

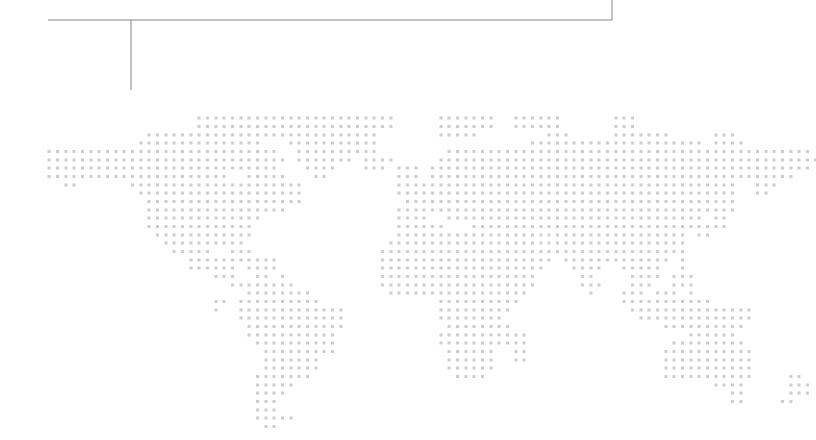
Cisco UCS Integrated Infrastructure for Big Data with MapR With Optional Multi-Tenancy Extension

Last Updated: May 27, 2015



Building Architectures to Solve Business Problems

· I | I · I | I · CISCO ..



About the Authors

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.

Ashwin Manjunatha, Technical Marketing Engineer, Data Center Solutions Group (Cisco Systems)

Ashwin Manjunatha works in the Data Center Solutions Group at Cisco Systems. Ashwin holds Master of Science Degree in Computer Engineering from Wright State University. He specializes in Hadoop and Distributed Computing.

James Sun, Senior Solutions Architect (MapR Technologies)

James Sun manages the technological relationship with worldwide alliances at MapR Technologies. James has over 15 years of experience in information technology. Prior to MapR, he held several senior technical positions at technological companies such as NetApp, Yahoo and EMC. He holds a PhD. from Stanford University.



Karthik Kulkarni



Ashwin Manjunatha



James Sun

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 (COLLEC-TIVELY, "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 SUP-PLIERS 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 contributions of Manankumar Trivedi, Karthik Karupasamy and Sindhu Sudhir in developing this document.

1



Cisco UCS Integrated Infrastructure for Big Data with MapR

Audience

This document describes the architecture and deployment procedures for MapR on a 64 Cisco UCS C240 M4 node cluster based on Cisco UCS Integrated Infrastructure for Big Data. 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 MapR on Cisco UCS Integrated Infrastructure for Big Data.

Introduction

Big data technology and Apache Hadoop in particular, are finding use in an enormous number of applications and are being evaluated and adopted by enterprises of all kinds. As this important technology helps transform large volumes of data into actionable information, many organizations are struggling to deploy effective and reliable Hadoop infrastructure that performs and scales and is appropriate for mission–critical applications in the enterprise. Deployed as part of comprehensive data center architecture, the Cisco UCS with MapR delivers a powerful and flexible infrastructure that increases business and IT agility, reduces total cost of ownership (TCO), and delivers exceptional return on investment (ROI) at scale, while fundamentally transforming the way that organizations do business with Hadoop technology.

Cisco UCS Integrated Infrastructure for Big Data with MapR and Multi–Tenancy

The Cisco UCS solution for MapR 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:



Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco UCS 6200 Series Fabric Interconnects

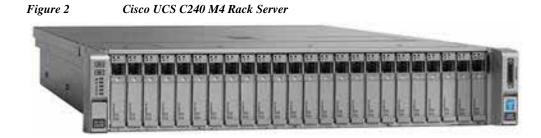
Cisco UCS 6200 Series Fabric Interconnects provide high-bandwidth, low-latency connectivity for servers, with integrated, unified management provided for all connected devices by Cisco UCS Manager. Deployed in redundant pairs, Cisco fabric interconnects offer the full active-active redundancy, performance, 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



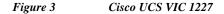
Cisco UCS C-Series Rack Mount Servers

Cisco UCS 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, Cisco UCS Virtual Interface Cards 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 GigabitEthernet 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.

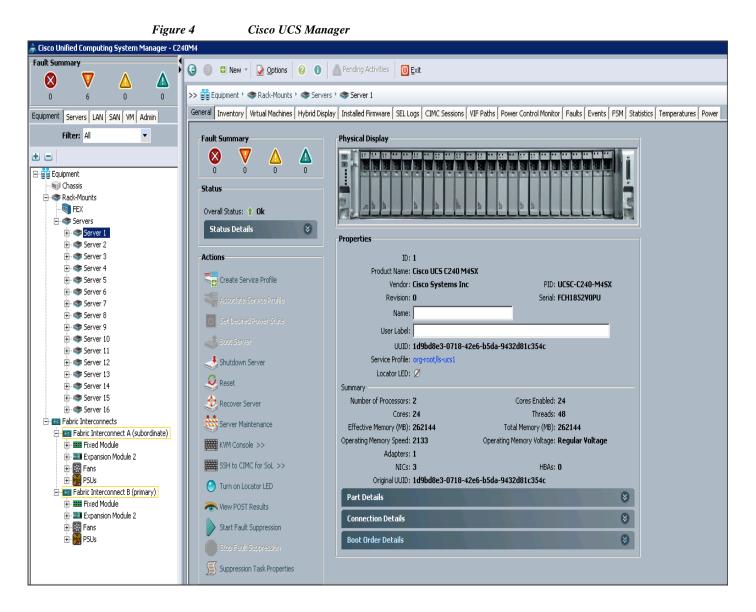




Cisco UCS Manager

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.



Cisco UCS Director Express for Big Data

Cisco UCS Director Express for Big Data provides a single-touch solution that automates deployment of Hadoop Distributions on leading Cisco UCS Integrated Infrastructure for Big Data.

It also provides a single management pane across both physical 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 Hortonworks, Cloudera, and MapR, 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.

The appendix section describes on how to go about configuring Cisco UCS Director Express for Big Data and deploying popular Hadoop distributions such as Cloudera, MapR and Hortonworks on the Cisco UCS Integrated Infrastructure for Big Data cluster.

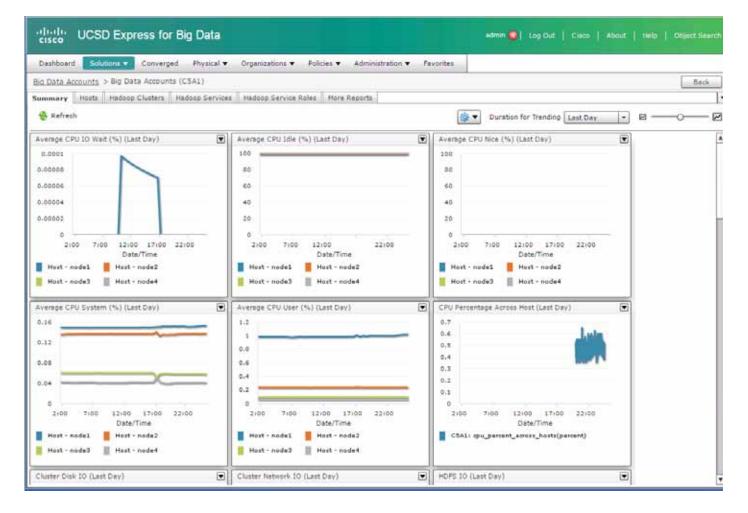


Figure 5 Cisco USCD Express for Big Data

MapR Distribution Including Apache Hadoop: A Complete Hadoop Platform

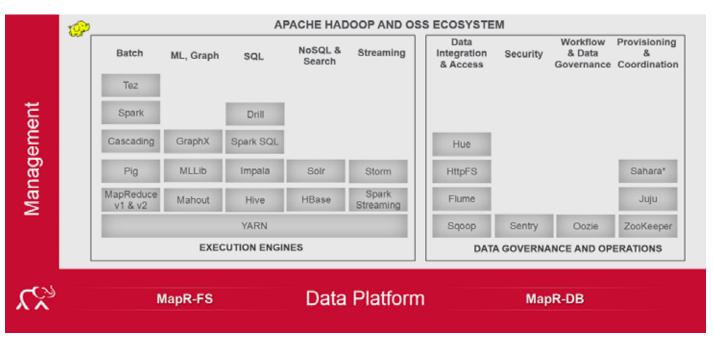
As one of the technology leaders in Hadoop, the MapR Distribution Including Apache Hadoop provides enterprise–class Hadoop solutions that are fast to develop and easy to administer. With significant investment in critical technologies, MapR offers industry's one of the most comprehensive Hadoop

platforms, fully optimized for performance scalability. MapR's distribution delivers more than a dozen tested and validated Hadoop software modules over a fortified data platform, offering exceptional ease of use, reliability, and performance for Hadoop solutions.

Key highlights of MapR Distribution Including Apache Hadoop are:

- Performance Ultra–fast performance and throughput
- Scalability Up to a trillion files, with no restrictions on the number of nodes in a cluster
- Standards-based API's and tools Standard Hadoop API's, ODBC, JDBC, LDAP, Linux PAM, and more
- MapR Direct Access NFS Random read/write, real-time data flows, existing non-Java applications work seamlessly
- Manageability Advanced management console, rolling upgrades, REST API support
- Integrated security Kerberos and non–Kerberos options with wire–level encryption
- Advanced multi-tenancy Volumes, data placement control, job placement control, queues, and more
- Consistent snapshots Full data protection with point-in-time recovery
- High availability Ubiquitous HA with no NameNode architecture, YARN HA, NFS HA
- Disaster recovery Cross-site replication with mirroring
- MapR-DB Integrated Enterprise–Grade NoSQL database

Figure 6 MapR Data Platform



Benefits of Multi-Tenancy in MapR

The MapR Distribution Including Apache Hadoop offers multi-tenancy out-of-the box. It provides powerful features to logically partition a physical cluster to provide separate administrative control, data placement, job execution, and user quotas. Volumes, which is a unique feature in MapR is one of the features that contribute to multi-tenancy. Volumes provide a way to organize data and apply different policies to different data sets, applications and users/groups. A single cluster can have more than thousands of volumes.

In a typical deployment, the data for each user, group, application or business unit is grouped into a single volume so that it can be managed separately from the data of other users, groups, applications, and business units.

Other Hadoop distributions do not support volumes, so policies can only be defined at the file or directory level (too granular) or at the cluster level (too coarse). As a workaround, organizations using other Hadoop distributions create separate physical clusters for each tenant, which results in increased architectural complexities, and higher error/ failure rate.

Multi-tenancy in MapR also has significant total cost of ownership (TCO) advantages, allowing organizations to leverage a single cluster for multiple use cases rather than maintaining a large number of isolated clusters. This reduces overall administrative overhead, and also enables the higher utilization efficiency of a common resource pool.

In a typical deployment, the data for each user, group, application, or business unit is grouped into a single volume so that it can be managed separately from the data of the other users, groups, applications, and business units.

Data Placement Control

With MapR, a volume can be restricted to a subset of a cluster's nodes. This provides the ability to isolate sensitive data/applications, as well as the ability to leverage heterogeneous hardware.

For example, data placement control can be used to keep data such as the personally identifiable information (PII) on separate nodes, or Apache Spark data on nodes that have SSDs. Further, it can be used for more advanced storage tiering policies, such as keeping old data on nodes having a higher storage capacity (such as Cisco UCS C3160) and less compute power, thus providing lower cost per TB storage. In combination with the MapR warden pluggable services, data placement control also enables administrators to designate specific nodes for an application or service, such as for Spark, effectively creating a "mini–cluster" within the larger cluster to guarantee SLAs, and resource availability.

Job Placement Control

MapR provides the ability to restrict a specific job, or jobs from a specific user or group, to a subset of the nodes in the cluster. This enables administrators to guarantee SLAs for specific applications, and to create separation between different applications or business units. This also allows administrators to designate a small subset of the nodes for low–priority jobs or jobs that require access to external systems through the corporate firewall.

Access Control and Security

MapR provides fine–grained access control based on Access Control Expressions (ACEs) for tables, column families, and columns; POSIX access control lists for files; and strong role–based access control (RBAC) for tables, column families, and columns.

MapR provides cryptographically secure wire-level authentication and encryption. Organizations that have a Kerberos infrastructure can leverage it for authentication, while organizations that do not have a Kerberos infrastructure can leverage an integrated, key-based scheme that provides the same security without the complexity associated with deploying and managing Kerberos.

Administration and Reporting

From an administrative perspective, MapR allows organizations to define and enforce storage, CPU, and memory quotas at the volume, user, and group levels. For service providers to provide accurate usage and billing information, MapR offers reporting on resource usage for over 60 different metrics. These metrics are available via the MapR Control System (MCS) browser–based user interface, and—for up–stream integration—via the command–line interface and the REST API.

Solution Overview

This CVD describes architecture and deployment procedures for MapR Distribution on a 64 Cisco UCS C240 M4SX node cluster based on Cisco UCS Integrated Infrastructure for Big Data. The solution describes in detail configuring MapR on the infrastructure. Further, this CVD describes steps to setup Multi–Tenancy on the same MapR installation.

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

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

Table 1 Cisco UCS Integrated Infrastructure for Big Data Configuration Details



This CVD describes the install process of MapR for a 64 node of Performance Optimized cluster configuration.

The Performance cluster configuration consists of the following:

- Two Cisco UCS 6296UP Fabric Interconnects
- 64 UCS C240 M4 Rack-Mount servers (16 per rack)
- Four Cisco R42610 standard racks
- Eight vertical power distribution units (PDUs) (Country Specific)

Rack and PDU Configuration

Each rack consists of two vertical PDUs. The master rack consists of two Cisco UCS 6296UP Fabric Interconnects, sixteen Cisco UCS C240 M4 Servers connected to each of the vertical PDUs for redundancy; thereby, ensuring availability during power source failure. The expansion racks consists of sixteen Cisco UCS C240 M4 Servers connected to each of the vertical PDUs for redundancy; thereby, ensuring availability during power source failure, similar to the master rack.

Note

Please contact your Cisco representative for country specific information.

Table 2 and Table 3 describe the rack configurations of rack 1 (master rack) and racks 2-4 (expansion racks).

Cisco 42URack	Master Rack		
42	Cisco UCS FI 6296UP		
41			
40	Cisco UCS FI 6296UP		
39			
38	Unused		
37	Unused		
36	Unused		
35			
34	Unused		
33			
32	Cisco UCS C240 M4		
31			
30	Cisco UCS C240 M4		
29			
28	Cisco UCS C240 M4		
27			
26	Cisco UCS C240 M4		
25			

Table 2Rack 1 (Master Rack)

Cisco 42URack	Master Rack
24	Cisco UCS C240 M4
23	
22	Cisco UCS C240 M4
21	
20	Cisco UCS C240 M4
19	
18	Cisco UCS C240 M4
17	
16	Cisco UCS C240 M4
15	
14	Cisco UCS C240 M4
13	
12	Cisco UCS C240 M4
11	
10	Cisco UCS C240 M4
9	
8	Cisco UCS C240 M4
7	
6	Cisco UCS C240 M4
5	
4	Cisco UCS C240 M4
3	
2	Cisco UCS C240 M4
1	

Table 2	Rack 1	(Master	Rack)

L

Γ

Table 3Rack 2-4 (Expansion Racks)

Cisco 42URack	Expansion Rack		
42	Unused		
41	Unused		
40	Unused		
39	Unused		
38	Unused		
37	Unused		
36	Unused		
35	Unused		

Cisco 42URack	Expansion Rack
34	Unused
33	Unused
32	Cisco UCS C240 M4
31	
30	Cisco UCS C240 M4
29	
28	Cisco UCS C240 M4
27	
26	Cisco UCS C240 M4
25	
24	Cisco UCS C240 M4
23	
22	Cisco UCS C240 M4
21	
20	Cisco UCS C240 M4
19	
18	Cisco UCS C240 M4
17	
16	Cisco UCS C240 M4
15	
14	Cisco UCS C240 M4
13	
12	Cisco UCS C240 M4
11	
10	Cisco UCS C240 M4
9	
8	Cisco UCS C240 M4
7	
6	Cisco UCS C240 M4
5	
4	Cisco UCS C240 M4
3	
2	Cisco UCS C240 M4
1	

1

Table 3Rack 2-4 (Expansion Racks)

Port Configuration on Fabric Interconnects

	Table 4	Port Types and Port Numbers
Port Type		Port Number
Network		1
Server		2 to 65

Server Configuration and Cabling for C240M4

The C240 M4 rack server is equipped with Intel Xeon E5–2680 v3 processors, 256 GB of memory, Cisco UCS Virtual Interface Card 1227, Cisco 12–Gbps SAS Modular Raid Controller with 2–GB FBWC,24 1.2–TB 10K SFF SAS drives, 2 120–GB SATA SSD for Boot.

Figure 8, illustrates the port connectivity between the Fabric Interconnect and Cisco UCS C240 M4 server. Sixteen Cisco UCS C240 M4 servers are used in Master rack configurations.

Figure 7 Fabric Topology for C240 M4

Cisco UCS 6296UP Fabric Interconnect A

Cisco U(CS 6296UP Fabric Intercor	nnect B
Ciso	co UCS C240 M4 Server	

For more information on physical connectivity and single-wire management, see:

 $http://www.cisco.com/en/US/docs/unified_computing/ucs/c-series_integration/ucsm2.1/b_UCSM2-1_C-Integration_chapter_010.html$

For more information on physical connectivity illustrations and cluster setup, see:

http://www.cisco.com/en/US/docs/unified_computing/ucs/c-series_integration/ucsm2.1/b_UCSM2-1_ C-Integration_chapter_010.html#reference_FE5B914256CB4C47B30287D2F9CE3597

Figure 8 depicts a 64–node cluster. Every rack has 16 Cisco UCS C240 M4 servers. Each link in the figure represents 16 x 10 Gigabit Ethernet link from each of the 16 servers connecting to a Fabric Interconnect as a Direct Connect. Every server is connected to both Fabric Interconnect represented with dual link.

Figure 8 64 Nodes Cluster Configuration



Software Distributions and Versions

The software distributions required versions are listed below.

MapR

MapR Hadoop is API–compatible and includes or works with the family of Hadoop ecosystem components such as Spark, Hive, Pig, Flume, and others. For more information, see: https://www.mapr.com/

Red Hat Enterprise Linux (RHEL)

The operating system supported is Red Hat Enterprise Linux 6.5. For more information visit http://www.redhat.com

Software Versions

The software versions tested and validated in this document are shown in table 5.

Layer	Component	Version or Release	
Compute	Cisco UCS C240-M4	C240M4.2.0.3d	
Network	Cisco UCS 6296UP	UCS 2.2(3d)A	
	Cisco UCS VIC1227 Firmware	4.0(1d)	
	Cisco UCS VIC1227 Driver	2.1.1.66	
Storage	LSI SAS 3108	24.5.0-0020	
Software	Red Hat Enterprise Linux Server	6.5 (x86_64)	
	Cisco UCS Manager	2.2(3d)	
	MapR	Enterprise Edition (M5) and Enterprise Database Edition (M7)	

Table 5Software Versions



- The latest drivers can be downloaded from the link below: https://software.cisco.com/download/release.html?mdfid=283862063&flowid=25886&softwareid=283 853158&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.
- Cisco UCS C240 M4 Rack Servers are supported from UCS firmware 2.2(3d) onwards.

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.
- 9. Enter A for the switch fabric.
- **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:

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/2.0/b_UCSM_GUI_Configuration_Guide_2_0_chapter_0100.html

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.
- 2. Select Pools > IP Pools > IP Pool ext-mgmt.
- 3. Right-click IP Pool ext-mgmt
- 4. Select Create Block of IPv4 Addresses.

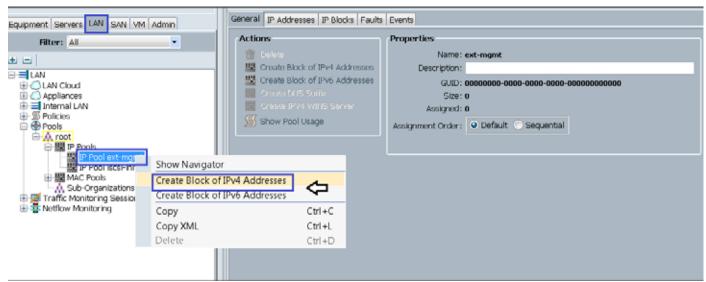


Figure 9 Adding Block of IPv4 Addresses for KVM Access Part 1

5. Enter the starting IP address of the block and number of IPs needed, as well as the subnet and gateway information.

🛕 Create Blo	ck of IPv4 Addresses				×
Create a	Create a Block of IPv4 Addresses				
From:	0.0.0.0	Size:			1 🜩
Subnet Mask:	255.255.255.0	Default Gateway:	0.0.0.0		
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0		
				СК	Cancel

Figure 10 Adding Block of IPv4 Addresses for KVM Access Part 2

- 6. Click **OK** to create the IP block.
- 7. Click **OK** in the message box.

Figure 11 Adding Block of IPv4 Addresses for KVM Access Part 3

🔺 Create Blo	ck of IPv4 Addresses				X	
Create a	Create a Block of IPv4 Addresses					
From:	10.29.160.30	Size:	b		64 🗘	
Subnet Mask:	255.255.255.0	Default Gateway:	10.29.160.1			
Primary DNS:	0.0.0.0	Secondary DNS:	0.0.0.0			
				OK	Cancel	

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.

- 3. Expand the Unconfigured Ethernet Ports section.
- 4. Select **port 1**, that is connected to the uplink switch, right-click, then select **Reconfigure > Configure as Uplink Port**.
- 5. Select Show Interface and select 10GB for Uplink Connection.
- 6. A pop-up window appears to confirm your selection. Click Yes, then click OK to continue.

- 7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- 8. Expand the Unconfigured Ethernet Ports section.
- 9. Select **port 1**, that is connected to the uplink switch, right-click, then select **Reconfigure > Configure as Uplink Port**.
- 10. Select Show Interface and select 10GB for Uplink Connection.
- 11. A pop-up window appears to confirm your selection. Click Yes, then click OK to continue.

Figure 12 Enabling Uplink Ports

Fabric Interconnects Fabric Interconnect A (primary)	Admin Sta	ate: Disabled	User	ID: 1 Slot ID: 1 r Label:
	Actions - Enable - Reconf - Reconf - Sho		Port Tra Port	MAC: S4:7F:EE:1C:03:A8 Mode: Access t Type: Physical Role: Unconfigured ansceiver 0GB CUIM 2053783-1 SCO-TYCO D1818A11K
Port 12		Configure as Appliance Po	ort	

Configuring VLANs

VLANs are configured as in shown in table 6.

VLAN	Fabric	NIC Port	Function	Failover
default(VLAN1)	А	eth0	Management, User connectivity	Fabric Failover to B
vlan11_DATA1	В	eth1	MapR	Fabric Failover to A
vlan12_DATA2	А	eth2	MapR	Fabric Failover to B

All of the VLANs created need to be trunked to the upstream distribution switch connecting the fabric interconnects. For this deployment default VLAN1 is configured for management access (Installing and configuring OS, clustershell commands, setup NTP, user connectivity, etc) and vlan11_DATA1 and vlan12_DATA2 is configured for Hadoop Data traffic.

With MapR supporting multiple NICs, where Hadoop uses multiple IP subnets for its data traffic, vlan12_DATA2 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 vlan12_DATA2 providing full 10GigE connectivity to this application on a different fabric without affecting Hadoop Data traffic on vlan11_DATA1



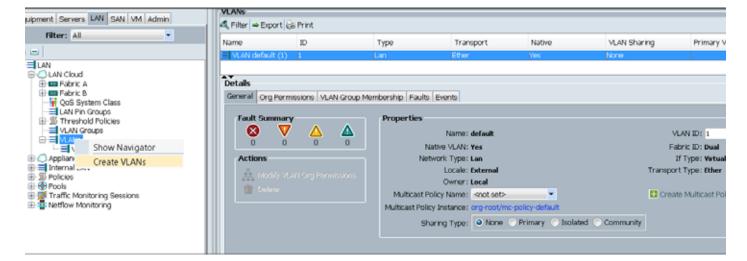
All applications talking to Hadoop should be able to reach Hadoop VLAN. That is, all applications should be able to access all the Hadoop nodes.

• We are using default VLAN1 for management traffic.

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.

Figure 13 Creating VLAN



- 5. Enter vlan11_DATA1 for the VLAN Name.
- 6. Click the Common/Global radio button for the vlan11_DATA1.

- 7. Enter 11 on VLAN IDs of the Create VLAN IDs.
- 8. Click OK and then, click Finish.
- 9. Click OK in the success message box.

Create VLANs	X
Create VLANs	0
VLAN Name/Prefix: vlan11_DATA1	
Common/Global C Fabric A C Fabric B Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.	
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 11	
Sharing Type: O None O Primary O Isolated O Community	
▲ []	۰.
Check Overlap OK	Cancel

Figure 14 Creating VLAN for Data

- 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 vlan12_DATA2 for the VLAN Name.
- **15.** Click the **Common/Global** radio button for the vlan12_DATA2.
- 16. Enter 12 on VLAN IDs of the Create VLAN IDs.
- 17. Click OK and then, click Finish.

ſ

Figure 15	Creating VLAN for Hadoop Data	
▲ Create VLANs		X
Create VLANs		•
	▼ 🗈 Create Multicast Policy /Global 🔵 Fabric A 🔵 Fabric B 🔵 Both Fabrics Configured Differently	
You are creating global VLANs that map to the Enter the range of VLAN IDs. (e.g. "2009-201 VLAN IDs: 12 Sharing Type: None Primary Isola	19", "29,35,40-45", "23", "23,34-45")	
•	III	Þ
	Check Overlap OK Cano	:el

1

18. The below screenshot shows the created VLANs.

Figure 16

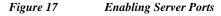
List of VLANs created for Hadoop Data

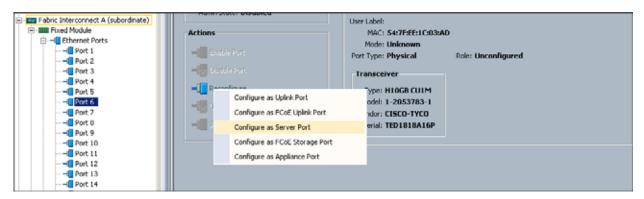
ment Servers LAN SAN VM Admin	VLANs						
ment Servers Dave San VM admin	💐 Filter 👄 Export 🎯 Print						
Filter: All	Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Nan
a	VLAN default (1)	1	Lan	Ether	Yes	None	
LAN	VLAN vian11_DATA1 (11)	11	Lan	Ether	No	None	
LAN Cloud	VLAN vian12_DATA2 (12)	12	Lan	Ether	No	None	
Fabric B Fabric B	Details General Org Permissions Fault Summary		ship Faults Events		FII		

Enabling Server Ports

These steps provide details for enabling server ports.

- 19. Select the Equipment tab on the top left of the window.
- 20. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
- 21. Expand the Unconfigured Ethernet Ports section.
- 22. Select all the ports that are connected to the Servers right-click them, and select **Reconfigure** > **Configure as a Server Port**.
- 23. A pop-up window appears to confirm your selection. Click Yes then OK to continue.
- 24. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- 25. Expand the Unconfigured Ethernet Ports section.
- 26. Select all the ports that are connected to the Servers right-click them, and select **Reconfigure** > **Configure as a Server Port**.
- 27. A pop-up window appears to confirm your selection. Click Yes then OK to continue.





Creating Pools for Service Profile Templates

Creating an Organization

I

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.

Figure 18 Creating MAC Pool Window

A Create MAC Pool		X
Unified Co	omputing System Ma	anagei
Create MAC Pool	Define Name and Description	Ø
 1. √<u>Define Name and</u> <u>Description</u> 2. △<u>Add MAC Addresses</u> 	Name: ucs Description:	_
	Assignment Order: O Default O Sequential	Cancel



12. Click Finish.

ſ

Figure 20 Adding MA	C Addresses			
🗼 Create MAC Pool				×
Unified Co	omputing Syst	tem M	anag	er
Create MAC Pool	Add MAC Addresses			Ø
 1. ✓ <u>Define Name and</u> <u>Description</u> 2. ✓ <u>Add MAC Addresses</u> 	Name	From 000:25:85:00:00	To 00:25:85:00:00	. <u> </u>
	🗄 Add 🥤	Delete		
	< Prev	Next	Finish Cance	el

13. When the message box displays, click OK.



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

1

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.

	Figure 22	Setting Name and Description of Server Pool			
📥 Create Server Pool					×
Unified	Comput	ing System Manager			
Create Server Pool	Set Name a	nd Description			0
1. √ <u>Set Name and</u> Description					
2. Add Servers					
	u lucel				
	Name: UCS				
	Description:				
			< Prev Next >	Finish	Cancel

- 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.

ſ

10. Click OK, and then click Finish.

Create Server Pool				-	-						-	U	X
Unified	Cor	nputi	ing Syste	em	Ма	nage	er						
ate Server Pool	Add	I Servers	E.										
 <u>Set Name and</u> Description 													
2. Add Servers	S	ervers					Pooled Server	s					
		Nel (Maldina		1.1	6	Ŧ		192				2	Ē
	C.,	. Sl R		2017	in na me	<u> </u>		PIL) A	A	A	C	. 🛡
			UCSC-C240-M4SX			^ · · · ·							*
			UCSC-C240-M45X		/000								
			UCSC-C240-M4SX										
			UCSC-C240-M4SX		12.11								
			UCSC-C240-M4SX UCSC-C240-M4SX										
			UCSC-C240-M45X										
			UCSC-C240-M45X		14.44								
			UCSC-C240-M45X		10.00	-	<u>a</u>						
		10	UCSC-C248-M45X			>>							
		11	UCSC-C240-M4SX		1000								
		12	UCSC-C240-M4SX			<<							
		13	UCSC-C240-M4SX										
		14	UCSC-C240-M4SX										
		15	UCSC-C240-M4SX		144								
		16	UCSC-C240-M4SX			+							Ŧ
	D	etails for rack-	unit-1				Details	_	_			_	
		Model:	UCSC-C240-M4SX				Mode	e					
	54	erial Number :	FCH1852V0PU				Serial Number	<u></u>	_	_			-
		Vendor:	Cisco Systems Inc				Vendor						=
								•		_			

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 24 Creating Host Firmware Package

Create Host Firmware Package	X
Create Host Firmware Package	0
Name: ucs Description:	
How would you like to configure the Host Firmware Package? Simple O Advanced	
Blade Package: <not set=""> Rack Package: 2.2(3d)C</not>	
Rack Package: 2.2(3d)C	
	Cancel

Creating QoS Policies

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

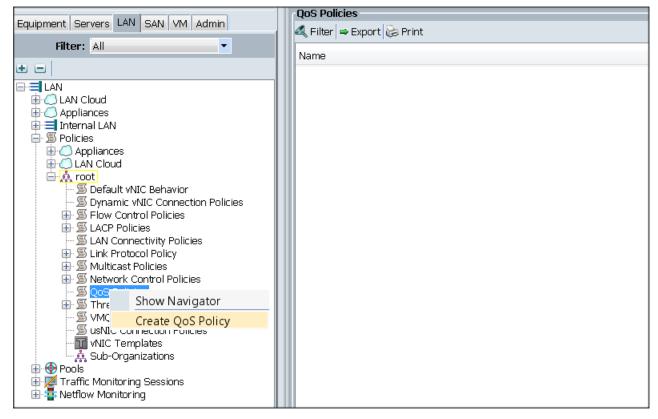
Best Effort Policy

I

- 1. Select the LAN tab in the left pane in the UCS Manager GUI.
- 2. Select Policies > root.

- 3. Right-click QoS Policies.
- 4. Select Create QoS Policy.

Figure 25 Creating QoS Policy



- 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.

Figure 26	Creating BestEffor	t QoS Policy		
📥 Create Qo5	Policy			×
Create C	QoS Policy			0
		Create	QoS Policy	×
Name: BestEf			Successfully created QOS Policy BestEffort.	
	/: Best Effort	•	Show Navigator for QOS Policy BestEffort	
Burst(Bytes): 10240): line-rate		OK	
Host Contro				_
			OK C	Cancel

Platinum Policy

I

- 1. Select the LAN tab in the left pane in the UCS Manager GUI.
- 2. Select **Policies** > **root**.
- 3. Right-click QoS Policies.
- 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.

Figure 27 Creating Platinum QoS Policy

me: Platinum	1	-	Create Qo5 Policy
gress		_	Successfully created QOS Policy Platinum.
Priority:	Platinum		Show Navigator for QOS Policy Platinum
Burst(Bytes):	10240		OK
Rate(Kbps):	line-rate		
Host Control:	💿 None 🔿 Full		

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. In the Platinum row, enter 9000 for MTU.
- 5. Check the Enabled Check box next to Platinum.
- 6. In the Best Effort row, select best-effort for weight.
- 7. In the Fiber Channel row, select none for weight.
- 8. Click Save Changes.
- 9. Click OK.

Figure 28

Setting Jumbo Frames

Equipment Servers LAN SAN VM Admin	General Events	FSM						
Filter: All	Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	мти	Multicast Optimized
± =	Platinum	v	5		10	90	9000	• 🔳
	Gold		4	V	9	N/A	normal	- 🗆
🖨 🦳 LAN Cloud 🕀 🚥 Fabric A	Silver		2	V	0	N/A	normal	•
Fabric B OoS System Class	Bronze		1	V	7	N/A	normal	
LAN Pin Groups	Best Effort		Any		best-effort	9	normal	
VLAN Groups	Fibre Channel		3		none	1	£ .	N/A
Appliances Traffic Monitoring Sessions Sessions								

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.

I

Figure 29	Configuring Local Disk Policy
🔺 Create	Local Disk Configuration Policy
Create	Local Disk Configuration Policy
	Name: ucs
	Description:
	Mode: Any Configuration
	Protect Configuration: 🔽
is disasso with the s associated	erver. In that case, a configuration error will be raised when a new service profile is d with er if the local disk configuration in that profile is different.
	FlexFlash State: 💿 Disable 🔵 Enable
	sh State is disabled, SD cards will become unavailable immediately. sure SD cards are not in use before disabling the FlexFlash State.
FlexFlash	RAID Reporting State: O Disable C Enable
	OK Cancel

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.

I

Γ

- 5. Enter your preferred BIOS policy name (ucs).
- 6. Change the BIOS settings as per the following figures:

Figure 30 Creating Server BIOS Policy

A Create BIOS Policy	X
Unified C	omputing System Manager
Create BIOS Policy	Main Ø
\frac{√Main}{2} \begin{aligned} Processor. 3. □ Intel Directed IO 4. □ <u>RAS Memory 5. □ Serial Port 6. □ USB 7. □ PCI 8. □ OPI 9. □ LOM and PCIe Slots 10. □ <u>Boot Options 11. □ Server Management } } </u></u>	Name: ucs Description: Reboot on BIOS Settings Change: Quiet Boot: disabled enabled Platform Default Post Error Pause: disabled enabled Platform Default Resume Ac On Power Loss: stay-off last-state reset Platform Default Front Panel Lockout: disabled enabled Platform Default
	< Prev Next > Finish Cancel

1	Figure 31 Creating Server BIOS Policy for Processor
🖨 Create BIOS Policy	
Unified	Computing System Manager
	Processor
Create BIOS Policy	FIOCESSO
1. √ <u>Main</u> 2. √ <u>Processor</u>	
3. Intel Directed IO	Turbo Boost: C disabled C Platform Default
4. BRAS Memory 5. Serial Port	Enhanced Intel Speedstep: C disabled C enabled C Platform Default
6. 🛄 <u>USB</u>	Hyper Threading: O disabled O enabled O Platform Default
7. D _{PCI} 8. D _{OPI}	Core Multi Processing: all
9. D _{LOM and PCIe Slots}	Execute Disabled Bit: C disabled C enabled C Platform Default
10. Boot Options 11. Server Management	Virtualization Technology (VT): 📀 disabled 🔿 enabled 🔿 Platform Default
	Hardware Pre-fetcher: C disabled C enabled C Platform Default
	Adjacent Cache Line Pre-fetcher: C disabled C enabled C Platform Default
	DCU Streamer Pre-fetch: C disabled C enabled C Platform Default
	DCU IP Pre-fetcher: C disabled C enabled C Platform Default
	Direct Cache Access: C disabled C enabled C Platform Default
	Processor C State: disabled C enabled C Platform Default
	Processor C1E: 💽 disabled 🔿 enabled 🔿 Platform Default
	Processor C3 Report: 🕞 disabled 🔿 acpi-c2 🔿 acpi-c3 🔿 Platform Default
	Processor C6 Report: 💿 disabled 🔿 enabled 🔿 Platform Default
	Processor C7 Report: C disabled C enabled C Platform Default
	CPU Performance: C enterprise C high-throughput C hpc C Platform Default
	Max Variable MTRR Setting: C auto-max C 8 C Platform Default
	Local X2 APIC: C x2apic C auto C Platform Default Power Technology: performance
	Energy Performance
	Frequency Floor Override: C disabled C Platform Default
	P-STATE Coordination:
	DRAM Clock Throttling: performance
	Channel Interleaving: Platform Default
	Rank Interleaving: Platform Default 🔹
	Demand Scrub: 💽 disabled 🔿 enabled 🔿 Platform Default
	Patrol Scrub: C disabled C Platform Default
	< Prev Next > Finish Cancel

FI	igure 32 Creating Server BIOS Policy for Intel Directed IO	
Create BIOS Policy	And I wanted and the second se	×
Unified C	Computing System Manager	
Unined C		
Create BIOS Policy	Intel Directed IO	0
1. VMain		
2. √Processor 3. √Intel Directed ID	VT For Directed IO: Citicabled Consubled @ Platform Default	
4. DRAS Memory 5. Diserial Port	Interrupt Remap: 🕜 disabled 🕜 enabled 👄 Platform Default	
6. D <u>USB</u> 7. D <u>PCI</u>	Coherency Support: Codisabled Comabled Platform Default	
0. Dopt		
9. DLOM and PCIe Slots 10. DBoot Options		
11. Server Management	Pass Through DMA Support: Cideabled Cienabled @ Platform Default	
		alsh Canad]
	< Prev Next > Fi	nish Cancel

Figure 22 Creating Service DIOS Policy for Intel Directed IO

- 7. Click **Finish** to complete creating the BIOS policy.
- 8. Click OK.

L

Γ

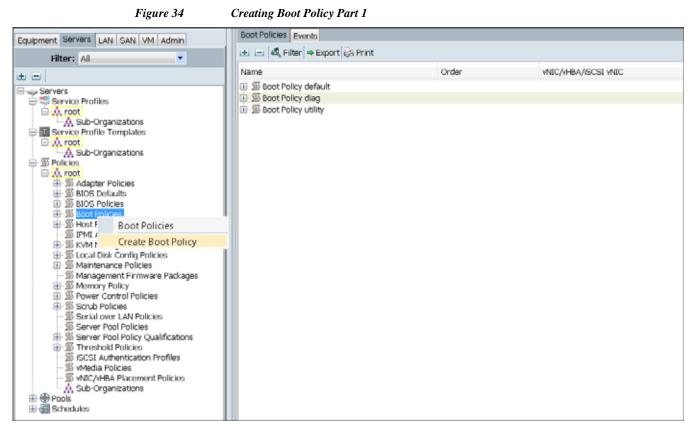
	Figure 33	Creating Server BIOS Policy for Memory	
Create BIOS Policy		a water and the second s	×
Unified	Computi	ng System Manager	Conservation of the local division of the lo
Create BIOS Policy	RAS Memory		0
 Vitain Vintel Directed 10 Vintel Directed 10 VIRAS Memory Direct Port <l< td=""><td>NUMA LV DOR Mode DRAM Refresh Rate</td><td>o power-saving-mode o performance-mode o auto O Platform Default</td><td></td></l<>	NUMA LV DOR Mode DRAM Refresh Rate	o power-saving-mode o performance-mode o auto O Platform Default	
		< Prov Next > Finish	Cancel

1

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.
- 9. Keep Boot Mode Default (Legacy).
- 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.

ſ

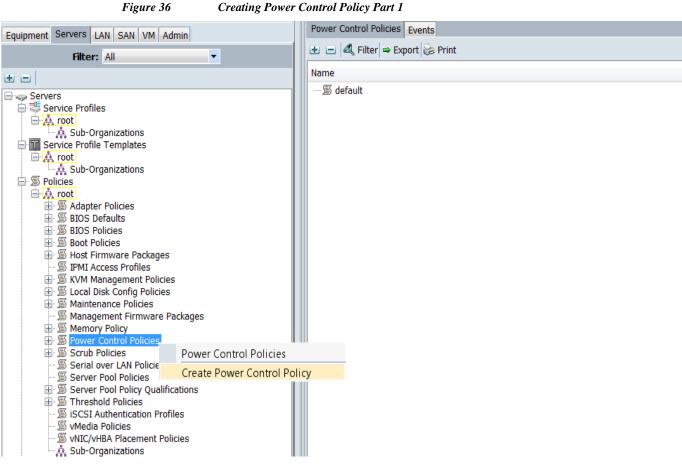
Fų	gure 35	Creating Boot P	olicy Part 2	;				
Create Boot Policy	A							X
Create Boot Policy								0
Name: Description: Reboot on Boot Order Change: Enforce vNIC//HBA/ISCSI Name: Boot Mode: WARNINGS: The type (primary/secondary) do The effective order of boot device If Enforce vNIC//VHBA/ISCSI N If it is not selected, the vNICs/VHB	Legacy Uefi Legacy Uefi es not indicate a boot o es within the same devi ame is selected and the	ce class (LAN/Storage e vNIC/VHBA/ISCSI do	es not exist, a	config error will b	be reported.	scan order is used	L.	
Add CD/DVD	Boot Order	👄 Export 🍪 Print	_	-	_	_	_	
Add Remote CD/DVD	Name CD/DVD SLocal Disk LAN	3	vNIC/vHB/	VISCSI VNIC	Type Primary	Lun ID	WWN	P
Add Remote Virtual Drive CIMC Mounted vMedia VIICs Add LAN Bopt VHBAs	E		≤un	Add LAN B Add LAN WIC: ethol	oot	OK	(P) Cancel	-
							ОК С	ancel

1

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.
- **16.** Select **Policies > root**.
- 17. Right-click the Power Control Policies.
- 18. Select Create Power Control Policy.



Creating Power Control Policy Part 1

- 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.

I

gure 37	Creating Power Control Policy Part 2	
Create P	ower Control Policy	×
Create	Power Control Policy	Ø
Name	ucs	
Description		
Power Ca	apping	
the higher capping.	vithin its power group. Priority values range from est priority. If you choose no-cap , the server is e	
require mo	Manager only enforces power capping when the re power than is currently available. With sufficie city regardless of their priority.	
		OK Cancel

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.

Figure 38

Creating Service Profile Template

Equipment Servers L	AN SAN VM Admin	Service Profile Templates	
Filter: All	-	te te da Filter ⇒ Export i Print	Address
Servers		root	
E- Service Profit	Service Profile Template:	5	
B Policies	Create Service Profile Ter	mplate	
🕀 😯 Pools 🖲 🎆 Schedules			

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.

i	Figure 39 Identify Service Profile Template
A Create Service Profile Te	mplate
Unified	Computing System Manager
Create Service Profile Template Profile Template Profile Template Subscrape Control Control	You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description. Name: uss The template will be created in the following organization. Its name must be unique within this organization. Where: org.root The template will be created in the following organization. Its name must be unique within this organization. Type: Initial Template I Updating Template Specify how the UUID will be assigned to the server associated with the service generated by this template. UUID Assignment: Hardware Default The UUID assigned by the manufacturer will be used. Note: This UUID will not be migrated if the service profile is moved to a new server. Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.
	< Prev Next > Finish Cancel

Configuring Network Settings for the Template

I

- 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.

	Figure 40	Configuring Network Setti	ngs jor the Template		
Create Service Profile T	emplate				
Unified	Computi	ng System M	lanager		
ate Service Profile Templat	Ontinnally specif	fy LAN configuration information			
Template 2. √Networking 3. □ Storage 4. □ Zoning 5. □VNC/MBA Placeme	Defensioner en serve	ection Policy: Select a Policy to use	(no Dynamic VNIC Policy by de	fa • Crosalte Dynamic	vNIC Connectio
G. Dy <u>Media Policy</u> Z. D <u>Server Boot Order</u> Diserver Assignment	How wor Click Add to specify	uld you like to configure LAN con one or more willCs that the server sl		No. of the second s	nectivity Policy
10. Coperational Policies	1 Name	MAC Address	Fabric ID	Native VLAN	4
					-
	-	100 100	elette 🖬 Add 💐 Modify		
	ISCSI WILLS	御 9	elette 🖬 Addi 🏬 Modify		
	ISCSI VNICS	潮 2	elete 🖸 Add 🌉 Modify	_	
	ISCSI VNICS		elette 🚦 Add 🏨 Modify		0
	ISCSI VNICS		elette 🖬 Addi 🌉 Modify		8
	isest while		elete 🖸 Add 🦥 Modify		S
	ISCSI VNICS		elette 🕻 Add 🖏 Modify		0
	ISCSI VNICS		elette 🕻 Add 🏨 Modify		8

- 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.

1

- 7. Check the default check box for VLANs and click the Native VLAN 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.

create vNIC		
Name: eth0	MAC Address	
0	MAC Address Assignment: ucs(512/512)	
ise vNIC Template:		
	Create MAC Pool	
	The MAC address will be automatically assigned from the	
Create vNIC Template	selected pool.	
VLANs	Enable Failover ce over the Appliance Cloud when there is a name clash.	
A Filter Skport 😪 Print		
Select Name	Native VLAN	
default	<u> </u>	
vlan11_DATA1 vlan12_DATA2		
Create VLAN		
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same to corresponding to the Egress priority of t	value in the <u>QOS System Class</u> the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same corresponding to the Egress priority of Pin Group: <not set=""></not>	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same corresponding to the Egress priority of Pin Group: <not set=""></not>	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same torresponding to the Egress priority of 1 Pin Group: <not set=""></not>	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same v corresponding to the Egress priority of 1 Pin Group: single-complements Decreational Parameters Adapter Performance Profile Adapter Policy: Linux	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same v corresponding to the Egress priority of 1 Pin Group: <not set=""> Deperational Parameters Adapter Performance Profile Adapter Policy: Linux QoS Policy: BestEffort</not>	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same to corresponding to the Egress priority of I Pin Group: mtu: ison Operational Parameters Adapter Performance Profile Adapter Policy: Linux QoS Policy: BestEffort Network Control Policy: default Connection Policies	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same 4 corresponding to the Egress priority of 1 Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withes/withe-base-filt Pin Group: https://www.com/estimates/withes	the selected QoS Policy. ate LAN Pin Group	
Create VLAN MTU: 1500 Warning Make sure that the MTU has the same 4 corresponding to the Egress priority of 1 Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withe-base-filt Pin Group: https://www.com/estimates/withes/withe-base-filt Pin Group: https://www.com/estimates/withes	the selected QoS Policy. ate LAN Pin Group	

... c. . MG 40

- **15.** Click **Add** to add a vNIC to the template.
- 16. The Create vNIC window appears. Name the vNIC eth1.
- 17. Select ucs in the Mac Address Assignment pool.
- 18. Click the Fabric B radio button and Check the Enable failover check box for the Fabric ID.
- 19. Check the vlan11_DATA1 check box for VLANs, and click the Native VLAN radio button.
- 20. Select MTU size as 9000.

ſ

- 21. Select adapter policy as Linux.
- 22. Select QoS Policy as Platinum.
- 23. Keep the Network Control Policy as Default.

- 24. Keep the Connection Policies as Dynamic vNIC.
- 25. Keep the Dynamic vNIC Connection Policy as <not set>.
- 26. Click OK.

reate vNIC			
Name: eth1	MAC Address		
e vNIC Template:	MAC Address Assignment: uc	s(512/512)	
se ware remplate.			
	Create MAC Pool	- 12 B	
Create vNIC Template	The MAC address will be auto selected pool.	omatically assigned from the	
COLUMN D	3 ✓ Enable Failover redence over the Appliance Cloud when	there is a name clash.	
VLANS			
♣ Filter ⇒ Export & Print			
Select Name	Native VLAN		
default	<u>©</u>		
Vlan11_DATA1			
Vlan11_DATA1 Vlan12_DATA2	Ŏ		
Vian11_DATA1 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the e corresponding to the Egress prior	ame value in the <u>QOS System Class</u>	÷	
	ame value in the <u>QOS System Class</u> ity of the selected QoS Policy.		
	ame value in the <u>CoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group		
Vian11_DATA1 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the s corresponding to the Egress prior Pin Group: <not set=""> Derational Parameters Coperational Parameters Coperati</not>	ame value in the <u>CoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group	apter Policy	
	ame value in the <u>CoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group	apter Policy	
Vian11_DATA1 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the s corresponding to the Egress prior Pin Group: <not set=""> Derational Parameters Coperational Parameters Coperati</not>	ame value in the <u>CoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group	apter Policy	
	ame value in the <u>QoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group Create Ethemet Ad Create Ethemet Ad Create QoS Policy Create Network Cor	apter Policy	
	ame value in the <u>QoS System Class</u> ity of the selected QoS Policy. Create LAN Pin Group Create Ethemet Ad Create Ethemet Ad Create QoS Policy Create Network Cor	apter Policy itrol Policy	

1

- 27. Click Add to add a vNIC to the template.
- 28. The Create vNIC window appears. Name the vNIC eth2.
- 29. Select ucs in the Mac Address Assignment pool.
- 30. Click the Fabric A radio button, and then Check the Enable failover check box for the Fabric ID.
- 31. Check the vlan12_DATA2 check box for VLANs, and then click the Native VLAN radio button.
- 32. Select MTU size as 9000.

- **33.** Select adapter policy as Linux.
- **34.** Select QoS Policy as Platinum.
- **35.** Keep the Network Control Policy as Default.
- 36. Keep the Connection Policies as Dynamic vNIC.
- 37. Keep the Dynamic vNIC Connection Policy as <not set>.
- 38. Click OK.

I

Γ

reate vNIC			
Name: eth2	MAC Address MAC Address Assignment:	ucs(512/512)	•
se vNIC Template:	Create MAC Pool		
Create vNIC Template	The MAC address will be selected pool.	automatically assigned from the	
abric ID: 🛛 Fabric A 🚫 Fabric	B ✓ Enable Failover		
	cedence over the Appliance Cloud w	hen there is a name clash.	
VLANS			
A Filter ⇒ Export ⊗ Print			
Select Name	Native VLAN		
default		A	
		10.00	
vian12_DATA2	0		
Vlan12_DATA2			
Vian12_DATA2 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the corresponding to the Egress prior	same value in the <u>QoS System Clas</u>		
	same value in the <u>QoS System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group	0	
Vian12_DATA2 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the corresponding to the Egress prio Pin Group: <not set=""></not>	Same value in the <u>QoS System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group Create Ethernet Create Ethernet	Adapter Policy	
	Same value in the <u>QoS System Class</u> rity of the selected QoS Policy. Create LAN Pin Group Create LAN Pin Group Create Ethernet Create Ethernet Create QoS Polis	Adapter Policy Y	
Vian12_DATA2 Vian12_DATA2 Create VLAN MTU: 9000 Warning Make sure that the MTU has the corresponding to the Egress prio Pin Group: <not set=""></not>	Same value in the <u>QoS System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group Create Ethernet Create Ethernet	Adapter Policy Y	
	Same value in the <u>QoS System Class</u> rity of the selected QoS Policy. Create LAN Pin Group Create LAN Pin Group Create Ethernet Create Ethernet Create QoS Polis	Adapter Policy Y	
	Same value in the Qo <u>S System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group Create LAN Pin Group Create Ethernet Create Ethernet Create Retwork Create Network	Adapter Policy Y	
	Same value in the Qo <u>S System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group Create LAN Pin Group Create Ethernet Create Ethernet Create Retwork Create Network	Adapter Policy Y	
	Same value in the Qo <u>S System Clas</u> rity of the selected QoS Policy. Create LAN Pin Group Create LAN Pin Group Create Ethernet Create Ethernet Create Retwork Create Network	Adapter Policy Y. Control Policy	

1

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.

Configuring Storage Settings

Figure 44

I

Γ

A Create Service Profile Temp	plate 🗾	٢
Unified C	Computing System Manager	
Create Service Profile Template 1. √Identify Service Profile	Storage Optionally specify disk policies and SAN configuration information.	0
Template 2. √Networking 3. √Storage	Select a local disk configuration policy.	ŕ
4. Zoning 5. VAICAHBA Placement 6. VAICAHBA Placement 6. VAICAHBA Placement 7. Server Boot Order 8. Maintenance Policy 9. Server Assignment 10. Operational Policies	Local Storage: Local Disk Configuration Policy Mode: Any Configuration Create Local Disk Configuration Policy Protect Configuration is set, the local disk configuration is preserved if the service profile is disassociated with the server. In that case, a configuration in that profile is different. HereFlash FlexFlash State: Disable FlexFlash State: Disable If HexFlash State: State: Disable If HexFlash State: Disable How would you like to configure SAN connectivity? Simple © Expert © No VHBAS © Use Connectivity Policy This server associated with this service profile will not be connected to a storage area network. Use Connectivity Policy	=
	۲. III (۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲. ۲	÷
	< Prev Next > Finish Cance	

4. Click Next once the zoning window appears to go to the next section.

F	Figure 45 Configure Zoning	
A Create Service Profile Tem	nplate	×
Unified C	Computing System Manager	
Create Service Profile Template 1. √Identify Service Profile Template		0
2. √Networking 3. √Storage 4. √2oning 5. √vtlC/M-BA Placement 6. □ <u>vMedia Policy</u> 7. □ <u>Server Boot Order</u> 8. □ <u>Maintenance Policy</u> 9. □ <u>Server Assignment</u> 10. □ <u>Operational Policies</u>	2. Select vHBA Initiator (o) (more a e dealed of statage page) 2. Select vHBA Initiator (o) to selected Initiator Group(s) 3. Add selected Initia Select vHBA Initia Select vHBA Initia	
	Name R Name Storage Connection Policy Name	[
	Delete 🖬 Add 🌇 Modify	
		•
	< Prev Next > Finish	h Cancel

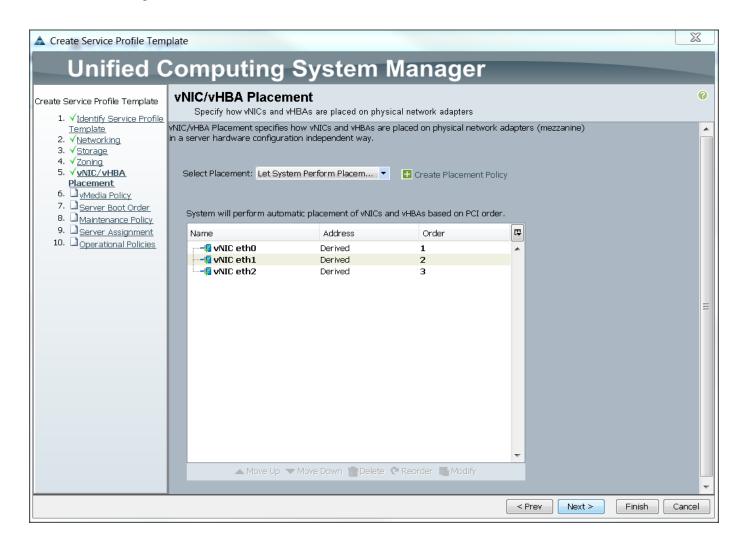
1

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.

Figure 46 vNIC/vHBA Placement



Configuring vMedia Policy for the Template

1. Click Next once the vMedia Policy window appears to go to the next section.

Fi	gure 47 UCSM vMedia Policy Window	
A Create Service Profile Tem	plate	X
Unified C	Computing System Manager	
Create Service Profile Template 1. √ <u>Identify Service Profile</u> Template	vMedia Policy Optionally specify the Scriptable vMedia policy for this service profile template.	0
2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. √ <u>vhICAHBA Placement</u>	vMedia Policy: Select vMedia Policy to use 🔹 🖬 Create vMedia Policy	
S. ▼ <u>INIC/WEAK Placement</u> G. ✓ <u>vMedia Policy</u> 7. □ <u>Server Boot Order</u> 8. □ <u>Maintenance Policy</u>	The default boot policy will be used for this service profile.	
9. Server Assignment 10. Operational Policies		
		< Prev Next > Finish Cancel

1

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.

Figure 48

Creating Boot Policy

te Service Profile Template	Server Boot Ord Optionally specify the		service profile template.			
Terrolate 2. < batworking 3. < Storage 4. < Zoning 5. < yMcCAHBA Placement 6. < yMedia Policy 7. < Server Boot Order 0. Maintenance Policy 9. Diserver Assignment 10. Digerational Policies	Select a boot policy. Boot Policy: Luce Des Reboot on Boot Order Enforce VAIC/VHBA/ISCS	COMPANY AND ADDRESS	Crassite Boot Policy			
	The effective order of b If Enforce VNIC/VHBA If it is not selected, the Boot Order	oot devices within th /ISCSI Name is sels MICs/MBAs/ISCSI a	ate a boot order presence. e same device class (LAV/Storage inted and the vNIC/VHBA//sCSI doe re solucted if they exist, otherwise	as not exist, a config	error will be report	ted.
	The type (primary/second) The effective order of b If Enforce VNIC/VHBA If it is not selected, the	oot devices within th /ISCSI Name is sels MICs/MBAs/ISCSI a	e same device class (LAN/Storage acted and the vNIC/VHBA//SCSI doe	es not exist, a config the vNRC/VHBA/ISC	error will be report	ted.
	The type (primary/second) The effective order of b If Enforce VNIC/VHBA If it is not selected, the Boot Order (b) (c) (d) Filter (c) Eq	oot devices within th /ISCSI Name is sele /NICo/VHBAo/ISCSI a cort GB Print	e same device class (LAN/Storage cted and the vNIC/HBA/GCSI do re selected if they exist, otherwise	as not exist, a config	error will be repor 51 with the lowest P	ted. Clo bus scan

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.

I

Unineu	Computing Sys	terri wanayer	and the second second
Treate Service Profile Templat	Optionally specify a server pool for th	iis service profile template.	9
Template 2. ∀ <u>Notworking</u> 3. √ <u>Storage</u>	You can select a server pool you want to a	issociate with this service profile template.	
 ✓ Zoning ✓ √MICAHBA Placement 	Pool Assignment: UCS	Create Server Pool	
 ✓<u>vMedia Policy</u> ✓<u>Server Boot Order</u> ✓Maintenance Policy 		Select the power state to be applied when this profile is associated with the server.	
9. ✓ Server Assignmen	nt.	O Up Down	
10. Operational Policies	The service profile template will be ass	ociated with one of the servers in the selected pool. I server pool policy qualification that the selected server must	
	The service profile template will be ass If desired, you can specify an additiona meet. To do so, select the qualification	ociated with one of the servers in the selected pool. I server pool policy qualification that the selected server must	
	The service profile template will be ass If desired, you can specify an additional meet. To do so, select the qualification Server Pool Qualification: www.select.com Server Pool Qualification: www.select.com	actated with one of the servers in the selected pool. I server pool policy qualification that the selected server must from the list.	
	The service profile template will be ass If desired, you can specify an additional meet. To do so, select the qualification Server Pool Qualification:		

1

Configuring Operational Policies for the Template

In the Operational Policies Window, follow these steps:

- 6. Select ucs in the BIOS Policy field.
- 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.

Fi	gure 50 Selecting BIOS and Power Control Policy		
A Create Service Profile Temp	plate		X
Unified C	Computing System Manager		
Create Service Profile Template 1. √ <u>Identify Service Profile</u> <u>Template</u> 2. √ <u>Natworking</u> 3. √ <u>Storage</u>	Operational Policies Optionally specify information that affects how the system operates. BIOS Configuration	8	0
4. √Zoning 5. √ <u>vNIC/vHBA Placement</u> 6. √ <u>vMedia Policy</u> 7. √ <u>Server Boot Order</u>	If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile BIOS Policy: UCS		
 ✓ Maintenance Policy ✓ Server Assignment 	External IPMI Management Configuration	۲	
10. √ <u>Operational Policies</u>	Management IP Address	8	
	Monitoring Configuration (Thresholds)	8	
	Power Control Policy Configuration	8	
	Power control policy determines power allocation for a server in a given power group. Power Control Policy:		
	Scrub Policy	8	
	KVM Management Policy	8	
			Cancel
	< Prev Next > Finis	h	Cancel

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

1. Go to Service Profile **Templates** > **root**.

I

Γ

- 2. Right-click Service Profile Templates ucs.
- 3. Select Create Service Profiles From Template.

Fault Summary		🕽 🏐 🖽 New - 🔀 Options 😢 📵 📥 Perio		
0 28 2	-	>> 🥪 Servers 🕴 🎹 Service Profile Templates 🖲		
Equipment Servers LAN SAN VM	Admin	General Storage Network ISCSI vNICs vMed	fia Policy Boot Order Policies Events FSM	
Filter: All	•	Actions	Properties	
± =		Create Service Profiles From Template	Name: ucs	
Servers		Create a Clone	Description:	
🚍 🍣 Service Profiles		Cisassociate Template	UUID: Hardware Default	
☐ M root A Sub-Organizations			Power State: 1 Up	
😑 📊 Service Profile Templates		Associate with Server Pool	Type: Updating Template	
 		🚿 Change Maintenance Policy	Associated Server Pool	۲
-A Sub-Organizations	Show Navigator		Maintenance Policy	8
S Policies General Pools	Create Service Pr	rofiles From Template	Management IP Address	8
🕀 🚱 Schedules	Create a Clone			
	Disassociate Ten	nplate		
	Associate with Se	erver Pool		
	Change UUID			
	Change World W	vide Node Name		
	Change Local Di	sk Configuration Policy		
	Change Dynamic	vNIC Connection Policy		
	Change Serial ov	ver LAN Policy		
	Modify vNIC/vH	BA Placement		
	Сору	Ctrl+C		
	Copy XML	Ctrl +L		
	Delete	Ctrl+D		

Figure 51 Creating Service Profiles from Template

4. The Create Service Profile from Template window appears.

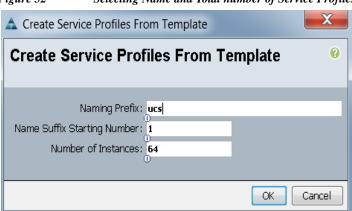


Figure 52 Selecting Name and Total number of Service Profiles

Association of the Service Profiles will take place automatically. The Final Cisco UCS Manager window is shown in Figure 46.

Servers LAN SAN VH Admin															
liber: Al 💌 🔍 Fite	👄 Export 😹 Prin	t													
	ne Overall Status	PID	Model	Serial	User Label	Cores	Memory	Adapters	NICS	HBAs	Operability	Power State	Assoc State	Profile	Fa
de Ser	ner 1 🕇 Ok	UCSC-C240	Cisco UCS C	POH1852Y0PU		24	262144	1	3	0	1 Operable	t On	1 Associated	org-root/ls	79'4
nt. 🗇 Ser	ver2 1 Ok	UCSC-C240	Cisco UCS C	FCH1850V36U		24	262144	1	3	0	1 Operable	1 On	1 Associated	org-root/ls	N/A
de Ser	ver 3 🕇 Ok	UCSC-C240	Gieco UCS C	FO-0844V0QK		24	262144	1	9	0	1 Operable	1 On	1 Associated	orp-root/ls	N/A
unts 🐵 Ser	ner4 🕇 Ok	UCSC-C240	Cisco UCS C	POH1652Y0PY		24	262144	1	3	0	t Operable	1 On	Associated	org-root/ls	N/A
et ser	ner5 1t Ok	UC5C-C240	Cisco UCS C	POH1851V1ZZ		24	262144	1	3	0	1 Operable	1 On	1 Associated	org-root/ls	N/A
rconnects 🐲 Ser	ver6 🕈 Ok	UCSC-C240	Cieco UCS C	FOH1852V0L4		24	262144	1	3	0	t Operable	1 On	* Associated	orp-root/ls	N/A
eter wets	ner7 🕇 Ok	UCSC-C240	Cieco UCS C	POH1852V0Q3		24	262144	1	3	0	t Operable	1 On	1 Associated	org-root/le	N/A
de Ser	ner8 🕇 Ok	UCSC-C240	Cisco UCS C	POH1852V0QC		24	262144	1	3	0	t Operable	1 On	1 Associated	orp-root/ls	N/A
other Ser	ver9 🕇 Ok	UC5C-C240	Cisco UCS C	POH1851V233		24	262144	1	3	0	t Operable	t On	1 Associated	orp-root/ls	N/A
I Ser	ver 10 👔 Ok.	UC5C-C240	Cisco UCS C	FOH1852VONF		24	262144	1	3	0	t Operable	1 On	t Associated	org-root/la	N/A
de Ser	ver 11 🕇 Ok	UCSC-C240	Cisco UCS C	POH1852Y0PP		24	262144	1	з	0	1 Operable	1 On	1 Associated	org-root/ls	N/A
de Ser	ver 12 🛊 Ok	UCSC-C240	Gisto UCS C	POH1851V213		24	262144	1	3	0	1 Operable	1 On	Associated	org-root/ls	N/A
of Ser	ner 13 🚦 Ok.	UCSC-C240	Gisco UCS C	FOH1852V0QF		24	262144	1	3	0	† Operable	t On	Associated	org-root/ls	N/A
de Ser	rer 14 🚦 Ok	UC5C-C240	Cisco UCS C	FOH1851V243		24	262144	1	3	0	1 Operable	t On	1 Associated	org-root/ls	N/A
de Ser	ver 15 🚦 Ok	UC\$C-C240	Osco UCS C	PCH1851V216		24	262144	1	3	0	1 Operable	1 On	1 Associated	org-root/ls	N/A
de Sar	av 16 🔮 Ok	LICSC-C240	Ciero LICS C	FOH1852VONA		24	262144	1	3	0	Coevable	1 On	# Associated	pen-root/k	BU/A

Figure 53	UCS Manager showing all Nodes
	e es manager showing an moues

Installing Red Hat Enterprise Linux 6.5 using software RAID on C240 M4 Systems

The following section provides detailed procedures for installing Red Hat Enterprise 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.

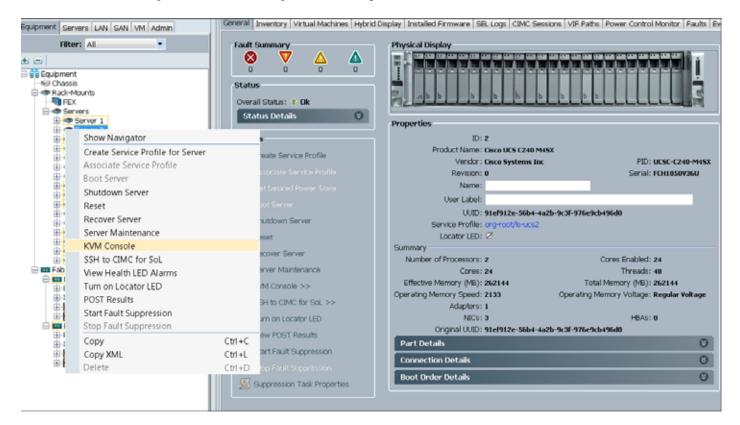
Note

This requires RHEL 6.5 DVD/ISO for the installation.

- 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 then Servers.
- 4. Right click on the server and select KVM Console.

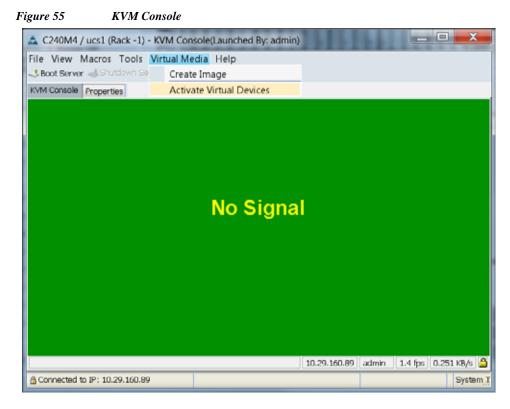
Cisco UCS Integrated Infrastructure for Big Data with MapR

Figure 54 Selecting KVM Console Option



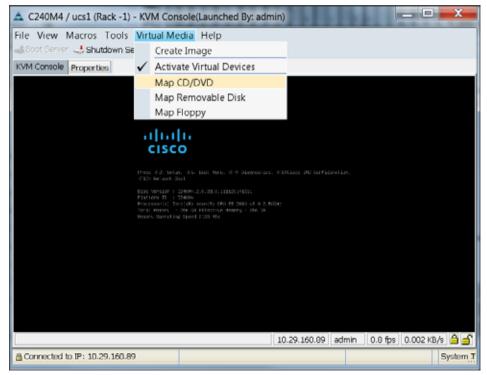
- 5. In the KVM window, select the Virtual Media tab.
- 6. Click the Activate Virtual Devices from the Virtual Media tab.

1



- 7. In the KVM window, select the Virtual Media tab and Click the Map CD/DVD.
- Figure 56 KVM Console

I



8. Browse to the Red Hat Enterprise Linux Server 6.5 installer ISO image file.



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

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

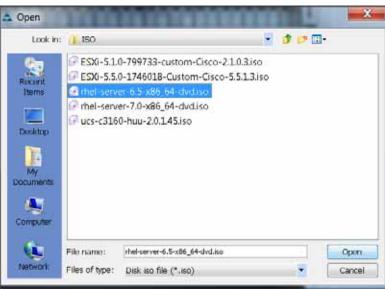
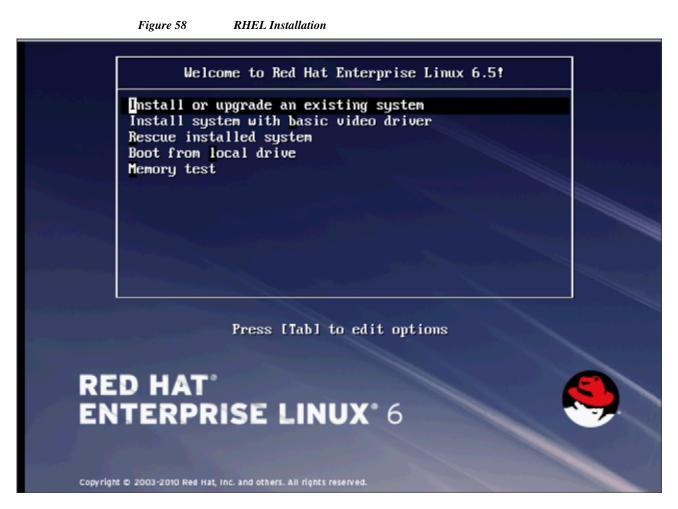


Figure 57 Browse to Red Hat Enterprise Linux ISO Image

- 10. In the KVM window, select the KVM tab to monitor during boot.
- 11. In the KVM window, select the Macros > Static Macros > Ctrl-Alt-Del button in the upper left corner.
- 12. Click OK.
- 13. Click **OK** to reboot the system.
- 14. On reboot, the machine detects the presence of the Red Hat Enterprise Linux Server 6.5 install media.

15. Select the Install or Upgrade an Existing System



16. Skip the Media test and start the installation.

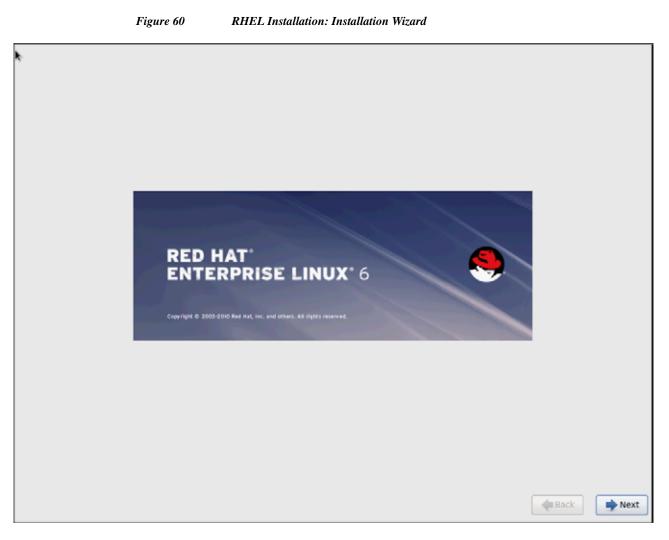
I



I

1

17. Click Next



18. Select language of installation, and then Click Next

Γ

Arabic (العربية)	
Assamese (অসমীয়া)	
Bengali (बाश्ला)	
Bengali(India) (বাংলা (ভারত))	
Bulgarian (Български)	
Catalan (Català)	
Chinese(Simplified) (中文(蜀倅))	
Chinese(Traditional) (中文(正體))	
Croatian (Hrvatski)	
Czech (Čeština)	
Danish (Dansk)	
Dutch (Nederlands)	
English (English)	
Estonian (eesti keel)	
Finnish (suomi)	
French (Français)	
German (Deutsch)	
Greek (Ελληνικά)	
Gujarati (ગુજરાતી)	
Hebrew (עברית)	
Hindi (हिन्दी)	
Hungarian (Magyar)	

Figure 61

1 RHEL Installation: Language Selection

de Back

i Next

1

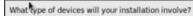
Manual -	
italian (IBM)	
italian (IDM)	
Japanese	
Korean	
Latin American	
Macedonian	
Norwegian	
Polish	
Portuguese	
Bomanian	
Pussian	
Serbian	
Serbian (latin)	
Slovak (qwerty)	
Slovenian	
Spanish	
Swedish	
Swiss French	
Swiss French (latin1)	
Swiss German	
Swiss German (latin1)	
Turkish	
U.S. English	
U.S. International	
Ukrainian	
United Kingdom	

Figure 62 RHEL Installation: Language Selection

19. Select Basic Storage Devices and Click Next

Γ

Figure 63 **RHEL Installation: Installation Type**



- Basic Storage Devices Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it. ۲
- Specialized Storage Devices
 O Installs or upgrades to enterprise devices such as Storage Area Networks (SANs). This option will allow
 you to add PCoE / ISCSI / zPCP disks and to filter out devices the Installer should ignore.

		Back Ne
*		
	Storage Device Warning	
_	torage device below may contain data.	
	ATA INTEL SSDSC2BB12 L14473.460938 MB pci-0000:00:1f.2-scsi-4:0:0:0	
We coul	ld not detect partitions or filesystems on this device.	
not, the in this is	uld be because the device is blank , unpartitioned , or virtual . If ere may be data on the device that can not be recovered if you use it installation. We can remove the device from this installation to the data.	
Are you	a sure this device does not contain valuable data?	
	ly my choice to all devices with undetected partitions or filesystems	
⊠ Appl	, , , , entree to an actively inter anactively provide a completence	
⊠ Appl	Yes, discard any data No, keep any data	
⊠ Appi		
⊠ Appl		Back Nex

1

20. Provide hostname and configure Network for the host.

Figure 64	RHEL Installation: Provide	Host Name		
	Please name this computer. The hostname identifies the computer on a network.			
Hostname	e: rhel65]		
Configur	e Network			
			Back	Next

Figure 65 RHEL Installation: IPV4 Setting for eth0

			Editing e	eth0		
Connect	ion name:	eth0				
	nect automa lable to all u		/			
Wired	802.1x Sec	urity	IPv4 Setti	ngs	IPv6 Sett	tings
Metho	od: Manua	I				•
Addr	esses					
	dress	N. Contractor	nask	Letter states	teway	Add
10.	29.160.165	255.	255.255.0	10.	29.160.1	Delete
Sea DHG	5 servers: rch domains CP client ID: Require IPv4		essing for	this	connectio	n to complete
				[Cancel	Apply

Γ

igure oo	KIIEL Instatiati		
	Editing	eth1	
Connection name	e: eth1		
 Connect autor Available to a 	-		
Wired 802.1x S	Security IPv4 Sett	ings IPv6 Settin	gs
Method: Mar	ual		\$
Addresses			
Address	Netmask	Gateway	Add
192.168.11.	165 255.255.255.	•	Delete
DNS servers:			
Search doma	ins:		
DHCP client	D:		
Require IF	v4 addressing for	this connection t	o complete
			Routes
		Cancel	Apply

Figure 66 RHEL Installation: IPV4 Setting for eth1

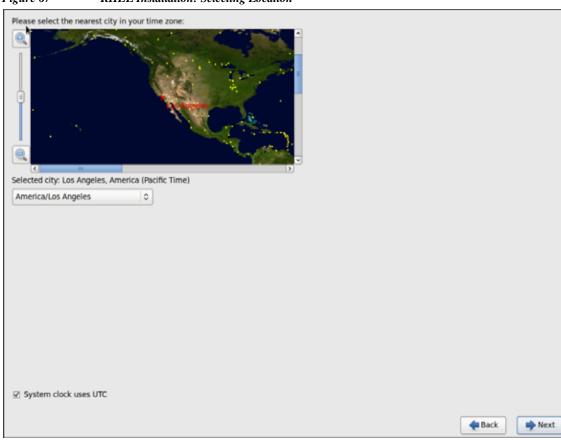


Figure 67 RHEL Installation: Selecting Location

Γ

rigure 68	RHEL Installation: E	nter Root Credent	ials		
The root the syste user.	account is used for administering em. Enter a password for the root				
Root Password:	•••••]			
Confirm:	•••••]			
				ack	Next 🔶

1

.... DITET I ~0 11 .. n ~ 1

21. Choose Create custom layout for Installation type.

Figure 69	RHEL Installation: Create Custom Layout		
Which type	of installation would you like?		
OS	Use All Space Removes all partitions on the selected device(s). This includes partitions created by other operating systems.		
	TIp: This option will remove data from the selected device(s). Make sure you have backups.		
05	Replace Existing Linux System(s) Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).		
	Tip: This option will remove data from the selected device(s). Make sure you have backups.		
	Shrink Current System Shrinks existing partitions to create free space for the default layout.		
0	Use Free Space Retains your current data and partitions and uses only the unpartitioned space on the selected device (s), assuming you have enough free space available.		
	Create Custom Layout Manually create your own custom layout on the selected device(s) using our partitioning tool.		
Encrypt :	system		
☑ Review a	and modify partitioning layout		
		Back	Next

Following steps can be used to create two software RAID 1 partitions for boot and / (root) partitions.

22. Choose free volume and click on Create and choose RAID Partition.

I

ſ

×.		Drive Free 11447		Idd (114473 MB) (Model: ATA INTEL SSDSC28B12)
Device	Size (MB)	Mount Point/ RAID/Volume	Туре	Format
▼ sdd (/dev/sdd)				
Free	114470			
♥ sde (/dew/sde) Free	114470			Create Storage Create Partition Standard Partition General purpose partition creation Information Create Software RAID Information Real Partition Create a RAID formated partition Create a RAID formated partition Information Create a RAID formated partition Information Create a RAID formated partition Information Create LVM Information LVM Volume Group Requires at least 1 free LVM formated partition LVM Logical Volume Create a logical volume on selected volume group Create an LVM formated partition LVM Physical Volume
				Create Edit Delete Reset

1

Figure 70 RHEL Installation: Create RAID Partition

23. Choose "Software RAID" for File system Type and set size for Boot volume.

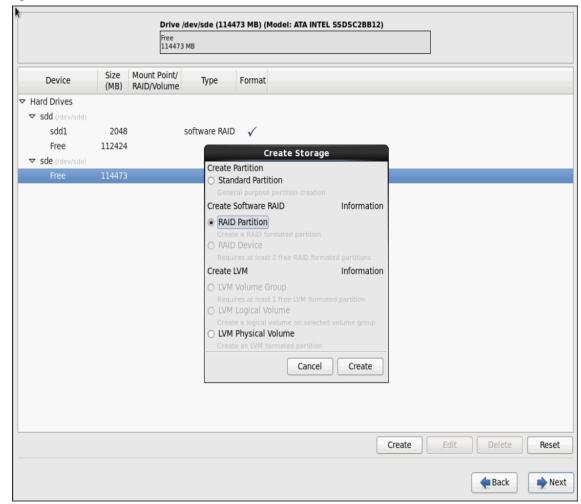
Device Size (MB) Mount Point/ RADD/Volume Type Format * Jadd Drives			Free 11447	/dev/sdd (114473 M 1 MD	B) (Model: ATA IP	ITEL SSD	(\$5,28812)			
v sdd mannad Free 114470 Mount Point:	Device 🕅			Type Format						
Free 114470 Add Partition Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of the system Type: Software RAID Image: Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of Software RAID Image: Solution of S										
Free 114470 File System Type: software RAID Drive Size Model 114473 MB Allowable Drives: sde Size (MB): 2048 Additional Size Options Fixed size Fill all space up to (MB): 2048 Fill or maximum allowable size Force to be a primary partition Encrypt Cancel	Free	114470		1	Add	Partitio	n			
File System Type: software RAID Drive Size Model display="block">display="block">display="block" Allowable Drive: size Size (MB): 2048 Additional Size Options # Fill all space up to (MB): 2048 Fill to maximum allowable size Fill to maximum allowable size Force to be a primary partition Encrypt		512-12-22-2		Mount Point:	<not applicable<="" td=""><td>FI.</td><td></td><td>10</td><td></td><td></td></not>	FI.		10		
Drive Size Model ✓ 6dd 114473 MB ATA INTEL SSDSC29812 Allowable Drives: sde 114473 MB ATA INTEL SSDSC28812 Size (MB): 2048 Image: Comparison of the system	Free	114470		File System Type:	software RAID	1		0		
Allowable Drives: dd 114473 MB ATA INTEL SSDSC28812 Size (MB): 2048 Additional Size Options Fixed size Fixed size Fill all space up to (MB): 2048 Fill to maximum allowable size Force to be a primary partition Encrypt Cancel OK							todal	-		
Allowable Drives: sde 114473 MB ATA INTEL SSDSC2BB12 Size (MB): 2048 Additional Size Options Fixed size Fill all space up to (MB): 2048 Fill to maximum allowable size Force to be a primary partition Encrypt Cancel OK					a second second					
Additional Size Options Fixed size Fixed size Fill all space up to (MB): Force to be a primary partition Force to be a primary partition Cancel OK				Allowable Drives:	GARCUSCUS AND ADDRESS		A REAL PROPERTY AND A REAL PROPERTY.			
Additional Size Options Fixed size Fill all space up to (MB): Fill to maximum allowable size Force to be a primary partition Encrypt Cancel OK				Size (MB):	2048			1		
Fill all space up to (MB): Fill to maximum allowable size Force to be a primary partition Encrypt Cancel OK				The second s	ptions					
Cancel OK				O Fill all space of			2048			
				Contraction of the second s	rimary partition					
Create Cdt Delete A							Cancel OK			
							Create	Edit	Delete	Rese

Figure 71 RHEL Installation: Add Partition

I

Γ

24. Similarly, do the RAID partitioning for the other free volume.



1

Figure 72 RHEL Installation: Create RAID Partition

×.		Free 114473 MB		
Device	Size (MB)	Mount Point/ RAID/Volume	Format	
Hard Drives				
▼ sdd (/dev/sdd)			Add Partition	
sdd1 Free	2048 112424	Mount Doint:	<not applicable=""></not>	~
♥ sde (/dev/sde)		File System Typ	e: software RAID	0
Free	114473			L SSDSC28B12
		Allowable Drive	s: 🗹 sde 114473 MB ATA INTE	L SSDSC28812
		Size (MB):	2048	6
		Additional Size	Options	
		Fixed size		
		 Fill all space 	e up to (MB):	 x
		 Fill to maxi 	mum allowable size	
		Force to be Encrypt	a primary partition	
			Can	cel OK
				Create Edit Delete R

Figure 73 RHEL Installation: Add Partition

I

Γ

25. Now similarly create RAID partitions for root (/) partition on both the devices and use rest of the available space.

		//free 21124	24 MB	- E.	73 MB) (Mode						
Device	Size (MB)	Mount Point/ RAID/Volume	η	ype	Format						
Hard Drives											
♥ sdd											
sddl	2048		softwa	are RAID	~						
Free	112424	; ;			Creat	e Storage	2				
▼ sde				Create P		e-scorage					
sdel	2048		softw		ard Partition						
Free	112424										
				Create 5	oftware RAID		Informatio	ari -			
				The Grouperson	Partition						
				O RAID	Device						
				Create L	/M		Informatio	n			
					ogical Volum						
				O LVM F	hysical Volun	ne					
						Cancel	Create	3			
			1	_							
							-	Transferra	11 - 2011	1111/02/02	10.000
								Create	Edit.	Delete	Res

1

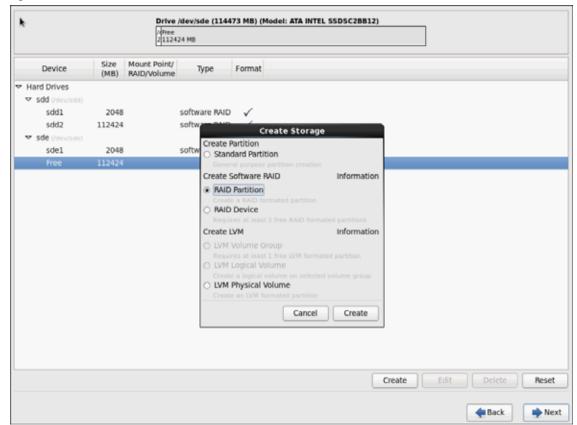
Figure 74 RHEL Installation: Create RAID Partition

		Drive /dev/sdd (1) /dRee 2112424 MB	4473 MB) (Model: ATA INTEL SSDSC2BB12)		
Device		Mount Point/ RAID/Volume	Format		
Hard Drives					
♥ Sdd (/dev/sdd)			Add Partition		
sddl	2048	Mount Point:	<not applicable=""></not>		
Free	112424				
▼ sde (/dev/sde)		File System Type:	software RAID	•	
sdel Free	2048 112424		O Drive Size Model		
nee	112424		✓ sdd 114473 MB ATA INTEL SSDSC2881	2	
		Allowable Drives:	sde 114473 MB ATA INTEL SSDSC2BB1	2	
		Size (MB):	200	•	
		 Additional Size O Fixed size 	tions		
		 Fill all space u Fill to maximu 	p to (MB): 1 m allowable size	< <u>x</u>	
		 Force to be a p Encrypt 	rimary partition		
			Cancel	к	
			Creat	e Ed	fit Delete Re

Figure 75 RHEL Installation: Add Partition

I

Γ



1

Figure 76 RHEL Installation: Create RAID Partition

h :		Drive /dev/sde (1) /free 2112424 MB	14473 MB) (Model: ATA IN	TEL SSDSC28812)			
Device		Mount Point/ Type RAID/Volume	Format				
 Hard Drives 							
♥ sdd			Add Partiti	on			
sdd1 sdd2	2048 112424	Mount Point:	<24rd Applicable>		1		
▼ sde (monte) sde1	2048	File System Type:	software RAID		0		
free	112424		O Drive Size	Model			
	and a storight		🖸 sdd 114473 MB	ATA INTEL SSD5C2BB12			
		Allowable Drives:	2 son 114473 MB	ATA INTEL SSDSC2BH12			
		Size (M8):	200		0		
		Additional Size O	ptions				
		O Fill all space u	p to (MB):	1	Tel.		
		Fill to maximu	im allowable size		- 101		
		Force to be a p Encrypt	rimary partition				
				Cancel			
				Create	1 64	t. Deiete	Res
					-		
						de Back	-

Figure 77 RHEL Installation: Add Partition

Γ

26. The above steps created 2 boot and 2 root (/) partitions. Following steps will RAID1 devices.



1

Figure 78 RHEL Installation: Selected RAID Devices

27. Choose one of the boot partitions and click on Create > RAID Device

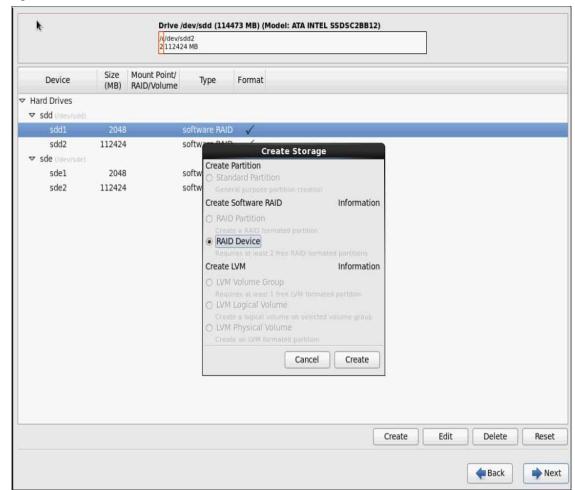


Figure 79 RHEL Installation: Create RAID Device

ſ

28. 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

		Drive Voldew 21124	sdd2	3 MB) (Model: ATA INTEL SSDSC288	12)]		
Device	Size (MB)	Mount Point/ RAID/Volume	Туре	ormat				
Hard Drives								
♥ sdd connorm								
sdd1	2048	1	software RAID	1				
sdd2	112424		software RAID	Make RAID Device				
sde ommen o s								
sdel	2048		Mount Point:	/boot	~			
sde2	112424		File System Typ	e: ext4	0			
				(mark)				
			RAID Device:	md0	0			
			RAID Level:	RAID1	0			
					10			
			RAID Members:	□ sdd2 112424 MB	5			
			INIT HEHIDERS	₹ tde1 2048 MB				
				117474 MD				
			Number of spar	es: [0	1			
			Encrypt					
				Cancel	ок			
					<u></u>			
					Consta	Edit	Delate	Barr
					Create	cuit	Delete	Rese
								-
							Back	R No

1

Figure 80 RHEL Installation: Make RAID Device

29. Similarly repeat for / partitions created above choosing both members with mount point as "/".

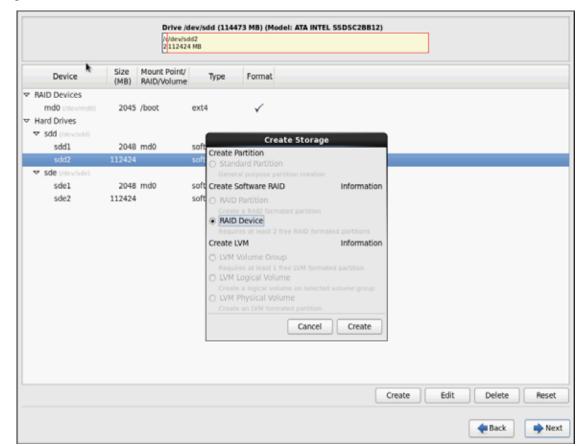


Figure 81 RHEL Installation: Create RAID Device

Γ

RAID Devices md0 (dev/md0) 2045 /boot sdd1 2048 md0 sdd2 112424 Sdd1 2048 md0 sdd2 112424 Sdd1 2048 md0 sdd2 112424 RaiD Device Sdd2 112424 RaiD Device: md1 © RaiD Device: md1 © RaiD Level: RAID1 © Sdd2 112424 MB RAID Level: RAID1 © Sdd2 112424 MB RAID Members: Sde2 112424 MB RAID Members: Sde2 112424 MB RAID Members: Cancel OK	Device	Size (MB)	Mount Point/ RAID/Volume		Format		
sdd1 2048 md0 Make RAID Device sdd2 112424 Mount Point: / ✓ sde1 2048 md0 file System Type: ext4 ○ sde2 112424 RAID Device: md1 ○ RAID Level: RAID1 ○ Padd2 112424 MB RAID Members: Intervention Intervention Intervention Image: Substance Intervention I	md0 (/dev/md0)	2045	/boot	ext4	×		
side1 2046 mido side2 112424 Side1 2048 md0 side2 112424 RAID Device: md1 RAID Level: RAID1 Image: Side2 112424 RAID Device: md1 Image: Side2 112424 RAID Level: RAID1 Image: Side2 112424 MB RAID Members: Side2 Image: Side2 112424 MB Number of spares: Image: Side2 Image: Side2 Image: Side2 Image: Side3 Image: Side3 Image: Side3 </td <td></td> <td></td> <td></td> <td></td> <td>Make DAID Device</td> <td></td> <td></td>					Make DAID Device		
✓ sde (/dev/sde) sde1 2048 md0 sde2 112424 File System Type: ext4 ↓ ↓ RAID Device: md1 ↓ ↓ RAID Level: RAID1 ↓ ↓ RAID Level: RAID1 ↓ ↓ Interpret Sdd2 112424 MB RAID Members: Interpret Sdd2 112424 MB Number of spares: 0 ↓ ↓ Encrypt				Mount Deintr	(
sde1 2048 md0 sde2 112424 RAID Device: md1 ↓ RAID Level: RAID1 ↓ RAID Level: RAID1 ↓ RAID Members: sde2 112424 MB Number of spares: 0 ↓ Encrypt		112424			-		
RAID Level: RAID1 Ø sdd2 112424 MB RAID Members: Ø sde2 Number of spares: 0 Encrypt		2048	md0	File System Type	ext4	\$	
Number of spares: 0 □ Encrypt	sde2	112424		RAID Device:	md1	0	
RAID Members: sde2 112424 MB Number of spares: 0 Encrypt				RAID Level:	RAID1	0	
RAID Members: Sde2 112424 MB Number of spares: Image: Comparison of the spare					Sdd2 112424 MB		
Encrypt				RAID Members:			
Encrypt				Number of spare	к 0		
Cancel							
					Cancel	ок	

1

Figure 82 RHEL Installation: Make RAID Device

 RAID Devices md0 devender 2045 /boot ext4 ✓ Hard Drives sdd1 2048 md0 software RAID ✓ sdd2 112424 md1 software RAID ✓ sde1 2048 md0 software RAID ✓ sde1 2048 md0 software RAID ✓ sde2 112424 md1 software RAID ✓ 	Device	Size (MB)	Mount Point/ RAID/Volume	Туре	Format		
md1 menoreti 112359 / ext4 ✓ ♥ Hard Drives ♥ sdd menoreti software RAID ✓ sdd2 112424 md1 software RAID ✓ ♥ sde menoreti software RAID ✓	RAID Devices						
 Hard Drives sdd sdd1 2048 md0 software RAID √ sdd2 112424 md1 software RAID √ sde sde1 2048 md0 software RAID √ 	md0	2045	/boot	ext4	×		
 ✓ sdd ✓ sdd ✓ sdd2 ✓ 112424 md1 ✓ software RAID ✓ ✓ sde ✓ sde ✓ ✓ sde ✓ sde 	md1 minimut	112359	1	ext4	~		
sdd1 2048 md0 software RAID ✓ sdd2 112424 md1 software RAID ✓ ≈ sde :::::::::::::::::::::::::::::::::::	 Hard Drives 						
sdd2 112424 md1 software RAID √ ▼ sde [mitry/mail] sde1 2048 md0 software RAID √	∞ sdd						
✓ sde (minuland) sde1 2048 md0 software RAID √	sddl	2048	md0	software RAID	~		
sde1 2048 md0 software RAID 🗸	sdd2	112424	md1	software RAID	~		
	♥ sde (manine)						
sde2 112424 md1 software RAID ✓	sde1	2048	md0	software RAID	×		
	sde2	112424	md1	software RAID			

Figure 83 RHEL Installation: Selected RAID Devices

30. Click on Next.

Γ

Device	Size (MB)	Mount Point/ RAID/Volume	Туре	Format					
RAID Devices									
md0	2045	/boot	ext4	× .					
md1	112359	1	ext4	~					
Hard Drives		-		Partitionia	g Warnings				
♥ sdd			The partiti	oning scheme yo	Company of the local division of the local d	wated the			
sdd1	2048		following		a reduction doin	and the second second			
sdd2	112424	md1	You have r	not specified a sv	ap partition. Alt	hough not			
v sde sdel	2048	mdi	strictly res	quired in all case nce for most insta	, it will significan	tly impro	ve		
sde2	112424	1.12776	pertormar	ice for most insta	nacions.				
			Would you	i like to continue	with your reques	ted partiti	onion		
			scheme?	THE OF COLUMN	man your reques	ours beaution	Second .		
					No	Y	15		
					1				

I

1

Figure 84	RHEL Installation:	Partitioning Warning
-----------	--------------------	----------------------



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

31. Click Next, and Format.

× .			Ple	ease Selec	t A Device	Ē.			
Device	Size (MB)	Mount Point/ RAID/Volume	Туре	Format					
 ♥ RAID Devices md0 md1 ♥ Hard Drives ♥ sdd \$ sdd1 \$ sdd2 ♥ sde \$ sde1 \$ sde2 	2045 112359 2048 112424 2048 112424	md0 md1 md0	ext4 ext4 The followi formatted, /dev/sdd /dev/sde	Format W/	rices have been se MSDOS)	elected to be			
						Create	abeter -	0+iate	Reset
								da Back	Nex

Figure 85 RHEL Installation: Format Warning

32. Select default settings and click Next.

Γ

' I z	gure ou		istantanton: Inst	an Door Load	ier			
k	🗹 instal	l boot loader on /dev/sdd.	Change device					
	🗌 Use a	a boot loader password	Change password					
	Boot lo	ader operating system	list					
	Default	Label	Device					Add
	۲	Red Hat Enterprise Linux	/dev/md1					Edit
								Delete
							Heack 🗧	📄 Next

1

Figure 86 RHEL Installation: Install Boot Loader

33. Continue with RHEL Installation as shown below.

 Basic Server 			
 Database Server 			
O Web Server			
 Identity Management Server 			
 Virtualization Host 			
 Desktop 			
 Software Development Workstation 			
 Minimal 			
	tion.		
High Availability	tion.		
High Availability	tion.		
High Availability Load Balancer	tion.		
High Availability Load Balancer ✓ Red Hat Enterprise Linux	tion.		
lease select any additional repositories that you want to use for software instal ☐ High Availability ☐ Load Balancer ☑ Red Hat Enterprise Linux ☐ Add additional software repositories ☑ Modify repository	tion.		
High Availability Load Balancer ✓ Red Hat Enterprise Linux On-Illent Channel Image: Add additional software repositories			
High Availability Load Balancer Red Hat Enterprise Linux			

Figure 87 RHEL Installation: Keep the Default Installation

34. Once the installation is complete reboot the system.

Repeat the steps 1 through 34, to install Red Hat Enterprise Linux 6.5 on Servers 2 through 64.

Note

ſ

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

The host-names and their corresponding IP addresses are shown in Table 7.

Hostname	eth0	eth1	eth2
rhel1	10.29.160.101	192.168.11.101	192.168.12.101
rhel2	10.29.160.102	192.168.11.102	192.168.12.102
rhel3	10.29.160.103	192.168.11.103	192.168.12.103
rhel4	10.29.160.104	192.168.11.104	192.168.12.104
rhel5	10.29.160.105	192.168.11.105	192.168.12.105
rhel6	10.29.160.106	192.168.11.106	192.168.12.106

Table 7Host-names and IP Addresses

Hostname	eth0	eth1	eth2
rhel7	10.29.160.107	192.168.11.107	192.168.12.107
rhel8	10.29.160.108	192.168.11.108	192.168.12.108
rhel9	10.29.160.109	192.168.11.109	192.168.12.109
rhel10	10.29.160.110	192.168.11.110	192.168.12.110
rhel11	10.29.160.111	192.168.11.111	192.168.12.111
rhel12	10.29.160.112	192.168.11.112	192.168.12.112
rhel13	10.29.160.113	192.168.11.113	192.168.12.113
rhel14	10.29.160.114	192.168.11.114	192.168.12.114
rhel15	10.29.160.115	192.168.11.115	192.168.12.115
rhel16	10.29.160.116	192.168.11.116	192.168.12.116
rhel64	10.29.160.164	192.168.11.164	192.168.12.164

Table 7	Host-names and IP Addresses
---------	-----------------------------

Post OS Install Configuration

Choose one of the nodes of the cluster or a separate node as Admin Node for management such as MapR installation, cluster parallel shell, creating a local Red Hat repo and others. In this document, we use rhell for this purpose.

Setting Up Password-less Login

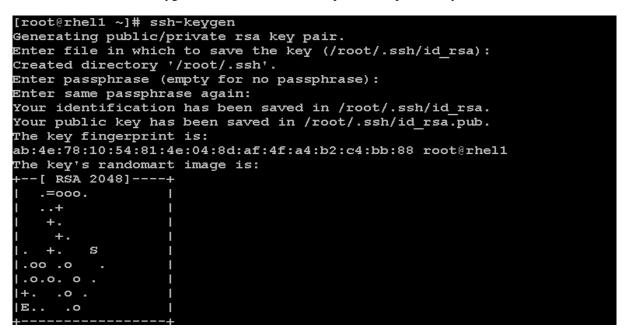
To manage all of the clusters nodes from the admin node we need to setup password-less login. It assists in automating common tasks with cluster-shell (clush, a cluster wide parallel shell), and shell-scripts without having to use passwords.

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 10.29.160.101

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



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 local host localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.29.160.101 rhel1.mgmt
10.29.160.102 rhel2.mgmt
10.29.160.103 rhel3.mgmt
10.29.160.104 rhel4.mgmt
10.29.160.105 rhel5.mgmt
10.29.160.107 rhel7.mgmt
10.29.160.108 rhel8.mgmt
10.29.160.109 rhel9.mgmt
10.29.160.110 rhel10.mgmt
10.29.160.111 rhel11.mgmt
```

10.29.160.112 rhel12.mgmt 10.29.160.113 rhel13.mgmt 10.29.160.114 rhel14.mgmt 10.29.160.115 rhel15.mgmt 10.29.160.116 rhel16.mgmt 10.29.160.164 rhel64.mgmt 192.168.11.101 rhel1 192.168.11.102 rhel2 192.168.11.103 rhel3 192.168.11.104 rhel4 192.168.11.105 rhel5 192.168.11.106 rhel6 192.168.11.107 rhel7 192.168.11.108 rhel8 192.168.11.109 rhel9 192.168.11.110 rhel10 192.168.11.111 rhel11 192.168.11.112 rhel12 192.168.11.113 rhel13 192.168.11.114 rhel14 192.168.11.115 rhel15 192.168.11.116 rhel16 . . . 192.168.11.164 rhel64 192.168.12.101 rhel1-2 192.168.12.102 rhel2-2 192.168.12.103 rhel3-2 192.168.12.104 rhel4-2 192.168.12.105 rhel5-2 192.168.12.106 rhel6-2 192.168.12.107 rhel7-2 192.168.12.108 rhel8-2 192.168.12.109 rhel9-2 192.168.12.120 rhel10-2 192.168.12.121 rhel12-2 192.168.12.122 rhel12-2 192.168.12.123 rhel13-2 192.168.12.124 rhel14-2 192.168.12.125 rhel15-2 192.168.12.126 rhel16-2 . . . 192.168.12.164 rhel64-2

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

1

scp clustershell-1.6-1.el6.noarch.rpm rhell:/root/ Login to rhell 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[1-64].mgmt
```



For more information and documentation on ClusterShell, visit https://github.com/cea-hpc/clustershell/wiki/UserAndProgrammingGuide



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 for rhel<host> and rhel<host>.mgmt.

[root@rhel1 ~]# ssh rhel2 The authenticity of host 'rhel2 (192.168.11.102)' can't be established. RSA key fingerprint is 9e:4d:91:3d:b9:ef:eb:97:b4:80:dc:3b:85:f5:ad:20. Are you sure you want to continue connecting (yes/no)?

[root@rhel1 ~]# ssh rhel5.mgmt
The authenticity of host 'rhel5.mgmt (10.29.160.105)' can't be established.
RSA key fingerprint is 7a:98:75:9a:6a:1a:80:a4:97:43:6c:8a:12:57:db:74.
Are you sure you want to continue connecting (yes/no)?

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.

mkdir -p /var/www/html/rhelrepo

- 2. Copy the contents of the Red Hat DVD to /var/www/html/rhelrepo directory.
- 3. Alternatively, if you have access to a Red Hat ISO Image, Copy the ISO file to rhel1.

 $\tt scp \ rhel-server-6.5-x86_64-dvd.iso \ rhell:/root/$ Here we assume you have the Red Hat ISO file located in your present working directory.

```
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
```

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

[root@rhel1 ~]# mkdir -p /var/www/html/rhelrepo [root@rhel1 ~]# mkdir -p /mnt/rheliso [root@rhel1 ~]# [root@rhel1 ~]# mount -t iso9660 -o loop /root/rhel-server-6.5-x86_64-dvd.iso /mnt/rheliso/ [root@rhel1 ~]# cp -r /mnt/rheliso/* /var/www/html/rhelrepo/

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

```
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

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.

clush -a -b -c /etc/yum.repos.d/rheliso.repo --dest=/etc/yum.repos.d/

[root@rhel1 ~]# 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.



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

```
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
```

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

[root@rhel1 ~]# yum -y install createrepo			
Loaded plugins: product-id, refresh-packagekit, security, subscription-manager			
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register			
rhel6.5	3.9]	kB	00:00
rhel6.5/primary_db	3.11	MB	00:00
Setting up Install Process			
Resolving Dependencies			
> Running transaction check			
> Package createrepo.noarch 0:0.9.9-18.el6 will be installed			
> Processing Dependency: python-deltarpm for package: createrepo-0.9.9-18.el6.noarch			
> Running transaction check			
> Package python-deltarpm.x86_64 0:3.5-0.5.20090913git.el6 will be installed			
> Processing Dependency: deltarpm = 3.5-0.5.20090913git.el6 for package: python-deltarpm-3.5-0.5.20090913git	.el6	.x86_64	
> Running transaction check			

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

```
createrepo .
[root@rhell rhelrepo]# createrepo .
Spawning worker 0 with 3763 pkgs
Workers Finished
Gathering worker results
Saving Primary metadata
Saving file lists metadata
Saving other metadata
Generating sqlite DBs
Sqlite DBs complete
```

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

cd /var/www/html/rhelrepo

```
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 192.168.11.101
```

S.

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:192.168.11.101
Address:192.168.11.101#53
Name: rhel1
Address: 192.168.11.101 •
[root@rhel2 ~]# nslookup rhel1.mgmt
Server: 192.168.11.101
Address: 192.168.11.101#53
Name: rhel1.mgmt
Address: 10.29.160.101 •
[root@rhel2 ~]# nslookup 10.29.160.101
Server: 192.168.11.101
Address: 192.168.11.101#53
101.160.29.10.in-addr.arpa name = rhel1.mgmt. •
```

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

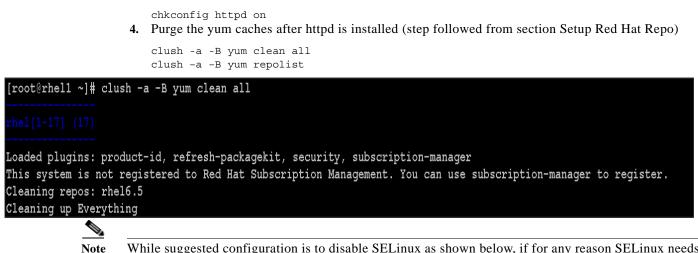
2. Add ServerName and make the necessary changes to the server configuration file.

```
vi /etc/httpd/conf/httpd.conf
ServerName 10.29.160.101:80
```

```
[root@rhel1 ~]# vi /etc/httpd/conf/httpd.conf
[root@rhel1 ~]# cat /etc/httpd/conf/httpd.conf | grep ServerName
# ServerName gives the name and port that the server uses to identify itself.
#ServerName www.example.com:80
ServerName 10.29.160.101:80
# ServerName directive.
# ServerName durective.
```

3. Start httpd

service httpd start



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 repofiles 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 rhell (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"
```

filename:	/lib/modules/2.6.32-431.el6.x86_64/extra/enic/enic.ko
version:	2.1.1.66
license:	GPL v2
author:	Scott Feldman <scofeldm@cisco.com></scofeldm@cisco.com>
description:	Cisco VIC Ethernet NIC Driver

Setting up JAVA

MapR requires JAVA 7, download jdk-7u75–linux-x64.rpm from oracle.com (http://www.oracle.com/technetwork/java/javase/downloads/jdk7–downloads-1880260.html) to admin node (rhel1).

Create the following files java-set-alternatives.sh and java-home.sh on admin node (rhel1)

vi java-set-alternatives.sh

```
#!/bin/bash
for item in java javac javaws jar jps javah javap jcontrol jconsole jdb; do
  rm -f /var/lib/alternatives/$item
  alternatives --install /usr/bin/$item $item /usr/java/jdk1.7.0_75/bin/$item 9
  alternatives --set $item /usr/java/jdk1.7.0_75/bin/$item
done
```

vi java-home.sh

```
export JAVA_HOME=/usr/java/jdk1.7.0_75
Run the following commands on admin node (rhell) to install and setup java on all nodes
```

1. Copying JDK rpm to all nodes

clush -b -a -c /root/jdk-7u75-linux-x64.rpm --dest=/root/

2. Make the two java scripts created above executable

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

3. Copying java-set-alternatives.sh to all nodes

```
clush -b -a -c ./java-set-alternatives.sh --dest=/root/
```

4. Extract and Install JDK on all nodes

clush -a -b rpm -ivh /root/jdk-7u75-linux-x64.rpm

5. Setup Java Alternatives

clush -b -a ./java-set-alternatives.sh6. Ensure correct java is setup on all nodes (should point to newly installed java path)

- clush -b -a "alternatives --display java | head -2"
- 7. Setup JAVA_HOME on all nodes

```
clush -b -a -c ./java-home.sh --dest=/etc/profile.d
```

- 8. Display JAVA_HOME on all nodes
- clush -a -b "echo \\$JAVA_HOME" 9. Display current java -version
 - clush -B -a java -version

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.

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

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 nodes by executing the following command in the admin node (rhell)

for SERVER in {102..168}; do scp /root/ntp.conf
10.29.160.\$SERVER:/etc/ntp.conf; done

[root@rhel1 ~]# for	SERVER in	{102168};	do scp	/root/ntp.conf	10.29.160	.\$SERVER:/etc/	ntp.c	onf; done	
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00
ntp.conf						100%	136	0.1KB/s	00:00

<u>Note</u>

Instead of the above for loop, this could be run as a clush command with "-w" option.

```
clush -w rhel[2-68] -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 thef following to syncronize the time and restart NTP daemon on all nodes

```
clush -a -B "yum install -y ntpdate"
clush -a -b "service ntpd stop"
clush -a -b "ntpdate rhell"
clush -a -b "service ntpd start"
Ensure restart of NTP daemon across reboots
```

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:

clush -B -a rsyslogd -v

syslogd 5.8.10, compiled with:	
FEATURE_REGEXP:	Yes
FEATURE LARGEFILE:	No
GSSAPI Kerberos 5 support:	Yes
FEATURE DEBUG (debug build, slow code):	No
32bit Atomic operations supported:	Yes
64bit Atomic operations supported:	Yes
Runtime Instrumentation (slow code):	No

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:

root soft nofile 64000 root hard nofile 64000



Copy the /etc/security/limits.conf file from admin node (rhell) to all the nodes using the following command.

1

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

[root@rhel1 ~]# clush -a -b -c /etc/security/limits.conf --dest=/etc/security/

Verify the **ulimit** setting with the following steps:



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"
```

coot@rhel1 ~]# clush -a -b "sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config "



The above command may fail if SELinux is already disabled.

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"
```

Swapping

Lowering vm.swappiness reduces anonymous paging and minimizes OOM killer invocations. With vm.swappiness set to 1, the kernel will try to reclaim from the page cache instead of application (anonymous) pages.

In order to reduce Swapping, run the following on all nodes. Variable vm.swappiness defines how often swap should be used. 0 is No Swapping, 60 is the default value.

clush -a -b " echo \'vm.swappiness=0\' >> /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
```

copy me 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"

Install Openssl

Install Openssl and Openssl-devel version 1.0.1e-30 and above for RHEL6.5. If openssl is already installed (generally the case), use the following command to upgrade openssl.

```
clush -a -b -c /root/openssl-*
clush -a -b rpm -Uvh openssl-1.0.1e-*.rpm openssl-devel-1.0.1e-*.rpm
```

[root@rhel1 ~]# rpm -U	<pre>tvh openssl-1.0.1e-30.el6_6.5.x86_64.rpm openssl-devel-1.0.1e-30.el6_6.5.x86_64.rpm</pre>
warning: openssl-1.0.1	e-30.el6_6.5.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
Preparing	######################################
1:openssl	#######################################
2:openssl-devel	

(RPMs are available at:

http://mirror.centos.org/centos/6/updates/x86_64/Packages/openssl-1.0.1e-30.el6_6.5.x86_64.rpm and

http://mirror.centos.org/centos/6/updates/x86_64/Packages/openssl-devel-1.0.1e-30.el6_6.5.x86_64.rp m)

Note

This requires krb5-devel and zlib-devel as dependencies. If not installed, install it as follows on the nodes throwing error "yum –y install krb5-devel zlib-devel"

Disable IPv6 Defaults

Disable IPv6 as the addresses used are IPv4.

```
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
```

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

Configuring Data Drives

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 MapRFS (HDFS supported) Data.

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

From the website download storcli: http://www.lsi.com/downloads/Public/RAID%20Controllers/RAID%20Controllers%20Common%20Fi les/1.14.12_StorCLI.zip

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.

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

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

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

- clush -a -b rpm -ivh storcli-1.14.12-1.noarch.rpm
- 4. Run the below command to copy storcli64 to root directory.

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

```
[root@rhel1 ~]# cd /opt/MegaRAID/storcli/
[root@rhel1 storcli]# ls
install.log libstorelibir-2.so libstorelibir-2.so.14.07-0 storcli64
[root@rhel1 storcli]# cp storcli64 /root/
```

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

```
clush -a -b -c /root/storcli64 --dest=/root/
clush -a -B ./storcli64 -cfgeachdskraid0 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

Cluster Verification and Micro-Benchmark

This section provides a set of micro-benchmarks and prerequisites scripts to verify that all the systems are configured correctly:

- Prerequisite script to verify configuration across the cluster
- STREAM benchmark to test memory bandwidth
- RPCtest to test network bandwidth
- IOzone to test I/O

Running these tests is optional. Test results can vary based on topology and configuration.

Running Cluster Verification Script

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=' \ [0; 32m'
red='\e[0;31m'
NC='\e[Om' # 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 ""
```

I

```
echo ""
echo -e "${green}Memory ${NC}"
clush -a -B "cat /proc/meminfo | grep -i ^memt | uniq"
echo ""
echo ""
echo -e "${green}Number of Dimms ${NC}"
clush -a -B "echo -n 'DIMM slots: '; `which dmidecode` |grep -c \setminus
'^[[:space:]]*Locator:'"
clush -a -B "echo -n 'DIMM count is: '; `which dmidecode` | grep \ "Size"| grep -c
"MB""
clush -a -B "`which dmidecode` | awk '/Memory Device$/,/^$/ {print}' |\ grep -e
'^Mem' -e Size: -e Speed: -e Part | sort -u | grep -v -e 'NO \ DIMM' -e 'No Module
Installed' -e Unknown"
echo ""
echo ""
# probe for cpu info #
echo -e "${green}CPU ${NC}"
clush -a -B "grep '^model name' /proc/cpuinfo | sort -u"
echo ""
clush -a -B "`which lscpu` | grep -v -e op-mode -e ^Vendor -e family -e\ Model: -e
Stepping: -e BogoMIPS -e Virtual -e 'Byte -e ''NUMA node(s)'"
echo ""
echo ""
# probe for nic info #
echo -e "${green}NIC ${NC}"
`which ethtool` | grep -e ^Settings -e Speed"
echo ""
clush -a -B "`which lspci` | grep -i ether"
echo ""
echo ""
# probe for disk info #
echo -e "${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 ${NC}"
clush -a -B date
echo ""
echo ""
echo -e "${green}NTP Status ${NC}"
clush -a -B "ntpstat 2>&1 | head -1"
echo ""
echo ""
echo -e "${green}SELINUX ${NC}"
clush -a -B "echo -n 'SElinux status: '; grep ^SELINUX= \ /etc/selinux/config 2>&1"
echo ""
```

ſ

```
echo ""
echo -e "${green}IPTables ${NC}"
clush -a -B "`which chkconfig` --list iptables 2>&1"
echo ""
clush -a -B "`which service` iptables status 2>&1 | head -10"
echo ""
echo ""
echo -e "${green}Transparent Huge Pages ${NC}"
clush -a -B " cat /sys/kernel/mm/*transparent hugepage/enabled"
echo ""
echo ""
echo -e "${green}CPU Speed${NC}"
clush -a -B "echo -n 'CPUspeed Service: '; `which service` cpuspeed \ status 2>&1"
clush -a -B "echo -n 'CPUspeed Service: '; `which chkconfig` --list \ cpuspeed 2>&1"
echo ""
echo ""
echo -e "${green}Java Version${NC}"
clush -a -B 'java -version 2>&1; echo JAVA HOME is ${JAVA HOME:-Not \ Defined!}'
echo ""
echo ""
echo -e "${green}Hostname Lookup${NC}"
clush -a -B " ip addr show"
echo ""
echo ""
echo -e "${green}Open File Limit${NC}"
clush -a -B 'echo -n "Open file limit(should be >32K): "; ulimit -n'
# MapR related RPMs
clush -a -B 'rpm -ga | grep -i nfs |sort'
clush -a -B 'rpm -qa | grep -i nfs |sort'
clush -a -B 'echo Missing RPMs: ; for each in make patch redhat-lsb irqbalance
syslinux hdparm sdparm dmidecode nc; do rpm -q $each | grep "is not installed"; done'
clush -a -B "ls -d /opt/mapr/* | head"
# mapr login for hadoop
clush -a -B 'echo "mapr login for Hadoop"; getent passwd mapr'
clush -a -B 'echo "Root login"; getent passwd root'
exit
```

Change permissions to executable

chmod 755 cluster_verification.sh

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

./cluster_verification.sh

Running STREAM Benchmark

The STREAM benchmark measures sustainable memory bandwidth (in MB/s) and the corresponding computation rate for simple vector kernels. To download the STREAM benchmark, see:

http://www.cs.virginia.edu/stream/

Follow these steps to run the STREAM benchmark:

1. Log on to the admin node. Copy and extract STREAM file to each node (/root/).

clush -B -a "tar -xvf stream.tgz"

2. Run the following command to run the STREAM benchmark on all nodes:

clush -B -a "/root/stream/runme.sh > /root/stream.log"

3. Run the following command to verify the results:

```
Extract the five lines of the result as shown and verify it on all the nodes.
$clush -B -a "grep -A5 \"Function
                                 \" stream.log"
_____
rhel1
_____
Function
          Rate (MB/s)
                       Avg time
                                  Min time
                                               Max time
         53289.0222
                        0.0241
                                    0.0240
                                                0.0243
Copy:
Scale:
           73664.0430
                          0.0175
                                     0.0174
                                                 0.0177
Add:
            75339.0246
                          0.0257
                                      0.0255
                                                  0.0259
Triad:
            76845.8770
                          0.0252
                                      0.0250
                                                  0.0254
```



Results can vary based on the configuration.

Running RPCtest

MapR RPCtest is network bandwidth measurement test. In this solution the methodology adopted to verify the network bandwidth across the cluster requires configuring half the nodes as senders and remaining half as receivers. This test is included in MapR software available at /opt/mapr/servers/tools/rpctest as part of the installation.

Follow the steps below to run RPCtest:

1. Log on to the admin node and run the following commands to create the script:

```
#!/bin/bash
# Define sender nodes
# 8 servers in each rack act as servers and the other half as clients
senders=( 192.168.12.11 192.168.12.12 192.168.12.13 192.168.12.14
192.168.12.19 192.168.12.20 192.168.12.21 192.168.12.22
192.168.12.27 192.168.12.28 192.168.12.29 192.168.12.30
192.168.12.35 192.168.12.36 192.168.12.37 192.168.12.38
192.168.12.43 192.168.12.44 192.168.12.45 192.168.12.46
192.168.12.51 192.168.12.52 192.168.12.53 192.168.12.54
192.168.12.59 192.168.12.60 192.168.12.61 192.168.12.62
192.168.12.67 192.168.12.68 192.168.12.69 192.168.12.70 )
for node in "${half1[@]}"; do
 ssh -n $node /opt/mapr/servers/tools/rpctest -server &
done
sleep 9 # let the servers set up
# Define receiver nodes
receivers=( 192.168.12.15 192.168.12.16 192.168.12.17 192.168.12.18
192.168.12.23 192.168.12.24 192.168.12.25 192.168.12.26
192.168.12.31 192.168.12.32 192.168.12.33 192.168.12.34
192.168.12.39 192.168.12.40 192.168.12.41 192.168.12.42
192.168.12.47 192.168.12.48 192.168.12.49 192.168.12.50
192.168.12.55 192.168.12.56 192.168.12.57 192.168.12.58
192.168.12.63 192.168.12.64 192.168.12.65 192.168.12.66
192.168.12.71 192.168.12.72 192.168.12.73 192.168.12.74 )
i - 0
for node in "${receivers[@]}"; do
 ssh -n $node "/opt/mapr/servers/tools/rpctest -client 5000 \ ${senders[$i]} >
rpctest.log" &
  ((i++))
```

```
done
#wait $! # Comment/uncomment this to make it sequential/concurrent
sleep 5
tmp=${half1[@]}
clush -w ${tmp// /,} pkill rpctest
```

- 2. Run runRPCtest.sh command from the admin node.
- 3. Results are generated on receiver nodes. Verify results for all the nodes.

```
Note
```

Results can vary based on the topology and configuration.

Running IOzone Benchmark

IOzone is a filesystem benchmark that measures the performance of various I/O operations, such as read, write, re–read, re–write, fread, fwrite, random read and random write.



IOzone is data destructive. Do not run the test on disks with data.

Follow these steps to run IOzone benchmark test:

- 1. Download IOzone from http://www.iozone.org/ and copy to all nodes at /root/.
- 2. Create the following script, run IOzone.sh on the admin node.

```
#!/bin/bash
# Parallel IOzone tests to stress/measure disk controller
# These tests are destructive therefore
# Test must be run BEFORE MapR filesystem is formatted with disksetup
# Run iozone command once on a single device to verify iozone command
D=$(dirname "$0")
abspath=$(cd "$D" 2>/dev/null && pwd || echo "$D")
# run iozone with -h option for usage, adjust path below for iozone location
# Set list of device names for the 'for' loop
lsblk -id | grep -o ^sd. | sort > /tmp/iozone.disks
for i in `lsblk -i | grep -B2 md[0-1] | grep -v '-' | awk '{print $1}'`; do sed
-i "/$i/d" /tmp/iozone.disks; done
disks=`cat /tmp/iozone.disks | xargs`
echo $disks
set -x
for disk in $disks; do
echo $abspath/iozone -I -r 1M -s 80G -i 0 -i 1 -i 2 -f /dev/$disk >
$disk-iozone.log&
   sleep 3 #Some controllers seem to lockup without a sleep
done
```

- **3.** Copy runIOzone.sh to all the nodes at location /root/.
- 4. Run the following command to start the test:

```
clush -B -a runIOzone.sh
```

5. Verify that the tests are running and wait for its completion.

clush -B -a "ps -aef | grep iozone | wc -l" -----rhel[1-64] (64)

6. Run the following command to verify the test results.

```
Result is generated for each disk as sd<x>-iozone.log, where <x> is the device id.
These logs have sequential and random write and read latencies from each disks.
$ grep " 83886080 " sd*.log
sdb-iozone.log: 83886080 1024 97978 97951 100673 99254 49002 66552
sdc-iozone.log: 83886080 1024 101290 100745 97803 97006 48863 66671
sdd-iozone.log: 83886080 1024 94286 94937 96752 95872 48871 65605
```

```
Note
```

Results can vary based on configuration.

Installing MapR

Installing MapR software across the cluster involves performing several steps on each node. To make the installation process simpler, start with the installation of core MapR components such as CLDB, MapR–FS, NFS gateway and Yarn. Any additional Hadoop ecosystem components can be easily installed by following instructions on http://doc.mapr.com/display/MapR/Ecosystem+Guide. Follow Figure 91 for role assignments for installation of services on the 64–node cluster.

The following sections describe the steps and options for installing MapR software:

- Preparing Packages and Repositories
- MapR Installation
 - Installing MapR packages
 - Verify successful installation
- Configure the Node with the configure.sh Script
- Formatting Disks with the disksetup Script

Planning the Cluster

The first step towards deploying the MapR is planning which nodes contribute to the cluster, and selecting the services that will run on each node.

MapR Services

In a typical cluster, most nodes are dedicated to data processing and storage, and a smaller number of nodes run services that provide cluster coordination and management. Some applications run on cluster nodes and others run on client nodes that can communicate with the cluster.

The following table shows some of the services that can be run on a node.

Figure 88 shows the list of MapR services and the corresponding descriptions.

-							
	MapReduce	Storage	Management	Application			
Service			Descri	iption			
Warden	Warden runs on	every no	de, coordinating	the node's contribution to the cluster.			
TaskTracker (optional)	TaskTracker sei manages task e	vice recei xecution.	ves task assign	apReduce tasks on a node. The ments from the JobTracker service and			
NodeManager	resources and n	nonitors th	e health of the r	e NodeManager manages node node. It works with the tainers that run on the node.			
FileServer	FileServer is the MapR service that manages disk storage for MapR- MapR-DB on each node.						
CLDB		a storage :	services among	e (CLDB) service. The CLDB service MapR–FS FileServer nodes, MapR			
NFS	Provides read- support for cond			NFS access to the cluster, with full ess.			
MapR HBase Client (optional)	Provides access nodes that will a			HBase APIs. Required on all client L–FS			
JobTracker (optional)				ker service coordinates the execution of askTracker nodes and monitoring task			
ResourceManager				e. The ResourceManager manages age and node health.			
ZooKeeper	Enables high av coordination.	/ailability (HA) and fault tol	lerance for MapR clusters by providing			
HistoryServer	Archives MapRe	educe job	metrics and met	tadata.			
Web Server	Runs the MapR	Control S	ystem.				
Hue	Hue is Hadoop ecosystem com			ts with Apache Hadoop and its g, and Oozie.			
Pig	Pig is a high-le	vel data-fl	ow language an	nd execution framework.			
Hive	Hive is a data w summarization.	arehouse	that supports S	QL–like ad hoc querying and data			
Flume	Flume is a servi	ce for agg	regating large a	mounts of log data			
Oozie	Oozie is a workt	flow sched	luler system for	managing Hadoop jobs.			
Mahout	Mahout is a set behavior.	of scalabl	e machine–lean	ning libraries that analyze user			
Spark	Spark is a proce	essing eng	ine for large dat	tasets.			
Sqoop	Sqoop is a tool databases.	for transfe	rring bulk data b	between Hadoop and relational			

1

Figure 88 MapR Services

Node Types

The MapR installer categorizes nodes as control nodes (which runs only cluster management services to manage the cluster), data nodes, control-as-data nodes (which combine the functions of control and data nodes), or client nodes. For deployment of MapR on Cisco UCS Integrated Infrastructure for Big Data, control services co-exist on data nodes (control-as-data node) as control services have a small footprint. Client node could be any node accessing the MapR cluster (all nodes in the MapR cluster are also client nodes).

F	igure 89	Node Types
	Node Type	Description
	Data node	Used for processing data, so they have the FileServer and TaskTracker services installed. If MapR–DB or HBase is run on a data node, the HBase Client service is also installed. Data nodes are used for running YARN applications and MapReduce jobs, and for storing file and table data. These nodes run the FileServer service along with NodeManager (for YARN nodes), TaskTracker (for MapReduce nodes), and HBase client (for MapR–DB and HBase nodes).
	Control– as–data node	Acts as both control and data nodes. They perform both functions and have both sets of services installed.
	Client node	Provides access to the cluster so the user can communicate via the command line or the MapR Control System. Client nodes provide access to each node on the cluster so the user can submit jobs and retrieve data. A client node can be an edge node of the cluster, laptop, or any Windows machine.

Node Types and Associated Services

The following table shows which services are assigned to each node type. When deploying MapR on Cisco UCS Integrated Infrastructure for Big Data, all Control Node services are deployed on Control–as–data node. There are no nodes running purely as control nodes as they also run data node services.

Node Type	YARN Main Services	Core MapR Services	Additional MRv1 Services	Additional HBase Service
Control- as-data node	ResourceManager (RM) HistoryServer (HS) NodeManager (NM)	CLDB ZooKeeper FileServer NFS Webserver FileServer	JobTracker (optional) TaskTracker (optional)	
Data node	NodeManager (NM)	FileServer	TaskTracker (optional)	
Client node			MapR Client	HBase Client (optional)

Figure 90 Services Assigned on Various Node Types

Hostnames and Roles

I

This section describes the cluster plan of a 64–node cluster with hostnames and roles assignments for the following services as shown in Figure 91 below.

- ResourceManager (RM)
- HistoryServer (HS)
- NodeManager (NM)
- TaskTracker (TT, optional)
- JobTracker (JT, optional), FileServer (FS)
- Container Location Database (CLDB)

- Zookeeper, and
- Webserver

Note Starting with MapR version 4.0, both Yarn and MapReduce V1 are supported not only in the same cluster but also on the same node.

Figure 91 Host names and Role Assignn	ient
---------------------------------------	------

Rack-1 Hostnames	MapR Roles	Rack–2 Hostnames	MapR Roles	Rack–3 Hostnames	MapR Roles	Rack-4 Hostnames	MapR Roles
rhei1	CLDB,FS, NM, NFS,HS	rhei17	CLDB, FS, NM, NFS, HS	rhei33	CLDB, FS, NM, NFS,HS	rhel49	FS, NM, NFS
rhel2	ZooKeeper	rhel18	ZooKeeper	rhel34	ZooKeeper	rhel50	FS, NM, NFS
meiz	FS, NM, NFS	merra	FS, NM, NFS	inei34	FS, NM, NFS	meloo	FO, NM, NFO
rhei3	Webserver,	rhei19	Webserver,	rhel35	Webserver,	rhel51	Webserver,
meia	FS, NM, NFS	meins	FS, NM, NFS	meioo	FS, NM, NFS	meion	FS, NM, NFS
rhel4	FS, NM, NFS	rhel20	FS, NM, NFS	rhel36	FS, NM, NFS	rhel52	FS, NM, NFS
rhel5	FS, NM, NFS, RM	rhel21	FS, NM, NFS, RM	rhel37	FS, NM, NFS, RM	rhel53	FS, NM, NFS
rhel6	FS, NM, NFS	rhel22	FS, NM, NFS	rhel38	FS, NM, NFS	rhel54	FS, NM, NFS
rhei7	FS, NM, NFS	rhei23	FS, NM, NFS	rhei39	FS, NM, NFS	rhel55	FS, NM, NFS
rhel8	FS, NM, NFS	rhel24	FS, NM, NFS	rhel40	FS, NM, NFS	rhel56	FS, NM, NFS
rhel9	FS, NM, NFS	rhel25	FS, NM, NFS	rhel41	FS, NM, NFS	rhel57	FS, NM, NFS
rhel10	FS, NM, NFS	rhel26	FS, NM, NFS	rhel42	FS, NM, NFS	rhel58	FS, NM, NFS
rhel11	FS, NM, NFS	rhel27	FS, NM, NFS	rhel43	FS, NM, NFS	rhel59	FS, NM, NFS
rhel12	FS, NM, NFS	rhel28	FS, NM, NFS	rhel44	FS, NM, NFS	rhel60	FS, NM, NFS
rhei13	FS, NM, NFS	rhei29	FS, NM, NFS	rhel45	FS, NM, NFS	rhel61	FS, NM, NFS
rhel14	FS, NM, NFS	rhel30	FS, NM, NFS	rhel46	FS, NM, NFS	rhel62	FS, NM, NFS
rhel15	FS, NM, NFS	rhel31	FS, NM, NFS	rhel47	FS, NM, NFS	rhel63	FS, NM, NFS
rhel16	FS, NM, NFS	rhel32	FS, NM, NFS	rhel48	FS, NM, NFS	rhel64	FS, NM, NFS

Note

All Job management are performed by Resource Manager and Node Manager. In this CVD, TaskTracker and JobTracker are not installed.

Preparing Packages and Repositories

A local repository on the admin node is set up to provide access to installation packages. With this method, the package manager on each node retrieves the installations package from the admin node (rhell is used as admin node as already mentioned) and installs the packages. Nodes do not need to have an Internet access.

Below are instructions on setting up a local repository for Red Hat Linux distribution. These instructions create a single repository that includes both MapR components and the Hadoop ecosystem components.

RPM Repositories for MapR Core Software

MapR hosts rpm repositories for installing the MapR core software using Linux package management tools. For every release of the core MapR software, a repository is created for each supported platform.

These platform-specific repositories are hosted at: http://package.mapr.com/releases/<version>/<platform>

http://package.mapr.com/releases/v4.1.0/redhat/mapr-v4.1.0GA.rpm.tgz

http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-ecosystem-20150503.rpm.tgz

RPM Repositories for Hadoop Ecosystem Tools

MapR hosts rpm repositories for installing Hadoop ecosystem tools, such as Spark, Flume, Hive, Mahout, Oozie, Pig and Sqoop. At any given time, MapR's recommended versions of ecosystem tools that work with the latest version of MapR core software are available in the link below.

These platform-specific repositories are hosted at: http://package.mapr.com/releases/ecosystem/<platform>

To create the local repositories follow the steps below:

- 1. Login as root on the admin node (rhel1).
- 2. Create the following directory on rhell

```
mkdir -p /var/www/html/mapr.local
```

3. On a node that is connected to the Internet, download the following files, substituting the appropriate <version> and <datestamp>:

```
wget
http://package.mapr.com/releases/v<version>/redhat/mapr-v<versi
on>GA.rpm.tgz
```

```
wget
http://package.mapr.com/releases/ecosystem/redhat/mapr-ecosystem-<datestamp>.rpm.t
qz
```



For this document we use the version 4.1.0. See MapR Repositories and Package Archives for the correct paths for all past releases at: http://archive.mapr.com/releases/

```
[root@internet-host ~]# wget
http://package.mapr.com/releases/v4.1.0/redhat/mapr-v4.1.0GA.rp
m.tgz
```

```
[root@internet-host ~]# wget
http://package.mapr.com/releases/ecosystem/redhat/mapr-ecosystem-20150420.rpm.tgz
```

```
Note
```

The server internet-host is an edge host that has access to the Internet and to the admin node (rhel1). It is not a part of the MapR cluster. It is only used to download and transfer files to the admin node from the Internet as the admin node is not directly connected to the Internet.

4. Copy the files to /var/www/html/mapr.local on the admin node, and extract them there.

```
[root@internet-host ~]# scp mapr-v4.1.0GA.rpm.tgz
rhel1:/var/www/html/mapr.local/
[root@internet-host ~]# scp mapr-ecosystem-20150420.rpm.tgz
rhel1:/var/www/html/mapr.local/
```

[root@rhel1 mapr.local]# tar -xvzf mapr-v4.1.0GA.rpm.tgz
[root@rhel1 mapr.local]# tar -xvzf
mapr-ecosystem-20150420.rpm.tgz

5. Create the base repository headers:

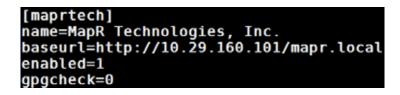
[root@rhel1 mapr.local]# createrepo /var/www/html/mapr.local

```
[root@rhell mapr.local]# createrepo /var/www/html/mapr.local
Spawning worker 0 with 128 pkgs
Workers Finished
Gathering worker results
Saving Primary metadata
Saving file lists metadata
Saving other metadata
Generating sqlite DBs
Sqlite DBs complete
```

To add the repository on each node follow the steps below:

6. Create repo file /etc/yum.repos.d/maprtech.repo on the admin node (rhell):

```
vi /etc/yum.repos.d/maprtech.repo
[maprtech]
name=MapR Technologies, Inc.
baseurl=http://10.29.160.101/mapr.local
enabled=1
gpgcheck=0
```



7. Copy the maprtech.repo specification to all the nodes of the cluster. Then, update the yum metadata cache so that the repository files will be properly accessed.

```
clush -a -c /etc/yum.repos.d/maprtech.repo
clush -a yum makecache
```

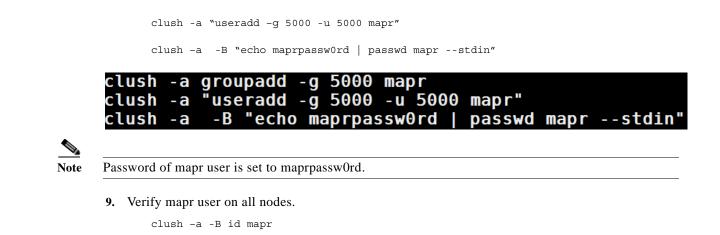
clush a -c /etc/yum.repos.d/maprtech.repo clush -a yum makecache

8. Create mapr user across all nodes

Users of the cluster must have the same credentials and uid on every node in the cluster. Each user (or department) that runs the MapR jobs needs an account and must belong to a common group (gid). If a directory service, such as LDAP, is not used, this user is created on each node. Every user must have the same uid and primary gid on every node.

In addition, a MapR user with full privileges to administer the cluster is created. If a user named 'mapr' does not exist. It is recommended that the user named 'mapr' is created in advance in order to test the connectivity issues prior to the installation step.

clush -a groupadd -g 5000 mapr



[root@rhel1 ~]# clush -a -B id mapr uid=5000(mapr) gid=5000(mapr) groups=5000(mapr)

MapR Software Installation

ſ

Perform the following steps on each node:

- 1. Install the planned MapR services as shown in Figure 92.
- 2. Run the configure.sh script to configure the node.
- 3. Format raw drives and partitions allocated to MapR using the disksetup script.

Figure 92 shows services and corresponding packages.

Service	Package
MapR core	mapr-core
Cluster location DB (CLDB)	mapr-cldb
History server	mapr-historyserver
ResourceManager and/or JobTracker	mapr-resourcemanager and/or mapr-jobtracker
MapR Control System	mapr-webserver
MapR File Server	mapr-fileserver
NFS	mapr-nfs
NodeManager and/or TaskTracker	mapr-nodemanager and/or mapr-tasktracker
ZooKeeper	mapr-zookeeper
Hadoop Ecosystem Components	Package
Drill	mapr-drill
Drill Spark	mapr-drill mapr-spark
Spark	mapr-spark
Spark Hive	mapr-spark mapr-hive
Spark Hive Mahout	mapr-spark mapr-hive mapr-mahout

Figure 92 MapR Services and Packages

Installing MapR packages

Based on the Cluster Plan for which services to run on which nodes, as shown in Table 8 above, use the commands in this section to install the appropriate packages for each node. Configuring the local yum repository ensures that the package dependencies will be managed correctly.

Installing CLDB

clush -B -w rhel[1,17,33] 'yum -y install mapr-cldb'

Installing ResourceManager

clush -B -w rhel[5,21,37] 'yum -y install mapr-resourcemanager'

Installing Mapr Webserver

clush -B -w rhel[3,19,35,51] 'yum -y install mapr-webserver'



Make sure httpd is not installed on these nodes.

Installing Mapr–Zookeeper

clush -B -w rhel[2,18,34] 'yum -y install mapr-zookeeper'

Installing NFS, Fileserver and Nodemanager on all cluster nodes

clush -B -a 'yum -y install mapr-fileserver mapr-nfs mapr-nodemanager'

clush	- B	- W	rhel[1,17,33] 'yum -y install mapr-cldb'
clush	- B	- W	rhel[5,21,37] 'yum -y install mapr-resourcemanager'
clush	- B	- W	rhel[3,19,35,51] 'yum -y install mapr-webserver'
clush	- B	- W	rhel[2,18,34] 'yum -y install mapr-zookeeper'
clush	- B	- a	'yum -y install mapr-fileserver mapr-nfs mapr-nodemanager'

Configure mapr-nfs

Run the following commands from the admin node (rhel1):

```
clush -a mkdir -p /mapr
echo "localhost:/mapr /mapr hard,nolock" > /opt/mapr/conf/mapr_fstab
clush -a -c /opt/mapr/conf/mapr_fstab --dest /opt/mapr/conf/mapr_fstab
```

```
clush -a mkdir -p /mapr
echo "localhost:/mapr /mapr hard,nolock" > /opt/mapr/conf/mapr_fstab
clush -a -c /opt/mapr/conf/mapr_fstab --dest /opt/mapr/conf/mapr_fstab
```

Verification

To verify that the software has been installed successfully, check the /opt/mapr/roles directory on each node. The software is installed in directory /opt/mapr and a file is created in /opt/mapr/roles for every service that installs successfully. Examine this directory to verify installation for the node. For example:

clush -a -B "ls -l /opt/mapr/roles"

Configure the Node with the configure.sh Script

A Configure the node first, then prepare raw disks and partitions with the disksetup command.

The script configure.sh configures a node to be part of a MapR cluster, or modifies services running on an existing node in the cluster. The script creates (or updates) configuration files related to the cluster and the services running on the node. Before performing this step, make sure to have a list of the hostnames of the CLDB and ZooKeeper nodes, Optionally specify the ports for the CLDB and ZooKeeper nodes as well. If not specified, the default ports are assigned as:

- CLDB 7222
- ZooKeeper 5181

The script configure.sh takes an optional cluster name and log file, and comma-separated lists of CLDB and ZooKeeper host names or IP addresses (and optionally ports), using the following syntax:

```
/opt/mapr/server/configure.sh -C <host>[:<port>][,<host>[:<port>]...] -Z
<host>[:<port>][,<host>[:<port>]...] [-L <logfile>][-N <cluster name>]
```

Configure All nodes with CLDB and Zookeeper locations

clush -B -a '/opt/mapr/server/configure.sh -C rhel1,rhel17,rhe33 -Z rhel2,rhel18,rhel34 -HS rhel1 -RM rhel5,rhel21,rhel37 -N ciscomapr -no-autostart'

clush -B -a '/opt/mapr/server/configure.sh -C rhel1,rhel17,rhe33 -Z rhel2,rhel18 ,rhel34 -∭S rhel1 -RM rhel5,rhel21,rhel37 -N ciscomapr -no-autostart'

Formatting Disks with the disksetup Script

If mapr-fileserver is installed on this node, use the following procedure to format disks and partitions to be used by MapR.

Contract Representation Representatio Representation Representation Representation Representa

The disksetup script is used to format disks to be used by the MapR cluster. Create a text file /tmp/MapR.disks listing the disks and partitions to be used by MapR on the node. Each line lists either a single disk or all applicable partitions on a single disk. When listing multiple partitions on a line, separate them by spaces.

Identify and format the data disks for MapR

• Create a list of disks to be formatted:

Create the following script on rhell and copy it to all the nodes:

```
vim mapr_disks.sh
```

```
#!/bin/bash
#This script creates file (MapR.disks) containing list of non-os disk #drives used
during MapR Installation
[[ "-x" == "${1}" ]] && set -x && set -v && shift 1
count=1
for HD in /sys/class/scsi_host/host?/scan
do
echo '- - - ' > \{HD\}
done
for HD in /dev/sd?
do
if [[ -b ${HD} && `/sbin/parted -s ${HD} print quit |/bin/grep -c boot` -ne 0
11
then
continue
else
echo $HD >> /tmp/MapR.disks
fi
done
```

Copy the scipt to nodes:

```
chmod +x mapr_disks.sh
clush -a -c mapr_disks.sh
clush -a -B /root/mapr_disks.sh
```

Verify the file on all nodes does not contain os drives:

clush -aB cat /tmp/MapR.disks

Confirm that the disks are not in use

The cfdisk, mount, and pvdisplay utilities can be used to confirm that the system is not using the disks listed in /tmp/MapR.disks. This confirmation is not necessary during the initial setup, but may be relevant when nodes are removed or re–added to the cluster. Format the disks to MapR-FS

```
clush -B -a '/opt/mapr/server/disksetup -F /tmp/MapR.disks'
```

Contraction of the second data from the specified disks. Make sure to specify the disks correctly, and that all data has been backed up elsewhere.

This procedure assumes free, un-mounted physical partitions or hard disks for use by MapR.

After successful installation of MapR software on each node according to the cluster plan, bring up the cluster.

Updating environment variables in /opt/mapr/conf/env.sh

There are a few key environment variables for the MapR software saved in /opt/mapr/conf/env.sh. These values must be properly configured BEFORE launching the cluster software. The default file is as shown below:

```
#!/bin/bash
# Copyright (c) 2009 & onwards. MapR Tech, Inc., All rights reserved
# Please set all environment variable you want to be used during MapR cluster
# runtime here.
# namely MAPR_HOME, JAVA_HOME, MAPR_SUBNETS
#export JAVA_HOME=
#export MAPR_SUBNETS=
#export MAPR HOME=
```

```
#export MAPR_ULIMIT_U=
#export MAPR_ULIMIT_N=
#export MAPR_SYSCTL_SOMAXCONN=
```

For this deployment, we need to explicitly set values for JAVA_HOME and MAPR_SUBNETS as shown below;

```
export JAVA_HOME=/usr/java/jdk1.7.0_75
export MAPR SUBNETS=192.168.11.0/24,192.168.12.0/24
```

```
<u>Note</u>
```

By mentioning MAPR_SUBNETS and providing the two vlans, this enables MapR to use both VLANs (NICs) for traffic and thus using full 20 GiGE for Hadoop traffic.

Make those changes in rhell:/opt/mapr/conf/env.sh and then distribute them to the entire cluster with the command

\$ clush -B -a -c /opt/mapr/conf/env.sh

Bringing Up the Cluster

The installation of software across a cluster of nodes will go more smoothly if the services have been pre-planned and each node has been validated. Referring to the cluster design developed in section "Planning the Cluster", ensure that each node has been prepared and that the MapR packages have been installed on each node in accordance with the plan. The process for launching the cluster can be broken down into several steps:

- Initialization Sequence
- Troubleshooting
- Installing the Cluster License
- Verifying Cluster Status
- Setting up a multi-tenancy MapR cluster

The initialization sequence involves starting the ZooKeeper service, starting the CLDB service, setting up the administrative user, and installing a MapR license. Once these initial steps are done, the cluster is functional on a limited set of nodes. Not all services are started yet, but the MapR Control System Dashboard, or the MapR Command Line Interface are available, to examine nodes and activity on the cluster.

Initialization Sequence

First, start the ZooKeeper service. It is important that all ZooKeeper instances start up, because the rest of the system cannot start unless a majority of ZooKeeper instances are up and running. Next, start the **warden** service on each node, or at least on the nodes that host the CLDB and webserver services. The warden service manages all MapR services on the node (except ZooKeeper) and helps coordinate communications. Starting the warden automatically starts the CLDB.

To bring up the cluster, follow these steps:

1. Start **ZooKeeper** on all nodes where it is installed, by issuing one of the following commands:

clush -B -w rhel[2,18,34] service mapr-zookeeper start

```
JMX enabled by default
Using config: /opt/mapr/zookeeper/zookeeper-3.4.5/conf/zoo.cfg
Starting zookeeper ... STARTED
```

2. Verify that the ZooKeeper service is running properly:

clush -B -w rhel[2,18,34] service mapr-zookeeper status

JMX enabled by default Using config: /opt/mapr/zookeeper/zookeeper-3.4.5/conf/zoo.cfg zookeeper running as process 1287.

The servers should display the running pid for the zookeeper process

3. On the nodes running CLDB or webserver, start the **warden** by issuing one of the following commands

clush -a service mapr-warden start

[root@rhell -]# clush -a service mapr-warden start rhel3.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log.
<pre>rhel3.mgmt: rhel3.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure services log files</pre>
rhel2.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log.
rhel2.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure services log files
rhell.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log. rhell.mgmt:
rhell.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure services log files
<pre>rhel4.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log. rhel4.mgmt:</pre>
<pre>rhel4.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure services log files</pre>
<pre>rhel8.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log. rhel8.mgmt: rhel8.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure</pre>
services log files rhel7.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log.
<pre>rhel7.mgmt: rhel7.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure</pre>
services log files rhel5.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log.
<pre>rhel5.mgmt: rhel5.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure</pre>
services log files rhel6.mgmt: Starting WARDEN, logging to /opt/mapr/logs/warden.log.
<pre>rhel6.mgmt: rhel6.mgmt: For diagnostics look at /opt/mapr/logs/ for createsystemvolumes.log, warden.log and configure services lon_files</pre>

Before continuing, wait 30 to 60 seconds for the warden to start the CLDB service. Calls to MapR (such as maprcli) may fail if executed before the CLDB has started successfully.

1. Log in to rhel1 and issue the following command to give full permission to the chosen administrative user mapr:

clush -B -w rhel1 /opt/mapr/bin/maprcli acl edit -type cluster -user mapr:fc

2. Confirm that the cluster is up before bringing up other nodes

clush -B -w rhel[17,33] 'hadoop fs -ls /'

[root@rhel1 Found 8 item		fs -ls /			
drwx	- devuser1	dev	Θ	2015-05-06	00:08 /DEV
drwx	- qauser1	qa	e	2015-05-05	22:30 /QA
drwxr-xr-x	- mapr	mapr			22:55 /apps
drwxr-xr-x	- mapr	mapr			22:55 /hbase
drwxr-xr-x	- mapr	mapr		2015-04-28	
drwxrwxrwx	- mapr	mapr		2015-05-05	
drwxr-xr-x	- mapr	mapr			22:55 /user
drwxr-xr-x	- m <u>a</u> pr	mapr	1	2015-04-28	22:55 /var

Troubleshooting

Difficulty bringing up the cluster seems daunting, but most cluster problems are easily resolved. For the latest support tips, visit http://answers.mapr.com.

- Can each node connect with the others? For a list of ports that must be open, see http://answers.mapr.com.
- Is the warden running on each node? On the node, run the following command as root:

\$ service mapr-warden status WARDEN running as process 18732 If the warden service is not running, check the warden log file, /opt/mapr/logs/warden.log, for clues.

To restart the warden service:

\$ service mapr-warden start

- The ZooKeeper service is not running on one or more nodes
 - Check the warden log file for errors related to resources, such as low memory
 - Check the warden log file for errors related to user permissions
 - Check for DNS and other connectivity issues between ZooKeeper nodes
- The MapR CLI program /opt/mapr/bin/maprcli won't run
 - Did you configure this node? See Installing MapR Software.
- Permission errors appear in the log
 - Check that MapR changes to the following files have not been overwritten by automated configuration management tools:

	Table 8	MapR Dependant Files
--	---------	----------------------

/etc/sudoers	Allows the mapr user to invoke commands as root
/etc/security/limits.conf	Allows MapR services to increase limits on resources such as memory, file handles, threads and processes, and maximum priority level
<pre>/etc/udev/rules.d/99-mapr-disk .rules</pre>	Covers permissions and ownership of raw disk devices

Before contacting Support, collect cluster's logs using the mapr-support-collect script.

Installing Cluster License



Contact MapR sales representative to obtain a valid MapR license key. This is necessary to enable the enterprise-class features of the MapR packages (eg MapR-DB, NFS, ResourceManager HA, storage snapshots and mirrors, etc.).

Using web-based MCS to install the license:

1. On a machine that is connected to the cluster and to the Internet, perform the following steps to open the MapR Control System and install the license:

2. In a browser, view the MapR Control System by navigating to the node that is running the MapR Control System. For example, rhel3.

https://<MCS node>:8443

The node won't have an HTTPS certificate yet, so the browser will warn that the connection is not trustworthy. Ignore the warning this time. The first time MapR starts, accept the Terms of Use and choose whether to enable the MapR Dial Home service.

3. Log in to the MapR Control System as the administrative user. Until a license is applied, the MapR Control System dashboard might show some nodes in the amber "degraded" state.



The nodes health will be in amber until the license is applied. Once the license is applied, the node health should come up as green.

•) •) • https://rhel3:8-	443/#disku	usage			∽ C 🚺 ~ Goo	gle	的众自专业	ł
	5		ame: ciscomapr		Logged in a	s mapr Blog Support Manage Licenses v. 4.1.0.3		-
Cluster MapR-FS	0.0	Overview						*
S NFS HA		П Туре	Accounting Entity	Disk Usage	Volume Count	Hard Quota	Advisory Quota	
Alarms System Settings		User	mapr	83 MB	34	none	none	
HBase Job Tracker CLDB ResourceManager JobHistoryServer Nagios								

Figure 93 MapR Control System

- 4. In the navigation pane of the MapR Control System, expand the System Settings Views group and click Manage Licenses to display the MapR License Management dialog.
 - a. Click Add Licenses via copy/paste and paste the license key.
 - **b.** If the cluster is already registered, the license is applied automatically. Otherwise, click **OK** to register the cluster on MapR.com and follow the instructions there.

I

Figure 94 MapR License Management Dialog

Current Lic	enses		Cluster ID:	919388449250260526
Name	Issued	Expires	Nodes	Delete
MapR Base Edition			unlimited	N/A
MapR M5 Trial Edition	Apr 8, 2015	May 8, 2015	unlimited	[X]
Base MapR POSIX	Issued	Expires		
Additional F			POSIX Client Nodes	Delete
Base MapR POSIX		100000		
Client for fast secure file access			10	N/A
Total			10	
Available nodes: unlin Maximum allowed no Add licenses via Web	odes: unlimited			
Add licenses via uplo	Vinanta			

Installing a license from the command line (optional)

Use the following steps if the cluster and the Internet are not accessible at the same time.

- 1. Obtain a valid license file from MapR
- 2. Copy the license file to a cluster node
- 3. Run the following command to add the license:

maprcli license add [-cluster <name>] -license <filename> -is_file true

Restarting MapR services after license installation

Certain HA features of the MapR cluster will not start properly until a valid license is installed. Once successfully installed the trial license or a permanent one provided by mapr, restart the distributed CLDB services, as well as the ResourceManager service and the NFS service. This can be done from any node in the cluster with the following commands:

```
maprcli node services -name cldb -action start -filter "[csvc==cldb]"
maprcli node services -name resourcemanager -action start -filter
    "[csvc==resourcemanager]"
    maprcli node services -name nfs -action start -filter "[csvc==nfs]"
maprcli node services name cldb action start filter "[csvc==cldb]"
maprcli node services name resourcemanager action start filter "[csvc==resourcemanager]"
maprcli node services name nfs action start filter "[csvc==resourcemanager]"
```

The effect of those commands is to start the respective services on all nodes in the cluster configured with those services. Nodes on which the service is already running will not be affected.

Managing Log Files

Over time, the log directories increase in size. For regular maintenance/compliance, it is a good practice to move the files in the directories mentioned below to different location either in the cluster (on one of the MapR Volumes) or to a different location for any compliance/audit requirements. This action could be setup as a cron job.

On each node, the two directories that contain the log files are:

/opt/mapr/hadoop/hadoop-0.20.2/logs /opt/mapr/hadoop/hadoop-2.5.1/logs

Verifying Cluster Status

Verify cluster status using the web interface:

- 1. Log in to the MapR Control System.
- 2. Under the Cluster group in the left pane, click Dashboard.
- 3. Check the **Services** pane and make sure each service is running the correct number of instances, according to the cluster plan.

Verify cluster status using the command line interface

- 1. Log in to a cluster node
- 2. Use the following command to list MapR services:

\$maprcli service list
\$maprcli license list
\$maprcli disk list -host <name or IP address>

iskname	powerstatus	status	vendor	hostname	modelnum	availablespace	storagepoolid	fstype	mount	firmwareversion
dev/sdal	running		Cisco	rhel3	UCSC-MRAID12G	3664		ext4	1	4.25
dev/sda2	running	.0	Cisco	rhel3	UCSC-MRAID126	1049359		ext4	1	4.25
dev/sda3	running	.0	Cisco	rhel3	UCSC-MRAID126			swap	0	4.25
dev/sdb	running	0	Cisco	rhel3	UCSC-MRAID12G	1143257	1	MapR-FS	. 0	4.25
dev/sdd	running	8	Cisco	rhel3	UCSC-MRAID126	1143257	1	MapR - FS	8	4.25
dev/sde	running	0	Cisco	rhel3	UCSC-MRAID126	1143249	2	MapR-FS	0	4.25
dev/sdc	running	8	Cisco	rhel3	UCSC-MRAID12G	1143257	1	MapR-FS	8	4.25
dev/sdf	running		Cisco	rhe13	UCSC-MRAID126	1143249	2	MapR-FS	0	4.25
dev/sdg	running	8	Cisco	rhe13	UCSC-MRAID126	1143249	2	HapR-FS	. 0	4.25

Installing Additional Hadoop Components

The final step in installing a MapR cluster is to install and bring up Hadoop ecosystem components such as the following and integrating them with a MapR cluster:

Please refer to MapR Install guide at http://doc.mapr.com/display/MapR/Ecosystem+Guide for detailed instructions on installation and configuration of Hadoop components.

- Apache Drill Installing and using Drill on a MapR cluster
- Cascading Installing and using Cascading on a MapR cluster
- Flume Installing and using Flume on a MapR cluster
- HBase Installing and using HBase on MapR
- Hive Installing and using Hive on a MapR cluster, and setting up a MySQL metastore

- Hue Installing and using Hue on MapR
- Impala Installing and using Impala on a MapR cluster
- Mahout Environment variable settings needed to run Mahout on MapR
- Oozie Installing and using Oozie on a MapR cluster
- Pig Installing and using Pig on a MapR cluster
- Spark and Shark Installing and running Spark and Shark on MapR
- Sqoop Installing and using Sqoop on a MapR cluster
- Storm (Version 0.9.3–1411) Installing and using Storm on a MapR cluster

Setting up a Multi-Tenancy MapR cluster

After installing the MapR core and any desired Hadoop components, perform the optional steps to prepare the cluster for production with Multi–Tenancy. Review the topics below for next steps that might apply to the cluster.

- Setting up Topology
- Setting up Volumes (with ownership, quota, replication factor, QoS etc)
- · Associate volumes with topologies
- Setting up ACL policies for volumes.
- Different Data placement policies for Different QoS with/without heterogeneous Servers based on SLA
- Different Replication Factor
- · Different Latencies for Data replication
- Access control (two different user groups can't or can access data between the groups through Access control)
- Job Placement (current consideration) with/without heterogeneous Servers based on SLA
- Administration and Reporting

Note

With Multi-Tenancy, the cluster could be a heterogeneous cluster with Cisco UCS C240 M4 with SFF (Small Form Factor) drives as in this CVD, Cisco UCS C240 M4 with LFF (Large Form Factor) drives and Cisco UCS C3160 (with 60 LFF drives). Based on the SLA requirements different servers can be part of the different tenants.

Creating user groups for Multi-Tenancy

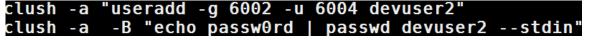
Here we provide an example to setup tenents (QA) and (DEV) and assign it to a two user groups. Tenets are separated from each other through a concept of "Volumes" which will be described in detail in the following sections. Users of the cluster must have the same credentials and uid on every node in the cluster. Each user (or department) that runs the MapR jobs needs an account and must belong to a common group (gid). If a directory service, such as LDAP, is not used, this user is created on each node. Every user must have the same uid and primary gid on every node.

1. Create qauser1 user across all nodes.

clush -a groupadd -g 6001 qa clush -a "useradd -g 6001 -u 6001 qauserl"

Password of qauser1 user is set to passw0rd.	
reate devuser1 user across all nodes	
clush -a groupadd -g 6002 dev	
clush -a "useradd -g 6002 -u 6002 devuser1"	
clush -a -B "echo passw0rd passwd devuser1stdi	in″
sh -a groupadd -g 6002 dev sh -a "useradd -g 6002 -u 6002 de sh -a -B "echo password passwo Password of devuser1 user is set to password.	evuser1"

clush -a -B "echo passw0rd | passwd devuser2 --stdin"





Password of devuser2 user is set to passw0rd.

Setting Up Topologies

Setting the physical topology of a MapR cluster node is done via the maprcli command

maprcli node move -serverids <ids> -topology <topology>

For this UCS deployment, we'll use the following simple script /root/set_topology on each node that allows the simple migration to a new topology

```
$cat /root/set_topology
#!/bin/bash
if [ -z ``${1}" ] ; then
    echo ``usage: $0 <topology>"
    exit 1
fi
hexid=`cat /opt/mapr/hostid`
myid=`printf ``%d````0x$hexid```
maprcli node move -serverids $myid -topology $1
```

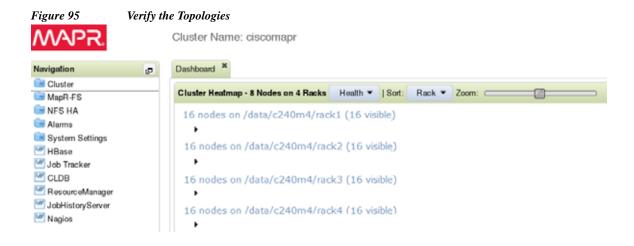
Save the above commands into a script file (set_topology) on the administrative node. Distribute it to all the other nodes in the cluster

```
$ chmod a+x /root/set_topology
$ clush -B -a -c /root/set_topology
```

Now that it is distributed, we can set the topology appropriately for 4 racks of C240M4 nodes:

\$ clush -B -w rhel[1-16] '/root/set_topology /data/c240m4/rack1'
\$ clush -B -w rhel[17-32] '/root/set_topology /data/c240m4/rack2'
\$ clush -B -w rhel[33-48] '/root/set_topology /data/c240m4/rack3'
\$ clush -B -w rhel[49-64] '/root/set_topology /data/c240m4/rack4'

Verify the topologies by logging into MapR Control System (MCS) through the browser https://rhel3:8443



Create and Associate Volumes to Topologies, setting QoS policies and Quota

Now we will create a volume named 'QA' associated with the '/data/c240m4/rack1' topology, have it mounted under path /QA in the root directory of MapR-FS, set replication factor as 2 (default 3) and minimum replication factor as 1 (default 2). Note that we can also assign quota to this volume, in our case, it is 1TB as hard limit and 800GB as soft limit. Also, the workload in this volume could be latency sensitive, we will use the low_latency QoS policy.

\$ maprcli volume create -nodelay 1 -type rw -advisoryquota 800G -minreplication 1 -quota 1000G -replication 2 -name QA -path /QA -topology /data/c240m4/rack1 -rootdirperms 700 -replicationtype low_latency -readonly 0 -user mapr:fc

Now we will create a volume named 'DEV' associated with the '/data/c240m4/rack2' topology, have it mounted under path /DEV in the root directory of MapR-FS, set replication factor as 3 and minimum replication factor as 2. Note that we can also assign quota to this volume, in our case, it is 2TB as hard limit and 1200GB as soft limit. Also, the workload in this volume could be throughput sensitive, we will use the high_throughput QoS policy.

\$ maprcli volume create -nodelay 1 -type rw -advisoryquota 1200G -minreplication 2 -quota 2000G -replication 3 -name DEV -path /DEV -topology /data/c240m4/rack2 -rootdirperms 700 -replicationtype high_throughput -readonly 0 -user mapr:fc

Parameter	Description					
Advisoryquota	The advisory quota for the volume as integer plus unit. Units: B, K, M, G, T, P					
Minreplication	The minimum replication level. Default: 2 When the replication factor falls below this minimum, re-replication occurs as aggressively as possible to restore the replication level. If any containers in the CLDB volume fall below the minimum replication factor, writes are disabled until aggressive re–replication restores the minimum level of replication.					
Name	The name of the volume to create.					
Path	The path at which to mount the volume.					
Quota	The quota for the volume as integer plus unit. Example: quota=500G; Units: B, K, M, G, T, P					
Readonly	Specifies whether or not the volume is read-only:					
	0 = Volume is read/write.					
	1 = Volume is read–only.					
Replication	The desired replication level. Default: 3 When the number of copies falls below the desired replication factor, but remains equal to or above the minimum replication factor, re-replication occurs after the timeout specified in the cldb.fs.mark.rereplicate.sec parameter.					
Replicationtype	The desired replication type. You can specify low_latency (star replication) or high_throughput (chain replication). The default setting is high_throughput.					
Rootdirperms	Permissions on the volume root directory.					
Topology	The rack path to the volume.					
Туре	The type of volume to create.					
	mirror – standard mirror (read-only) volume (promotable to standard read–write volume)					
	rw - standard (read-write) volume (convertible to standard mirror volume)					
	0 - standard (read-write) volume (for backward compatibility)					
	1 - non-convertible mirror (read-only) volume (for backward compatibility)					
User	Space-separated list of user:permission pairs.					

1

Verify the topologies by logging into MapR Control System (MCS) through browser https://rhel3:8443.

Figure 96		Verif	y the Top	pologies										
MapR - paconagr +														
Arrow mast hits and a										*# U *	÷		8 0.0 4	
MAPR	ç	luster h	lame: ciecom	up#						Linge	din la n	ner J. Biog. 1. Report 1 Managel James = 413.0		
Nevigelian c	1 1	diama *												
Maple-Ft		Oversee	• T File Mu	henourtad System Non	Volume Volu	ene Azzona 🐲	Antipi Cia	ar Wide provis	terary space is	10				
T MapR Tables		I MH	Vol Nema	Mount Path	Creator	Quete	Vol Size	Data Nor	Sines Size	Total Size	(Pepl.)	Physical Topology	Type	
Volumes		4	DOV	-DEV	rist.	2.78	none	10110	-	ture		terristoretrand	Dansberd Vol.	-
C Minur Voluniae		4	SA.	.cA	rpat	1000-048	none	noné	none	none	2	itsiaic(40m4/reckf	Standard Vol-	me
T Simplehors		4	10000	144	mapr	none	1019	7074	1078	tone		1001	Elandard Vol.	ine
Scholdum Sc														

Setting up ACL policies for volumes

ſ

To Change the ownership and permission of the /QA and /DEV directories perform the following commands:

\$ hadoop	fs	-chown	-R	qauser1 /QA
\$ hadoop	fs	-chgrp	-R	qa /QA
\$ hadoop	fs	-chmod	-R	700 /QA
\$ hadoop	fs	-chown	-R	devuser1 /DEV
\$ hadoop	fs	-chgrp	-R	dev /DEV
\$ hadoop	fs	-chmod	-R	700 /DEV

```
[root@rhel1 ~]# hadoop fs -chown -R qauser1 /QA
[root@rhel1 ~]# hadoop fs -chgrp -R qa /QA
[root@rhel1 ~]# hadoop fs -chmod -R 700 /QA
```

root@rhel1 ~]# hadoop fs -chown - R devuser1 /DEV [root@rhel1 # hadoop fs -chgrp dev /DEV R [root@rhel1]# hadoop fs -chgrp - R dev /DEV

Now we can issue a hadoop fs -ls / to verify read-write permissions.

\$ hadoop fs -ls /

[root@rhel1 - Found 8 item		fs -ls /				
drwx	- devuser1	dev	θ	2015-05-06	00:08	/DEV
drwx	- qauser1	qa	θ	2015-05-05	22:30	/QA
drwxr-xr-x	- mapr	mapr	e	2015-04-28	22:55	/apps
drwxr-xr-x	- mapr	mapr	θ	2015-04-28	22:55	/hbase
drwxr-xr-x	- mapr	mapr	θ	2015-04-28	22:55	/opt
drwxrwxrwx	- mapr	mapr	3	2015-05-05	22:05	/tmp
drwxr-xr-x	- mapr	mapr	Θ	2015-04-28	22:55	/user
drwxr-xr-x	- mapr	mapr	1	2015-04-28	22:55	/var

Alternatively, the volume is mounted through NFS and is available under /mapr/<cluster name> as a directory.

[root@rhel1 total 2	~	# ls -al	/map	r/(cisco	omap	or	
drwxr-xr-x	10	mapr	mapr	9	May	6	00:24	
dr-xr-xr-x	3	root	root	θ	May	6	00:25	
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	apps
d rwx	2	devuser1	dev	θ	May	6	00:0 8	DEV
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	hbase
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	opt
d rwx	2	qauser1	qa	θ	May	5	22:30	QA
drwxrwxrwx	3	mapr	mapr	3	May	5	22:θ5	tmp
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	user
drwxr-xr-x	3	ma <u>p</u> r	mapr	1	Apr	28	22:55	var

\$ ls -al /mapr/ciscomapr

Now the volume looks like a Unix directory chown command can be used to change its ACLs.

\$ chown -R devuser2:dev /mapr/ciscomapr/DEV

\$ chmod -R 750 /mapr/ciscomapr/DEV

\$ ls -al /mapr/ciscomapr/DEV

[root@rhel1	~	# chown ⊣	-R dev	/U	ser2	:dev	/map	r/ciscomapr/DEV
[root@rhel1	~	# chmod ⊦	-R 756	Э,	/mapi	r/ci	iscoma	pr/DEV
[root@rhel1	~	# ls -al	/map	r/(cisco	omap	or/	
total 2								
drwxr-xr-x	10	mapr	mapr	9	May	6	00:24	
dr-xr-xr-x	3	root	root	θ	May	6	00:39	
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	apps
drwxr-x	2	devuser2	dev	θ	May	6	00:08	DEV
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	hbase
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	opt
drwx	2	qauser1	qa	θ	May	5	22:30	QA
drwxrwxrwx	3	mapr	mapr	3	May	5	22:05	tmp
drwxr-xr-x	2	mapr	mapr	θ	Apr	28	22:55	user
drwxr-xr-x	3	ma <u>p</u> r	mapr	1	Apr	28	22:55	var

Job Placement

Assume a mixture of high and low processing power servers in the same cluster. Job placement allows users to submit important jobs that can only run on the high power servers to get fast turnaround time.

Follow these steps to set up Job Placement:

1. Edit /opt/mapr/hadoop/hadoop-2.5.1/etc/hadoop/yarn-site.xml on resource manager nodes. Add the following content between <configuration> and </configuration> tags.

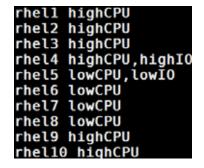
```
<property>
<name>node.labels.file</name>
<value>/tmp/label.txt</value>
<description>The path to the node labels file.</description>
</property>
<name>node.labels.monitor.interval</name>
```

<value>120000</value>

```
property>
<name>node.labels.file</name>
<value>/tmp/label.txt</value>
<description>The path to the node labels file.</description>
</property>
<name>node.labels.monitor.interval</name>
<value>l20000</value>
<description>Interval for checking the labels file for updates (default is 120000 ms)</description:
</property>
```

2. Create label.txt with following content

vi label.txt
rhel1 highCPU
rhel2 highCPU
rhel3 highCPU
rhel4 highCPU,highIO
rhel5 lowCPU,lowIO
rhel6 lowCPU
rhel7 lowCPU
rhel8 lowCPU
rhel9 highCPU
rhel10 highCPU
<upto>
rhel64 highCPU



3. Change permission of that file and copy to MapR–FS.

chmod 755 label.txt
cp label.txt /mapr/ciscomapr/tmp



4. Restart Resource manager

```
maprcli node services -name resourcemanager -action restart -filter
"[csvc==resourcemanager]"
```



5. Refresh Labels.

I

yarn rmadmin -refreshLabels

yarn rmadmin -refreshLabels

6. Verify the Labels.

yarn rmadmin -showLabels



7. Run a sample teragen jobs as two different users (qauser1 and devuser1):

As qauser1, submit the job to nodes labled as "highCPU" (i.e. rhel1 – rhel4):

```
yarn jar
/opt/mapr/hadoop/hadoop-2.5.1/share/hadoop/mapreduce/hadoop-mapreduce-examples-2.5
.1-mapr-1503.jar teragen -Dmapreduce.job.label=highCPU 1000000000 /QA/teragen
```

yarn jar /opt/mapr/hadoop/hadoop-2.5.1/share/hadoop/mapreduce/hadoop-mapreducexamples-2.5.1-mapr-1503.jar teragen -Dmapreduce.job.label=highCPU 100000000000 / A/teragen

Also on another console, run this command to show CPU utilization of the nodes:

while :; do maprcli node list -column cpu; sleep 1; done

The first horizontal screen displays CPU Utilization while the second displays the output of teragen. Observe the servers rhell through rhel4 have higher utilization.

4 rbsl2 192.168 8 rbsl3 192.168 8 rbsl3 192.168 1 rbsl4 192.168 1 rbsl5 192.168 1 rbsl5 192.168 1 rbsl6 192.168	.11.101,152.168.12.101 .11.102,152.168.12.102 .11.103,152.168.12.103 .11.104,152.168.12.104 .11.104,152.168.12.105 .11.104,152.168.12.105 .11.104,152.168.12.105 .11.104,152.168.12.107
Instead use the mapred command 15/65/65 22:20:50 IMFO client. Killed job job L48807607477.0 [qauserightell -15 m -rf /mip [qauserightell -15 yrm jar /or bel-highCPU -Dmapred mapr.task 15/65/65 22:21:13 IMFO client. 15/65/65 22:21:13 IMFO mapredu 15/65/65 22:21:13 IMFO mapredu 15/65/65 22:21:13 IMFO mapredu 15/65/65 22:21:13 IMFO mapredu 15/65/65 22:21:13 IMFO mapredu	HMProxy: Connecting to ResourceManager at rhel5/192.148.11.105:0022 002 r/cliscompr/QA/teragen/ pt/mapr/hadoop/hadoop.2.5.1/share/hadoop/mapreduce/hadoop-mapreduce-mismples-2.5.1-mapr-1583.jar teragen -Omepreduce.jol sil2 100000000000 (0/A/teragen RMProxy: Connecting to ResourceManager at rhel5/192.168.11.105:08032 t.TeraSort: Generating 100000000005 using 2 ce.JobSubmitter: Submit ing tokens for job: job_1430873871477_0003 y.ExternalTokenManagerFactory: Initialized external token manager class - com.mapr.hadoop.yarm.security.MapRTicketManager ce.JobSubmit Submitter in to track the job: http://rhel5.100031003 ce.Job: The url to track the job: http://rhel5.10003/

The same command does not work if devuser1 runs it due to ACL restriction.

[devuserlachell -]5 yarm jar /opt/mapr/hadoop/hadoop-2.5.1/share/hadoop/mapreduce/hadoop-mapreduce-maxmples-2.5.1-mapr-1503.jar teragem -Demapreduce.job.l
bel-hiptru 100000008 /0A/tersen
org.apache.hadoop.security.AccessControlException: User devuser1(user id 6002) does not have access to /0A/teragen
at com.mapr.fs.MapRFiloSystem.getMapRFileStatus(MapRFileSystem.java:1386)
at com.mapr.fs.MapRFileSystem.getFileStatus(MapRFileSystem.java:928)
at org.spache.hadoop.fs.FileSystem.exists(FileSystem.java:1434)
at org.apache.hadoop.examples.terasort.TeraGen.run(TeraGen.java:292)
at.org.apache.badoop.util.ToolRunner.run(ToolRunner.java:70)
at org.apache.badoop.examples.terasort.TeraGen.main(TeraGen.java;309)
at sum.reflect.NativeHethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeHethodAccessorImpl.invoke(NativeHethodAccessorImpl.java:57)
at sum.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:606)
at org.apache.badoop.util.ProgramDriverSProgramDescription_invoke(ProgramDriver.java:72)
at org.spache.hadoop.util.ProgramDriver.run(ProgramDriver.java:145)
at org.apache.hadoop.oxamples.ExampleOriver.main(ExampleOriver.java:90)
at sum.reflect.NativeHethodAccessorImpl.invoke0(Native Hethod)
at sum.reflect.NativeHethodAccessorImpl.invoke(NativeHethodAccessorImpl.java:57)
at sum.reflect.DelegatingHethodAccessorImpl.invoke(DelegatingHethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method java:606)
at org.apache.hadoop.util.RunJar.main(RunJar.java:212)

Administration and Reporting

I

Administration and Reporting From an administrative perspective, MapR allows organizations to define and enforce storage, CPU, and memory quotas at the volume, user, and group levels. For service providers to provide accurate usage and billing information, MapR

offers reporting on resource usage on over 60 different metrics. These metrics are available via the MapR Control System (MCS) browser-based user interface, and for up-stream integration—via the command–line interface and the REST API.

The following command demonstrates how to save above metrics in a log file in json format for later analysis:

while :; do maprcli node list -limit 50 -start 0 -json >> maprlog.json; sleep

10;	done
F	
[root@rnell	. −]# maprcli node list -limit 50 -start 0 -json
"ti "st	umestamp":1430971312393, umeofday":"2015-05-07 12:01:52.393 GMT-0400", atus":"0K", otal":8,
*da	ita":[
526C	£
	"id":"8865112475414864155",
	"ip":["192.168.11.101",
	"192.166.12.101" "192.166.12.101"
	1.
	"hostname":"rhell",
	"racktopo":"/data/c240m4/rack1/rhell",
	"health":0,
	"healthDesc":"Healthy",
	"service":"historyserver,nodemanager,cldb,fileserver,nfs,hoststats", "configuredservice":"historyserver,nodemanager,cldb,fileserver,nfs,hostst
ts",	
	"fs-heartbeat":0,
	"jt-heartbeat":2, "dtotal":3186.
	advat 1510,
	"dava1":3185,
	"rpcs":0,
	"rpcin":285,
	"rpcout":711,
	"disks":7,
	"MapRfs disks":3,
	"faileddisks":0,
	"dreads":0,
	"dreadK":0, "dwrites":0,
	"dwriteK":0,
	°cpus*16,



All the metrics are documented here: http://doc.mapr.com/display/MapR/node

The following figure shows all the performance metrics in the MapR Control System (MCS) at https://rhel3:8443/#nodes?path=/data/c240m4&report=performance

Figure 97	Performance	Metrics in	MapR	Controller	System

A https://rhel3.6443/enodes?path=/dsta/c240m4&report=performance										v tr∥ 📴 v Google					đ	1 ☆ 自	+ #	
MAPR.	Cluster Name	e: cis	scomap	r -									Log	god in as map N		Support - 20 v: 4.1.0.311		it.com Lo MapReckica (
Navigation (P	Dashboard M	Nodes	nod	io_rhel1 🕷														
Cluster R Dashboard	Performance •	0	Filter		an treas (). Norman	Formal Pro-												. de
R Nodes	Topology		Health	Hostname	Memory	Memory Total	Memory Used	% CPU	# CPUs	Disk Read	Disk Write	# Disk	# RPCs	RPC In	RPC Out	Bytes	# Disk	Bytes
🔁 Node Heatmap 🛱 Jobs	Cluster data			rhol7	17% of 252.2 GB	252.2 GB	41.8 GB	1%	16	Bytea	Bynama	Writes	1. Constanting	By244 B	ByBRF B	Ser985 B	Reads	Real-194
	c240m4			rhol5	17% of 252.2 GB	252.2 GB	41.8 GB	1%	16	none	none	+	÷.	214 B	607 B	1.2 KB		475 E
MapR-FS NFS HA	rack1 rack2			rhol4	17% of 252.2 GB	252.2 GB	41.8 GB	1%	16	none	none		3	136 B	375 B	1.1 KB	12	513 E
Alarms	rack3			rholt	37% of 252.2 GB	252.2 GB	93.5 GB	1%	16	none	none		10	136 B	326 B	1 KB	12	587 Ē
I System Settings I HBase I Job Tracker	rack4			rhal8	17% of 252.2 GB	252.2 GB	41.8 GB	1%	16	nona	none	1	1	1.1 KB	832 B	1.4 KB		656 B
	default-rack test			rhol3	30% of 252.2 GB		76.7 GB	1%	16	none	none	÷	1	333 B	1.4 KB	1.5 KB	- 9	1.2 K
	default-rack			rhel5	17% of 252.2 GB	252.2 GB	42 GB	1%	16	none	none		13	285 B	758 B	1.7 KB	12	2.7 K
CLDB				rhel2	30% of 252.2 GB	252.2 GB	76.7 GB	1%	16	none	80 KB	8		136 B	375 B	2.6 KB		5.7 K

Conclusion

Hadoop has evolved into a leading data management platform across all verticals. The Cisco UCS Integrated Infrastructure for Big Data with MapR and Multi–Tenancy offers a dependable deployment model for enterprise Hadoop that offers a fast and predictable path for businesses to unlock value in Big Data.

The configuration detailed in the document can be extended to clusters of various sizes depending on what application demands. Up to 80 servers (5 racks) can be supported with no additional switching in a single UCS domain with no network over–subscription. Scaling beyond 5 racks (80 servers) can be implemented by interconnecting multiple UCS domains using Nexus 6000/7000 Series switches, scalable to thousands of servers and to hundreds of petabytes storage, and managed from a single pane using UCS Central.

Bill of Materials

This section provides the BOM for 64 nodes Performance Optimized Cluster.

Part Number	Description	Quantity
UCS-SL-CPA3-P	Performance Optimized Cluster	1
UCSC-C240-M4SX	UCS C240 M4 SFF 24 HD w/o CPU, mem, HD, PCIe, PS, railkt w/expndr	16
UCSC-MRAID12G	Cisco 12G SAS Modular Raid Controller	16
UCSC-MRAID12G-2GB	Cisco 12Gbps SAS 2GB FBWC Cache module (Raid 0/1/5/6)	16

I

Table 10Bill of Materials for C240M4SX Base rack

Part Number	Description	Quantity
UCSC-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	16
CAB-9K12A-NA	Power Cord 125VAC 13A NEMA 5-15 Plug North America	32
UCSC-PSU2V2-1200W	1200W V2 AC Power Supply for 2U C-Series Servers	32
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	16
UCSC-HS-C240M4	Heat Sink for UCS C240 M4 Rack Server	32
UCSC-SCCBL240	Supercap cable 250mm	16
UCS-CPU-E52680D	2.50 GHz E5-2680 v3/120W 12C/30MB Cache/DDR4 2133MHz	32
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	256
UCS-HD12T10KS2-E	1.2 TB 6G SAS 10K rpm SFF HDD	384
UCS-SD120G0KSB-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD (BOOT)	32
UCSC-PCI-1C-240M4	Right PCI Riser Bd (Riser 1) 20nbd SATA bootdrvs+ 2PCI slts	16
UCS-FI-6296UP-UPG	UCS 6296UP 2RU Fabric Int/No PSU/48 UP/ 18p LIC	2
CON-SNTP-C240M4SX	SMARTNET 24X7X4 UCS C240 M4 SFF 24 HD w/o CPU, mem	16
CON-SNTP-FI6296UP	SMARTNET 24X7X4 UCS 6296UP 2RU Fabric Int/2 PSU/4 Fans	2
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	32
UCS-ACC-6296UP	UCS 6296UP Chassis Accessory Kit	2
UCS-PSU-6296UP-AC	UCS 6296UP Power Supply/100-240VAC	4
N10-MGT012	UCS Manager v2.2	2
UCS-L-6200-10G-C	2rd Gen FI License to connect C-direct only	70
UCS-BLKE-6200	UCS 6200 Series Expansion Module Blank	6
UCS 6296UP Fan Module	UCS 6296UP Fan Module	8
CAB-9K12A-NA	Power Cord 125VAC 13A NEMA 5-15 Plug North America	4
UCS-FI-E16UP	UCS 6200 16-port Expansion module/16 UP/ 8p LIC	4
RACK-UCS2	Cisco R42610 standard rack w/side panels	1
CON-OS-R42610	ONSITE 8X5XNBD Cisco R42610 expansion rack no side panel	1

Table 10Bill of Materials for C240M4SX Base rack

L

Γ

Part Number	Description Quanti
RP208-30-1P-U-2=	Cisco RP208-30-U-2 Single Phase PDU 20x C13 2 4x C19 (Country Specific) 2
CON-OS-RPDUX	ONSITE 8X5XNBD Cisco RP208-30-U-X Single 2 Phase PDU 2x

Table 10Bill of Materials for C240M4SX Base rack

Part Number Description Quantity UCSC-C240-M4SX UCS C240 M4 SFF 24 HD w/o CPU, mem, HD, 48 PCIe, PS, railkt w/expndr UCSC-MRAID12G Cisco 12G SAS Modular Raid Controller 48 UCSC-MRAID12G-2GB Cisco 12Gbps SAS 2GB FBWC Cache module 48 (Raid 0/1/5/6) UCSC-MLOM-CSC-02 Cisco UCS VIC1227 VIC MLOM - Dual Port 48 10Gb SFP+ Power Cord 125VAC 13A NEMA 5-15 Plug 96 CAB-9K12A-NA North America UCSC-PSU2V2-1200W 1200W V2 AC Power Supply for 2U C-Series 96 Servers UCSC-RAILB-M4 Ball Bearing Rail Kit for C220 M4 and C240 M4 48 rack servers UCSC-HS-C240M4 Heat Sink for UCS C240 M4 Rack Server 48 UCSC-SCCBL240 48 Supercap cable 250mm 96 UCS-CPU-E52680D 2.50 GHz E5-2680 v3/120W 12C/30MB Cache/DDR4 2133MHz UCS-MR-1X162RU-A 16GB DDR4-2133-MHz 768 RDIMM/PC4-17000/dual rank/x4/1.2v UCS-HD12T10KS2-E 1.2 TB 6G SAS 10K rpm SFF HDD 1152 UCS-SD120G0KSB-EV 120 GB 2.5 inch Enterprise Value 6G SATA SSD 96 (BOOT) UCSC-PCI-1C-240M4 Right PCI Riser Bd (Riser 1) 20nbd SATA 48 bootdrvs+ 2PCI slts SFP-H10GB-CU3M= 10GBASE-CU SFP+ Cable 3 Meter 96 CON-SNTP-C240M4SX SMARTNET 24X7X4 UCS C240 M4 SFF 24 HD 48 w/o CPU, mem RACK-UCS2 3 Cisco R42610 standard rack w/side panels CON-OS-R42610 ONSITE 8X5XNBD Cisco R42610 expansion 3 rack no side panel

Table 11Bill of Materials for Expansion Racks

Part Number	Description	Quantity
RP208-30-1P-U-2=	Cisco RP208-30-U-2 Single Phase PDU 20x C13 4x C19 (Country Specific)	6
CON-OS-RPDUX	ONSITE 8X5XNBD Cisco RP208-30-U-X Single Phase PDU 2x	3

Table 12R

Red Hat Enterprise Linux License

Bill of Materials for MapR Software

Red Hat Enterprise Linux							
RHEL-2S-1G-3A	Red Hat Enterprise Linux	64					
CON-ISV1-RH2S1G3A	3 year Support for Red Hat Enterprise Linux	64					
CON-15 V 1-KH25103A	5 year Support for Ked Hat Enterprise Linux	04					



Choose one of the part numbers.

Table 13

Part Number	Description	Quantity
UCS-BD-M5-SL=	MapR M5 EDITION	64
UCS-BD-M7-SL=	MapR M7 EDITION	64

Appendix

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 98) 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

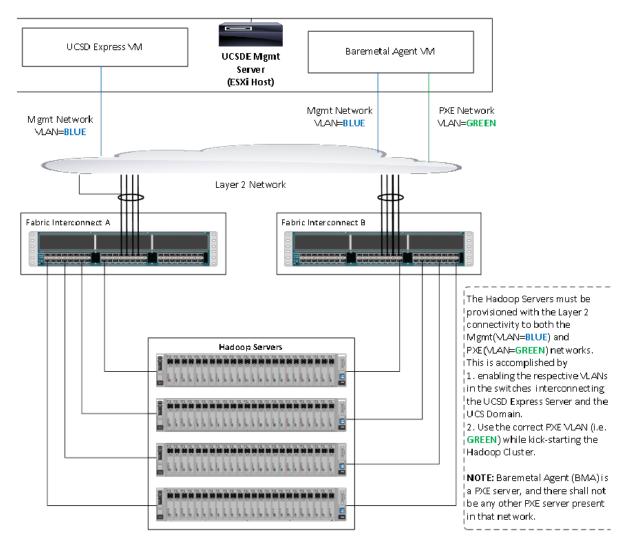
- Faster and Easier Big Data Infrastructure Deployment: Cisco UCS Director Express for Big Data extends the Cisco UCS Integrated Infrastructure for Big Data with one-click provisioning, installation, and configuration, delivering a consistent, repeatable, flexible, and reliable end-to-end Hadoop deployment.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

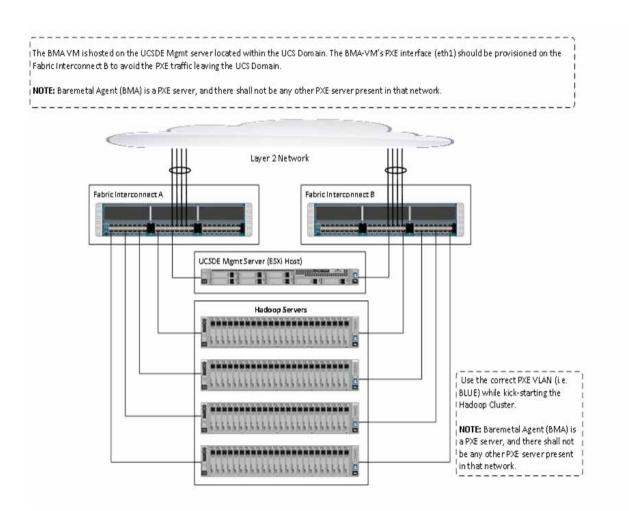


ſ

Figure 98 UCSD Express Management Server that lives outside 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.

Figure 99 UCSD Express Management Server that is being managed as part of the same UCS Domain

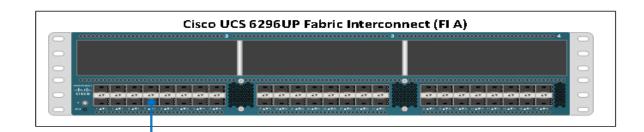


UCSD Management Server Cabling

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 100. The ports on the on the Fabric Interconnects must be configured as server ports.

Figure 100 Fabric Topology for C220 M4



Cisco UCS 6296UP Fabric Interconnect (FI B)
ц.
Cisco UCS C220 M4 Rack Server

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 . See Software Distributions and Versions. In addition, the following software distributions are necessary.

UCS Director Express for Big Data (1.1)

For more information visit

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director-express-big-data-1-1/mo del.html

VMware vSphere 5.5

UCS Director express requires the VMware vSphere 5.5 hypervisor. For more information see 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 14

UCSD Express Management Server vNIC configurations

VLAN	Fabric	NIC Port	Function	Failover
default(VLAN1)	А	eth0	Management, User connectivity	Fabric Failover to B
vlan85_PXE	В	eth1	PXE	Fabric Failover to A

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 cisco validated design.



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.

1

Creating Service Profile from the Template

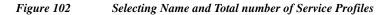
Select the Servers tab in the left pane of the UCS Manager GUI.

- 1. Go to Service Profile **Templates > root**.
- 2. Right-click Service Profile Templates ESXi_Host.
- 3. Select Create Service Profiles From Template.

Fault Summary	▲ ▲ ♀ ●	🖸 New - 🔄 Options 🛛 😧 🌒 📥 Pending Activities 🔤 Exit	-di-di- cisco
1 14		iervice Profile Templates + 🙏 root + 🌃 Service Template ESIQ_Host	Service Template ESI _Host
Equipment Servers LAN SAN V	M Admin General	Storage Network ISCSI vHICs Boot Order Policies Events PSM	
Equipment Services LAN SAN Y Filter: Service Profile Service Profile Templates Service Template RP Service Template RP	Templa Action Templa Action Action A	ns Create Service Profiles From Template Create a Clone Ver Pool Ver Pool Ce Policy Int IP Address Typercition	0 0 0
	Change Serial over LAN Policy Modify vNBC/vHBA Placement		
	Сору Сору XML	Chri+C Chri+L	
	Delete	Ctri+D	Save Changes Reset Values

Figure 101 Creating Service Profiles from Template

4. The Create Service Profile from Template window appears.



🚔 Create Service Profiles From Template	×
Create Service Profiles From Template	0
Naming Profix: ESXI Name Suffix Starting Number: 1 Number of Instances: 1	
OK	Cancel

Association of the Service Profiles will take place automatically.

Installing VMware vSphere ESXi 5.5

I

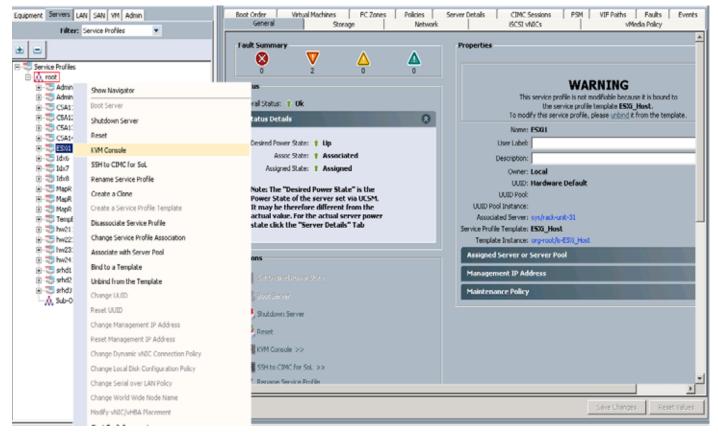
The following section provides detailed procedures for installing VMware vSphere ESXi 5.5.

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.

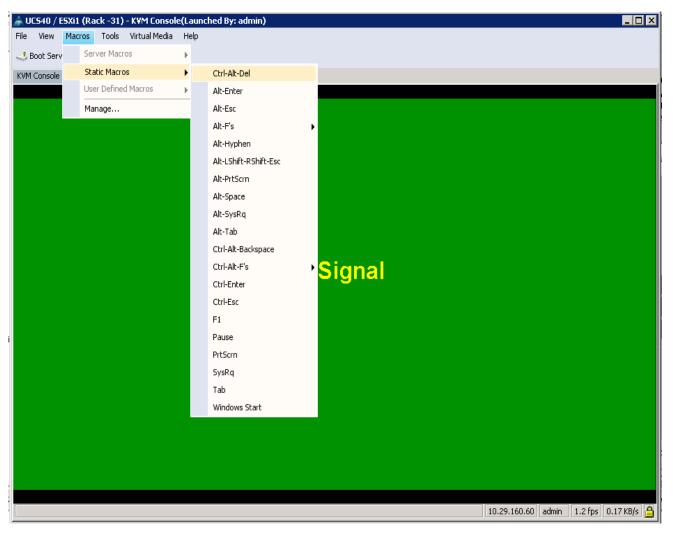
1. Log in to the Cisco UCS 6296 Fabric Interconnect and launch the Cisco UCS Manager application.

- 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 103 Selecting KVM Console



5. In the KVM window, force a reboot by executing the Ctrl-Alt-Del macro.



I

Figure 104 Sending Ctrl-Alt-Del to Reset the Server

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.

Tigure 105 Rynn minuow displaying the Lot meganeme on one-min biob screet	Figure 105	KVM Window displaying the LSI MegaRAID SAS-MFI BIOS screen
---	------------	--

1

	Macros Tools Virt	M Console(Launched By: admin) ual Media Help			
Boot Serve	er 🛛 🛃 Shutdown Serv	ver 🤐 Reset			
KVM Console					
	Properties				
	gaRAID SAS				
		0 (Build May 07, 2014) 4 LSI Corporation			
oopgri	gnetter Loi				
		0) Cisco 12G SAS Modular Ra	id Controller		
		Fully charged			
PCI SI	ot Number:	0			
ID LUN	VENDOR	PRODUCT	REVISION	CAPACITY	
		Cisco 12G SAS Modular Raid		2048MB	
20 0 21 0	SEAGATE SEAGATE	ST9146803SS ST9146803SS	0004 0004	140014MB 140014MB	
	TOSHIBA	MBF2300RC	5704	286102 M B	
23 0	ATA	Micron_M500_MTFD	MU03	114473MB	
		on the host adapter			
0 JROD	(s) handle	a by Blus			
0 Virt	ual Drive(s) found on the host adapter			
	0 Virtual Drive(s) handled by BIOS				
Press	Press <ctrl><r> to Run MegaRAID Configuration Utility</r></ctrl>				
			10.29.160.6	60 admin 0.4 fps 0.001 KB/s 🔒	

- 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.

Cisco 12G SAS Modular Raid Controller BIOS Conf	iguration Utility 5.06-0004
VD Mgmt PD Mgmt Ctrl Mgmt Properties	
Virtual Drive Managemen	
[-] Cisco 12G SAS Modular Rai (Bus 0x09, Dev 0x00 −[-] Drive Group: 0, RAID 5	Create Virtual Drive
<pre>-[-] Virtual Drives L ID: 0, 271.94 GB[+] Drives</pre>	Clear Configuration
-[+] Available size: 0.00 KB - Hot spare drives	Foreign Config
└─[-] Drive Group: 1, RAID 0 └─[-] Virtual Drives	Manage Preserved Cache
└── ID: 1, 110.82 GB ─[+] Drives	Drive Security
-[+] Available size: 0.00 KB 	Disable Data Protection
	Advanced Software Options
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page	Ctal P Prou Page F12 Ct la
ri-nerp re-operations ro-herresh ctri-n-next rage	CULT-I-TEV Taye LIZ-CULL

L

Γ

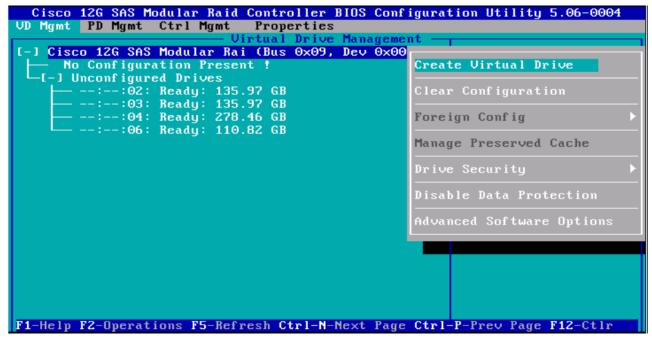
10. To the question Are you sure you want to clear the configuration? click **YES** and press **ENTER** key.



11. In the VD Mgmt section, use the arrow keys to select the Cisco 12G SAS Modular RAID (Bus 0xNN, Dev 0xNN) line item.

1

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.

Cisco 126 SAS Modular Raid Controller BIOS Configuration Utility 5.06-0004
UD Mgmt PD Mgmt Ctrl Mgmt Properties
Uirtual Drive Management
Create New VD
RAID Level: RAID-5 PD per Span : NZA Drives
Secure VD: No ID Type Size # [X]:-:02 135.97 GB 00 [X]:-:03 135.97 GB 01
Data Protection: Disable IX3::04 278.46 GB 02 I]::06 FDE 110.82 GB
Basic Settings Size: 271.945 GB Advanced OK CANCEL
Name :
F1-Help F12-Ctlr

- 15. Select the Advanced button, and Check the Initialize checkbox.
- 16. Press OK to continue with initialization.

I



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

Cisco 12G SAS Modular Raid Controller BIOS Configura	tion Utility 5.06-0004
UD Mgmt PD Mgmt Ctrl Mgmt Properties	
Uirtual Drive Management — [-] Cisco 12G SAS Modular Rai (Bus 0x09, Dev 0x00) —[-] Drive Group: 0, RAID 5 —[-] Virtual Drives — [D: 0, 271.94 GB	Virtual Drive O: State: Optimal RAID Level: 5
<pre>(+) Drives (+) Availab Hot spare (-) Unconfigur::06: OK</pre>	Stoup 0: 1 Drives: 1 : 3 ap.: 0.00 KB reas: 0
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl	-P-Prey Page F12-Ctlr

- 18. Press Ctrl-N twice to navigate to the Ctrl Mgmt screen.
- 19. Select Boot device field and press ENTER.

Cisco 12G SAS Modular Raid Controller BIOS	S Configuration Utility 5.06-0004
UD Mgmt PD Mgmt Ctrl Mgmt Properties	
Controller Set	ttings
Alarm Control — Coercion Mode: I	BIOS Mode: Boot device:
Enable Silence 1GB	Ignore err UD 0 271.94 GB
Rebuild Rate: 30 Patrol Rate : 30	0 [] Maintain PD Fail History
BGI Rate : 30 Cache flush Interval: 4	[X] Enable controller BIOS
CC Rate : 30 Spinup delay : 12	E] Enable Stop CC on Error
Recon. Rate : 30 Spinup drive : 2	[X] Auto Enhanced Import
	[] Enable JBOD
Set Factory Defaults APPLY	CANCEL < Next >
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-	Prev Page F12-Ctlr Ctrl-S-Save

- 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.

Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility 5.06-0004
VD Mgmt PD Mgmt Ctrl Mgmt Properties
Controller Settings
Alarm Control — Coercion Mode: BIOS Mode: Boot device:
Enable Silence 16B Ignore err UD 0 271.94 GB
Are you sure you want to exit?
Rebuild Rate: 30 PD Fail History
BGI Rate : 30 ontroller BIOS
CC Rate : 30 OK Cancel top CC on Error
Recon. Rate : 30 anced Import
[] Enable JBOD
Set Factory Defaults APPLY CANCEL < Next >
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr Ctrl-S-Save

23. In the KVM window, select the Virtual Media menu.

Γ

24. Click the Activate Virtual Devices found in the right hand corner of the Virtual Media selection menu.

A C240M4 / ucs1 (Rack -1) - KVM Cc	onsole(Launched By: admin)				X
File View Macros Tools Virtual N					
Shutdown Se Crea	ate Image				
KVM Console Properties Acti	ivate Virtual Devices				
	No Signa	10.29.160.89	admin 1	4 fps 0.25	11 KB/S
B Connected to IP: 10.29.160.89					System T

25. In the KVM window, select the Virtual Media menu and Select Map CD/DVD.

1

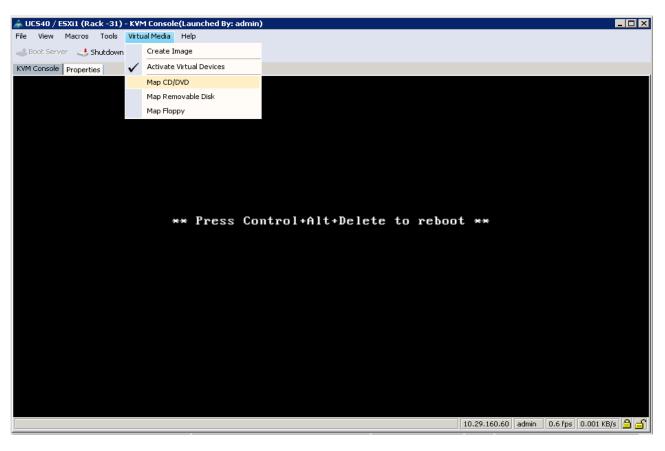


Figure 106 Mapping the CD/DVD Virtual Media

26. Browse to the VMware vSphere ESXi 5.5 installer ISO image file.



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

ſ

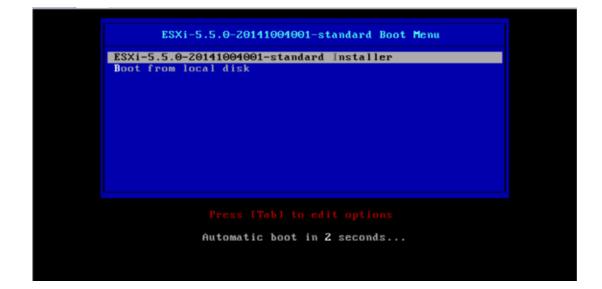
📥 Open						×
Look in:	<u> I</u> mages			- 6	• 🖻 🏷	
Recent Items Desktop My Documents Computer	RHEL6.5-2	0130130.0-5erver- 0131111.0-5erver- r-7.0-x86_64-dvd.i:	x86_64-DVD1.iso	i6_64.iso		
	File name:	Mware-VMvisor-In	nstaller-201410001-2	2143827.×86	_64.iso	Open
Network	Files of type:	Disk iso file (*.iso)			•	Cancel

Figure 107 Browse to VMWare ESXi Hypervisor ISO Image

- 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 108 ESXi Standard Boot Menu



32. Select the ESXi-5.5.0-yyyymmddnnnn-standard Installer. The installer begins automatically.

	Loading ESXi installer
Loading /net_nlx4.v01 Loading /net_nx_n.v00	
,, , ,, , ,	

Figure 109 Loading the ESXi Installer

I

ſ





33. Press ENTER to continue.

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

1

Figure 111 Accept End User License Agreement (EULA)

End User License Agreement (EULA)
VMNARE END USER LICENSE AGREEMENT
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTHARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTHARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTHARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT
Use the arrow keys to scroll the EULA text
(ESC) Do not Accept (F11) Accept and Continue

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

Figure 112 Selecting the Storage Device for installing the ESXi operating system.

Select a Disk to Install or Upgrade * Contains a VMFS partition # Claimed by VMware Virtual SAN (VSAN)				
Storage Device	Capacity			
Local: Cisco UCSC-MRAID126 (noo.670da6e715b126a01c9be Remote: (none)) 271.95 GiB			
(Esc) Cancel (F1) Details (F5) Refresh (Enter)	Cont inve			

36. Select the Keyboard US Default. Press ENTER to continue.

Figure 113 Choose the Keyboard layout

Please select a keyboard layout
Suiss French Suiss German Turkish Us Default US Dvorak Ukrainian United Kingdom
Use the arrow keys to scroll.
(Esc) Cancel (F9) Back (Enter) Continue

37. Choose the root password and confirm it. Press ENTER to continue.

Figure 114 Choose the root password

En	ter a root pa	ssword	_
Root password: Confirm password:			
	Passwords nat		
(Esc) Cancel		(Enter) Continue	

38. Press F11 to confirm and begin installation.

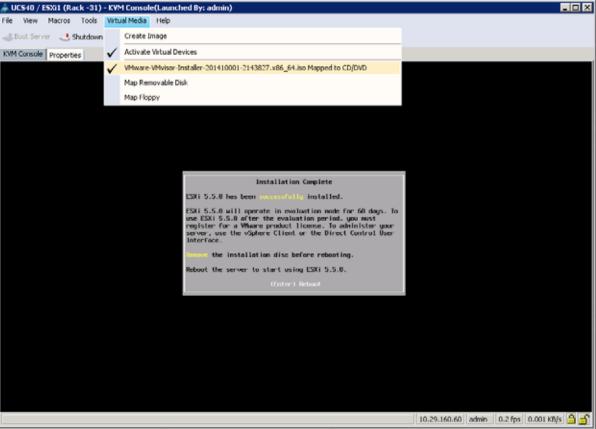
ſ

- **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.

Figure 115



ESXi installation complete – Unmount the Virtual Media



- 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.

Figure 116 VMWare ESXi initial screen as seen via the KVM Console

VMнаге ESXi 5.5.0 (VMKernel Release Build 2143827)	
Cisco Systems Inc UCSC-C220-M4S	
2 x Intel(R) Xeon(R) CPU E5-2623 v3 @ 3.00GHz 256 GiB Memory	
Download tools to manage this host from: http://0.0.0.0/ http://Ife80::225:b5ff:feae:9f]/ (STATIC)	
<f2></f2> Custonize System/View Logs	(F12) Shut Down/Restart

3. Press F2 to continue

Γ

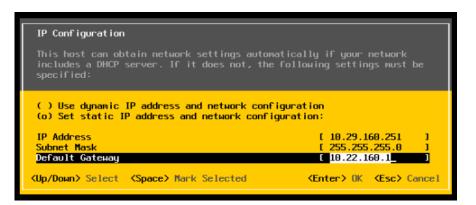
- 4. Select Configure Management Network, and press ENTER.
- 5. Select IP Configuration option.

Figure 117 Enter the IP configuration option of the Management Network

Configure Management Network	IP Configuration
Network Adapters VLAN (optional) IPv6 Configuration DNS Configuration Custon DNS Suffixes	Autonatic IP Address: 169.254.63.159 Subnet Mask: 255.255.0.0 Default Gateway: Not set This host can obtain an IP address and other networking parameters automatically if your network includes a DHCP server. If not, ask your network administrator for the appropriate settings.
<up down=""> Select</up>	⟨Enter⟩ Change ⟨Esc⟩ Exit

- 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.

Figure 118 Enter the IP Address configuration details



- 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.

Configure Management Network System Customization Configure Password Hostname: localhost Configure Lockdown Mode Configure Management Network IP Address: 10.29.160.251 tart Management Networ Test Management Network IPv6 Addresses: fe80::225:b5ff:feae:9f/64 Network Restore Options Configure Keyboard Troubleshooting Options View System Logs View Support Information Reset System Configuration <Enter> More

Figure 119 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 120 Accessing the ESXi web interface

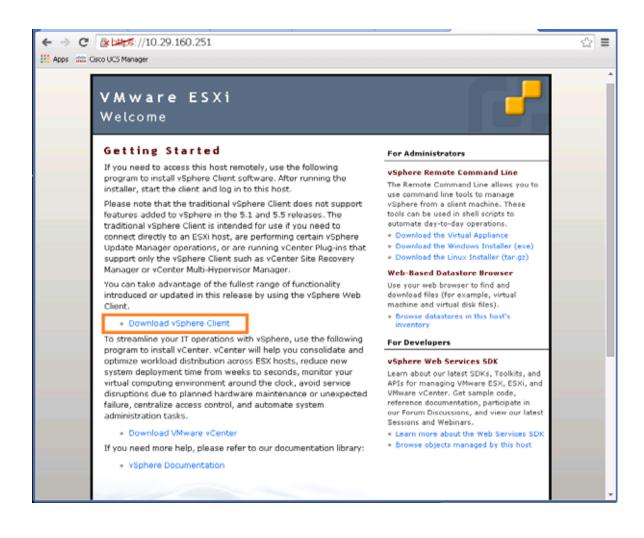


Figure 121

Download the VMWare vSphere ESXI client software



VMware-viclient-all-5.5.0-1993072.exe

http://vsphereclient.vmware.com/vsphereclient/1/9/9/3/0/7/2/VMware-viclient-all-5.5.0-199... Show in folder Remove from list

3. Proceed to install the downloaded VMWare client software.

Figure 122 Installing the vSphere Client software

🙀 VMware vSphere Client 5.	
vmware	Welcome to the installation wizard for VMware vSphere Client 5.5
	The installation wizard will allow you to remove VMware vSphere Client 5.5. To continue, click Next.
VMware vSphere® Client [™]	
	Next > Cancel

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.

Γ

Figure 123

🚱 ¥Mware vSphere Client	X			
vmware [.] VMware vSphere ^{**} Client	<u> </u>			
 In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5. The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager). To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server. 				
IP address / <u>N</u> ame: User name: <u>P</u> assword:	10.29.160.251			
	Use Windows session credentials			

Logging into the ESXi using vSphere Client

- 4. In the vSphere Client, click on the Configuration tab on the right, and within the Hardware section, click on Networking.

1

5. Click on Add Networking link on the upper right hand side.

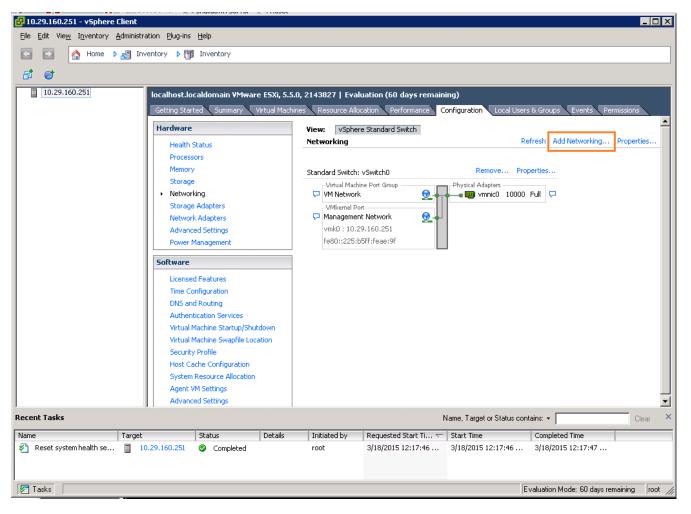


Figure 124 vSphere Client Networking screen

ſ

6. In the Add Networking dialog box, click the Virtual Machine radio button and click Next.

Figure 125 Adding a new Virtual Machine Network

🚱 Add Network Wizard		_ 🗆 X
Connection Type Networking hardware can l	be partitioned to accommodate each service that requires connectivity.	
Connection Type Network Access Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.	
Help	<back next=""></back>	Cancel

7. Click the **Create a vSphere standard switch** radio button and make sure that the checkbox next to vmnic1 is checked.

1

8. Click Next.

Figure 126 Creating a new vSphere Standard Switch

I

Γ

🛃 Add Network Wizard				
Virtual Machines - Network Virtual machines reach net	t Access works through uplink adapters attached to vSph	ere standard swit	tches.	
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed ne			eate a new
Connection Settings Summary	Create a vSphere standard switch Cisco Systems Inc Cisco VIC Ethern	Speed et NIC	Networks	
	Vmnic1	10000 Full	None	
	C Use vSwitch0 Cisco Systems Inc Cisco VIC Ethern	Speed	Networks	
	vmnic0	10000 Full	10.29.160.1-10.29.160.254	
	Providence -			
	Preview: Virtual Machine Port Group VM Network 2	Physical Adapters		
Help			< Back Next >	Cancel

- 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.

Elauna 127	Creating the Port Group	for the DVE VIAN
Figure 127	Creating the Fort Group	JOI THE I AL VLAN

🗿 Add Network Wizard				
Virtual Machines - Conne Use network labels to ic	ection Settings lentify migration compatible connect	ions common to two or more hosts.		
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional):	PXE_VLAN85 None (0)		
	Preview: Virtual Machine Port Group - PXE_VLAN85	Physical Adapters		
Help			< Back Next >	Cancel

1

12. Click **Finish** to complete adding the Network.

Figure 128 Verify the Created vSphere Standard Switches

I

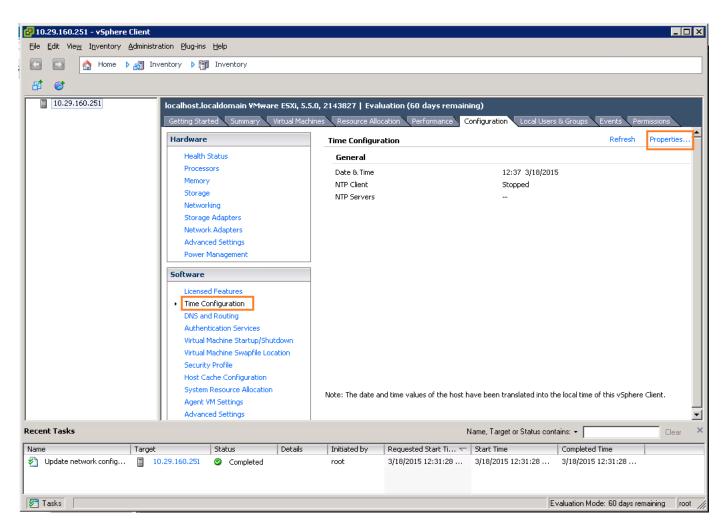
Γ

🛃 Add Network Wizard	
Ready to Complete Verify that all new and mo	dified vSphere standard switches are configured appropriately.
Connection Type Network Access Connection Settings Summary	Host networking will include the following new and modified standard switches: Preview: Virtual Machine Port Group Physical Adapters PXE_VLAN85 Output Pixe_vLaN85 Output Pixe_vLaN85
Help	< Back Finish Cancel

13. Click on the Time Configuration under the Software section.

14. Click on Properties at the upper right hand corner.

Figure 129 Enabling the NTP Client on th
--



- 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.

NTP Daemon (ntpd) Op General NTP Settings	Status Stopped Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually Service Commands Start Stop Restart
	OK Cancel <u>H</u> elp

- 18. Click on NTP Settings option.
- 19. Click on Add button to add the NTP server's IP address.
- 20. Press OK to continue.

Γ

Figure 131 Adding a new NTP Server to the ESXi NTP Settings

🛃 NTP Daemon (ntpd) Op	tions	X
General NTP Settings	NTP Servers NTP Server NTP Server Address: 10.29.160.100 OK Cancel	1
	Add Edit Remove	
	OK Cancel <u>H</u> elp	

- 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.

Figure 132	Restart NTP Service
riguie 152	Result MII Service

🛃 NTP Daemon (ntpd) Options	5 X
General NTP Settings	NTP Servers 10.29.160.100 Add Edit Remove Restart NTP service to apply changes
	OK Cancel <u>H</u> elp

24. Time configuration option would now show that the NTP client is running, along with the IP address of the NTP client.

I

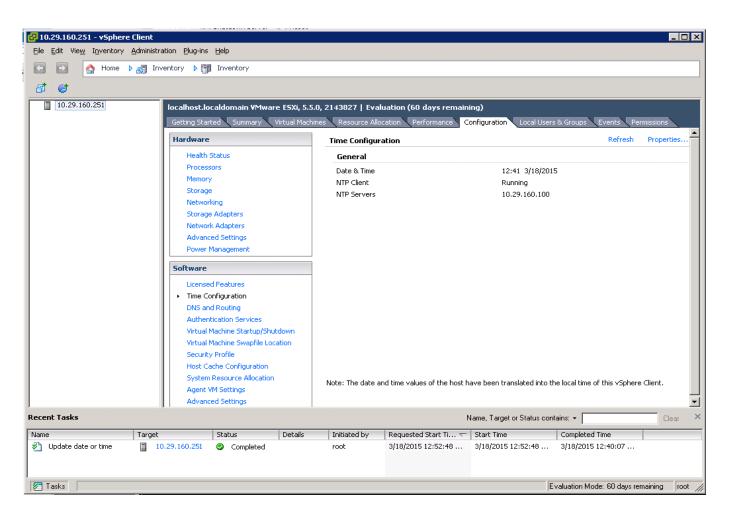


Figure 133 Verifying the NTP Client

Downloading the UCS Director Express Software Components

I

The software components of UCS Director Express for Big Data need to be downloaded from three different locations.

Software component	File Names	Link to Download	
Cisco UCS Director Express 1.0 OVF	CUCSD_Express_1_0_0_0_GA.z	https://software.cisco.c om/download/release.ht ml?mdfid=286281255 &flowid=71403&softw areid=285018084&rele ase=1&relind=AVAILA BLE&rellifecycle=&rel type=latest	
Cisco UCS Director 5.2.0.1 patch	cucsd_patch_5_2_0_1.zIP	https://software.cisco.c	
Cisco UCS Director Baremetal Agent 5.2 OVF	CUCSD_BMA_5_2_0_0_VMWA RE_GA.zip	om/download/release.ht ml?mdfid=286283454 &flowid=72903&softw areid=285018084&rele ase=5&relind=AVAILA BLE&rellifecycle=&rel type=latest	
Cisco UCS Director Express for Big Data 1.1 Upgrade Package	UCSDExpress_Big_Data_1.1_Up grade_Package.zip	https://software.cisco.c om/download/release.ht	
25. Cisco UCS Director Express for Big Data BMA Update Package	UCSDExpress_BMA_Big_Data_ 1.1_Upgrade_Package.zip	ml?mdfid=286284995 &flowid=73724&softw areid=285018084&rele ase=1&relind=AVAILA BLE&rellifecycle=&rel type=latest	

I

1

Download the Software Components

1. Using the links provided Table 15 above, download the Cisco UCS Director Express for Big Data 1.0 OVF Appliance zip file.

	Figure 134	Cisco	UCS Director E.	xpress for Big	Data 1.0 Dow	vnload Page	
🗲 🔿 C 🙆 http	os:// <mark>software.cisco.co</mark>	om/download	l/release.html?md	lfid=28628125	5&flowid=7140	03&softwareid:	=285018084&rel 🕅 🖒
ululu cisco	Products & Services	Support	How to Buy	Training & Eve	Worldwide [change] ents Partne	_	Register My Cisco 🔻
	Software Products > Servers - Unifie press for Big Data ?		UCS Director > UCS D	Virector Express for	·	•••	(0 items) 🕞 Feedback Help ppliance Software-1
Search Expand All Collapso		Patch as well as f	BMA Patch for Cisco UCSE) Express for Big Data	a1.0		Add Devices
1	File Information				Release Date 🔻	Size	
→ All Releases ▶ 0		eed to be applie 11950f07837e29b	t Patch for Cisco UCS D d on top Cisco UCS Dire dcc52dca301) 🚡		19-NOV-2014	10.37 MB	Download Add to cart
	Cisco UCSD Expres 5 Checksum - ca44 cucsde_patch_1_0_0	a9a25057af5072ac	tch (Patch needs to be afaf7fc7d933) 🚡	applied on 1.0. MD	19-NOV-2014	1.76 MB	Download Add to cart
		71, CVE-2014-716 tch 🚡	Code Injection Vulnera 9) Note: Patch has READ		06-OCT-2014	1.82 MB	Download Add to cart
Cisco UCS Direc 8d6cb7dc36107d	Cisco UCS Director 8d6cb7dc36107ca5c CUCSD_Express_1_0	1f93a9faf69d49c	Data 1.0 (OVF Appliance) 🚡) MD5 Checksum	05-SEP-2014	2663.09 MB	Download Add to cart
Cisco UCS Director m - 517fa2a881b8cal UCSDExpress_BMA_5		b6dff0c3ad17a1c		ge MD5 Checksu	05-SEP-2014	343.95 MB	Download Add to cart
Related Information							-
Dashboard Info	ormation Sources						
Select different info	ormation sources for access to	o relevant troublest	nooting information.				
Information Sourc	es						

I

Γ

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.

Figure 135 Cisco UCS Director 5.2 Download Page

Downloads Home > Products > Servers - Unified Computing > UCS Director > UCS Director 5.2 > UCS Director Virtual Appliance Software-5

UCS Director 5.2

Search Expand All Collapse All	Release 5			Rdd Device	
 Latest All Releases 5 	CUCSD 5.2.0.1 Patch				
	File Information	Release Date 🔹	Size		
	Cisco UCS Director 5.2.0.1 Patch (Patch need to be applied on top of 5.2 MD5 Checksum - 1ef745cd8bbd43a46aa1398247dbfc1c) cucsd_patch_5_2_0_1.zip	03-FEB-2015	1141.61 MB	Download Add to cart	^
	Cisco UCS Director 5.2.0.0A HOTFIX Patch (PSIRT FIX FOR NTP - Patch need to be applied on top of 5.2.0.0 MD5 Checksum - 24f9a3c0c2c6aa1ab83fc0da70cf5c e7)		1.45 MB	Download Add to cart	
	Cisco UCS Director 5.2 (HyperV Appliance) MD5 Checksum - f04047c63e5c142 2ff49fe575a77d143 CUCSD_5_2_0_0_HYPERV_GA.zip	20-DEC-2014	9344.73 MB	Download Add to cart	
	Cisco UCS Director 5.2 (VMWare vSphere OVF Appliance. MD5 Checksum - 06 bfb6fe95aabef9c69555b535946363) 🚡 CUCSD_5_2_0_0_VMVARE_GA.zip	20-DEC-2014	2869.15 MB	Download Add to cart	
	Cisco UCS Director Baremetal Agent 5.2 (HyperV Appliance MD5 Checksum - 0fd872b48f9f302416b6769a247cbbec)	20-DEC-2014	8195.32 MB	Download Add to cart	
	Cisco UCS Director Baremetal Agent 5.2 (VMWare vSphere OVF Appliance MD 5 Checksum - a0c34c4c924720dc9d2f9b099c5b9b5c) CUCSD_BMA_5_2_0_0_VMWARE_GA.zip	20-DEC-2014	1857.43 MB	Download Add to cart	•

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.

1

Figure 136 Cisco UCS Director Express for Big Data 1.1 Download Page

Downloads Home > Products > Servers - Unified Computing > UCS Director > UCS Director Express for Big Data 1.1 > UCS Director Virtual Appliance Software-1

UCS Director Express for Big Data 1.1

Search Expand All Collapse All	Release 1				Add Devices
▼ Latest	Cisco UCSD Express 1.1 (Upgrade Package and BMA Patch)				
1 ▼All Releases	File Information	Release Date	•	Size	
▶ 0	Cisco UCS Director Express for Big Data 1.1 BMA Update Package (MD5 Check sum 25e434da9b06465cade4902e0e5b0d81) UCSDExpress_BMA_5.2_Big_Data_1.1_Upgrade_Package.zip	10-MAR-2015		353.13 MB	Download Add to cart
	Cisco UCS Director Express for Big Data 1.1 Upgrade_Package (MD5 Checksu m 8748164497a2b42ee4ba079098a0a1e3) (UCSDExpress_Big_Data_1.1_Upgrade_Package.zip	10-MAR-2015		2.05 MB	Download Add to cart

- 4. Place all the files in a directory in the client windows workstation.
- 5. Unzip the contents of the CUCSD_Express_1_0_0_0GA.zip and CUCSD_BMA_5_2_0_0_VMWARE_GA.zip.

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.

I

4. From the File menu, Select Deploy OVF Template.

Figure 137 Deploy OVF in the vSphere Client

Export Incalhost.localdomain VMware ESXi, 5.5.0, 2143827 Evaluation (60 days remaining) Browse VA Marketplace Prict Maps Prict Maps Incalhost.localdomain VMware ESXi, 5.5.0, 2143827 Evaluation (60 days remaining) Setting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions Dist A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the GPU and memory resources that virtual machines use and give virtual appliance. Not is a computer that uses virtual appliance. Incalhost Jocal Users & Groups Host You can add a virtual appliance. A virtual appliance. Not virtual appliance. Not virtual appliance. Host The easiest way to add a virtual appliance. The easiest way to add a virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux. Visphere Client Basic Tasks Deploy from VA Marketplace Explore Further Larn about vSphere Create a new virtual machine Larn about vSphere Manage multiple hosts, eliminate downtime, load	New	rentory D 🛐 Inventory
Report Browse VA Marketplace Print Maps Exit What is a Host? A host is a computer that uses virtualization software, such as ESX or ESX, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual appliance. A virtual appliance. The easiest way to add a virtual machine is to deploy a virtual appliance. The easiest way to add a virtual appliance. Basic Tasks Image: Implicit CA in the virtual machine will need an operating system and software already installed on it, such as Windows or Linux Visphere Client Explore Further I can about vSphere Manage multiple hosts, eliminate downtime, load text Tasks Toreate a new virtual machine Name, Taget or Stalus conteix: * [International context virtual splance] The task is context virtual machine text is a point of the poin	Deploy OVF Template	
Browse VA Marketplace Print Maps Exit		
Print Maps close tab (C) Exit What is a Host? A host is a computer that uses virtualization software, such as ESX or ESX, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity. Virtual Machines were and give virtual machines to a host by creating a new one or by deploying a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux. Host Basic Tasks Deploy from VA Marketplace Explore Further Image multiple hosts, eliminate downtime, load Nare, Target or Status contain: * (clear)		
Pills Maps What is a Host? A host is a computer that uses virtualization software, such as ESX or ESX, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines. Hosts provide the CPU and memory resources that virtual machines was and give virtual appliance access to storage and network connectivity. Virtual Machines Virtual Machines Host You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance. The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine will need an operating system installed on it, such as Windows or Linux. Host Basic Tasks Deploy from VA Marketplace Explore Further Image multiple hosts, eliminate downtime, load Learn about v Sphere Mange multiple hosts, eliminate downtime, load Name, Target or Status contairs: * Ctert	Browse VA Marketplace	
Ext A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult B A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult A host is a consult and plance. A host is a consult A host is a consult appliance. The easiest way to add a virtual machine is to deploy a virtual appliance. A new virtual appliance is a pre-built virtual machine with no operating system and software alreadult virtual machine with no perating system and software alreadult virtual machine with no perating system and software alreadult virtual machine with no perating system and software alreadult virtual machine Basic Tasks Deploy from VA Marketplace P create a new virtual machine Explore Further Manage multiple hosts, eliminate downtime, load Name, Target or Statu contain: •) Ctert Name, Target or Statu contain: •) Ctert <td>Print Maps</td> <td></td>	Print Maps	
as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity. You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance. The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux. Basic Tasks Create a new virtual machine tert Tasks tert Tasks	Exit	
one or by deploying a virtual appliance. The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux. Basic Tasks Deploy from VA Marketplace Create a new virtual machine Explore Further Learn about v Sphere Manage multiple hosts, eliminate downtime, load Name, Target or Status contains: • Clear		as ESX or ESX, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network
virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux. Basic Tasks Deploy from VA Marketplace Create a new virtual machine Create a new virtual machine Explore Further Learn about v Sphere Manage multiple hosts, eliminate downtime, load Name, Target or Status contains: • Clear		7 0
Basic Tasks Deploy from VA Marketplace Create a new virtual machine Explore Further Learn about v Sphere Manage multiple hosts, eliminate downtime, load cent Tasks Name, Target or Status contains: • Clear		virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating
Image: Deploy from VA Marketplace Explore Further Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace Image: Deploy from VA Marketplace		vSphere Client
Explore Further Create a new virtual machine Explore Further Learn about v Sphere Manage multiple hosts, eliminate downtime, load Name, Target or Status contains: Clear		Basic Tasks
Explore Further Create a new virtual machine Explore Further Learn about v Sphere Manage multiple hosts, eliminate downtime, load Name, Target or Status contains: Clear		Fit Deploy from VA Marketplace
ent Tasks Name, Target or Status contains:		Explore Eurther
Manage multiple hosts, eliminate downtime, load ent Tasks Name, Target or Status contains: •		Treate a new virtual machine
ent Tasks Name, Target or Status contains: - Clear		📃 Learn about v Sphere
		Manage multiple hosts, eliminate downtime, load
me Target Status Details Initiated by Requested Start Ti 💎 Start Time Completed Time	ent Tasks	Name, Target or Status contains: -
	me T	Iarget Status Details Initiated by Requested Start Ti < Start Time Completed Time

1

- 5. Choose the Cisco UCS Director Baremetal Agent 5.2.0.0 OVF template. Click Open.
- 6. Click Next to continue.

🛃 Deploy OVF Template		_ 🗆 🗙
Source Select the source location		
Source OVF Template Details Name and Location Disk Format Ready to Complete	Deploy from a file or URL CSD_BMA_5_2_0_0_VMWARE_GA\cucsd_bma_5_2_0_0.ovff Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
Help	< Back Next >	Cancel //

Figure 138 Select the Cisco UCS Director Baremetal Agent OVF file

7. Review the details of the OVF template, Click Next.

Γ

- 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.

Figure 139 Enter Cisco UCS Director Baremetal Agent VM N	er Cisco UCS Director Baremetal Agent VM Name
--	---

1

Peploy OVF Template		_ 🗆 🗙
Name and Location	n for the deployed template	
specify a name and locador	n or the deployed template	
<u>Source</u> OVF Template Details	Name:	
End User License Agreement	CUCSD-BM-5.2.0.0_36 The name can contain up to 80 characters and it must be unique within the inventory folder.	
Name and Location Disk Format		
Network Mapping Ready to Complete		
Ready to Complete		
Help	<u>≤</u> Back Next ≥	Cancel

10. In the Disk Format option, click the **Thick Provision Lazy Zeroed** radio button. Click **Next** to continue.

Figure 140 Select the Disk Format for the VM

Deploy OVF Template			
Disk Format	nt to store the virtual disks?		
Source OVF Template Details End User License Agreement Name and Location Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): Thick Provision Lazy Ze Thick Provision Eager Z Thin Provision		
Help		 < Back Nex	t > Cancel

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.

ſ

Figure 141 Network Mapping for Deployed Template

🛃 Deploy O¥F Template			
Network Mapping What networks should the	deployed template use?		
Source OVF Template Details End User License Agreement Name and Location Disk Format Network Mapping Ready to Complete	Map the networks used in this OV Source Networks Network 1 Network 2 Description: The Network 1 network	F template to networks in your inventory Destination Networks VM Network PXE_VLAN85	
Help		< Back Next >	Cancel

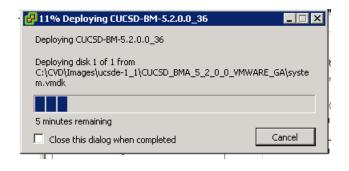
13. Review the details of the VM, click the check box **Power on after deployment** and click **Finish** to proceed with the VM deployment.

1

Figure 142 Deploy the Cisco UCS Director Baremetal Agent VM

🛃 Deploy OVF Template		
Ready to Complete		
Are these the options you	want to use?	
Source	When you click Finish, the deploymer	ht task will be started
OVF Template Details End User License Agreement	Deployment settings:	ic case will be searced.
Name and Location	OVF file:	C:\CVD\Images\ucsde-1_1\CUCSD_BMA_5_2_0_0_VMW
Disk Format	Download size:	1.8 GB
Network Mapping	Size on disk:	40.0 GB
Ready to Complete	Name:	CUCSD-BM-5.2.0.0_36
	Host/Cluster:	localhost.
	Datastore:	datastore1
	Disk provisioning:	Thick Provision Lazy Zeroed
	Network Mapping:	"Network 1" to "VM Network"
	Network Mapping:	"Network 2" to "PXE_VLAN85"
	1	
	Power on after deployment	
Help		< Back Finish Cancel

Figure 143 Cisco UCS Director Baremetal Agent VM Deployment in Progress



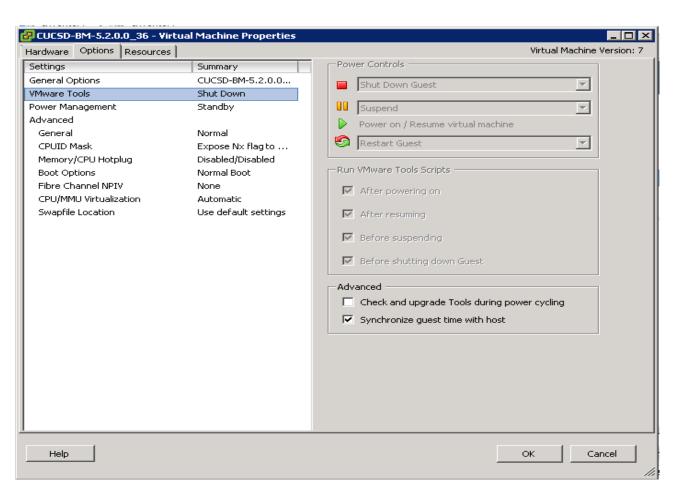
ſ

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 144 Edit VM Settings to Synchronize the Guest Time with the ESXi Host



5. Right click on the BMA-VM, and select Open Console.

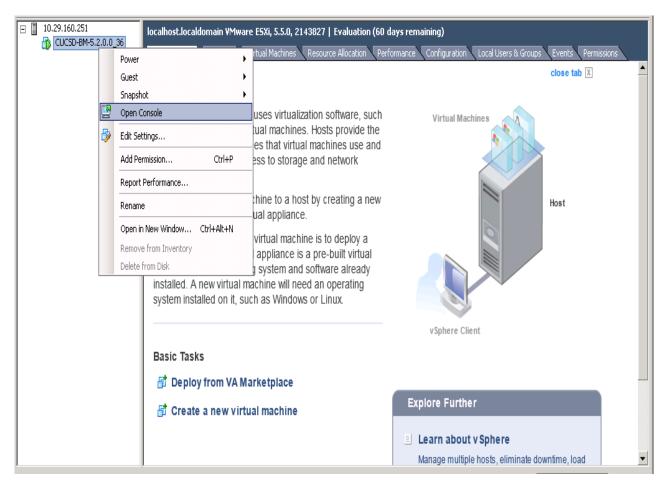


Figure 145 Access the VM Console of the BMA-VM

6. In the console accept the End User License Agreement by typing yes and press ENTER.

Figure 146 Accept the EULA



- 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 16BMA-VM network configurations

Network Interface	Configuration
eth0	IP Address: 10.29.160.36, Subnet Mask: 255.255.255.0
eth 1	IP Address: 192.168.85.36, Subnet Mask: 255.255.255.0

1

Figure 147 Editing the	BMA-VM NIC eth0
------------------------	-----------------

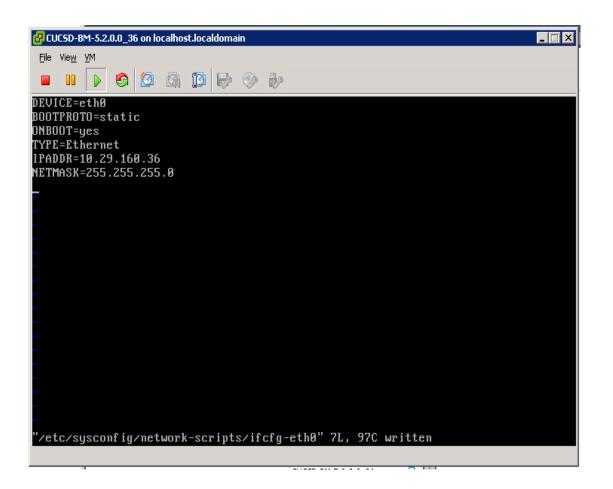
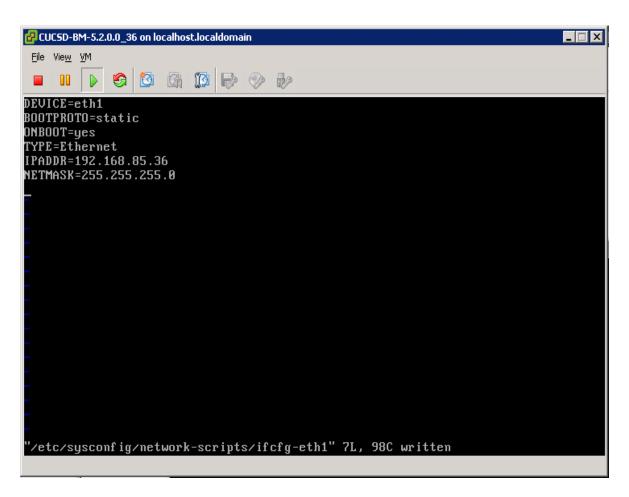


Figure 148 Editing the BMA-VM NIC eth1

I

ſ



9. Restart the network service by using the service command.

service network restart

Figure 149 Restart the network

[root@localhost ~]# service network restart	
Shutting down interface eth0:	[FAILED]
Shutting down interface eth1:	E OK 1
Shutting down loopback interface:	E OK 1
Bringing up loopback interface:	E OK 1
Bringing up interface eth0:	E OK 1
Bringing up interface eth1:	E OK 1

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

Figure 150 Install the Cisco UCS Director Express Big Data Upgrade Package

```
[root@localhost stage] # 1sCentOSLivebd_bma_version.infofeature-bigdata-intel.jarHortonworks-2.1cloudera-5.0.1mapr_common_templatesHortonworks-2.2cloudera-5.2.0ntp_server_config.shMapR-3.1.1cloudera-5.2.1run.sh.templateMapR-4.0.1cloudera-5.3.0scriptsbd-sw-repcommon_templatestemplates[root@localhost stage] # cd scripts/bin[root@localhost bin] # 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

- 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.

Figure 151	Copy the Contents of RHEL6.5 ISO into the BMA-VM
1 15 11 0 101	copy the contents of MillEole 150 the billing the

```
[root@localhost ~]# cd /opt/cnsaroot/RHEL6.5
[root@localhost RHEL6.5]# cp /opt/cnsaroot/images/RHEL6.5/isolinux/* .
[root@localhost RHEL6.5]# ls
FRANS.TBL boot.msg initrd.img isolinux.cfg splash.jpg vmlinuz
boot.cat grub.conf isolinux.bin memtest vesamenu.c32
[root@localhost RHEL6.5]#
```

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

Figure 152 Copy the Cluster-Shell and Passwordless-SSH Utilities

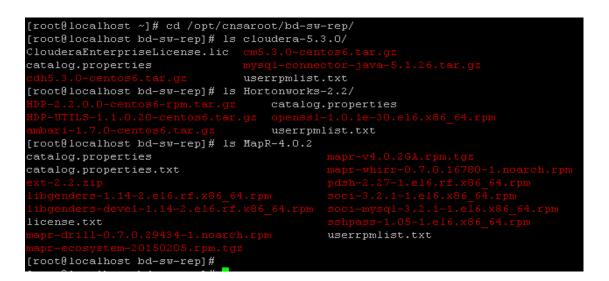
```
-rw-r--r-- 1 root root 250400 Feb 18 21:18 clustershell-1.6-1.el6.noarch.rpm
-rw-r--r-- 1 root root 23427 Feb 18 21:17 pssh-2.3.1.tar.gz
[root@localhost bd-sw-rep]# pwd
/opt/cnsaroot/bd-sw-rep
[root@localhost bd-sw-rep]#
```

- 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. http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-director-express/bma-install-con fig/1-1/b_ucsd_express_bma_install_config_guide_1-1/b_ucsd_express_bma_install_config_guide e_chapter_0101.html#reference_F3FE769E6A114DAD8CD5E3296556B70E
- 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.



distribution does not require any license file.

Figure 153 Copy the RPM Packages for the Hadoop Distributions



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 154 Setup a UCSD Patch Directory in the HTTP Root Path

```
[root@localhost ~]# ls -1 /var/www/html/patches
total 1172256
-rw-r--r- 1 root root 2139421 Feb 18 04:52 UCSDExpress Big Data 1.1 Upgrade Package.zip
-rw-r--r- 1 root root 1197064934 Feb 3 13:16 cucsd patch 5 2 0 1.zip
```

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

service httpd start

Figure 155 Start the HTTPD



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

Figure 156 Verify the Accessibility of the Cisco UCS Director Express Patches

← → C 🗋 10.29.160.36/patches/		☆ 〓
Apps disco UCS Manager		
Index of /patches		
Name	Last modified	<u>Size</u> Description
Parent Directory		_
UCSDExpress_Big_Data_1.1_Upgrade_Page	<u>:kage.zip</u> 18-Feb-2015 04:52 2	2.0 M
🔁 <u>cuesd_patch_5_2_0_1.zip</u>	03-Feb-2015 13:16	1.1G
	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 157 Deploy the Cisco UCSD Express 1.0 OVF

Deploy OVF Template Source Select the source location.		×
Source OVF Template Details Name and Location Disk Format Ready to Complete	Deploy from a file or URL CUCSD Express 1 0 0 0 GA\cucsd express 1 0 0 0.ovf Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
Help	≤ Back Next ≥ Cancel	

- 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.

I

Figure 158 Name the Cisco UCS Director Express
--

Poploy OVF Template		
Name and Location	n for the deployed template	
Source OVF Template Details End User License Agreement Name and Location Disk Format Network Mapping Ready to Complete	Name: CUCSDE-1_1_35 The name can contain up to 80 characters and it must be unique within the inventory folder.	
Help	<back next=""></back>	Cancel

9. Choose the destination network VM Network for the source network Network 1. Click Next to continue.

I

Figure 159 Cisco UCS Director Express VM Network Configuration

Poploy OVF Template			
Network Mapping What networks should the	deployed template use?		
Source OVF Template Details End User License Agreement		template to networks in your inventory	
<u>Name and Location</u> Disk Format	Source Networks Network 1	Destination Networks VM Network	
Network Mapping Ready to Complete	Description: The "Network 1" network		A V
Help		<u>≤</u> Back Next ≥	Cancel

- **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.

ſ

Figure 160	Deploy the	Cisco UCS	Director	Ernross	VM
rigure 100	Deploy the	Cisco UCS	Director	Express	V IVI

1

Deploy OVF Template Ready to Complete Are these the options you	want to use?	
Source OVF Template Details End User License Agreement Name and Location Disk Format Network Mapping Ready to Complete	When you click Finish, the deploym Deployment settings: OVF file: Download size: Size on disk: Name: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network Mapping:	ent task will be started. C:\CVD\Images\UCSD-1_0\CUCSD_Express_1_0_0_0_GA 2.6 GB 100.0 GB CUCSDE-1_1_3S localhost. datastore1 Thick Provision Lazy Zeroed "Network 1" to "VM Network"
Неір		< Back Finish Cancel

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.

Hardware Options Resources Virtual Machine Version: 7 Settings Summary Fower Controls General Options CUCSOE-1_1_35 VMware Tools Shut Down Power Management Standby Advanced Image: Summary General Normal CPUID Mask Expose NX flag to Boot Options Normal Boot Fibre Channel NPTV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Before suppending Effore suppending Advanced Check and upgrade Tools during power cycling Synchronize guest time with host Synchronize guest time with host	🔁 CUCSDE-1_1_35 - Virtual M	-	
Consigned CUCSDE-1_135 VMware Tools Shut Down Power Management Standby Advanced Image: Standby General Normal CPUID Mask Expose Nx flag to Boot Options Normal Boot CPUID Mask Expose Nx flag to Boot Options Normal Boot CPU/MMU Virtualization Automatic Swapfile Location Use default settings After resuming Before suspending Before shutting down Guest Advanced Advanced Check and upgrade Tools during power cycling Synchronize guest time with host Synchronize guest time with host	Hardware Options Resources		Virtual Machine Version: 7
Witware Tools Shut Down Power Management Standby Advanced Image: Suppose Nx flag to General Normal CPUID Mask Expose Nx flag to Boot Options Normal Boot Fibre Channel NPTV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: Before suspending Image: Before suspending Image: Before suppending Image: Before suppending Image: Check and upgrade Tools during power cycling Synchronize guest time with host	Settings	Summary	Power Controls
Power Management Standby Advanced Image: Standby General Normal CPUID Mask Expose Nx flag to Boot Options Normal Boot Fibre Channel NPIV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: Before suspending Image: Before suspending Image: Before shutting down Guest Advanced Advanced Check and upgrade Tools during power cycling Image: Synchronize guest time with host Synchronize guest time with host			Shut Down Guest
Advanced General Normal CPUID Mask Expose Nx flag to Boot Options Normal Boot Fibre Channel NPTV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings We default settings After resuming Before suspending Before shutting down Guest Advanced Check and upgrade Tools during power cycling Synchronize guest time with host			
General Normal CPUID Mask Expose Nx flag to Boot Options Normal Boot Fibre Channel NPIV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Synchronize guest time with host Image: CPU/MU Virtualization Image: CPU/MU Virtualization <th>-</th> <th>Standby</th> <th>Suspend 🗾</th>	-	Standby	Suspend 🗾
CPUID Mask Expose Nx flag to Boot Options Normal Boot Fibre Channel NPIV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Before suspending Before suspending Before shutting down Guest Advanced Check and upgrade Tools during power cycling Synchronize guest time with host			Power on / Resume virtual machine
Boot Options Normal Boot Fibre Channel NPIV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: CPU/MMU Virtualization Automatic Image: CPU/MMU Virtualization Use default settings Image: CPU/MMU Virtualization Automatic Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MMU Virtualization Image: CPU/MU Virtualization Image: CPU/MU Virtualization	l		Portert Guest
Fibre Channel NPIV None CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: After powering on Image: After resuming Image: Before suspending Image: Before shutting down Guest Advanced Image: Check and upgrade Tools during power cycling Image: Synchronize guest time with host			
CPU/MMU Virtualization Automatic Swapfile Location Use default settings Image: After resuming After resuming Image: Before shutting down Guest Advanced Image: Check and upgrade Tools during power cycling Synchronize guest time with host	· ·		
Swapfile Location Use default settings After resuming Before suspending Before shutting down Guest Advanced Check and upgrade Tools during power cycling Synchronize guest time with host			
 After resuming Before suspending Before shutting down Guest Advanced Check and upgrade Tools during power cycling Synchronize guest time with host 	l '		After powering on
Before shutting down Guest Advanced Check and upgrade Tools during power cycling Synchronize guest time with host	Swapnie Location	Use der adit settings	After resuming
Advanced Check and upgrade Tools during power cycling Synchronize guest time with host			Before suspending
Check and upgrade Tools during power cycling Synchronize guest time with host			🔽 Before shutting down Guest
Check and upgrade Tools during power cycling Synchronize guest time with host			Advanced
Synchronize guest time with host			
Help OK Cancel			Synchronize guest time with host
Help OK Cancel			
	Help		OK Cancel

Figure 161 Edit VM Settings to Synchronize the Guest Time with the ESXi Host

- 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.

Figure 162 Assigning the Static IP Address to the UCSD-VM eth0

This script is executed on first boot only. Configuring static IP configuration
Do you want to Configure static IP [y/n]? : y Do you want to configure IPv4/IPv6 [v4/v6] ? : v4
Configuring static IP for appliance. Provide the necessary access credentials
IP Address: 10.29.160.35 Netmask: 255.255.255.0 Gateway: 10.29.160.1
Configuring Network with : IP(10.29.160.35), Netmask(255.255.255.0), Gateway(10. 29.160.1)
Do you want to continue [y/n]? : y_

- 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 163 Choose the UCSD Express Personality



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

Figure 164 UCSD-VM First-Boot Initializations



Note This ste

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.

Figure 165 Logging onto the UCSD-VM Shell Administration Tool

login as: shelladmin shelladmin@10.29.160.35's password: <mark>-</mark>

- 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.

Figure 166 Issuing the Command to Stop all the Services Via Shell Administration Tool.

	Standalone Node		
Select a	a number from the menu below		
1)	Change ShellAdmin Password		
2)	Display Services Status		
3)	Stop Services		
4)	Start Services		
5)	Stop Database		
6)	Start Database		
7)	Backup Database		
8)	Restore Database		
9)	Time Sync		
10)	Ping Hostname/IP Address		
11)	Show Version		
12)	Import CA Cert (JKS) File		
13)	Import CA Cert(PEM) File for VNC		
14)	Configure Network Interface		
15)	Display Network Details		
16)	Enable Database for Cisco UCS Director Baremetal Agent		
17)	Add Cisco UCS Director Baremetal Agent Hostname/IP		
18)	Tail Inframgr Logs		
19)	Apply Patch		
20)	Shutdown Appliance		
21)	Reboot Appliance		
22)	Manage Root Access		
23)	Login as Root		
24)	Configure Multi Node Setup (Advanced Deployment)		
25)	Clean-up Patch Files		
26)	Collect logs from a Node		
27)	Collect Diagnostics		
28)	Change Personality		
29)	Quit		
SEL	SELECT> 3		
Do you wa	nt to stop services [y/n]? : y		

I

5. In the Shell Admin menu, type 2 to view the status of the services. They all should be **NOT-RUNNING** as shown below.

	SELECT> 2	
Service	Status	PID
broker	NOT-RUNNING	_
controller	NOT-RUNNING	—
eventmgr	NOT-RUNNING	—
client	NOT-RUNNING	—
idaccessmgr	NOT-RUNNING	—
inframgr	NOT-RUNNING	
TOMCAT	NOT-RUNNING	—
websock	NOT-RUNNING	
3467 ?	00:00:00 mysqld_safe	
3888 ?	00:03:05 mysqld	
Press return	to continue	

Verifying the Status of the UCSD-VM Services Figure 167

- 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]**?.

1

- 8. At the prompt, Patch URL: enter http://<BMA_IP>/patches/cucsd_patch_5_2_0_1.zip
- 9. Hit ENTER to continue.

Figure 168	Cisco UCS Director 5.2.0	.1 Patch Application Process

Select	a number from the menu below
1)	Change ShellAdmin Password
2)	Display Services Status
3)	Stop Services
4)	Start Services
5)	Stop Database
6)	Start Database
7)	Backup Database
8)	Restore Database
9)	Time Sync
10)	Ping Hostname/IP Address
11)	Show Version
12)	Import CA Cert (JKS) File
13)	Import CA Cert(PEM) File for VNC
	Configure Network Interface
15)	Display Network Details
	Enable Database for Cisco UCS Director Baremetal Agent
17)	Add Cisco UCS Director Baremetal Agent Hostname/IP
18)	Tail Inframgr Logs
19)	Apply Patch
	Shutdown Appliance
21)	Reboot Appliance
22)	Manage Root Access
23)	Login as Root
24)	Configure Multi Node Setup (Advanced Deployment)
25)	Clean-up Patch Files
26)	Collect logs from a Node
27)	Collect Diagnostics
	Change Personality
29)	Quit
	ECT> 19
Applying Patch	
	ke database backup before applying patch[y/n]? n
	ion not to take backup, proceeding with applying patch
Applying Patch	
Patch URL :htt	p://10.29.160.36/patches/cucsd_patch_5_2_0_1.zip
Applying the Patc	h http://10.29.160.36/patches/cucsd_patch_5_2_0_1.zip [y/n]? y

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.

I

Figure 169 Cisco UCS Director Express for Big Data 1.1 Upgrade Package Installation Process



Figure 170 Cisco UCS Director Express for Big Data 1.1 Upgrade Package Application Complete

```
Jed Jan 21 22:10:45 UTC 2015 : Copying ui.properties file
*****
irectory doesn't exit, continuing with installation process
* * * * * * * * * * * * * * * * * * *
Jed Jan 21 22:10:45 UTC 2015 : Copying SSL File
* * * * * * * * * * * * * * * * * * *
**********************************
Jed Jan 21 22:10:45 UTC 2015 : Copying VMWare Files & scalability folder
calability folder exists, taking backup /opt/scalability-01-21-2015-22-10-45
)iagnostics folder exists, taking backup /opt/diagnostics-01-21-2015-22-10-45
Jed Jan 21 22:10:45 UTC 2015 : Copying localization related files
Japanese Directory exits.
TrueType folder is present
Jed Jan 21 22:10:45 UTC 2015 : Copying sysmgr jar to T1 library locations if exist
ed Jan 21 22:10:45 UTC 2015 : Personality specific changes for upgrade
ersonality details --> Product Name : UCSD Express for Big Data , Product Version :
0.0.0
Restored account-type-exclusion-list.properties for UCSD Express for Big Data
Restored DefaultRoleMenuMappings.properties for UCSD Express for Big Data
Restored RegularSet menu.xml for UCSD Express for Big Data
lestored AdminSet menu.xml for UCSD Express for Big Data
Restored feature-exclusion-list.properties for UCSD Express for Big Data
Restored reports.xml for UCSD Express for Big Data
lestored about.json for UCSD Express for Big Data
lestored signed-sku-mapping.xml for UCSD Express for Big Data
lestart services and database for the changes to take effect
INFO (FileUtil.java:958) *********
INFO (FileUtil.java:963)
INFO (FileUtil.java:967) 150121 22:10:45 [FileUtil] RunCommandThread: Completed thre
      Thread[Thread-1,5,main]
Completed installing package O
Press return 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.

	SELECT> 2		
Service	Status	PID	
broker	RUNNING	7756	
controller	RUNNING	7888	
eventmgr	RUNNING	7966	
client	RUNNING	8025	
idaccessmgr	RUNNING	8113	
inframgr	RUNNING	8172	
TOMCAT	RUNNING	8240	
websock	RUNNING	8320	
3467 ?	00:00:00 mysqld_safe		
3888 ?	00:05:52 mysqld		
Press return	to continue		

Figure 171 Verify the Status of the Services in the UCSD-VM

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.

UCSD Express for Big Data
Username: admin Password: Login
2014, Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

1

- 3. Navigate to Administration > License screen.

Solutions Converge	ed Physical 🔻 Organiz	ations 🔻 Policies 🔻	Administration Favorites	
Data Containers			License	
g Data IP Pools UC:	S SP Templates for Big Data	Hadoop Cluster Profi	System Users and Groups	eploy Templates Deploy
🖇 Refresh 🛛 🔝 Favorit	e 🗣 Add		Virtual Accounts	
ig Data IP Pools			Physical Accounts Integration	
Name	Description	Assignment Orde	Mobile Access	Assigned
			User Interface Settings Open Automation	
			Support Information	

Figure 173 Accessing the License Administration Page

- 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.

ſ

8. After the license file gets uploaded, Click **Submit** to apply the license.

Figure 174	Applying the Base Cisco UCS Director License.
------------	---

1

Solutions 👻	Converged Physical ▼ Organizations ▼ Policies ▼ Administration ▼ Favorites
License	
License Keys	License Utilization License Utilization History Resource Usage Data
🚷 Refresh 🛛	🖞 Favorite 🛭 🏘 Update License 🛛 🏘 Apply Upgrade License 🛛 🏘 Update Big Data License
License Keys	
	Update License
	License Select a file for upload:
	CCUIC201501181941456050.lic Browse Upload
	Enter License Text
	Submit Close

9. The license keys are displayed as shown below.

Figure 175 Cisco UCS Director Base Licenses got Applied Successfully

UCSD Express for Big Data		admin 😡 Log Out Cisco About Help	Object Search
Solutions Converged Physical Organization	ns 🔻 🛛 Policie	es 🔻 Administration 🔻 Favorites	
License			
License Keys License Utilization License Utilization H	listory Resc	ource Usage Data	•
🛞 Refresh 🔟 Favorite 🏘 Update License 🏼 🏘 Al	oply Upgrade L	License 🛛 🏘 Update Big Data License	
License Keys		🖻 🐼 🖪 😵	
	License E	License Value/Status	
Total 3 items			

- 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.

Γ

13. After the license file gets uploaded, Click Submit.

Figure 176 Applying the Cisco UCS Director Express Big Data Subscription License

1

diale UCSE	Express for Big Data admin 🚳 Log Out Cisco About Help Object Search
Solutions 🔻 Conv	verged Physical 🔻 Organizations 👻 Policies 👻 Administration 🛩 Favorites
License	
License Keys	ense Utilization License Utilization History Resource Usage Data
🛞 Refresh 🛛 🛄 Fa	vorite 🛭 💩 Update License 🛛 🏘 Apply Upgrade License 🛛 🎯 Update Big Data License
License Keys	
	Update Big Data Subscription
▶ 🧰 PAK: <internal></internal>	License Select a file for upload:
	UCSD201501181943322190.lic Browse Upload
	Enter License Text
	Submit Close
Total 3 items	

Solutions Converged Physical Organizati	ons 🔻 Policies 🔻 🔼	dministration V Favorites
icense		
License Keys License Utilization License Utilization	History Resource Usa	ge Data
🛞 Refresh 🔟 Favorite 🔗 Update License 🚳 /	Apply Upgrade License	🔗 Update Big Data License
License Keys		
	License Entry	License Value/Status
🛛 🗁 PAK: <internal> (#20150118194332219 - 2)</internal>		
	Expiration Date	March 18, 2015
	License ID	PAK: <internal> (#20150118194332219 - 2)</internal>
	CUIC-EBDS	1
	CUIC-EBDS	1
/ 🗁 PAK: <internal> (#20150118194145605 - 1)</internal>		
	Expiration Date	March 19, 2015
D	License ID	PAK: <internal> (#20150118194145605 - 1)</internal>
	CUIC-BASE-K9	1

Figure 177 Completion of the License Application.

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.

I

Figure 178 Adding the UCS Manager as a Physical Account in the UCSD-VM

1

ultuilte UCSD Express for Big Da	Add Account			admin 🥥 Log Dut Cieco About Help-
Solutions • Converged Physical • Orga	Pod	Default Pod 💌 🏶	<u> </u>	
Physical Accounts	Category	Computing 👻 🐐		
Site Management Pods Physical Accounts	Account Type	UCSM	ha in the second se	1
🚱 Refresh 🔝 Favorite 🛛 🖨 Add	Authentication Type	Locally Authenticated		
Physical Accounts	Server Management	All Servers 💌 🐐		
Account Nami Account Type Connection S	Account Name	UCSM40	•	Tag
	Server Address	10.29.160.40	*	
		Use Credential Policy		
	User ID	admin	*	
	Password	******]*	
	Transport Type	https 💌 🏶		
	Port	443]*	
	Description]	
			Add Close	

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.

- 4. Goto Administration > System.
- 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.

Figure 179 Start the UCS Inventory Collection System Task

Soldans . Concerped.	Physical . Organizati	ins V. Pola	HARD ADDRESS	start first	101				
inten :									
Pattern Information, Mail D	the Distant Farmenia's	Thisten	ia tritain karam	Any CANADA	Controls. Sys	tem Tesks	men Tala Spicy 7	Email Templahes	Line A.
Statiant IB farmite	😦 Manage Tata 😐 Ru	nine 🔤 v	en Detals						
Scine Tribe						12	0.15.14.10		
	Citil .	Disting.	Patience	REAL PROFESSION	Destadore that	Incompany and	Evenishini Dur	StateTime	Garging
D D D D D	UCS Hunthly Hatarical J Delated UCSAlmourt Co UCS Server Transford J UCS Syste Restrict Purp	Are you sur	e you want to run	task VosInventor	yCollector:UCSM	40' now? Close		02/14/2015 PE- 02/16/2015 06:	
00000	UCS Historical Data Agen UCS Event Subscription 7 UCS Fault Record Purge 7	Enabled	2 Inse 4 Inset 32 Insets	Localmost. Localmost	LocaPrest -	Scheduled Scheduled		02/18/2015 06/	
0	UCS Dely materical Detail UCS Hontaring DataCalle	Distint	4 hours 13 monutes	Localmost. Localmost	LocalPost LocalPost	Scheduled OK	I minutes 25 pe		02/18/201
5	UCS Investory Enlector	Erabled	2.http://	Locareast	trainer .	05	5 minutes 45 se-	22/28/2018 17-	82755/201
 General Physical Network Tasks Physical Network Tasks 									

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 180	Adding the	Rare Metal	Agent Appliance	Information
rigure 100	Auting the	Dare Meiai	Адет Арриансе	injormation

1

Add Bare Metal Agent Appli	iance
BMA Name	BMA36 *
BMA Management Address	10.29.160.36
Login ID	NOTE: This address must be reachable from the Cisco UCS Director appliance root
Password	*****
	☑ BMA Uses Different Interfaces for Management and PXE Traffic
BMA PXE Interface Address	192.168.85.36 *
Description	
Location	
UCSD Database Address	10.29.160.35 💌 *
	Submit Close

Configure the Bare Metal Agent's DHCP services

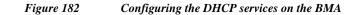
- 1. Navigate to Administration > Physical Accounts >Bare Metal Agents.
- 2. Select the BMA entry.
- 3. On the menu items row, click on the downward facing arrow located at the far right.
- 4. Select Configure DHCP.

Figure 181 Configuring the DHCP

	Solutions Converged	- Animore - Coldanata	ourse ranges	 Administra 	ibon 💎 Favorite				
hysical Accou									
Site Managem	ent Pode Physical Accou	nts Managed Network Ele	ments Bare Me	etal Agents		110-2			
🚱 Refresh	📑 Favorite 🗳 Add 🔯	Edit 🔠 View Details	💥 Delete 🔹	Start Services	😚 Stop Services	🔮 Service St	tatus 🔮 Set I	Default BM	Refresh
Bare Metal A	sents						0 = 0	6 24	Favorite
BHA Name	BMA Management Addri	PXE Server Address	Reachable	Location	Description	Default BMA	Status		Add Edit
DMA36	10.29.160.36	192.168.100.36	VYES			Yes	Active	03/23	View Details
									Delete
								_	Start Services
									Stop Services
									Service Status
									Set Default BMA Configure Interf
									Configure DHCP
									View DHCP Conf
								-	View BNA logs
									View DHCP Configu
								1	

- 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.

ſ



Configure DHCP		
DHCP Subnet	192.168.85.0	*
DHCP Netmask	255.255.255.0	*
DHCP Start IP	192.168.85.160	*
DHCP End IP	192.168.85.254	*
Router IP Address	192.168.85.36	
	Submit	Close

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.

1

Figure 183 Starting the BMA Services

cisco UCSD Express for Big Data	
Soldies + Georged Pound + Dipersities + Policy + Ministration +	Taintin
Tryici Amerik	
Bis Nanopeneet 7 Poin 7 Proved America 7 Hanaged Second Demonts 7 Bare Hetal Age	eets
🔮 Antrein 🔝 fermite 🔹 Ant. 🔆 Ant. 🤮 Date 💥 Dente 🐠 Start Services 🐠 Start 5	arrient 🧕 farriez Status 🧌 Set Default BMA 🐞 Configure Intenface 🛛 👔
Bare Hetal Aperta	(a) <u>m</u> (b) (b)
Ans New Dive New Part Free A Sectored Control	an Distant Status Last Kass AV Image Catal) Distinct Review 20029 Servers 1
A REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY A REAL PROPERT	
Are you sure you want to start services for the sele	rcteil Bare Metal Agent appliance(10.29-160-36)?
Are you sure you want to start services for the sele	rcted Bare Metal Agent appliance(10.29.160.36)?
Are you sure you want to start services for the sele	rcted Bare Metal Agent appliance(10.29.160.36)) Start Close
Are you sure you want to start services for the sele	
Are you sure you want to start services for the sele	
Are you want to start services for the sele	
Are you sure you want to start services for the sele	
Are you want to start services for the sele	
Are you want to start services for the sele	
Are you want to start services for the sele	

5. Click on Service Status, to check the status of the services.

ſ

6. The Bare Metal Agent Service Status **message box should display both the** Network Services status and Database connectivity status as UP.

Figure 184 Verifying the Bare Metal Agent Services Status

cisco UCS	SD Expres	is for Big De	ita'				
Soldina V . C	soverged. P	Nutrical 🐖 Orga	cizidio	a · Joldan Alministratur · Ferentes			
tysical Amounts							
lis Panaperent.	Page The	and Associate 1. Pr	in a second	Delivery, Extractly, Bare Hetal Agents			
Steven 13	Auren 🏘	AN (2 MR.)	20	lete 🙊 Start Services 👰 Stop Services 👰 Service Status 🐞 Se	e Defairt BHA	Collipore Interf	ion (🔟
Bare Metal Agents					Skin N	100	
Ritz Same	HA Manapai	FILE DRIVER, A	-	and I can be an Incare I among			Insted Serve
RAILER IS	11-29-250-26	111.118.85.55	100	Bare Metal Agent Service Status			Dich Servert
				Network Services status in the Bare Metal Agent Appliance : UP Database connectivity status from Bare Metal Agent Appliance : UP Close			
•							<u> </u>
Tabal S (Berry)						_	

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.

1

1

7. Double click on the BMA entry to verify the RHEL operating system repository.

Figure 185 Verifying the RHEL Operating System Software

ysical Accounts > Bare Metal Agent (BMA36) IA OS List PXE Service Requests RFS Mount Point Refresh I Fovorite		Back
🖟 Refresh 🛛 🔝 Favorite		
MA OS List	() II V R	
Image Catalog Name	Last Updated	1
ent0560	03/21/2015 02:05:13 GMT-0700	
entOSLive	03/21/2015 02:05:13 GMT-0700	
£15.4	03/21/2015 02:05:13 GMT-0700	
i£16.5	03/21/2015 02:05:13 GMT-0700	
in2k12R2x64	03/21/2015 02:05:13 GMT-0700	
in2k12x64	03/21/2015 02:05:13 GMT-0700	
in2k8R2x64	03/21/2015 02:05:13 GMT-0700	

Note

BMA-VM software periodically scan the /opt/cnsaroot directory to update the available list of operating system software repositories.

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.



C240/C220 M4 Rack Servers are supported from UCS firmware 2.2(3d) onwards.

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.

Figure	186
--------	-----

Creating the IP Address Pools

cisco	UCSD Expre	ess for Big Da	ıta				admin 🥥	Log Out C	isco /	About He	elp Object Sea	
Dashboard	Solutions 🔻	Converged Phys	ical 🔻 Organ	zations 🔻 Policies 🔻	Administration 🔻	Favorites						
Big Data Cor	lig Data Containers											
Big Data IP	Pools UCS SP T	emplates for Big Da	ta Hadoop Cl	uster Profile Templates	Hadoop Cluster De	oloy Templates	Deployed Clust	ters				٠
🚯 Refresh	🛄 Favorite 📢	bbA 🖣										
Big Data IP	Pools							(j)	3 😵 🛛			
Name	Description	Assignment C	Size				Assigned					
Total 0 item	i	A	1									-

- 6. In the Create an IP Pool dialog box.
- 7. Enter the name MGMT. Click Next to continue.

Create an IP Pool	Create an IP Pool					
IP Pool	IP Pool Management					
IPv4 Addresses		MGMT]•			
				Next	Close	

Figure 187 Creating the IP Address pool for MGMT VLAN

- 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.

ſ

Figure 188	Adding a Block of IP Address to the MGMT IP Address Pool
1 igure 100	Auturg a Dioek of II Auturess to the MOMI II Auturess I out

1

IP Pool		IP Pool - IPv4 Addresses							
IPv4 Addresses		IPv4 Blocks	cks 🗣 🖉 🕱						
			Static IP Pool	Subnet Mask	Default Gatew	Primary DNS	Secondary D1		
	Add Entry to	IPv4 Blocks	1						
	Static IP Po	ol 10.29.16	50.101 - 10.29.16	0.200 *					
		Static IP	Pool. Example (If	PV4): 192.168.0.1	- 192.168.0.50,19	2.168.0.100,192.	168.1.20-192.168.1.7		
	Subnet Mas	APRIL 1 State State State	and the state of the	٠					
		Subnet Mask, ex (IPV4): 255.255.0							
Default G		Sateway 10.29.160.1							
	Derault Gat	eway 10.29.16	50.1						
	Primary DN		50.1						
	Primary DN	is 0.0.0.0	50,1						
		is 0.0.0.0	50.1						
	Primary DN	is 0.0.0.0					Submit		
	Primary DN	is 0.0.0.0					Submit		
	Primary DN	is 0.0.0.0				_	Submit		
	Primary DN	is 0.0.0.0		-			Submit		
	Primary DN	is 0.0.0.0					Submit		
	Primary DN	is 0.0.0.0					Submit		

Note

The Default Gateway, Primary and Secondary DNS fields are optional.

11. Click **Submit** again to create the Big Data IP Pool.

Create an IP Pool		_						
V IP Pool	ol IP Pool - IPv4 Addresses							
IPv4 Addresses	IPv4 Blocks	4						
		Image: Constraint of the second sec				Secondary Df		
				0.0.0.0	0.0,0.0			
		Total 1 items						
	-					Back	Submit	Close

Figure 189 IP Address Pool Added Successfully

ſ

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.

Figure 190 All the IP Address Pools have been Configured Successfully

Solution	Converged	Physical 🔻 Orga	nizations 🔻	Policies 🔻 Administration 🔻 Favorites
ig Data (Containers			
Big Data	IP Pools UCS S	SP Templates for Big D	ata Hado	op Cluster Profile Templates Hadoop Cluster Deploy Templates Deployed
🛞 Refre	esh 🔳 Favorite	🖶 Add		
Big Data	IP Pools	10		
Name	Description	Assignment Order	Size	Assigned
MGMT		default	100	0
HDFS		default	100	0
DATA		default	100	0

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 filed, 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.

I



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.

```
<u>Note</u>
```

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 MapR from the drop-down list.
- 14. In the Hadoop Distribution Version field, select MapR-4.0.2 from the drop down list.

Cloudera + + Hadoop Distribution cloudera cloudera-5.2.0 Hadoop Distribution Version cloudera-5.2.0 cloudera-5.3.0 cloudera-5.0.1 UCS Manager Account cloudera-5.2.1 Hortonworks Hadoop Distribution Hortonworks w. Hadoop Distribution Version Hortonworks-2.1 Hortonworks-2.1 Hortonworks-2.2 MapR Hadoop Distribution MapR -MapR-4.0.1 Hadoop Distribution Version MapR-4.0.1 MapR-3.1.1 MapR-4.0.2 UCS Manager Account

Figure 191 Selecting the Hadoop Distribution Version

- 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 192 Editing the vNIC Template to Provide the MGMT Network Configurations

1

	Edit Entry		
	vNIC Name	eth0 💌 🏶	
l	IP Pool	MGMT(10.29.160.101 - 10.29.160.200) 💌 *	
	MAC Address Pool	mac_pool1 (1978) 💌 🔹	
l	VLAN ID	1	•
L		[4048-4093],[1-3967]	
		(MGMT VLAN)	
L			
		[Submit Close

19. Double-click on **eth1** and select appropriate IP-pool, MAC Address Pool and enter the DATA1 VLAN ID. Click **Submit**.

Figure 193 Editing the vNIC Template to Provide the DATA1 Network Configurations

Edit Entry		
vNIC Name	eth1 💌 🏶	
IP Pool	HDFS(192.168.11.101 - 192.168.11.200)	
MAC Address Pool	mac_pool1 (1978) 🔻 *	
VLAN ID	11	*
	[4048-4093],[1-3967]	_
	(DATA1 VLAN)	
		Submit Close

20. Double-click on **eth2** and select appropriate IP-pool, MAC Address Pool and enter the DATA VLAN ID. Click **Submit**.

Edit Entry		
vNIC Name	eth2 💌 🏶	
IP Pool	DATA(192.168.12.101 - 192.168.12.200)	
MAC Address Pool	mac_pool1 (1978) 💌 *	
VLAN ID	12	*
	[4048-4093],[1-3967]	
	(DATA2 VLAN)	
		Submit Close

Figure 194 Editing the vNIC Template to Provide the DATA2 Network Configurations



Γ

The following figure show the expanded version of the Instant Hadoop Cluster Creation dialog box with all the fields filed in.

Figure 195

Creating an Instant Hadoop Cluster

1

Instant Hadoop Cluster Creation				
Big Data Account Name	BD101		*	-
UCSM Policy Name Prefix	Account name can have a BD101	atmost 10 alphanumer	ric characters	
Hadoop Cluster Name	UCSM Policy Name Prefix BD101	can have atmost 5 ch	haracters	
Hadoop Node Count	4			
SSH (root) Password		*		
Confirm SSH Password	****	*		
Hadoop Manager Password		*		
Confirm Hadoop Manager Password		*		
Host Node Prefix	node		*	
OS Version	RHEL6.5 👻 * Choose RHEL 6.5 for M4 S	Servers		
Hadoop Distribution	Hortonworks 👻 🚸			
Hadoop Distribution Version	Hortonworks MapR			
	cloudera			
UCS Manager Account	UCSM40 - *			
Organization	root 🔻 *			
Server UUID pool	uuid_pool1 (2029) 🔻	•		
PXE VLAN ID	85		*	
Server Pool	[4048-4093],[1-3967]			
Server Pool	ID Se	rver Pool Server	Pool F Assigned	Size
	UCSM40;org-roc M4		8	13
	Total 1 items			
Host Firmware Package			W	
		ganization Nan		Mode
	UCSM40 roo UCSM40 roo		t org-root/fw-h es_FW org-root/fw-h	
	UCSM40 roo	ot ESXi_F	W_Packa org-root/fw-h	
				*
	◄ Total 4 items			
vNIC Template	 Image: A state of the state of			
and complete	VNIC Name		irst MAC Address	VLAN ID
			00:25:B5:00:00:00 1 00:25:B5:00:00:00 11	
			00:25:B5:00:00:00 12	
	Total 3 items			
				Submit Close

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.

eshboerd Solutions 🕶 C	onverged Physical	Organizations	Policies 👻 Admir	nistration •	Favorites			
vice Requests for All User Gr	oups							
	Service Requests	Archived Service R	equests Service Req	uest Statistic	a CloudSense More Reports			
All User Groups	😪 Refresh 🙆 F	avorite 🕤 Create	Request 😵 Search a	and Replace	🔟 View Details 🛛 🧑 Cancel Request 👙	Resubmit Recu	est 💩 Archive 🗳 A	id Notes
A Default Group	Service Requests							
	Service Request I	Request Type	Initiating User	-	Catalog/Workflow Name	Initiator d	Request Time	Request Stal
	Surface and an other states of the second	Advanced	admin	1	UCS CPA Node BareNetal	Distance of	03/17/2015 23/38:05 GM	the second s
	2-11	Advanced	admin		UCS CPA Node BareNetal		03/17/2015 23:38:05 GM	and a state of the
Child Baremetal workflows	346	Advanced	admin		UCS CPA Node BareNetal		03/17/2015 23:38:05 GM	Contraction of the American Street Street
	343	Advanced	admin		UCS CPA Node BareMetal		03/17/2015 23:36:04 GM	17-07 Complete
	344	Advanced	admin		Single UCSM Server Configuration WF		03/17/2015 23:36:19 08	17-07i Complete
	[343	Advanced	admin		UCS CPA Multi-UCSM Hadoop Cluster WF	_	03/17/2015 23:35:24 GM	(T-07) Complete
	141	Advanced	admin		UCS CPA Node BareMetal		03/17/2015 14:31:27 GM	T-07 Complete
	341	Advanced	admin		UCS CPA Node BareMetal		03/17/2015 14:31:27 GM	17-07 Complete
	340	Advanced	admin		UCS CPA Node BareNetal		03/17/2015 14:31:27 GM	T-07 Complete
	329	Advanced	admin		Single UCSH Server Configuration WF		03/17/2015 14:29:38 GM	11-07 Complete
/	338	Advanced	admin		UCS CPA Multi-UCSM Hadoop Cluster WF		03/17/2015 14:28:54 GM	T-07 Complete
	337	Advanced	admin	11	UC5 CPA Node BareMetal	7	03/17/2015 11:24:20 GM	rt-07 Complete
1	336	Advanced	admin		UCS CPA Node BareNetal		03/17/2015 11:24:20 GM	T-07i Complete
A CONTRACTOR OF A CONTRACTOR	335	Advanced	admin		UCS CPA Node BareNetal		03/17/2015 11:24:20 GM	17-07 Complete
Master workflows	224	Advanced	admin	_	UCS CPA Node BareMetal	_	03/17/2015 11:24:19 GM	(T-07) Complete
	333	Advanced	admin		Single UCSM Server Configuration WF	_	03/17/2015 11:22:37 GM	17-07 Complete
	332	Advanced	admin		UCS CPA Multi-UCSM Hadoop Cluster WF		03/17/2015 11:21:44 G8	fT-07i Complete

Figure 196 List of Workflows Recently Complete

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.

Workflow Status Log Objects	s Created and Modified Input/Output		
Service Request			
Status			
Status			🚱 Refresh
		Current status for the service request.	· ·
▼ Overview		 Table to device 	00/17/0015 00.05.00
Request ID	343	1 Initiated by admin	03/17/2015 23:35:30
Request Type	Advanced	Multi-UCSM Hadoop Cluster Profile	03/17/2015 23:35:53
Workflow Name	UCS CPA Multi-UCSM Hadoop Cluster WF	Y	
Workflow Version Label	0	3 Setup Hadoop Cluster Env	03/17/2015 23:36:13
Request Time	03/17/2015 23:35:24 GMT-0700	Multi UCSM Configuration WF	03/17/2015 23:36:20
Request Status	Complete		
Comments		5 Multi BareMetal WF Monitor	03/18/2015 00:25:04
▼ Ownership			03/18/2015 00:25:27
Initiating User	admin	6 Synchronized Command Execution	03/18/2015 00:25:27
		Custom SSH Command	03/18/2015 00:26:02
		8 Provision Hadoop Cluster Completed action	03/18/2015 00:41:06
		Complete Completed successfully.	03/18/2015 00:41:09
	1		
			Close

1

1

Figure 197 Viewing a Completed Master Workflow

<u>Note</u>

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.

Workflow Status Log Objects	Created and Modified Input/Output		
Service Request			
Status			
			🛞 Refre
▼ Overview		Current status for the service request.	
Request ID	345	1 Initiated by admin	03/17/2015 23:38:05
Request Type	Advanced	Modify Workflow Priority (High)	03/17/2015 23:38:08
Workflow Name	UCS CPA Node BareMetal		03/17/2015 23:38:11
Workflow Version Label Request Time	0 03/17/2015 23:38:04 GMT-0700	Assign BareMetal SK ID	03/17/2013 23:38:11
Request Status	Complete	Create UCS Service Profile from template	03/17/2015 23:38:17
Comments		5 Service Profile unbind/rebind Action	03/17/2015 23:39:21
▼ Ownership		Y	
Initiating User	admin	6 Modify UCS Service Profile Boot Policy	03/17/2015 23:40:23
		Associate UCS Service Profile	03/17/2015 23:45:59
			03/17/2015 23:46:00
		Bind/Unbind vNIC Template	03/17/2015 23:46:09
		Bind/Unbind vNIC Template	03/17/2015 23:46:13
			03/17/2015 23:46:38
		(1) Setup PXE Boot (OS Type: CentOSLive)	03/17/2013 23:46:38
		(12) Setup RAID Commands	03/17/2015 23:46:50
▼ Overview		Current status for the service request.	
Request ID	345	UCS Blade Power ON Action	03/17/2015 23:47:34
Request Type	Advanced	Monitor PXE Boot	03/17/2015 23:53:16
Workflow Name	UCS CPA Node BareMetal	(14) Monitor PXE Boot	
Workflow Version Label	0	15 Monitor RAID Configuration	03/17/2015 23:53:17
Request Time Request Status	03/17/2015 23:38:04 GMT-0700 Complete	UCS Blade Power OFF Action	03/17/2015 23:53:31
Comments	Complete		03/17/2015 23:53:54
▼ Ownership			
Initiating User	admin	18 Setup RAID Commands	03/17/2015 23:53:57
		UCS Blade Power ON Action	03/17/2015 23:57:17
			03/18/2015 00:04:19
		21 Modify UCS Service Profile Boot Policy Server has Local Disks	03/18/2015 00:04:20
		(22) Service Profile unbind/rebind Action	03/18/2015 00:05:23
			03/18/2015 00:11:08
		23	00,10,2010 00.11.00
		(24) Assign IP Status	03/18/2015 00:11:08
Request Status	Complete	\checkmark	
Comments		(24) Assign IP Status	03/18/2015 00:11:08
▼ Ownership			00/10/0015 00.15.07
		25 Custom SSH Command	03/18/2015 00:16:37
Initiating User	admin	Custom SSH Command	03/18/2015 00:17:10
		(27) Synchronized Command Execution	03/18/2015 00:18:14
		Y	
		(28) UCS Blade Power OFF Action	03/18/2015 00:18:27
		\checkmark	02/10/2015 00:10:10
		29 UCS Blade Power ON Action	03/18/2015 00:19:40
		Synchronized Command Execution	03/18/2015 00:24:29
		30 Completed action	
		31 Complete	03/18/2015 00:24:32
		Completed successfully.	

Figure 198 A Completed UCS CPA Node Baremetal workflow.

I

Γ

Host and Cluster Performance Monitoring

1. In the UCSD-Express web console, navigate to **Solutions > Big Data Accounts** for viewing the Hadoop cluster accounts.

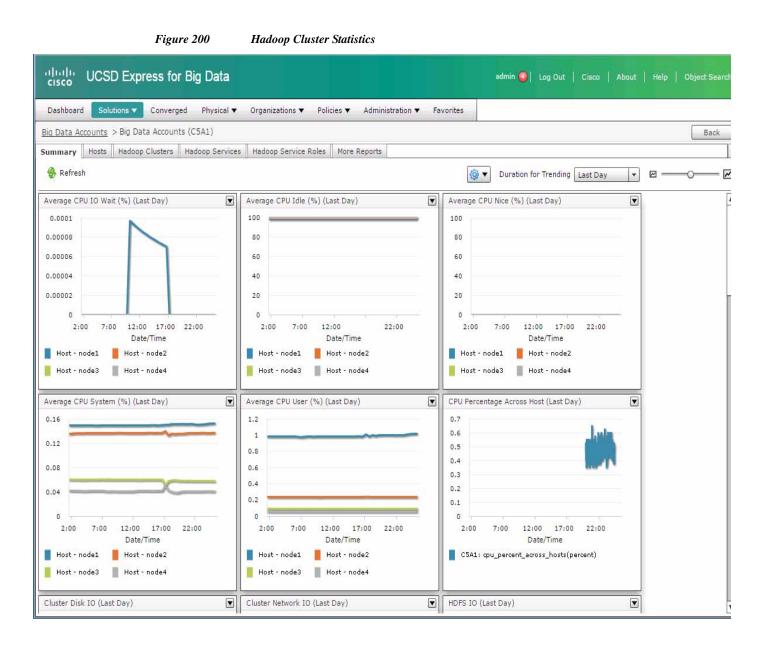
1

Figure 1	199	Big
Figure 1	199	Bl

9 Big Data Accounts Summary Screen

cisco UCSD Express 1	for Big Data			104 Case Alaus 1992 Chief
Daahboard Selations - Conve	erged Physical • Organizations • Police	n 🔻 Administration 🔻 Pavorbes		
g Data Accounts				
lig Data Accounts				
🗞 Refresh 🛗 favorita 🖕 Add	é			
Big Data Accounts				0 10 10 10
Account fiame	Account Type	Data Center	Management Console IP	Login
CSA1	Clouders Derived Account	Default Pod.	19.29.160.124	7908
Марйі	MapR Derived Account	Default PoS	10.29.160.128	root
142	Hortonworks Derived Account	Default Pod	10,29.160.131	rost

2. Double-click on one of the accounts to view the cluster-wide performance charts.



Cluster Management

ſ

- 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.

Dashboard	Solutions	Converged Pl	hysical 🔻 Orga	nizations 🔻 🕴	olicies 🔻 Administration 🔻 Fa	srites		
in Data Accou	nts > Rig Data	Accounts (CSA)	1)					
ummary Ho	sts Hadoop C	lutters Hadoor	Services Had	op Service Role	More Reports			(T)
& Refresh	🗿 Favorite 😽	Add Managed N	iode 👙 Add Lu	ve Node 😽 A	dd BareMetal Nodes 🛛 🔠 View Deta	nia 🛛 💥 Delete N	ode 👙 Assign Reck	👙 Recommission Node/Decommission Node
Hosta								() II V
Host IP	Kernel Name:	Host Name	Rack Name	Health	Server Identity	BareMetal WF		Commission 5
0.29.160.124	Linux	node1	/Default	Good	UCSM40;sys/rack-umit-5	334	Commissioned	
0.29.160.125	Linux	node2	/Default	Good	UCSM40;eys/rack-unit-16	335	Commissioned	
0.25,160.126	Linux	node3	/Default	Good	UCSM40;sys/rack-umit-10	336	Commissioned	
0.29.160.127	Linice	node4	/Default	Good	UCSM40jays/rack-unit-11	337	Commissioned	

Figure 201 Big Data Accounts – Viewing the List of Hosts of a Particular Hadoop Cluster

1

1

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.

Figure 202 Viewing the Services Provisioned in Specific Hadoop Cluster						
cisco L	ICSD Expr	ess for Big D	Data	admin 🧕 Log Out Cisco About Help Object Sea		
Dashboard	Solutions 🔻	Converged Ph	ysical ♥ Organizations ♥ Policies ♥ Administration ♥ Favorites			
Big Data Acco	<u>unts</u> > Big Dat	a Accounts (C5A1		Back		
Summary Ho	osts Hadoop (lusters Hadoop	Services Hadoop Service Roles More Reports			
10		Start All Service				
Hadoop Servic	es					
Status	Health	Service Type		Service Name		
STARTED	GOOD	FLUME	flume			
STARTED	GOOD	SQOOP	sqoop			
STARTED	GOOD	KS_INDEXER	ks_indexer			
STARTED	GOOD	HUE	hue			
STARTED	GOOD	SENTRY	Sentry			
STARTED	GOOD	ZOOKEEPER	zookeeper			
STARTED	GOOD	OOZIE	oozie			
STARTED	GOOD	IMPALA	impala			
STARTED	GOOD	HDFS	hdfs			
STARTED	GOOD	SOLR	solr			
STARTED	GOOD	SPARK	spark			
STARTED	GOOD	HBASE	hbase			
STARTED	GOOD	YARN	yarn			
STARTED	GOOD	HIVE	hive			
Total 14 items						

Host level Monitoring

Γ

In the Hosts tab, double-click on one of the hosts to view the host's statistics.

Dashboard Solutions Converged Physic	(▼ Organizations ▼ Policies ▼ Administration ▼	Pavocitea	
No Data Accounts > Bis Data Accounts (CSA1) >	Heats (CSA1)		- Beck
ommary Post Fault Host CPU Host Dicks	ost Disk In State Host specific roles More Reports		
😵 Refresh		Durat	tion for Transing Last Day
Average CFU 10 Wart (%) (Last Dav)	Average CPU Idle (%) (Last Day)	Average CPU Nice (%) (Lest Day)	Auersge CPU System (%) (Last Day) 0.14 0.15 0.08 0.08 0.09 14:00 19:00 0:00 Date:Time Heat - node1
Averinge CPU User (%) (Lest Day)	Load Average(%) (Last Day) L.A L.2 B.B 2,4	Host CPU Usage (%) (Lest Day)	Host Memory Usege (%) (Lest Day) #4000000000 #4000000000 0 1+00 2000 0 1+00 2000 0 1+00 2000

Figure 203 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:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-director-express/management-guide/ 1-1/b_Management_Guide_for_Cisco_UCS_Director_Express_1_1.html

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.

CUIC-SVR-OFFERS=	Cisco UCS Director Server Offerings	1
CON-SAU-SVROFFERS	Cisco UCS Director Server Offerings Software Application Sup	1
CUIC-BASE-K9	Cisco UCS Director Software License	1
CON-SAU-CUICBASE	SW APP SUPP + UPGR Cisco UCS Director Base Software	1
CUIC-TERM	Acceptance of Cisco UCS Director License Terms	1

 Table 17
 Bill of Material for UCSD for Big Data Subscription Licenses for up to 64 Servers

CUIC-EBDS-LIC=	UCSD Express for Big Data - Standard Edition (SE)	1
CUIC-EBDS-LIC	UCSD Express for Big Data - Standard Edition (SE)	64
CUIC-EBDS-S1-3YR	UCSD Express for Big Data - SE 3 year	64
CUIC-TERM	Acceptance of Cisco UCS Director License Terms	1

 Table 17
 Bill of Material for UCSD for Big Data Subscription Licenses for up to 64 Servers

Table 18 Bill of Material for Various Hadoop Platforms

Γ

Part Number	Description
UCS-BD-CEBN=	CLOUDERA ENTERPRISE BASIC EDITION
UCS-BD-CEFN=	CLOUDERA ENTERPRISE FLEX EDITION
UCS-BD-CEDN=	CLOUDERA ENTERPRISE DATA HUB EDITION
UCS-BD-HDP-ENT=	HORTONWORKS ENTERPRISE EDITION
UCS-BD-HDP-EPL=	HORTONWORKS ENTERPRISE PLUS EDITION
UCS-BD-M5-SL=	MAPR M5 EDITION
UCS-BD-M7-SL=	MAPR M7 EDITION