NameNode</td>
<td>rhel1, rhel3 (HA)</td>
</tr>
<tr>
<td>HistoryServer</td>
<td>rhel1</td>
</tr>
<tr>
<td>ResourceManager</td>
<td>rhel2, rhel3 (HA)</td>
</tr>
<tr>
<td>Hue Server</td>
<td>rhel2</td>
</tr>
<tr>
<td>HiveMetastore Server</td>
<td>rhel1</td>
</tr>
<tr>
<td>HiveServer2</td>
<td>rhel2</td>
</tr>
<tr>
<td>HBase Master</td>
<td>rhel2</td>
</tr>
<tr>
<td>Oozie Server</td>
<td>rhel1</td>
</tr>
<tr>
<td>Zookeeper</td>
<td>rhel1, rhel2, rhel3</td>
</tr>
</tbody>
</table>
Installing Cloudera

Scaling the Cluster

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

HDFS High Availability (HA)

The HDFS HA feature provides the option of running two NameNodes in the same cluster, in an Active/Passive configuration. These are referred to as the Active NameNode and the Standby NameNode. Unlike the Secondary NameNode, the Standby NameNode is hot standby, allowing a fast failover to a new NameNode in the 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, see:
http://www.cloudera.com/content/cloudera/en/documentation/core/v5-3-x/topics/cdh_hag_hdfs_ha_intro.html

Note: Setting up HDFS HA is done after Cloudera Install.

Map-Reduce HA (YARN/MRv2)

The YARN ResourceManager (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.
Installating Cloudera

For more information, see:
http://www.cloudera.com/content/cloudera/en/documentation/core/v5-3-x/topics/cdh_hag_rm_ha_conf
ig.html

Note

Setting up YARN HA is done after Cloudera Install.

To install Cloudera Enterprise Data Hub, follow these steps:

2. Login to the Cloudera Manager. Enter "admin" for both the Username and Password fields.

![Login to Cloudera Manager](image)

3. If you do not have a Cloudera license, click Cloudera Enterprise Data Hub Trial Edition. If you do have a Cloudera license, Click “Upload License” and select your license.
4. Based on requirement Choose appropriate Cloudera Editions for Installation.
Welcome to Cloudera Manager. Which edition do you want to deploy?

Upgrading to Cloudera Enterprise Data Hub Edition provides important features that help you manage and monitor your Hadoop clusters in mission-critical environments.

<table>
<thead>
<tr>
<th>Cloudera Express</th>
<th>Cloudera Enterprise Data Hub Edition Trial</th>
<th>Cloudera Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Free</td>
<td>60 Days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node Limit</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For full list of features available in Cloudera Express and Cloudera Enterprise, click here.

5. Click **Continue** in the confirmation page.
Installing Cloudera

### Edit the Cloudera Enterprise Parcel Settings to Use the CDH 5.3.2 Parcels

1. At this point, open another tab in the same browser window and visit the URL:
   http://10.0.145.45:7180/cmf/parcel/status for modifying the parcel settings.
2. Click **Edit Settings** on this page:
3. Click – to remove all the remote repository URLs, and add the URL to the location where we kept the CDH 5.3.2 parcels i.e. http://10.0.145.45/CDH5.3parcels/
4. Click **Save Changes** to finish the configuration.

Now navigate back to the Cloudera installation home page i.e. http://10.0.145.45:7180

5. Click **Continue** in the confirmation page.
6. Specify the hosts that are part of the cluster using their IP addresses or hostname. The figure below shows use of a pattern to specify IP addresses range.

10.0.146.[45-204] or rhel[1-160]

Note: Here, eth1 IP is provided as this is provided with better QoS policy than management VLAN.

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

Specify hosts for your CDH cluster installation.

Hint: Search for hostnames and/or IP addresses using patterns.

rhe{1-160]
8. Cloudera Manager will "discover" the nodes in the cluster. Verify that all desired nodes have been found and selected for installation.

9. For the method of installation, select the **Use Parcels (Recommended)** radio button.

10. For the CDH version, select the **CDH5** radio button.

11. For the specific release of Cloudera Manager, select the **Custom Repository** radio button.

12. Enter the URL for the repository within the admin node:
    http://10.0.145.45/clouderarepo/cloudera-manager and click **Continue**.

**Figure 169  Cluster Installation: Selecting Repository**

**Cluster Installation**

**Select Repository**

Cloud recommends the use of parcels for installation over packages, because parcels enable Cloudera Manager to easily manage the software on your cluster, deployment and upgrade of service binaries. Ejecting noto use parcels will require you to manually upgrade packages on all hosts in your cluster when software up available, and will prevent you from using Cloudera Manager's rolling upgrade capabilities.

**Choose Method**

- Use Packages
- Use Parcels (Recommended)
- More Options

**Select the version of CDH**

- CDH5.3.2-1.cdh5.3.2.0.10

**Select the specific release of the Cloudera Manager Agent you want to install on your hosts.**

- Matched release for this Cloudera Manager Server
- Custom Repository

http://10.0.145.45/clouderarepo/cloudera-manager

**Example for SLES, RedHat or other RPM-based distributions:**

http://archive.cloudera.com/cw6/redhat/6/cw6/cw6-2.0.0.0-1.1

**Example for Ubuntu or other Debian-based distributions:**

deb http://archive.cloudera.com/cw6/ubuntu/cw6-2.0.0.0-1.1 contrib

Enter a custom URL for the location of the GPG signing key (applies to all custom repositories and without internet access)

- Back

13. Check “install Oracle java SE Development kit (JDK)” and click **Continue**.
Figure 170  Cluster Installation: JDK Installation

14. Click **Continue** again.
15. Provide SSH login credentials for the cluster and click Continue.
16. After the installation is successful click **Continue** to begin the parcel installation.
17. Installation using parcels begins.

**Figure 173**  
*Cluster Installation: Installation Selected Parcels*

18. Once the installation is completed successfully click **Continue** to select the required services.
19. Wait for Cloudera Manager to inspect the hosts on which it has just performed the installation.
20. Review and verify the summary. Click Finish.

21. Select services that need to be started on the cluster.
22. This is one of the critical steps in the installation. Inspect and customize the role assignments of all the nodes based on your requirements and click **Continue**.

Reconfigure the service assignment to match the table in “Role Assignment” section on page 188.
### Installing Cloudera

**Cluster Setup: Role Assignment - Part 1**

**Customize Role Assignments**

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**

<table>
<thead>
<tr>
<th>Role</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBase</td>
<td></td>
</tr>
<tr>
<td>Master</td>
<td>rhel2</td>
</tr>
<tr>
<td>HBase REST Server</td>
<td></td>
</tr>
<tr>
<td>HBase Thrift Server</td>
<td></td>
</tr>
<tr>
<td>RegionServer</td>
<td></td>
</tr>
<tr>
<td>NameNode</td>
<td></td>
</tr>
<tr>
<td>SecondaryNameNode</td>
<td></td>
</tr>
<tr>
<td>DataNode</td>
<td></td>
</tr>
<tr>
<td>HDFS</td>
<td></td>
</tr>
<tr>
<td>NFS Gateway</td>
<td></td>
</tr>
<tr>
<td>Hive</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Hive Metastore Server</td>
<td></td>
</tr>
<tr>
<td>WebHCat Server</td>
<td></td>
</tr>
<tr>
<td>HiveServer2</td>
<td></td>
</tr>
</tbody>
</table>

**Cluster Setup: Role Assignment - Part 2**

<table>
<thead>
<tr>
<th>Role</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hue</td>
<td></td>
</tr>
<tr>
<td>Impala</td>
<td></td>
</tr>
<tr>
<td>Key-Value Store Indexer</td>
<td></td>
</tr>
<tr>
<td>Cloudera Management Service</td>
<td></td>
</tr>
</tbody>
</table>

Cisco UCS Integrated Infrastructure for Big Data with Cloudera for Enterprise Data Hub
Using Custom Database

The role assignment recommendation above is for clusters of up to 160 servers. For clusters larger than 160 nodes the recommendation is to dedicate one server each for name node, secondary name node and YARN Resource Manager.

1. Select the **Use Custom Database** radio button.
2. In Database Host Name sections use port 3306 for TCP/IP because connection to the remote server always uses TCP/IP.
3. Enter the Database Name. Username and password that was used during the database creation stage. (Please refer Setting MySQL Database for Cloudera Manager section).
4. Click **Test Connection** to verify the connection, once the connection is successful click **Continue**.
Configuring Yarn (MR2 Included) and HDFS Services

The following parameters are used for Cisco UCS Integrated Infrastructure for Big Data 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 12  Yarn-MR2 Included

<table>
<thead>
<tr>
<th>Service</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mapreduce.map.memory.mb</td>
<td>3 GiB</td>
</tr>
<tr>
<td>mapreduce.reduce.memory.mb</td>
<td>3 GiB</td>
</tr>
<tr>
<td>mapreduce.map.java.opts.max.heap</td>
<td>2560 MiB</td>
</tr>
<tr>
<td>yarn.nodemanager.resource.memorymb</td>
<td>180 GiB</td>
</tr>
<tr>
<td>yarn.nodemanager.resource.cpu-vcores</td>
<td>32</td>
</tr>
<tr>
<td>yarn.scheduler.minimum-allocation-mb</td>
<td>4 GiB</td>
</tr>
<tr>
<td>yarn.scheduler.maximum-allocation-mb</td>
<td>180 GiB</td>
</tr>
</tbody>
</table>
Figure 181

Table 12  Yarn-MR2 Included

<table>
<thead>
<tr>
<th>Service</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>yarn.scheduler.maximum-allocation-vcores</td>
<td>40</td>
</tr>
<tr>
<td>mapreduce.task.io.sort.mb</td>
<td>256 MiB</td>
</tr>
</tbody>
</table>

Table 13  HDFS

<table>
<thead>
<tr>
<th>Service</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dfs.datanode.failed.volumes.tolerated</td>
<td>11</td>
</tr>
<tr>
<td>dfs.datanode.du.reserved</td>
<td>10 GiB</td>
</tr>
<tr>
<td>dfs.datanode.data.dir.perm</td>
<td>755</td>
</tr>
<tr>
<td>Java Heap Size of Namenode in Bytes</td>
<td>2628 MiB</td>
</tr>
<tr>
<td>dfs.namenode.handler.count</td>
<td>54</td>
</tr>
<tr>
<td>dfs.namenode.service.handler.count</td>
<td>54</td>
</tr>
<tr>
<td>Java Heap Size of Secondary namenode in Bytes</td>
<td>2628 MiB</td>
</tr>
</tbody>
</table>

Cluster Setup

Review Changes

- **HDFS Root Directory**
  - Hbase (Service-Wide): 
  - The HDFS directory shared by HBase RegionServers.

- **Enable Replication**
  - HBase (Service-Wide): 
  - Allow HBase tables to be replicated.

- **Enable Indexing**
  - HBase (Service-Wide): 
  - Allow indexing of tables in HBase by Lily HBase Indexer.
  - **Note:** Replication must be enabled for indexing to work.

- **DataNode Data Directory**
  - DataNode Default Group: 
  - Comma-delimited list of directories on the local file system where the DataNode stores HDFS block data. Typical values are /data/disk[1-3]/dn for HBase.
  - These directories should be mounted using the -mnt option and the disks should be configured using RAID. RAID is not recommended.

6. Hadoop services are installed, configured and now running on all the nodes of the cluster. Click **Continue** to complete the installation.
Note

In case Sqoop2 service doesn’t startup due to error “Unable to create database”, while cluster setup stage, please go to troubleshooting section in the Appendix A.
### Starting the Cluster Services

<table>
<thead>
<tr>
<th>Command Progress</th>
<th>Completed 93 of 93 steps</th>
</tr>
</thead>
</table>
| ✓ Initializing Zookeeper Service | |}
| ✓ Starting Zookeeper Service | |}
| ✓ Creating the same directories of the NameNode are empty. Formatting HDFS only if empty. | |}
| ✓ Starting HDFS Service | |}
| ✓ Creating HDFS tmp directory | |}
| ✓ Creating HBase root directory | |}
| ✓ Starting HBase Service | |}
| ✓ Initializing Sot in Zookeeper | |}
| ✓ Starting HBase 2 Service | |}
| ✓ Starting YARN (MR2 included) Service | |}
| ✓ Creating HIVE metastore | |}
| ✓ Creating HIVE user directory | |}
| ✓ Starting HIVE metastore | |}
| ✓ Starting HIVE service | |}
| ✓ Starting HIVE 2 service | |}
| ✓ Executing command CreateSparkRediServiceCommand on service Spark | |}
| ✓ Executing command CreateSparkRediServiceCommand on service Spark | |}
| ✓ Executing command CreateSparkRediServiceCommand on service Spark | |}
| ✓ Executing command CreateSparkRediServiceCommand on service Spark | |}
| ✓ Starting Spark 2 Service | |}
| ✓ Starting Spark 2 Service | |}
| ✓ Creating Spark 2 user directory | |}
| ✓ Creating Spark 2 database | |}

---

Figure 182: Starting the Cluster Services
7. Cloudera Manager will now show the status of all Hadoop services running on the cluster.

![Cluster Setup Completion](image1)

**Cluster Setup**

**Congratulations!**

The services are installed, configured, and running on your cluster.

![Service Status of the Cluster](image2)

**Setting up HDFS HA**

The **Enable High Availability** workflow leads through adding a second (standby) NameNode and configuring JournalNodes. During the workflow, Cloudera Manager creates a **federated namespace**.

1. Log in to the admin node (rhel1) and create the Edit directory for the JournalNode hosts.

   ```bash
   clush -w rhel[1-3] mkdir -p /data/disk1/namenode-edits
   clush -w rhel[1-3] chmod 777 /data/disk1/namenode-edits
   ```
2. Log in to the Cloudera manager and go to the HDFS service.

3. In the top right corner Select Actions > Enable High Availability. A screen showing 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.

5. In the NameNode Hosts field, click Select a host. The host selection dialog displays.
6. Check the checkbox next to the hosts (rhel3) where you want the standby NameNode to be set up and click **OK**.

**Note** 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.

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**. Here we are using the same nodes as Zookeeper nodes.
Installing Cloudera

Note  JournalNodes should be hosted on hosts with similar hardware specification as the NameNodes. It is recommended that you put a JournalNode each on the same hosts as the active and standby NameNodes, and the third JournalNode on ResourceManager node.

9. Click Continue.

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

Note  The directories you specify 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.

Note  If choosen not to do so, the data should be in sync across the edits directories of the JournalNodes and should have the same version data as the NameNodes.

12. 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.

**Note** Formatting of name directory is expected to fail as the directories are not empty as is the case here.
13. In the next screen additional steps are suggested by the Cloudera Manager to update the Hue and Hive metastore. Click **finish** for the screen shown below.

**Note** The following subsections will cover configuring Hue and Hive for HA as needed.

14. In the Cloudera Manager, Click on **Home > HDFS > Instances** to see Namenode in High Availability.

### Configuring Hive Metastore to Use HDFS HA

The Hive metastore can be configured to use HDFS high availability.

1. Go to the Hive service.
2. Select **Actions > Stop**.
3. Click **Stop** to confirm the command.
4. Back up the Hive metastore database.
5. Select **Actions > Update Hive Metastore NameNodes** and confirm the command.
6. Select **Actions > Start**.
7. Restart the Hue and Impala services if stopped prior to updating the metastore.

### Configuring Hue to Work with HDFS HA

1. Go to the HDFS service.
2. Click the **Instances** tab.
3. Click **Add Role Instances**.
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**.
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 you just created instead of the NameNode role, and save your changes.

12. Restart the Hue service.

**Configuring Impala to Work with HDFS HA**

1. Complete the steps to reconfigure the Hive metastore database, as described in the preceding section. Impala shares the same underlying database with Hive, to manage metadata for databases, tables, and so on.
2. Log in to the admin node (rhel1) and ssh to rhel2. Run command impala-shell.
3. Issue the **INVALIDATE METADATA** statement from an Impala shell. This one-time operation makes all Impala daemons across the cluster aware of the latest settings for the Hive metastore database. Alternatively, restart the Impala service.
For more information, see: http://www.cloudera.com/content/cloudera/en/documentation/core/v5-3-x/topics/impala_invalidate_metadata.html

Configuring Oozie to Use HDFS HA

To configure an Oozie workflow to use HDFS HA, use the HDFS nameservice (nameservice1) instead of the NameNode URI in the <name-node> element of the workflow.

Setting up MapReduce v2 (YARN) HA

1. Log in to the Cloudera manager and go to the YARN service.
2. Select Actions > Enable High Availability. A screen showing 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 (rhel3) where the standby ResourceManager is to be installed, and click Continue.

4. 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 redeploy the relevant client configurations.
5. Click **Finish** once the installation is completed successfully.

**Changing the log directory**

To change the default log from the /var prefix to /data/disk1, follow these steps:

1. Log into the cloudera home page and click **Clusters**.
2. From the configuration drop-down menu select “All Log Directories”.
3. Change the path of the log directory to /data/disk1/log/<service-name> as shown in the fig below.
Figure 186  Change Path of the Log Directory - Part1
Conclusion

Hadoop has become a popular data management across all verticals. Cisco UCS Integrated Infrastructure for Big Data and Cisco Application Centric Infrastructure (ACI) along with Cloudera offers a dependable deployment model for enterprise Hadoop that offer a fast and predictable path for businesses to unlock value in big data. This architecture allows using the UCS Manager capabilities in F1 for provisioning the servers within a single domain while interconnecting multiple Fabric Interconnect domains with ACI.

The configuration detailed in the document can be extended to clusters of various sizes depending on what application demands as discussed in the Scalability section. Next generation Big Data Infrastructure needs to cater to the emerging trends in Big Data Applications to meet multiple Lines of Business (LOB) SLAs. Cisco UCS Integrated Infrastructure for Big Data and Cisco ACI brings numerous advantages to a Big Data cluster – fewer point of management for the network, enhanced performance, superior failure handling characteristics, unprecedented scalability. Further, ACI paves way to the next generation data center network accelerating innovation with its SDN capabilities in the Big Data space.

Bill of Materials

This section gives the BOM for the 160 node Performance optimized Cluster. See Table 14 for BOM for the master rack, Table 15 for the expansion rack, Table 16 and 17 for software components and Table 18 for Nexus 9k and APIC.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS-SL-CPA3-P</td>
<td>Performance Optimized Cluster</td>
<td>1</td>
</tr>
<tr>
<td>UCSC-C240-M4SX</td>
<td>UCS C240 M4 SFF 24 HD w/o CPU, mem, HD, PCIe, PS, railkt w/expandr</td>
<td>16</td>
</tr>
</tbody>
</table>
**Table 14  Bill of Materials for C240M4SX Base Rack**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSC-MRAID12G</td>
<td>Cisco 12G SAS Modular Raid Controller</td>
<td>16</td>
</tr>
<tr>
<td>UCSC-MRAID12G-2GB</td>
<td>Cisco 12Gbps SAS 2GB FBWC Cache module (Raid 0/1/5/6)</td>
<td>16</td>
</tr>
<tr>
<td>UCSC-MLOM-CSC-02</td>
<td>Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+</td>
<td>16</td>
</tr>
<tr>
<td>CAB-9K12A-NA</td>
<td>Power Cord 125VAC 13A NEMA 5-15 Plug North America</td>
<td>32</td>
</tr>
<tr>
<td>UCSC-PSU2V2-1200W</td>
<td>1200W V2 AC Power Supply for 2U C-Series Servers</td>
<td>32</td>
</tr>
<tr>
<td>UCSC-RAILB-M4</td>
<td>Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers</td>
<td>16</td>
</tr>
<tr>
<td>UCSC-HS-C240M4</td>
<td>Heat Sink for UCS C240 M4 Rack Server</td>
<td>32</td>
</tr>
<tr>
<td>UCSC-SCCBL240</td>
<td>Supercap cable 250mm</td>
<td>16</td>
</tr>
<tr>
<td>UCS-CPU-E52680D</td>
<td>2.50 GHz E5-2680 v3/120W 12C/30MB Cache/DDR4 2133MHz</td>
<td>32</td>
</tr>
<tr>
<td>UCS-MR-1X162RU-A</td>
<td>16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v</td>
<td>256</td>
</tr>
<tr>
<td>UCS-HD12T10KS2-E</td>
<td>1.2 TB 6G SAS 10K rpm SFF HDD</td>
<td>384</td>
</tr>
<tr>
<td>UCS-SD120G0KSB-EV</td>
<td>120 GB 2.5 inch Enterprise Value 6G SATA SSD (BOOT)</td>
<td>32</td>
</tr>
<tr>
<td>UCSC-PCI-1C-240M4</td>
<td>Right PCI Riser Bd (Riser 1) 2onbd SATA bootdrvs+ 2PCI slts</td>
<td>16</td>
</tr>
<tr>
<td>UCS-FI-6296UP-UPG</td>
<td>UCS 6296UP 2RU Fabric Int/No PSU/48 UP/18p LIC</td>
<td>2</td>
</tr>
<tr>
<td>CON-SNTP-FI6296UP</td>
<td>SMARTNET 24X7X4 UCS 6296UP 2RU Fabric Int/2 PSU/4 Fans</td>
<td>2</td>
</tr>
<tr>
<td>SFP-H10GB-CU3M</td>
<td>10GBASE-CU SFP+ Cable 3 Meter</td>
<td>60</td>
</tr>
<tr>
<td>UCS-ACC-6296UP</td>
<td>UCS 6296UP Chassis Accessory Kit</td>
<td>2</td>
</tr>
<tr>
<td>UCS-PSU-6296UP-AC</td>
<td>UCS 6296UP Power Supply/100-240VAC</td>
<td>4</td>
</tr>
<tr>
<td>N10-MGT012</td>
<td>UCS Manager v2.2</td>
<td>2</td>
</tr>
<tr>
<td>UCS-L-6200-10G-C</td>
<td>2nd Gen FI License to connect C-direct only</td>
<td>108</td>
</tr>
<tr>
<td>UCS-BLKE-6200</td>
<td>UCS 6200 Series Expansion Module Blank</td>
<td>6</td>
</tr>
<tr>
<td>UCS 6296UP Fan Module</td>
<td>UCS 6296UP Fan Module</td>
<td>8</td>
</tr>
<tr>
<td>CAB-9K12A-NA</td>
<td>Power Cord 125VAC 13A NEMA 5-15 Plug North America</td>
<td>4</td>
</tr>
<tr>
<td>UCS-FI-E16UP</td>
<td>UCS 6200 16-port Expansion module/16 UP/8p LIC</td>
<td>6</td>
</tr>
<tr>
<td>RACK-UCS2</td>
<td>Cisco R42610 standard rack w/side panels</td>
<td>1</td>
</tr>
</tbody>
</table>
### Table 14  Bill of Materials for C240M4SX Base Rack

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP208-30-1P-U-2=</td>
<td>Cisco RP208-30-U-2 Single Phase PDU 20x C13 4x C19 (Country Specific)</td>
<td>2</td>
</tr>
<tr>
<td>CON-UCW3-RPDUX</td>
<td>UC PLUS 24X7X4 Cisco RP208-30-U-X Single Phase PDU 2x (Country Specific)</td>
<td>6</td>
</tr>
</tbody>
</table>

### Table 15  Bill of Materials for C240M4SX Expansion Rack

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSC-C240-M4SX</td>
<td>UCS C240 M4 SFF 24 HD w/o CPU, mem, HD, PCIe, PS, railkt w/expndr</td>
<td>64</td>
</tr>
<tr>
<td>UCSC-MRAID12G</td>
<td>Cisco 12G SAS Modular Raid Controller</td>
<td>64</td>
</tr>
<tr>
<td>UCSC-MRAID12G-2GB</td>
<td>Cisco 12Gbps SAS 2GB FBWC Cache module (Raid 0/1/5/6)</td>
<td>64</td>
</tr>
<tr>
<td>UCSC-MLOM-CSC-02</td>
<td>Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+</td>
<td>64</td>
</tr>
<tr>
<td>CAB-9K12A-NA</td>
<td>Power Cord 125VAC 13A NEMA 5-15 Plug North America</td>
<td>128</td>
</tr>
<tr>
<td>UCSC-PSU2V2-1200W</td>
<td>1200W V2 AC Power Supply for 2U C-Series Servers</td>
<td>128</td>
</tr>
<tr>
<td>UCSC-RAILB-M4</td>
<td>Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers</td>
<td>64</td>
</tr>
<tr>
<td>UCSC-HS-C240M4</td>
<td>Heat Sink for UCS C240 M4 Rack Server</td>
<td>128</td>
</tr>
<tr>
<td>UCSC-SCCBL240</td>
<td>Supercap cable 250mm</td>
<td>64</td>
</tr>
<tr>
<td>UCSC-CPU-E52680D</td>
<td>2.50 GHz E5-2680 v3/120W 12C/30MB Cache/DDR4 2133MHz</td>
<td>128</td>
</tr>
<tr>
<td>UCSC-MR-1X162RU-A</td>
<td>16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v</td>
<td>1024</td>
</tr>
<tr>
<td>UCSC-HD12T10KS2-E</td>
<td>1.2 TB 6G SAS 10K rpm SFF HDD</td>
<td>1536</td>
</tr>
<tr>
<td>UCSC-SD120G0KSB-EV</td>
<td>120 GB 2.5 inch Enterprise Value 6G SATA SSD (BOOT)</td>
<td>128</td>
</tr>
<tr>
<td>UCSC-PCI-1C-240M4</td>
<td>Right PCI Riser Bd (Riser 1) 2onbd SATA bootdrvs+ 2PCI slts</td>
<td>64</td>
</tr>
</tbody>
</table>

**Note**  If using 6 TB drives for C3160, use the following PID instead of 4TB drives.

SFP-H10GB-CU5M= 10GBASE-CU SFP+ Cable 5 Meter  128
RACK-UCS2Cisco R42610 standard rack w/side panels  4
<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP208-30-1P-U-2=</td>
<td>Cisco RP208-30-U-2 Single Phase PDU 20x C13 4x C19 (Country Specific)</td>
<td>8</td>
</tr>
<tr>
<td>CON-UCW3-RPDUX</td>
<td>UC PLUS 24X7X4 Cisco RP208-30-U-X Single Phase PDU 2x (Country Specific)</td>
<td>24</td>
</tr>
</tbody>
</table>

**Table 16  Red Hat Enterprise Linux License**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL-2S-1G-3A</td>
<td>Red Hat Enterprise Linux</td>
<td>160</td>
</tr>
<tr>
<td>CON-ISV1-RH2S1G3A</td>
<td>3 year Support for Red Hat Enterprise Linux</td>
<td>160</td>
</tr>
</tbody>
</table>

**Table 17  Cloudera License**

Note: Choose one of the part numbers.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS-BD-CEBN=</td>
<td>Cloudera Enterprise Basic Edition</td>
<td>160</td>
</tr>
<tr>
<td>UCS-BD-CEFN=</td>
<td>Cloudera Enterprise Flex Edition</td>
<td>160</td>
</tr>
<tr>
<td>UCS-BD-CEDN=</td>
<td>Cloudera Enterprise Data Hub Edition</td>
<td>160</td>
</tr>
</tbody>
</table>

**Table 18  Bill of Materials for Nexus Device and APIC**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>N9K-C9508-B2</td>
<td>Nexus 9508 Chassis Bundle with 1 Sup, 3 PS, 2 SC, 6 FM, 3 FT</td>
<td>2</td>
</tr>
<tr>
<td>N9K-C9396PX</td>
<td>Nexus 9300 with 48p 1/10G SFP+ and 1 uplink module slot</td>
<td>2</td>
</tr>
<tr>
<td>N9k-X9736PQ</td>
<td>Spine Line-Card</td>
<td>2</td>
</tr>
<tr>
<td>APIC-L1</td>
<td>APIC Appliance</td>
<td>3</td>
</tr>
<tr>
<td>N9K POWERCABLES</td>
<td>Power Cables</td>
<td>3</td>
</tr>
<tr>
<td>CAB-C13-C14-AC</td>
<td>Power cord, C13 to C14 (recessed receptacle), 10A</td>
<td>4</td>
</tr>
<tr>
<td>QSFP-H40G-CU3M</td>
<td>40GBASE-CR4 Passive Copper Cable, 3m</td>
<td>24</td>
</tr>
<tr>
<td>N9K-M12PQ</td>
<td>ACI Uplink Module for Nexus 9300, 12p 40G QSFP</td>
<td>3</td>
</tr>
<tr>
<td>N9K-C9500-RMK</td>
<td>Nexus 9500 Rack Mount Kit</td>
<td>2</td>
</tr>
<tr>
<td>CAB-C19-CBN</td>
<td>Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors</td>
<td>6</td>
</tr>
<tr>
<td>N9K-C9500-LC-CV</td>
<td>Nexus 9500 Linecard slot cover</td>
<td>16</td>
</tr>
<tr>
<td>N9K-C9500-SUP-CV</td>
<td>Nexus 9500 Supervisor slot cover</td>
<td>2</td>
</tr>
</tbody>
</table>
Appendix A

Troubleshooting

Troubleshooting Sqoop2 process startup

In case Sqoop2 service doesn’t startup due to error “Unable to create database”, while cluster setup stage, do the following:

1. Form the node connected to the internet download and Copy derby from Apache Derby.
   ```
   wget http://apache.mirrors.pair.com//db/derby/db-derby-10.11.1.1/db-derby-10.11.1.1-bin.zip
   ```
2. Copy to Admin node (rhel1) and unzip the file.
   ```
   scp db-derby-10.11.1.1-bin.zip rhel1:/root/
   unzip db-derby-10.11.1.1-bin.zip
   ```
3. Copy derby.jar and derbyclient.jar to /var/lib/sqoop2/ on Admin Node (rhel1).
   ```
   cd db-derby-10.11.1.1-bin/lib/
   cp derby.jar /var/lib/sqoop2/
   cp derbyclient.jar /var/lib/sqoop2/
   ```
4. Copy derby.jar and derbyclient.jar to /var/lib/sqoop2/ on all Nodes.
   ```
   cd /var/lib/sqoop2/
   # ls
   derbyclient.jar derby.jar mysql-connector-java.jar postgresql-9.0-801.jdbc4.jar
   tomcat-deployment
   clush -a -b -c derby*
   clush -a -b ls /var/lib/sqoop2/
   ```
5. Change the link to derby.jar and derbyclient.jar in parcels.
   ```
   clush -a -b rm -f
   /opt/cloudera/parcels/CDH-5.3.2-1.cdh5.3.2.p0.10/lib/sqoop2/webapps/sqoop/WEB-INF/lib/
   derby-10.8.2.2.jar
   ```

Note
This step is not needed if Sqoop2 service comes up fine.
6. Retry cluster setup operation.

Cisco UCS Director Express for Big Data

Introduction

Hadoop has become a strategic data platform embraced by mainstream enterprises as it offers the fastest path for businesses to unlock value in big data while maximizing existing investments.

As you consider Hadoop to meet your growing data and business needs, operational challenges often emerge. Despite its compelling advantages, Hadoop clusters can be difficult, complex, and time consuming to deploy. Moreover, with so much data increasing so quickly, there is a need to find ways to consistently deploy Hadoop clusters and manage them efficiently.

The UCSD Express appliances (UCSD Express VM and Baremetal Agent VM) can also be installed on an existing VMware ESXi server with proper network connectivity (See Figure 174) to the UCS domain that manages the Hadoop servers. In such a case, skip the sections until Downloading the UCS Director Express software components.

UCS Director Express for Big Data

Cisco UCS Director Express for Big Data provides a single-touch solution that automates deployment of Hadoop on Cisco UCS Common Platform Architecture (CPA) for Big Data infrastructure. It also provides a single management pane across both Cisco UCS integrated infrastructure and Hadoop software. All elements of the infrastructure are handled automatically with little need for user input. Through this approach, configuration of physical computing, internal storage, and networking infrastructure is integrated with the deployment of operating systems, Java packages, and Hadoop along with the provisioning of Hadoop services. Cisco UCS Director Express for Big Data is integrated with major Hadoop distributions from Cloudera, MapR, and Hortonworks, providing single-pane management across the entire infrastructure. It complements and communicates with Hadoop managers, providing a system wide perspective and enabling administrators to correlate Hadoop activity with network and computing activity on individual Hadoop nodes.
Key features of UCS Director (UCSD) Express for Big Data

- **Faster and Easier Big Data Infrastructure Deployment**: Cisco UCS Director Express for Big Data extends the Cisco UCS Integrated Infrastructure for Big Data with one-click provisioning, installation, and configuration, delivering a consistent, repeatable, flexible, and reliable end-to-end Hadoop deployment.

- **Massive Scalability and Performance**: Cisco’s unique approach provides appliance-like capabilities for Hadoop with flexibility that helps ensure that resources are deployed right the first time and can scale without arbitrary limitations.

- **Centralized Visibility**: Cisco UCS Director Express for Big Data provides centralized visibility into the complete infrastructure to identify potential failures and latent threats before they affect application and business performance.

- **Open and Powerful**: Provides open interfaces that allows further integration into third-party tools and services while allowing flexibility for your own add-on services.

UCSD Express Management Server Configuration

The basic requirement for deploying and executing the UCSD Express software is a server with VMWare ESXi based virtualization environment. Such a physical server machine with ESXi must be connected to the target Hadoop servers in the UCS domain by means of the management network and a dedicated PXE network.

The following are the potential network topologies:

1. The UCSD Express Management server is outside of the UCS Domain containing the C-Series servers that would be used to form the Hadoop cluster. For example, a standalone (CIMC managed) C220 M4 rack server provisioned with UCSD Express VMs is connected to the UCS Domain.
2. The UCSD Express Management server is hosted on a C220 M4 rack server that is connected to and managed by the same UCS Domain. This is the method used in this document.
For this deployment a C220 M4 rack server equipped with Intel Xeon E5-2620 v3 processors, 128 GB of memory, Cisco UCS Virtual Interface Card 1227, Cisco 12-Gbps SAS Modular Raid Controller with 512-MB FBWC, 4 X 600 GB 10K SFF SAS drives is used (any other Cisco UCS server can also be used for this purpose).

The C220 M4 server shall be connected to the UCS Fabric Interconnects as shown in Figure 188. The ports on the on the Fabric Interconnects must be configured as server ports.
Software Versions

The UCSD management server is a C220 M4 server that is managed by the UCS Manager. Refer to the software information section in the main part of this Cisco UCS Integrated Infrastructure for Big Data with Hortonworks. See Software Distributions and Versions. In addition, the following software distributions are necessary.

**UCS Director Express for Big Data (1.1)**


**VMware vSphere 5.5**

UCS Director express requires the VMware vSphere 5.5 hypervisor. For more information see [http://www.vmware.com](http://www.vmware.com)
Fabric Configuration

The UCSD management server is a C220 M4 server that is managed by the UCS Manager. Refer to the Fabric Configuration section in the main part of this document for more details.

Configuring VLANs

UCSD Express management server requires two network interfaces. It’s service profile need to be

- Management Network – default (VLAN 1)
- PXE Network

Table 19 UCSD Express Management Server vNIC configurations

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Fabric</th>
<th>NIC Port</th>
<th>Function</th>
<th>Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>default(VLAN1)</td>
<td>A</td>
<td>eth0</td>
<td>Management, User connectivity</td>
<td>Fabric Failover to B</td>
</tr>
<tr>
<td>vlan85_PXE</td>
<td>B</td>
<td>eth1</td>
<td>PXE</td>
<td>Fabric Failover to A</td>
</tr>
</tbody>
</table>

PXE VLAN dedicated for PXE booting purpose. Follow these steps in Configuring VLANs to create a dedicated VLAN for PXE. The management network shall continue to be on the default VLAN.

Other UCS configurations

Perform all other UCS configurations such as QOS policy, necessary policies and service profile template by following the documentation above. See the section Creating Pools for Service Profile Templates onwards in this Cisco UCS Integrated Infrastructure for Big Data with Hortonworks cisco validated design.

Note

Create the service profile template named as ESXi_Host with two vNICs as shown in the above table. For vNIC eth0, select default VLAN as the native VLAN, and for vNIC eth1, select PXE VLAN (vlan85_PXE) as the native VLAN.

Creating Service Profile from the Template

Select the Servers tab in the left pane of the UCS Manager GUI.

1. Go to Service Profile Templates > root.
2. Right-click Service Profile Templates ESXi_Host.
3. Select Create Service Profiles From Template.
4. The Create Service Profile from Template window appears.

Association of the Service Profiles will take place automatically.

Installing VMware vSphere ESXi 5.5

The following section provides detailed procedures for installing VMware vSphere ESXi 5.5. There are multiple methods to install VMware vSphere ESXi 5.5. The installation procedure described in this deployment guide uses KVM console and virtual media from Cisco UCS Manager.

1. Log in to the Cisco UCS 6296 Fabric Interconnect and launch the Cisco UCS Manager application.
2. Select the **Servers** tab.

3. In the navigation pane expand Service Profiles.

4. Right click on the newly created service profile ESXi1 and select KVM Console.

**Figure 193  Selecting KVM Console**

5. In the KVM window, force a reboot by executing the **Ctrl-Alt-Del** macro.
6. As the server goes through a reboot, monitor the progress via the KVM window. When the LSI MegaRAID SAS-MFI BIOS screen appears, press **Ctrl-R** to Enter the Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility.
7. In the MegaRAID configuration utility, under VD Mgmt section, use the arrow keys to select the Cisco 12G SAS Modular RAID (Bus 0xNN, Dev 0xNN) line item.

8. Press the function key **F2**.

9. Select the option **Clear Configuration**, and press **ENTER**.
10. To the question Are you sure you want to clear the configuration? click **YES** and press **ENTER** key.
11. In the VD Mgmt section, use the arrow keys to select the Cisco 12G SAS Modular RAID (Bus 0xNN, Dev 0xNN) line item.

12. Press the function key F2, select Create Virtual Drive and press ENTER.
13. In the RAID Level: press ENTER and choose RAID-5.

14. In the Drives section, press SPACE on the desired number of drives to select them to be part of the RAID group. Use the Up and Down arrow keys to navigate.

15. Select the Advanced button, and Check the Initialize checkbox.

16. Press OK to continue with initialization.
17. After the initialization is complete, the following message appears. Press OK to continue.

18. Press Ctrl-N twice to navigate to the Ctrl Mgmt screen.
19. Select Boot device field and press ENTER.
20. Select the **VD 0**, and press **ENTER** again.
21. Press **Ctrl+S** to save the configuration.
22. Press **ESC** to exit the MegaRAID configuration utility.

23. In the KVM window, select the Virtual Media menu.
24. Click the Activate Virtual Devices found in the right hand corner of the Virtual Media selection menu.
25. In the KVM window, select the Virtual Media menu and Select Map CD/DVD.
26. Browse to the VMware vSphere ESXi 5.5 installer ISO image file.

Note The VMware vSphere ESXi 5.5 installable ISO is assumed to be on the client machine.

27. Click Open to add the image to the list of virtual media.
28. In the KVM window, select the **KVM** tab to monitor during boot.

29. In the KVM window, select the **Macros > Static Macros > Ctrl-Alt-Del** button in the upper left corner.

30. Click **OK** to reboot the system.

31. On reboot, the machine detects the presence of the VMWare ESXi install media.

---

**Figure 197** Browse to VMWare ESXi Hypervisor ISO Image

**Figure 198** ESXi Standard Boot Menu
32. Select the ESXi-5.5.0-yyyymmddnnn-standard Installer. The installer begins automatically.

Figure 199  Loading the ESXi Installer

Figure 200  VMWare ESXi Installation screen

33. Press ENTER to continue.
34. Press **F11** to accept End user License Agreement (EULA) and continue.

*Figure 201   Accept End User License Agreement (EULA)*

35. Select the storage device. Press **ENTER** to proceed with the installation.

*Figure 202   Selecting the Storage Device for installing the ESXi operating system.*

36. Select the Keyboard US Default. Press **ENTER** to continue.
37. Choose the root password and confirm it. Press ENTER to continue.

38. Press F11 to confirm and begin installation.

39. Once the installation completes, the following message is displayed in the KVM.

40. Remove the VMWare vSphere Hypervisor’s ISO from the Virtual Media menu, by selecting it as shown.
41. Click **Yes** to proceed with un-mapping of the ISO.

42. Press **ENTER** to reboot the server.

The VMWare vSphere ESXi installation is complete.

### Configuring the Management Network

1. Once the server reboots, press **F2** to log on.
2. Enter username as root, and the password chosen above.
3. Press **F2** to continue
4. Select Configure Management Network, and press **ENTER**.
5. Select **IP Configuration** option.
6. Press **ENTER** to continue.

7. Use the Up/Down arrow keys to highlight the Set Static IP address and network configuration option, and press **SPACE** key to select it.

8. Enter the static IP address, Subnet Mask and Default Gateway.
9. Press **OK** to submit the changes.

10. Press **ESC** key exit the Management Network Screen.

11. In the Configure Management Network: Confirm dialog box, Press **Y** to restart the Management Network.

12. Verify the IP address settings in the System Customization screen.

**Figure 208** Enter the IP Address configuration details

**Figure 209** Verify the IP address details in the System Customization screen
Installing the VMWare ESXi client software

1. Using a web browser, visit the url: https://10.29.160.251/
2. Click on Download vSphere Client.

**Figure 210**  Accessing the ESXi web interface

![ESXi web interface](image)

**Figure 211**  Download the VMWare vSphere ESXi client software

![VMware vSphere ESXi client software download](image)

3. Proceed to install the downloaded VMWare client software.
Installing VMware vSphere ESXi 5.5

Figure 212 Installing the vSphere Client software

Configuring the vSphere ESXi hypervisor

1. After the installation is complete, launch the VMWare vSphere client.
2. Enter the chosen IP address, the username as root, and the chosen password.
3. Click on Login to continue.
4. In the vSphere Client, click on the Configuration tab on the right, and within the Hardware section, click on Networking.

5. Click on Add Networking link on the upper right hand side.
6. In the Add Networking dialog box, click the **Virtual Machine** radio button and click **Next**.
7. Click the **Create a vSphere standard switch** radio button and make sure that the checkbox next to vmnic1 is checked.

8. Click **Next**.
9. In the Port Group Properties, change the Network Label field to PXE_VLAN85.
10. Leave the VLAN ID(Optional) field as None(0).
11. Click Next.
Figure 217  Creating the Port Group for the PXE VLAN

12. Click **Finish** to complete adding the Network.
13. Click on the **Time Configuration** under the Software section.

14. Click on **Properties** at the upper right hand corner.
15. In the NTP Daemon (ntpd) Options dialog box, click **Options**.
16. Click on the **General** options.
17. Click to select the start and stop with **host** radio button.
18. Click on NTP Settings option.

19. Click on Add button to add the NTP server’s IP address.

20. Press OK to continue.

21. In the next screen, verify the IP-address in the NTP Servers list.

22. Click on the checkbox Restart NTP service to apply changes.

23. Press the button OK twice to complete the time configurations.
24. Time configuration option would now show that the NTP client is running, along with the IP address of the NTP client.
Downloading the UCS Director Express Software Components

The software components of UCS Director Express for Big Data need to be downloaded from three different locations.
**Table 20  Cisco UCS Director Express Big Data 1.1 Software Components**

<table>
<thead>
<tr>
<th>Software component</th>
<th>File Names</th>
<th>Link to Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Director Express 1.0 OVF</td>
<td>CUCSD_Express_1_0_0_0_GA.zip</td>
<td><a href="https://software.cisco.com/download/release.html?mdfid=286281255&amp;flowid=71403&amp;softwareid=285018084&amp;release=1&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest">https://software.cisco.com/download/release.html?mdfid=286281255&amp;flowid=71403&amp;softwareid=285018084&amp;release=1&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest</a></td>
</tr>
<tr>
<td>Cisco UCS Director 5.2.0.1 patch</td>
<td>ccsd_patch_5_2_0_1.zip</td>
<td><a href="https://software.cisco.com/download/release.html?mdfid=286283454&amp;flowid=72903&amp;softwareid=285018084&amp;release=5&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest">https://software.cisco.com/download/release.html?mdfid=286283454&amp;flowid=72903&amp;softwareid=285018084&amp;release=5&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest</a></td>
</tr>
<tr>
<td>Cisco UCS Director Baremetal Agent 5.2 OVF</td>
<td>CUCSD_BMA_5_2_0_0_VMWARE_GA.zip</td>
<td></td>
</tr>
<tr>
<td>Cisco UCS Director Express for Big Data 1.1 Upgrade Package</td>
<td>UCSDExpress_Big_Data_1.1_Upgrade_Package.zip</td>
<td><a href="https://software.cisco.com/download/release.html?mdfid=286284995&amp;flowid=73724&amp;softwareid=285018084&amp;release=1&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest">https://software.cisco.com/download/release.html?mdfid=286284995&amp;flowid=73724&amp;softwareid=285018084&amp;release=1&amp;relind=AVAILABLE&amp;rellifecycle=&amp;reltype=latest</a></td>
</tr>
<tr>
<td>25. Cisco UCS Director Express for Big Data BMA Update Package</td>
<td>UCSDExpress_BMA_Big_Data_1.1_Upgrade_Package.zip</td>
<td></td>
</tr>
</tbody>
</table>

**Download the Software Components**

1. Using the links provided Table 15 above, download the Cisco UCS Director Express for Big Data 1.1 OVF Appliance zip file.
2. Using the links provided Table 15 above; download the Cisco UCS Director 5.2.0.1 Patch zip file, and Cisco UCS Director Baremetal Agent 5.2 VMware vSphere OVF Appliance zip file.
3. Using the links provided Table 21 above; download the Cisco UCS Director 5.2.0.1 Patch zip file, and the Cisco UCS Director Baremetal Agent 5.2 VMWare vSphere OVF Appliance zip file.
Installing Cisco UCS Director Express for Big Data

The Cisco UCS Director Express for Big Data shall be installed on the VMWare vSphere hypervisor using the vSphere Client software.

Deploying the Cisco UCS Director Baremetal Agent OVF

1. Launch the VMWare vSphere client software
2. Enter the chosen IP address, the username as root, and the chosen password.
3. Click on Login to continue.
4. From the File menu, Select Deploy OVF Template.
5. Choose the Cisco UCS Director Baremetal Agent 5.2.0.0 OVF template. Click **Open**.

6. Click **Next** to continue.
7. Review the details of the OVF template, Click Next.
8. Accept the End User License Agreement. Click Next to continue.
9. In the Name and Location option, Enter the name of the VM. Click Next to continue.
10. In the Disk Format option, click the **Thick Provision Lazy Zeroed** radio button. Click **Next** to continue.
11. In the Network Mapping option,
   - Choose **VM Network** as the destination network for source Network 1.
   - Choose **PXE_VLAN85** as the destination network for source Network 2.

12. Click **Next** to continue.
13. Review the details of the VM, click the check box **Power on after deployment** and click **Finish** to proceed with the VM deployment.
Installing Cisco UCS Director Express for Big Data

Figure 232  Deploy the Cisco UCS Director Baremetal Agent VM

![Deploy OVF Template](image1)

**Source**
- DVOF Template Details
- Download size: 1.8 GB
- Size on disk: 40.0 GB
- Name: CLUCSD-BM-5.2.0.0_36
- Host/Cluster: localhost
- Datastore: datastore
- Disk provisioning: Thick Provision Lazy Zeroed
- Network Mapping: “Network 1” to “VM Network”
- Network Mapping: “Network 2” to “PXE_VLAN88"

When you click Finish, the deployment task will be started.

![Cisco UCS Director Baremetal Agent VM Deployment in Progress](image2)

Figure 233  Cisco UCS Director Baremetal Agent VM Deployment in Progress
Configuring the Cisco UCS Director Baremetal Agent VM (BMA-VM)

The Cisco UCS Director Baremetal Agent VM named as CUCSD-BM-5.2.0.0_36 shall be known as BMA-VM here onwards.

1. Right click on the BMA-VM, and select Edit Settings.
2. In the Virtual Machine Properties dialog box, click on the Options Tab.
3. Click on the VMware Tools, Click on the Synchronize guest time with host option in the Advanced section.
4. Click on OK button to accept the changes.

Figure 234   Edit VM Settings to Synchronize the Guest Time with the ESXi Host

5. Right click on the BMA-VM, and select Open Console.
6. In the console accept the End User License Agreement by typing **yes** and press **ENTER**.

7. Login as **root** user using the default password **pxeboot**.

8. Configure the network interfaces by editing the ifcfg-eth0 and ifcfg-eth1 files located at `/etc/sysconfig/network-scripts/` directory, as follows:

<table>
<thead>
<tr>
<th>Network Interface</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>IP Address: 10.29.160.36, Subnet Mask: 255.255.255.0</td>
</tr>
</tbody>
</table>
Figure 237  Editing the BMA-VM NIC eth0

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
TYPE=Ethernet
IPADDR=192.168.85.36
NETMASK=255.255.255.0
```

"/etc/sysconfig/network-scripts/ifcfg-eth0" 7L, 97C written
9. Restart the network service by using the service command.

   `service network restart`

   `Figura 239 Restart the network`
Installing the Cisco UCS Director Express Big Data Upgrade Package

1. Copy over the **UCSDExpress_BMA_5.2_Big_Data_1.1_Upgrade Package.zip** that was downloaded from cisco.com to this VM, by using a secure shell FTP session.

2. Unzip the contents in a temporary staging directory.

3. Change directory into the scripts/bin directory.

4. Change the permissions to add execute permissions to the copyfiles.sh script file and execute it.

   ```
   chmod +x copyfiles.sh
   ```

5. Execute the copyfiles.sh script.

   ```
   ./copyfiles.sh
   ```

   This script copies the number of software modules such as CentOSLive image into the BMA-VM and creates a new repository directory by name **bd-sw-rep** under the /opt/cnsaroot directory. This new directory acts as the repository of all the Big Data specific 3rd party hadoop distribution directories.

Configuring the Big Data software repositories

Copy the Contents of RHEL6.5 ISO into the BMA-VM

1. Copy over the contents of the RHEL6.5 ISO into the directory /opt/cnsaroot/images/RHEL6.5 on the BMA-VM.

2. Copy the contents of the directory /opt/cnsaroot/images/RHEL6.5/isolinux into the directory /opt/cnsaroot/RHEL6.5.

   ```
   [root@localhost ~]# cd /opt/cnsaroot/RHEL6.5
   [root@localhost RHEL6.5]# cp /opt/cnsaroot/images/RHEL6.5/isolinux/* .
   [root@localhost RHEL6.5]# ls
   TRANS.TBL boot.msg initrd.img isolinux.cfg splash.jpg vmlinuz
   boot.cat grub.conf isolinux.bin memtest vossmenu.c32
   ```
Download and Place the Common Utility files in BMA-VM

3. From a host connected to the Internet, download the Parallel-SSH and Cluster-Shell utility tools and copy them over to the /opt/cnsaroot/bd-sw-rep directory.
   - Download Parallel SSH archive from https://pypi.python.org/packages/source/p/pssh/pssh-2.3.1.tar.gz
   - Download Cluster-Shell RPM package from http://dl.fedoraproject.org/pub/epel/6/x86_64/clustershell-1.6-1.el6.noarch.rpm

   ![Copy the Cluster-Shell and Passwordless-SSH Utilities](image)

4. By following the instructions on this page of the BMA-Install guide, download and copy over the Hadoop Distro RPMs into their respective directories under /opt/cnsaroot/bd-sw-rep.

   ![Copy the RPM Packages for the Hadoop Distributions](image)

5. Upload the appropriate License files to the Hadoop distribution directories
   - Place the Cloudera License in a file called ClouderaEnterpriseLicense.lic and place it under the /opt/cnsaroot/bd-sw-rep/cloudera05.x.y.
   - Place the MapR license in a file called license.txt MapR License and place it under the directory /opt/cnsaroot/bd-sw-rep/MapR-X.Y.Z.

   ![Note](image)

   Hortonworks distribution does not require any license file.
Setup a UCSD Patch Directory in the BMA-VM

Cisco UCS Director Express for Big Data VM which will be installed in the next section, requires the patches to be kept in a web server. The BMA-VM comes pre-configured with a web-server used during PXE booting process. This section walks through the steps to create a directory to hold these patches in the BMA-VM.

1. In BMA-VM, create a directory by name patches under /var/www/html.

   mkdir /var/www/html/patches

2. Copy over the Cisco UCS Director Express for Big Data 1.1 specific patch files (See Table 3) to this patch directory.

   Figure 244   Setup a UCSD Patch Directory in the HTTP Root Path

3. Start the HTTPD server in the BMA-VM.

   service httpd start

   Figure 245   Start the HTTPD

4. Verify if these files are accessible by visiting the URL http://<BMA-VM’s >IP address/patches/.

   Figure 246   Verify the Accessibility of the Cisco UCS Director Express Patches

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCSDExpress_Big_Data_1_1_Upgrade_Package.zip</td>
<td>18-Feb-2015 04:52 2.0M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cucesd_patch_5_2_0_1.zip</td>
<td>03-Feb-2015 13:16 1.1G</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apache2 2.2.3 (CentOS) Server at 10.29.160.36 Port 80
BMA-VM configurations are complete.

Deploying the Cisco UCS Director Express OVF

1. Launch the VMWare vSphere client software
2. Enter the chosen IP address, the username as root, and the chosen password.
3. Click Login to continue.
4. From the File menu, Select Deploy OVF Template.
5. Choose the Cisco UCS Director Express for Big Data 1.0 OVF template. Click Open.

Figure 247  Deploy the Cisco UCSD Express 1.0 OVF

6. Review the details of the OVF, and Click Next to continue.
7. Accept the EULA, Click Next to continue.
8. Name the VM, Click Next to continue.
Choose the destination network **VM Network** for the source network **Network 1**. Click **Next** to continue.
10. In the Disk Format option, click the **Thick Provision Lazy Zeroed** radio button. Click **Next** to continue.

11. Review the details of the VM, Check the checkbox **Power On after deployment**.

12. Click **Finish** to proceed with deployment.
Configuring the Cisco UCS Director Express VM (UCSD-VM)

The Cisco UCS Director Express VM named as CUCSDE-1_1_35 shall be known as UCSD-VM here onwards.

1. Right click on the UCSD-VM, and select Edit Settings.
2. In the Virtual Machine Properties dialog box, click on the Options tab.
3. Click on the VMware Tools, Click on the Synchronize guest time with host option in the Advanced section.
4. Click on OK button to accept the changes.
5. Right-click on the UCSD-VM and select **Open Console**.

6. Accept the End User License Agreement by typing **yes** and press the **ENTER**.

7. In the prompt to configure the static IP for the network interface, enter the IP address, Netmask and Gateway information.

8. Enter **y** to continue with the network configuration.
9. Configure the UCSD Express as the personality by entering the number 2.

10. At the prompt Switching personality to UCSD Express, Are you sure to continue [y/n]? Type y and hit ENTER.

   Figure 253 Choose the UCSD Express Personality

11. The UCSD-VM goes through a personality change configuration as shown below.

   Figure 254 UCSD-VM First-Boot Initializations

Note This step takes about 10-15 minutes to complete.

Applying the Upgrade Patches

1. Open a SSH/Putty session to the UCSD-VM.

2. Login as the user shelladmin with password changeme.
3. In the Shell Admin Menu, enter 3 to stop the services.

4. At the prompt, **Do you want to stop services [y/n]?** Type y to confirm and hit **ENTER** to continue.

5. In the Shell Admin menu, type 2 to view the status of the services. They all should be **NOT-RUNNING** as shown below.
6. In the Shell Admin menu, type 19 and ENTER to start the patching process.
7. Type n to the prompt Do you want to take database backup before applying patch[y/n]?
8. At the prompt, Patch URL: enter http://<BMA_IP>/patches/cucsd_patch_5.2.0.1.zip
9. Hit ENTER to continue.
This 5.2.0.1 patch that is being applied to the UCSD-VM’s, upgrades all the core application software to the latest Cisco UCS Director’s code base. After this step completes, the Big Data Upgrade package for release 1.1 needs to be applied.

10. In the Shell Admin menu, type 19 and ENTER to start the patching process.
11. Type n to the prompt Do you want to take database backup before applying patch[y/n]?
12. At the prompt, Patch URL:, enter http://<BMA_IP>/patches/
   UCSDExpress_Big_Data_1.1_Upgrade_Package.zip
13. Hit ENTER to continue.
14. After the successful application of the patch, type 4 and ENTER to start the services.

Note It takes about a few minutes for all the services to get started.

15. Type 2 to check on the services status. All the services should now be in RUNNING state.
Installing Cisco UCS Director Express for Big Data

Figure 261   Verify the Status of the Services in the UCSD-VM

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>broker</td>
<td>RUNNING</td>
<td>7756</td>
</tr>
<tr>
<td>controller</td>
<td>RUNNING</td>
<td>7888</td>
</tr>
<tr>
<td>eventmgr</td>
<td>RUNNING</td>
<td>7966</td>
</tr>
<tr>
<td>client</td>
<td>RUNNING</td>
<td>8025</td>
</tr>
<tr>
<td>idaccessmgr</td>
<td>RUNNING</td>
<td>8113</td>
</tr>
<tr>
<td>inframgr</td>
<td>RUNNING</td>
<td>8172</td>
</tr>
<tr>
<td>TOMCAT</td>
<td>RUNNING</td>
<td>8240</td>
</tr>
<tr>
<td>websocket</td>
<td>RUNNING</td>
<td>8320</td>
</tr>
</tbody>
</table>

3467 ? 00:00:00 mysql_safe
3888 ? 00:05:52 mysql

Note Even after all the services are in a RUNNING state, it would take an additional 3 to 5 minutes for the UCSD-VM client services to become available.

Configuring the Cisco UCS Director Express for Big Data (UCSD Express)

The Cisco UCS Director Express for Big Data, henceforth known as UCSD-Express, needs to be configured with the IP address to the UCS domain (i.e. UCS Manager’s) physical account. This allows the UCSD-Express to query the UCS Manager and perform inventory collection.

The UCSD-Express will also need to be configured with the BMA’s physical account and configure it’s services such as DHCP.

Add the licenses to UCSD-Express

1. Using a web browser, visit the URL http://<UCSD-VM’s IP>/.
2. Login as user admin with the default password admin.
3. Navigate to Administration > License screen.

Figure 262  
Logging onto the Cisco UCS Director Express for Big Data
4. Click on License Keys tab.
5. Click on Update License.
6. In the Update License dialog box, click Browse to select the license file.
7. Click Upload.
8. After the license file gets uploaded, Click Submit to apply the license.
9. The license keys are displayed as shown below.
10. Click on Update Big Data License.

11. In the Update Big Data Subscription dialog box, click Browse to select the Big Data specific license file.

12. Click Upload.

13. After the license file gets uploaded, Click Submit.
Figure 266  Applying the Cisco UCS Director Express Big Data Subscription License
Add the UCS Manager physical account to the UCSD-Express

1. In the UCSD-Express web console, navigate to Administration > Physical Accounts.
2. Click + ADD button
   a. Input the UCS Manager Account details as follows.
   b. In the Account Name field, enter a name to this UCS Manager account.
   c. In the Server Address field, enter the IP address of the UCS Manager.
   d. In the User ID field, enter admin.
   e. In the Password field, enter the password to the UCS Manager’s admin user.
   f. In the Transport Type field, choose https.
3. Click Add.
Installing Cisco UCS Director Express for Big Data

Figure 268  Adding the UCS Manager as a Physical Account in the UCSD-VM

Note  After adding a physical account, the UCSD-Express will query the UCS Manager to perform the inventory collection. This process of inventory collection happens at scheduled intervals. Optionally, you may kick start the inventory collection process manually. These optional steps are described in the steps 4 to 8 below.

5. Click on System Tasks tab.
6. Open the folder Cisco UCS Tasks.
7. Click on UCS Inventory Collector Task.
8. Click Run Now button to execute the task.
Add the Bare Metal Agent physical account to the UCSD-Express

1. In the UCSD-Express web console, navigate to Administration > Physical Accounts.
2. Click on Bare Metal Agents tab; Click + Add.
3. Enter the BMA physical account information details as follows:
4. In BMA Name field, enter a name to this BMA physical account.
5. In the BMA Management Address field, enter the BMA-VM’s IP address assigned to NIC eth0.
6. In the Login ID field, enter root.
7. In the Password field, enter the password. Default password is pxeboot.
8. Check the checkbox BMA Uses Different Interfaces for Management and PXE Traffic.
9. In the BMA PXE Interface Address field, enter PXE IP address i.e. BMA-VM’s IP address assigned to NIC eth1.
10. Click Submit.
Figure 270 Adding the Bare Metal Agent Appliance Information

**Configure the Bare Metal Agent’s DHCP services**

1. Navigate to Administration > Physical Accounts > Bare Metal Agents.
2. Select the BMA entry.
3. On the menu items row, click on the downward facing arrow located at the far right.
4. Select Configure DHCP.
5. In the **Configure DHCP** dialog box, enter the following
6. In the **DHCP Subnet** field, enter the subnet that’s associated with the BMA-VM’s **eth1** NIC.
7. In the **DHCP Netmask**, enter the appropriate subnet mask value for this network.
8. In the **DHCP Start IP**, enter a starting IP address in the same subnet.
9. In the **DHCP End IP**, enter a starting IP address in the same subnet.
10. In the **Router IP Address**, enter the IP address of the gateway router in the network if available, if not may be left as blank or input the IP address of the BMA-VM’s **eth1** NIC.
11. Click **Submit**.
Start the BMA services

1. Navigate to Administration >Physical Accounts >Bare Metal Agents.
2. Select the BMA entry.
3. Click Start Services.
4. In the Start Bare Metal Agent Appliance dialog box, click Start to start the services.
5. Click on **Service Status**, to **check the status of the services**.

6. The Bare Metal Agent Service Status **message box should display both the** Network Services status and Database connectivity status as UP.
Note  It may take a little while for the service status and on the BMA entry to get updated. The UCSD-Express and the associated BMA parts are now ready.

7. Double click on the BMA entry to verify the RHEL operating system repository.
Creating the Hadoop Cluster using UCSD-Express

For creating a Hadoop cluster of a desired distribution, the UCS Manager that’s managing the target servers must be pre-configured to meet the following requirements. For performing these configurations, refer to any Cisco UCS Integrated Infrastructure for Big Data Cisco Validated Designs found at http://www.cisco.com/go/bigdata_design

a. The uplink ports fabric Interconnects must be reachable to that the UCSD-Express appliances management network (i.e. eth0).

b. The UCS-Manager must be configured with a host firmware policy containing C-series rack mount server firmware packages.

c. UCS Manager must be configured to discover the Rack Servers in its domain, and the respective ports are configured as server ports.

d. The server pool must be configured with appropriate set of physical servers that are part of the UCS domain.

e. The QOS System Classes Platinum and Best Effort must be configured and enabled.

Note
BMA-VM software periodically scan the /opt/cnsaroot directory to update the available list of operating system software repositories.
Create the IP Address pools

1. Using a web browser, visit the URL `http://<UCSD-VM's IP>/`.
2. Login as user admin with the default password `admin`.
3. Navigate to Solutions > Big Data Containers.
4. Click on the Big Data IP Pools Tab.
5. Click on + Add.

6. In the Create an IP Pool dialog box.
7. Enter the name MGMT. Click Next to continue.
8. In the IPv4 Blocks table, click on +.

9. In the Add Entry to IPv4 Blocks dialog box, enter the following.
   - In the Static IP Pool field, enter the Static IP Address pool range in the format A.B.C.X – A.B.C.Y.
   - In the Subnet Mask field, enter the appropriate subnet mask.
   - In the Default Gateway field, enter the IP address of the Gateway if present.
   - In the Primary DNS field, enter the IP address of the DNS server.

10. Click Submit.
Note: The Default Gateway, Primary and Secondary DNS fields are optional.

11. Click **Submit** again to create the Big Data IP Pool.
Repeat this process for two more interfaces, by creating an IP address pool by name HDFS for Hadoop configurations to be associated with vNIC eth1, and an IP address pool by name DATA to be associated with vNIC eth2 in the service profiles. Please refer to “Configuring VLAN Section” above in Cisco UCS Integrated Infrastructure for Big Data CVDs.

The following figure shows the UCSD-Express that is fully provisioned all the necessary Big Data IP address Pools.
Creating the Hadoop Cluster using UCSD-Express

Figure 280 All the IP Address Pools have been Configured Successfully

Creating a Hadoop Cluster

1. Using a web browser, visit the URL http://<UCSD-VM’s IP>/.
2. Login as user admin with the default password admin.
3. Navigate to Solutions > Big Data Containers.
4. Click on the Hadoop Cluster Deploy Templates Tab.
5. Click on Create Instant Hadoop Cluster.
6. In the Instant Hadoop Cluster Creation dialog box, enter the following.
7. In Big Data Account Name field, enter a preferred name.
8. In the UCS Manager Policy Name Prefix field, enter a prefix that is less than equal to 5 letters long.
9. In the Hadoop Cluster Name field, enter a preferred name of the cluster – this will be the name assigned to the Hadoop cluster within the context of selected Hadoop Manager.
10. In the Hadoop Node Count field, enter the desired number of nodes.

The minimum number of nodes allowed for Cloudera and Hortonworks Hadoop cluster is 4 and for MapR cluster it is 3.
Creating the Hadoop Cluster using UCSD-Express

Note: There should be sufficient number of servers available in the server pool.

11. In the password fields, enter the preferred passwords and confirm them.
12. Choose the OS Version from the drop-down box. For C220 M4/C240 M4 rack servers, only OS supported is RHEL 6.5.

Note: At the time of this writing, RHEL6.5 is the only OS that is supported on C220 M4/C240 M4 rack servers.

13. In the Hadoop Distribution field, select Hadoop from the drop-down list.

Figure 281 Selecting the Desired Hadoop Distribution

14. In the Hadoop Distribution Version field, select Cloudera-5.3.0 from the drop down list.
15. In the UCS Manager Account, select the appropriate UCS-Manager account.

16. Select the organization.

17. vNIC Template Entry

18. Double-click on row eth0 and select appropriate Mgmt IP-pool, MAC Address Pool and enter the MGMT VLAN id. Click Submit.

---

**Figure 282**  Selecting the Hadoop Distribution Version

<table>
<thead>
<tr>
<th>Cloudera</th>
<th>Hadoop Distribution</th>
<th>Hadoop Distribution Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloudera-5.2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloudera-5.2.1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hortonworks</th>
<th>Hadoop Distribution</th>
<th>Hadoop Distribution Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hortonworks-2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hortonworks-2.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MapR</th>
<th>Hadoop Distribution</th>
<th>Hadoop Distribution Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MapR-4.0.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MapR-3.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MapR-4.0.2</td>
<td></td>
</tr>
</tbody>
</table>

---

**Figure 283**  Editing the vNIC Template to Provide the MGMT Network Configurations

- **vNIC Name**: eth0
- **IP Pool**: MGMT(10.25.160.101 - 10.25.160.200)
- **MAC Address Pool**: mac_pool1 (1976)
- **VLAN ID**: 1
19. Double-click on eth1 and select appropriate IP-pool, MAC Address Pool and enter the DATA1 VLAN ID. Click Submit.

Figure 284 Editing the vNIC Template to Provide the DATA1 Network Configurations

![Editing the vNIC Template to Provide the DATA1 Network Configurations](image)

20. Double-click on eth2 and select appropriate IP-pool, MAC Address Pool and enter the DATA VLAN ID. Click Submit.

Figure 285 Editing the vNIC Template to Provide the DATA2 Network Configurations

![Editing the vNIC Template to Provide the DATA2 Network Configurations](image)

**Note** The following figure show the expanded version of the Instant Hadoop Cluster Creation dialog box with all the fields filed in.
Creating the Hadoop Cluster using UCSD-Express

**Figure 286 Creating an Instant Hortonworks Hadoop Cluster**

<table>
<thead>
<tr>
<th>Instant Hadoop Cluster Creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big Data Account Name: BD101</td>
</tr>
<tr>
<td>UCSM Policy Name Prefix: BD101</td>
</tr>
<tr>
<td>Hadoop Cluster Name: BD101</td>
</tr>
<tr>
<td>Hadoop Node Count: 4</td>
</tr>
<tr>
<td>SSH (root) Password: *********</td>
</tr>
<tr>
<td>Confirm SSH Password: *********</td>
</tr>
<tr>
<td>Hadoop Manager Password: *********</td>
</tr>
<tr>
<td>Confirm Hadoop Manager Password: *********</td>
</tr>
<tr>
<td>Host Node Prefix: node</td>
</tr>
<tr>
<td>OS Version: RHEL6.5 for M4 Servers</td>
</tr>
<tr>
<td>Hadoop Distribution: Hortonworks</td>
</tr>
<tr>
<td>Hadoop Distribution Version: MapR cloudera</td>
</tr>
<tr>
<td>UCS Manager Account: UCSM40</td>
</tr>
<tr>
<td>Organization: root</td>
</tr>
</tbody>
</table>

| Server UUID pool: uuid_pool1 (2020.2) |
| PXE VLAN ID: 99 |

<table>
<thead>
<tr>
<th>Server Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
</tr>
<tr>
<td>UCSM40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host Firmware Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
</tr>
<tr>
<td>UCSM40</td>
</tr>
<tr>
<td>UCSM40</td>
</tr>
<tr>
<td>UCSM40</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vNIC Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNIC Name</td>
</tr>
<tr>
<td>eth0</td>
</tr>
<tr>
<td>eth1</td>
</tr>
<tr>
<td>eth2</td>
</tr>
</tbody>
</table>

| Total 4 items |
| Total 3 items |
21. Click Submit.

Monitoring the Hadoop Cluster Creation

1. In the UCSD-Express web console, navigate to Organization ? Service Requests.

2. Browse through the workflows. There are 3 types of workflows executed.
   - There would be one Master Workflows i.e. UCS CPA Multi-UCS Manager Hadoop cluster WF, per the Hadoop cluster creation request. Master workflow kick starts one or more UCS Manager-specific workflows. Besides that, this master workflow is responsible for Hadoop cluster provisioning.
   - UCS Manager specific workflows i.e. Single UCS Manager Server Configuration WF, would in turn kick start one or more UCS CPA Node Baremetal workflows.
   - UCS CPA Baremetal workflows provision the UCS service profiles and perform OS installation and custom configuration per node.

   ![Figure 287 List of Workflows Recently Complete](image)

3. Double-click on one of the master workflows i.e. UCS CPA Multi-UCS Manager Hadoop Cluster to view the various steps undertaken to provision a Hadoop cluster.
Figure 288  Viewing a Completed Master Workflow

![Workflow Status](image)

Note: If necessary click on the Log tab to view the logs generated during the provisioning of the Hadoop Cluster.

4. Double-click on one of the child workflows: i.e. UCS CPA Node Baremetal.
Monitoring the Hadoop Cluster Creation

Figure 289  A Completed UCS CPA Node Baremetal workflow.
Host and Cluster Performance Monitoring

1. In the UCSD-Express web console, navigate to **Solutions > Big Data Accounts** for viewing the Hadoop cluster accounts.

   Figure 290  Big Data Accounts Summary Screen

2. Double-click on one of the accounts to view the cluster-wide performance charts.
Cluster Management

1. In the UCSD-Express web console, navigate to Solutions > Big Data Accounts for viewing the Hadoop cluster accounts.
2. Double-Click on one of the accounts to drill into the cluster.
3. Click on the Hosts tab.
In this screen, the user can perform various management operations such as,

- Add one/more Baremetal nodes to the cluster.
- Delete a node back to Baremetal
- Decommission/Recommission

4. Click on the **Services** tab, where one could Start/Stop the Hadoop services.
Host level Monitoring

In the Hosts tab, double-click on one of the hosts to view the host’s statistics.
Figure 294  Summary Statistics Screen of a Specific Host in a Hadoop Cluster

The user may monitor various resource utilization metrics of the particular host by clicking on the other tabs in this screen.

Reference

For details on managing the Hadoop clusters deployed on the Cisco UCS Integrated Infrastructure for Big Data, see the *Cisco UCS Director Express for Big Data Management Guide* at:


Bill of Materials

Table 23 provides the BOM for Cisco UCSD Big Data subscription licenses for up to 64 servers and Table 24 provides the BOM for the various Hadoop platforms.

Table 22  Bill of Material for UCSD for Big Data Subscription Licenses for up to 64 Servers

<table>
<thead>
<tr>
<th>CUIC-SVR-OFFERS=</th>
<th>Cisco UCS Director Server Offerings</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CON-SAU-SVROFFERS</td>
<td>Cisco UCS Director Server Offerings Software Application Sup</td>
<td>1</td>
</tr>
<tr>
<td>CUIC-BASE-K9</td>
<td>Cisco UCS Director Software License</td>
<td>1</td>
</tr>
<tr>
<td>CON-SAU-CUICBASE</td>
<td>SW APP SUPP + UPGR Cisco UCS Director Base Software</td>
<td>1</td>
</tr>
<tr>
<td>CUIC-TERM</td>
<td>Acceptance of Cisco UCS Director License Terms</td>
<td>1</td>
</tr>
</tbody>
</table>
### Table 22  Bill of Material for UCSD for Big Data Subscription Licenses for up to 64 Servers

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUIC-EBDS-LIC</td>
<td>UCSD Express for Big Data - Standard Edition (SE)</td>
<td>1</td>
</tr>
<tr>
<td>CUIC-EBDS-LIC</td>
<td>UCSD Express for Big Data - Standard Edition (SE)</td>
<td>64</td>
</tr>
<tr>
<td>CUIC-EBDS-S1-3YR</td>
<td>UCSD Express for Big Data - SE 3 year</td>
<td>64</td>
</tr>
<tr>
<td>CUIC-TERM</td>
<td>Acceptence of Cisco UCS Director License Terms</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table 23  Bill of Material for Various Hadoop Platforms

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS-BD-CEBN</td>
<td>CLOUDERA ENTERPRISE BASIC EDITION</td>
</tr>
<tr>
<td>UCS-BD-CEFN</td>
<td>CLOUDERA ENTERPRISE FLEX EDITION</td>
</tr>
<tr>
<td>UCS-BD-CEDN</td>
<td>CLOUDERA ENTERPRISE DATA HUB EDITION</td>
</tr>
<tr>
<td>UCS-BD-HDP-ENT</td>
<td>HORTONWORKS ENTERPRISE EDITION</td>
</tr>
<tr>
<td>UCS-BD-HDP-EPL</td>
<td>HORTONWORKS ENTERPRISE PLUS EDITION</td>
</tr>
<tr>
<td>UCS-BD-M5-SL</td>
<td>MapR M5 EDITION</td>
</tr>
<tr>
<td>UCS-BD-M7-SL</td>
<td>MapR M7 EDITION</td>
</tr>
</tbody>
</table>