



Cisco UCS Director Express for Big Data Deployment and Management Guide, Release 3.7

First Published: 2019-01-09

Last Modified: 2020-03-09

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](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. (1721R)

© 2019–2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	xi
Audience	xi
Conventions	xi
Related Documentation	xiii
Documentation Feedback	xiii
Communications, Services, and Additional Information	xiii

CHAPTER 1

New and Changed Information for this Release	1
New and Changed Information in Release 3.7	1
New and Changed Information in Release 3.7(1.0)	1
New and Changed Information in Release 3.7(2.0)	2
New and Changed Information in Release 3.7(2.1)	2
New and Changed Information in Release 3.7(4.0)	2

CHAPTER 2

Overview	3
Cisco UCS Director Express for Big Data	4
Cisco UCS Integrated Infrastructure for Big Data	4
Managing Cisco UCS Director and Cisco UCS Director Express for Big Data Personalities	4
Creating User Roles	5
Hadoop Administrator Permissions	5
Hadoop User Permissions	8
Installing Cisco UCS Director Express for Big Data on VMware vSphere	10
Installing Cisco UCS Director Express for Big Data Bare Metal Agent on VMware vSphere	12
Downloading Cisco UCS Storage and Network Drivers	14
NTP Server Configuration on Cisco UCS Director Express for Big Data Bare Metal Agent	15
Adding Oracle JDK Software Versions to Bare Metal Agent	16

Cisco Server Support for Big Data Cluster Deployments	16
Cisco Server Support for Splunk Enterprise Deployments	17
Adding a New Red Hat Version for Hadoop Cluster	17
New RHEL Version	18
Supported Hadoop Distributions	18
Supported Splunk Distribution	19
Supported Oracle JDK Software Versions	19
Supported Upgrade Scenarios for Cloudera	19
Supported Upgrade Scenarios for MapR	20
Supported Upgrade Scenarios for Hortonworks	20
Upgrade Hadoop Distribution Software	20
Digitally Signed Images	22
Requirements for Verifying Digitally Signed Images	22
Verifying a Digitally Signed Image	22
Upgrade of Bare Metal Agent	24
Updating Bare Metal Agent	24
Monitoring Big Data Statistics for MapR Account	24
Configuring Cisco UCS Manager Accounts	24
High-level Workflow to Create an Instant Hadoop Cluster	24
High-level Workflow to Create a Customized Hadoop Cluster	25
Device Connector	25
Configuring Device Connector	25
Viewing Device Connector Properties	26
Launching Cisco UCS Director Express for Big Data from Cisco Intersight	28
Base Platform Pack and System Update Manager	30
Upgrading Base Platform Pack	30
Upgrading the System Update Manager	31
Connector Pack Management	32
Upgrading Connector Packs	33
Upgrade Process Validation and Failure Scenarios	35
Viewing Connector Pack Upgrade Information	36
<hr/>	
CHAPTER 3	Licenses for Cisco UCS Director Express for Big Data
	39
About Licenses	39

Fulfilling the Product Access Key 39

Updating the License 40

Standard License Features 41

CHAPTER 4**Managing Hadoop Accounts 43**

Adding a Hadoop Account 43

Running a Cluster Inventory for a Hadoop Account 44

Purging Big Data Cluster Account Details 45

Rolling Back a Hadoop Cluster for a Hadoop Account 45

Access to Hadoop Managers from Cisco UCS Director Express for Big Data 45

CHAPTER 5**Managing Splunk Accounts 47**

Cisco UCS Director Express for Big Data with Splunk Enterprise 47

Adding a Splunk Account 47

Running a Cluster Inventory for a Splunk Account 49

Rolling Back a Cluster for a Splunk Account 49

Access Splunk Enterprise Monitoring Console User Interface from Cisco UCS Director Express for Big Data 49

CHAPTER 6**Managing Bare Metal OS Accounts 51**

Creating a Local Disk Configuration Policy for Deploying Baremetal OS 51

Creating a Disk Group Policy 52

Deploying a BareMetal OS Account 53

CHAPTER 7**Configuring Big Data IP Pools 55**

Big Data IP Pools 55

Adding a Big Data IP Pool 55

Managing Big Data IP Pools 56

CHAPTER 8**Configuring Cisco UCS Service Profile Templates for Big Data 59**

Cisco UCS Service Profile Templates for Big Data 59

Creating a Cisco UCS Service Profile Template for Big Data 60

Creating a QoS Policy 61

Creating a VLAN Policy 62

Creating a vNIC Policy	63
Creating a Boot Order Policy	65
Creating a BIOS Policy	66
Creating a Local Disk Configuration Policy	68
Editing RAID Policy for Hadoop	69
Editing RAID Policy for Splunk	71
Configuring Local Disk Partitions	73
Creating a Customized Service Profile Template	74
Cloning a Cisco UCS Service Profile Template	75

CHAPTER 9**Configuring and Deploying Hadoop Cluster Deployment Templates 77**

Hadoop Cluster Profile Templates	77
Creating a Hadoop Cluster Profile Template	78
Creating a Services Selection Policy	79
Configuring the Rack Assignment Policy	80
Configuring the HDFS Policy	81
Configuring the CLDB Policy	82
Configuring the YARN Policy	82
Configuring the ZooKeeper Policy	83
Configuring the Kafka Policy	83
Configuring the HBase Policy	84
Configuring the Hive Policy	84
Configuring the Oozie Policy	85
Configuring the Hue Policy	85
Configuring the Spark Policy	85
Configuring the Key-Value Store Indexer Policy	86
Configuring the Solr Policy	86
Configuring the Sqoop Policy	87
Configuring the Impala Policy	87
Configuring the Flume Policy	87
Configuring the PIG Policy	88
Configuring the MAHOUT Policy	88
Configuring the Falcon Policy	89
Configuring the Tez Policy	89

Configuring the Storm Policy	89
Configuring the Ganglia Policy	90
Configuring the SmartSense Policy	90
Cloning a Hadoop Cluster Profile Template	91
Creating a Cluster Deployment Template	91

CHAPTER 10**Managing Hadoop Clusters 93**

Creating an Instant Hadoop Cluster	93
Creating a Customized Hadoop Cluster	97
Creating a Hadoop Cluster Using Workflow	101
Provisioning an Instant and Customized Hadoop Cluster	101
Managing a Hadoop Cluster	103
View Hadoop Cluster Details	105
Viewing a Cluster Snapshot	106
Adding a New Hadoop Service	107
Managing Nodes in a Cluster	107
Delete Node and Delete Node to Bare Metal Actions in Cloudera and Hortonworks	109
Deleting an Unreachable Node from Hadoop Distribution	109
Deleting an Unreachable Cluster Node from MapR Distribution	109
Deleting an Unreachable Cluster Node from Cloudera Distribution	110
Deleting an Unreachable Cluster Node from Hortonworks Distribution	110
Adding Managed Nodes to the Hadoop Cluster	111
Adding Live Nodes to the Hadoop Cluster	111
Adding Bare Metal Nodes to the Hadoop Cluster	112
Adding Disks to the Hadoop Cluster	114
Service Roles	115

CHAPTER 11**Managing Splunk Clusters 117**

Creating an Instant Splunk Cluster	117
Creating a Splunk Cluster Using Workflow	121
Customizing Splunk Cluster Creation	122
Adding Bare Metal Nodes to the Splunk Cluster	126
Deleting an Unreachable Cluster Node from Splunk Distribution	129
Deploying Splunk Cluster with Archival Node and NFS Support	129

Managing a Splunk Cluster 130

CHAPTER 12

Big Data Cluster Configuration Settings 133

Creating an External Database Configuration 133

 Default Databases Used in Hadoop Distribution Services 134

Creating a Hadoop Cluster Configuration Parameters Template 135

Updating Hadoop Cluster Configuration Parameters Template - Post Hadoop Cluster Creation 136

Quality of Service System Classes 136

 Editing QoS System Classes 137

Pre Cluster Performance Testing Settings 139

Approving Hadoop Cluster and Splunk Deployment Workflows 139

Adding NTP Server Details 141

Uploading Required OS and Big Data Software to Cisco UCS Director Bare Metal Agent 141

 Supported Oracle JDK Software Versions 144

 Supported Upgrade Scenarios for Cloudera 144

 Supported Upgrade Scenarios for MapR 144

 Supported Upgrade Scenarios for Hortonworks 145

Cloudera, MapR, and Hortonworks RPMs on Cisco UCS Director Express for Big Data Bare Metal Agent 145

Cloudera and MapR RPMs for Upgrading Hadoop Cluster Distributions 151

Installation of User-Defined Software Post Hadoop Cluster Creation 153

Configuration Check Rules 153

Checking Hadoop Cluster Configuration 154

Fixing Configuration Violations 154

CHAPTER 13

Cisco UCS CPA Workflows 157

Workflows for Big Data 157

About Service Requests for Big Data 160

 Monitoring Service Requests for Big Data 161

 Viewing UCS CPA Workflow Tasks 162

 Viewing UCS CPA Workflow Tasks for BareMetal OS 165

Workflow Customization to Deploy a Hadoop or Splunk Cluster 169

 Deploying a Hadoop or Splunk Cluster Through Workflow Customization 169

 Assigning Big Data Accounts to User Groups 170

Unassigning Big Data Accounts 170

Cloning UCS CPA Workflows 171

CHAPTER 14**Monitoring and Reporting 175**

About Monitoring and Reporting 175

Cisco UCS Director Express for Big Data Dashboard 175

Viewing a Deployed Cluster Report 176

Reports 176

Cluster-specific Metrics Supported per Hadoop Distribution 177

Host-specific Metrics Supported per Hadoop Distribution 178

CHAPTER 15**Proactive Status Monitoring and Diagnostics 179**

Aggregate CPU, Disk, and Network Bandwidth Utilization 179

Monitoring Aggregate CPU, Disk, and Network Bandwidth Utilization 180

Monitoring Top Jobs Based on CPU Utilization and Time 180

Performance Metrics for CPU, Disk, and Network 181

Viewing CPU, Disk, and Network Statistics for a Hadoop Cluster 181

Analyzing Performance Bottlenecks Through Historical Metrics 182

Setting Alerts for Hadoop Cluster Service Failures 183

Types of Disk and Network Failure Alerts 184

Setting Alerts for Disk and Network Failures 185

Setting Disk Utilization Threshold Alerts 186



Preface

- [Audience, on page xi](#)
- [Conventions, on page xi](#)
- [Related Documentation, on page xiii](#)
- [Documentation Feedback, on page xiii](#)
- [Communications, Services, and Additional Information, on page xiii](#)

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director Express for Big Data and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .

Text Type	Indication
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: <http://www.cisco.com/go/unifiedcomputing/c-series-doc>.



Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed Information for this Release

- [New and Changed Information in Release 3.7, on page 1](#)
- [New and Changed Information in Release 3.7\(1.0\), on page 1](#)
- [New and Changed Information in Release 3.7\(2.0\), on page 2](#)
- [New and Changed Information in Release 3.7\(2.1\), on page 2](#)
- [New and Changed Information in Release 3.7\(4.0\), on page 2](#)

New and Changed Information in Release 3.7

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Director Express for Big Data, Release 3.7

Feature	Description	Where Documented
Updates to Overview chapter	Added the Splunk Distribution and Hadoop Distribution support details.	Overview
Updates to Configuring and Deploying Hadoop Cluster Deployment Templates chapter	Added the SmartSense support details for Hortonworks.	Configuring and Deploying Hadoop Cluster Deployment Templates

New and Changed Information in Release 3.7(1.0)

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

- Enhancement to OS Disk Partition—The Local Disk Configuration policy is enhanced to support the OS disk partition value to be greater than 50 GB. However, we recommend that you allocate the OS disk partition value based on the available actual disk size.

New and Changed Information in Release 3.7(2.0)

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

- Support for Cloudera 6.1

New and Changed Information in Release 3.7(2.1)

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

- Support for Deployment of Linux OS on Multiple Server Nodes

New and Changed Information in Release 3.7(4.0)

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

- Support for monitoring the big data statistics for MapR account



CHAPTER 2

Overview

This chapter contains the following sections:

- [Cisco UCS Director Express for Big Data, on page 4](#)
- [Cisco UCS Integrated Infrastructure for Big Data, on page 4](#)
- [Managing Cisco UCS Director and Cisco UCS Director Express for Big Data Personalities, on page 4](#)
- [Installing Cisco UCS Director Express for Big Data on VMware vSphere, on page 10](#)
- [Installing Cisco UCS Director Express for Big Data Bare Metal Agent on VMware vSphere, on page 12](#)
- [Downloading Cisco UCS Storage and Network Drivers, on page 14](#)
- [NTP Server Configuration on Cisco UCS Director Express for Big Data Bare Metal Agent, on page 15](#)
- [Adding Oracle JDK Software Versions to Bare Metal Agent, on page 16](#)
- [Cisco Server Support for Big Data Cluster Deployments, on page 16](#)
- [Cisco Server Support for Splunk Enterprise Deployments, on page 17](#)
- [Adding a New Red Hat Version for Hadoop Cluster, on page 17](#)
- [Supported Hadoop Distributions, on page 18](#)
- [Supported Splunk Distribution, on page 19](#)
- [Supported Oracle JDK Software Versions, on page 19](#)
- [Upgrade Hadoop Distribution Software, on page 20](#)
- [Digitally Signed Images, on page 22](#)
- [Upgrade of Bare Metal Agent, on page 24](#)
- [Updating Bare Metal Agent, on page 24](#)
- [Monitoring Big Data Statistics for MapR Account, on page 24](#)
- [Configuring Cisco UCS Manager Accounts, on page 24](#)
- [High-level Workflow to Create an Instant Hadoop Cluster, on page 24](#)
- [High-level Workflow to Create a Customized Hadoop Cluster, on page 25](#)
- [Device Connector, on page 25](#)
- [Launching Cisco UCS Director Express for Big Data from Cisco Intersight, on page 28](#)
- [Base Platform Pack and System Update Manager, on page 30](#)
- [Connector Pack Management, on page 32](#)
- [Upgrading Connector Packs, on page 33](#)
- [Upgrade Process Validation and Failure Scenarios, on page 35](#)
- [Viewing Connector Pack Upgrade Information, on page 36](#)

Cisco UCS Director Express for Big Data

Cisco UCS Director Express for Big Data is a single-touch solution within Cisco UCS Director that automates deployment of Big Data infrastructure. Cisco UCS Director Express for Big Data provides a single management pane across physical infrastructure and across Hadoop and Splunk Enterprise software. It supports key Hadoop distributions, including Cloudera, MapR, and Hortonworks.

Cisco UCS Director Express for Big Data delivers end-to-end automation of Hadoop cluster deployment, allowing you to spin up and expand clusters on-demand. The physical infrastructure configuration is handled automatically, with minimal user input. The configuration includes compute, internal storage, network, and installation of operating system, Java packages, and Hadoop, along with the provisioning of Hadoop services. This is achieved through Cisco UCS service profiles wherein both the physical infrastructure and Hadoop configuration are incorporated into a Hadoop cluster deployment profile.

Cisco UCS Director Express for Big Data also delivers end-to-end automation of Splunk cluster deployment, with minimal user input. This is achieved through Cisco UCS service profiles wherein both the physical infrastructure and Splunk configuration are incorporated into a Splunk cluster deployment profile.

Cisco UCS Integrated Infrastructure for Big Data

Cisco UCS Integrated Infrastructure for Big Data is an industry leading architecture designed to meet various Big Data workloads. It scales as processing and storage needs grow without increasing management challenges and delivers predictable performance along with reduced total cost of ownership (TCO).

Cisco UCS Integrated Infrastructure consists of the following components:

- Cisco UCS Fabric Interconnects
- Cisco UCS Fabric Extenders
- Cisco UCS C-Series Rack-Mount Servers
- Cisco UCS S-Series Storage Servers
- Cisco UCS Virtual Interface Cards (VICs)
- Cisco UCS Manager

You can read more about the Cisco UCS Integrated Infrastructure for Big Data in the [Data Center Designs Cloud Computing - Design Zone for Big Data](#).

Managing Cisco UCS Director and Cisco UCS Director Express for Big Data Personalities

Cisco UCS Director is the default personality made available after deployment, but you can choose to use only Cisco UCS Director Express for Big Data, or use both Cisco UCS Director and Cisco UCS Director Express for Big Data.

You can manage personalities here: **Administration > License > License Keys > Manage Personalities**.

**Important**

You must first configure the optimized multi-node setup and then select **Cisco UCS Director Express for Big Data** or **Cisco UCS Director and Cisco UCS Director Express for Big Data** personality. We also recommend that you do not change the personality in the appliance that is already in use. For more information on how to configure the multi-node, see [Cisco UCS Director Multi-Node Installation and Configuration Guide](#).

Table 2: Personality Switch Behavior

Personality Selection	Cisco UCS Director Features	Cisco UCS Director Express for Big Data Features
Cisco UCS Director (Default)	Yes	No
Cisco UCS Director Express for Big Data	No	Yes
Cisco UCS Director and Cisco UCS Director Express for Big Data	Yes	Yes

**Note**

Depending on the personality, you start with and the personality selection, Cisco UCS Director and Cisco UCS Director Express for Big Data features are enabled or disabled with the restart of services on the appliance.

Creating User Roles

You can create user roles that are specific to Cisco UCS Director Express for Big Data, and define menu settings and permissions for those users. Ensure that you create a group before you add users to any role.

**Note**

You can determine the default roles only if the **Default Role** column on the **User Roles** page is marked with **Yes** in the system. Navigate to **Administration > System > User Roles**.

For example, you can create the following user roles, and then create users with those role:

- HadoopUser—A Hadoop user
- HadoopAdmin—A Hadoop administrator

For more information on Managing Users and Groups, see the latest *Cisco UCS Director Administration Guide*.

Hadoop Administrator Permissions

A Hadoop administrator can:

- Read—Permission to only read a file.
- Write—Permission to read, write, and modify a file.

- Read/Write—Permission to read and/or write to a file

The following table shows a list of operations that a Hadoop administrator can do:

Operations	Permissions	
	Read	Write
Virtual Computing	Yes	Yes (Only VM Management Actions)
VM Label	Yes	—
Assign VM to VDC	Yes	—
Virtual Storage	Yes	Yes
Virtual Network	Yes	Yes
Physical Computing	Yes	Yes
Physical Storage	Yes	Yes
Physical Network	Yes	Yes
Group Service Request	Yes	Yes
Approver Service Request	Yes	Yes
Budgeting	Yes	Yes
Resource Accounting	Yes	—
Chargeback	Yes	—
System Admin	Yes	Yes
Users and Groups	Yes	Yes
Virtual Accounts	Yes	Yes
Catalogs	Yes	Yes
VDC	Yes	Yes
Computing Policy	Yes	Yes
Storage Policy	Yes	Yes
Network Policy	Yes	Yes
Service Delivery	Yes	Yes
Resource Limit Report	Yes	Yes
Group Users	Yes	Yes

Operations	Permissions	
	Read	Write
Cloudsense Reports	Yes	Yes
Cloudsense Assessment Reports	Yes	Yes
Orchestration	Yes	Yes
Open Automation Modules	Yes	Yes
CS Shared Reports	Yes	Yes
Remote VM Access	—	Yes
Mobile Access Settings	Yes	Yes
End User Chargeback	Yes	—
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Big Data Infra	Yes	—
Big Data Accounts	—	Yes
Big Data Cluster Management	—	Yes
Big Data Node Management	—	Yes
Big Data Performance Test	—	Yes
Big Data Service Management	—	Yes
Big Data Role Management	—	Yes
Big Data UCS SP Template	—	Yes
Big Data Hadoop Profile Template	—	Yes
Big Data Hadoop Deploy Template	—	Yes
Big Data Cluster Deployment	—	Yes
Big Data License Upload	—	Yes
Big Data Configuration Parameters Template	—	Yes
Big Data Faults	—	Yes
Big Data Settings - QoS	—	Yes
Big Data Settings - IP Pool	—	Yes

Operations	Permissions	
	Read	Write
Big Data Settings - Pre_Cluster Sanity	—	Yes
Big Data Settings - Hadoop Software Upload	—	Yes
Big Data Settings - Configuration Check Rules	—	Yes
REST API access	Yes	Yes
Allow Change Password - Users	Yes	Yes

Hadoop User Permissions

A Hadoop user can:

- Read—Permission to only read a file.
- Write—Permission to read, write, and modify a file.
- Read/Write—Permission to read and/or write to a file.

The following table shows a list of operations that a Hadoop user can do:

Operations	Permissions	
	Read	Write
Virtual Computing	Yes	—
VM Label	Yes	—
Assign VM to VDC	Yes	—
Virtual Storage	Yes	—
Virtual Network	Yes	—
Physical Computing	Yes	—
Physical Storage	Yes	—
Physical Network	Yes	—
Group Service Request	Yes	Yes
Approver Service Request	Yes	Yes
Budgeting	Yes	—
Resource Accounting	Yes	—

Operations	Permissions	
	Read	Write
Chargeback	Yes	—
System Admin	Yes	—
Users and Groups	Yes	—
Virtual Accounts	Yes	—
Catalogs	Yes	—
VDC	Yes	—
Computing Policy	Yes	—
Storage Policy	Yes	—
Network Policy	Yes	—
Service Delivery	Yes	—
Resource Limit Report	Yes	—
Group Users	Yes	—
Cloudsense Reports	Yes	—
Cloudsense Assessment Reports	Yes	—
Orchestration	—	—
Open Automation Modules	—	—
CS Shared Reports	—	—
Remote VM Access	—	—
Mobile Access Settings	—	—
End User Chargeback	—	—
Resource Groups	—	—
Tag Library	—	—
Big Data Infra	Yes	—
Big Data Accounts	—	—
Big Data Cluster Management	—	—
Big Data Node Management	—	—
Big Data Performance Test	—	—

Operations	Permissions	
	Read	Write
Big Data Service Management	—	—
Big Data Role Management	—	—
Big Data UCS SP Template	—	—
Big Data Hadoop Profile Template	—	—
Big Data Hadoop Deploy Template	—	—
Big Data Cluster Deployment	—	—
Big Data License Upload	—	—
Big Data Configuration Parameters Template	—	—
Big Data Faults	—	—
Big Data Settings - QoS	—	—
Big Data Settings - IP Pool	—	—
Big Data Settings - Pre_Cluster Sanity	—	—
Big Data Settings - Hadoop Software Upload	—	—
Big Data Settings - Configuration Check Rules	—	—
REST API access	Yes	—
Allow Change Password - Users	—	—

Installing Cisco UCS Director Express for Big Data on VMware vSphere

The Cisco UCS Director, Release 6.5 OVF file includes Cisco UCS Director Express for Big Data, Release 3.5.



Note We recommend that you use VMware vCenter for OVF deployment. VMware vCenter versions 5.x and above are supported. OVF deployment wizards support only IPv4 addresses. If you require IPv6, deploy the OVF with IPv4 addresses and then use the ShellAdmin to configure IPv6 addresses.

Before you begin

You need administrator privileges to connect to VMware vCenter. Cisco UCS Director requires a user account with system administrator privileges to discover, manage and automate VMware vCenter configuration from Cisco UCS Director. These operations include creating, deleting and modifying VMs, ESXi hosts and clusters, datastores and datastore clusters, standard and DV switches, and virtual network port groups.



Note If you do not want to use DHCP, you need the following information: IPv4 address, subnet mask, and default gateway.

Step 1 Log in to VMware vSphere Client.

Step 2 In the **Navigation** pane, choose the **Data Center** where you want to deploy Cisco UCS Director.

See [Cisco UCS Director Installation on VMware vSphere](#).

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the **Source** pane, do one of the following to choose your OVF source location:

- Click **Browse**, navigate to the location where you downloaded the OVF, choose the file, and click **Open**.
- Replace *FQDN* (Fully Qualified Domain Name) with the path to the URL on your local area network where the OVF is stored, including the IP address or domain name, and click **Next**.

Step 5 In the **OVF Template Details** pane, verify the details, and click **Next**.

Step 6 In the **Name and Location** pane, do the following:

- a) In the **Name** field, edit the default VM name.
- b) From the **Inventory Location** area, choose the inventory location where Cisco UCS Director Express for Big Data is being deployed, and click **Next**.

Note If you chose a Data Center in Step 2, option b might not be available.

- c) Click **Next**.

Step 7 In the **Resource Pool** pane, choose the required host, cluster, or resource pool, and click **Next**.

Step 8 In the **Disk Format** pane, choose one of the following options and click **Next**:

- **Thick Provisioned (Lazy Zeroed)** format—To allocate storage immediately in thick format. This is the recommended format. All Cisco UCS Director Express for Big Data performance data is verified with this format.
- **Thick Provisioned (Eager Zeroed)** format—To allocate storage in thick format. It might take longer to create disks using this option.
- **Thin Provisioned** format—To allocate storage on demand as data is written to disk.

Important We recommend that you do not choose the **Thin Provisioned** format.

Step 9 In the **Properties** pane, enter the following information and click **Next**:

- **Management IP Address**—The management IP address to be used for eth0. If your network uses DHCP, leave the default value of 0.0.0.0.
- **Management IP Subnet Mask**—The management IP subnet mask to be used for eth0. If your network uses DHCP, leave the default value of 0.0.0.0.

- **Gateway IP Address**

Step 10 In the **Ready to Complete** pane, do the following:

- a) Verify the options that you chose in the previous panes.
- b) Check **Power on after deployment**.

If you do not check this box, you must power on the VM manually after deployment.

- c) Click **Finish**.

Step 11 After the appliance has booted up, copy and paste the Cisco UCS Director Express for Big Data management IP address (from the IP address that is shown) into a supported web browser to access the **Login** page.

Step 12 On the **Login** page, enter `admin` as the username and `admin` for the login password.

Note We recommend that you change the default admin password after this initial login.

Step 13 Choose **Administration > License**.

Step 14 On the **License** page, click **License Keys**.

Step 15 Click **Manage Personalities**.

Step 16 On the **Personality Configuration** screen, check the required personalities.

You can check either **UCSD** or **Big Data** or both personalities if required.

Step 17 Click **Submit**.

Step 18 Log in to the Cisco UCS Director VM console with the default shelladmin credentials (for example, shelladmin/changeme) to apply the selected personalities.

- a) Follow the prompts to change the default password.
 - b) From the **Cisco UCS Director Shell Menu**, choose **Stop Services** and press **Enter**.
 - c) Press **Enter** to return to the main menu.
 - d) From the **Cisco UCS Director Shell Menu**, choose **Start Services** and press **Enter**.
 - e) Press **Enter** to return to the main menu.
 - f) To verify that all services have started, choose `Display services status`.
 - g) Choose **Quit**.
-

Installing Cisco UCS Director Express for Big Data Bare Metal Agent on VMware vSphere

Before you begin

- You must have system administrator privileges for VMware vSphere or vCenter.
- If you want to use a static IP address rather than DHCP, you must know the following information:
 - IP address
 - Subnet mask
 - Default gateway

-
- Step 1** On the Cisco.com download site for Cisco UCS Director, download Cisco UCS Director Bare Metal Agent and unzip the OVF file.
- Step 2** Log in to VMware vSphere Client.
- Step 3** In the **Navigation** pane, click the vSphere host on which you want to deploy Cisco UCS Director Express for Big Data Bare Metal Agent.
- Step 4** Choose **File > Deploy OVF Template**.
- Step 5** On the **Source** screen of the **Deploy OVF Template** window, do one of the following to choose your OVF source location and then click **Next**:
- If the OVF file is stored on your local computer, browse to the location, choose the file, and click **Open**.
 - If the OVF file is stored on a server on your local area network, enter the location of the file including the IP address or fully qualified domain name of the server.
- Step 6** On the **OVF Template Details** screen, verify the details and click **Next**.
- Step 7** On the **End User License Agreement** screen, review the license agreement and click **Accept**.
- Step 8** On the **Name and Location** screen, do the following:
- a) In the **Name** field, enter a unique name for the VM.
 - b) In the **Inventory Location** area, choose the location where you want the VM to reside.
 - c) Click **Next**.
- Step 9** On the **Storage** screen, choose the storage location for the VM and click **Next**.
- Step 10** On the **Disk Format** screen, click **Next** to accept the default radio button for **Thick Provision (Lazy Zeroed)** format.
- Step 11** On the **Network Mapping** screen, choose the network for the VM and click **Next**.
- Step 12** On the **Properties** screen, do the following:
- a) Configure the IP addresses for both the NICs (eth0 and eth1) that you want to assign, as follows:
 - To use DHCP to assign the IP addresses, leave the default of 0.0.0.0 in the IP address fields.
 - To use static IP addresses, enter the desired IP addresses in the IP address fields. If you only want to configure one NIC, only complete one set of IP addresses and leave the second set at the default.
 - b) Click **Next**.
- Step 13** On the **Ready to Complete** screen, verify the settings and click **Finish**.
- A message appears to indicate that Cisco UCS Director Express for Big Data Bare Metal Agent is being deployed.
- Step 14** Log in to the Cisco UCS Director Express for Big Data Bare Metal Agent server with root privileges, and check if you are able to ping the Cisco UCS Director Express for Big Data Bare Metal Agent server.
- Step 15** In the **Navigation** pane, right-click the Cisco UCS Director Express for Big Data Bare Metal Agent server and choose **Edit Settings**.
- a) Choose the **Resources** tab.
 - b) In the **Resource Allocation** window, set CPU and Memory **Reservation** settings to the maximum.
 - c) Click **OK**.
- Step 16** Power on the VM.
-

Downloading Cisco UCS Storage and Network Drivers

From Cisco UCS Director, Release 6.6.1.0, we are not packaging the Cisco UCS storage and network drivers along with Cisco UCS Director Express for Big Data. We recommend you to download the relevant drivers using the UCS Hardware and Software Compatibility tool.

Step 1 Go to UCS Hardware and Software Compatibility tool.

<https://ucshcltool.cloudapps.cisco.com/public/>

Step 2 Click **Search**.

Step 3 Click the required radio button. For example, click the **Server** radio button to identify the compatible software for the Cisco UCS server.

Step 4 On the **Search Options** section, choose the required **Server Type**, **Server Model**, **Processor Version**, **Operating System**, and **Operating System Version** from the drop-down menus.

Step 5 On the **Search Results** section, refine the search results by checking or unchecking checkboxes next to **Product Category** (Adapters) and **UCS Server Firmware** version number

Step 6 Click **Driver ISO** under **Details** section.

Note By clicking the **View Notes** and **Install & Upgrade Guides** links under **Documents**, you can view the note details and install and upgrade details.

Step 7 Download a compatible Driver ISO file from the **Software Download** window.

Step 8 Extract the Storage ISO files.

Note To extract the ISO files, navigate to `Storage > Intel > C600 > RHEL` or `Storage > LSI > C600 > RHEL` and choose the required OS. For example,

- For M.2 flash/devices—`Storage > Intel > C600 > RHEL > RHEL7.5 > megasr-18.0*.iso`
- For SAS HDD—`Storage > LSI > UCSC-RAID-M5 > RHEL > RHEL7.5 > megaraid_sas-07.0*.iso`. You need to extract the `iso.gz` file, locate the `.iso` file, and rename the `.iso` file name with `iso.gz` file name.

Step 9 Extract the Network ISO file.

Note To extract the ISO files, navigate to `Network > Cisco > VIC > RHEL` and choose the required OS and copy the `.rpm` file. For example, `Network > Cisco > VIC > RHEL > RHEL7.5`

Step 10 Login to Bare Metal Agent through VM Console or SSH client to access the CLI.

Step 11 Create directories for the operating system in the `/opt/cnsaroot/bd-sw-rep` directory of the Bare Metal Agent VM.

```
mkdir /opt/cnsaroot/bd-sw-rep/RHEL7.4_MEGARAID_SAS_DRIVERS
```

```
mkdir /opt/cnsaroot/bd-sw-rep/RHEL7.4_KMOD_ENIC_DRIVERS
```

```
mkdir /opt/cnsaroot/bd-sw-rep/RHEL7.4_MEGASR_DRIVERS
```

Note We recommend that you make the directory name descriptive enough that you can identify the operating system of the images within it. For example, we recommend that you name the directory `RHEL7.5_MEGASR_DRIVERS`.

The `RHEL7.5_MEGARAID_SAS_DRIVERS`, `RHEL7.5_KMOD_ENIC_DRIVERS`, and `RHEL7.5_MEGASR_DRIVERS` directories are used to store the operating system image files.

Step 12 Execute `ln -s <<path of the original iso file>> <<target link name>>` to provide links to the ISO images.

For example,

```
ln -s /opt/cnsaroot/bd-sw-rep/RHEL7.4_MEGARAID_SAS/megaraid_sas-07.703.06.00_el7.4-1.x86_64.iso
megaraid_sas_drivers_softlink_to_original.iso
```

```
ln -s /opt/cnsaroot/bd-sw-rep/RHEL7.4_MEGASR_DRIVERS/megasr-18.01.2017.1219-1-rhel74-x86_64.iso
megasr_drivers_softlink_to_original.iso
```

```
ln -s /opt/cnsaroot/bd-sw-rep/RHEL7.4_KMOD_ENIC_DRIVERS/kmod-enic-2.3.0.44-rhel7u4.el7.x86_64.rpm
kmod_enic_drivers_softlink_to_original.rpm
```

Note The links to the `RHEL7.5_KMOD_ENIC_DRIVERS` should refer to the rpm file, and the `MEGASR` and `MEGARAID` should refer to the iso files.

Note We recommend that you make the directory name based on the operating system used for the cluster deployment. For example, `CentOS7.5_MEGASR_DRIVERS`, `CentOS7.5_MEGARAID_SAS`, and `CentOS7.5_KMOD_ENIC_DRIVERS` directories are used to store the operating system driver image file. You use the same set of RHEL drivers for CentOS as well.

NTP Server Configuration on Cisco UCS Director Express for Big Data Bare Metal Agent

You can configure Cisco UCS Director Express for Big Data Bare Metal Agent to have its clock synchronized to an external NTP server. This ensures that the correct calendar time is maintained on the Bare Metal Agent.

Ensure that you synchronize Cisco UCS Director Express for Big Data and Cisco UCS Director Express for Big Data Bare Metal Agent before you deploy any Hadoop cluster. It is recommended that you also synchronize Cisco UCS Manager and Cisco UCS Director Express for Big Data on the configured NTP server.

Follow the steps to locate the `ntp_server_config.sh`:

- Locate `/opt/cnsaroot/bigdata_templates/ntp_server_config.sh`
- Add execute permissions (`chmod+x ntp_server_config.sh`)
- Execute (`./ntp_server_config.sh <ntp_server_ip or hostname>`) on the Cisco UCS Director Express for Big Data Bare Metal Agent server.

Adding Oracle JDK Software Versions to Bare Metal Agent

You can upload Oracle JDK software and use Oracle JDK for all Hadoop distributions (Cloudera, MapR, and Hortonworks) through an instant Hadoop cluster and customized Hadoop cluster creation actions. You can also add new nodes to the existing cluster and support upgrading existing clusters.

-
- Step 1** Log in to the Cisco UCS Director Bare Metal Agent server.
- Step 2** Navigate to **Solutions > Big Data > Settings** and click the **Software Catalogs** tab to create JDK software version folder names for each version.
- Step 3** Copy JDK files in .rpm or .gz format to the respective version folders.
- Step 4** On the menu bar, choose **Administration > Integration** to track software uploads.
- Step 5** Click the **Change Record** tab to track the software upload in progress and verify if completed, failed, or timeout.
-

Cisco Server Support for Big Data Cluster Deployments

The table shows Cisco UCS Director Express for Big Data compatibility with Cisco UCS hardware and software. This table does not reflect the compatibility between Cisco UCS hardware and software.

For information regarding Cisco UCS compatibility, see the [Cisco UCS Hardware and Software interoperability Matrices](#) for the appropriate releases.



Note All Cisco UCS Director Express for Big Data functionality may not be available across all supported Cisco UCS software versions. Certain features may not be available in older versions of Cisco UCS software.

Software Components	Certified Versions	Supported Versions
Cisco UCS Manager	Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Releases: <ul style="list-style-type: none"> • 4.0(4c) (Cisco UCS Director Express for Big Data is supported with fourth generation fabric interconnect i.e. Cisco UCS 6454.) • 3.2(3a) 	Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Releases: <ul style="list-style-type: none"> • 4.x • 3.2(x) • 3.1(x) • 3.0(x) • 2.2(x)

Software Components	Certified Versions	Supported Versions
Cisco UCS C-Series Rack-Mount Servers (Managed by Cisco UCS Manager)	Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Release 3.2(2d)	<p>Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Release 3.1(2b), Release 3.1(2f), and Release 3.2(2d) for M3 Rack servers</p> <p>Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Release 3.1(2b), Release 3.1(2f), and Release 3.2(2d) for M4 Rack servers and Storage servers</p> <p>Cisco UCS Infrastructure Bundle and Cisco UCS Manager Software Bundle, Release 3.2(2d) for M5 Rack servers</p>

Cisco Server Support for Splunk Enterprise Deployments

The table shows Cisco UCS Director Express for Big Data compatibility with Cisco UCS hardware and software. This table does not reflect the compatibility between Cisco UCS hardware and software.

For information regarding Cisco UCS compatibility, see the [Cisco UCS Hardware and Software interoperability Matrices](#) for the appropriate releases.



Note All Cisco UCS Director Express for Big Data functionality may not be available across all supported Cisco UCS software versions. Certain features may not be available in older versions of Cisco UCS software.

Software Components	Certified Versions	Supported Versions
Cisco UCS Manager		
Cisco UCS C-Series Rack-Mount Servers (Managed by Cisco UCS Manager)		

Adding a New Red Hat Version for Hadoop Cluster

For more information on uploading supported Red Hat Enterprise Linux versions, see Chapter 12, Managing Hadoop and Splunk Clusters in *Cisco UCS Director Express for Big Data Management Guide*.

- Step 1** On the menu bar, choose **Solutions > Big Data > Settings**.
- Step 2** Click the **Software Catalogs** tab.
- Step 3** Click **Add**.

- Step 4** Click **Upload**.
- Step 5** Choose the target Cisco UCS Director Express for Big Data Bare Metal Agent from the **Target BMA** drop-down list.
- Step 6** Check the **Restart BMA Services** check box to restart Cisco UCS Director Express for Big Data Bare Metal Agent after uploading the required files.
- Step 7** To verify that the new Red Hat version (operating system software) is available in the Cisco UCS Director Express for Big Data server, perform the following:
- Log in to the Cisco UCS Director Express for Big Data user interface.
 - On the menu bar, choose **Administration > Physical Accounts**.
 - Click the **Bare Metal Agents** tab.
- You can find the new Red Hat version listed in the **Image Catalogs** column of the **Bare Metal Agents** report.

New RHEL Version

Red Hat Enterprise Linux 7.2

Download the following file:

- `rhel-server-7.2-x86_64-dvd.iso` from [Red Hat Enterprise Linux](#)

Supported Hadoop Distributions

Cisco UCS Director Express for Big Data supports the following Hadoop distributions:

Hadoop Distribution	Supported Hadoop Distribution Version
Cloudera	5.14.0, 5.15.0, 6.0.0, and 6.1.0 ¹
MapR	5.2.2, 6.0.0, and 6.1.0
Hortonworks	2.6.4 and 3.0.0

¹ Supported with Cisco BigData Express Connector Pack release 3.7.1.1



Note For more information on the supported JDK versions and upgrade scenarios, see Cloudera, MapR, and Hortonworks sites.



Important Upgrade is not supported for the following:

- Cloudera 5.14.0 to Cloudera 6.0
- Cloudera 5.15.0 to Cloudera 6.0
- Hortonworks 2.6.4 to Hortonworks 3.0.0
- MapR 5.2.2 to MapR 6.1.0
- MapR 6.0.0 to MapR 6.1.0

Supported Splunk Distribution

Cisco UCS Director Express for Big Data supports the following Splunk distribution:

Splunk Distribution	Supported Splunk Distribution Version
Splunk	7.0.0, 7.1.3, and 7.2.0



Note For more information on the upgrade scenarios, see Splunk Enterprise site.



Important Upgrade is not supported for the following:

- Splunk 7.0.0 to Splunk 7.2.0
- Splunk 7.1.3 to Splunk 7.2.0

Supported Oracle JDK Software Versions

This section lists the supported Oracle JDK software versions:

Supported Upgrade Scenarios for Cloudera

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.5.0, JDK 1.8
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.6.x, JDK 1.8
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.8.x, JDK 1.8
Cloudera Enterprise 5.6.x, JDK 1.8	Cloudera Enterprise 5.8.x, JDK 1.8

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Cloudera Enterprise 5.8.0, JDK 1.8	Cloudera Enterprise 5.10.0, JDK 1.8
Cloudera Enterprise 5.8.0, JDK 1.8	Cloudera Enterprise 5.11.1, JDK 1.8
Cloudera Enterprise 5.8.2, JDK 1.8	Cloudera Enterprise 5.13.1, JDK 1.8
Cloudera Enterprise 5.11.1, JDK 1.8	Cloudera Enterprise 5.13.1, JDK 1.8



Note For more information on the supported JDK versions, see Cloudera site.

Supported Upgrade Scenarios for MapR

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
MapR 5.2.1, JDK 1.8	MapR 6.0.0, JDK 1.8
MapR 5.0.0, JDK 1.8	MapR 5.1.0, JDK 1.8
MapR 4.0.2, JDK 1.8	MapR 5.2.0, JDK 1.8



Note For more information on the supported JDK versions, see MapR site.

Supported Upgrade Scenarios for Hortonworks

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Hortonworks 2.2, JDK 1.7	Hortonworks 2.3, JDK 1.8
Hortonworks 2.2, JDK 1.7	Hortonworks 2.4, JDK 1.8



Note For more information on the supported JDK versions, see Hortonworks site.

Upgrade Hadoop Distribution Software

You can upgrade to the latest Hadoop distributions from the following Hadoop distributions:

Table 3: Cloudera

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Cloudera-5.0.1	Cloudera-5.4.1
Cloudera-5.0.6	Cloudera-5.4.1
Cloudera-5.2.0	Cloudera-5.4.1
Cloudera-5.2.1	Cloudera-5.4.1
Cloudera-5.3.0	Cloudera-5.4.1
Cloudera-5.4.x	Cloudera-5.6.x
Cloudera-5.8.0	Cloudera-5.10.0
Cloudera-5.8.0	Cloudera-5.11.1
Cloudera-5.8.2	Cloudera-5.13.1
Cloudera-5.8.2	Cloudera-5.14.0
Cloudera-5.11.1	Cloudera-5.13.1
Cloudera-5.11.1	Cloudera-5.14.0

Table 4: MapR

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
MapR-4.0.2	MapR-4.1.0
MapR-4.0.2	MapR-5.0.0
MapR-4.1.0	MapR-5.0.0
MapR-5.2.0	MapR-6.0.0

Table 5: Hortonworks

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Hortonworks-2.2 (ambari-1.7.0-centos6.tar.gz)	Hortonworks-2.3 Note Download <code>ambari-2.1.1-centos6.tar.gz</code> from http://public-repo-1.hortonworks.com/ambari/centos6

Digitally Signed Images

Cisco UCS Director Express for Big Data images are delivered in digitally signed zip files. These signed zip files are wrapped in a container zip file that includes the following:

- Digitally signed zip file—Contains the Cisco UCS Director Express for Big Data installation or upgrade image
- Verification program—Verifies the certificate chain and signature. During certificate chain validation, the program verifies the authenticity of the end-entity certificate using Cisco's SubCA and root CA certificates. Then, the authenticated end-entity certificate is used to verify the signature.
- Digital signature file—Contains the signature that you can verify before installation or upgrade.
- Certificate file—Enables you to verify the digital signature. This Cisco-signed x.509 end-entity certificate contains a public key that can be used to verify the signature. This certificate is chained to the Cisco root posted on <http://www.cisco.com/security/pki/certs/crcam2.cer>.
- ReadMe file—Provides the information and instructions required to verify the digitally signed zip file.

Verify the image offline. Once the image is verified, you can begin the installation or upgrade of Cisco UCS Director Express for Big Data.

Requirements for Verifying Digitally Signed Images

Before you verify a Cisco UCS Director Express for Big Data digitally signed image, ensure that you have the following on your local machine:

- Connectivity to <https://www.cisco.com> during the verification process
- Python 2.7.4
- OpenSSL

Verifying a Digitally Signed Image

Before you begin

Download the Cisco UCS Director Express for Big Data image from [Cisco.com](https://www.cisco.com).

Step 1 Unzip the file you downloaded from [Cisco.com](https://www.cisco.com) and verify that it contains the following files:

- ReadMe file
- Digitally signed zip file, for example `CUCSD_6_6_0_0_66365_VMWARE_GA.zip`, `CUCSD_6_6_0_0_66717_HYPERV_GA.zip`, or `cucsd_patch_6_6_0_0_66365.zip`
- Certificate file, for example `UUCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer`

- Digital signature generated for the image, for example `CUCSD_6_6_0_0_66365_VMWARE_GA.zip.signature`, `CUCSD_6_6_0_0_66717_HYPERV_GA.zip.signature`, or `cucsd_patch_6_6_0_0_66365.zip.signature`
- Signature verification program, for example `cisco_x509_verify_release.py`

Step 2 Review the instructions in the ReadMe file.

Note If there are any differences between these instructions and those in the ReadMe, follow the ones in the ReadMe.

Step 3 Run the signature verification program from the directory where you have unzipped the downloaded content.

Example: Signature Verification for Upgrade Patch

```
python ./cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i cucsd_patch_6_6_0_0_66365.zip -s cucsd_patch_6_6_0_0_66365.zip.signature -v dgst -sha512
```

Example: Signature Verification for VMware OVF Installation

```
python ./cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i CUCSD_6_6_0_0_66365_VMWARE_GA.zip -s CUCSD_6_6_0_0_66365_VMWARE_GA.zip.signature -v dgst -sha512
```

Example: Signature Verification for Hyper-V VHD Installation

```
python ./cisco_x509_verify_release.py -e UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
-i CUCSD_6_6_0_0_66717_HYPERV_GA.zip -s CUCSD_6_6_0_0_66717_HYPERV_GA.zip.signature -v dgst -sha512
```

Step 4 Review the output and ensure that the verification has succeeded.

Example: Expected Output for Upgrade

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of cucsd_patch_6_6_0_0_66365.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for VMware OVF Installation

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of CUCSD_6_6_0_0_66365_VMWARE_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

Example: Expected Output for Hyper-V VHD Installation

```
Downloading CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully downloaded and verified crcam2.cer.
Downloading SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully downloaded and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully verified the signature of CUCSD_6_6_0_0_66717_HYPERV_GA.zip using
UCS_GENERIC_IMAGE_SIGNING-CCO_RELEASE.cer
```

What to do next

Install or upgrade Cisco UCS Director Express for Big Data.

Upgrade of Bare Metal Agent

For detailed information on upgrading Bare Metal Agent, see the [Cisco UCS Director Upgrade Guide](#).

Updating Bare Metal Agent

A new system task (Update BMA Appliance Task) is created within the account. Navigate to the Big Data Tasks folder here: **Administration > System > System Tasks**. The system scheduler connects to all Bare Metal Agents that are currently managed, performs a version check, stops services, pushes the required updates, and starts the services. This task is performed when

- the Cisco Big Data Express connector pack is upgraded.
- a BMA is added.

**Note**

If any of the BMA goes down and update fails, you should add the BMA to kickstart the process again. You can use the system task history to check for any failures and add the BMA again to trigger the process.

Monitoring Big Data Statistics for MapR Account

A new system task (monitor) is created within the MapR account. Navigate to the Big Data Tasks folder here: **Administration > System > System Tasks**. The system task connects to the MapR account and generates the relevant statistical data based on your requirement.

Configuring Cisco UCS Manager Accounts

Each Cisco UCS Manager account represents a single Cisco UCS domain that has to be managed by Cisco UCS Director Express for Big Data. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).

High-level Workflow to Create an Instant Hadoop Cluster

-
- Step 1** Create a Cisco UCS Manager account. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
 - Step 2** Configure Big Data IP pools. See [Adding a Big Data IP Pool](#).
 - Step 3** Create an Instant Hadoop Cluster. See [Creating an Instant Hadoop Cluster](#).
-

High-level Workflow to Create a Customized Hadoop Cluster

-
- Step 1** Configure a Cisco UCS Service Profile template for Big Data. For more information, see [Creating a Cisco UCS Service Profile Template for Big Data](#).
 - Step 2** Create a Hadoop cluster configuration parameters template. See [Creating a Hadoop Cluster Configuration Parameters Template](#).
 - Step 3** Configure a Hadoop cluster profile template. See [Creating a Hadoop Cluster Profile Template](#).
 - Step 4** Configure a Hadoop cluster deployment template. See [Creating a Cluster Deployment Template](#).
 - Step 5** Create a customized Hadoop cluster. See [Creating a Customized Hadoop Cluster](#).
-

Device Connector

The device connector connects Cisco UCS Director Express for Big Data to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Director Express for Big Data to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Configure the device connector proxy settings to connect with Cisco Intersight.
This is required only if you have proxy configuration enabled.
2. Validate your access to the device from Cisco Intersight using the device serial number and the security code and claim the device.



Note After a system running Cisco UCS Director Express for Big Data is claimed in Cisco Intersight, you must refresh the information displayed on the **Device Connector** screen. Choose **Administration > Device Connector** to view the updated information.

Configuring Device Connector

-
- Step 1** Choose **Administration > Device Connector**.
 - Step 2** Click **Settings**.
 - Step 3** In the **Settings** dialog box, choose **Proxy Configuration**.
 - Step 4** For the **HTTPS Proxy** field, move the slider to **Enabled**.
 - Step 5** Enter the proxy hostname or IP address in the **Proxy Hostname/IP** field.
 - Step 6** Enter the proxy port number in the **Proxy Port** field.
 - Step 7** To authenticate access to the proxy server, turn the **Authentication** mode on and enter the **Username** and **Password**.
 - Step 8** Click **Ok**.



Based on the connectivity to Cisco Intersight, the **Status** field displays one of the following messages:

- When the connection to Cisco Intersight is successful, the status messages could be one of the following:
 - **Unclaimed**—Implies that the connection is successful but the device is not claimed. You can claim an unclaimed connection through Cisco Intersight.

For information on claiming a device, see the integrated guided walkthrough titled *Learn How to Claim a Device* available within the **Online Help** menu in the Cisco Intersight user interface.

- **Claimed**—Implies that the connection to Cisco Intersight is successful and you have claimed the device.

Note The header pane of the user interface now includes an icon to indicate the status of the device in Cisco Intersight. This icon is visible only to administrator users and the status change is reflected only when the browser is refreshed or when a new login session is initiated.

Icon	Description
	Indicates that the device is not claimed in Cisco Intersight.
	Indicates that the device is claimed in Cisco Intersight.

- When the connection to Cisco Intersight is unsuccessful, the status messages could be one of the following:
 - **Administratively disabled**—Implies that the administrator has disabled managing the device from Cisco Intersight.
 - **Certification Validation Error**—Implies that an invalid certificate exists on the system.
 - **Not Claimed**—Indicates that the device is registered, but not claimed in Cisco Intersight.
 - **DNS is not configured** or **DNS is mis-configured**.
 - **Unable to resolve DNS name of the service**—Indicates that although DNS is configured, the DNS name of the Cisco Intersight platform cannot be resolved.
 - **NTP is not configured**
 - **Unable to establish a network connection**—Indicates that Cisco UCS Director cannot connect to Cisco Intersight.

Viewing Device Connector Properties

Step 1 Choose **Administration > Device Connector**.

Step 2 In the subsequent screen, review the following information:

Name	Description
Intersight Management Area	

Name	Description
Current Status Indicator	<p>Displays if you have enabled connections to the Cisco Intersight management platform. It can be one of the following:</p> <ul style="list-style-type: none"> • Enabled • Disabled
Access Mode	<p>Displays the current access mode to connect to the Cisco Intersight management platform. It can be one of the following:</p> <ul style="list-style-type: none"> • Read-only—Permission to only view the reports. • Allow Control—Permission to perform all the operations as an administrator.
Connection Area	
HTTPS Proxy Settings button	<p>Whether HTTPS proxy settings are disabled or manually configured. This can be one of the following:</p> <ul style="list-style-type: none"> • Off—Select this option if you want to disable the HTTPS proxy settings configuration. This is the default HTTPS proxy setting. • Manual—Select this option if you want to enable the HTTPS proxy settings configuration. <ul style="list-style-type: none"> • Proxy Hostname/IP—Enter the proxy hostname or IP address. • Proxy Port— Enter the proxy port number. • Authentication—Enable this option to authenticate access to the proxy server. Enter the Username and Password to authenticate access.

Name	Description
Status	<p>The current status of the connection to the Cisco Intersight management platform. It can be one of the following:</p> <ul style="list-style-type: none"> • Administratively disabled—Implies that the administrator has disabled managing the device from Cisco Intersight. • Certification Validation Error—Implies that an invalid certificate exists on the system. • Claimed—Indicates that the device is claimed in Cisco Intersight. • Not Claimed—Indicates that the device is registered, but not claimed in Cisco Intersight. • DNS is not configured or DNS is mis-configured. • Unable to resolve DNS name of the service—Indicates that although DNS is configured, the DNS name of the Cisco Intersight platform cannot be resolved. • NTP is not configured • Unable to establish a network connection—Indicates that Cisco UCS Director cannot connect to Cisco Intersight. <p>To learn why the connection failed, click the Details & Recommendations drop-down list and then click Retry Connection.</p>
Device ID	The unique identification number of the device.

Launching Cisco UCS Director Express for Big Data from Cisco Intersight

After the device connector is configured and the device is claimed, you can launch the Cisco UCS Director Express for Big Data user interface from Cisco Intersight.



Important

If any of the Cisco UCS Director Express for Big Data services are down, you cannot launch Cisco UCS Director Express for Big Data from Cisco Intersight.

A message stating that there is no service is displayed.

Although you can launch Cisco UCS Director Express for Big Data from Cisco Intersight, following are some of the restrictions that you need to be aware of:

- You cannot edit a user profile.
- You cannot perform any import and export actions.
- The main menu and the Dashboard are disabled.
- The **Device Connector** tab is not visible.
- You cannot perform any launch actions.
- You cannot upgrade connector packs.
- You cannot generate any summary reports.
- The user name is displayed as Cisco Intersight user when you launch Cisco UCS Director Express for Big Data.
- All service requests and audit log details are logged as Admin user.

Step 1 Log into the Cisco Intersight user interface.

Step 2 Choose **Devices**.

The **Devices** screen appears that displays a list of available Cisco UCS Director Express for Big Data systems.

Step 3 Select a Cisco UCS Director Express for Big Data device from the list, and click

You must scroll to the far right of the list of devices to see the option.

Note The IP address displayed for the Cisco UCS Director Express for Big Data device in Cisco Intersight is determined by the IP address you entered for the **Server IP address** field while configuring the outgoing mail server for Cisco UCS Director Express for Big Data.

If you modify the server IP address after the Device Connector process is up, you must restart the Device Connector process. To do so, login to the Cisco UCS Director Express for Big Data device, and run the following commands:

```
/opt/infra/bin/stopdc.sh  
/opt/infra/bin/startdc.sh
```

Refresh the **Devices** screen in Cisco Intersight to view the updated server IP address.

Step 4 Choose **Launch UCSD**.

Cisco Intersight is connected to the Cisco UCS Director Express for Big Data system and the Cisco UCS Director Express for Big Data user interface opens in a new tab.

Note Users with read-only permissions created in Cisco Intersight cannot perform any actions. These users can only view reports.

Base Platform Pack and System Update Manager

Cisco UCS Director Express for Big Data includes the capability to update the following components of the software:

- **Base Platform Pack**—Includes basic infrastructure components such as the user interface, Shell admin console changes, and critical defect fixes.
- **System Update Manager**—Includes the framework that helps you upgrade all connector packs and the base platform pack.
- **Connector Packs**—Includes connector-specific updates and critical defect fixes, which you can upgrade in your environment without affecting other connectors. See [Connector Pack Management, on page 32](#).

Prior to upgrading any of these packs, ensure that the following prerequisites are met:

- You must have system administrator privileges in Cisco UCS Director Express for Big Data.
- Cisco UCS Director Express for Big Data has been claimed in Cisco Intersight.
- Cisco UCS Director Express for Big Data is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

When you login to the user interface, the header pane will indicate the number of updates that are available for your system. Clicking that number will display the **Available System Upgrades** screen. This screen displays information on base packs and the connector packs that are available for upgrade. From this screen, you can perform the following actions:

- Upgrade connector packs that you need for your environment.
See [Upgrading Connector Packs, on page 33](#).
- Upgrade the Base Platform pack—Selecting this base pack will also automatically select the System Update Manager Pack, and the connector packs that are available for upgrade.
- Upgrade only the System Update Manager
See [Upgrading the System Update Manager, on page 31](#).
- Upgrade the connector packs, Base Platform pack and System Update Manager together

If you select all three options, the System Update Manager is upgraded first, followed by the connector packs, and then finally the Base Platform pack. After the System Update Manager upgrade is complete, the System Update Manager service is restarted, following which the upgrade process for the connector packs and the Base Platform pack is initiated. If the upgrade process for the connector packs fail, then the versions on the system are reverted to the previously installed versions, and the upgrade of the Base Platform pack is also terminated.

Upgrading Base Platform Pack

Before you begin

- You must have system administrator privileges in Cisco UCS Director Express for Big Data.

- Cisco UCS Director Express for Big Data has been claimed in Cisco Intersight.
- Cisco UCS Director Express for Big Data is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the **Base Platform** check box.

Checking this check box will also automatically select the System Update Manager and connector packs, if available.

Step 3 Click **Upgrade**.

To complete the upgrade, the required Cisco UCS Director Express for Big Data services will restart.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.

After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.

For more information on possible outcomes of the validation and upgrade process, see [Upgrade Process Validation and Failure Scenarios, on page 35](#).

Step 5 Review the status messages on the **System Upgrade Status** screen.

Step 6 After the upgrade process completes successfully, click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking Logout, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director.

Step 7 Login to the user interface.

Upgrading the System Update Manager

Before you begin

- You must have system administrator privileges in Cisco UCS Director Express for Big Data.
- Cisco UCS Director Express for Big Data has been claimed in Cisco Intersight.
- Cisco UCS Director Express for Big Data is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the **System Update Manager** check box.

Step 3 Click **Upgrade**.

To complete the upgrade, the required Cisco UCS Director Express for Big Data services will restart.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.

After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.

For more information on possible outcomes of the validation and upgrade process, see [Upgrade Process Validation and Failure Scenarios, on page 35](#).

Step 5 Review the status messages on the **System Upgrade Status** screen.

Step 6 After the System Update Manager upgrade process completes successfully, click **Logout**.

After the upgrade process is complete, the System Update Manager service is restarted.

Step 7 Login to the user interface.

Connector Pack Management

Connector packs help you perform connector level upgrade in Cisco UCS DirectorCisco UCS Director Express for Big Data without impacting other connectors. After a system running Cisco UCS DirectorCisco UCS Director Express for Big Data is claimed in Cisco Intersight, as a system administrator, you can view information on new versions of connector packs that are available for upgrade. The top header pane of the user interface displays a notification indicating that new connector pack versions are available. You can select and upgrade the connector packs on the system. For more information, see [Upgrading Connector Packs, on page 33](#).

Following are the connectors that are available in this release:

- Cisco UCS which includes Cisco UCS Central and Cisco UCS Manager
- ACI APIC
- ACI Multi-Site Controller
- F5 Load Balancer
- Network Devices
- EMC Isilon
- EMC RecoverPoint
- EMC VMAX
- EMC VNX

- EMC VNXe
- EMC VPLEX
- EMC Unity
- EMC XtremIO
- IBM
- NetApp ONTAP
- VCE VisionIO
- Microsoft Hyper-V
- RedHat KVM
- Vmware
- Bare Metal Agent
- Cisco IMC
- Cisco BigData Express
- Cisco HyperFlex

**Important**

Latest versions of these connectors are made available to Cisco UCS DirectorCisco UCS Director Express for Big Data only through Cisco Intersight. So Cisco UCS DirectorCisco UCS Director Express for Big Data must be claimed in Cisco Intersight.

Upgrading Connector Packs

As a system administrator, you can upgrade connector packs using the Cisco UCS Director Express for Big Data graphical user interface. When new connector pack versions are available, the system notifies you in the following ways:

- Pop-up message when you log in to Cisco UCS Director user interface.

When you log in to the user interface of Cisco UCS Director, and if there are new connector pack versions available for upgrade, a pop-up message prompting you to upgrade these versions is displayed. Click **Yes** to upgrade these connector pack versions immediately or click **No** to upgrade at a later time.



Note This pop-up notification message is displayed once every 3 days. It is not displayed every time you log in to the user interface.

- An alert with a downward facing arrow image and a number in the header pane of the user interface. This number indicates the number of connector packs that are available for upgrade.

The pop-up message and the alert on the header pane are displayed only when Cisco UCS Director Express for Big Data has been claimed in Cisco Intersight. For information on establishing a connection with Cisco Intersight, see [Configuring Device Connector, on page 25](#).



Note You can upgrade system packs (System Update Manager, Base Platform Pack and Connector Pack versions) in a standalone setup and in a multi-node setup. In a multi-node setup, you must upgrade the versions only on the primary node.

Before you begin

- You must have system administrator privileges in Cisco UCS Director Express for Big Data.
- Cisco UCS Director Express for Big Data has been claimed in Cisco Intersight.
- Cisco UCS Director Express for Big Data is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears and will display all available connector packs for upgrade along with version information. Upon login, if you clicked **Yes** to the pop-up message, then the very same upgrade screen appears.

Note The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the check box of a connector pack from the list.

You can check the check boxes of multiple connector packs.

Step 3 Click **Upgrade**.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes**.

After you confirm that the connector version must be upgraded, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled.

Step 5 Click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking **Logout**, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director Express for Big Data.

What to do next

You can view the upgrade reports by choosing **Administration > System > System Updates**. From this screen, you can double-click on a report, and view additional details on the upgrade process. For more information, see [Viewing Connector Pack Upgrade Information, on page 36](#).

Upgrade Process Validation and Failure Scenarios

After you initiate a system pack upgrade, a validation process is initiated in the system. The following table describes the possible outcomes of the validation for system packs:

Scenario	Validation Process Outcome	Information in the User Interface	Recommended Action
No problems with any system pack versions No workflows in progress No users logged into the system	Succeeds	The System Upgrade Validation screen displays the status	None. The upgrade process is initiated.
Problems with one or more system packs	Fails	The System Upgrade Validation screen displays an error message and corrective action.	Review the information and perform the corrective action suggested.
Other users are logged into the system or Workflows are in progress	Fails	The System Upgrade Validation screen displays an error message and corrective action.	Review the corrective action, and click Force Upgrade to proceed with the upgrade. Note The Force Upgrade option is available only for Base Platform pack and connector packs. It is not displayed for the System Update Manager. The System Upgrade Status screen is displayed with current status for the upgrade request. Users are automatically logged out of the system with a system broadcast message about the upgrade.

After validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the status. On successful completion of the upgrade process, the **Logout** option is enabled on the user interface. The following table describes the possible issues that you could encounter during an upgrade process:

Scenario	Information in the User Interface	Impact to Upgrade Process
System pack upgrade is in progress and other users with administrator privileges logs in to the user interface.	The System Upgrade Status screen is displayed to the user with current status for the upgrade request.	The upgrade process completes successfully.
System pack upgrade is in progress and an end user logs in to the user interface.	The system startup page is displayed to the user.	The upgrade process completes successfully.
You selected multiple packs for upgrade, and the upgrade for one system pack fails.	The System Upgrade Status screen displays the status of the upgrade. The overall upgrade status is indicated as partially completed. The status for each system pack will help you determine the system pack that was not upgraded.	When the upgrade process for any system pack fails, then the version of that system pack is reverted to the previously installed version.
You selected the base platform pack for upgrade and you are logged out of the user interface before the System Upgrade Status screen displays the complete workflow of the upgrade process.	If the base platform pack that you selected for upgrade includes an update to the Tomcat service, then the System Upgrade Status screen does not display the complete workflow of the upgrade process. This is because the Tomcat service restarts in the system which results in terminating your session in the user interface. Also, you are automatically directed to the system start-up screen. You can login to the user interface only after all Cisco UCS Director services are restarted.	Although the System Upgrade Status screen does not display the complete workflow, the upgrade process completes successfully.

Viewing Connector Pack Upgrade Information

-
- Step 1** Choose **Administration > System**.
- Step 2** On the **System** page, click **Connector Pack Upgrades**. Information such as upgrade request ID, user that initiated the upgrade, upgrade start time and end time, and the upgrade status are displayed.
- Step 3** Select a connector pack and choose **View Details** to view details such as connector pack name, upgraded version, and prior version.
- Step 4** Click **State History** to view the various states of the connector pack upgrade process. For example, upgrade request received, upgrade process initiated or upgrade process completed.

Step 5 Click **Stages** to view the entire lifecycle of the connector pack upgrade request.



CHAPTER 3

Licenses for Cisco UCS Director Express for Big Data

This chapter contains the following sections:

- [About Licenses, on page 39](#)
- [Fulfilling the Product Access Key, on page 39](#)
- [Updating the License, on page 40](#)
- [Standard License Features, on page 41](#)

About Licenses

You must obtain a license to use Cisco UCS Director Express for Big Data, as follows:

1. Before you install Cisco UCS Director Express for Big Data, generate the Cisco UCS Director Express for Big Data license key and claim a certificate (Product Access Key).
2. Register the Product Access Key (PAK) on the Cisco software license site, as described in [Fulfilling the Product Access Key, on page 39](#).
3. After you install Cisco UCS Director Express for Big Data, update the license in Cisco UCS Director Express for Big Data as described in [Updating the License, on page 40](#).
4. After the license has been validated, you can start to use Cisco UCS Director Express for Big Data.

Fulfilling the Product Access Key

Before you begin

You need the PAK number.

-
- Step 1** Navigate to the [Cisco Software License website](#).
- Step 2** If you are directed to the Product License Registration page, you can take the training or click **Continue to Product License Registration**.
- Step 3** On the Product License Registration page, click **Get New Licenses from a PAK or Token**.

Step 4 In the **Enter a Single PAK or TOKEN to Fulfill** field, enter the PAK number.

Step 5 Click **Fulfill Single PAK/TOKEN**.

Step 6 Complete the additional fields in **License Information** to register your PAK:

Name	Description
Organization Name	The organization name.
Site Contact Name	The site contact name.
Street Address	The street address of the organization.
City or Town	The city or town.
State or Province	The state or province.
Zip or Postal Code	The zip code or postal code.
Country	The country name.

Step 7 Click **Issue Key**.

The features for your license appear, and you receive an email with the Digital License Agreement and a zipped license file.

Updating the License

Before you begin

If you received a zipped license file by an email, extract and save the license (.lic) file to your local machine.

Step 1 Choose **Administration > License**.

Step 2 On the **License** page, click **License Keys**.

Step 3 Click **Update License**.

Step 4 On the **Update License** screen, do the following:

- a) Drop the `.lic` file from your local system or click **Select a File** and navigate to the location where you stored the `.lic` file.

To enter license text instead of file upload, check the **Enter License Text** checkbox and enter the license text in the **License Text** field.

- b) Click **Submit**.

The license file is processed, and a message appears confirming the successful update.

Standard License Features

The following table lists the features supported for the standard licenses:

Features	Standard License
Operating system and Hadoop software installation	X
Server, Network, and Storage provisioning	X
On-demand cluster creation and expansion	X
Customized cluster creation	X
Automated cluster node addition and deletion	X
Add pre-existing Hadoop nodes	X
Start and stop cluster services	X
Start, stop, and restart Cluster	X
Dashboard for health and status monitoring	X
Support for latest Cloudera, MapR, and Hortonworks releases	X
Monitoring Storage and Network utilization	X
Monitoring Top Active and Long Running Jobs	X
On-Demand inventory collection	X
DIMM, Disk, Node, and Service Failure Alerts	X
Capacity Planning Alerts	X
HDFS rebalancing	X
LDAP integration	X
Hadoop parameter configuration	X
Globalization and localization Support	X
Cusotmizable workflows	X
North Bound REST API support	X
Cluster configuration consistency checks	X
Cluster performance analysis	X
Historical performance analysis	X

Features	Standard License
Automated install and setup of new Hadoop services	X
Automated Hadoop version upgrade	X
Role-Based Access Control (RBAC)	X
Approval workflows	X



CHAPTER 4

Managing Hadoop Accounts

This chapter contains the following sections:

- [Adding a Hadoop Account, on page 43](#)
- [Running a Cluster Inventory for a Hadoop Account, on page 44](#)
- [Purging Big Data Cluster Account Details, on page 45](#)
- [Rolling Back a Hadoop Cluster for a Hadoop Account, on page 45](#)
- [Access to Hadoop Managers from Cisco UCS Director Express for Big Data, on page 45](#)

Adding a Hadoop Account

If you want to manage your Hadoop cluster using Cisco UCS Director Express for Big Data, add a Hadoop account.

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Click **Add**.
- Step 4** On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	The pod to which you add the Hadoop account.
Account Name field	The account name.
Account Type drop-down list	The type of Hadoop distribution used for the cluster. Choose one of the following: <ul style="list-style-type: none">• Cloudera• MapR• Hortonworks
Management Console IP field	The management console IP address.
SSH (root) Password field	The password associated with the SSH username.

Name	Description
Confirm Password field	The password associated with the SSH username.
Management Console Protocol drop-down list	Choose HTTP or HTTPS protocol.
Management Console Port Number field	Enter the port number. Enter an integer between 1024 and 65535.
Hadoop Manager Password field	The password associated with the Hadoop Manager for that account type.
Confirm Password field	The password associated with the Hadoop Manager for that account type.

Step 5 Click **Submit**.

Step 6 For the following actions, select a Hadoop account.

Name	Description
Edit	Allows you to edit a Hadoop account.
Delete	Deletes a Hadoop account.
Check Configuration	Allows you to validate an existing cluster configuration.
Rollback Cluster	Allows you to roll back a cluster and make all the nodes in the cluster available for bare metal servers. Roll back is not supported for a derived cluster account.
Launch Hadoop Manager	Allows you to launch the Hadoop manager from Cisco UCS Director Express for Big Data
View Details	Provides details of a Hadoop account.
Run Inventory	Collects the inventory of the Hadoop cluster for the selected Hadoop Account and the data persists in the Cisco UCS Director Express for Big Data database.
Configure Cluster	Allows you to customize the Hadoop cluster after creation.
Modify Credentials	Allows you to modify the SSH, admin Console credentials, and management console protocol and port details for a Hadoop account.

Running a Cluster Inventory for a Hadoop Account

When you create a Hadoop Account, a new system task (inventory collector) is created within the account. Navigate to the Big Data Tasks folder here: **Administration > System > System Tasks**. The system task collects the inventory of the Hadoop cluster for the selected Hadoop Account and establishes data in the Cisco

UCS Director database. This collector adds to the system scheduler so that the system scheduler can be called at the interval configured in the collector (for example, 30 minutes).

For more information on how to manage system tasks in Cisco UCS Director, see the latest *Cisco UCS Director Administration Guide*.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** On the **Accounts** screen, choose the Hadoop Account for which you want to run the inventory.
- Step 4** Click **Run Inventory**.
- Step 5** Click **Submit**.
-

Purging Big Data Cluster Account Details

A new system task (purging) is created within the account. Navigate to the Big Data Tasks folder here: **Administration > System > System Tasks**. The system scheduler deletes the monitoring and metric data that are older than 18 days. When the Cisco UCS Director Express for Big Data is up:

- the stale entries are deleted for the valid accounts that do not have add nodes.
- the account details are deleted for the invalid accounts.

Rolling Back a Hadoop Cluster for a Hadoop Account

You can roll back a Hadoop cluster and make all the nodes in the cluster available for a bare metal server. However, roll back is not supported for a derived cluster account.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** On the **Accounts** screen, choose the Hadoop account for which you want to roll back the cluster.
- Step 4** Click **Rollback Cluster**.
- Step 5** On the **Rollback Cluster** screen, click **Submit**.
-

Access to Hadoop Managers from Cisco UCS Director Express for Big Data

You can access Hadoop managers for all the Hadoop accounts that you create in Cisco UCS Director Express for Big Data. Choose **Solutions > Big Data > Accounts**, and then click **Hadoop Accounts**. You can launch the Hadoop manager in supported browsers by clicking **Launch Hadoop Manager**.



CHAPTER 5

Managing Splunk Accounts

This chapter contains the following sections:

- [Cisco UCS Director Express for Big Data with Splunk Enterprise](#) , on page 47
- [Adding a Splunk Account](#), on page 47
- [Running a Cluster Inventory for a Splunk Account](#), on page 49
- [Rolling Back a Cluster for a Splunk Account](#), on page 49
- [Access Splunk Enterprise Monitoring Console User Interface from Cisco UCS Director Express for Big Data](#), on page 49

Cisco UCS Director Express for Big Data with Splunk Enterprise

Cisco UCS Director Express for Big Data with Splunk Enterprise deployment reliably collects and indexes machine data, from a single source to tens of thousands of sources, all in real time. Splunk Enterprise deployments expand to terabytes of operational data. Cisco UCS Director supports the massive scalability that Splunk Enterprise deployments to deliver exceptional performance.

Splunk Enterprise deployments consist of Cisco UCS as indexer and C220 M4 Server as search heads, along with administrative functions.

Splunk Enterprise deployments include the following:

- Cisco UCS
- Cisco UCS C-Series Rack-Mount Servers
- Cisco UCS Manager

Adding a Splunk Account

If you want to manage your Splunk cluster using Cisco UCS Director Express for Big Data, add a Splunk account.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
 - Step 2** Click **Splunk Accounts**.
 - Step 3** Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	The pod to which the Splunk account to be added.
Account Name field	The Splunk account name.
Management Console IP field	The management console IP address.
SSH (Root) Password field	The password associated with the SSH username.
Confirm Password field	The password associated with the SSH username.
Monitoring Console Protocol drop-down list	Choose HTTP or HTTPS protocol.
Monitoring Console Port Number field	Enter the port number. Enter an integer between 1024 and 65535.
Splunk Manager Password field	The password associated with the Splunk Enterprise.
Confirm Password field	The password associated with the Splunk Enterprise.

Step 5 Click **Submit**.

Step 6 For the following actions, select a Splunk account.

Name	Description
Edit	Allows you to edit a Splunk account.
Delete	Deletes a Splunk account.
Check Configuration	Allows you to validate an existing cluster configuration.
Rollback Cluster	Allows you to roll back a cluster and make all the nodes in the cluster available for a bare metal server. Roll back is not supported for a derived cluster account.
Launch Splunk DMC	Allows you to launch the Splunk Enterprise from Cisco UCS Director Express for Big Data.
View Details	Provides details of a Splunk account.
Run Inventory	Collects the inventory of the Splunk cluster for the selected Splunk account and establishes data in the Cisco UCS Director Express for Big Data database.
Modify Credentials	Allows you to modify the SSH, admin Console credentials, and monitoring console protocol and port details for a Splunk account.

Running a Cluster Inventory for a Splunk Account

With each new Splunk Account, a new system task (inventory collector) is created. Navigate to the Big Data Tasks folder here: **Administration > System > System Tasks**. The system task collects the inventory of the Splunk cluster for the selected Splunk Account and establishes data in the Cisco UCS Director database. This collector adds to the system scheduler so that it can be called at the interval configured in the collector (for example, 30 minutes).

For more information on how to manage system tasks in Cisco UCS Director, see the latest *Cisco UCS Director Administration Guide*.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
 - Step 2** Click **Splunk Accounts**.
 - Step 3** Choose the Splunk Account for which you want to run the inventory.
 - Step 4** Click **Run Inventory**.
 - Step 5** Click **Submit**.
-

Rolling Back a Cluster for a Splunk Account

You can roll back a cluster and make all the nodes in the cluster available for a bare metal server. However, roll back is not supported for a derived cluster account.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
 - Step 2** Click **Splunk Accounts**.
 - Step 3** Choose the Splunk account for which you want to roll back the cluster.
 - Step 4** Click **Rollback Cluster**.
 - Step 5** On the **Rollback Cluster** screen, click **Submit**.
-

Access Splunk Enterprise Monitoring Console User Interface from Cisco UCS Director Express for Big Data

You can access the Splunk Enterprise user Interface from Cisco UCS Director Express for Big Data. On the menu bar, choose **Solutions > Big Data > Accounts**, and then click **Splunk Accounts**. You can launch the Splunk Enterprise user interface in supported browsers by clicking the **Launch Splunk DMC**.



CHAPTER 6

Managing Bare Metal OS Accounts

This chapter contains the following sections:

- [Creating a Local Disk Configuration Policy for Deploying Baremetal OS, on page 51](#)
- [Deploying a BareMetal OS Account, on page 53](#)

Creating a Local Disk Configuration Policy for Deploying Baremetal OS

This policy defines disk configuration for disk partitions, and storage local to the server for the selected baremetal OS. It enables you to set a local disk configuration for all servers associated with a service profile.

Step 1 Choose **Solutions > Big Data > Containers**.

Step 2 Click **UCS SP Templates**.

Step 3 Click **Add (+)**.

Step 4 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, complete the following fields:

Name	Description
Use LVM For Disk Configuration check box	Create Logical Volume Manager (LVM) groups for disk partitions.
Partition Configuration table	Create partitions other than the /, /boot, swap, /tmp, /var/tmp, and /home partitions.
Set JBOD to Unconfigured Good check box	Set the JBOD to unconfigured good state. This is applicable only to disks or controllers which support unconfigured good state. This is not applicable for Cisco Boot-Optimized M.2 RAID controller (UCS-M2-HWRAID).
Delete LUN check box	Delete the Logical Unit Numbers (LUNs) that already exist.

Name	Description
Scrub Policy check box	Check the check box to include a scrub policy. The scrub policy is set to erase the information in the disks associated with the server, when the service profile is disassociated from the server.
Manual Disk Group Policy table	Specify the disk slot numbers. This is applicable only for SAS and SATA controllers. This is not applicable for PCH controllers such as Lewisburg SSATA controller with SWRAID mode and Lewisburg SSATA controller with AHCI mode.. For a SAS controller, you can choose any two consecutive available disk slot numbers. For example, 1 and 2 or 5 and 6. For a SATA controller, you can choose any two consecutive available disk slot numbers. For example, 253 and 254.
Stripe Size (KB) table	Stripe size for a virtual drive.

Step 5 Click **Submit**.

What to do next

Deploy a baremetal OS account.

Creating a Disk Group Policy

Use this procedure to manually create disk group policies for OS deployment.

-
- Step 1** Choose **Solutions > Big Data > Containers**.
 - Step 2** Click **UCS SP Templates**.
 - Step 3** Click **Add (+)**.
 - Step 4** On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, click **Add** in the **Manual Disk Group Policy** table.
 - Step 5** On the **Add Entry to Manual Disk Group Policy** screen, specify the slot number, role, and span ID for OS deployment.
 - Step 6** Click **Submit**.
-

Deploying a BareMetal OS Account

Before you begin

- Create a service profile template that Cisco UCS Director Express for Big Data uses to deploy a baremetal OS.
- Create a server pool in the Cisco UCS Manager account that you plan to use for this cluster. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
- Add a big data IP pool.

Step 1 Choose **Solutions > Big Data > Containers**.

Step 2 Click **Cluster Deploy Templates**.

Step 3 Click **Deploy BareMetal OS Account**.

Step 4 On the **Deploy BareMetal OS Account** screen, complete the following fields.

Name	Description
BareMetal OS Account Name field	Enter the name of the BareMetal OS account.
UCS SP Template table	Click Select to choose an existing UCS Service Profile template and click Select .
UCSM Policy Name Prefix field	Enter a prefix that needs to be added to Cisco UCS Manager policy name.
SSH root Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Confirm SSH root Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Linux OS Version drop-down list	Choose the operating system to be installed on the servers.
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account.
Organization table	Click Select to choose the organization in which the servers are located and click Select .
PXE VLAN ID field	Enter the PXE VLAN ID.

Step 5 In the **vNIC Template** table, review and, if desired, edit the vNIC templates available for the cluster.

Step 6 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 7 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	Displays the vNIC name.

Name	Description
IP Pool field	Choose the big data IP pool that you want to use for IP addresses assigned to this vNIC.
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
VLAN ID field	Enter the VLAN ID for this cluster.

Note When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool, and VLAN ID to the first vNIC in the **vNIC Template** table.

Step 8 Specify the host name prefix and node count.

Step 9 In the **Server Pool** table, choose the required server pool.

Note The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.

Step 10 Click **Submit**. After successful deployment, you can view the baremetal OS account details by choosing **Solutions > Big Data > Accounts** and clicking **BareMetal OS Accounts**. If you want to rollback, click **Rollback Account**.

What to do next

You can view and monitor the workflow that gets triggered after deploying a baremetal OS.



CHAPTER 7

Configuring Big Data IP Pools

This chapter contains the following sections:

- [Big Data IP Pools, on page 55](#)
- [Adding a Big Data IP Pool, on page 55](#)
- [Managing Big Data IP Pools, on page 56](#)

Big Data IP Pools

Big Data IP pools contain blocks of IP addresses that Cisco UCS Director Express for Big Data uses during the creation of Hadoop clusters. The IP addresses in each block must belong to the same subnet mask, default gateway, primary domain name server (DNS), and secondary DNS.



Note All IP addresses in a Big Data IP pool must be IPv4 addresses.

Adding a Big Data IP Pool

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **Big Data IP Pools**.

Step 3 Click **Add**.

Step 4 In the **IP Pool Management Specification** page of the **Create an IP Pool** wizard, complete the following fields:

Name	Description
IP Pool Name field	A unique name for the IP Pool.
Description field	A short description that identifies the purpose of the pool.

Name	Description
Assignment Order drop-down list	The assignment order. Choose one of the following: <ul style="list-style-type: none"> • Default—A random identity is selected from the pool. • Sequential—The lowest available identity is selected from the pool.
Domain Name field	Enter the domain name. For example, cisco.com.

Step 5 Click **Next**.

Step 6 In the **IPv4 Addresses** page of the **Create an IP Pool** wizard, complete the following fields:

- a) In the IPv4 Blocks table, click **Add (+)**.
- b) On the **Add Entry to IPv4 Blocks** screen, enter the IPv4 addresses to be included in the IP pool in the **Static IP Pool** field.

This can be a range of IP addresses, or a series of IP addresses separated by commas (,).
- c) Enter the subnet mask.
- d) Enter the default gateway.
- e) Enter the primary DNS server IPv4 address.
- f) Enter the server DNS server IPv4 address.
- g) Click **Submit** to save and exit.

Step 7 Click **Submit**.

Managing Big Data IP Pools

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **Big Data IP Pools**. The following buttons are displayed.

Name	Description
Refresh	Refreshes the current page.
Add	Adds a new IP pool.

Step 3 For the following actions, choose an IP Pool from the table:

Name	Description
Edit	Modifies the IP pool specification.
Delete	Deletes the IP pool specification.

Name	Description
View Details	Allows you to view the IPv4 addresses in the IP pool and to view more reports. Note If you see a License Status tab, it indicates a licensing issue.

Step 4 With an IP Pool selected, click **View Details**.

Step 5 Click **IPv4 Addresses** to display the IP Addresses associated with the selected IP Pool.

Step 6 Select an IP Address from the table. The following buttons are displayed.

Name	Description
Release IP Address	The IP address is made available to be assigned against any bare metal server.
Release Multiple IP Addresses	Enables you to choose and release more than one IP address from the Release Multiple IP Addresses dialog box.



CHAPTER 8

Configuring Cisco UCS Service Profile Templates for Big Data

This chapter contains the following sections:

- [Cisco UCS Service Profile Templates for Big Data, on page 59](#)
- [Creating a Cisco UCS Service Profile Template for Big Data, on page 60](#)
- [Creating a Customized Service Profile Template, on page 74](#)
- [Cloning a Cisco UCS Service Profile Template, on page 75](#)

Cisco UCS Service Profile Templates for Big Data

Cisco Unified Computing System (Cisco UCS) service profiles are a powerful means for streamlining the configuration and management of Cisco UCS servers. They provide a mechanism for rapidly provisioning servers and their associated network connections with consistency in all details of the environment. They can be set up in advance before physically installing the servers.

Service profiles are built on policies—Administrator-defined sets of rules and operating characteristics such as the server identity, interfaces, and network connectivity. Every active server in your Hadoop cluster must be associated with a service profile.

The Cisco UCS service profile template for the Big Data enables you to set up the configuration for the servers in your Hadoop cluster. The service profile template for Big Data is included in a cluster deploy template. When the cluster deploy template is applied to the servers, the service profile template configures one or more service profiles that are applied to the servers.



Note The service profile template for Big Data wizard gathers the information required to create a service profile template. You can only apply this service profile template through the cluster deploy template.

For more information about service profiles and service profile templates, see the [Cisco UCS Manager configuration guides](#).

Creating a Cisco UCS Service Profile Template for Big Data

Before you begin

Add a Cisco UCS Manager account.

- Step 1** Choose **Solutions > Big Data > Containers**.
- Step 2** Click **UCS SP Templates**.
- Step 3** Click **Add (+)**.
- Step 4** On the **UCS SP Template Specification** page of the **Create UCS SP Template for Big Data** wizard, complete the following fields:

Name	Description
Template Name field	A unique name for the template.
Template Description field	The description of the template.
Template Type drop-down list	Choose a service profile template. Service profiles created from an initial template inherit all the properties of the template. However, changes to the initial template do not automatically propagate to the bound service profiles. If you want to propagate changes to bound service profiles, unbind and rebind the service profile to the initial template.
Container Type drop-down list	The type of container for the cluster. Choose one of the following: <ul style="list-style-type: none"> • Hadoop • Splunk • Baremetal OS
Use vNIC Bonding check box	Check the check box to use vNIC bonding. Eight vNICs are available in the Create vNIC Policy page of the Create UCS SP Template for Big Data wizard.
Use Multiple vNIC check box	Check the check box to have more than one vNIC interface and the required policies for creating a template. This option is only available when you select Hadoop or Splunk in the Container Type drop-down list. It is not displayed for Baremetal OS .

- Step 5** Click **Next**.

What to do next

Create a QoS policy.

Creating a QoS Policy

The quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify more controls on the outgoing traffic, such as burst and rate.

- Step 1** On the **Create QoS Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:
- To accept the default QoS policies, click **Next**.
 - To create one or more custom QoS policies, click **Add (+)** and continue with Step 2.
 - To review or modify one of the default QoS policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit QoS Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to QoS Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Priority drop-down list	Choose the priority assigned to this QoS policy. Choose one of the following: <ul style="list-style-type: none"> • Fe—Use this priority for QoS policies that control only vHBA traffic. • Platinum—Use this priority for QoS policies that control only vNIC traffic. • Gold—Use this priority for QoS policies that control only vNIC traffic. • Silver—Use this priority for QoS policies that control only vNIC traffic. • Bronze—Use this priority for QoS policies that control only vNIC traffic. • Best Effort—It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Burst(Bytes) field	The normal burst size for servers that use this policy. This field determines the maximum size of traffic bursts beyond which the traffic is considered to exceed the rate limit. The default is 10240. The minimum value is 0, and the maximum value is 65535. This setting is not applicable to all adapters.

Name	Description
Rate drop-down list	<p>Choose the expected average rate of traffic. Choose one of the following:</p> <ul style="list-style-type: none"> • Line-rate—Equals a value of 0 and specifies no rate limiting. This is the default value. • Specify Manually—Enables you to specify the rate in a field. The minimum value is 0, and the maximum value is 40,000,000. <p>The granularity for rate limiting on a Cisco UCS M81KR Virtual Interface Card adapter is 1 Mbps. The adapters treat the requested rate as a "not-to-exceed" rate. Therefore, a value of 4.5 Mbps is interpreted as 4 Mbps. Any requested rate of more than 0 and less than 1 Mbps is interpreted as 1 Mbps, which is the lowest supported hardware rate limit.</p> <p>Rate limiting is not applicable to all adapters. For example, this setting is not supported on the Cisco UCS VIC-1240 Virtual Interface Card.</p>
Host Control drop-down list	<p>Determines whether Cisco UCS controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA.</p> <p>The default setting is None. Cisco UCS uses the CoS value associated with the priority regardless of the CoS value assigned by the host.</p>

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a VLAN policy.

Creating a VLAN Policy

The VLAN policy creates a connection to a specific external LAN in the underlying infrastructure of a Hadoop cluster that is within a single Cisco UCS domain. The VLAN isolates traffic to that external LAN, including broadcast traffic.

Step 1 On the **Create VLAN Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:

- To accept the default VLAN policies, click **Next**.
- To create one or more custom VLAN policies, click **Add (+)** and continue with Step 2.
- To review or modify one of the default VLAN policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit VLAN Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to VLAN Policy** screen, complete the following fields:

Name	Description
VLAN Name field	The name of the VLAN policy.
Fabric ID drop-down list	Choose how to configure the VLAN. The setting can be one of the following: <ul style="list-style-type: none"> • Common or Global—The VLAN maps to the same VLAN ID in all available fabrics. • Fabric A—The VLAN maps to a VLAN ID that exists only in fabric A. • Fabric B—The VLAN maps to a VLAN ID that exists only in fabric B.
Sharing drop-down list	The default setting is None .

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a vNIC policy.

Creating a vNIC Policy

The vNIC policy defines how a vNIC on a server connects to the LAN. Each server in a Hadoop cluster requires a vNIC policy for each of the following NICs:

- MGMT
- DATA



Note In addition to MGMT NIC, DATA NIC is available if you have checked **Multiple vNIC** in the **Create UCS SP Template for Big Data** wizard.

Step 1 On the **Create vNIC Policy** page of the **Create UCS SP Template for Big Data** wizard, do one of the following:

- To accept the default vNIC policies, click **Next**.
- To create one or more custom vNIC policies, click **Add (+)** and continue with Step 2.
- To delete a vNIC policy, choose a policy in the table and click **Delete**.

Note When you delete the vNICs, ensure that at least one vNIC is available per fabric interconnect.

- To review or modify one of the default vNIC policies, choose the policy in the table and click **Edit**. For information about the fields on the **Edit vNIC Policy Entry** screen, see Step 2.

Step 2 On the **Add Entry to vNIC Policy** screen, complete the following fields:

Name	Description
vNIC Name field	Name of the vNIC.
Fabric ID drop-down list	<p>Choose the fabric interconnect with which the vNICs created with this policy are associated.</p> <p>If you want vNICs created from this policy to access the second fabric interconnect when the default choice is unavailable, check the Enable Failover check box. When the Use vNIC Bonding check box is checked in the UCS SP Template Specification page of the Create UCS SP Template for Big Data wizard, the Enable Failover check box is disabled.</p> <p>Do not enable vNIC fabric failover under the following circumstances:</p> <p>Note</p> <ul style="list-style-type: none"> • If the Cisco UCS domain is running in Ethernet Switch Mode, vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to other fabric interconnect. • If you associate one or more vNICs created from this template and associate the service profile with the server that has an adapter without the fabric failover support (For example, Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter) Cisco UCS Manager generates a configuration fault.
VLANs area	<p>In the VLANs area, do the following to select the VLAN to be assigned to vNICs created from this policy:</p> <ol style="list-style-type: none"> a. Click Add. b. On the Add Entry to VLANs screen, complete the following fields: <ul style="list-style-type: none"> • Name drop-down list—Choose the VLAN that you want to associate with the vNIC template. • Set as Native VLAN check box—Check the check box if you want this VLAN to be the native VLAN for the port. c. Click Submit.

Name	Description
MTU field	The MTU, or packet size, to be used by the vNICs created from this vNIC policy. Enter an integer between 1500 and 9216. Note If the vNIC template has an associated QoS policy, the MTU specified has to be equal to, or less than the MTU specified in the associated QoS System class. If this MTU value exceeds the MTU value in the QoS system class, packets are dropped during data transmission.
Pin Group drop-down list	This is a <i>display-only</i> field.
Adapter Policy field	This field is autopopulated with Linux .
Dynamic vNIC Connection Policy drop-down list	This is a <i>display-only</i> field.
QoS Policy drop-down list	Choose the quality of service policy that is used by the vNICs created from this vNIC policy.
Network Control Policy drop-down list	This is a <i>display-only</i> field.

Step 3 Click **Submit**.

Step 4 Click **Next**.

What to do next

Create a boot order policy.

Creating a Boot Order Policy

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu, and determines the following:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

Step 1 On the **Create Boot Order Policy** page of the **Create UCS SP Template for Big Data** wizard, set the boot order for the following devices:

- **CD-ROM**
- **Storage**
- **LAN**

If you do not want to boot from a specific device, choose the blank space at the bottom of the drop-down list.

Note If you are booting for the first time, choose **1** for the LAN drop-down list to set it as the first boot device.

Step 2 In the **Select vNIC Policy for LAN Ethernet** table, click **Add (+)**.

Step 3 On the **Add Entry to Select vNIC Policy for LAN Ethernet** screen, do the following:

- a) From the **Select vNIC** drop-down list, choose the vNIC that you want to assign to the LAN.
- b) If you want the VLAN shown in the **VLAN** field to be the primary VLAN, check the **Set as Primary** check box.
- c) Click **Submit**.

Step 4 If you want to choose vNIC policies for other VLANs, repeat Steps 2 and 3 with a different vNIC from the **Select vNIC** drop-down list.

Step 5 Click **Next**.

What to do next

Create a BIOS policy.

Creating a BIOS Policy

The BIOS policy automates the configuration of certain BIOS settings for the servers in the cluster.



Note All the drop-down lists on the **Create UCS BIOS Policy** page are set to **Platform Default**—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. For more information, see [BIOS Parameters by Server Model](#).

Step 1 On the **Create UCS BIOS Policy** page of the **Create UCS SP Template for Big Data** wizard, complete the following fields:

Name	Description
Main	
Quiet Boot drop-down list	Determines what the BIOS displays during Power On Self-Test (POST).
POST Error Pause drop-down list	Determines what happens when the server encounters a critical error during POST.
Resume AC on Power Loss drop-down list	Determines the server behavior when the power is restored after an unexpected power loss.
From Panel Lockout drop-down list	Determines whether the server ignores the power and reset buttons on the front panel.
Processor	

Name	Description
Turbo Boost	<p>Determines whether the processor uses Intel Turbo Boost Technology. This allows the processor to automatically increase its frequency if it is running below specifications for power, temperature, or voltage.</p> <p>Choose either Enabled or Disabled.</p>
Enhanced Intel SpeedStep	<p>Determines whether the processor uses Enhanced Intel SpeedStep Technology. This allows the system to dynamically adjust processor voltage and core frequency.</p> <p>Choose either Enabled or Disabled.</p>
Hyper Threading	<p>Determines whether the processor uses Intel Hyper-Threading Technology. This allows multithreaded software applications to execute threads in parallel within each processor.</p> <p>Choose either Enabled or Disabled.</p>
Excute Disabled Bit	<p>Classifies the memory areas on the server to specify where the application code can execute.</p> <p>Choose either Enabled or Disabled.</p>
Virtualization Technology	<p>Determines whether the processor uses Intel Virtualization Technology (VT). This allows a platform to run multiple operating systems and applications in independent partitions.</p> <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p> <p>Choose either Enabled or Disabled.</p>
Processor C State	<p>Determines whether the system enters into the power savings mode during idle periods.</p> <p>Choose either Enabled or Disabled.</p>
Processor C1E	<p>Determines whether the CPU transitions to its minimum frequency when entering the C1 state.</p> <p>Choose either Enabled or Disabled.</p>

Name	Description
Processor C3 Report	<p>Determines whether the BIOS sends the C3 report to the operating system. When the OS receives the report, it can transition the processor into the lower C3 power state to decrease energy usage while maintaining optimal processor performance. This option can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not send the C3 report. • ACPI C2—The BIOS sends the C3 report using the ACPI C2 format, allowing the OS to transition the processor to the C3 low-power state. • ACPI C3—The BIOS sends the C3 report using the ACPI C3 format, allowing the OS to transition the processor to the C3 low-power state.
Processor C6 Report	<p>Determines whether the BIOS sends the C6 report to the operating system. When the OS receives the report, it can transition the processor into the lower C6 power state to decrease energy usage while maintaining optimal processor performance.</p> <p>Choose either Enabled or Disabled.</p>
RAS Memory (reliability, availability, and serviceability of the memory)	
NUMA(nonuniform memory access)	<p>Determines the BIOS support for NUMA. Choose either Enabled or Disabled.</p> <ul style="list-style-type: none"> • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.

Step 2 Click Next.

What to do next

Create a Local Disk Configuration Policy.

Creating a Local Disk Configuration Policy

This policy defines disk configuration for disk partitions, and storage local to the server for the selected Hadoop and Splunk container types. It provides a flexible mechanism to define the RAID levels and JBOD configuration for name nodes and data nodes resident in a Hadoop cluster. This policy enables you to set a local disk configuration for all servers associated with a service profile.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, review the following fields:

Name	Description
Configure RAID Policy for the Hadoop cluster table	RAID level configuration for Hadoop NameNode and DataNode (OS and data drives).
Configure Splunk RAID Policy table	RAID level configuration for Splunk Indexer, Search Heads, and Administrative nodes.
Use LVM For Disk Configuration check box	Create Logical Volume Manager (LVM) groups for disk partitions.
Partition Configuration table	Create partitions other than the /, /boot, swap, /tmp, /var/tmp, and /home partitions.

Step 2 Click **Submit**.

What to do next

- Create a Hadoop cluster profile template to deploy a Hadoop cluster.
- Create Cluster Deploy Templates for Hadoop and Splunk Enterprise clusters.

Editing RAID Policy for Hadoop

Use this procedure to edit the local disk drive configuration associated with the hardware RAID controller for C220 and C240 M3/M4/M5 servers, and for the standalone (PCH Controlled SSD disks) on C240 M4/M5 and C220 M5.

Before you begin

Create a Local Disk Configuration Policy.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, choose the node type in the **Configure RAID Policy** table.

Step 2 In the **Configure RAID Policy** table, click the **Edit selected entry in the table below** icon.

Step 3 On the **Edit Configure RAID Policy Entry** screen, complete the following fields:

Name	Description
Node Type	<p>The selected node type.</p> <p>Note The following are the supported nodes:</p> <ul style="list-style-type: none"> • Cluster node is applicable only for MapR cluster • Master and Data Nodes are applicable only for Cloudera and Hortonworks clusters. • Kafka Node is applicable only for Cloudera and Hortonworks clusters. • Edge Node is applicable for all the Hadoop clusters.
OS Disks	
Use HDD drives on servers with insufficient standalone boot drives check box	Allows you to enable an alternate policy for Cisco UCS servers with insufficient standalone boot drives.
Use standalone boot drives check box	By default, this option is checked and disabled. Check this check box for Cisco UCS servers with sufficient standalone boot drives.
RAID Level [OS] drop-down list	Choose the RAID level for the OS (operating system) disks.
Disks Per Group field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either Write through to write data without the RAID controller cache, or Write back to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the Use Cache check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the Use Cache if Bad BBU check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, Write back will be disabled and Write Through will be enabled.
Strip Size (KB) drop- down list	Allows specification, in KB, of the strip size for each disk within a stripe.
Data Disks	
Use JBOD mode [Data] check box	Check the Use JBOD mode [Data] check box to configure Hadoop data disks in JBOD mode.
RAID Level [Data] drop-down list	Choose the RAID level for the Hadoop data disks.

Name	Description
Disks Per Group field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either Write through to write data without the RAID controller cache, or Write back to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the Use Cache check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the Use Cache if Bad BBU check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, Write back will be disabled and Write Through will be enabled.
Strip Size (KB) drop- down	Allows specification, in KB, of the strip size for each disk within a stripe.

Step 4 Click **Submit**.

Editing RAID Policy for Splunk

Use this procedure to edit the local disk drive configuration associated with the hardware RAID controller for C220 and C240 M4/M5 servers, and for the standalone (PCH Controlled SSD disks) on C240 M4/M5 and C220 M5 servers.

Before you begin

- Create a UCS Service Profile Policy for the Splunk cluster deployment.
- Create a Local Disk Configuration Policy.

Step 1 On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, go to the **Configure Splunk RAID Policy** table and choose the node type.

Step 2 Click the **Edit selected entry in the table below** icon.

Step 3 On the **Edit Configure Splunk RAID Policy Entry** screen, complete the following fields:

Name	Description
Node Type	The selected node type.
OS Disks	
Use standalone boot drives check box	By default, this option is checked for Cisco UCS servers with sufficient standalone boot drives.

Name	Description
Use HDD drives on servers with insufficient standalone boot drives check box	Allows you to enable an alternate policy for Cisco UCS servers with insufficient standalone boot drives.
RAID Level [OS] drop-down list	Choose the RAID level for the OS (operating system) disks.
Disks Per Groups field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either Write through to write data without the RAID controller cache, or Write back to write data with the cache.
Read Mode drop down-list	Choose the method to read data from the disks.
Use Cache check box	Check the Use Cache check box to use the RAID controller cache to read and write operations.
Use Cache if Bad BBU check box	Check the Use Cache if Bad BBU check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, Write back will be disabled and Write Through will be enabled.
Strip Size (KB) drop- down list	Allows specification, in KB, of the strip size for each disk within a stripe.
Data Disks for Hot Data	
Use only NVMe disks [Hot] check box	Check the Use only NVMe disks [Hot] check box to choose NVMe disks.
RAID Level [Hot Data] drop-down list	Choose the RAID level for the splunk data disks.
Disks Per Groups field	Specifies the number of disks that can exist per group during RAID configuration.
Write Mode drop-down list	Choose either Write through to write data without the RAID controller cache, or Write back to write data with the cache. This field is not displayed when Use only NVMe disks [Hot] is checked.
Read Mode drop down-list	Choose the method to read data from the disks. This field is not displayed when Use only NVMe disks [Hot] is checked.
Use Cache check box	Check the Use Cache check box to use the RAID controller cache to read and write operations. This field is not displayed when Use only NVMe disks [Hot] is checked.

Name	Description
Use Cache if Bad BBU check box	<p>Check the Use Cache if Bad BBU check box to ensure that if the Battery Backup Unit (BBU) is not available for any reason, Write back will be disabled and Write Through will be enabled.</p> <p>This field is not displayed when Use only NVMe disks [Hot] is checked.</p>
Strip Size (KB) drop- down	<p>Allows specification, in KB, of the strip size for each disk within a stripe.</p> <p>This field is not displayed when Use only NVMe disks [Hot] is checked.</p>
Data Disks for Cold Data	
Same Disk As Hot Data check box	<p>Check the check box to enable that the same disk is configured for Hot Data to also host Cold Data.</p> <p>Note By default, all RAID configurations are available in Data Disks for Cold Data. Checking this check box hides all RAID configuration for cold data.</p>
Data Disks for Frozen Data	
Same Disk As Cold Data check box	<p>Check the check box to enable that the same disk is configured for Cold Data to also host Frozen Data.</p> <p>Note By default, all RAID configurations are available in Data Disks for Frozen Data. Checking this check box hides all RAID configuration for frozen data.</p>

- Note**
- The RAID configuration of Data disks for hot, cold, or frozen data is applicable only for Indexer nodes. The RAID configuration of OS disks applies to Search Head and Administrative nodes.
 - One RAID group is created for each RAID configuration for hot, cold, or frozen data (for example, /data/disk1 for Hot, /data/disk2 for Cold, and /data/disk3 for Frozen).

Configuring Local Disk Partitions

Each partition in the disk has two attributes, mount point and size. You can create, edit, and delete partitions as per your requirements. The **Partition Configuration** table displays the /, /boot, swap, /tmp, /var/tmp, and /home partitions by default. You can update the size allocated for these partitions except for the root (/) and boot (/boot) partitions, but cannot delete the entries.

Table 6: Sample Partitions Table

Mount Point	Size	Editable
/	1 GB with grow	Not Editable
/boot	1024 MB	Not Editable
Swap	Any value	Editable
/tmp	5 GB	Editable
/var/tmp	5 GB	Editable
/home	5 GB	Editable

-
- Step 1** On the **Local Disk Configuration Policy** page of the **Create UCS SP Template for Big Data** wizard, click **Add** in the **Partition Configuration** table.
- Step 2** On the **Add Partition Configuration Entry** screen, enter the mount name in the **Mount Point** field.
- Step 3** Enter the size in the **Size** field. The OS disk partition value can be greater than 50 GB. However, we recommend that you should allocate the OS disk partition value based on the available actual disk size.
- Step 4** Click **Submit**.
-

Creating a Customized Service Profile Template

- Step 1** Choose **Physical > Compute**.
- Step 2** In the left pane, expand the pod and then click the Cisco UCS Manager account.
- Step 3** In the right pane, click **VLANS**.
- Step 4** Click **Add (+)** to add three VLANS for creating three vNIC templates.
- Step 5** In the right pane, click **Organizations**.
- Step 6** Select the organization in which you want to create the service profile template and then click **View Details**.
- Step 7** Click **vNIC Template** and click **Add (+)**.
- Step 8** Create three vNIC templates using the created VLANS.
- Step 9** Click **Boot Policy** and click **Add (+)** to create a Boot policy by adding a local disk.
- Step 10** Click **QoS Policy** and click **Add (+)** to create a QoS policy.
- Step 11** Choose **Policies > Physical Infrastructure Policies > UCS Manager**.
- Step 12** Click **Storage Policy** and specify the Cisco UCS connections for the storage policy.
- Step 13** Click **Network Policy** and specify the required details.
- Step 14** Click **vNIC** and create three vNICs by mapping the vNIC templates. The name of the vNIC should be eth0, eth1, and eth2 respectively. After the service profile template creation, vNIC name will be generated as eth0-1, eth1-2, and eth2-3 respectively.
- Step 15** Click **Placement Policy** and specify the required details.

- Step 16** Choose **Physical > Compute > Organizations**.
- Step 17** Open the root and click **Service Profile Template**.
- Step 18** Click **Add (+)** and choose the created policies and provide the required information.
- Step 19** Click **Submit**.
- Step 20** Log on to UCSM. Launch the created service profile template and update the desired placement as 1, 2, and 3 for the three vNIC templates respectively.
- Step 21** Click **Save Changes**.
- Note** In the Storage module, select the **No vHBAs** option in the **How would you like to configure SAN connectivity?** field. This option does not allow you to create any vHBAs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the SAN.
-

Cloning a Cisco UCS Service Profile Template

- Step 1** Choose **Solutions > Big Data > Containers**.
- Step 2** Click **UCS SP Templates for Big Data**.
- Step 3** Click the row for the template that you want to clone.
- Step 4** Click **Clone**.
- Step 5** In the **UCS SP Template Specification** page of the Clone UCS SP Template for Big Data wizard, do the following:
- Enter a unique name and description for the new service profile template.
 - Choose the Template Type from the drop-down list.
 - Click **Next**, review the information on each page, and modify if necessary.
 - Click **Submit**.
-



CHAPTER 9

Configuring and Deploying Hadoop Cluster Deployment Templates

This chapter contains the following sections:

- [Hadoop Cluster Profile Templates, on page 77](#)
- [Creating a Hadoop Cluster Profile Template, on page 78](#)
- [Cloning a Hadoop Cluster Profile Template, on page 91](#)
- [Creating a Cluster Deployment Template, on page 91](#)

Hadoop Cluster Profile Templates

The Hadoop cluster profile template specifies the number of nodes in the cluster. The template also takes care of provisioning and configuring the Hadoop cluster services. Apache Software Foundation projects around the world develop services for Hadoop deployment and integration. Some Hadoop distributions support only a subset of these services, or have their own distribution-specific services.

Each of the following supplies a dedicated function:



Note You cannot uncheck some of the services because they are necessary to create a Hadoop cluster. All mandatory services are checked by default.

Hadoop Services	Cloudera	MapR	Hortonworks
HDFS	Yes	—	Yes
CLDB	—	Yes	—
YARN/MapReduce	Yes	Yes	Yes
ZooKeeper	Yes	Yes	Yes
HBase	Yes	Yes	Yes
Hive	Yes	Yes	Yes
Oozie	Yes	Yes	Yes

Hadoop Services	Cloudera	MapR	Hortonworks
Hue	Yes	—	—
Spark	Yes	Yes	Yes
Key-Value Store Indexer	Yes	—	—
Solr	Yes	—	—
Sqoop	—	Yes	Yes
Impala	Yes	—	—
Flume	Yes	Yes	—
PIG	—	Yes	Yes
MAHOUT	—	Yes	—
Falcon	—	—	Yes
SmartSense	—	—	Yes
Tez	—	—	Yes
Storm	—	—	Yes
Ganglia/Ambari Metrics	—	—	Yes
Drill	—	Yes	—
Kafka	Yes	—	Yes

Creating a Hadoop Cluster Profile Template

Before you begin

Create a Hadoop cluster Configuration Template.

-
- Step 1** On the menu bar, choose **Solutions > Big Data > Containers**.
- Step 2** On the **Containers** page, click **Hadoop Cluster Profile Templates**.
- Step 3** Click **Add (+)**.
- Step 4** On the **Hadoop Cluster Profile Template** page of the **Create Hadoop Cluster Profile Template** wizard, complete the following fields:

Name	Description
Template Name field	A unique name for the template.
Template Description field	A short description for the template.

Name	Description
Node Count field	The number of nodes in the cluster. The default is four nodes.
Hadoop Distribution drop-down list	The type of Hadoop distribution. The Hadoop cluster services are displayed based on the selected Hadoop distribution.
Hadoop Distribution Version	Choose the Hadoop distribution version.
Hadoop Cluster Configuration Parameters Template drop-down list	Choose the cluster configuration parameters template.
Secure check box	Check this check box if you want to enable security for the cluster. This option is applicable only for MapR cluster.
Storage Pool Disk Grouping Configuration	
No.of disks per pool for the servers with disks 1-12 field	The number of disks per pool for the servers with disks ranging from 1 to 12. This field is displayed only for MapR cluster. You need to enter the value before creating a new node in the MapR cluster.
No.of disks per pool for the servers with disks 13-24 field	The number of disks per pool for the servers with disks ranging from 13 to 24. This field is displayed only for MapR cluster. You need to enter the value before creating a new node in the MapR cluster.
No.of disks per pool for the servers with disks >24 field	The number of disks per pool for the servers with disks ranging from 24 to 96. This field is displayed only for MapR cluster. You need to enter the value before creating a new node in the MapR cluster.

Step 5 Click Next.

What to do next

Create a Services Selection policy.

Creating a Services Selection Policy

The cluster policy contains the Hadoop cluster services that you want to enable in the Hadoop cluster.



Note The **Service Selection Page** displays the Hadoop cluster services, depending on the Hadoop distribution already selected on the **Hadoop Cluster Profile Template** page.

Step 1 On the **Services Selection Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Check the check box for the optional Hadoop cluster services that you want to enable in your cluster.

Some Hadoop cluster services are required for the distribution and cannot be disabled. The available Hadoop cluster services include the following:

- **HDFS**—A file system that spans all nodes in a Hadoop cluster for data storage. This service replicates data across multiple nodes to avoid data loss.
- **YARN**—A resource-management platform responsible for managing compute resources in clusters and using them for scheduling your applications.
- **HBase**—A high-speed read and write column-oriented database.
- **Hive**—The query engine framework for Hadoop that facilitates easy data summarization, ad-hoc queries, and the analysis of large data sets stored in HDFS and HBase. With SQL-like semantics, Hive makes it easy for RDBMS users to transition into querying unstructured data in Hadoop.
- **Oozie**—A workflow environment for coordinating complex data processing operations.
- **ZooKeeper**—An infrastructure for cross-node synchronization. The applications ensure that tasks across the cluster are serialized or synchronized.
- **Hue**—An interface that aggregates the most common Hadoop components to improve user experience. This allows you to avoid the underlying complexity of the system, and bypasses the command-line interface.
- **Spark**—An open-source data analytics engine.
- **Key-Value Store Indexer**—A method for indexing data across the cluster.
- **SOLR**—A method for searching data across the cluster.
- **Sqoop**—A client-server tool that transfers bulk data between Hadoop and structured data stores, such as relational databases.
- **Impala**—A massively parallel processing (MPP) SQL query engine that runs natively in Apache Hadoop.
- **Flume**—A distributed, reliable, and available service for efficiently collecting, aggregating, and moving large amounts of streaming data into the Hadoop Distributed File System (HDFS).
- **SmartSense**—A server that analyzes the cluster diagnostic information and produces recommended configurations affecting performance, security, and operations.
- **Kafka**—A fast, scalable, durable, and fault-tolerant publish-subscribe messaging system.

Step 3 Click Next.

What to do next

Configure the Rack Assignment policy.

Configuring the Rack Assignment Policy

Step 1 On the **Rack Assignment Policy** page of the **Create Hadoop Cluster Profile Template** wizard, you can:

- Create one or more Hadoop node configuration policies. Click **Add (+)**, and continue with Step 2.

- Modify the default node configuration policy. Choose the default policy in the table. Click **Edit**, and continue with Step 2.

Step 2 On the **Add Entry to Hadoop Node Configuration Policy** screen, do the following:

- In the **Rack Name** field, enter the name of the rack server.
- In the **DataNodes** field, click **Select** and check the check box for each node that you want to configure on that server.

Note Some Hadoop cluster services require a minimum number of nodes. For example, ZooKeeper requires a minimum of three nodes.

- Click **Submit**.

Step 3 Click **Next**.

What to do next

Configure the HDFS policy.

Configuring the HDFS Policy

Step 1 On the **HDFS Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Click the row in the table with the node for which you want to change the HDFS policy configuration, and click **Edit**.

Step 3 On the **Edit HDFS Policy Entry** screen, review and, if necessary, change the following fields:

- Choose **Yes** from the **DataNode** drop-down list if you want the node to act as the DataNode for HDFS. The data nodes store and retrieve data on request by the name node or by the client.

Note The node that act as a DataNode for HDFS is not allocated to Node1, Node2, and Node3 when the

 - node count is greater than 5 for Cloudera
 - node count is greater than 3 for Hortonworks.
- Choose **Yes** from the **Primary NameNode** drop down-list if you want the node to act as the primary name node for HDFS. The primary name node maintains all the operations of the HDFS cluster. There can be only one primary name node for the HDFS cluster.
- Choose **Yes** from the **Secondary NameNode** drop down-list if you want the node to act as a secondary name node for HDFS. The secondary name node is not a direct replacement for the primary name node. The main role of a secondary name node is to periodically merge the FSImage and edit log, to prevent the edit log from becoming too large. A secondary name node runs on a separate physical system because it requires more memory to merge two files. It keeps a copy of the merged file in its local file system so that it is available for use if the primary name node fails.
- Choose **Yes** from the **Balancer** drop down-list if you want the node to act as a balancer for HDFS.
- Choose **Yes** from the **HTTPFS** drop down-list if you want the node to act as HTTPFS for HDFS. This service provides HTTP access to HDFS.
- Choose **Yes** from the **Fail Over Controller** drop down-list if you want the node to act as Fail Over Controller for HDFS.
- Choose **Yes** from the **Gateway** drop down-list if you want the node to act as Gateway for HDFS.

Step 4 Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for HDFS.

Step 6 Click **Next**.

What to do next

Configure the CLDB policy.

Configuring the CLDB Policy

Step 1 On the **CLDB Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Click the row in the table with the node for which you want to change the CLDB policy configuration, and click **Edit**.

Step 3 On the **Edit CLDB Policy Entry** screen, choose **Yes** if you want the node to act as a CLDB agent.

Step 4 Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for CLDB.

Step 6 Click **Next**.

What to do next

Configure the YARN policy.

Configuring the YARN Policy

Step 1 On the **YARN Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Click the row in the table with the node for which you want to change the YARN policy configuration, and click **Edit**.

Step 3 On the **Edit YARN Policy Entry** screen, review and, if necessary, change the following fields:

- a) Choose **Yes** from the **Resource Manager** drop-down list if you want the node to act as a Resource Manager. The Resource Manager is the ultimate authority that allocates resources among all the applications in the system.
- b) Choose **Yes** from the **Node Manager** drop down-list if you want the node to act as a task Node Manager. The Node Manager is responsible for launching the applications' containers, monitoring their resource usage (CPU, memory, disk, network), and reporting to the Resource Manager.

Note The node that act as a DataNode for HDFS is not allocated to Node1, Node2, and Node3 when the

- node count is greater than 5 for Cloudera
- node count is greater than 3 for Hortonworks.

c) Choose **Yes** from the **Gateway** drop down-list if you want the node to act as a Gateway.

d) Choose **Yes** from the **JobHistory** drop down-list if you want the node to preserve the Job History.

e) Click **Submit**.

Step 4 Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for Yarn.

Step 6 Click **Next**.

What to do next

Configure the ZooKeeper policy.

Configuring the ZooKeeper Policy



Note Configure a minimum of three nodes for ZooKeeper.

- Step 1** On the **ZooKeeper Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the ZooKeeper policy configuration, and click **Edit**
- Step 3** On the **Edit ZooKeeper Policy Entry** screen, choose **Yes** to make the node to act as a ZooKeeper.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for ZooKeeper.
- Step 6** Click **Next**.
-

What to do next

Configure the HBase policy.

Configuring the Kafka Policy

-
- Step 1** On the **Kafka Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Kafka policy configuration, and click **Edit**.
- Step 3** On the **Edit Kafka Policy Entry** screen, choose **Yes** from the **Kafka Broker** drop-down list if you want the node to act as a Kafka broker.
- Note** All nodes are Kafka nodes, only if **Kafka** and **Zookeeper** check boxes are selected in the **Services Selection Policy** page while creating Cloudera or Hortonworks clusters. If it is a HDFS and Kafka cluster, then last two nodes of the template are selected for kafka by default.
- Note** Addition of Kafka role is not supported in Cloudera and Hortonworks clusters.
- Note** Adding an additional Kafka node to an existing cluster (with working Kafka nodes) is not supported.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Kafka.

Step 6 Click **Next**.

Configuring the HBase Policy

- Step 1** On the **HBase Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the HBase policy configuration, and click **Edit**.
- Step 3** On the **Edit HBase Policy Entry** screen, review and, if necessary, change the following fields:
- Choose **Yes** from the **HBase Master** drop-down list if you want the node to act as a HBase master.
 - Choose **Yes** from the **Region Server** drop down-list if you want the node to act as a region server.
- Note** The node that act as a DataNode for HDFS is not allocated to Node1, Node2, and Node3 when the
- node count is greater than 5 for Cloudera
 - node count is greater than 3 for Hortonworks.
- Choose **Yes** from the **HBase Thrift Server** drop down-list if you want the node to act as a HBase Thrift.
 - Click **Submit**.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for HBase.
- Step 6** Click **Next**.
-

What to do next

Configure the Hive policy.

Configuring the Hive Policy

- Step 1** On the **Hive Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Hive policy configuration, and click **Edit**.
- Step 3** On the **Edit Hive Policy Entry** screen, review and, if necessary, change the following fields:
- Choose **Yes** from the **HiveServer2** drop-down list if you want the node to act as a HiveServer2.
 - Choose **Yes** from the **Hive Metastore Server** drop down-list if you want the node to act as a Hive metastore.
 - Choose **Yes** from the **WebHCat** drop down-list if you want the node to act as a WebHCat. WebHCat is the REST API for HCatalog, a table and storage management layer for Hadoop.
 - Choose **Yes** from the **Gateway** drop down-list if you want the node to act as a Gateway for Hive.
 - Click **Submit**.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Hive.

Step 6 Click **Next**.

What to do next

Configure the Oozie policy.

Configuring the Oozie Policy

- Step 1** On the **Oozie Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Oozie policy configuration, and click **Edit**.
- Step 3** On the **Edit Oozie Policy Entry** screen, choose **Yes** to make the node to act as an Oozie server.
- Step 4** Repeat Steps 1 and 2 to configure the other nodes for Oozie.
- Step 5** Click **Next**.
-

What to do next

Configure the Hue policy.

Configuring the Hue Policy

- Step 1** On the **Hue Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Hue policy configuration, and click **Edit**.
- Step 3** On the **Edit Hue Policy Entry** screen, do the following:
- Choose **Yes** from the **Hue Server** drop-down list if you want the node to act as a Hue server.
 - Choose **Yes** from the **BeesWax Server** drop down-list if you want the node to act as a BeesWax server.
 - Choose **Yes** from the **Kt Renewer** drop down-list if you want the node to act as a Kt Renewer.
 - Click **Submit**.
- Step 4** Repeat Steps 1 and 2 to configure the other nodes for Hue.
- Step 5** Click **Next**.
-

What to do next

Configure the Spark policy.

Configuring the Spark Policy

- Step 1** On the **Spark Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Spark policy configuration, and click **Edit**.

- Step 3** On the **Edit Spark Policy Entry** screen, review and, if necessary, change the following fields:
- Choose **Yes** from the **History Server** drop-down list if you want the node to act as a History Server.
 - Choose **Yes** from the **Gateway** drop down-list if you want the node to act as a gateway.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Spark.
- Note** When Spark applications run on a YARN cluster manager, resource management, scheduling, and security are controlled by YARN. In Cloudera cluster, configuring th Spark on Yarn policy is supported.
- Step 6** Click **Next**.

What to do next

Configure the Key-Value Store Indexer policy.

Configuring the Key-Value Store Indexer Policy

- Step 1** On the **Key-Value Store Indexer Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Key-Value Store Indexer policy configuration, and click **Edit**.
- Step 3** On the **Edit KSIndexer Policy Entry** scree, choose **Yes** if you want the node to act as a KSIndexer server.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for KSIndexer.
- Step 6** Click **Next**.

What to do next

Configure the Solr policy.

Configuring the Solr Policy

- Step 1** On the **Solr Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Solr policy configuration, and click **Edit**.
- Step 3** On the **Edit Solr Policy Entry** screen, choose **Yes** if you want the node to act as a Solr server.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Solr.
- Step 6** Click **Next**.
-

What to do next

Configure the Sqoop policy.

Configuring the Sqoop Policy

- Step 1** On the **Sqoop Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
 - Step 2** Click the row in the table with the node for which you want to change the Sqoop policy configuration, and click **Edit**.
 - Step 3** On the **Edit Sqoop Policy Entry** screen, choose **Yes** if you want the node to act as a Sqoop server.
 - Step 4** Click **Submit**.
 - Step 5** Repeat Steps 1 and 2 to configure the other nodes for Sqoop.
 - Step 6** Click **Next**.
-

What to do next

Configure the Impala policy.

Configuring the Impala Policy

- Step 1** On the **Impala Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
 - Step 2** Click the row in the table with the node for which you want to change the Impala policy configuration, and click **Edit**.
 - Step 3** On the **Edit Impala Policy Entry** screen, do the following:
 - a) Choose **Yes** from the **Impala Daemon** drop-down list if you want the node to act as an Impala daemon.
 - b) Choose **Yes** from the **Impala StateStore** drop-down list if you want the node to act as an Impala Statestore.
 - c) Choose **Yes** from the **Impala Catalog Server** drop-down list if you want the node to act as an Impala catalog server.

The other fields in this dialog box are for your information only.

 - d) Click **Submit**.
 - Step 4** Repeat Steps 1 and 2 to configure the other nodes for Impala.
 - Step 5** Click **Submit**.
-

What to do next

Configure the Flume policy.

Configuring the Flume Policy

- Step 1** On the **Flume Policy** page of the **Create Hadoop Cluster Profile Template** wizard do the following:
- Step 2** Click the row in the table with the node for which you want to change the Flume policy configuration, and click **Edit**.

- Step 3** On the **Edit Flume Policy Entry** screen, choose **Yes** if you want the node to act as a Flume agent.
 - Step 4** Click **Submit**.
 - Step 5** Repeat Steps 1 and 2 to configure the other nodes for Flume.
 - Step 6** Click **Next**.
-

What to do next

Configure the PIG Policy.

Configuring the PIG Policy

- Step 1** On the **Pig Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
 - Step 2** Click the row in the table with the node for which you want to change the Pig policy configuration, and click **Edit**.
 - Step 3** On the **Edit Pig Policy Entry** screen, choose **Yes** if you want the node to act as a Pig agent.
 - Step 4** Click **Submit**.
 - Step 5** Repeat Steps 1 and 2 to configure the other nodes for Pig.
 - Step 6** Click **Next**.
-

What to do next

Configure the MAHOUT Policy.

Configuring the MAHOUT Policy

- Step 1** On the **MAHOUT Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
 - Step 2** Click the row in the table with the node for which you want to change the MAHOUT policy configuration, and click **Edit**.
 - Step 3** On the **Edit MAHOUT Policy Entry** screen, choose **Yes** if you want the node to act as a MAHOUT agent.
 - Step 4** Click **Submit**.
 - Step 5** Repeat Steps 1 and 2 to configure the other nodes for MAHOUT.
 - Step 6** Click **Submit**.
-

What to do next

Configure a Falcon Policy.

Configuring the Falcon Policy

- Step 1** On the **Falcon Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Falcon policy configuration, and click **Edit**.
- Step 3** On the **Edit Falcon Policy Entry** dialog box, choose **Yes**. You can make the node act as a Falcon server from the **Falcon Server** and the Falcon client from **Falcon Client** drop-down lists.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Falcon.
- Step 6** Click **Submit**.
-

What to do next

Configure the Tez Policy.

Configuring the Tez Policy

- Step 1** On the **Tez Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Tez policy configuration, and click **Edit**.
- Step 3** On the **Edit Tez Policy Entry** screen, choose **Yes** if you want the node to act as a Tez agent.
- Step 4** Click **Submit**.
- Step 5** Repeat Steps 1 and 2 to configure the other nodes for Tez.
- Step 6** Click **Submit**.
-

What to do next

Configure the Storm Policy.

Configuring the Storm Policy

- Step 1** On the **Storm Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:
- Step 2** Click the row in the table with the node for which you want to change the Storm policy configuration, and click **Edit**.
- Step 3** On the **Edit Storm Policy Entry** screen, do the following:
- Choose **Yes** in the **DRPC Server** drop-down list if you want the node to act as a DRPC server.
 - Choose **Yes** in the **Nimbus** drop-down list if you want the node to act as a Nimbus server.
 - Choose **Yes** in the **Storm REST API Server** drop-down list if you want the node to act as a Storm REST API server.
 - Choose **Yes** in the **Storm UI Server** drop-down list if you want the node to act as a Storm UI server.
 - Choose **Yes** in the **Supervisor** drop-down list if you want the node to act as a supervisor.
- Step 4** Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for Storm.

Step 6 Click **Submit**.

What to do next

Configure the Ganglia Policy.

Configuring the Ganglia Policy

Step 1 On the **Ganglia Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Click the row in the table with the node for which you want to change the Ganglia policy configuration, and click **Edit**.

Step 3 On the **Edit Ganglia Policy Entry** screen, choose **Yes**. You can make the node to act as a Ganglia server from the **Ganglia Server** and the Ganglia monitor from the **Ganglia Monitor** drop-down lists.

Step 4 Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for Ganglia.

Step 6 Click **Submit**.

Configuring the SmartSense Policy



Note SmartSense policy is supported only for Hortonworks 3.0.0 clusters.

Step 1 On the **SmartSense Policy** page of the **Create Hadoop Cluster Profile Template** wizard, do the following:

Step 2 Click the row in the table with the node for which you want to change the SmartSense policy configuration, and click **Edit**.

Step 3 On the **Edit SmartSense Policy Entry** screen, review and, if necessary, change the following fields:

Note For more information on the selecting the HST server and HST agent and configuring SmartSense gateway, see the SmartSense Installation guide available in <https://docs.hortonworks.com/>.

- a) Choose **Yes** from the **HST Server** drop-down list if you want the node to act as a HST server.
- b) Choose **Yes** from the **HST Agent** drop-down list if you want the node to act as a HST agent.
- c) Choose **Yes** from the **Activity Analyzer** drop-down list if required.
- d) Choose **Yes** from the **Activity Explorer** drop-down list if required.

Step 4 Click **Submit**.

Step 5 Repeat Steps 1 and 2 to configure the other nodes for SmartSense.

Step 6 Click **Next**.

Cloning a Hadoop Cluster Profile Template

- Step 1** On the menu bar, choose **Solutions > Big Data > Containers**.
- Step 2** On the **Containers** page, click the **Hadoop Cluster Profile Templates**.
- Step 3** Click the row for the template that you want to clone.
- Step 4** Click **Clone**.
- Step 5** On the **Clone Hadoop Cluster Profile Template** screen, do the following:
- Enter a unique name and description for the new Hadoop cluster profile template.
 - Click **Next**, review the information on each page, and modify, if necessary.
 - Click **Submit**.

Creating a Cluster Deployment Template

Before you begin

- Create a Cisco UCS Service Profile Template for Big Data
- Create a Hadoop Cluster Profile Template

- Step 1** Choose **Solutions > Big Data > Containers**.
- Step 2** Click **Cluster Deploy Templates**.
- Step 3** Click **Add (+)**.
- Step 4** On the **Add Cluster Deploy Template** screen, complete the following fields:

Name	Description
Template Name field	Enter a unique name for the Hadoop cluster deployment template.
Description field	Enter a short description of the template.
Container Type drop-down list	Choose the type of container for the cluster.
Select UCS Template drop-down list	Choose the UCS service profile template for Big Data that you want to use in the Hadoop cluster. Note If you choose Splunk as the container type, choose the UCS service profile template for Big Data with Splunk software to create a Splunk cluster.

Name	Description
Hadoop Cluster Profile Template drop-down list	Choose the Hadoop cluster profile template that you want to use. This option is displayed when you choose the container type as Hadoop.

Step 5 Click **Add**.



CHAPTER 10

Managing Hadoop Clusters

This chapter contains the following sections:

- [Creating an Instant Hadoop Cluster](#), on page 93
- [Creating a Customized Hadoop Cluster](#), on page 97
- [Creating a Hadoop Cluster Using Workflow](#), on page 101
- [Provisioning an Instant and Customized Hadoop Cluster](#), on page 101
- [Managing a Hadoop Cluster](#), on page 103
- [Managing Nodes in a Cluster](#), on page 107
- [Delete Node and Delete Node to Bare Metal Actions in Cloudera and Hortonworks](#), on page 109
- [Deleting an Unreachable Node from Hadoop Distribution](#), on page 109
- [Adding Managed Nodes to the Hadoop Cluster](#), on page 111
- [Adding Live Nodes to the Hadoop Cluster](#), on page 111
- [Adding Bare Metal Nodes to the Hadoop Cluster](#), on page 112
- [Adding Disks to the Hadoop Cluster](#), on page 114
- [Service Roles](#), on page 115

Creating an Instant Hadoop Cluster

Before you begin

- Create a service profile template .
- Create a server pool in the Cisco UCS Manager account that you plan to use for this cluster. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
- Create a MAC address pool .

-
- Step 1** Choose **Solutions > Big Data > Containers**.
 - Step 2** Click **Cluster Deploy Templates**.
 - Step 3** Click **Instant Hadoop Cluster**.
 - Step 4** On the **Instant Hadoop Cluster Creation** screen, complete the following fields.

Name	Description
Big Data Account Name field	Enter the name of the Big Data account.
UCSM Policy Name Prefix field	Enter the UCSM Policy Name prefix.
Hadoop Cluster Name field	Enter a unique name for the Hadoop cluster.
Hadoop Node Count field	Enter the number of nodes in the Hadoop cluster.
SSH (root) Password field	<p>Enter the SSH root password. Special characters such as \$, %, and & are not supported.</p> <p>Note The SSH username pertains to the root user.</p>
Confirm SSH Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Hadoop Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
Confirm Hadoop Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
Host Node Prefix field	Enter the Host Node prefix for the cluster.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Hadoop Distribution drop-down list	Choose the Hadoop distribution to be used for this cluster.
Hadoop Distribution Version drop-down list	Choose the Hadoop distribution version.
Management Console Protocol drop-down list	<p>Choose HTTP or HTTPS protocol.</p> <p>Note Only HTTPS protocol is supported in MapR.</p>
Management Port Number field	<p>Enter the port number. Enter an integer between 1024 and 65535.</p> <p>Usage of reserved ports by Hadoop services or Linux OS should be avoided so that the web server path is reachable.</p> <p>Note Management port number is supported only in MapR 6.0 version.</p>
Oracle JDK drop-down list	Choose the Oracle JDK version.
External Database drop-down list	Choose an external database. You can also configure a new database from here.

Name	Description
Multi-UCSM check box	<p>Check the Multi-UCSM check box if you use multiple UCSM accounts.</p> <p>Note If you use the multiple UCSM accounts option, you can configure the Hadoop Server Roles as described in Step 5. You can add UCSM Specific Inputs in the Add Entry to UCSM Specific Inputs table.</p> <p>The following workflows are established during an Instant and Customized Hadoop Cluster creation:</p> <ul style="list-style-type: none"> • UCS CPA Multi-UCSM Hadoop Cluster WF • Single UCSM Server Configuration WF. (This WF is triggered per UCSM Account. For example, UCSM 120, UCSM121.) • UCS CPA Node Bare Metal. (This WF is triggered per Node.) <p>The UCSM Specific Input area is displayed when the Multi-UCSM check box is checked.</p>
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account for this cluster.
Organization drop-down list	Choose the organization in which the servers for this cluster are located.
UCS SP Template table	Choose an existing UCS Service Profile Template for cluster creation.
SSD Boot Drives Available for OS check box	<p>Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain Solid-State Drive (SSD).</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p>
PXE VLAN ID field	Enter the PXE VLAN ID.
UCS SP Template table	Choose an existing UCS Service Profile Template for Hadoop cluster creation.

Step 5 If you want to edit a Hadoop Server Role, select the row for that role, and click **Edit**.

Step 6 On the **Edit Hadoop Server Roles Entry** screen, complete the following fields and click **Submit**.

Name	Description
Node Type field	Displays the Hadoop node role. Note Kafka node is supported only for Cloudera and Hortonworks clusters. Note Cloudera clusters with Data node require a minimum of three Master nodes and three Data nodes. Also, the Data node should have minimum 14 disks since the tolerance value is set to 6.
Node Count field	The number of nodes in the Hadoop cluster for the selected node type.
SSD Boot Drives Available for OS check box	Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD. If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level. Note This check box is not displayed when the UCSM version is greater than or equal to 3.
Server Pool table	Enter the server pool that you want to use for the cluster for the selected node type. The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.

Step 7 In the **vNIC Template** table, review and, if necessary, edit the vNIC templates available for the cluster.

Step 8 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 9 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	The vNIC name in the selected template. This field is for your information only.
IP Pool drop-down list	Choose the big data IP pool that you want to use for IP addresses assigned to this vNIC.
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
First MAC Address field	Enter the MAC address pool that you want to use for this cluster.

Name	Description
Size field	Enter the size. (This field is disabled if an existing UCS SP Template is selected.)
VLAN ID field	Enter the VLAN ID for this cluster. (This field is disabled if an existing UCS SP Template is selected.)

Step 10 Click **Submit**.

What to do next

You can view and monitor the workflow that is triggered after you create an instant Hadoop cluster.

Creating a Customized Hadoop Cluster

Before you begin

- Create a service profile template.
- Create a Hadoop cluster profile template.
- Setup the details for Hadoop Config Parameters.
- Create a Hadoop cluster deployment template that Cisco UCS Director Express for Big Data uses to create the Hadoop cluster.
- Create a server pool in the Cisco UCS Manager account you plan to use for this cluster. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
- Create a MAC address pool.

Step 1 Choose **Solutions > Big Data > Containers**.

Step 2 Click **Cluster Deploy Templates**.

Step 3 Select the template that you want to use for the Hadoop cluster and click **Customized Hadoop Cluster**.

Step 4 On the **Customized Hadoop Cluster Creation** screen, complete the following fields.

Name	Description
Big Data Account Name field	Enter the name of the Big Data account.
UCSM Policy Name Prefix field	Enter the UCSM Policy Name prefix.
Hadoop Cluster Name field	Enter a unique name for the Hadoop cluster.
Hadoop Node Count field	Enter the number of nodes in the Hadoop cluster.

Name	Description
SSH (root) Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported. Note The SSH username pertains to the root user.
Confirm SSH Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Hadoop Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
Confirm Hadoop Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
Host Node Prefix field	Enter the Host Node prefix for the cluster.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Hadoop Distribution drop-down list	Choose the Hadoop distribution to be used for this cluster.
Hadoop Distribution Version drop-down list	Choose the Hadoop distribution version.
Management Console Protocol drop-down list	Choose HTTP or HTTPS protocol. Note Only HTTPS protocol is supported in MapR.
Management Port Number field	Enter the port number. Enter an integer between 1024 and 65535. Usage of reserved ports by Hadoop services or Linux OS should be avoided so that the web server path is reachable. Note Management port number is supported only in MapR 6.0 version.
Oracle JDK drop-down list	Choose the Oracle JDK version.
External Database drop-down list	Choose an external database. You can also configure a new database from here.

Name	Description
<p>Multi-UCSM check box</p>	<p>Click the Multi-UCSM check box if you use multiple UCSM accounts.</p> <p>Note If you use the multiple UCSM accounts option, you can configure the Hadoop Server Roles as described in Step 5. You can add UCSM Specific Inputs in the Add Entry to UCSM Specific Inputs table.</p> <p>The following workflows are created during an Instant Hadoop cluster creation and Customized Hadoop cluster creation:</p> <ul style="list-style-type: none"> • UCS CPA Multi-UCSM Hadoop Cluster WF • Single UCSM Server Configuration WF. (This WF is triggered per UCSM Account. For example, UCSM 120, UCSM121.) • UCS CPA Node Bare Metal. (This WF is triggered per Node.) <p>The UCSM Specific Input area is displayed when the Multi-UCSM check box is checked.</p>
<p>UCS Manager Account drop-down list</p>	<p>Choose the Cisco UCS Manager account for this cluster.</p>
<p>Organization drop-down list</p>	<p>Choose the organization in which the servers for this cluster are located.</p>
<p>SSD Boot Drives Available for OS check box</p>	<p>Click this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD.</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p>
<p>PXE VLAN ID field</p>	<p>Enter the PXE VLAN ID.</p>
<p>UCS SP Template table</p>	<p>Choose an existing UCS Service Profile Template for Hadoop cluster creation.</p>

Step 5

If you want to edit a Hadoop Server Role, select the row for that role, and click **Edit**.

Step 6

On the **Edit Hadoop Server Roles Entry** screen, complete the following fields and click **Submit**.

Name	Description
<p>Node Type field</p>	<p>Displays the Hadoop node role.</p>
<p>Node Count field</p>	<p>The number of nodes in the Hadoop cluster for the selected node type.</p>

Name	Description
SSD Boot Drives Available for OS check box	<p>Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD.</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p> <p>Note This check box is not displayed when the UCSM version is greater than or equal to 3.</p>
Server Pool table	<p>Enter the server pool that you want to use for the cluster for the selected node type.</p> <p>The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.</p>

Step 7 In the **vNIC Template** table, review and, if desired, edit the vNIC templates available for the cluster.

Step 8 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 9 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	The vNIC name in the selected template. This field is for your information only.
IP Pool field	Choose the big data IP pool that you want to use for IP addresses assigned to this vNIC.
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
First MAC Address field	Enter the MAC address.
Size field	Enter the size.
VLAN ID field	The VLAN ID for this cluster. (This field is disabled if an existing UCS SP Template is selected.)

Note When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool, and VLAN ID to the first vNIC in the **vNIC Template** table.

Step 10 Click **Submit**.

What to do next

You can view and monitor the workflow that gets triggered after creating a customized Hadoop cluster.

Creating a Hadoop Cluster Using Workflow

In Cisco UCS Director Express for Big Data, administrator can map the advanced catalog option to Hadoop cluster creation workflow, with limited user inputs, so that the service end user can trigger cluster creation. See [Cisco UCS Director End User Portal Guide](#).

Before you begin

- Create a service profile template
- Create a server pool in the Cisco UCS Manager account that you plan to use for this cluster. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
- Create a MAC address pool
- Create a user with user role as service end user.

-
- Step 1** Log into Cisco UCS Director Express for Big Data using admin credentials.
- Step 2** Choose **Orchestration** and click **Workflows**.
- Step 3** Click **Add Workflow**.
- Step 4** On the **Add Workflow Details** page, enter the workflow name and choose a folder. Click **Next**.
- Step 5** On the **Add User Inputs** page, enter the required details and click **Next**.
- Step 6** On the **Add User Outputs** page, enter the required details and click **Submit**.
- Step 7** Double-click the workflow in the **Workflow Designer**.
- Step 8** Add the Initiate Hadoop Cluster task.
- Step 9** Select the attributes that you want to map to the workflow input fields. Check the **Map to User Input** check box to provide user inputs, if required.
- Step 10** Enter required details in the **Hadoop Service Role** table and **vNIC Template** table, and click **Submit**.
- Step 11** Choose **Policies > Catalogs** and click **Add Catalog**.
- Step 12** On the **Add Catalog page**, choose the catalog type as Advanced and select a workflow. Click **Submit** to map the workflow to the catalog.
- Step 13** Log into Cisco UCS Director Express for Big Data using service end user credentials.
- Step 14** Choose **Catalogs**. The **Catalogs** page displays the list of catalogs available for the service end user.
- Step 15** Select a catalog and click **Create Request**. The **Create Server Request** page displays the mapped user inputs.
- Step 16** Specify the required details.
- Step 17** Click **Next** and enter the cluster details in the **Customize Workflow** page.
- Step 18** Click **Next** and view the cluster details in the **Summary** page.
- Step 19** Click **Submit** to trigger a workflow for creating a Hadoop cluster.
-

Provisioning an Instant and Customized Hadoop Cluster

Create and customize a Cluster Deploy Template to trigger the workflow.

Before you begin

- Create a UCS Service Profile template for a Customized Hadoop Cluster
- Create a Hadoop Cluster Profile template for a Customized Hadoop Cluster

Step 1 Choose **Policies > Orchestration**.

Step 2 Click the **UCS CPA** folder from the **Workflows** tab.

Step 3 Double-click the workflow to open the workflow designer and execute the workflow.

- a) When you open the workflow designer for an instant Hadoop Cluster, you get the following tasks, which are processed sequentially.

Task Name	Description
Instant Hadoop Cluster UCS SP	Cisco UCS Director Express for Big Data automatically specifies parameters for installing the OS and Hadoop distribution software at the back end.
Instant Hadoop Cluster Profile	Cisco UCS Director Express for Big Data automatically configures Hadoop cluster services at the back end.
Setup Hadoop Cluster Env	Sets up the environment for cluster-specific scripts and software files.
Muti Bare Metal OS Install WF	Attaches the UCS profile and sets up all boot files required to boot the operating system (Linux). When the Power ON task is executed, the boot files are picked up, and the operating system is installed successfully.
Multi Bare Metal WF Monitor	Checks the status of bare metal OS install workflow.
Synchronized Command Execution	—
Custom SSH Command	Installs and configures the Hadoop distribution software.
Provision Hadoop Cluster	Sends the Hadoop cluster properties to the Web Console.
Completed	The Hadoop cluster is provisioned successfully. Note If any of the tasks fail, you are informed that the provisioning has failed. For more information on how to monitor the workflow, see Monitoring Service Requests for Big Data , on page 161.

- b) When you open the workflow designer for a customized Hadoop Cluster, you get the following tasks that get processed sequentially.

Task Name	Description
Create UCS Service Profile Template	Specifies parameters for installing the OS and Hadoop distribution software.

Task Name	Description
Create Hadoop Cluster Profile	Configures Hadoop cluster services.
Setup Hadoop Cluster Env	Sets up the environment for cluster-specific scripts and software files.
Muti Bare Metal OS Install WF	Attaches the UCS profile and sets up all boot files required to boot the operating system (Linux). When the Power ON task is executed, the boot files are picked up, and the operating system is installed successfully.
Multi Bare Metal WF Monitor	Checks the status of bare metal OS install workflow.
Synchronized Command Execution	—
Custom SSH Command	Installs and configures the Hadoop distribution software.
Provision Hadoop Cluster	Sends the Hadoop cluster properties to the Web Console.
Completed	The Hadoop cluster is provisioned successfully. Note If any of the tasks fail, you are informed that the provisioning has failed. For more information on how to monitor the workflow, see Monitoring Service Requests for Big Data , on page 161.

Managing a Hadoop Cluster

You can manage an existing cluster.

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Select an account and click **View Details**.
- Step 4** Click **Summary** to view the statistics data report for the selected Hadoop Account and the high-level report on the cluster and node account.
- Step 5** Click **Hosts** to view node details. For more information on **Hosts** page, see [Managing Nodes in a Cluster](#).
- Step 6** Click **Hadoop Clusters** to view the cluster details and list of actions that you can perform on an existing Hadoop cluster.
 - a) Click **Role Topology** to view the topology of the nodes. (This tab is not editable.)
 - b) Click **View Details** to view the inputs for the Hadoop cluster you have created, and to view the virtual network interface configuration. (This information is not editable.)
 - c) Click **Shutdown Cluster** to stop all the services and power off all the nodes in the Hadoop cluster.
 - d) Click **Start Cluster** to power up all the nodes in the Hadoop cluster and start all services in the Hadoop cluster.
 - e) Click **Restart Cluster** to power off and then power up all nodes in the Hadoop cluster.

- f) Click **Rebalance** to configure the threshold percentage to rebalance Hadoop clusters. For MapR cluster, configure the threshold percentage using CLDB Balancer **Disk Paused** and CLDB Balancer **Disk Max Switches in Nodes**.
- g) Click **Upgrade Cluster** to upgrade Hadoop distributions from the current version, if available.

Note For a derived account, install and configure pssh and clush for the nodes in the Hadoop cluster and password less between nodes.

1. Click **Upgrade Cluster**.
2. Choose the JDK version from the **Oracle JDK** drop-down list.
3. Choose the Hadoop distribution that you want to upgrade from the current version from the **Available Version** drop-down list.
4. Check the **Enable HA** check box to enable high availability for the Hadoop cluster, if Cloudera or Hortonworks is the Hadoop distribution.

Note To enable high availability in a Hortonworks cluster, you require a minimum of four nodes and node 1, 2, and 3 should be selected as Journal nodes.

5. Click **Submit**.

- h) Enable Hadoop cluster high availability.

1. Click **Enable High Availability**.
2. From the **Enable High Availability** screen, access the **Standby Name Node** drop-down list and choose the Standby Name Node.
3. Check a minimum of three nodes from the **Journal Nodes** table.

Note Journal nodes selection is recommended to be on first three Master nodes and should be increased by the node count in odd number only.

4. Click **Submit**.

- i) Disable Hadoop cluster high availability. This action is supported only for Cloudera and Hortonworks.

1. Click **Disable High Availability**.
2. From the **Disable High Availability** screen, access the **Standby Name Node** drop-down list and choose the Standby Name Node.
3. Check a minimum of three nodes from the **Journal Nodes** table.

Note Journal nodes selection is recommended to be on first three Master nodes and should be increased by the node count in odd number only.

4. Click **Submit**.

- j) Click **Cluster Snapshot** to view the snapshot.
- k) Click **View Reports** to view performance and monitoring reports.

Step 7 Click **Hadoop Services** to view the list of Hadoop services and their status. You can do the following:

- a) Click **Start All Services** to start all Hadoop services, depending on their status.
- b) Click **Stop All Services** to stop all Hadoop services, depending on their status.

- c) Click **Add New Service** to add a new Hadoop service.
- d) Click **Edit Service** to start and stop a particular Hadoop service.

Step 8 Click **Hadoop Service Roles** to view the list of Hadoop services. You can do the following:

- a) To add a role to the cluster, do the following on the **Add Role** screen:
 1. From the **Hadoop Service Name** drop-down list, choose the Hadoop service.
 2. From the **Role Type** drop-down list, choose the role type.
 3. From the **Node Name** drop-down list, choose the node name.
 4. From the **Role Name** drop-down list, choose the role name.
 5. Click **Submit**.
- b) To start or stop any role that you have created, do the following on the **Start/Stop Role** screen:
 1. From the **Hadoop Service Roles** tab, choose the Hadoop service.
 2. Click **Start/Stop Role**.
 3. Click **Submit**.
- c) To delete a role in the cluster, do the following on the **Delete Role** screen:
 1. From the **Hadoop Service Roles** tab, choose the Hadoop service.
 2. Click **Delete**.
 3. Click **Submit**.

Step 9 Click **More Reports** to view the list of additional reports that you can generate about data usage and CPU utilization.

View Hadoop Cluster Details

For each Big Data Account, use the **Hadoop Clusters** tab to view details of all Hadoop clusters associated with the account. See [Managing a Hadoop Cluster](#)

You can view the following details by clicking **Hadoop Clusters**.

Name	Description
Big Data Account name	The name of the Big Data account.
UCS SP Template for Big Data	The UCS SP Template for Big Data that you used to create service profiles for the servers in the Hadoop cluster.
Hadoop Cluster Profile Template	The Hadoop cluster profile template that you used to configure the cluster services.
Hadoop Cluster Deploy Template	A unique name that you used for the Hadoop cluster deployment template.

Name	Description
UCSM Policy Name Prefix	The UCSM Policy Name prefix.
Hadoop Cluster Name	A unique name that you used for the Hadoop cluster.
Hadoop Node Count	The number of nodes in the Hadoop cluster.
Hadoop Node Prefix	The Host Node prefix for the cluster.
OS Version	The operating system that you installed on the servers for the Hadoop cluster.
Hadoop Distribution	The Hadoop distribution that you used for this cluster.
Hadoop Distribution Version	The Hadoop distribution version that used for this cluster.
PXE VLAN ID	The VLAN ID used for PXE boot of the servers.
UCS Service Profile Template	The UCS Service Profile Template that you specified parameters for installing the OS and Hadoop distribution software.
Host Maintenance Policy	–
Host Firmware Package	–
UCSM Version	Displays the Cisco UCS Manager version
vNIC: eth0	Displays IPv4 network information for the management interface and the management VLAN ID.
vNIC: eth1	Displays IPv4 network information for the DATA1 interface and the VLAN ID. This field is not displayed when the Use one vNIC check box is selected while creating a Cisco UCS Service Profile Template for Big Data.
vNIC: eth2	Displays IPv4 network information for the DATA2 interface and the VLAN ID. This field is not displayed when the Use one vNIC check box is selected while creating a Cisco UCS Service Profile Template for Big Data.

Viewing a Cluster Snapshot

A cluster snapshot displays configuration details of a Hadoop cluster, such as hosts, roles, and services. To view the current snapshot of a cluster, do the following:

Step 1 Choose **Solutions > Big Data > Accounts**.

- Step 2** Click **Hadoop Accounts**.
- Step 3** Choose the Hadoop Account for which you want to view the snapshot and click **View Details**.
- Step 4** Click **Hadoop Clusters**.
- Step 5** Choose the Hadoop cluster for which you want to view the snapshot and click **Cluster Snapshot**.
- Step 6** Click **Submit**.
You can view the snapshot for the selected Hadoop cluster.

Adding a New Hadoop Service

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Choose a Cloudera account for which you can add a new Hadoop service.
Adding a new Hadoop service is not supported for MapR and Hortonworks distributions.
- Step 3** Click **View Details**.
- Step 4** Click **Hadoop Services**.
- Step 5** Click **Add New Service**.

On the **Add New Service** screen, complete the following fields:

Name	Description
Workflow Inputs	
(Hadoop) Account Name	Choose the Cloudera Account.
Service Type	Enter the Hadoop service for Cloudera.
Role Assignment Pairs	Enter Role Assignment Pairs, separated by commas. For example, RoleType1:hostname1, RoleType2:hostname2
Dependant Services	Enter the list of dependent services. Use commas to separate list entries.
Pre Install Commands	Enter the list of commands. Use the "\n" command to insert a new line after each list entry.
Post Install Commands	Enter the list of commands. Use the "\n" command to insert a new line after each list entry.

- Step 6** Click **Submit**.

Managing Nodes in a Cluster

You can add, delete, decommission, and recommission nodes in a cluster.

- **Managed Node**—Any node that was already a member (managed) in the cluster and deleted, which can be added again in the cluster.
- **Live Node**—Any node that has the operating system installed and is reachable from the Hadoop cluster.
- **Bare Metal Node**—Any node that is available and is not associated with the Hadoop cluster.

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Select an account and click **View Details**.
- Step 4** Click **Hosts** to perform the following actions:

Name	Description
Refresh	Refreshes the page.
Favorite	Adds the page to Favorites.
Add Managed Node	Adds managed nodes to the Hadoop cluster.
Add Live Node	Adds live nodes to the Hadoop cluster.
Add Bare Metal Nodes	Adds bare metal nodes to the Hadoop cluster.
Add New Disks	Adds disks to the Hadoop cluster.
Remove Disks	Remove disks from the Hadoop cluster. Note This function is supported only in HDFS Data Node and Yarn Node Manager for Hortonworks and Cloudera clusters only. However, there is no restriction for MapR clusters and you can delete any disks from any nodes.
Disk Locator	Locates the disks in Cisco UCS Manager and turns on the LED on the selected disk of the server.
Report Metadata	

- Step 5** Select a host that allows you to perform the following actions:

Name	Description
View Details	Displays the summary of the CPU usage, the I/O status of the hosts disks, and so on. Note If you see a License Status tab, it indicates a licensing issue.
Delete Node	Deletes node from the cluster.
Assign Rack	Assigns the node to the rack server.

Name	Description
Recommission Node/ Decommission Node	Decommissioning or Recommissioning a node depends on its status. Note When the node is in decommissioned status, it means that all the roles for that node have been withdrawn.
Delete Node to Bare Metal	The node is removed from the cluster and disassociated from the service profile. The node becomes a bare metal server.
Host Mappings	Lists DNS entries of all the hosts in the Hadoop cluster.
Run Inventory	Collects the hardware inventory for the selected server. For example, disk details.

Delete Node and Delete Node to Bare Metal Actions in Cloudera and Hortonworks

When you perform the Delete Node or Delete Node to Bare Metal actions, the UCS CPA Delete Node (a new workflow) is created for Cloudera and Hortonworks. You can also execute this workflow for MapR to perform the delete node operation. If you execute the UCS CPA Delete Node workflow for Cloudera and Hortonworks, this workflow also provides the functionality of Delete Node to Bare Metal action. This functionality is based on the Delete Node to Bare Metal flag setting as true or false. In addition, the Rollback UCS CPA Node Bare Metal workflow is created.

Deleting an Unreachable Node from Hadoop Distribution

This section explains about deleting the unreachable nodes.

Deleting an Unreachable Cluster Node from MapR Distribution

In a MapR distribution with four cluster node, when a cluster node is unreachable and the node status is displayed as **Critical** in the Cisco UCS Director Express for Big Data user interface, you can delete a cluster node by performing the following:

- Step 1** Click **Delete Node**. The status of the node becomes unknown and the node is deleted from the MapR user interface.
- Step 2** Click **Delete Node to Bare Metal**. The rollback of the node occurs.
- Step 3** Click **Delete Node** to delete the node from the Cisco UCS Director Express for Big Data user interface.

Note You can also delete a node by clicking **Delete Node to Bare Metal**. The node is not deleted but rollback of nodes occurs (refer CSCvg90939 bug). You need to manually delete the node from both the MapR user interface and Cisco UCS Director Express for Big Data user interface.

Deleting an Unreachable Cluster Node from Cloudera Distribution

In a Cloudera distribution with three fresh cluster node and one data node added through bare metal workflow, when a node is unreachable and the node status is displayed as **Bad**, you can delete the node by performing the following:

-
- Step 1** Click **Delete Node**. The status of the node becomes unknown and the commissioned state is displayed as deleted.
 - Step 2** Click **Delete Node to Bare Metal** to delete a Data or Edge node. The node is deleted from the Cloudera user interface and the status is not updated in the Cisco UCS Director Express for Big Data user interface.
 - Step 3** Click **Delete Node** to remove the node from the Cisco UCS Director Express for Big Data user interface (refer CSCvg90939 bug).

Note You can also delete a cluster node clicking **Delete Node to Bare Metal**. The node is deleted from both the Cloudera user interface and Cisco UCS Director Express for Big Data user interface.

Note In a four node Cloudera cluster, when one of the data node becomes unreachable you cannot delete the node as some cluster services require a minimum of three nodes.

Deleting an Unreachable Cluster Node from Hortonworks Distribution

In a Hortonworks distribution with three fresh cluster node and one data node added through bare metal workflow, when a node is unreachable and the node status is displayed as **Unknown**, you can delete the node by performing the following:

-
- Step 1** Click **Delete Node**. The status of the node becomes unknown and the commissioned state is displayed as deleted.
 - Step 2** Click **Delete Node to Bare Metal** to delete a Data node, Edge node, or a cluster node. The node is deleted from both the Ambari user interface and Cisco UCS Director Express for Big Data user interface.

Note You can also delete a Data node, Edge node, or a cluster node by clicking **Delete Node to Bare Metal**. The node is deleted from both the Ambari user interface and Cisco UCS Director Express for Big Data user interface.

Note In a four node Hortonworks cluster, when one of the data node becomes unreachable you cannot delete the node as some cluster services require a minimum of three nodes.

Adding Managed Nodes to the Hadoop Cluster

Add managed nodes to the Hadoop cluster.



Note This **Add Managed Nodes** functionality is not supported for Hortonworks 2.3 and later versions, and MapR distribution, but you can use the Add Live Nodes functionality.

This feature allows you to add nodes that are available only from the following URLs, but not the members of the cluster.

- Cloudera—<http://serverip:7180/api/v6/hosts>, where the serverIP is the IPv4 address of the administration node.
- Hortonworks—<http://serverIP:8080/api/v1/hosts>, where the serverIP is the IPv4 address of the administration node



Note The **Add Managed Nodes** functionality is not supported in Cloudera when you select the node type as **Edge Node**.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Double-click the Hadoop account.
- Step 4** Click **Hosts**.
- Step 5** Click **Add Managed Node**.
- Step 6** From the **Host Name** drop-down list, choose the host name.
- Step 7** Click **Submit**.
-

Adding Live Nodes to the Hadoop Cluster

Add live nodes to the Hadoop cluster.

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Double-click the Hadoop account.
- Step 4** Click **Hosts**.
- Step 5** Click **Add Live Node**.
- Step 6** Enter the IPv4 address in the **Host Management IPv4 Address** field.
- Step 7** Enter the name of the rack server in the **Rack Name** field.

- Step 8** Enter the password in the **(New Node) Password** field for that rack server.
- Step 9** Choose the Cluster Manager Version for the Hadoop distribution from the **Cluster Management Version** drop-down list.
- Step 10** Choose the operating system to be installed on the servers in this cluster from the **OS Version** drop-down list.
- Step 11** Choose the node type from the **Node Type** drop-down list.
- Step 12** Choose a MapR cluster template from the **Hadoop Template Name** drop-down list. This field is displayed only when you select the MapR cluster.
- Step 13** Click **Submit**.

Adding Bare Metal Nodes to the Hadoop Cluster

Add bare metal nodes to the Hadoop cluster.



Note To add bare metal nodes to the Hadoop clusters using RHEL 7.4 or CentOS7.4 (created prior to Release 6.6.0.1), create a service profile template in Cisco UCS Manager with UEFI boot option.

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Hadoop Accounts**.
- Step 3** Double-click the Hadoop account.
- Step 4** Click **Hosts**.
- Step 5** Click **Add Bare Metal Nodes**.
- Step 6** Create a service profile template in Cisco UCS Manager with UEFI boot option, if you want to add bare metal nodes to the Hadoop clusters using RHEL 7.4 or CentOS7.4 (created prior to Release 6.6.0.1).
- Step 7** On the **Add Bare Metal Nodes** screen, complete the following fields:

Name	Description
Big Data Account Name field	The name of the Big Data account.
UCSM Policy Name Prefix field	The UCSM Policy Name prefix.
Hadoop Cluster Name field	A unique name for the Hadoop cluster.
Hadoop Node Count field	The number of nodes in the Hadoop cluster.
Host Node Prefix field	The Host Node prefix for the cluster.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Hadoop Distribution drop-down list	Choose the Hadoop distribution to be used for this cluster.
Hadoop Distribution Version drop-down list	Choose the Hadoop distribution version.

Name	Description
Oracle JDK Version drop-down list	Choose the Oracle JDK version.
External Database drop-down list	Choose an external database. You can also configure a new database from here.
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account for this cluster.
Organization drop-down list	Choose the organization in which the servers for this cluster are located.
SSD Boot Drives Available for OS check box	Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain Solid-State Drive (SSD). If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.
Hadoop Template Name drop-down list	Choose a template for a MapR cluster. This field is displayed only when you select the MapR cluster.
UCS SP Template table	Choose an existing UCS Service Profile Template for Hadoop cluster creation.
PXE VLAN ID field	Enter the PXE VLAN ID.
UCSTemplate Name table	Check the UCS Service Profile Template check box that you want to use and click Submit to confirm the selection.

Step 8

If you want to edit a Hadoop Server Role, select the row for that role, and click **Edit**.

Step 9

On the **Edit Hadoop Server Roles Entry** screen, complete the following fields and click **Submit**.

Name	Description
Node Type field	Displays the Hadoop node role. Note Kafka node is supported only for Cloudera and Hortonworks clusters.
Node Count field	The number of nodes in the Hadoop cluster for the selected node type.
SSD Boot Drives Available for OS check box	Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD. If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level. Note This check box is not displayed when the UCSM version is greater than or equal to 3.

Name	Description
Server Pool table	Enter the server pool that you want to use for the cluster for the selected node type. The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.

Step 10 In the **vNIC Template** table, verify the vNIC templates available for the cluster.

Step 11 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 12 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	The vNIC name in the selected template. This field is for your information only.
IP Pool drop-down list	Choose the Big Data IP pool that you want to use for IP addresses assigned to this vNIC.
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster.
First MAC Address field	Enter the MAC address.
Size field	Enter the size.
VLAN ID field	The VLAN ID for this cluster.

Step 13 Click **Submit**.

Adding Disks to the Hadoop Cluster

Step 1 Choose **Solutions > Big Data > Accounts**.

Step 2 Click **Hadoop Accounts**.

Step 3 Double-click the Hadoop account.

Step 4 Click **Hosts**.

Step 5 From the **More Actions** drop-down list, choose **Add New Disks**.

Step 6 Expand **Select disks** and check each disk that you want to use.

Step 7 Choose the method to write the data in the disks from the **Write Mode** drop-down list.

Step 8 Choose the method to read data from the disks from the **Read Mode** drop-down list.

Step 9 Check **Use Cache** to use the RAID controller cache to read and write operations.

Step 10 Check **Use Cache if Bad BBU** to ensure that if the Battery Backup Unit (BBU) is not available for any reason, **Write back** will be disabled and **Write Through** will be enabled.

Step 11 Choose a strip size for each disk within a stripe from the **Stripe Size (MB)** drop-down list.

Step 12 Click **Submit**.

Service Roles

If you use Add Node Bare Metal, Add Managed Node, and Add Live Node actions, the following nodes-specific roles are added for each Hadoop distribution.

Service Roles	Cloudera	MapR	Hortonworks
FileServer	No	Yes	No
DataNode	Yes	No	Yes
NodeManager	Yes	Yes	Yes
Ganglia Monitor	No	No	Yes
NFS Gateway	No	Yes	No



CHAPTER 11

Managing Splunk Clusters

This chapter contains the following sections:

- [Creating an Instant Splunk Cluster, on page 117](#)
- [Creating a Splunk Cluster Using Workflow, on page 121](#)
- [Customizing Splunk Cluster Creation, on page 122](#)
- [Adding Bare Metal Nodes to the Splunk Cluster, on page 126](#)
- [Deleting an Unreachable Cluster Node from Splunk Distribution, on page 129](#)
- [Deploying Splunk Cluster with Archival Node and NFS Support, on page 129](#)
- [Managing a Splunk Cluster, on page 130](#)

Creating an Instant Splunk Cluster

Use this procedure to create an instant Splunk cluster with the predefined values for the UCS Service Profile template. The system creates the QUICK_UCS_SPLUNK template, a new UCS SP Template of container type splunk while creating the instant splunk cluster. You can create a multi-site Splunk cluster or migrate an existing Splunk cluster to a multi-site Splunk cluster. Use the **UCS CPA Migrate Splunk Cluster to Multi-Site** workflow to migrate an existing Splunk cluster to a multi-site Splunk cluster. Until migrations are performed, you cannot completely manage an account in Cisco UCS Director Express for Big Data. **Splunk Cluster Multisite Configuration Generator** task should be modified for the account and site information before executing the workflow.

Step 1 Choose **Solutions > Big Data > Containers**.

Step 2 Click **Cluster Deploy Template**.

Step 3 Click **Instant Splunk Cluster Creation**.

Step 4 On the **Instant Splunk Cluster Creation** screen, complete the following fields:

Name	Description
Big Data Account Name field	The name of the Big Data account.
UCSM Policy Name Prefix field	The UCSM Policy Name prefix.
Monitoring Console Protocol drop-down list	Choose HTTP or HTTPS protocol.

Name	Description
Monitoring Console Port Number field	Enter the port number. Enter an integer between 1024 and 65535. Usage of reserved ports by Linux OS should be avoided so that the web server path is reachable.
SSH (root) Password field	The SSH root password. Special characters such as \$, %, and & are not supported. Note The SSH username pertains to the root user.
Confirm SSH Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Splunk Manager Password field	The management console password. Special characters such as \$, %, and & are not supported.
Confirm Splunk Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Splunk Distribution Version drop-down list	Choose the Splunk Enterprise version to be used for this cluster.
Multi-UCSM check box	Check the Multi-UCSM check box if you use multiple UCSM accounts. Note If you use the multiple UCSM accounts option, you can configure the Splunk Server Roles as described in Step 7. You can add UCSM Specific Inputs in the Add Entry to UCSM Specific Inputs table. The following workflows are created during an Instant Splunk Cluster creation and Customized Splunk Cluster creation: <ul style="list-style-type: none">• UCS CPA Multi-UCSM Splunk Cluster WF• Single UCSM Server Configuration WF (This WF is triggered per UCSM Account. For example, UCSM 120, UCSM121)• UCS CPA Node Bare Metal (This WF is triggered per Node)
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account for this cluster.
Organization drop-down list	Choose the organization in which the servers for this cluster are located.

Name	Description
UCS SP Template table	Choose an existing UCS Service Profile Template for cluster creation.
PXE VLAN ID field	Enter the PXE VLAN ID. Enter an integer between 1 and 3967 or between 4048 and 4093.

Step 5

In the **Splunk Server Roles** table, if you want to edit a Splunk Server Role, select the row for that role, and click **Edit**.

Step 6

On the **Edit Splunk Server Roles Entry** screen, complete the following fields and click **Submit**. The fields displayed in the **Edit Splunk Server Roles Entry** screen is based on the server role selection.

Note Admin roles such as deploying roles on a bare metal agent and choosing license master, cluster master, and bare metal of the deployment server are only supported during fresh cluster creation. Also, existing IP addresses for the admin roles are only supported through fresh cluster creation.

Name	Description
Node Type field	Displays the Splunk node role.
Node Count field	The number of nodes in the splunk cluster for the selected node type.
Host Name Prefix drop-down list	Choose the host name prefix for this splunk cluster.
SSD Boot Drives Available for OS check box	<p>Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD.</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p> <p>Note This check box is not displayed when the UCSM version is greater than or equal to 3.</p>
Search Head to be part of cluster	By default, this option is checked and disabled. The search head role is added to all Search Head cluster.
Validate Page check box	Check Validate Page to recalculate admin hostnames per given hostname prefix and node count.
Deploy roles on Bare Metal check box	Check Deploy roles on Bare Metal to deploy roles on a bare metal agent. By default, this option is checked. Uncheck this option to deploy admin roles on Live Nodes.
Use Existing License Master check box	Check Use Existing License Master to use the existing license master.
License Master BM drop-down list	Choose the license master bare metal.
Monitoring Console BM drop-down list	Choose the monitoring console bare metal.
Cluster Master BM drop-down list	Choose the cluster master bare metal.

Name	Description
Deployer BMs table	Choose the bare metal of the deployer server.
Deployment Server BMs table	Choose the bare metal of the deployment server.
Current License Master Live IPs	Enter the IP addresses of the current license master. This field is displayed when Use Existing License Master is checked.
New License Master Live IP	Enter the IP address of the new license master. This field is displayed when Deploy roles on Bare Metal is unchecked.
Monitoring Console Live IP	Enter the IP address of the monitoring console. This field is displayed when Deploy roles on Bare Metal is unchecked.
Cluster Master Live IP	Enter the IP address of the new license cluster master. This field is displayed when Deploy roles on Bare Metal is unchecked.
Deployer Live IPs	Enter the IP addresses of the deployer server. This field is displayed when Deploy roles on Bare Metal is unchecked.
Deployment Server Live IPs	Enter the IP addresses of the deployment server. This field is displayed when Deploy roles on Bare Metal is unchecked.
Server Pool table	Enter the server pool that you want to use for the cluster for the selected node type. The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.

Note All Live IPs provided for admin roles of a Splunk cluster except for Existing Licensing server and running OS should be same as the Splunk Indexer or Search Head cluster.

Note Hostnames separated by comma or IP addresses can be provided and the hostname resolution should happen from the Cisco UCS Director appliance.

Step 7 In the **vNIC Template** table, review and, if desired, edit the vNIC templates available for the cluster.

Step 8 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 9 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	The vNIC name in the selected template. This field is for your information only.
IP Pool field	Choose the Big Data IP pool that you want to use for IP addresses assigned to this vNIC.

Name	Description
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
VLAN ID field	The VLAN ID for this cluster. (This field is disabled if an existing UCS SP Template is selected.)

Step 10 In the **Site Preferences** table, click **Add (+)** to add one or more sites.

Step 11 On the **Add Entry to Site Preferences** screen, complete the following fields and click **Submit**.

Name	Description
Site Name drop-down list	Choose the site in which the servers for this cluster are located.
Indexers field	Click Select to choose the indexers for the site and click Select .
Search Heads field	Click Select to choose the search heads for the site and click Select .
Replication Factor drop-down list	Choose replication factor for the site.
Search Factor drop-down list	Choose search factor for the site. The search factor must be less than or equal to the replication factor.

Step 12 Click **Submit**.

Step 13 Specify the origin and total site replication factors.

Step 14 Specify the origin and total site search factors.

Step 15 Choose a mater site from **Master Site Name**.

Step 16 Click **Submit**.

Creating a Splunk Cluster Using Workflow

In Cisco UCS Director Express for Big Data, administrator can map the advanced catalog option to Splunk cluster creation workflow, with limited user inputs, so that the service end user can trigger cluster creation. See [Cisco UCS Director End User Portal Guide](#).

Before you begin

- Create a service profile template
- Create a server pool in the Cisco UCS Manager account that you plan to use for this cluster. See [Cisco UCS Director Management Guide for Cisco UCS Manager](#).
- Create a MAC address pool
- Create a user with user role as service end user.

-
- Step 1** Log into Cisco UCS Director Express for Big Data using admin credentials.
- Step 2** Choose **Orchestration** and click **Workflows**.
- Step 3** Click **Add Workflow**.
- Step 4** On the **Add Workflow Details** page, enter the workflow name and choose a folder. Click **Next**.
- Step 5** On the **Add User Inputs** page, enter the required details and click **Next**.
- Step 6** On the **Add User Outputs** page, enter the required details and click **Submit**.
- Step 7** Double-click the workflow in the **Workflow Designer**.
- Step 8** Add the Initiate Splunk Cluster task.
- Step 9** Select the attributes that you want to map to the workflow input fields. Check the **Map to User Input** check box to provide user inputs, if required.
- Step 10** Enter required details in the **Splunk Service Role** table, **vNIC Template** table, and **Site Preferences** table, and click **Submit**.
- Step 11** Choose **Policies > Catalogs** and click **Add Catalog**.
- Step 12** On the **Add Catalog** page, choose the catalog type as Advanced and select a workflow. Click **Submit** to map the workflow to the catalog.
- Step 13** Log into Cisco UCS Director Express for Big Data using service end user credentials.
- Step 14** Choose **Catalogs**. The **Catalogs** page displays the list of catalogs available for the service end user.
- Step 15** Select a catalog and click **Create Request**. The **Create Server Request** page displays the mapped user inputs.
- Step 16** Specify the required details.
- Step 17** Click **Next** and enter the cluster details in the **Customize Workflow** page.
- Step 18** Click **Next** and view the cluster details in the **Summary** page.
- Step 19** Click **Submit** to trigger a workflow for creating a Splunk cluster.
-

Customizing Splunk Cluster Creation

You can create a multi-site Splunk cluster or migrate an existing Splunk cluster to a multi-site Splunk cluster. Use the **UCS CPA Migrate Splunk Cluster to Multi-Site** workflow to migrate an existing Splunk cluster to a multi-site Splunk cluster. Until migrations are performed, you cannot completely manage an account in Cisco UCS Director Express for Big Data. **Splunk Cluster Multisite Configuration Generator** task should be modified for the account and site information before executing the workflow.

Before you begin

- Create a UCS Service Profile Template.
- Create a Cluster Deploy Template.

-
- Step 1** Choose **Solutions > Big Data > Containers**.
- Step 2** Click **Cluster Deploy Templates**.
- Step 3** Click **Add** to create a cluster deploy template for the Splunk cluster. See [Creating a Cluster Deployment Template](#).

Step 4 Click **Customized Splunk Cluster Creation**.

Step 5 On the **Customized Splunk Cluster Creation** screen, complete the following fields.

Name	Description
Big Data Account Name field	The name of the Big Data account.
UCSM Policy Name Prefix field	The UCSM Policy Name prefix.
Monitoring Console Protocol drop-down list	Choose HTTP or HTTPS protocol.
Monitoring Console Port Number field	Enter the port number. Enter an integer between 1024 and 65535.
SSH (root) Password field	The SSH root password. Special characters such as \$, %, and & are not supported. Note The SSH username pertains to the root user.
Confirm SSH Password field	Enter the SSH root password. Special characters such as \$, %, and & are not supported.
Splunk Manager Password field	The management console password. Special characters such as \$, %, and & are not supported.
Confirm Splunk Manager Password field	Enter the management console password. Special characters such as \$, %, and & are not supported.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Splunk Distribution Version drop-down list	Choose the Splunk distribution version to be used for this cluster.
Multi-UCSM check box	Check the Multi-UCSM check box if you use multiple UCSM accounts. Note If you use the multiple UCSM accounts option, you can configure the Splunk Server Roles as described in the Step 8. You can add UCSM Specific Inputs in the Add Entry to UCSM Specific Inputs table. The following workflows are created during an Instant Splunk Cluster creation and Customized Splunk Cluster creation: <ul style="list-style-type: none"> • UCS CPA Multi-UCSM Splunk Cluster WF • Single UCSM Server Configuration WF (This WF is triggered per UCSM Account. For example, UCSM 120, UCSM121) • UCS CPA Node Bare Metal (This WF is triggered per Node)

Name	Description
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account for this cluster.
Organization drop-down list	Choose the organization in which the servers for this cluster are located.
UCS SP Template table	Choose an existing UCS Service Profile Template for cluster creation.
PXE VLAN ID field	Enter the PXE VLAN ID.

Step 6

In the **Splunk Server Roles** table, if you want to edit a Splunk Server Role, select the row for that role, and click **Edit**.

Step 7

On the **Edit Splunk Server Roles Entry** screen, complete the following fields and click **Submit**. The fields displayed in the **Edit Splunk Server Roles Entry** screen is based on the server role

Note Admin roles such as deploying roles on a bare metal agent and choosing license master, cluster master, and bare metal of the deployment server are only supported during fresh cluster creation. Also, existing IP addresses for the admin roles are only supported through fresh cluster creation.

Name	Description
Node Type field	Displays the Splunk node role.
Node Count field	The number of nodes in the splunk cluster for the selected node type.
Host Name Prefix drop-down list	Choose the host name prefix for this splunk cluster.
SSD Boot Drives Available for OS check box	<p>Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD.</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p> <p>Note This check box is not displayed when the UCSM version is greater than or equal to 3.</p>
Search Head to be part of cluster	By default, this option is checked and disabled. The search head role is added to all Search Head cluster.
Validate Page check box	Check Validate Page to recalculate admin hostnames per given hostname prefix and node count.
Deploy roles on Bare Metal check box	Check Deploy roles on Bare Metal to deploy roles on a bare metal agent. By default, this option is checked. Uncheck this option to deploy admin roles on Live Nodes.
Use Existing License Master check box	Check Use Existing License Master to use the existing license master.
License Master BM drop-down list	Choose the license master bare metal.

Name	Description
Monitoring Console BM drop-down list	Choose the monitoring console bare metal.
Cluster Master BM drop-down list	Choose the cluster master bare metal.
Deployer BMs table	Choose the bare metal of the deployer server.
Deployment Server BMs table	Choose the bare metal of the deployment server.
Current License Master Live IPs	Enter the IP addresses of the current license master. This field is displayed when Use Existing License Master is checked.
New License Master Live IP	Enter the IP address of the new license master. This field is displayed when Deploy roles on Bare Metal is unchecked.
Monitoring Console Live IP	Enter the IP address of the monitoring console. This field is displayed when Deploy roles on Bare Metal is unchecked.
Cluster Master Live IP	Enter the IP address of the new license cluster master. This field is displayed when Deploy roles on Bare Metal is unchecked.
Deployer Live IPs	Enter the IP addresses of the deployer server. This field is displayed when Deploy roles on Bare Metal is unchecked.
Deployment Server Live IPs	Enter the IP addresses of the deployment server. This field is displayed when Deploy roles on Bare Metal is unchecked.
Server Pool table	Enter the server pool that you want to use for the cluster for the selected node type. The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.

Step 8 In the **vNIC Template** table, review and, if desired, edit the vNIC templates available for the cluster.

Step 9 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 10 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Name	Description
vNIC Name drop-down list	The vNIC name in the selected template. This field is for your information only.
IP Pool field	Choose the big data IP pool that you want to use for IP addresses assigned to this vNIC.

Name	Description
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
VLAN ID field	The VLAN ID for this cluster. (This field is disabled if an existing UCS SP Template is selected.)

Note When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool, and VLAN ID to the first vNIC in the **vNIC Template** table.

Step 11 In the **Site Preferences** table, click **Add (+)** to add one or more sites.

Step 12 On the **Add Entry to Site Preferences** screen, complete the following fields and click **Submit**.

Name	Description
Site Name drop-down list	Choose the site in which the servers for this cluster are located.
Indexers field	Click Select to choose the indexers for the site and click Select .
Search Heads field	Click Select to choose the search heads for the site and click Select .
Replication Factor drop-down list	Choose replication factor for the site.
Search Factor drop-down list	Choose search factor for the site. The search factor must be less than or equal to the replication factor.

Step 13 Click **Submit**.

Step 14 Specify the origin and total site replication factors.

Step 15 Specify the origin and total site search factors.

Step 16 Choose a mater site from **Master Site Name**.

Step 17 Click **Submit**.

Adding Bare Metal Nodes to the Splunk Cluster

To add a Bare Metal node to a single-site Splunk cluster, cluster should be migrated to multi-site Splunk cluster using the **UCS CPA Migrate Splunk Cluster to Multi-Site** workflow.



Note To add bare metal nodes to the Splunk clusters using RHEL 7.4 or CentOS7.4 (created prior to Release 6.6.0.1), create a service profile template in Cisco UCS Manager with UEFI boot option.

Step 1 Choose **Solutions > Big Data > Accounts**.

Step 2 Click **Splunk Accounts**.

Step 3 Double-click the Splunk account.

You can see only the **Hosts** tab.

Step 4 Click **Add Bare Metal Nodes**.

Step 5 Create a service profile template in Cisco UCS Manager with UEFI boot option, if you want to add bare metal nodes to the Splunk clusters using RHEL 7.4 or CentOS7.4 (created prior to Release 6.6.0.1).

Step 6 On the **Add Bare Metal Nodes** screen, complete the following fields:

Name	Description
Big Data Account Name field	The name of the Big Data account.
UCSM Policy Name Prefix field	The UCSM Policy Name prefix.
Monitoring Console Port Number field	Enter the port number. Enter an integer between 1024 and 65535. Usage of reserved ports by Linux OS should be avoided so that the web server path is reachable.
Monitoring Console Protocol drop-down list	Choose HTTP or HTTPS protocol.
OS Version drop-down list	Choose the operating system to be installed on the servers in this cluster.
Splunk Version drop-down list	Choose the Splunk version.
UCS Manager Account drop-down list	Choose the Cisco UCS Manager account for this cluster.
Organization drop-down list	Choose the organization in which the servers for this cluster are located.
UCS SP Template	Choose an existing UCS Service Profile Template for the cluster creation.
PXE VLAN ID field	Enter the PXE VLAN ID.
UCSTemplate Name table	Choose the UCS Service Profile Template for Splunk.

Step 7 In the **Splunk Server Roles** table, if you want to edit a Splunk Server Role, select the row for that role, and click **Edit**.

Step 8 On the **Edit Splunk Server Roles Entry** screen, complete the following fields and click **Submit**.

Name	Description
Node Type field	Displays the Splunk node role.
Node Count field	The number of nodes in the splunk cluster for the selected node type.
Host Name Prefix drop-down list	Choose the host name prefix for this splunk cluster.

Name	Description
SSD Boot Drives Available for OS check box	<p>Check this check box if you do not want to validate the server disk availability for RAID level OS disks. Ensure that the servers contain SSD.</p> <p>If the check box is not selected, the disk availability for both the OS disk and data disk are validated based on their RAID level.</p> <p>Note This check box is not displayed when the UCSM version is greater than or equal to 3.</p>
Search Head to be part of cluster	By default, this option is checked and disabled. The search head role is added to all Search Head cluster.
Server Pool table	<p>Enter the server pool that you want to use for the cluster for the selected node type.</p> <p>The Cisco UCS Manager account and the organization that you choose determine which server pools are displayed in this area.</p>

Step 9 In the **vNIC Template** table, review and, if desired, edit the vNIC templates available for the cluster.

Step 10 If you want to edit a vNIC template, select the row for that template and click **Edit**.

Step 11 On the **Edit vNIC Template Entry** screen, complete the following fields and click **Submit**.

Table 7:

Name	Description
vNIC Name drop-down list	This field is for your information only.
IP Pool drop-down list	Choose the Big Data IP pool that you want to use for IP addresses assigned to this vNIC.
MAC Address Pool drop-down list	Choose the MAC address pool that you want to use for this cluster. (This drop-down list is disabled if an existing UCS SP Template is selected.)
First MAC Address field	Choose the MAC address pool that you want to use for this cluster.
Size field	Enter the size.
VLAN ID field	The VLAN ID for this cluster.

Step 12 Click **Submit**.

Note By default, the hardware default is used as UUID pool for the servers in the cluster.

Step 13 In the **Site Preferences** table, click **Add (+)** to add one or more sites.

Note Click **Edit** to add a node in the existing site.

Step 14 On the **Add Entry to Site Preferences** screen, complete the following fields and click **Submit**.

Name	Description
Site Name drop-down list	Choose the site in which the servers for this cluster are located.
Indexers field	Click Select to choose the indexers for the site and click Select .
Search Heads field	Click Select to choose the search heads for the site and click Select .
Replication Factor drop-down list	Choose replication factor for the site.
Search Factor drop-down list	Choose search factor for the site. The search factor must be less than or equal to the replication factor.

Step 15 Click **Submit**.

Step 16 Specify the origin and total site replication factors.

Step 17 Specify the origin and total site search factors

Step 18 Click **Submit**.

Deleting an Unreachable Cluster Node from Splunk Distribution

In a Splunk distribution, when a node is unreachable and the node status is displayed as **Unknown**, you can delete a node by clicking **Delete Node to Bare Metal**. The node gets deleted from the Splunk user interface and the status is not updated in the Cisco UCS Director Express for Big Data user interface (refer CSCvg90939 bug). You should click **Delete Node** to delete the node from the Cisco UCS Director Express for Big Data user interface.

Deploying Splunk Cluster with Archival Node and NFS Support

The following are the scenarios to deploy a Splunk cluster along with Archival node:

- Configure Archival Node along with a Splunk Cluster—Archival node is configured along with the cluster automatically.
- Configure Archival Node on a Bare Metal—You can use the add Bare Metal option along with archival node settings like hostname prefix, number of archival nodes, and server pool. When the node comes up, the UCS CPA Splunk Add Live Archival Node workflow is used to configure NFS related setting on the node and configure mount point on indexers.
- Configuring Archival Node on a Live Node—You can use this to configure NFS related setting on the node and add it to the cluster.

For more information on how archival node disks are allocated to indexers, see the latest *Cisco UCS Integrated Infrastructure for Big Data with Splunk Enterprise*.

Managing a Splunk Cluster

You can manage the Splunk cluster from the **Hosts** tab.

Step 1 Choose **Solutions > Big Data > Accounts**.

Step 2 Click **Splunk Accounts**.

Step 3 Click **Summary** to view the statistics data report for the selected Splunk Account and the high-level report on the cluster and node account.

Step 4 Click **Hosts** to perform the following actions:

Name	Description
Refresh	Refreshes the page.
Favorite	Adds the page to Favorites.
Add Bare Metal Nodes	Add bare metal nodes to the Splunk cluster. You can add Indexer, Search Head, or Administrative node through Add Bare Metal workflow. You need to provide the Replication Factor based on the Indexer count.

Note You can also start, stop, or restart the Splunk cluster.

Step 5 Select a host that allows you to perform the following actions:

Name	Description
View Details	Displays the summary of the CPU usage, the I/O status of the hosts disks, and so on. Note If you see a License Status tab, it indicates a licensing issue.
Start	Starts the services on the node.
Stop	Stops the services on the node.
View Details	Restarts the services on the node.
Restart	Deletes node from the cluster.
Delete Node to Bare Metal	The node is removed from the cluster and disassociated from the service profile. The node becomes a Bare Metal server.

Step 6 Select an account and click **View Details**.

You can start, stop, or restart the Splunk cluster.

Step 7 Click the **Performance** tab.

Step 8 Click **Run Test**.

The Performance tab displays a default Big Data Metrics Report. This report shows the statistics collected for each host before the Splunk cluster creation and the reports post Splunk cluster creation only when you check the **Memory Test**, **Network Test**, and **Disk Test** check boxes in the **Pre Cluster Performance Tests** section of the **Management** tab. If you enable the precluster disk test, it impacts Splunk cluster creation.

Step 9 Click **Submit**, and then click **OK**.

For the following actions, choose the performance report:

Name	Description
View	Displays the metrics in the Big Data Metrics Report.
Compare	Compares and displays the metrics in the Big Data Metrics Report.
View Graph Report	Displays graphically the following reports from the Summary tab: <ul style="list-style-type: none"> • Average TRIAD Rate (MB/Sec) • Average Network Bandwidth (MB/Sec)
Delete	Deletes the Big Data Metrics Report.
More Reports	Displays the metrics on an hourly, daily, weekly, or monthly basis.

Step 10 Click **Monitoring**.

Every time an inventory collection cycle is triggered, an entry listing the aggregate CPU, network bandwidth, and disk utilization metrics appears on the Monitoring Page.

Step 11 Select the entry you want to analyze and click **View Details**.

Step 12 Click **Back** to return to the **Monitoring** page.



CHAPTER 12

Big Data Cluster Configuration Settings

This chapter contains the following sections:

- [Creating an External Database Configuration, on page 133](#)
- [Creating a Hadoop Cluster Configuration Parameters Template, on page 135](#)
- [Updating Hadoop Cluster Configuration Parameters Template - Post Hadoop Cluster Creation, on page 136](#)
- [Quality of Service System Classes, on page 136](#)
- [Pre Cluster Performance Testing Settings, on page 139](#)
- [Approving Hadoop Cluster and Splunk Deployment Workflows, on page 139](#)
- [Adding NTP Server Details, on page 141](#)
- [Uploading Required OS and Big Data Software to Cisco UCS Director Bare Metal Agent , on page 141](#)
- [Cloudera, MapR, and Hortonworks RPMs on Cisco UCS Director Express for Big Data Bare Metal Agent, on page 145](#)
- [Cloudera and MapR RPMs for Upgrading Hadoop Cluster Distributions, on page 151](#)
- [Installation of User-Defined Software Post Hadoop Cluster Creation, on page 153](#)
- [Configuration Check Rules, on page 153](#)
- [Checking Hadoop Cluster Configuration, on page 154](#)
- [Fixing Configuration Violations, on page 154](#)

Creating an External Database Configuration

You can deploy each Hadoop cluster with its own external database for all Hadoop distributions (Cloudera, MapR, and Hortonworks) using instant Hadoop cluster and customized Hadoop cluster creation actions.

You can configure a new database or use an existing database in Cisco UCS Director Express for Big Data. The Oozie, Hive, and Hue services use configured database information that you have created using the **Create External Database Configurations** dialog.



Note MySQL is the only supported external database in Cisco UCS Director Express for Big Data.

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **External Database**.

Step 3 Click **Add**.

You can modify or delete any database you have previously created from the external database table.

Step 4 On the **Create External Database Configurations** screen, complete the following fields:

Name	Description
Database Name field	Enter a unique name for the database type you want to create.
Database Type field	Choose the database type from the list.
Server Name field	Enter an IPv4 address for the database server.
Port field	Enter a port number based on the database type.
User Name field	Enter a username to access the database server.
Password field	Enter the password to access the database server.
Confirm Password field	Confirm the password to access the database server.

Step 5 Click **Submit**.

What to do next

Deploy Hadoop clusters through instant Hadoop cluster and customized Hadoop cluster creation actions.

Default Databases Used in Hadoop Distribution Services

Default Databases for Cloudera (Service Names):

- Cloudera Manager—mysql
- Oozie—mysql
- Hive—mysql
- Hue—mysql

Default Databases for MapR (Service Names):

- Oozie—Derby
- Hive—mysql
- Hue—SQLite

Default Databases for Hortonworks (Service Names):

- Ambari—PostGres

- Oozie—Derby
- Hive—mysql

Creating a Hadoop Cluster Configuration Parameters Template

You can create the Hadoop Cluster Configuration Parameters Template only from the **Hadoop Config Parameters** tab on the menu bar here: **Solutions > Big Data > Settings** before triggering a Hadoop cluster. You can select the Hadoop cluster configuration parameters template to edit, clone, or delete.

- Step 1** Choose **Solutions > Big Data > Settings**.
- Step 2** Click **Hadoop Config Parameters**.
- Step 3** Click **Add**.
- Step 4** On the **Hadoop Config Parameters** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, complete the following fields:

Name	Description
Template Name field	A unique name for the Hadoop cluster configuration parameter template.
Template Description field	The description for the Hadoop cluster configuration parameter template.
Hadoop Distribution drop-down list	Choose the Hadoop distribution.
Hadoop Distribution Version drop-down list	Choose the Hadoop distribution version.

- Step 5** Click **Next**.
- Step 6** On the **Hadoop Config Parameters - HDFS Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, specify the Hadoop cluster HDFS service parameter name, value, and the minimum supported Hadoop distribution.
- Step 7** On the **Hadoop Config Parameters - YARN Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the parameters.
- Step 8** On the **Hadoop Config Parameters - HBase Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the parameters.
- Step 9** On the **Hadoop Config Parameters - MapReduce Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the parameters.
- Step 10** On the **Hadoop Config Parameters - Zookeeper Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the parameters.
- Step 11** On the **Hadoop Config Parameters - SmartSense Service** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the parameters.
- Step 12** On the **Hadoop Config Parameters - Miscellaneous Parameters** page of the **Create Hadoop Cluster Configuration Parameters Template** wizard, configure the (ServiceLevel and RoleLevel) parameters.
- Step 13** Click **Submit**.

Updating Hadoop Cluster Configuration Parameters Template - Post Hadoop Cluster Creation

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click the **Hadoop Accounts** tab and choose an existing Hadoop Account.
- Step 3** Click **Configure Cluster**.
- Step 4** On the **Hadoop Config Parameters** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, choose the Hadoop distribution.
- Step 5** Click **Next**.
- Step 6** On the **Hadoop Config Parameters - HDFS Service** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, specify the Hadoop cluster HDFS service parameter name, value, and the minimum supported Hadoop distribution version, if any.
- Step 7** On the **Hadoop Config Parameters - YARN Service** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, update the parameters as required.
- Step 8** On the **Hadoop Config Parameters - HBase Service** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, update the parameters as required.
- Step 9** On the **Hadoop Config Parameters - MapReduce Service** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, update the parameters as required.
- Step 10** On the **Hadoop Config Parameters - Miscellaneous Parameters** page of the **Update Hadoop Cluster Configuration Parameters Template** wizard, update the (ServiceLevel and RoleLevel) parameters as required.
- Step 11** Click **Submit**.
-

Quality of Service System Classes

For more information on Quality of Service and System Classes, see [QoS System Classes](#).

Quality of Service

Cisco Unified Computing System provides the following methods to implement quality of service (QoS):

- System classes that specify the global configuration for certain types of traffic across the entire system.
- QoS policies that assign system classes for individual vNICs.
- Flow control policies that determine how uplink Ethernet ports handle pause frames.

System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS domain. This industry-standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system use and management traffic. You can configure quality of service (QoS) for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS domain.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic, which provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

The following table describes the system classes that you can configure:

System Class	Description
Best Effort	<p>A system class that sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified.</p> <p>For example, this class has a drop policy that allows it to drop data packets if necessary. You cannot disable this system class.</p>
<ul style="list-style-type: none"> • Platinum • Gold • Silver • Bronze 	<p>A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.</p>
Fibre Channel	<p>A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified.</p> <p>For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class.</p> <p>Note FCoE traffic has a reserved QoS system class that cannot be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is re-marked to 0</p>

Editing QoS System Classes

For more information on Quality of Service and System Classes, see [QoS System Classes](#).

-
- Step 1** Choose **Solutions > Big Data > Settings**.
- Step 2** Click **QoS System Class**.
- Step 3** Choose the QoS System Class (by Priority) that you want to edit and click **Edit**.
- Best Effort
 - Platinum
 - Gold

- Silver
- Bronze

Step 4 On the **Modify QoS System Class** screen, complete the following fields:

Name	Description
Enabled check box	<p>If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy.</p> <p>If unchecked, the class is not configured on the fabric interconnect. Any QoS policies associated with this class default to Best Effort or, if a system class is configured with a CoS of 0, to the CoS 0 system class.</p> <p>This check box is checked for Best Effort and Fibre Channel.</p>
CoS drop-down list	<p>The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled.</p> <p>This field is set to 7 for internal traffic and to any for Best effort. Both of these values are reserved and cannot be assigned to any other priority.</p>
Packet Drop check box	<p>This field is unchecked for the Fibre Channel class, which never allows dropped packets, and is checked for Best Effort, which always allows dropped packets.</p>
Weight drop-down list	<p>A choice may be one of the following:</p> <ul style="list-style-type: none"> • An integer between 1 and 10. If you select an integer, Cisco UCS determines the percentage of network bandwidth assigned to the priority level as described in the Weight (%) field. • Best-effort. • None.
Multicast Optimized check box	<p>If checked, the class is optimized to send packets to multiple destinations simultaneously. This option is not applicable to the Fibre Channel.</p>

Name	Description
MTU drop-down list	<p>The maximum transmission unit for the channel. This can be one of the following:</p> <ul style="list-style-type: none"> • An integer between 1500 and 9216. This value corresponds to the maximum packet size. • fc—A predefined packet size of 2240. • Normal—A predefined packet size of 1500. • Specify Manually—A packet size between 1500 to 9216. <p>This field is always set to fc for Fibre Channel.</p>

Step 5 Click **Submit**.

Pre Cluster Performance Testing Settings

You can analyze memory, network, and disk metrics. A default Big Data Metrics Report provides the statistics collected for each host before creating any Hadoop cluster.

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **Management**.

Step 3 On the **Pre Cluster Performance Tests** page, check the check boxes for the following:

- Memory Test
- Network Test
- Disk Test

Note By default, the check boxes to run the memory, network, and the disk tests are unchecked. If you enable the pre cluster disk test, it impacts Hadoop cluster creation.

Step 4 Click **Submit**.

Approving Hadoop Cluster and Splunk Deployment Workflows

Before you begin

Choose **Administration > Users and Groups** and click **Users**, and add users with the following user roles:

- Network Admin (system default user role)

- Computing Admin (system default user role)
- Big Data User

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **Management**.

Step 3 Check the **Require OS User Approval** check box.

- From the **User ID** table, check the **Login Name** of the user against the Network Admin user role.
- Enter the **Number of Approval Request Reminders**.

Note Set the number of approval request reminders to zero if the reminder email has to be sent at a specified interval until the Network Admin approves or rejects the request.

- Enter the **Reminder Interval(s)** in hours.

Note Check the **Approval required from all the users** check box, if you want all users to approve or reject the request.

Step 4 Check the **Require Compute User Approval** check box.

- From the **User ID** table, select the **Login Name** of the user against the Computing Admin user role.
- Enter the **Number of Approval Request Reminders**.

Note Set the number of approval request reminders to zero if the reminder email has to be sent at a specified interval until the Computing Admin approves or rejects the request.

- Enter the **Reminder Interval(s)** in hours.

Note Check the **Approval required from all the users** check box, if you want the users to approve or reject the request.

Step 5 Check the **Require Accounts User Approval** check box.

- From the **User ID** table, select the **Login Name** of the user against the Hadoop User role.
- Enter the **Number of Approval Request Reminders**.

Note Set the number of approval request reminders to zero if the reminder email has to be sent at a specified interval until the Hadoop User approves or rejects the request.

- Enter the **Reminder Interval(s)** in hours.

Note Check the **Approval required from all the users** check box, if you want the users to approve or reject the request.

Step 6 Click **Submit**.

What to do next

Verify whether users of Network Admin, Computing Admin, and Big Data Accounts User roles have approved the request before deploying any Big Data software.

Adding NTP Server Details

- Step 1** Choose **Solutions > Big Data > Settings**.
- Step 2** Click **Management**.
- Step 3** Click **Add (+)**.
- Step 4** On the **Add Entry to Servers** screen, complete the following fields:

Name	Description
Server Name field	The IP address of NTP server.
Is Primary Server check box	Click the check box if you want the server to be a primary server.

- Step 5** Click **Submit**.

Uploading Required OS and Big Data Software to Cisco UCS Director Bare Metal Agent

You can upload (add) required RHEL or CentOS ISO files, Big Data software and common software, and Oracle JDKs to Cisco UCS Director Bare Metal Agent. You can upload the required files from your local system or any remote system, and the files are first uploaded to Cisco UCS Director. Click the **Submit** button in the **Create Software Catalogs** screen to move the required files to the target Cisco UCS Director Bare Metal Agent.

To upload the software packages using **Web Server**, create a directory on the web server path and place all the required software packages in the directory. For example, IPaddress/web/folder (containing the software).

Supported file formats for the **Upload Type** as **Desktop File**:

- Linux OS— [OS version].iso. For example, rhel-server-7.5-x86_64-dvd.iso, CentOS-7.5-x86_64-DVD-1708.iso
- Big Data software—[Big Data-Distro]-[Major version].[Minor version].[Patch version].zip (.gz or .tgz or .tar) For example, MapR-5.2.2.zip, cloudera-5.14.0.zip, and Splunk-7.3.3.zip.
- Common software—bd-sw-rep.zip (.gz or .tgz or .tar)
- JDK software—jdk-8u181-linux-x64 (.rpm or gz)



Tip If the required software column is empty for Big Data, then Cisco UCS Director Bare Metal Agent already contains all the files required.

You must add software catalogs to upload the required software packages. Perform the following to add software catalogs:

Step 1 Choose **Solutions > Big Data > Settings**.

Step 2 Click **Software Catalogs**.

Step 3 Click **Add**.

Step 4 To upload the files from your local system, you can either drag and drop the required files or click **Select a File**.

Note Create a folder to include all the required files for the Big Data software, and compress the folders before uploading in the format specified.

Step 5 On the **Create Software Catalogs** page, complete the following fields:

Note Refresh the **Software Catalogs** page after 5 to 10 minutes to see new and modified catalogs.

Name	Description
Linux OS Upload	
OS Type drop-down list	Choose the OS image type that you want to install on the server. The drop-down list includes all OS types supported by the Cisco UCS Director Bare Metal Agent.
Catalog Name field	Operating System Name (for example, RHEL, CentOS)
Upload Type drop-down list	<p>Choose one of the following:</p> <ul style="list-style-type: none"> • Desktop file • The web server path that is reachable by the Cisco UCS Director Bare Metal Agent (For example, IPaddress/web/folder (containing the software)) • Mountpoint in Cisco UCS Director Bare Metal Agent (For example, /root/iso) • Path to ISO in Cisco UCS Director Bare Metal Agent (For example, /temp/rhel75/iso) <p>Note If you select the Desktop file or web server path option, the .iso file is uploaded to BMA and then it is mounted. If you select the Mountpoint or Path to ISO option, the .iso file is directly mounted since it is already available in the Bare Metal Agent.</p>
Location field	Location of the OS file.
Big Data Software Upload	
Distribution drop-down list	Choose the big data distribution. For example, Cloudera, MapR.

Name	Description
Distribution Version drop-down list	Choose the big data software version. For example, Hadoop Distribution (for example, Distribution_name-Major version.Minor version.Patch version) or splunk enterprise software (Splunk-.Major version.Minor version.Patch version)
OS Type drop-down list	Choose the required OS type. For MapR and Splunk, choose the type as Any option. The file path for the OS-specific software for Cloudera and Hontonwork are modified. For example, the file paths for the repository in Cisco UCS Director Bare Metal Agent is <code>/opt/cnsaroot/bd-sw-rep.</code>
Upload Type drop-down list	Choose one of the following: <ul style="list-style-type: none"> • Desktop file • The web server path that is reachable by the Cisco UCS Director Bare Metal Agent to upload remote software to Bare Metal Agent <p>Note If you select the Desktop file or web server path option, the big data software is copied to respective the folders in <code>/opt/cnsaroot/bd-sw-rep/</code> location.</p>
Location field	Location of the big data software.
Common Software Upload	
Upload Type drop-down list	Choose one of the following: <ul style="list-style-type: none"> • Desktop file • The web server path that is reachable by the Cisco UCS Director Bare Metal Agent to upload remote software to Bare metal Agent
Location field	Location of the common software.
JDK Upload	
JDK Version field	JDK version. For example, <code>jdk-8u60-linux-x64.rpm</code>
Upload Type drop-down list	Choose one of the following: <ul style="list-style-type: none"> • Desktop file • The web server path that is reachable by the Cisco UCS Director Bare Metal Agent to upload remote software to Bare metal Agent

Name	Description
Location field	Location of the JDK file.

Step 6 Click **Submit**.

What to do next

You can track software uploads here: **Administration** > **Integration**. Click **Change Record** to track the software upload in progress and verify its status.

Supported Oracle JDK Software Versions

This section lists the supported Oracle JDK software versions:

Supported Upgrade Scenarios for Cloudera

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.5.0, JDK 1.8
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.6.x, JDK 1.8
Cloudera Enterprise 5.4.x, JDK 1.8	Cloudera Enterprise 5.8.x, JDK 1.8
Cloudera Enterprise 5.6.x, JDK 1.8	Cloudera Enterprise 5.8.x, JDK 1.8
Cloudera Enterprise 5.8.0, JDK 1.8	Cloudera Enterprise 5.10.0, JDK 1.8
Cloudera Enterprise 5.8.0, JDK 1.8	Cloudera Enterprise 5.11.1, JDK 1.8
Cloudera Enterprise 5.8.2, JDK 1.8	Cloudera Enterprise 5.13.1, JDK 1.8
Cloudera Enterprise 5.11.1, JDK 1.8	Cloudera Enterprise 5.13.1, JDK 1.8



Note For more information on the supported JDK versions, see Cloudera site.

Supported Upgrade Scenarios for MapR

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
MapR 5.2.1, JDK 1.8	MapR 6.0.0, JDK 1.8
MapR 5.0.0, JDK 1.8	MapR 5.1.0, JDK 1.8
MapR 4.0.2, JDK 1.8	MapR 5.2.0, JDK 1.8



Note For more information on the supported JDK versions, see MapR site.

Supported Upgrade Scenarios for Hortonworks

Hadoop Distribution Version to Upgrade	Supported Upgrade Version
Hortonworks 2.2, JDK 1.7	Hortonworks 2.3, JDK 1.8
Hortonworks 2.2, JDK 1.7	Hortonworks 2.4, JDK 1.8



Note For more information on the supported JDK versions, see Hortonworks site.

Cloudera, MapR, and Hortonworks RPMs on Cisco UCS Director Express for Big Data Bare Metal Agent

Common Packages for Cloudera, MapR, and Hortonworks



Note For any Hadoop software that is not available, update the `/opt/cnsaroot/bigdata_templates/common_templates/HadoopDistributionRPM.txt` file with an appropriate file from the online repository of the vendor.



Note We recommend that you verify the supported versions from the Hadoop Vendor Support Documentation.

Download the following common packages to `/opt/cnsaroot/bd-sw-rep/`:

- `pssh-2.3.1.tar.gz` from <https://pypi.python.org/packages/source/p/pssh>
- `clustershell-1.7.1-1.el6.noarch.rpm`
- `clustershell-1.7.1-1.el7.noarch.rpm`

Common Packages for Cloudera

Download the following packages to `/opt/cnsaroot/bd-sw-rep/cloudera-X.X.X:`

- `ClouderaEnterpriseLicense.lic`—Get the license keys from Cloudera
- `userrpmlist.txt`—For more packages lists

- `catalog.properties`—Provides the label name for the Cloudera version (x represents the Cloudera version on the Cisco UCS Director Express for Big Data Bare Metal Agent)
- `mysql-connector-java-5.1.39.tar.gz` from MySQL site
- `ext-2.2.zip` from <http://archive.cloudera.com/gplextras/misc/ext-2.2.zip>

Cloudera 5.14.0 Packages and Parcels

Download the following packages to `/opt/cnsaroot/bd-sw-rep/cloudera-5.14.0`:

- `CDH-5.14.0-1.cdh5.14.0.p0.24-el7.parcel` from <https://archive.cloudera.com/cdh5/parcels/5.14.0/>
- `CDH-5.14.0-1.cdh5.14.0.p0.24-el7.parcel.sha1` from <https://archive.cloudera.com/cdh5/parcels/5.14.0/>
- `cm5.14.0-centos7.tar.gz` from <https://archive.cloudera.com/cm5/repo-as-tarball/5.14.0/>
- `manifest.json` from <https://archive.cloudera.com/cdh5/parcels/5.14.0/>
- `mysql-connector-java-5.1.45.tar.gz` from MySQL site
- `ojdbc7.jar` from Oracle site
- `instantclient-basic-linux.x64-12.1.0.2.0.zip` from Oracle site
- `oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm` from Oracle site
- `oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm` from Oracle site

Cloudera 6.0 Packages and Parcels

Download the following packages to `/opt/cnsaroot/bd-sw-rep/cloudera-6.0`:

- `CDH-6.0.0-1.cdh6.0.0.p0.537114-el7.parcel` from <https://archive.cloudera.com/cdh6/6.0.0/parcels/CDH-6.0.0-1.cdh6.0.0.p0.537114-el7.parcel>
- `CDH-6.0.0-1.cdh6.0.0.p0.537114-el7.parcel.sha256` from <https://archive.cloudera.com/cdh6/6.0.0/parcels/CDH-6.0.0-1.cdh6.0.0.p0.537114-el7.parcel.sha256>
- `manifest.json` from <https://archive.cloudera.com/cdh6/6.0.0/parcels/manifest.json>
- `cloudera-manager-daemons-6.0.0-530873.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.0.0/redhat7/yum/RPMS/x86_64/cloudera-manager-daemons-6.0.0-530873.el7.x86_64.rpm
- `cloudera-manager-server-db-2-6.0.0-530873.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.0.0/redhat7/yum/RPMS/x86_64/cloudera-manager-server-db-2-6.0.0-530873.el7.x86_64.rpm
- `cloudera-manager-server-6.0.0-530873.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.0.0/redhat7/yum/RPMS/x86_64/cloudera-manager-server-6.0.0-530873.el7.x86_64.rpm
- `CDH-6.0.0-1.cdh6.0.0.p0.537114-sles12.parcel.sha256` from <https://archive.cloudera.com/cdh6/6.0.0/parcels/CDH-6.0.0-1.cdh6.0.0.p0.537114-sles12.parcel.sha256>

- `cloudera-manager-agent-6.0.0-530873.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.0.0/redhat7/yum/RPMS/x86_64/cloudera-manager-agent-6.0.0-530873.el7.x86_64.rpm
- `mysql-connector-java-5.1.45.tar.gz` from MySQL site
- `ojdbc7.jar` from Oracle site
- `instantclient-basic-linux.x64-12.1.0.2.0.zip` from Oracle site
- `oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm` from Oracle site
- `oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm` from Oracle site

Cloudera 6.1 Packages and Parcels

Download the following packages to `/opt/cnsaroot/bd-sw-rep/cloudera-6.1`:

- `CDH-6.1.0-1.cdh6.1.0.p0.770702-el7` from <https://archive.cloudera.com/cdh6/6.1.0/parcels/CDH-6.1.0-1.cdh6.1.0.p0.770702-el7.parcel>
- `CDH-6.1.0-1.cdh6.1.0.p0.770702-el7.parcel.sha256` from <https://archive.cloudera.com/cdh6/6.1.0/parcels/CDH-6.1.0-1.cdh6.1.0.p0.770702-el7.parcel.sha256>
- `manifest.json` from <https://archive.cloudera.com/cdh6/6.1.0/parcels/manifest.json>
- `cloudera-manager-daemons-6.1.0-769885.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.1.0/redhat7/yum/RPMS/x86_64/cloudera-manager-daemons-6.1.0-769885.el7.x86_64.rpm
- `cloudera-manager-server-6.1.0-769885.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.1.0/redhat7/yum/RPMS/x86_64/cloudera-manager-server-6.1.0-769885.el7.x86_64.rpm
- `cloudera-manager-server-db-2-6.1.0-769885.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.1.0/redhat7/yum/RPMS/x86_64/cloudera-manager-server-db-2-6.1.0-769885.el7.x86_64.rpm
- `cloudera-manager-agent-6.1.0-769885.el7.x86_64.rpm` from https://archive.cloudera.com/cm6/6.1.0/redhat7/yum/RPMS/x86_64/cloudera-manager-agent-6.1.0-769885.el7.x86_64.rpm
- `oracle-j2sdk1.8-1.8.0+update141-1.x86_64.rpm` from https://archive.cloudera.com/cm6/6.1.0/redhat7/yum/RPMS/x86_64/oracle-j2sdk1.8-1.8.0+update141-1.x86_64.rpm
- `ClouderaEnterpriseLicense.lic` from Cloudera site
- `mysql-connector-java-5.1.45.tar.gz` from MySQL site
- `ojdbc7.jar` from Oracle site
- `instantclient-basic-linux.x64-12.1.0.2.0.zip` from Oracle site
- `oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm` from Oracle site
- `oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm` from Oracle site

Common Packages for MapR

Download the following common packages to `/opt/cnsaroot/bd-sw-rep/MapR-X.X.X` directories:

- `libgenders-devel-1.14-2.el6.rf.x86_64.rpm` from <http://pkgs.repoforge.org/libgenders/>
- `libgenders-1.14-2.el6.rf.x86_64.rpm` from <http://pkgs.repoforge.org/libgenders/>
- `ext-2.2.zip` from Apache.Hadoop site.
- `sshpass-1.05-1.el6.x86_64.rpm` from http://ftp.pbone.net/mirror/download.fedora.redhat.com/pub/fedora/epel/6/x86_64
- `soci-mysql-3.2.1-1.el6.x86_64.rpm` from http://ftp.is.co.za/mirror/fedora.redhat.com/epel/6/x86_64
- `soci-3.2.1-1.el6.x86_64.rpm` from http://ftp.is.co.za/mirror/fedora.redhat.com/epel/6/x86_64
- `pdsh-2.27-1.el6.rf.x86_64.rpm` from <http://pkgs.repoforge.org/pdsh>
- `mapr-whirr-0.7.0.16780-1.noarch.rpm` from <http://archive.mapr.com/releases/ecosystem-all/redhat>
- `mapr-drill-0.7.0.29434-1.noarch.rpm` from <http://archive.mapr.com/releases/ecosystem/redhat>
- catalog.properties—Provides the label name for the MapR version (x represents the MapR version on the Cisco UCS Director Express for Big Data Bare Metal Agent)
- license.txt

MapR 5.2.2 Packages

Download the following packages to `/opt/cnsaroot/bd-sw-rep/MapR-5.2.2`

- `libgenders-1.22-2.el7.x86_64.rpm` from http://rpm.pbone.net/index.php3/stat/4/idpl/29487566/dir/redhat_el_7/com/libgenders-1.22-2.el7.x86_64.rpm.html
- `libgenders-devel-1.22-2.el7.x86_64.rpm` from https://centos.pkgs.org/7/epel-x86_64/libgenders-devel-1.22-2.el7.x86_64.rpm.html
- `mapr-ecosystem-5.x-20170802.rpm.tgz` from <http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-ecosystem-5.x-20170802.rpm.tgz>
- `mapr-setup` from <http://package.mapr.com/releases/v5.2.2/redhat/mapr-setup>
- `mapr-v5.2.2GA.rpm.tgz` from <http://archive.mapr.com/releases/v5.2.2/redhat/mapr-v5.2.2GA.rpm.tgz>
- `mapr-whirr-0.7.0.16780-1.noarch.rpm` from <http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-whirr-0.7.0.16780-1.noarch.rpm>
- `mysql-connector-java-5.1.44.tar.gz` from MySQL site.
- `pdsh-2.31-1.el7.x86_64.rpm` from http://mirrors.isu.net.sa/pub/fedora/fedora-epel/7/x86_64/p/

- **soci-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962039/dir/redhat_el_7/com/soci-3.2.3-1.el7.x86_64.rpm.html
- **soci-mysql-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40172013/dir/redhat_el_7/com/soci-mysql-3.2.3-1.el7.x86_64.rpm.html
- **sshpass-1.06-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962109/dir/redhat_el_7/com/sshpass-1.06-1.el7.x86_64.rpm.html

MapR 6.0.0 Packages

Download the following packages to `/opt/cnsaroot/bd-sw-rep/MapR-6.0.0`

- **mapr-v6.0.0GA.rpm.tgz** from <http://archive.mapr.com/releases/v6.0.0/redhat/>
- **mapr-mep-v4.0.0.201711161643.rpm.tgz** from <http://archive.mapr.com/releases/MEP/MEP-4.0.0/redhat/>
- **libgenders-1.22-2.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/29487566/dir/redhat_el_7/com/libgenders-1.22-2.el7.x86_64.rpm.html
- **libgenders-devel-1.22-2.el7.x86_64.rpm** from https://centos.pkgs.org/7/epel-x86_64/libgenders-devel-1.22-2.el7.x86_64.rpm.html
- **mapr-whirr-0.7.0.16780-1.noarch.rpm** from <http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-whirr-0.7.0.16780-1.noarch.rpm>
- **mysql-connector-java-5.1.44.tar.gz** from MySQL site.
- **pdsh-2.31-1.el7.x86_64.rpm** from http://mirrors.isu.net.sa/pub/fedora/fedora-epel/7/x86_64/p/
- **soci-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962039/dir/redhat_el_7/com/soci-3.2.3-1.el7.x86_64.rpm.html
- **soci-mysql-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40172013/dir/redhat_el_7/com/soci-mysql-3.2.3-1.el7.x86_64.rpm.html
- **sshpass-1.06-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962109/dir/redhat_el_7/com/sshpass-1.06-1.el7.x86_64.rpm.html
- **ext-2.2.zip** from Apache.Hadoop site.

MapR 6.1.0 Packages

Download the following packages to `/opt/cnsaroot/bd-sw-rep/MapR-6.1.0`

- **mapr-v6.1.0GA.rpm.tgz** from <http://archive.mapr.com/releases/v6.1.0/redhat/mapr-v6.1.0GA.rpm.tgz>
- **mapr-mep-v6.0.0.201810030946.rpm.tgz** from <http://archive.mapr.com/releases/MEP/MEP-6.0.0/redhat/mapr-mep-v6.0.0.201810030946.rpm.tgz>
- **libgenders-1.22-2.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/29487566/dir/redhat_el_7/com/libgenders-1.22-2.el7.x86_64.rpm.html

- **libgenders-devel-1.22-2.el7.x86_64.rpm** from https://centos.pkgs.org/7/epel-x86_64/libgenders-devel-1.22-2.el7.x86_64.rpm.html
- **mapr-whirr-0.7.0.16780-1.noarch.rpm** from <http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-whirr-0.7.0.16780-1.noarch.rpm>
- **mysql-connector-java-5.1.44.tar.gz** from MySQL site.
- **pdsh-2.31-1.el7.x86_64.rpm** from http://mirrors.isu.net.sa/pub/fedora/fedora-epel/7/x86_64/p/
- **soci-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962039/dir/redhat_el_7/com/soci-3.2.3-1.el7.x86_64.rpm.html
- **soci-mysql-3.2.3-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40172013/dir/redhat_el_7/com/soci-mysql-3.2.3-1.el7.x86_64.rpm.html
- **sshpas-1.06-1.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/40962109/dir/redhat_el_7/com/sshpas-1.06-1.el7.x86_64.rpm.html
- **ext-2.2.zip** from Apache.Hadoop site.

Common Package for Hortonworks

Download the following common package to `/opt/cnsaroot/bd-sw-rep/Hortonworks-X.X`:

- **openssl-1.0.1e-30.el6.x86_64.rpm**
- **ext-2.2.zip** from Apache.Hadoop site.
- **catalog.properties**—Provides the label name for the Hortonworks version (x represents the Hortonworks version on the Cisco UCS Director Express for Big Data Bare Metal Agent)

Hortonworks 2.6.4 Packages

Download the following packages to `/opt/cnsaroot/bd-sw-rep/Hortonworks-2.6.4`:

- **ambari-2.6.1.0-centos7.tar.gz** from <http://public-repo-1.hortonworks.com/ambari/centos7/2.x/updates/2.6.1.0/ambari-2.6.1.0-centos7.tar.gz>
- **HDP-2.6.4.0-centos7-rpm.tar.gz** from <http://public-repo-1.hortonworks.com/HDP/centos7/2.x/updates/2.6.4.0/HDP-2.6.4.0-centos7-rpm.tar.gz>
- **HDP-UTILS-1.1.0.22-centos7.tar.gz** from <http://public-repo-1.hortonworks.com/HDP-UTILS-1.1.0.22/repos/centos7/HDP-UTILS-1.1.0.22-centos7.tar.gz>
- **libtirpc-0.2.4-0.10.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/38004637/dir/scientific_linux_7/com/libtirpc-0.2.4-0.10.el7.x86_64.rpm.html
- **libtirpc-devel-0.2.4-0.10.el7.x86_64.rpm** from http://rpm.pbone.net/index.php3/stat/4/idpl/37971478/dir/centos_7/com/libtirpc-devel-0.2.4-0.10.el7.x86_64.rpm.html
- **je-5.0.73.jar** from Oracle site.
- **ojdbc7.jar** from Oracle site.
- **oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm** from Oracle site.

- `oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm` from Oracle site.

Hortonworks 3.0.0 Packages

Download the following packages to `/opt/cnsaroot/bd-sw-rep/Hortonworks-3.0.0`:

- `ambari-2.7.0.0-centos7.tar.gz` from <http://public-repo-1.hortonworks.com/ambari/centos7/2.x/updates/2.7.0.0/ambari-2.7.0.0-centos7.tar.gz>
- `HDP-3.0.0.0-centos7-rpm.tar.gz` from <http://public-repo-1.hortonworks.com/HDP/centos7/3.x/updates/3.0.0.0/HDP-3.0.0.0-centos7-rpm.tar.gz>
- `HDP-UTILS-1.1.0.22-centos7.tar.gz` from <http://public-repo-1.hortonworks.com/HDP-UTILS-1.1.0.22/repos/centos7/HDP-UTILS-1.1.0.22-centos7.tar.gz>
- `HDP-GPL-3.0.0.0-centos7-gpl.tar.gz` from <http://public-repo-1.hortonworks.com/HDP-GPL/centos7/3.x/updates/3.0.0.0/HDP-GPL-3.0.0.0-centos7-gpl.tar.gz>
- `libtirpc-0.2.4-0.10.el7.x86_64.rpm` from http://rpm.pbone.net/index.php3/stat/4/idpl/38004637/dir/scientific_linux_7/com/libtirpc-0.2.4-0.10.el7.x86_64.rpm.html
- `libtirpc-devel-0.2.4-0.10.el7.x86_64.rpm` from http://rpm.pbone.net/index.php3/stat/4/idpl/37971478/dir/centos_7/com/libtirpc-devel-0.2.4-0.10.el7.x86_64.rpm.html
- `je-5.0.73.jar` from Oracle site.
- `ojdbc7.jar` from Oracle site.
- `oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm` from Oracle site.
- `oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm` from Oracle site.



Note Download the Splunk software from Splunk Suite.

Cloudera and MapR RPMs for Upgrading Hadoop Cluster Distributions

Cloudera 5.3.0 Packages and Parcels

- `cm5.3.0-centos6.tar.gz` from <http://archive.cloudera.com/cm5/repo-as-tarball/5.3.0>
- `CDH-5.3.0-1.cdh5.3.0.p0.30-el6.parcel` from <http://archive.cloudera.com/cdh5/parcels/5.3.0>
- `CDH-5.3.0-1.cdh5.3.0.p0.30-el6.parcel.sha1` from <http://archive.cloudera.com/cdh5/parcels/5.3.0>
- `manifest.json` from <http://archive.cloudera.com/cdh5/parcels/5.3.0>

Cloudera 5.4.1 Packages and Parcels

- `cm5.4.1-centos6.tar.gz` from <http://archive.cloudera.com/cm5/repo-as-tarball/5.4.1>
- `CDH-5.4.1-1.cdh5.4.1.p0.6-el6.parcel` from <http://archive.cloudera.com/cdh5/parcels/5.4.1>
- `CDH-5.4.1-1.cdh5.4.1.p0.6-el6.parcel.sha1` from <http://archive.cloudera.com/cdh5/parcels/5.4.1>
- `manifest.json` from <http://archive.cloudera.com/cdh5/parcels/5.4.1>

MapR 4.1.0 Packages

- `mapr-setup` from <http://package.mapr.com/releases/v4.1.0/redhat>
- `mapr-v4.1.0GA.rpm.tgz` from <http://package.mapr.com/releases/v4.1.0/redhat>
- `mysql-connector-java-5.1.26.tar.gz` from <http://cdn.mysql.com/archives/mysql-connector-java-5.1>

MapR 5.0.0 Packages

- `mapr-setup` from <http://package.mapr.com/releases/v5.0.0/redhat>
- `mapr-v5.0.0GA.rpm.tgz`: from <http://package.mapr.com/releases/v5.0.0/redhat>
- `mysql-connector-java-5.1.26.tar.gz` from <http://cdn.mysql.com/archives/mysql-connector-java-5.1>

MapR 5.2.0 Packages

- `mapr-setup` from <http://package.mapr.com/releases/v5.2.0/redhat/mapr-setup>
- `mapr-v5.2.0GA.rpm.tgz`: from <http://archive.mapr.com/releases/v5.2.0/redhat/mapr-v5.2.0GA.rpm.tgz>



Note `mapr-v5.2.0GA.rpm.tgz` contains the following `mapr-client-5.2.0.39122.GA-1.x86_64.rpm`, `mapr-posix-client-platinum-5.2.0.39122.GA-1.x86_64.rpm`, `mapr-posix-client-basic-5.2.0.39122.GA-1.x86_64.rpm`, `mapr-upgrade-5.2.0.39122.GA-1.x86_64.rpm`, `mapr-nfs-5.2.0.39122.GA-1.x86_64.rpm`, and `mapr-core-5.2.0.39122.GA-1.x86_64.rpm` files.

- `mysql-connector-java-5.1.26.tar.gz` from <https://downloads.mysql.com/archives/get/file/mysql-connector-java-5.1.26.tar.gz>
- `mapr-ecosystem-5.x-20160816.rpm.tgz` from <http://archive.mapr.com/releases/ecosystem-all/redhat/mapr-ecosystem-5.x-20160816.rpm.tgz>

Installation of User-Defined Software Post Hadoop Cluster Creation

Cisco UCS Director Express for Big Data provides an option to add user-defined installation packages (RPMs) post Hadoop cluster creation specific to a version. In Cisco UCS Director Express for Big Data, you cannot install more Hadoop related software other than what is required for the selected type of Hadoop distribution when creating an instant Hadoop cluster or customizing a Hadoop cluster.

To install user-defined Hadoop related software, you can specify a list of RPMs in the HadoopDistributionRPM.txt file. This modifiable list defines the required packages for each version of a Hadoop distribution. You can locate the HadoopDistributionRPM.txt here:

`/opt/cnsaroot/bigdata_templates/common_templates` in the

Cisco UCS Director Express for Big Data Bare Metal Agent

server.

For example, you can specify a list of RPMs in the HadoopDistributionRPM.txt file for MapR-5.0.0:

- `mapr-v5.0.0GA.rpm.tgz`
- `mapr-ecosystem-5.x-20150709.rpm.tgz`
- `mapr-whirr-0.8.1.18380-GA.noarch.rpm`

Configuration Check Rules

You can validate an existing cluster configuration by running a configuration check. The configuration check process involves comparing the current cluster configuration with reporting violations and configuration check rules.

Configuration check rules are predefined Cisco Validated Design (CVD) parameters for Hadoop clusters. Configuration check rules appear under **Solutions > Big Data > Settings**. After the configuration check is complete, violations appear in the **Faults** page under **Solutions > Big Data > Accounts**. You can enable or disable configuration check rules at any time, but you cannot add new rules.

Configuration Check Rule	Description
Parameter	The predefined CVD parameter of the configuration.
Enabled	The state of the configuration check rule, either enabled (true) or disabled (false).
Expected value	The value expected for a parameter as defined in the Cisco Validated Design (CVD).
Description	The description of the parameter of the configuration.
Distribution	The Hadoop distribution.
Minimum Supported Distribution	The minimum supported version of Hadoop distribution.

Configuration Check Rule	Description
Service	The Hadoop service.
Role	The Hadoop service role.
Type	The type of violation, either CVD or Inconsistent.
Fix Workflow	The reference to the workflow that can be triggered for fixing violations.

When the actual cluster configuration values differ from the expected values defined in the configuration check rules, then those configuration values are reported as violations. For example, CVD mandates that the NameNode heap size is 4 GB. But if the NameNode heap size in the cluster configuration is found to be 1 GB, then this is reported as a CVD violation. Also, inconsistent configuration parameters are reported. For example, NameNode heap size on both the primary and secondary nodes must be of the same size. If there is a mismatch in the size, then this parameter is reported as inconsistent.

Checking Hadoop Cluster Configuration

To validate the configuration of a cluster, do the following:

-
- Step 1** Choose **Solutions > Big Data > Accounts**.
 - Step 2** Click **Hadoop Accounts**.
 - Step 3** Choose the account for which you want to run the configuration check and click **Check Configuration**.
 - Step 4** Click **Submit**.
A page appears with the information that the configuration check is in progress.
 - Step 5** Click **OK**.
After the configuration check is complete, the violations appear under the **Faults** page for the selected Hadoop Account.
-

What to do next



Note You can track configuration checks here: **Administration > Integration**. Click **Change Record** to track the configuration checks in progress and verify if completed or failed.

Fixing Configuration Violations

After the configuration check is complete, the configuration violations appear in the **Faults** page for the selected big data account. You can either choose to fix these configuration violations manually on the **Big Data Cluster Configuration** page, or trigger a workflow. To trigger a workflow to fix the violation, create a workflow with the same name as the code specified in the violation.

To fix a configuration violation through a workflow, do the following:

- Step 1** Choose **Solutions > Big Data > Accounts**.
- Step 2** Click **Faults**.
- Step 3** Choose the configuration violation you want to fix and click **Trigger Workflow**.
If a workflow exists with the same name as the code specified in the violation, then the workflow is triggered.
- Step 4** Enter the required inputs for the workflow and click **Submit**.
A service request ID is generated after you submit the inputs. You can check the status of the service request on the **Service Requests** page.
-



CHAPTER 13

Cisco UCS CPA Workflows

This chapter contains the following sections:

- [Workflows for Big Data, on page 157](#)
- [About Service Requests for Big Data, on page 160](#)

Workflows for Big Data

Cisco UCS Director Express for Big Data defines a set of workflows in the **UCS CPA** folder under **Orchestration** page.

- **UCS CPA Multi-UCSM Hadoop Cluster WF**—This workflow is triggered if you use multiple UCSM Hadoop accounts.
- **UCS CPA Multi-UCSM Splunk Cluster WF**—This workflow is triggered if you use multiple UCSM Splunk accounts.
- **UCS CPA Single UCSM Server Configuration WF**—This workflow is triggered for every UCSM account.
- **UCS CPA Node Bare Metal**—This workflow is triggered per node in the cluster.
- **UCS CPA Node Bare Metal with Storage Profile WF**—This workflow is triggered using Cisco UCS S3260 storage server having SSD Server Boot Drive under SAS RAID controller to deploy OS.

Note Disk group policies are automatically created in the Cisco UCS Director Express for Big Data using workflows only for Cisco UCS Manager 3.2 or later version.

Table 8: Disk Group Policy

Servers Details	Disk Group Policy Required?	Disk Policy Allocation Details
Servers having PCH Controller and and Data drive slots with SSD disks	No	Not applicable

Servers Details	Disk Group Policy Required?	Disk Policy Allocation Details
SAS controller with dedicated boot drive slots (20x) and Data drive slots with SSD disks	Yes	For OS boot, if you want to manually allocate the SSD slot numbers to RAID 0 or RAID 1, BD_V1_SSM_RAID0 or BD_V1_SSM_RAID1 should be created. Currently dedicated boot drive slots 201 and 202 are supported only by Cisco UCS S3260 Storage Server.
SAS controller with dedicated boot drive slots (20x) with SSD disks and Data drive slots without SSD disks	Yes	For OS boot, if you want to automatically allocate the SSD slot numbers to RAID 0 or RAID 1, Boot_SSD_RAID0 or Boot_SSD_RAID1 should be created.
SAS controller and Data drive slots with HDD only	Yes	For OS boot, if you want to automatically allocate the HDD slot numbers to RAID 0 or RAID 1, Boot_HDD_RAID0 or Boot_HDD_RAID1 should be created. Note You can create Boot_HDD_RAID0 or Boot_HDD_RAID1 if SSD disks are available in Data drive slots in addition to HDD.
SAS controller and Data drive slots with SDD and HDD disks	Yes	During OS boot, if you want to manually allocate the slot numbers to RAID 1, BD_V1_ANYM_RAID1 should be created.



Note In some cases, **Wait for Complete Association** might fail for Cisco UCS 326x storage servers during UCS CPA Node Bare Metal with Storage Profile after a time out. In such cases, association process might have already failed after **Bind UCS Service Profile to Template** post 90% of FSM with Storage System initialisation error. You need to perform a re-acknowledgement on the Cisco UCS server and resubmit the Bare Metal workflow.

- UCS CPA Delete Node—This workflow is triggered if you delete a node from the Hadoop cluster.
- UCS CPA Cloudera Add Live Node—This workflow is triggered if you add a Live Node for Cloudera.

- UCS CPA MapR Add Live Node—This workflow is triggered if you add a Live Node for MapR.
- UCS CPA Hortonworks Add Live Node—This workflow is triggered if you add a Live Node for Hortonworks.
- UCS CPA Add New Disks—This workflow is triggered if you add new disks.
- UCS CPA Configure NFS Clients and Servers—This workflow is triggered if you configure NFS clients and servers.
- UCS CPA Enable HTTPS Modify Protocol and Port Number for Hadoop—This workflow is triggered if you modify protocol and port numbers for Hadoop.
- UCS CPA Enable HTTPS Modify Protocol and Port Number for Splunk—This workflow is triggered if you modify protocol and port numbers for Splunk.
- UCS CPA Migrate Splunk Cluster to Multi-Site—This workflow is triggered if you want to migrate an existing Splunk cluster to a multi-site Splunk cluster.
- UCS CPA Remove Disks—This workflow is triggered if you remove disks.
- UCS CPA Splunk Upgrade—This workflow is triggered if you upgrade the Splunk cluster.
- UCS CPA Instant Hadoop Cluster WF—This workflow is triggered if you create an instant Hadoop cluster based on the node count and other mandatory inputs such as the IP address range, memory, and number of interfaces. Cisco UCS Director Express for Big Data automatically creates one UCS service profile and a Hadoop cluster profile template at the back end that are required to create an instant Hadoop cluster. This saves you the effort of manually creating a service profile and a cluster profile.
- UCS CPA Customized Hadoop Cluster WF—This workflow is triggered if you choose to use a specific UCS service profile. A Hadoop cluster profile template with the specified number of nodes to be created in the Hadoop cluster.
- UCS CPA Disable High Availability WF—This workflow is triggered when you disable high availability.
- UCS CPA Enable High Availability WF—This workflow is triggered when you enable high availability.
- UCS CPA Shutdown Big Data Cluster WF—This workflow is triggered when you shut down the Hadoop cluster.
- UCS CPA Start Big Data Cluster WF—This workflow is triggered when you power up the Hadoop cluster.
- UCS CPA Splunk Add Live Archival Node—This workflow is triggered when if you add a Live Archival Node for Splunk.
- UCS CPA Upgrade Cluster WF—This workflow is triggered when you upgrade the Hadoop cluster.
- UCS CPA Cloudera Add New Service WF—This workflow is triggered when you add a new service for Cloudera.
- UCS CPA MapR Add New Service WF—This workflow is triggered when you add a new service for MapR.
- UCS CPA Hortonworks Add New Service WF—This workflow is triggered when you add a new service for Hortonworks.
- UCS CPA Multi-Node Bare Metal provisioning WF—This workflow is triggered when you deploy baremetal OS account using Cisco UCS server.

Table 9: Disk Group Policy

Servers Details	Disk Group Policy Required?	Disk Policy Allocation Details
Servers having PCH Controller	No	Disk group policy is not applicable for PCH controllers, for example, Lewisburg SATA Controller. The LUN gets created automatically by the PCH controller based on the controller definition.
Servers having SAS controller	Yes	The disks are configured for RAID 1. You can manually allocate two disks.
Servers having SATA controller	Yes	The disks are configured for RAID 1. You can manually allocate two disks.

- Bare-metal OS Deployment—This workflow is triggered per server to deploy baremetal OS. UCS CPA Multi-Node Bare Metal provisioning WF will automatically trigger the **Bare-metal OS Deployment** workflow when you deploy baremetal OS account per server and monitor it.

About Service Requests for Big Data

Cisco UCS Director Express for Big Data leverages Cisco UCS Director service requests and workflow orchestration for the overall deployment of Hadoop clusters. Each service request is a provisioning workflow that is created during a cluster creation.

For example, one UCS CPA Multi-UCSM Hadoop Cluster W/F, one Single UCSM Server Configuration W/F, and four UCS CPA Node Bare Metal W/Fs are created for a four-node Hadoop cluster. When the workflows are complete, the cluster is created under **Solutions > Big Data > Accounts** for that UCSM account.

A set of service requests is created under **Organizations > Service Requests** during a cluster creation.

- UCS CPA Multi-UCSM Hadoop Cluster WF—This workflow is triggered if you use multiple UCSM Hadoop accounts. It also applies when you create an instant or customized Hadoop cluster.
- UCS CPA Multi-UCSM Splunk Cluster WF—This workflow is triggered if you use multiple UCSM Splunk accounts. It also applies to when you create an instant or customized Splunk cluster.
- UCS CPA Single UCSM Server Configuration WF—This workflow is triggered for every UCSM account.
- UCS CPA Node Bare Metal—This workflow is triggered per node in the cluster.

The following service requests are created when you add a Bare Metal Node or a Live Node to the cluster.

- UCS CPA Cloudera Add Live Node—This workflow is triggered if you add a Live Node for Cloudera.
- UCS CPA MapR Add Live Node—This workflow is triggered if you add a Live Node for MapR.
- UCS CPA Hortonworks Add Live Node—This workflow is triggered if you add a Live Node for Hortonworks.

- UCS CPA BigInsights Add Live Node—This workflow is triggered if you add a Live Node for BigInsights.

The following service requests are created as explained, below:

- UCS CPA Disable High Availability WF—This workflow is triggered when you disable high availability.
- UCS CPA Enable High Availability WF—This workflow is triggered when you enable high availability.
- UCS CPA Shutdown Big Data Cluster WF—This workflow is triggered when you shut down the Hadoop cluster.
- UCS CPA Start Big Data Cluster WF—This workflow is triggered when you power up the Hadoop cluster.
- UCS CPA Upgrade Cluster WF—This workflow is triggered when you upgrade the Hadoop cluster.
- UCS CPA Cloudera Add New Service WF—This workflow is triggered when you add a new service for Cloudera.
- UCS CPA Hortonworks Add New Service WF—This workflow is triggered when you add a new service for Hortonworks.
- UCS CPA MapR Add New Service WF—This workflow is triggered when you add a new service for MapR.
- UCS CPA BigInsights Add New Service WF—This workflow is triggered when you add a new service for BigInsights.

For more information on the service requests and workflows, see the following guides:

- *Cisco UCS Director Self-Service Portal Guide*
- *Cisco UCS Director Orchestration Guide*

Monitoring Service Requests for Big Data

Before you begin

Create and customize a Cluster Deploy Template to monitor a service request.

-
- Step 1** Choose **Organizations > Service Requests**.
 - Step 2** Click **Service Requests**.
 - Step 3** Select the service request that you want to monitor and click **View Details**.

One of the following Request Status is displayed:

- Complete
 - In Progress
 - Cancelled
 - Failed
-

Viewing UCS CPA Workflow Tasks

From the **Service Request Status** screen, you can view the following:

- Workflow Status
- Log
- Objects Created and Modified
- Input/Output



Note You can only modify inputs for failed service requests.

Step 1 Choose **Organizations > Service Requests**.

You can see the list of user-specific service requests added to a specific group. For example, All User Groups.

Step 2 Choose the **Service Request ID** that you want to view.

Step 3 Double-click the **Service Request ID** that opens the **Service Request Status** screen. (You can also choose the Service Request ID by the workflow name associated with it, and click **View Details**. For example, choose the **UCS CPA Node Bare Metal** workflow and click **View Details**).

On the **Service Request Status** screen, you can view the following tasks for the workflow:

UCS CPA Multi-UCSM Hadoop Cluster WF/UCS CPA Multi-UCSM Splunk Cluster WF	UCS CPA Single UCSM Server Configuration WF	UCS CPA Node Bare Metal
<p>The following tasks are associated with the UCS CPA Multi-UCSM Hadoop Cluster WF/UCS CPA Multi-UCSM Splunk Cluster WF:</p> <ul style="list-style-type: none"> a. Initiated by Admin b. Multi-UCSM Hadoop Cluster profile/Multi-UCSM Splunk Cluster profile c. Setup Big Data Cluster Env d. User (Compute) Approval Required e. User (OS) Approval Required f. Multi-UCSM Configuration WF g. Multi Bare Metal WF Monitor h. Synchronized Command Execution i. User (Hadoop) Approval Required j. Custom SSH Command k. Monitor Shell Script Status l. Provision Hadoop Cluster/Provision Splunk Cluster m. SSH Command n. Monitor Shell Script Status o. Edit Hadoop Account/Edit Splunk Account p. Assign Big Data Account to Group q. Custom SSH Command r. Complete 	<p>The following tasks are associated with the Single UCSM Server Configuration WF:</p> <ul style="list-style-type: none"> a. Initiated by Admin b. Create UCS Service Profile Template c. Change Maintenance Policy UCS SP Template d. Muti-Bare Metal OS Install WF e. Create UCS Disk Group Policy f. Create UCS Disk Group Policy g. Create UCS Disk Group Policy h. Create UCS Disk Group Policy i. Multi-Bare Metal WF Monitor j. Change Maintenance Policy for UCS SP Template k. Complete 	

UCS CPA Multi-UCSM Hadoop Cluster WF/UCS CPA Multi-UCSM Splunk Cluster WF	UCS CPA Single UCSM Server Configuration WF	UCS CPA Node Bare Metal
		<p>The following tasks are associated with the UCS CPA Node Bare Metal:</p> <ul style="list-style-type: none"> a. Initiated by Admin b. Modify Workflow Priority (High) c. Assign Bare Metal SR ID d. Create Service Profile from Template e. Unbind UCS Service Profile from Template f. Modify UCS Service Profile Boot Policy g. Add VLAN to Service Profile h. Associate UCS Service Profile i. Assign ServerIdentity j. PXE Boot With BMA Selection k. Setup RAID Commands l. UCS Blade Reset Action m. PXE Boot Wait n. Monitor RAID Configuration o. Custom Archive PXE Boot Request p. UCS Blade Power OFF Action q. PXE Boot With BMA Selection r. Setup RAID Commands s. Custom Wait for Complete Association of SP t. UCS Blade Reset Action u. PXE Boot Wait v. Modify UCS Service Profile Boot Policy w. Delete VLAN from Service Profile vNIC

UCS CPA Multi-UCSM Hadoop Cluster WF/UCS CPA Multi-UCSM Splunk Cluster WF	UCS CPA Single UCSM Server Configuration WF	UCS CPA Node Bare Metal
		<ul style="list-style-type: none"> x. Bind UCS Service Profile to Template y. Wait for complete Association z. UCS Blade Reset Action aa. Assign IP Status ab. Custom SSH Command ac. Monitor Shell Script Status ad. Linux Shell Script Execution ae. Linux Shell Script Execution af. UCS Blade Power OFF Action ag. UCS Blade Power ON Action ah. Synchronized Command Execution ai. Assign UCS Server to Group aj. Assign Service Profile to Group ak. Complete

Step 4 Click **Close**.

Viewing UCS CPA Workflow Tasks for BareMetal OS

From the **Service Request Status** screen, you can view the following:

- Workflow Status
- Log
- Objects Created and Modified
- Input/Output



Note You can only modify inputs for failed service requests.

-
- Step 1** Choose **Organizations** > **Service Requests**. You can see the list of user-specific service requests added to a specific group. For example, All User Groups.
- Step 2** Choose the **Service Request ID** that you want to view.
- Step 3** Double-click the **Service Request ID** that opens the **Service Request Status** screen. (You can also choose the Service Request ID by the workflow name associated with it, and click **View Details**. For example, choose the **UCS CPA Node Bare Metal** workflow and click **View Details**). On the **Service Request Status** screen, you can view the following tasks for the workflow:

UCS CPA Multi-Node Bare Metal provisioning WF	Bare-metal OS Deployment
--	---------------------------------

UCS CPA Multi-Node Bare Metal provisioning WF	Bare-metal OS Deployment
<p>The following tasks are associated with the UCS CPA Multi-Node Bare Metal provisioning WF:</p> <ul style="list-style-type: none"> a. Initiated by Admin b. Get UCSM account authentication c. Get UCS Organization d. Create Multi UCS Policy for Linux Account e. Create Maintenance Policy f. Create BIOS Policy g. Create Local Boot Policy h. Create LAN Boot Policy i. Check Scrub Policy is required j. Create Scrub Policy (note only executed when check scrub policy is required is true) k. Check Selected slot is SATA l. Create Local Disk Config Policy (note only executed when check Selected slot is SATA is true) m. Create Service Profile Template n. Get UCSM Account Name o. Create PXE VLAN p. Modify Org Permission for PXE VLAN q. Get PXE VLAN ID r. Check if server have PCH s. Add UCS Storage Profile (only executed when Check if server have PCH is true) t. Create Storage Profile (only executed when Check if server have PCH is false) u. Get UCS Storage Profile (only executed when Check if server have PCH is false) v. Collect Inventory w. Request UCSM Inventory Collection By DN (for service profile template inventory) x. Wait for PXE VLAN y. Check if server have PCH 	<p>The following tasks are associated with the Bare-metal OS Deployment:</p> <ul style="list-style-type: none"> a. Initiated by Admin b. Create Service Profile from Template c. Unbind UCS Service Profile from Template d. Modify UCS Service Profile Boot Policy e. Get UCS Organization f. Add PXE VLAN to Service Profile (PXE VLAN is already created in the UCS CPA Multi-Node Bare Metal provisioning WF and passed here) g. Associate Storage Profile to Service Profile (Storage Profile is already created in the UCS CPA Multi-Node Bare Metal provisioning WF and passed here) h. Checking Set JBOD contains "true" i. Set JBOD to Unconfigured Good (only executed when checking Set JBOD contains "true") j. Select UCS Server k. Check if Delete LUN is enabled l. Delete LUNs From Server (only execute when check if Delete LUN is enabled) m. Reserve UCS IP address n. Associate UCS Service Profile o. Check if server have SAS p. Get UCS LUN ID (only execute when Check if server have SAS is true) q. Setup PXE Boot (OS Type: RHEL7.6) (only execute when Check if server have SAS is true) r. Setup PXE Boot (OS Type: RHEL7.6) (only execute when Check if server have SAS is false) s. Modify PXE Configuration for SATA Controller (only execute when Check if server have SAS is false)

UCS CPA Multi-Node Bare Metal provisioning WF	Bare-metal OS Deployment
<p>z. Request UCSM Inventory Collection By DN (for storage profile inventory & executed only when Check if server have PCH is false)</p> <p>aa. Wait for Service Profile Template Status</p> <p>ab. Install Multi Linux on UCS Server for Linux Account (it will automatically trigger the Bare-metal OS Deployment workflow per server)</p> <p>ac. Multi Bare Metal Account WF Monitor (it will monitor the Bare-metal OS Deployment workflow SR's)</p> <p>ad. Create Baremetal OS Account (once all the Bare-metal OS Deployment is successful, the baremetal OSs account will get created)</p> <p>ae. Complete</p>	<p>t. Wait for Complete Association</p> <p>u. UCS Blade Power ON Action</p> <p>v. Check if server have SAS</p> <p>w. Monitor PXE Boot</p> <p>x. Delete PXE VLAN from MGMT vNIC</p> <p>y. Bind UCS Service Profile to Template</p> <p>z. UCS Blade Power OFF Action</p> <p>aa. UCS Blade Power ON Action</p> <p>ab. IPconfig</p> <p>ac. vNIC Bonding</p> <p>ad. Complete</p>

Step 4 Click **Close**.

Workflow Customization to Deploy a Hadoop or Splunk Cluster

You can customize the following UCS CPA workflows and use them to deploy a Hadoop or Splunk cluster. You can add installation packages (RPMs) required for your cluster environment in the Cisco UCS Director Express for Big Data Bare Metal Agent.

- Rename the UCS CPA Multi-UCSM Hadoop Cluster WF
- Rename the UCS CPA Multi-UCSM Splunk Cluster WF
- Rename the Single UCSM Server Configuration WF
- Rename the UCS CPA Node Bare Metal

Deploying a Hadoop or Splunk Cluster Through Workflow Customization

Before you begin

For more information on workflow orchestration, see the *Cisco UCS Director Orchestration Guide*.

- Customize UCS CPA Node Bare Metal workflows that you want to use in the cloned Single UCSM Server Configuration WF.
- Customize the Single UCSM Server Configuration WF that you want to use in the UCS CPA Multi-UCSM Hadoop Cluster WF or UCS CPA Multi-UCSM Splunk Cluster WF.

Step 1 Choose **Orchestration**.

- Step 2** Click the **UCS CPA** folder from **Workflows**.
- Step 3** Double-click the workflow that you want to customize in the **Workflow Designer**. For instance, double-click the **UCS CPA Multi-UCSM Hadoop Cluster WF**.
- Step 4** Double-click the **Muti-UCSM Configuration WF** task in the **Workflow Designer**.
- Step 5** Click **Next** on the **Workflow Task Basic Information** page.
- Step 6** On the **User Input Mappings to Task Input Attributes** page, select the attributes that you want to map to the workflow input fields or provide values in the next step. If necessary, check the **Map to User Input** check box to provide user inputs.
- Step 7** Click **Next** on the **User Input Mappings to Task Input Attributes** page.
- Step 8** Enter the task values which are not mapped to workflow inputs. For example, enter the name of the cloned Single UCSM Server Configuration WF in the **Workflow Name** field.
- Step 9** Click **Revalidate** to validate task input values.
- Step 10** Click **Next**.
- Step 11** On the **User Output mappings to Task Output Attributes** page, select the attributes that you want to map to the workflow output fields.
- Step 12** Check the **Map to User Output** check box and choose the value from the **User Output** drop-down list.
- Step 13** Click **Submit**.

Assigning Big Data Accounts to User Groups

- Step 1** Choose **Orchestration** and click **Workflows**.
- Step 2** Click **Add Workflow**.
- Step 3** On the **Add Workflow Details** page, enter the workflow name and choose a folder. Click **Next**.
- Step 4** On the **Workflow Task Basic Information** page, enter the required details and click **Next**.
- Step 5** On the **User Input Mappings to Task Input Attributes** page, select the attributes that you want to map to the workflow input fields or provide values in the next step. If necessary, check the **Map to User Input** check box to provide user inputs..
- Step 6** On the **User Input Mappings to Task Input Attributes** page, choose big data account type and big data account.
- Step 7** Check the **Assign Users** checkbox and click **Submit**. The big data accounts are assigned to specified users if the **Allow resource assignment to users** option is enabled in the **Users Groups** page. When the **Assign Users** checkbox is not checked, the big data accounts are assigned to a specified group.

Unassigning Big Data Accounts

Before you begin

- Step 1** Choose **Orchestration** and click **Workflows**.
- Step 2** Click **Add Workflow**.
- Step 3** On the **Add Workflow Details** page, enter the workflow name and choose a folder. Click **Next**.
- Step 4** On the **Workflow Task Basic Information** page, enter the required details and click **Next**.

- Step 5** On the **User Input Mappings to Task Input Attributes** page, select the attributes that you want to map to the workflow input fields or provide values in the next step. If necessary, check the **Map to User Input** check box to provide user inputs..
- Step 6** On the **User Input Mappings to Task Input Attributes** page, choose big data account type and big data account.
- Step 7** Check the **Unassign Users** checkbox and click **Submit**. The big data accounts are unassigned from the group.

Cloning UCS CPA Workflows

To customize cluster deployment through bare metal workflows, you can clone the following workflows in the UCS CPA folder:

- Clone the UCS CPA Node Bare Metal workflows.
- Rename the Single UCSM Server Configuration WF using the cloned UCS CPA Node Bare Metal workflows.
- Rename the UCS CPA Multi-UCSM Hadoop Cluster WF using the cloned Single UCSM Server Configuration WF.

- Step 1** Choose **Orchestration**.
- Step 2** Click the **UCS CPA** folder from **Workflows** and choose the workflow that you want to clone.
- Step 3** Click **Clone Workflow**.
- Step 4** On the **Workflow Details** page of the **Clone Workflow** wizard, complete the following fields:

Name	Description
Workflow Name field	A unique name for the workflow.
Version field	The current version of the workflow that you are cloning. This is a display-only field.
Description field	The description of the workflow.
Workflow Context drop-down list	<p>The workflow context. Workflow Orchestration supports the following options:</p> <ul style="list-style-type: none"> • Any—Enables you to use the workflow in any context. • Selected VM—Enables you to use the execute workflow. This option can be selected only when you choose a VM. • Check the Save As Compound Task check box to define the workflow as a compound task. • Check the Place in New Folder check box, and enter the folder name in the Folder Name field, to assign the workflow to a new folder other than the UCS CPA folder.

Name	Description
Select Folder drop-down list	Choose a folder. UCS CPA is the default folder for Big Data.
Notify status of execution to initiator User check box	Check the check box to notify the user through email, then enter appropriate email addresses in the Additional User(s) to send Email Notification field.

Step 5 Click Next.

Step 6 On the **Workflow User Inputs** page of the **Clone Workflow** wizard, complete the following fields:

Name	Description
Associate to Activity check box	If the check box is checked then any existing workflow's user input is overridden by any selected activity user input.
Activity drop-down list.	Choose an activity. The user-input table is updated based on the selected activity.
Workflow User Inputs table	<p>On the Workflow User Inputs page:</p> <ol style="list-style-type: none"> a. Click the + icon to add workflow input properties. b. On the Add Entry to screen, complete the following fields: <ol style="list-style-type: none"> 1. Enter the name for the activity workflow input in the Input Label field. 2. Enter the description for the activity workflow input in the Input Description field. 3. Check the Optional check box to set the input as optional during workflow execution. 4. Click Select. On the Select screen, click Input Type. 5. Click Submit.

Step 7 Click Next.

Step 8 On the **Workflow User Outputs** page of the **Clone Workflow** wizard, do the following:

Name	Description
Workflow User Outputs table	<p>On the Workflow User Outputs page:</p> <ol style="list-style-type: none">a. Click the + icon to add workflow output properties.b. On the Add Entry to screen, complete the following fields:<ol style="list-style-type: none">1. Enter the name for the activity workflow output in the Output Label field.2. Enter the description for the activity workflow output in the Output Description field.3. Check the Optional check box to set the output as optional during workflow execution.4. Click Select. On the Select screen, click Output Type.5. Click Submit.

Step 9 Click **Submit**.



CHAPTER 14

Monitoring and Reporting

This chapter contains the following sections:

- [About Monitoring and Reporting](#), on page 175
- [Cisco UCS Director Express for Big Data Dashboard](#), on page 175
- [Viewing a Deployed Cluster Report](#), on page 176
- [Reports](#), on page 176

About Monitoring and Reporting

Cisco UCS Director Express for Big Data can monitor virtual infrastructure and system resources, and provide a wide array of reports.

Cisco UCS Director Express for Big Data monitors a range of cluster events:

- High CPU usage
- Memory usage
- Disk capacity
- Disk IO utilization

Cisco UCS Director Express for Big Data displays statistics from the respective pages for selected Big Data Account and Hosts. You can also generate reports that itemize system details.

Cisco UCS Director Express for Big Data Dashboard

Cisco UCS Director Express for Big Data provides complete system visibility through real-time and historical monitoring. See [Reports](#)



Note The **Dashboard** tab shows up in the menu bar only after a summary report is added to the dashboard.

The customizable dashboard displays processing, memory, storage, and network utilization metrics.

- Per-node statistics: CPU, memory, and disk

- Health of Hadoop cluster components: HDFS, MapReduce jobs
- Graphs based on historical data



Note Drag and Drop summary report icons from the **Customize** drawer to the **Summary** and **Hosts** tabs, where you can expand and close reports.

You can:

1. Add summary reports to the dashboard from the Big Data Account **Summary** tab. You can customize the summary reports to display the statistics for a specific time period, or export these reports from the dashboard.
2. Add summary reports to the dashboard from the Big Data Account **Hosts** tab. You can customize the summary reports to display the statistics for a specific time period, or export these reports from the dashboard.



Note Not all summary reports apply to MapR.

3. Add UCSM Accounts summary reports to the dashboard from **Physical > Compute**.
4. Add Data Center summary reports to the dashboard from **Physical > Compute**.

Viewing a Deployed Cluster Report

You can generate a **Big Data Account Summary Report** with or without credentials, to view the details of the deployed clusters.

-
- Step 1** On the menu bar, choose **Solutions > Big Data > Containers**.
- Step 2** Click the **Deployed Clusters** tab.
- Step 3** Choose the deployed cluster, and click **View Report**.
- Step 4** In the **View Report** dialog box, choose the report type that you want to generate.
- Step 5** Click **Submit**.
-

Reports

UCSM Account Summary Reports

- Overview
- UCS Chassis Inventory

- UCS Server Inventory
- UCS Fabric Interconnect Inventory
- UCS Servers Associated vs Unassociated
- Rack Server Discovery Policy
- Power Policy
- Global Power Allocation Policy

Big Data Account Summary Reports

- Overview

Cluster-specific Metrics Supported per Hadoop Distribution

Metrics	Cloudera Distribution	Hortonworks Distribution	MapR Distribution	Remarks
Average CPU IO Wait (%)	Yes	Yes	Yes	—
Average CPU idle (%)	Yes	Yes	Yes	—
Average CPU Nice (%)	Yes	Yes	Yes	—
Average CPU System (%)	Yes	Yes	Yes	—
Average CPU User	Yes	Yes	Yes	—
CPU Percentage Across Hosts	Yes	—	—	Metrics for Host CPU usage across hosts
Cluster Disk IO	Yes	—	—	Metrics for Total Disk Write and Read Bytes Across Disks
Cluster Network IO	Yes	—	—	Metrics for Total Bytes Transmitted and Received Across Network Interfaces
HDFS IO	Yes	—	—	Metrics for Total Bytes written and Read Across Data Nodes
Total Space Utilization	—	Yes	—	—
CPU	—	Yes	—	—

Metrics	Cloudera Distribution	Hortonworks Distribution	MapR Distribution	Remarks
Load	—	Yes	—	—
Memory	—	Yes	—	—
Network	—	Yes	—	—
Process	—	Yes	—	—

Host-specific Metrics Supported per Hadoop Distribution

Metrics	Cloudera Distribution	Hortonworks Distribution	MapR Distribution
Average CPU IO Wait (%)	Yes	Yes	Yes
Average CPU Idle (%)	Yes	Yes	Yes
Average CPU Nice (%)	Yes	Yes	Yes
Average CPU System (%)	Yes	Yes	Yes
Average CPU User	Yes	Yes	Yes
Load Average(%)	Yes	—	—
Host CPU Usage	Yes	—	—
Host Memory Usage	Yes	—	—
Host Network Throughput	Yes	—	—
Disk Latency	Yes	—	—
Aggregate Disk Throughput	Yes	—	—
Role-CPU Usage	Yes	—	—
HOST CPU	—	Yes	—
DISK Usage	—	Yes	—
LOAD Usage	—	Yes	—
Memory-CPU Usage	—	Yes	—
Network Usage	—	Yes	—
Process Usage	—	Yes	—



CHAPTER 15

Proactive Status Monitoring and Diagnostics

This chapter contains the following topics:

- [Aggregate CPU, Disk, and Network Bandwidth Utilization, on page 179](#)
- [Monitoring Aggregate CPU, Disk, and Network Bandwidth Utilization, on page 180](#)
- [Monitoring Top Jobs Based on CPU Utilization and Time, on page 180](#)
- [Performance Metrics for CPU, Disk, and Network, on page 181](#)
- [Viewing CPU, Disk, and Network Statistics for a Hadoop Cluster, on page 181](#)
- [Analyzing Performance Bottlenecks Through Historical Metrics, on page 182](#)
- [Setting Alerts for Hadoop Cluster Service Failures, on page 183](#)
- [Types of Disk and Network Failure Alerts, on page 184](#)
- [Setting Alerts for Disk and Network Failures, on page 185](#)
- [Setting Disk Utilization Threshold Alerts, on page 186](#)

Aggregate CPU, Disk, and Network Bandwidth Utilization

You can monitor the aggregate CPU, disk, and network bandwidth utilization across all the hosts in a cluster. The metrics are collected in the following ways:

- **Aggregate CPU and Disk metrics:** For every host that is running the job, the PID collects the percentage of CPU and memory used by the job. The sum of all these percentages gives the aggregate CPU and disk metrics.
- **Aggregate network bandwidth metrics:** For aggregate network bandwidth of one node, obtain the network bandwidth on each network interface, and then add them. Similarly network bandwidths are measured for all the nodes in the cluster. The sum of all these bandwidths provides the aggregate network bandwidth metrics for the cluster.
- **Duration of long-running jobs:** A Rest API collects the start time, elapsed time, and end time for each job identified on the cluster. The difference between start time and end time provides the duration of completed jobs. The elapsed time reports the duration of the jobs running currently.

Monitoring Aggregate CPU, Disk, and Network Bandwidth Utilization

Step 1 On the menu bar, choose **Solutions > Big Data > Accounts**.

Step 2 Click the **Big Data Accounts** tab.

Step 3 Choose the Big Data Account and click **View Details**.

Step 4 Click the **Hadoop Clusters** tab.

Step 5 Choose the big data cluster and click **View Reports**.

Step 6 Click the **Monitoring** tab.

Every time an inventory collection cycle is triggered, an entry listing the aggregate CPU, network bandwidth, and disk utilization metrics appears on the Monitoring Page.

Note For Splunk cluster, on clicking the **View Details** button, the **Monitoring** tab is displayed. Step 4 and Step 5 are specific to Hadoop cluster only.

Step 7 Select the entry you want to analyze and click **View Details**.

- a) Click the **Aggregate CPU** tab to view the aggregate CPU utilization of all nodes for a particular time period.
- b) Click the **Aggregate Disks** tab to view the aggregate disk utilization and available memory across the cluster.
- c) Click the **Aggregate Network Bandwidth Utilization** to view the aggregated network bandwidth across the cluster.

Step 8 Click **Back** to return to the **Monitoring** page.

Monitoring Top Jobs Based on CPU Utilization and Time

To monitor top jobs based on CPU utilization or time (both active and completed long-running jobs), do the following:

Step 1 On the menu bar, choose **Solutions > Big Data > Accounts**.

Step 2 Click the **Big Data Accounts** tab.

Step 3 Choose the Big Data Account and click **View Details**.

Step 4 Click the **Hadoop Clusters** tab.

Step 5 Choose the Hadoop cluster and click **View Reports**.

- a) Click the **Top 10 High CPU Jobs** tab to view the top ten jobs, based on CPU utilization.
- b) Click the **Top 10 Long Running Active Jobs** tab to view the current top ten long-running jobs.
- c) Click the **Top 10 Long Duration Jobs** tab to view the completed top ten long-running jobs.

Step 6 Click **Back** to return back to the **Hadoop Clusters** page.

Performance Metrics for CPU, Disk, and Network

You can find performance bottlenecks that occur in the compute, network, or Hadoop setup across the cluster. You can collect CPU, disk, and network metrics and analyze these metrics to fix bottlenecks.

The metrics reports are of the following types:

- **Pre-Cluster:** This metrics report is generated automatically for a server that has been installed with Red Hat Linux. This report is created before the server becomes part of a cluster.
- **Post-Cluster:** This metrics report is generated on demand when you run the performance test for a Hadoop cluster.

When you run the performance test for a Hadoop cluster, the following metrics are shown in detail:

- **Memory metrics:** Memory metrics measure the memory utilization of each host on the Hadoop cluster. The report includes the triad rate, which is the average rate at which read, write, and copy operations take place. The triad rate is a standard measure of memory bandwidth.
- **Network metrics:** Network metrics measure the network bandwidth of the Hadoop cluster. The report displays the rates at which network packets are transferred between the client and the server in the Hadoop cluster.
- **Disk metrics:** Disk metrics identify how fast a disk can perform. The disk metrics are included only in the pre-cluster report. The report lists the following:
 - The time taken to read and write a file.
 - The time taken to rewrite to an existing a file.
 - The time to randomly (nonsequentially) read and write files.
- **DFSIO metrics:** The DFSIO test is a Hadoop benchmark that stress-tests the storage I/O (read and write) capabilities of the cluster. The report measures the bytes processed, execution time, the average I/O rate, and throughput to read and write multiple files. The DFSIO metrics report is included only in the post-cluster report.
- **TeraSort metrics:** The TeraSort test is a Hadoop benchmark that tests the memory of the cluster. The report lists the counters for generating input, sorting the generated input, and validating the sorted output. The TeraSort metrics report is included only in the post-cluster report.

Viewing CPU, Disk, and Network Statistics for a Hadoop Cluster

You can collect and compare CPU, disk, and network metrics with the pre-cluster creation and post-cluster creation reports for a Hadoop cluster.

-
- Step 1** On the menu bar, choose **Solutions > Big Data >> Accounts**.
 - Step 2** Click the **Big Data Accounts** tab.
 - Step 3** Choose the Big Data Account and click **View Details**.
 - Step 4** Click the **Hadoop Clusters** tab.

Step 5 Choose the Hadoop cluster and click **View Reports**.

Step 6 Click the **Performance** tab.

Step 7 Click **Run Test**.

The Performance tab displays a default Big Data Metrics Report. This report shows the statistics collected for each host before the Hadoop cluster creation and the reports collected after Hadoop cluster creation.

Step 8 Click **Submit**, and then click **OK**.

For the following actions, choose the performance report:

Name	Description
View	Displays the metrics in the Big Data Metrics Report.
Compare	Compares and displays the metrics in the Big Data Metrics Report.
View Graph Report	Displays graphically the following reports from the Summary tab: <ul style="list-style-type: none"> • Average TRIAD Rate (MB/Sec) • Average Network Bandwidth (MB/Sec) • Average DFSIO Write (MB/Sec) • Average DFSIO Read (MB/Sec)
Delete	Deletes the Big Data Metrics Report.
More Reports	Displays the metrics as hourly, daily, weekly, or monthly values.

Analyzing Performance Bottlenecks Through Historical Metrics

You can compare a metrics report generated while the cluster was performing well with a report generated during poor performance. It helps you identify a cause or causes of a performance bottleneck in the Hadoop cluster.

To compare and analyze two metrics reports, do the following:

Step 1 On the menu bar, choose **Solutions > Big Data > Accounts**.

Step 2 Click the **Big Data Accounts** tab.

Step 3 Choose the Big Data Account and click **View Details**.

Step 4 Click the **Hadoop Clusters** tab.

Step 5 Choose the Hadoop cluster, and click **View Reports**.

Step 6 Click the **Performance** tab.

Step 7 Click **Run Test**.

The Performance tab displays a default Big Data Metrics Report. This report shows the statistics collected for each host before the Hadoop cluster creation and the reports collected after Hadoop cluster creation.

Step 8 Choose two reports that you want to compare, and click **Compare**.

You can compare a report generated while the cluster was performing well and a report generated during poor performance.

Step 9 Click **Submit**.

Setting Alerts for Hadoop Cluster Service Failures

You can create an alert to monitor the health of the Hadoop cluster whenever Hadoop services go down. Based on the trigger conditions, you can also activate customized workflows that automatically take corrective action.

Step 1 On the menu bar, choose **Policies > Orchestration**.

Step 2 Click the **Triggers** tab.

Step 3 Click **Add**.

On the **Trigger Information** page of the **Add Trigger** wizard, complete the following fields:

Name	Description
Trigger Name field	Name of the trigger.
Is Enabled check box	Check this box to enable the trigger.
Description	Description of the trigger.
Frequency	Choose the trigger rule validation frequency.
Trigger Type	Choose the type of trigger. <ul style="list-style-type: none"> • Stateful • Stateless

Step 4 Click **Next**.

Step 5 On the **Specify Conditions** page of the **Add Trigger** wizard, click **Add a new entry to the table below (+)**.

Step 6 In the **Add Entry to Conditions** dialog box, complete the following fields:

- a) From the **Type of Object to Monitor** drop-down list, choose **BigData Cluster**.
- b) From the **Object** drop-down list, choose the Hadoop cluster to be monitored.
- c) From the **Parameter** drop-down list, choose the parameter to use in validation.
- d) From the **Operation** drop-down list, choose **Equals** or **Not Equals**.
- e) From the **Value** drop-down list, choose **All Services Up** or **Any Service Down**.
- f) Click **Submit**.
- g) From the **Trigger When** drop-down list, make a choice to satisfy all the conditions, or any individual condition.

Step 7 Click **Next**.

Step 8 On the **Specify Workflow** page of the **Add Trigger** wizard, do the following when the Hadoop cluster service is down and when the trigger is reset:

- a) Choose the maximum number of invocations from the **Maximum Number of Invocations** drop-down list.
- b) Select a workflow for execution when the trigger state becomes active, and check the **Pass Monitored Object** check box, if necessary.
- c) Select the workflow input.
- d) Select a workflow for execution when the trigger state becomes clear, and check the **Pass Monitored Object** check box, if necessary.
- e) Select the workflow input.

Step 9 Click **Next**.

Step 10 On the **Specify Workflow Inputs** page of the **Add Trigger** wizard, enter the inputs for the selected workflows, and then click **Submit**.

Types of Disk and Network Failure Alerts

You can create alerts to detect faults related to disks and networks in a cluster.

The alerts that you can create for memory faults are as follows:

- **fltMemoryUnitInoperable:** Triggers when the number of correctable or uncorrectable errors have reached a threshold on a DIMM. The DIMM becomes inoperable.
- **fltMemoryUnitThermalThresholdNonRecoverable:** Triggers when the memory unit temperature on a server is out of the operating range. The issue is not recoverable.
- **fltMemoryArrayVoltageThresholdCritical:** Triggers when the memory array voltage exceeds the specified hardware voltage rating.
- **fltMemoryArrayVoltageThresholdNonRecoverable:** Triggers when the memory array voltage exceeds the specified hardware voltage rating, with potential memory hardware damage.
- **fltMemoryBufferUnitThermalThresholdCritical:** Triggers when the temperature of a memory buffer unit on a blade or rack server exceeds a critical threshold value.
- **fltMemoryBufferUnitThermalThresholdNonRecoverable:** Triggers when the temperature of a memory buffer unit on a blade or rack server is out of the operating range. The issue is not recoverable.
- **fltMemoryUnitDisabled:** Triggers when the server BIOS disables a DIMM. The BIOS could disable a DIMM for several reasons, including incorrect location of the DIMM or incompatible speed.

The alerts that you can create for disk faults are as follows:

- **fltStorageItemCapacityExceeded:** Triggers when the partition disk usage exceeds 70% but is less than 90%.
- **fltStorageItemCapacityWarning:** Triggers when the partition disk usage exceeds 90%.
- **fltStorageLocalDiskInoperable:** Triggers when the local disk has become inoperable.

- **fltStorageLocalDiskSlotEpUnusable:** Triggers when the server disk drive is in a slot that the storage controller does not support.
- **fltStorageLocalDiskMissing:** Triggers when a disk is missing.
- **fltStorageLocalDiskDegraded:** Triggers when the local disk has degraded. The fault description contains the physical drive state, which indicates the reason for the degradation.

The alerts that you can create for network faults are as follows:

- **fltAdaptorUnitMissing:** Triggers when the network adapter is missing, or the server cannot detect or communicate with the adapter.
- **fltAdaptorHostIfLink-down:** Triggers—
 - When the fabric interconnect is in End-Host mode and all uplink ports have failed.
 - When the server port to which the adapter is pinned have failed.
 - When a transient error causes the link to fail.
- **fltAdaptorExtIfLink-down:** Triggers—
 - When the adapter's connectivity to any of the fabric interconnects cannot be validated.
 - When a node reports that a vNIC is down, or reports a link-down event on the adapter link.

Setting Alerts for Disk and Network Failures

You can create alerts for disk or network failures in the Hadoop cluster. Alerts help you in proactive cluster maintenance. Based on the trigger conditions, you can activate customized workflows that automatically take corrective action.

Step 1 On the menu bar, choose **Policies > Orchestration**.

Step 2 Click the **Triggers** tab.

Step 3 Click **Add**.

On the **Trigger Information** page of the **Add Trigger** wizard, complete the following fields:

Name	Description
Trigger Name field	Name of the trigger.
Is Enabled check box	Check this box to enable the trigger.
Description	Description of the trigger.
Frequency	Choose the trigger rule validation frequency.
Trigger Type	Choose the type of trigger. <ul style="list-style-type: none"> • Stateful • Stateless

- Step 4** Click **Next**.
- Step 5** On the **Specify Conditions** page of the **Add Trigger** wizard, click **Add a new entry to the table below (+)**, and complete the following fields in the **Add Entry to Conditions** dialog box:
- From the **Type of Object to Monitor** drop-down list, choose **BigData Nodes**.
 - From the **Object** drop-down list, choose the disk to be monitored.
 - From the **Parameter** drop-down list, choose the parameter to use in validation.
 - From the **Operation** drop-down list, choose the type of operation.
 - From the **Value** drop-down list, choose the value to use in validation.
 - Click **Submit**.
 - From the **Trigger When** drop-down list, make a choice to satisfy all conditions, or any individual condition.
- Step 6** Click **Next**.
- Step 7** On the **Specify Workflow** page of the **Add Trigger** wizard, do the following when there is a network or disk failure and when the trigger is reset:
- From the **Maximum Number of Invocations** drop-down list, choose the maximum number of invocations.
 - Select a workflow for execution when the trigger state becomes active and check the **Pass Monitored Object** check box, if necessary.
 - Select the workflow input.
 - Select a workflow for execution when the trigger state becomes clear, and check the **Pass Monitored Object** check box, if necessary.
 - Select the workflow input.
- Step 8** Click **Next**.
- Step 9** On the **Specify Workflow Inputs** page of the **Add Trigger** wizard, enter the inputs for the selected workflows, and then click **Submit**.

Setting Disk Utilization Threshold Alerts

You can set an alert to be delivered when the disk capacity reaches a threshold. This helps you to proactively plan for capacity expansions.

Step 1 On the menu bar, choose **Policies > Orchestration**.

Step 2 Click the **Triggers** tab.

Step 3 Click **Add**.

On the **Trigger Information** page of the **Add Trigger** wizard, complete the following fields:

Name	Description
Trigger Name field	Name of the trigger.
Is Enabled check box	Check this box to enable the trigger.
Description	Description of the trigger.
Frequency	Choose the trigger rule validation frequency.

Name	Description
Trigger Type	Choose the type of trigger. <ul style="list-style-type: none"> • Stateful • Stateless

Step 4 Click **Next**.

Step 5 On the **Specify Conditions** page of the **Add Trigger** wizard, click +, and complete the following fields in the **Add Entry to Conditions** dialog box:

- a) From the **Type of Object to Monitor** drop-down list, choose **BigData Cluster**.
- b) From the **Object** drop-down list, choose the disk to be monitored.
- c) From the **Parameter** drop-down list, choose the **Disk Utilization (%)**.
- d) From the **Operation** drop-down list, choose the type of operation.
- e) From the **Value** drop-down list, choose the threshold value to use for validation.
- f) Click **Submit**.
- g) From the **Trigger When** drop-down list, make a choice to satisfy all conditions, or any individual condition.

Step 6 Click **Next**.

Step 7 On the **Specify Workflow** page of the **Add Trigger** wizard, do the following when the disk utilization reaches the threshold value and when the trigger is reset:

- a) From the **Maximum Number of Invocations** drop-down list, choose the maximum number for invocations.
- b) Select a workflow for execution when the trigger state becomes active, and check the **Pass Monitored Object** check box, if necessary.
- c) Select the workflow input.
- d) Select a workflow for execution when the trigger state becomes clear, and check the **Pass Monitored Object** check box, if necessary.
- e) Select the workflow input.

Step 8 Click **Next**.

Step 9 On the **Specify Workflow Inputs** page of the **Add Trigger** wizard, enter the inputs for the selected workflows, and then click **Submit**.
