

cloudera[®]

Cloudera Introduction

Important Notice

© 2010-2021 Cloudera, Inc. All rights reserved.

Cloudera, the Cloudera logo, and any other product or service names or slogans contained in this document are trademarks of Cloudera and its suppliers or licensors, and may not be copied, imitated or used, in whole or in part, without the prior written permission of Cloudera or the applicable trademark holder. If this documentation includes code, including but not limited to, code examples, Cloudera makes this available to you under the terms of the Apache License, Version 2.0, including any required notices. A copy of the Apache License Version 2.0, including any notices, is included herein. A copy of the Apache License Version 2.0 can also be found here: <https://opensource.org/licenses/Apache-2.0>

Hadoop and the Hadoop elephant logo are trademarks of the Apache Software Foundation. All other trademarks, registered trademarks, product names and company names or logos mentioned in this document are the property of their respective owners. Reference to any products, services, processes or other information, by trade name, trademark, manufacturer, supplier or otherwise does not constitute or imply endorsement, sponsorship or recommendation thereof by us.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Cloudera.

Cloudera may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Cloudera, the furnishing of this document does not give you any license to these patents, trademarks copyrights, or other intellectual property. For information about patents covering Cloudera products, see <http://tiny.cloudera.com/patents>.

The information in this document is subject to change without notice. Cloudera shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.

Cloudera, Inc.

**395 Page Mill Road
Palo Alto, CA 94306
info@cloudera.com
US: 1-888-789-1488
Intl: 1-650-362-0488
www.cloudera.com**

Release Information

Version: Cloudera Enterprise 5.4.x
Date: February 3, 2021

Table of Contents

About Cloudera Introduction.....	5
Documentation Overview.....	5
CDH Overview.....	8
Cloudera Impala Overview.....	8
<i>Impala Benefits.....</i>	<i>8</i>
<i>How Cloudera Impala Works with CDH.....</i>	<i>9</i>
<i>Primary Impala Features.....</i>	<i>9</i>
Cloudera Search Overview.....	10
<i>How Cloudera Search Works.....</i>	<i>11</i>
<i>Cloudera Search and Other Cloudera Components.....</i>	<i>12</i>
Apache Sentry Overview.....	13
Cloudera Manager 5 Overview.....	14
Terminology.....	14
Architecture.....	17
State Management.....	18
Configuration Management.....	19
Process Management.....	22
Software Distribution Management.....	22
Host Management.....	23
Resource Management.....	23
User Management.....	26
Security Management.....	27
Cloudera Management Service.....	28
Cloudera Manager Admin Console.....	29
<i>Starting and Logging into the Admin Console.....</i>	<i>31</i>
<i>Cloudera Manager Admin Console Home Page.....</i>	<i>31</i>
<i>Displaying Cloudera Manager Documentation.....</i>	<i>33</i>
<i>Displaying the Cloudera Manager Server Version and Server Time.....</i>	<i>34</i>
Cloudera Manager API.....	34
<i>Backing Up and Restoring the Cloudera Manager Configuration</i>	<i>35</i>
<i>Using the Cloudera Manager Java API for Cluster Automation.....</i>	<i>36</i>
Extending Cloudera Manager.....	38
Cloudera Manager 5 Frequently Asked Questions.....	38

General Questions.....38

Cloudera Navigator 2 Overview.....41

Cloudera Navigator Data Management Component Overview.....42
Cloudera Navigator Data Management Component UI.....42
Cloudera Navigator Data Management Component API.....42
Displaying the Cloudera Navigator Data Management Component Version.....43
Displaying Cloudera Navigator Data Management Component Documentation.....43
Cloudera Navigator 2 Frequently Asked Questions.....43

Cloudera Navigator Data Encryption Overview.....45

Cloudera Navigator Encryption Architecture.....46
Cloudera Navigator Encryption Integration with an EDH.....47
Cloudera Navigator Key Trustee Server Overview.....47
Key Trustee Server Architecture.....48
Cloudera Navigator Key HSM Overview.....48
Key HSM Architecture.....49
Cloudera Navigator Encrypt Overview.....50
Process-Based Access Control List.....51
Encryption Key Storage and Management.....52

Frequently Asked Questions About Cloudera Software.....53

Getting Support.....54

Cloudera Support.....54
Information Required for Logging a Support Case.....54
Community Support.....54
Get Announcements about New Releases.....54
Report Issues.....55

Appendix: Apache License, Version 2.0.....56

About Cloudera Introduction



Important: As of February 1, 2021, all downloads of CDH and Cloudera Manager require a username and password and use a modified URL. You must use the modified URL, including the username and password when downloading the repository contents described below. You may need to upgrade Cloudera Manager to a newer version that uses the modified URLs.

This can affect new installations, upgrades, adding new hosts to a cluster, and adding a new cluster.

For more information, see [Updating an existing CDH/Cloudera Manager deployment to access downloads with authentication.](#)

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

Cloudera provides the following products and tools:

- [CDH](#)—The Cloudera distribution of Apache Hadoop and other related open-source projects, including Impala and Cloudera Search. CDH also provides security and integration with numerous hardware and software solutions.
 - [Cloudera Impala](#)—A massively parallel processing SQL engine for interactive analytics and business intelligence. Its highly optimized architecture makes it ideally suited for traditional BI-style queries with joins, aggregations, and subqueries. It can query Hadoop data files from a variety of sources, including those produced by MapReduce jobs or loaded into Hive tables. The YARN and Llama resource management components let Impala coexist on clusters running batch workloads concurrently with Impala SQL queries. You can manage Impala alongside other Hadoop components through the Cloudera Manager user interface, and secure its data through the Sentry authorization framework.
 - [Cloudera Search](#)—Provides near real-time access to data stored in or ingested into Hadoop and HBase. Search provides near real-time indexing, batch indexing, full-text exploration and navigated drill-down, as well as a simple, full-text interface that requires no SQL or programming skills. Fully integrated in the data-processing platform, Search uses the flexible, scalable, and robust storage system included with CDH. This eliminates the need to move large data sets across infrastructures to perform business tasks.
- [Cloudera Manager](#)—A sophisticated application used to deploy, manage, monitor, and diagnose issues with your CDH deployments. Cloudera Manager provides the Admin Console, a web-based user interface that makes administration of your enterprise data simple and straightforward. It also includes the Cloudera Manager API, which you can use to obtain cluster health information and metrics, as well as configure Cloudera Manager.
- [Cloudera Navigator](#)—An end-to-end data management and security tool for the CDH platform. Cloudera Navigator enables administrators, data managers, and analysts to explore the large amounts of data in Hadoop, and simplifies the storage and management of encryption keys. The robust auditing, data management, lineage management, lifecycle management, and encryption key management in Cloudera Navigator allow enterprises to adhere to stringent compliance and regulatory requirements.

This introductory guide provides a general overview of CDH, Cloudera Manager, and Cloudera Navigator. This guide also includes frequently asked questions about Cloudera products and describes how to get support, report issues, and receive information about updates and new releases.

Documentation Overview

The following guides are included in the Cloudera documentation set:

Guide	Description
Overview of Cloudera and the Cloudera Documentation Set	<p>Cloudera provides a scalable, flexible, integrated platform that makes it easy to manage rapidly increasing volumes and varieties of data in your enterprise. Cloudera products and solutions enable you to deploy and manage Apache Hadoop and related projects, manipulate and analyze your data, and keep that data secure and protected.</p>
Cloudera Release Notes	<p>This guide contains release and download information for installers and administrators. It includes release notes as well as information about versions and downloads. The guide also provides a release matrix that shows which major and minor release version of a product is supported with which release version of Cloudera Manager, CDH and, if applicable, Cloudera Impala.</p>
Cloudera QuickStart	<p>This guide describes how to quickly install Cloudera software and create initial deployments for proof of concept (POC) or development. It describes how to download and use the QuickStart virtual machines, which provide everything you need to start a basic installation. It also shows you how to create a new installation of Cloudera Manager 5, CDH 5, and managed services on a cluster of four hosts. QuickStart installations should be used for demonstrations and POC applications only and are not recommended for production.</p>
#unique_10	<p>This guide provides Cloudera software requirements and installation information for production deployments. This guide also provides specific port information for Cloudera software.</p>
Cloudera Administration	<p>This guide describes how to configure and administer a Cloudera deployment. Administrators manage resources, availability, and backup and recovery configurations. In addition, this guide shows how to implement high availability, and discusses integration.</p>
Cloudera Data Management	<p>This guide describes how to perform data management using Cloudera Navigator. Data management activities include auditing access to data residing in HDFS and Hive metastores, reviewing and updating metadata, and discovering the lineage of data objects.</p>
Cloudera Operation	<p>This guide shows how to monitor the health of a Cloudera deployment and diagnose issues. You can obtain metrics and usage information and view processing activities. This guide also describes how to examine logs and reports to troubleshoot issues with cluster configuration and operation as well as monitor compliance.</p>
Cloudera Security	<p>This guide is intended for system administrators who want to secure a cluster using data encryption, user authentication, and authorization techniques. This topic also provides information about Hadoop security programs and shows you how to set up a gateway to restrict access.</p>

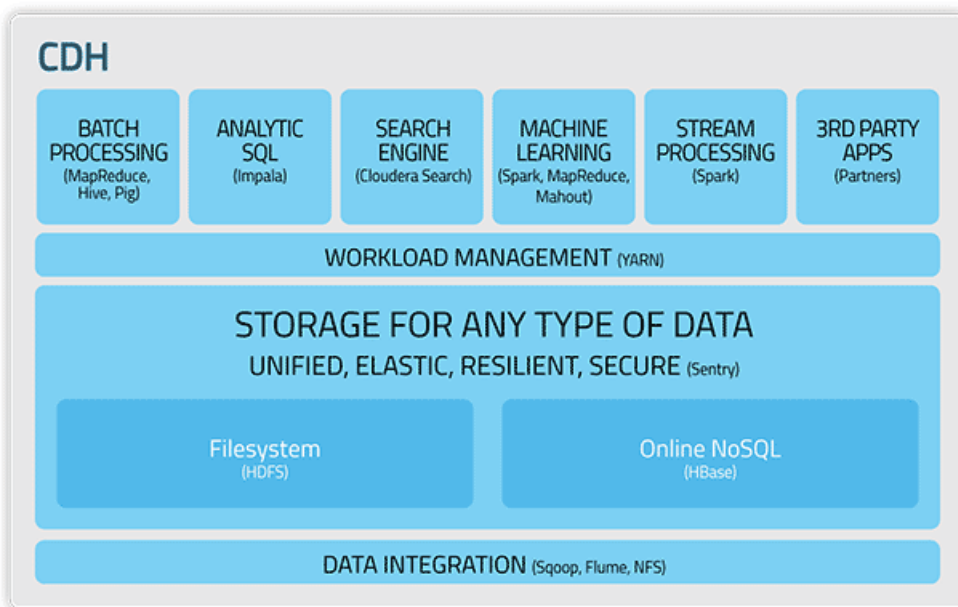
Guide	Description	
Cloudera Impala Guide	This guide describes Cloudera Impala, its features and benefits, and how it works with CDH. This topic introduces Impala concepts, describes how to plan your Impala deployment, and provides tutorials for first-time users as well as more advanced tutorials that describe scenarios and specialized features. You will also find a language reference, performance tuning, instructions for using the Impala shell, troubleshooting information, and frequently asked questions.	
Cloudera Search Guide	Cloudera Search Guide	This guide provides instructions for installing Cloudera software.
Cloudera Glossary	This guide contains a glossary of terms for Cloudera components.	

CDH Overview

CDH is the most complete, tested, and popular distribution of Apache Hadoop and related projects. CDH delivers the core elements of Hadoop – scalable storage and distributed computing – along with a Web-based user interface and vital enterprise capabilities. CDH is Apache-licensed open source and is the only Hadoop solution to offer unified batch processing, interactive SQL and interactive search, and role-based access controls.

CDH provides:

- Flexibility - Store any type of data and manipulate it with a variety of different computation frameworks including batch processing, interactive SQL, free text search, machine learning and statistical computation.
- Integration - Get up and running quickly on a complete Hadoop platform that works with a broad range of hardware and software solutions.
- Security - Process and control sensitive data.
- Scalability - Enable a broad range of applications and scale and extend them to suit your requirements.
- High availability - Perform mission-critical business tasks with confidence.
- Compatibility - Leverage your existing IT infrastructure and investment.



Cloudera Impala Overview

Cloudera Impala provides fast, interactive SQL queries directly on your Apache Hadoop data stored in HDFS, HBase, or the Amazon Simple Storage Service (S3). In addition to using the same unified storage platform, Impala also uses the same metadata, SQL syntax (Hive SQL), ODBC driver, and user interface (Cloudera Impala query UI in Hue) as Apache Hive. This provides a familiar and unified platform for real-time or batch-oriented queries.

Cloudera Impala is an addition to tools available for querying big data. Impala does not replace the batch processing frameworks built on MapReduce such as Hive. Hive and other frameworks built on MapReduce are best suited for long running batch jobs, such as those involving batch processing of Extract, Transform, and Load (ETL) type jobs.

Impala Benefits

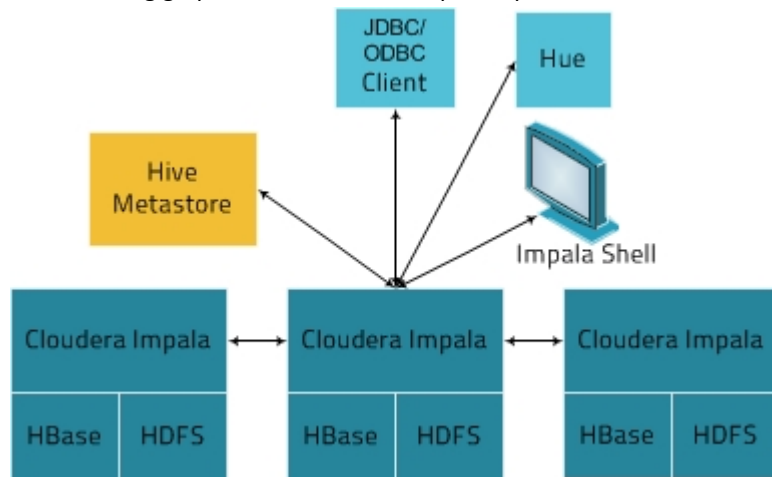
Impala provides:

- Familiar SQL interface that data scientists and analysts already know.

- Ability to query high volumes of data (“big data”) in Apache Hadoop.
- Distributed queries in a cluster environment, for convenient scaling and to make use of cost-effective commodity hardware.
- Ability to share data files between different components with no copy or export/import step; for example, to write with Pig, transform with Hive and query with Impala. Impala can read from and write to Hive tables, enabling simple data interchange using Impala for analytics on Hive-produced data.
- Single system for big data processing and analytics, so customers can avoid costly modeling and ETL just for analytics.

How Cloudera Impala Works with CDH

The following graphic illustrates how Impala is positioned in the broader Cloudera environment:



The Impala solution is composed of the following components:

- Clients - Entities including Hue, ODBC clients, JDBC clients, and the Impala Shell can all interact with Impala. These interfaces are typically used to issue queries or complete administrative tasks such as connecting to Impala.
- Hive Metastore - Stores information about the data available to Impala. For example, the metastore lets Impala know what databases are available and what the structure of those databases is. As you create, drop, and alter schema objects, load data into tables, and so on through Impala SQL statements, the relevant metadata changes are automatically broadcast to all Impala nodes by the dedicated catalog service introduced in Impala 1.2.
- Cloudera Impala - This process, which runs on DataNodes, coordinates and executes queries. Each instance of Impala can receive, plan, and coordinate queries from Impala clients. Queries are distributed among Impala nodes, and these nodes then act as workers, executing parallel query fragments.
- HBase and HDFS - Storage for data to be queried.

Queries executed using Impala are handled as follows:

1. User applications send SQL queries to Impala through ODBC or JDBC, which provide standardized querying interfaces. The user application may connect to any `impalad` in the cluster. This `impalad` becomes the coordinator for the query.
2. Impala parses the query and analyzes it to determine what tasks need to be performed by `impalad` instances across the cluster. Execution is planned for optimal efficiency.
3. Services such as HDFS and HBase are accessed by local `impalad` instances to provide data.
4. Each `impalad` returns data to the coordinating `impalad`, which sends these results to the client.

Primary Impala Features

Impala provides support for:

- Most common SQL-92 features of Hive Query Language (HiveQL) including [SELECT](#), [joins](#), and [aggregate functions](#).
- HDFS, HBase, and Amazon Simple Storage System (S3) storage, including:

- [HDFS file formats](#): delimited text files, Parquet, Avro, SequenceFile, and RCFile.
- Compression codecs: Snappy, GZIP, Deflate, BZIP.
- Common data access interfaces including:
 - [JDBC driver](#).
 - [ODBC driver](#).
 - Hue Beeswax and the Cloudera Impala Query UI.
- [impala-shell command-line interface](#).
- [Kerberos authentication](#).

Cloudera Search Overview

Cloudera Search provides near real-time (NRT) access to data stored in or ingested into Hadoop and HBase. Search provides near real-time indexing, batch indexing, full-text exploration and navigated drill-down, as well as a simple, full-text interface that requires no SQL or programming skills.

Search is fully integrated in the data-processing platform and uses the flexible, scalable, and robust storage system included with CDH. This eliminates the need to move large data sets across infrastructures to perform business tasks.

Cloudera Search incorporates [Apache Solr](#), which includes Apache Lucene, SolrCloud, Apache Tika, and Solr Cell. Cloudera Search is included with CDH 5.

Using Search with the CDH infrastructure provides:

- Simplified infrastructure
- Better production visibility
- Quicker insights across various data types
- Quicker problem resolution
- Simplified interaction and platform access for more users and use cases
- Scalability, flexibility, and reliability of search services on the same platform used to execute other types of workloads on the same data

The following table describes Cloudera Search features.

Table 1: Cloudera Search Features

Feature	Description
Unified management and monitoring with Cloudera Manager	Cloudera Manager provides unified and centralized management and monitoring for CDH and Cloudera Search. Cloudera Manager simplifies deployment, configuration, and monitoring of your search services. Many existing search solutions lack management and monitoring capabilities and fail to provide deep insight into utilization, system health, trending, and other supportability aspects.
Index storage in HDFS	Cloudera Search is integrated with HDFS for index storage. Indexes created by Solr/Lucene can be directly written in HDFS with the data, instead of to local disk, thereby providing fault tolerance and redundancy. Cloudera Search is optimized for fast read and write of indexes in HDFS while indexes are served and queried through standard Solr mechanisms. Because data and indexes are co-located, data processing does not require transport or separately managed storage.
Batch index creation through MapReduce	To facilitate index creation for large data sets, Cloudera Search has built-in MapReduce jobs for indexing data stored in HDFS. As a result, the linear scalability of MapReduce is applied to the indexing pipeline.

Feature	Description
Real-time and scalable indexing at data ingest	Cloudera Search provides integration with Flume to support near real-time indexing. As new events pass through a Flume hierarchy and are written to HDFS, those events can be written directly to Cloudera Search indexers. In addition, Flume supports routing events, filtering, and annotation of data passed to CDH. These features work with Cloudera Search for improved index sharding, index separation, and document-level access control.
Easy interaction and data exploration through Hue	A Cloudera Search GUI is provided as a Hue plug-in, enabling users to interactively query data, view result files, and do faceted exploration. Hue can also schedule standing queries and explore index files. This GUI uses the Cloudera Search API, which is based on the standard Solr API.
Simplified data processing for Search workloads	Cloudera Search relies on Apache Tika for parsing and preparation of many of the standard file formats for indexing. Additionally, Cloudera Search supports Avro, Hadoop Sequence, and Snappy file format mappings, as well as Log file formats, JSON, XML, and HTML. Cloudera Search also provides data preprocessing using Morphlines, which simplifies index configuration for these formats. Users can use the configuration for other applications, such as MapReduce jobs.
HBase search	Cloudera Search integrates with HBase, enabling full-text search of stored data without affecting HBase performance. A listener monitors the replication event stream and captures each write or update-replicated event, enabling extraction and mapping. The event is then sent directly to Solr indexers and written to indexes in HDFS, using the same process as for other indexing workloads of Cloudera Search. The indexes can be served immediately, enabling near real-time search of HBase data.

How Cloudera Search Works

In a near real-time indexing use case, Cloudera Search indexes events that are streamed through Apache Flume to be stored in CDH. Fields and events are mapped to standard Solr indexable schemas. Lucene indexes events, and integration with Cloudera Search allows the index to be directly written and stored in standard Lucene index files in HDFS. Flume event routing and storage of data in partitions in HDFS can also be applied. Events can be routed and streamed through multiple Flume agents and written to separate Lucene indexers that can write into separate index shards, for better scale when indexing and quicker responses when searching.

The indexes are loaded from HDFS to Solr cores, exactly like Solr would have read from local disk. The difference in the design of Cloudera Search is the robust, distributed, and scalable storage layer of HDFS, which helps eliminate costly downtime and allows for flexibility across workloads without having to move data. Search queries can then be submitted to Solr through either the standard Solr API, or through a simple search GUI application, included in Cloudera Search, which can be deployed in Hue.

Cloudera Search batch-oriented indexing capabilities can address needs for searching across batch uploaded files or large data sets that are less frequently updated and less in need of near-real-time indexing. For such cases, Cloudera Search includes a highly scalable indexing workflow based on MapReduce. A MapReduce workflow is launched onto specified files or folders in HDFS, and the field extraction and Solr schema mapping is executed during the mapping phase. Reducers use Solr to write the data as a single index or as index shards, depending on your configuration and preferences. Once the indexes are stored in HDFS, they can be queried using standard Solr mechanisms, as previously described above for the near-real-time indexing use case.

The Lily HBase Indexer Service is a flexible, scalable, fault tolerant, transactional, near real-time oriented system for processing a continuous stream of HBase cell updates into live search indexes. Typically, the time between data ingestion using the Flume sink to that content potentially appearing in search results is measured in seconds, although this duration is tunable. The Lily HBase Indexer uses Solr to index data stored in HBase. As HBase applies inserts, updates, and deletes to HBase table cells, the indexer keeps Solr consistent with the HBase table contents, using standard HBase

replication features. The indexer supports flexible custom application-specific rules to extract, transform, and load HBase data into Solr. Solr search results can contain `columnFamily:qualifier` links back to the data stored in HBase. This way applications can use the Search result set to directly access matching raw HBase cells. Indexing and searching do not affect operational stability or write throughput of HBase because the indexing and searching processes are separate and asynchronous to HBase.

Cloudera Search and Other Cloudera Components

Cloudera Search interacts with other Cloudera components to solve different problems. The following table lists Cloudera components that contribute to the Search process and describes how they interact with Cloudera Search:

Component	Contribution	Applicable To
HDFS	Stores source documents. Search indexes source documents to make them searchable. Files that support Cloudera Search, such as Lucene index files and write-ahead logs, are also stored in HDFS. Using HDFS provides simpler provisioning on a larger base, redundancy, and fault tolerance. With HDFS, Cloudera Search servers are essentially stateless, so host failures have minimal consequences. HDFS also provides snapshotting, inter-cluster replication, and disaster recovery.	All cases
MapReduce	Search includes a pre-built MapReduce-based job. This job can be used for on-demand or scheduled indexing of any supported data set stored in HDFS. This job utilizes cluster resources for scalable batch indexing.	Many cases
Flume	Search includes a Flume sink that enables writing events directly to indexers deployed on the cluster, allowing data indexing during ingestion.	Many cases
Hue	Search includes a Hue front-end search application that uses standard Solr APIs. The application can interact with data indexed in HDFS. The application provides support for the Solr standard query language, visualization of faceted search functionality, and a typical full text search GUI-based.	Many cases
ZooKeeper	Coordinates distribution of data and metadata, also known as shards. It provides automatic failover to increase service resiliency.	Many cases
Spark	The CrunchIndexerTool can use Spark to move data from HDFS files into Apache Solr, and run the data through a morphline for extraction and transformation.	Some cases
HBase	Supports indexing of stored data, extracting columns, column families, and key information as fields. Because HBase does not use secondary indexing, Cloudera Search can complete full-text searches of content in rows and tables in HBase.	Some cases
Cloudera Manager	Deploys, configures, manages, and monitors Cloudera Search processes and resource utilization across services on the cluster. Cloudera Manager helps simplify Cloudera Search administration, but it is not required.	Some cases
Cloudera Navigator	Cloudera Navigator provides governance for Hadoop systems including support for auditing Search operations.	Some cases
Oozie	Automates scheduling and management of indexing jobs. Oozie can check for new data and begin indexing jobs as required.	Some cases
Impala	Further analyzes search results.	Some cases
Hive	Further analyzes search results.	Some cases

Component	Contribution	Applicable To
Avro	Includes metadata that Cloudera Search can use for indexing.	Some cases
Sqoop	Ingests data in batch and enables data availability for batch indexing.	Some cases
Mahout	Applies machine-learning processing to search results.	Some cases

Apache Sentry Overview

Apache Sentry (incubating) is a granular, role-based authorization module for Hadoop. Sentry provides the ability to control and enforce precise levels of privileges on data for authenticated users and applications on a Hadoop cluster. Sentry currently works out of the box with Apache Hive, Hive Metastore/HCatalog, Apache Solr, Impala, and HDFS (limited to Hive table data).

Sentry is designed to be a pluggable authorization engine for Hadoop components. It allows you to define authorization rules to validate a user or application's access requests for Hadoop resources. Sentry is highly modular and can support authorization for a wide variety of data models in Hadoop.

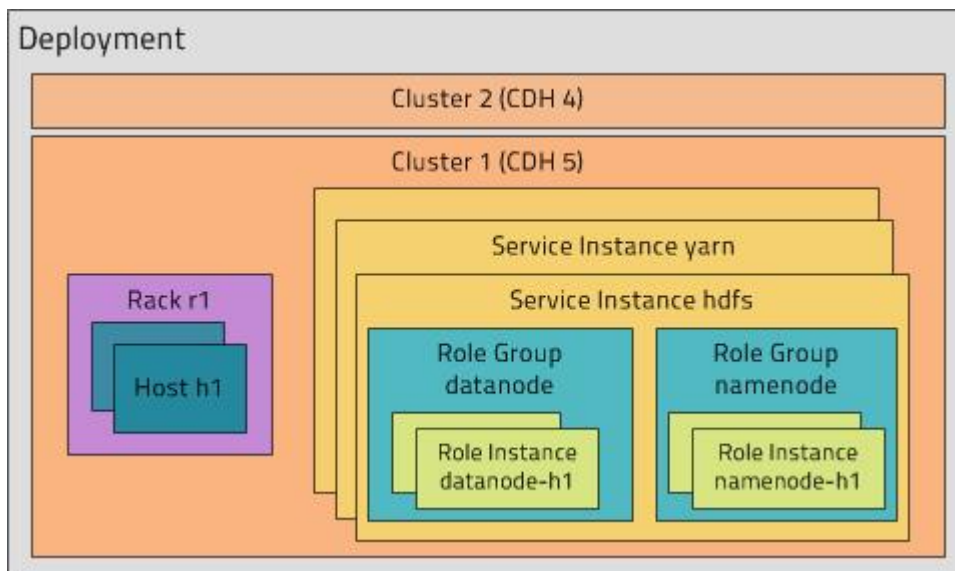
For more information, see [Sentry Overview](#).

Cloudera Manager 5 Overview

Cloudera Manager is an end-to-end application for managing CDH clusters. Cloudera Manager sets the standard for enterprise deployment by delivering granular visibility into and control over every part of the CDH cluster—empowering operators to improve performance, enhance quality of service, increase compliance and reduce administrative costs. With Cloudera Manager, you can easily deploy and centrally operate the complete CDH stack and other managed services. The application automates the installation process, reducing deployment time from weeks to minutes; gives you a cluster-wide, real-time view of hosts and services running; provides a single, central console to enact configuration changes across your cluster; and incorporates a full range of reporting and diagnostic tools to help you optimize performance and utilization. This primer introduces the basic concepts, structure, and functions of Cloudera Manager.

Terminology

To effectively use Cloudera Manager, you should first understand its terminology. The relationship between the terms is illustrated below and their definitions follow:



Some of the terms, such as cluster and service, will be used without further explanation. Others, such as role group, gateway, host template, and parcel are expanded upon in later sections.

A common point of confusion is the overloading of the terms **service** and **role** for both types and instances; Cloudera Manager and this section sometimes uses the same term for type and instance. For example, the Cloudera Manager Admin Console Home page and **Clusters > ClusterName** menu lists service instances. This is similar to the practice in programming languages where for example the term "string" may indicate either a type (`java.lang.String`) or an instance of that type ("hi there"). When it's necessary to distinguish between types and instances, the word "type" is appended to indicate a type and the word "instance" is appended to explicitly indicate an instance.

deployment

A configuration of Cloudera Manager and all the clusters it manages.

dynamic resource pool

In Cloudera Manager, a named configuration of resources and a policy for scheduling the resources among YARN applications or Impala queries running in the pool.

cluster

- A set of computers or racks of computers that contains an [HDFS](#) filesystem and runs [MapReduce](#) and other processes on that data. A pseudo-distributed cluster is a [CDH](#) installation run on a single machine and useful for demonstrations and individual study.
- In Cloudera Manager, a logical entity that contains a set of hosts, a single version of CDH installed on the hosts, and the service and role instances running on the hosts. A host can belong to only one cluster.

host

In Cloudera Manager, a physical or virtual machine that runs role instances.

rack

In Cloudera Manager, a physical entity that contains a set of physical hosts typically served by the same switch.

service

- **Linux** runs a System V init script in `/etc/init.d/` in as predictable an environment as possible, removing most environment variables and setting the current working directory to `/`.
- A category of managed functionality in Cloudera Manager, which may be distributed or not, running in a cluster. Sometimes referred to as a service type. For example: MapReduce, HDFS, YARN, Spark, and Accumulo. In traditional environments, multiple services run on one host; in distributed systems, a service runs on many hosts.

service instance

In Cloudera Manager, an instance of a service running on a cluster. For example: "HDFS-1" and "yarn". A service instance spans many role instances.

role

In Cloudera Manager, a category of functionality within a service. For example, the HDFS service has the following roles: NameNode, SecondaryNameNode, DataNode, and Balancer. Sometimes referred to as a role type. See also [user role](#).

role instance

In Cloudera Manager, an instance of a role running on a host. It typically maps to a Unix process. For example: "NameNode-h1" and "DataNode-h1".

role group

In Cloudera Manager, a set of configuration properties for a set of role instances.

host template

A set of role groups in Cloudera Manager. When a template is applied to a host, a role instance from each role group is created and assigned to that host.

gateway

In Cloudera Manager, role that designates a host that should receive a client configuration for a service when the host does not have any role instances for that service running on it.

parcel

A binary distribution format that contains compiled code and meta-information such as a package description, version, and dependencies.

Cloudera Manager 5 Overview

static service pool




















In Cloudera Manager, a static partitioning of total cluster resources—CPU, memory, and I/O weight—across a set of services.

Cluster Example

Consider a cluster **Cluster 1** with four hosts as shown in the following listing from Cloudera Manager:

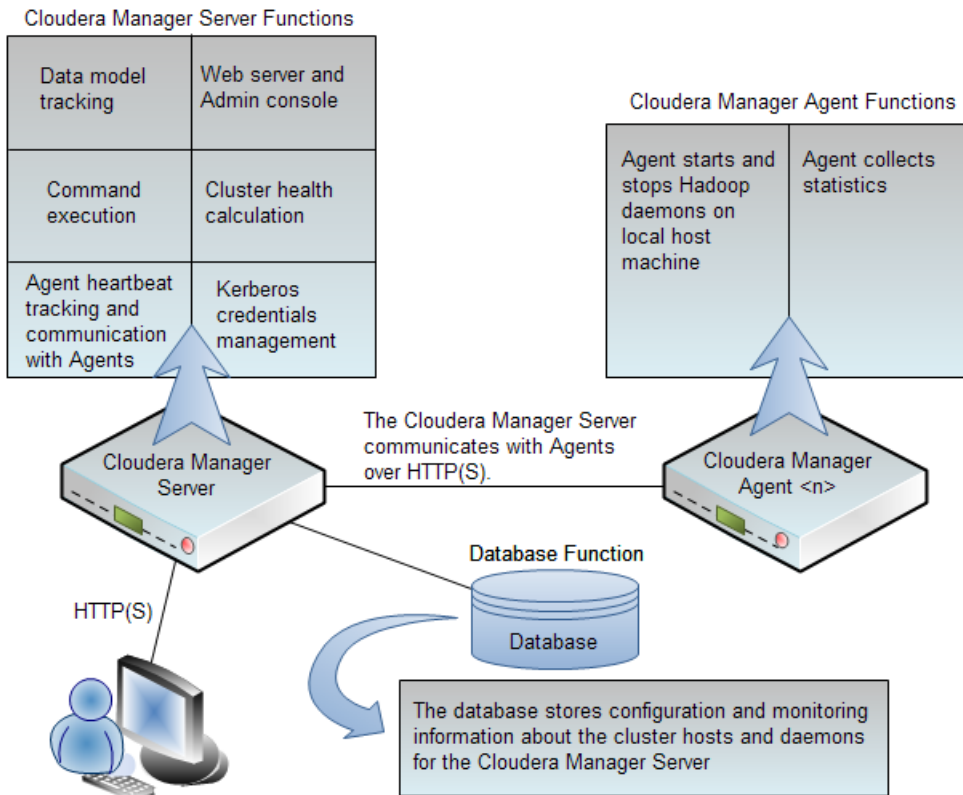
<input type="checkbox"/>	↕ Name	↕ IP	↕ Roles	↕ Load Average	↕ Disk Usage	↕ Physical Memory	↕ Swap Space
<input type="checkbox"/>	tcdn501-1.ent.cloudera.com	10.20.195.240	➤ 21 Role(s)	0.04 0.15 0.26	11.3 GiB / 57 GiB	6.3 GiB / 9.7 GiB	4.7 MB / 2 GiB
<input type="checkbox"/>	tcdn501-2.ent.cloudera.com	10.20.81.81	➤ 7 Role(s)	0.07 0.07 0.05	8.9 GiB / 57 GiB	2 GiB / 9.7 GiB	0 B / 2 GiB
<input type="checkbox"/>	tcdn501-3.ent.cloudera.com	10.20.190.234	➤ 7 Role(s)	0.08 0.11 0.04	8.9 GiB / 57 GiB	2 GiB / 9.7 GiB	0 B / 2 GiB
<input type="checkbox"/>	tcdn501-4.ent.cloudera.com	10.20.195.243	➤ 7 Role(s)	0.06 0.23 0.23	8.9 GiB / 57 GiB	2 GiB / 9.7 GiB	0 B / 2 GiB

The host **tcdn501-1** is the "master" host for the cluster, so it has many more role instances, 21, compared with the 7 role instances running on the other hosts. In addition to the CDH "master" role instances, **tcdn501-1** also has Cloudera Management Service roles:

Service	Instance	Name
None	None	deploy-client-config
 HBase	Master	hbase-MASTER
 HDFS	NameNode	hdfs-NAMENODE
 HDFS	SecondaryNameNode	hdfs-SECONDARYNAMENODE
 Hive	Hive Metastore Server	hive-HIVEMETASTORE
 Hive	HiveServer2	hive-HIVESERVER2
 Hue	Hue Server	hue-HUE_SERVER
 Impala	Impala Catalog Server	impala-CATALOGSERVER
 Impala	Impala StateStore	impala-STATESTORE
 Cloudera Management Service	Alert Publisher	cloudera-mgmt-ALERTPUBLISHER
 Cloudera Management Service	Event Server	cloudera-mgmt-EVENTSERVER
 Cloudera Management Service	Host Monitor	cloudera-mgmt-HOSTMONITOR
 Cloudera Management Service	Navigator Audit Server	cloudera-mgmt-NAVIGATOR
 Cloudera Management Service	Navigator Metadata Server	cloudera-mgmt-NAVIGATORMETASERVER
 Cloudera Management Service	Reports Manager	cloudera-mgmt-REPORTSMANAGER
 Cloudera Management Service	Service Monitor	cloudera-mgmt-SERVICEMONITOR
 Oozie	Oozie Server	oozie-OOZIE_SERVER
 Spark	Master	spark-SPARK_MASTER
 YARN (MR2 Included)	JobHistory Server	yarn-JOBHISTORY
 YARN (MR2 Included)	ResourceManager	yarn-RESOURCEMANAGER

Architecture

As depicted below, the heart of Cloudera Manager is the Cloudera Manager Server. The Server hosts the Admin Console Web Server and the application logic, and is responsible for installing software, configuring, starting, and stopping services, and managing the cluster on which the services run.



The Cloudera Manager Server works with several other components:

- **Agent** - installed on every host. The agent is responsible for starting and stopping processes, unpacking configurations, triggering installations, and monitoring the host.
- **Management Service** - a service consisting of a set of roles that perform various monitoring, alerting, and reporting functions.
- **Database** - stores configuration and monitoring information. Typically, multiple logical databases run across one or more database servers. For example, the Cloudera Manager Server and the monitoring roles use different logical databases.
- **Cloudera Repository** - repository of software for distribution by Cloudera Manager.
- **Clients** - are the interfaces for interacting with the server:
 - **Admin Console** - Web-based UI with which administrators manage clusters and Cloudera Manager.
 - **API** - API with which developers create custom Cloudera Manager applications.

Heartbeating

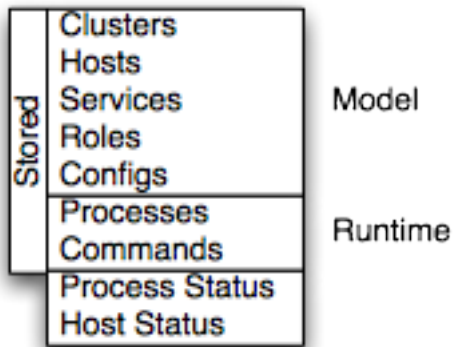
Heartbeats are a primary communication mechanism in Cloudera Manager. By default Agents send heartbeats every 15 seconds to the Cloudera Manager Server. However, to reduce user latency the frequency is increased when state is changing.

During the heartbeat exchange, the Agent notifies the Cloudera Manager Server of its activities. In turn the Cloudera Manager Server responds with the actions the Agent should be performing. Both the Agent and the Cloudera Manager Server end up doing some reconciliation. For example, if you start a service, the Agent attempts to start the relevant processes; if a process fails to start, the Cloudera Manager Server marks the start command as having failed.

State Management

The Cloudera Manager Server maintains the state of the cluster. This state can be divided into two categories: "model" and "runtime", both of which are stored in the Cloudera Manager Server database.

State Maintained by CM Server



Cloudera Manager models CDH and managed services: their roles, configurations, and inter-dependencies. *Model state* captures what is supposed to run where, and with what configurations. For example, model state captures the fact that a cluster contains 17 hosts, each of which is supposed to run a DataNode. You interact with the model through the Cloudera Manager Admin Console configuration screens and API and operations such as "Add Service".

Runtime state is what processes are running where, and what commands (for example, rebalance HDFS or execute a Backup/Disaster Recovery schedule or rolling restart or stop) are currently being executed. The runtime state includes the exact configuration files needed to run a process. When you select Start in the Cloudera Manager Admin Console, the server gathers up all the configuration for the relevant services and roles, validates it, generates the configuration files, and stores them in the database.

When you update a configuration (for example, the Hue Server web port), you've updated the model state. However, if Hue is running while you do this, it's still using the old port. When this kind of mismatch occurs, the role is marked as having an "outdated configuration". To resynchronize, you restart the role (which triggers the configuration re-generation and process restart).

While Cloudera Manager models all of the reasonable configurations, some cases inevitably require special handling. To allow you to work around, for example, a bug or to explore unsupported options, Cloudera Manager supports an "advanced configuration snippet" mechanism that lets you add properties directly to the configuration files.

Configuration Management

Cloudera Manager defines configuration at several levels:

- The service level may define configurations that apply to the entire service instance, such as an HDFS service's default replication factor (`dfs.replication`).
- The [role group](#) level may define configurations that apply to the member roles, such as the DataNodes' handler count (`dfs.datanode.handler.count`). This can be set differently for different groups of DataNodes. For example, DataNodes running on more capable hardware may have more handlers.
- The role instance level may override configurations that it inherits from its role group. This should be used sparingly, because it easily leads to configuration divergence within the role group. One example usage is to temporarily enable debug logging in a specific role instance to troubleshoot an issue.
- Hosts have configurations related to monitoring, software management, and resource management.
- Cloudera Manager itself has configurations related to its own administrative operations.

Role Groups

You can set configuration at the service instance (for example, HDFS) or role instance (for example, the DataNode on host17). An individual role inherits the configurations set at the service level. Configurations made at the role level override those inherited from the service level. While this approach offers flexibility, configuring a set of role instances in the same way can be tedious.

Cloudera Manager supports role groups, a mechanism for assigning configurations to a group of role instances. The members of those groups then inherit those configurations. For example, in a cluster with heterogeneous hardware, a DataNode role group can be created for each host type and the DataNodes running on those hosts can be assigned to their corresponding role group. That makes it possible to set the configuration for all the DataNodes running on the same hardware by modifying the configuration of one role group. The HDFS service discussed earlier has the following role groups defined for the service's roles:

<input type="checkbox"/>	<input type="checkbox"/>	Role Name	State	Host	Role Group
<input type="checkbox"/>	<input type="radio"/>	Balancer	N/A	tcdn501-1.ent.cloudera.com	Balancer Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	DataNode	Started	tcdn501-2.ent.cloudera.com	DataNode Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	DataNode	Started	tcdn501-3.ent.cloudera.com	DataNode Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	DataNode	Started	tcdn501-4.ent.cloudera.com	DataNode Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	NameNode (Active)	Started	tcdn501-1.ent.cloudera.com	NameNode Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	SecondaryNameNode	Started	tcdn501-1.ent.cloudera.com	SecondaryNameNode Default Group

In addition to making it easy to manage the configuration of subsets of roles, role groups also make it possible to maintain different configurations for experimentation or managing shared clusters for different users or workloads.

Host Templates

In typical environments, sets of hosts have the same hardware and the same set of services running on them. A host template defines a set of role groups (at most one of each type) in a cluster and provides two main benefits:

- Adding new hosts to clusters easily - multiple hosts can have roles from different services created, configured, and started in a single operation.
- Altering the configuration of roles from different services on a set of hosts easily - which is useful for quickly switching the configuration of an entire cluster to accommodate different workloads or users.

Server and Client Configuration

Administrators are sometimes surprised that modifying `/etc/hadoop/conf` and then restarting HDFS has no effect. That is because service instances started by Cloudera Manager do not read configurations from the default locations. To use HDFS as an example, when not managed by Cloudera Manager, there would usually be one HDFS configuration per host, located at `/etc/hadoop/conf/hdfs-site.xml`. Server-side daemons and clients running on the same host would all use that same configuration.

Cloudera Manager distinguishes between server and client configuration. In the case of HDFS, the file `/etc/hadoop/conf/hdfs-site.xml` contains only configuration relevant to an HDFS client. That is, by default, if you run a program that needs to communicate with Hadoop, it will get the addresses of the NameNode and JobTracker, and other important configurations, from that directory. A similar approach is taken for `/etc/hbase/conf` and `/etc/hive/conf`.

In contrast, the HDFS role instances (for example, NameNode and DataNode) obtain their configurations from a private per-process directory, under `/var/run/cloudera-scm-agent/process/unique-process-name`. Giving each process its own private execution and configuration environment allows Cloudera Manager to control each process independently. For example, here are the contents of an example `879-hdfs-NAMENODE` process directory:

```
$ tree -a /var/run/cloudera-scm-agent/process/879-hdfs-NAMENODE/
/var/run/cloudera-scm-agent/process/879-hdfs-NAMENODE/
  cloudera_manager_agent_fencer.py
  cloudera_manager_agent_fencer_secret_key.txt
  cloudera-monitor.properties
  core-site.xml
  dfs_hosts_allow.txt
  dfs_hosts_exclude.txt
  event-filter-rules.json
  hadoop-metrics2.properties
```

```

hdfs.keytab
hdfs-site.xml
log4j.properties
logs
  stderr.log
  stdout.log
topology.map
topology.py

```

Distinguishing between server and client configuration provides several advantages:

- Sensitive information in the server-side configuration, such as the password for the Hive Metastore RDBMS, is not exposed to the clients.
- A service that depends on another service may deploy with customized configuration. For example, to get good HDFS read performance, Cloudera Impala needs a specialized version of the HDFS client configuration, which may be harmful to a generic client. This is achieved by separating the HDFS configuration for the Impala daemons (stored in the per-process directory mentioned above) from that of the generic client (`/etc/hadoop/conf`).
- Client configuration files are much smaller and more readable. This also avoids confusing non-administrator Hadoop users with irrelevant server-side properties.

Deploying Client Configurations and Gateways

A client configuration is a zip file that contains the relevant configuration files with the settings for a service. Each zip file contains the set of configuration files needed by the service. For example, the MapReduce client configuration zip file contains copies of `core-site.xml`, `hadoop-env.sh`, `hdfs-site.xml`, `log4j.properties`, and `mapred-site.xml`. Cloudera Manager supports a **Download Client Configuration** action to enable distributing the client configuration file to users outside the cluster.

Cloudera Manager can deploy client configurations within the cluster; each applicable service has a **Deploy Client Configuration** action. This action does not necessarily deploy the client configuration to the entire cluster; it only deploys the client configuration to all the hosts that this service has been assigned to. For example, suppose a cluster has 10 hosts, and a MapReduce service is running on hosts 1-9. When you use Cloudera Manager to deploy the MapReduce client configuration, host 10 will not get a client configuration, because the MapReduce service has no role assigned to it. This design is intentional to avoid deploying conflicting client configurations from multiple services.

To deploy a client configuration to a host that does not have a role assigned to it you use a gateway. A **gateway** is a marker to convey that a service should be accessible from a particular host. Unlike all other roles it has no associated process. In the preceding example, to deploy the MapReduce client configuration to host 10, you assign a MapReduce gateway role to that host.

Gateways can also be used to customize client configurations for some hosts. Gateways can be placed in role groups and those groups can be configured differently. However, unlike role instances, there is no way to override configurations for gateway instances.

In the cluster we discussed earlier, the three hosts (**tcdn501-[2-5]**) that do not have Hive role instances have Hive gateways:

<input type="checkbox"/>	<input type="checkbox"/>	↑ Role Name	↑ State	↑ Host	↑ Role Group
<input type="checkbox"/>	<input type="radio"/>	Gateway	N/A	tcdn501-2.ent.cloudera.com	Gateway Default Group
<input type="checkbox"/>	<input type="radio"/>	Gateway	N/A	tcdn501-3.ent.cloudera.com	Gateway Default Group
<input type="checkbox"/>	<input type="radio"/>	Gateway	N/A	tcdn501-4.ent.cloudera.com	Gateway Default Group
<input type="checkbox"/>	<input type="radio"/>	Gateway	N/A	tcdn501-1.ent.cloudera.com	Gateway Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	Hive Metastore Server	Started	tcdn501-1.ent.cloudera.com	Hive Metastore Server Default Group
<input type="checkbox"/>	<input checked="" type="radio"/>	HiveServer2	Started	tcdn501-1.ent.cloudera.com	HiveServer2 Default Group

Process Management

In a non-Cloudera Manager managed cluster, you most likely start a role instance process using an init script, for example, `service hadoop-hdfs-datanode start`. Cloudera Manager does not use `init` scripts for the daemons it manages; in a Cloudera Manager managed cluster, starting and stopping services using `init` scripts will not work.

In a Cloudera Manager managed cluster, you can only start or stop role instance processes using Cloudera Manager. Cloudera Manager uses an open source process management tool called `supervisord`, that starts processes, takes care of redirecting log files, notifying of process failure, setting the effective user ID of the calling process to the right user, and so on. Cloudera Manager supports automatically restarting a crashed process. It will also flag a role instance with a bad health flag if its process crashes repeatedly right after start up.

Stopping the Cloudera Manager Server and the Cloudera Manager Agents will not bring down your services; any running role instances keep running.

The Agent is started by `init.d` at start-up. It, in turn, contacts the Cloudera Manager Server and determines which processes should be running. The Agent is monitored as part of Cloudera Manager's host monitoring. If the Agent stops heartbeating, the host is marked as having bad health.

One of the Agent's main responsibilities is to start and stop processes. When the Agent detects a new process from the Server heartbeat, the Agent creates a directory for it in `/var/run/cloudera-scm-agent` and unpacks the configuration. It then contacts `supervisord`, which starts the process.

These actions reinforce an important point: a Cloudera Manager process never travels alone. In other words, a process is more than just the arguments to `exec()` — it also includes configuration files, directories that need to be created, and other information.

Software Distribution Management

A major function of Cloudera Manager is to install CDH and managed service software in your cluster. Cloudera Manager supports two software distribution formats: packages and parcels.

A **package** is a binary distribution format that contains compiled code and meta-information such as a package description, version, and dependencies. Package management systems evaluate this meta-information to allow package searches, perform upgrades to a newer version, and ensure that all dependencies of a package are fulfilled. Cloudera Manager uses the native "system package manager" for each supported OS.

A **parcel** is a binary distribution format containing the program files, along with additional metadata used by Cloudera Manager. There are a few notable differences between parcels and packages:

- Parcels are self-contained and installed in a versioned directory, which means that multiple versions of a given parcel can be installed side-by-side. You can then designate one of these installed versions as the active one. With packages, only one package can be installed at a time so there's no distinction between what's installed and what's active.
- Parcels can be installed at any location in the filesystem and by default are installed in `/opt/cloudera/parcels`. In contrast, packages are installed in `/usr/lib`.
- Parcel handling automatically downloads, distributes, and activates the correct parcel for the operating system running on each host in the cluster. Mixed operating system type and version clusters are supported, however using the same version of the same operating system on all cluster hosts is strongly recommended.

As a consequence of their unique properties, parcels offer a number of advantages over packages:

- **CDH is distributed as a single object** - In contrast to having a separate package for each part of CDH, when using parcels there is just a single object to install. This is especially useful when managing a cluster that isn't connected to the Internet.
- **Internal consistency** - All CDH components are matched so there isn't a danger of different parts coming from different versions of CDH.
- **Installation outside of `/usr`** - In some environments, Hadoop administrators do not have privileges to install system packages. In the past, these administrators had to fall back to CDH tarballs, which deprived them of a lot

of infrastructure that packages provide. With parcels, administrators can install to `/opt` or anywhere else without having to step through all the additional manual steps of regular tarballs.



Note: With parcel software distribution, the path to the CDH libraries is `/opt/cloudera/parcels/CDH/lib` instead of the usual `/usr/lib`. You should not link `/usr/lib/` elements to parcel deployed paths, as such links may confuse scripts that distinguish between the two paths.

- **Installation of CDH without `sudo`** - Parcel installation is handled by the Cloudera Manager Agent running as root so it's possible to install CDH without needing `sudo`.
- **Decouples distribution from activation** - Due to side-by-side install capabilities, it is possible to stage a new version of CDH across the cluster in advance of switching over to it. This allows the longest running part of an upgrade to be done ahead of time without affecting cluster operations, consequently reducing the downtime associated with upgrade.
- **Rolling upgrades** - These are only possible with parcels, due to their side-by-side nature. Packages require shutting down the old process, upgrading the package, and then starting the new process. This can be hard to recover from in the event of errors and requires extensive integration with the package management system to function seamlessly. When a new version is staged side-by-side, switching to a new minor version is simply a matter of changing which version of CDH is used when restarting each process. It then becomes practical to do upgrades with [rolling restarts](#), where service roles are restarted in the right order to switch over to the new version with minimal service interruption. Your cluster can continue to run on the existing installed components while you stage a new version across your cluster, without impacting your current operations. Note that major version upgrades (for example, CDH 4 to CDH 5) require full service restarts due to the substantial changes between the versions. Finally, you can upgrade individual parcels, or multiple parcels at the same time.
- **Upgrade management** - Cloudera Manager can fully manage all the steps involved in a CDH version upgrade. In contrast, with packages, Cloudera Manager can only help with initial installation.
- **Distributing additional components** - Parcels are not limited to CDH. Cloudera Impala, Cloudera Search, LZ0, and [add-on service](#) parcels are also available.
- **Compatibility with other distribution tools** - If there are specific reasons to use other tools for download and/or distribution, you can do so, and Cloudera Manager will work alongside your other tools. For example, you can handle distribution with Puppet. Or, you can download the parcel to Cloudera Manager Server manually (perhaps because your cluster has no Internet connectivity) and then have Cloudera Manager distribute the parcel to the cluster.

Host Management

Cloudera Manager provides several features to manage the hosts in your Hadoop clusters. The first time you run Cloudera Manager Admin Console you can search for hosts to add to the cluster and once the hosts are selected you can map the assignment of CDH roles to hosts. Cloudera Manager automatically deploys all software required to participate as a managed host in a cluster: JDK, Cloudera Manager Agent, CDH, Impala, Solr, and so on to the hosts.

Once the services are deployed and running, the Hosts area within the Admin Console shows the overall status of the managed hosts in your cluster. The information provided includes the version of CDH running on the host, the cluster to which the host belongs, and the number of roles running on the host. Cloudera Manager provides operations to manage the life cycle of the participating hosts and to add and delete hosts. The Cloudera Management Service Host Monitor role performs health tests and collects host metrics to allow you to monitor the health and performance of the hosts.

Resource Management

Resource management helps ensure predictable behavior by defining the impact of different services on cluster resources. The goals of resource management features are to:

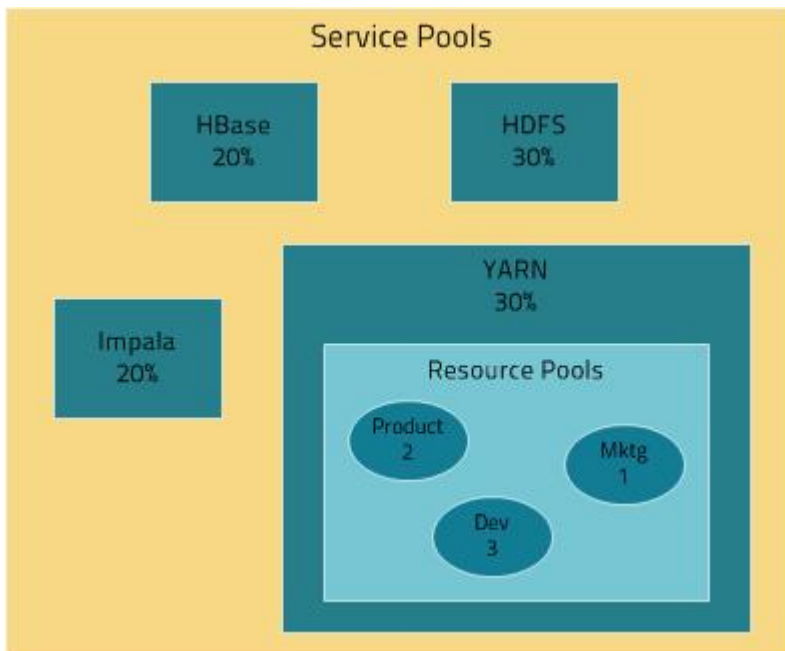
- Guarantee completion in a reasonable time frame for critical workloads

- Support reasonable cluster scheduling between groups of users based on fair allocation of resources per group
- Prevent users from depriving other users access to the cluster

Cloudera Manager 4 introduced the ability to partition resources across HBase, HDFS, Impala, MapReduce, and YARN services by allowing you to set configuration properties that were enforced by Linux control groups (Linux cgroups). With Cloudera Manager 5, the ability to statically allocate resources using cgroups is configurable through a single *static service pool wizard*. You allocate services a percentage of total resources and the wizard configures the cgroups.

Static service pools isolate the services in your cluster from one another, so that load on one service has a bounded impact on other services. Services are allocated a static percentage of total resources—CPU, memory, and I/O weight—which are not shared with other services. When you configure static service pools, Cloudera Manager computes recommended memory, CPU, and I/O configurations for the worker roles of the services that correspond to the percentage assigned to each service. Static service pools are implemented per role group within a cluster, using [Linux control groups \(cgroups\)](#) and cooperative memory limits (for example, Java maximum heap sizes). Static service pools can be used to control access to resources by HBase, HDFS, Impala, MapReduce, Solr, Spark, YARN, and [add-on](#) services. Static service pools are not enabled by default.

For example, the following figure illustrates static pools for HBase, HDFS, Impala, and YARN services that are respectively assigned 20%, 30%, 20%, and 30% of cluster resources.

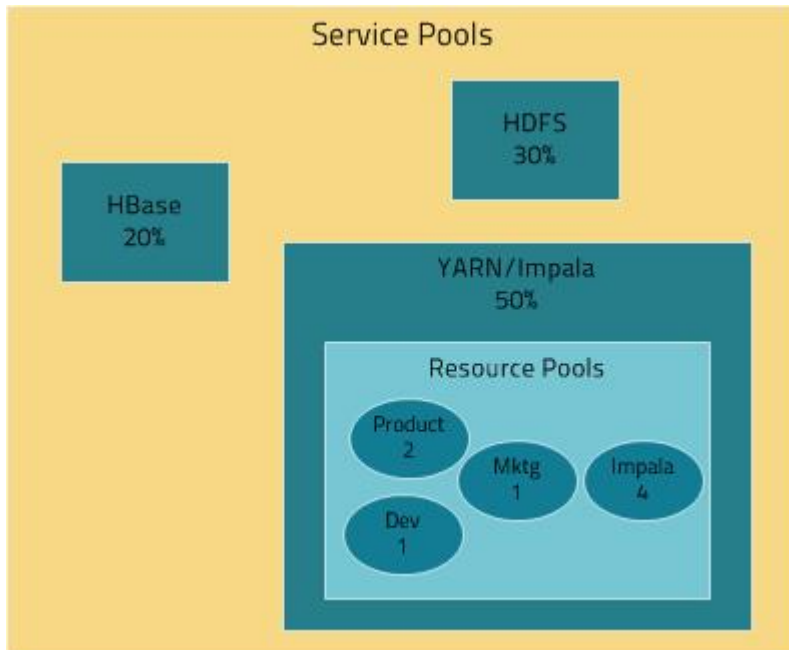


Cloudera Manager allows you to manage mechanisms for dynamically apportioning resources statically allocated to YARN and Impala using *dynamic resource pools*.

Depending on the version of CDH you are using, dynamic resource pools in Cloudera Manager support the following resource management (RM) scenarios:

- **(CDH 5) YARN Independent RM** - YARN manages the virtual cores, memory, running applications, and scheduling policy for each pool. In the preceding diagram, three dynamic resource pools - Dev, Product, and Mktg with weights 3, 2, and 1 respectively - are defined for YARN. If an application starts and is assigned to the Product pool, and other applications are using the Dev and Mktg pools, the Product resource pool will receive $30\% \times 2/6$ (or 10%) of the total cluster resources. If there are no applications using the Dev and Mktg pools, the YARN Product pool will be allocated 30% of the cluster resources.
- **(CDH 5) YARN and Impala Integrated RM** - YARN manages memory for pools running Impala queries; Impala limits the number of running and queued queries in each pool. In the YARN and Impala integrated RM scenario, Impala services can reserve resources through YARN, effectively sharing the static YARN service pool and resource pools with YARN applications. The integrated resource management scenario, where both YARN and Impala use the YARN resource management framework, require the [Impala Llama](#) role.

In the following figure, the YARN and Impala services have a 50% static share which is subdivided among the original resource pools with an additional resource pool designated for the Impala service. If YARN applications are using all the original pools, and Impala uses its designated resource pool, Impala queries will have the same resource allocation $50\% \times 4/8 = 25\%$ as in the first scenario. However, when YARN applications are not using the original pools, Impala queries will have access to 50% of the cluster resources.

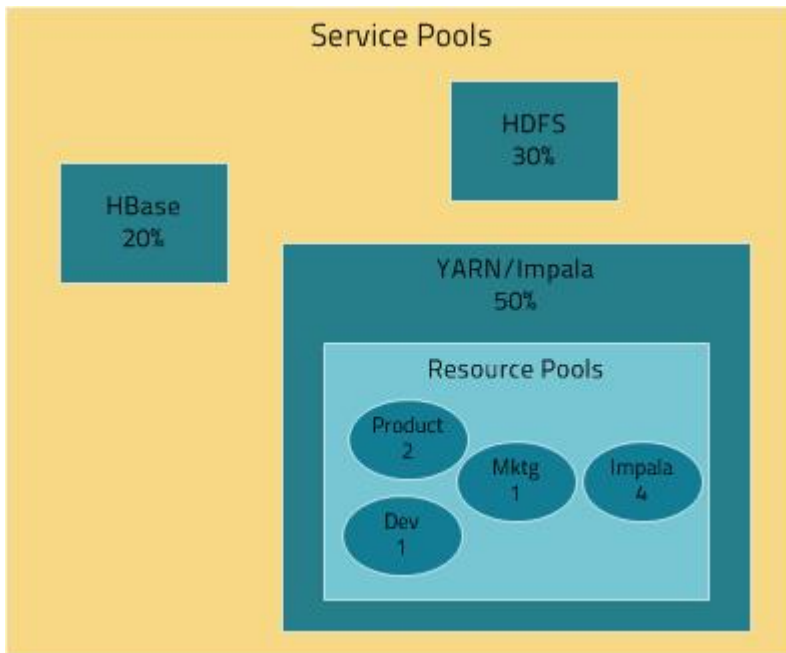


Note:

When using YARN with Impala, Cloudera recommends using the static partitioning technique (through a static service pool) rather than the combination of YARN and Llama. YARN is a central, synchronous scheduler and thus introduces higher latency and variance which is better suited for batch processing than for interactive workloads like Impala (especially with higher concurrency). Currently, YARN allocates memory throughout the query, making it hard to reason about out-of-memory and timeout conditions.

- **(CDH 5) YARN and Impala Independent RM** - YARN manages the virtual cores, memory, running applications, and scheduling policy for each pool; Impala manages memory for pools running queries and limits the number of running and queued queries in each pool.
- **(CDH 5 and CDH 4) Impala Independent RM** - Impala manages memory for pools running queries and limits the number of running and queued queries in each pool.

The scenarios where YARN manages resources, whether for independent RM or integrated RM, map to the YARN scheduler configuration. The scenarios where Impala independently manages resources employ the Impala [admission control](#) feature.



User Management

Access to Cloudera Manager features is controlled by user accounts. A user account identifies how a user is authenticated and determines what privileges are granted to the user.

Cloudera Manager provides several mechanisms for authenticating users. You can configure Cloudera Manager to authenticate users against the Cloudera Manager database or against an [external authentication service](#). The external authentication service can be an LDAP server (Active Directory or an OpenLDAP compatible directory), or you can specify another external service. Cloudera Manager also supports using the Security Assertion Markup Language (SAML) to enable single sign-on.

A user account can be assigned one of the following roles:

- **Auditor** - View data and audit events in Cloudera Manager.
- **Read-Only** - View monitoring information, as well as data.
- **Limited Operator** - Decommission hosts, as well as view service and monitoring information and data.
- **Operator** - Decommission and recommission hosts and roles, as well as view service and monitoring information and data.
- **Configurator** - Perform the Operator operations described above, configure services, enter and exit maintenance mode, and manage dashboards.
- **Cluster Administrator** - View all data and perform all actions except the following: administer Cloudera Navigator, perform replication and snapshot operations, view audit events, manage user accounts, and configure external authentication.
- **BDR Administrator** - View service and monitoring information and data, and perform replication and snapshot operations.
- **Navigator Administrator** - View service and monitoring information and data, view audit events, and administer Cloudera Navigator.
- **User Administrator** - Manage user accounts and configure external authentication, as well as view service and monitoring information and data.
- **Full Administrator** - View all data and do all actions, including reconfiguring and restarting services, and administering other users.

For more information about the privileges associated with each of the Cloudera Manager user roles, see [Cloudera Manager User Roles](#).

Security Management

Cloudera Manager strives to consolidate security configurations across several projects.

Authentication

The purpose of authentication in Hadoop, as in other systems, is simply to prove that a user or service is who he or she claims to be.

Typically, authentication in enterprises is managed through a single distributed system, such as a Lightweight Directory Access Protocol (LDAP) directory. LDAP authentication consists of straightforward username/password services backed by a variety of storage systems, ranging from file to database.

A common enterprise-grade authentication system is Kerberos. Kerberos provides strong security benefits including capabilities that render intercepted authentication packets unusable by an attacker. It virtually eliminates the threat of impersonation by never sending a user's credentials in cleartext over the network.

Several components of the Hadoop ecosystem are converging to use Kerberos authentication with the option to manage and store credentials in LDAP or AD. For example, Microsoft's Active Directory (AD) is an LDAP directory that also provides Kerberos authentication for added security.

Authorization

Authorization is concerned with who or what has access or control over a given resource or service. Since Hadoop merges together the capabilities of multiple varied, and previously separate IT systems as an enterprise data hub that stores and works on all data within an organization, it requires multiple authorization controls with varying granularities. In such cases, Hadoop management tools simplify setup and maintenance by:

- Tying all users to groups, which can be specified in existing LDAP or AD directories.
- Providing role-based access control for similar interaction methods, like batch and interactive SQL queries. For example, Apache Sentry permissions apply to Hive (HiveServer2) and Impala.

CDH currently provides the following forms of access control:

- Traditional POSIX-style permissions for directories and files, where each directory and file is assigned a single owner and group. Each assignment has a basic set of permissions available; file permissions are simply read, write, and execute, and directories have an additional permission to determine access to child directories.
- [Extended Access Control Lists](#) (ACLs) for HDFS that provide fine-grained control of permissions for HDFS files by allowing you to set different permissions for specific named users or named groups.
- Apache HBase uses ACLs to authorize various operations (`READ`, `WRITE`, `CREATE`, `ADMIN`) by column, column family, and column family qualifier. HBase ACLs are granted and revoked to both users and groups.
- Role-based access control with Apache Sentry.

Encryption

The goal of encryption is to ensure that only authorized users can view, use, or contribute to a data set. These security controls add another layer of protection against potential threats by end-users, administrators and other malicious actors on the network. Data protection can be applied at a number of levels within Hadoop:

- **OS Filesystem-level** - Encryption can be applied at the Linux operating system file system level to cover all files in a volume. An example of this approach is [Cloudera Navigator Encrypt](#) (formerly Gazzang zNcrypt) which is available for Cloudera customers licensed for Cloudera Navigator. Navigator Encrypt operates at the Linux volume level, so it can encrypt cluster data inside and outside HDFS, such as temp/spill files, configuration files and metadata databases (to be used only for data related to a CDH cluster). Navigator Encrypt must be used with [Cloudera Navigator Key Trustee Server](#) (formerly Gazzang zTrustee).
- **HDFS-level** - Encryption applied by the HDFS client software. [HDFS Data At Rest Encryption](#) operates at the HDFS folder level, allowing you to encrypt some folders and leave others unencrypted. Cannot encrypt any data outside HDFS. To ensure reliable key storage (so that data is not lost), Cloudera Navigator Key Trustee Server should be

used, while the default Java keystore can be used for test purposes. See [Integrating HDFS Encryption with Navigator Key Trustee Server](#) for more information.

- **Network-level** - Encryption can be applied to encrypt data just before it gets sent across a network and to decrypt it just after receipt. In Hadoop this means coverage for data sent from client user interfaces as well as service-to-service communication like remote procedure calls (RPCs). This protection uses industry-standard protocols such as TLS/SSL.

Cloudera Management Service

The Cloudera Management Service implements various management features as a set of roles:




- **Activity Monitor** - collects information about activities run by the MapReduce service. This role is not added by default.
- **Host Monitor** - collects health and metric information about hosts
- **Service Monitor** - collects health and metric information about services and activity information from the YARN and Impala services
- **Event Server** - aggregates relevant Hadoop events and makes them available for alerting and searching
- **Alert Publisher** - generates and delivers alerts for certain types of events
- **Reports Manager** - generates reports that provide an historical view into disk utilization by user, user group, and directory, processing activities by user and YARN pool, and HBase tables and namespaces. This role is not added in Cloudera Express.

In addition, for certain editions of the Cloudera Enterprise license, the Cloudera Management Service provides the [Navigator Audit Server](#) and [Navigator Metadata Server](#) roles for [Cloudera Navigator](#).

Health Tests

Cloudera Manager monitors the health of the services, roles, and hosts that are running in your clusters via **health tests**. The Cloudera Management Service also provides health tests for its roles. Role-based health tests are enabled by default. For example, a simple health test is whether there's enough disk space in every NameNode data directory. A more complicated health test may evaluate when the last checkpoint for HDFS was compared to a threshold or whether a DataNode is connected to a NameNode. Some of these health tests also aggregate other health tests: in a distributed system like HDFS, it's normal to have a few DataNodes down (assuming you've got dozens of hosts), so we allow for setting thresholds on what percentage of hosts should color the entire service down.

Health tests can return one of three values: **Good**, **Concerning**, and **Bad**. A test returns **Concerning** health if the test falls below a warning threshold. A test returns **Bad** if the test falls below a critical threshold. The overall health of a service or role instance is a roll-up of its health tests. If any health test is **Concerning** (but none are **Bad**) the role's or service's health is **Concerning**; if any health test is **Bad**, the service's or role's health is **Bad**.

In the Cloudera Manager Admin Console, health tests results are indicated with colors: **Good** , **Concerning** , and **Bad** .

One common question is whether monitoring can be separated from configuration. One of the goals for monitoring is to enable it without needing to do additional configuration and installing additional tools (for example, Nagios). By having a deep model of the configuration, Cloudera Manager is able to know which directories to monitor, which ports to use, and what credentials to use for those ports. This tight coupling means that, when you install Cloudera Manager all the monitoring is enabled.

Metric Collection and Display

To perform monitoring, the Service Monitor and Host Monitor collects metrics. A **metric** is a numeric value, associated with a name (for example, "CPU seconds"), an entity it applies to ("host17"), and a timestamp. Most metric collection is performed by the Agent. The Agent communicates with a supervised process, requests the metrics, and forwards them to the Service Monitor. In most cases, this is done once per minute.


A few special metrics are collected by the Service Monitor. For example, the Service Monitor hosts an HDFS canary, which tries to write, read, and delete a file from HDFS at regular intervals, and measure whether it succeeded, and how long it took. Once metrics are received, they're aggregated and stored.

Using the Charts page in the Cloudera Manager Admin Console, you can query and explore the metrics being collected. Charts display **time series**, which are streams of metric data points for a specific entity. Each metric data point contains a timestamp and the value of that metric at that timestamp.

Some metrics (for example, `total_cpu_seconds`) are counters, and the appropriate way to query them is to take their rate over time, which is why a lot of metrics queries contain the `dt0` function. For example, `dt0(total_cpu_seconds)`. (The `dt0` syntax is intended to remind you of derivatives. The 0 indicates that the rate of a monotonically increasing counter should never have negative rates.)

Events, Alerts, and Triggers

An **event** is a record that something of interest has occurred – a service's health has changed state, a log message (of the appropriate severity) has been logged, and so on. Many events are enabled and configured by default.

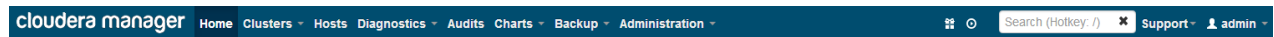
An **alert** is an event that is considered especially noteworthy and is triggered by a selected event. Alerts are shown with an  badge when they appear in a list of [events](#). You can configure the Alert Publisher to send alert notifications by email or via SNMP trap to a trap receiver.

A **trigger** is a statement that specifies an action to be taken when one or more specified conditions are met for a service, role, role configuration group, or host. The conditions are expressed as a [tsquery statement](#), and the action to be taken is to change the health for the service, role, role configuration group, or host to either Concerning (yellow) or Bad (red).

Cloudera Manager Admin Console



Cloudera Manager Admin Console is the web-based UI that you use to configure, manage, and monitor CDH.

If there are no services configured when you log into the Cloudera Manager Admin Console, the Cloudera Manager installation wizard displays. If services have been configured, the Cloudera Manager top navigation bar:



and [Home](#) page display. In addition to a link to the Home page, the Cloudera Manager Admin Console top navigation bar provides the following features:

- **Clusters > ClusterName**
 - **Services** - Display individual services, and the Cloudera Management Service. In these pages you can:
 - View the status and other details of a service instance or the role instances associated with the service
 - Make configuration changes to a service instance, a role, or a specific role instance
 - Add and delete a service or role
 - Stop, start, or restart a service or role.
 - View the commands that have been run for a service or a role
 - View an audit event history
 - Deploy and download client configurations
 - Decommission and recommission role instances
 - Enter or exit maintenance mode
 - Perform actions unique to a specific type of service. For example:
 - Enable HDFS high availability or NameNode federation
 - Run the HDFS Balancer
 - Create HBase, Hive, and Sqoop directories
 - **Hosts** - Displays the hosts in the cluster.

- **Dynamic Resource Pools** - Manage dynamic allocation of cluster resources to YARN and Impala services by specifying the relative weights of named pools.
- **Static Service Pools** - Manage static allocation of cluster resources to HBase, HDFS, Impala, MapReduce, and YARN services.
- **Reports** - Create reports about the HDFS, MapReduce, YARN, and Impala usage and browse HDFS files, and manage quotas for HDFS directories.
- **ImpalaServiceName Queries** - Query information about Impala queries running on your cluster.
- **MapReduceServiceName Jobs** - Query information about MapReduce jobs running on your cluster.
- **YARNServiceName Applications** - Query information about YARN applications running on your cluster.
- **Hosts** - Display the hosts managed by Cloudera Manager. In this page you can:
 - View the status and a variety of detail metrics about individual hosts
 - Make configuration changes for host monitoring
 - View all the processes running on a host
 - Run the Host Inspector
 - Add and delete hosts
 - Create and manage host templates
 - Manage parcels
 - Decommission and recommission hosts
 - Make rack assignments
 - Run the host upgrade wizard
- **Diagnostics** - Review logs, events, and alerts to diagnose problems. The subpages are:
 - **Events** - Search for and displaying events and alerts that have occurred.
 - **Logs** - Search logs by service, role, host, and search phrase as well as log level (severity).
 - **Server Log** - Display the Cloudera Manager Server log.
- **Audits** - Query and filter audit events across clusters.
- **Charts** - Query for metrics of interest, display them as charts, and display personalized chart dashboards.
- **Backup** - Manage replication schedules and snapshot policies.
- **Administration** - Administer Cloudera Manager. The subpages are:
 - **Settings** - Configure Cloudera Manager.
 - **Alerts** - Display when alerts will be generated, configure alert recipients, and send test alert email.
 - **Users** - Manage Cloudera Manager users.
 - **Kerberos** - Generate Kerberos credentials and inspect hosts.
 - **License** - Manage Cloudera licenses.
 - **Language** - Set the language used for the content of activity events, health events, and alert email messages.
 - **Peers** - Connect multiple instances of Cloudera Manager.
- **Indicators**
 - **Parcel Indicator**  indicates how many parcels are eligible for downloading or distribution.
 - **Running Commands Indicator**  displays the number of commands currently running for all services or roles.
- **Search** - Supports searching for services, roles, hosts, configuration properties, and commands. You can enter a partial string and a drop-down list with up to sixteen entities that match will display.
- **Support** - Displays various support actions. The subcommands are:
 - **Send Diagnostic Data** - Sends data to Cloudera Support to support troubleshooting.
 - **Support Portal (Cloudera Enterprise)** - Displays the Cloudera Support portal.
 - **Mailing List (Cloudera Express)** - Displays the Cloudera Manager Users list.
 - **Scheduled Diagnostics: Weekly** - Configure the frequency of automatically collecting diagnostic data and sending to Cloudera support.

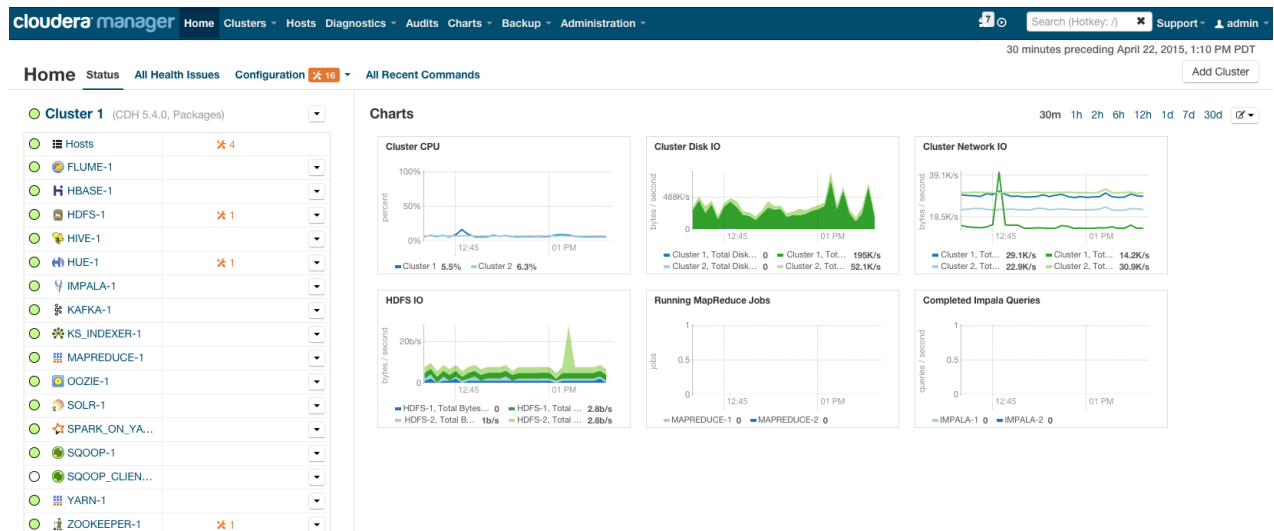
- The following links open the latest documentation on the Cloudera web site:
 - **Help**
 - **Installation Guide**
 - **API Documentation**
 - **Release Notes**
- **About** - Version number and build details of Cloudera Manager and the current date and time stamp of the Cloudera Manager server.
- **Logged-in User Menu** - The currently logged-in user. The subcommands are:
 - **Change Password** - Change the password of the currently logged in user.
 - **Logout**

Starting and Logging into the Admin Console

1. In a web browser, enter `http://Server host:7180`, where *Server host* is the fully qualified domain name or IP address of the host where the Cloudera Manager Server is running. The login screen for Cloudera Manager Admin Console displays.
2. Log into Cloudera Manager Admin Console using the [credentials](#) assigned by your administrator. User accounts are assigned [roles](#) that constrain the features available to you.

Cloudera Manager Admin Console Home Page

When you start the [Cloudera Manager Admin Console](#) on page 29, the Home page displays.



You can also go to the Home page by clicking **Home** in the top navigation bar.

Status

The default tab displayed when the Home page displays. It contains:

- **Clusters** - The clusters being managed by Cloudera Manager. Each cluster is displayed either in summary form or in full form depending on the configuration of the **Administration > Settings > Other > Maximum Cluster Count Shown In Full** property. When the number of clusters exceeds the value of the property, only cluster summary information displays.
 - **Summary Form** - A list of links to cluster status pages. Click **Customize** to jump to the **Administration > Settings > Other > Maximum Cluster Count Shown In Full** property.
 - **Full Form** - A separate section for each cluster containing a link to the cluster status page and a table containing links to the Hosts page and the status pages of the services running in the cluster.

Each service row in the table has a menu of actions that you select by clicking



and can contain one or more of the following indicators:

Indicator	Meaning	Description
	Health issue	<p>Indicates that the service has at least one health issue. The indicator shows the number of health issues at the highest severity level. If there are Bad health test results, the indicator is red. If there are no Bad health test results, but Concerning test results exist, then the indicator is yellow. No indicator is shown if there are no Bad or Concerning health test results.</p> <div style="border: 1px solid #f0e68c; padding: 10px; margin: 10px 0;"> <p> Important: If there is one Bad health test result and two Concerning health results, there will be three health issues, but the number will be one.</p> </div> <p>Click the indicator to display the Health Issues pop-up dialog.</p> <p>By default only Bad health test results are shown in the dialog. To display Concerning health test results, click the Also show <i>n</i> concerning issue(s) link. Click the link to display the Status page containing with details about the health test result.</p>
	Configuration issue	<p>Indicates that the service has at least one configuration issue. The indicator shows the number of configuration issues at the highest severity level. If there are configuration errors, the indicator is red. If there are no errors but configuration warnings exist, then the indicator is yellow. No indicator is shown if there are no configuration notifications.</p> <div style="border: 1px solid #f0e68c; padding: 10px; margin: 10px 0;"> <p> Important: If there is one configuration error and two configuration warnings, there will be three configuration issues, but the number will be one.</p> </div> <p>Click the indicator to display the Configuration Issues pop-up dialog.</p> <p>By default only notifications at the Error severity level are listed, grouped by service name are shown in the dialog. To display Warning notifications, click the Also show <i>n</i> warning(s) link. Click the message associated with an error or warning to be taken to the configuration property for which the notification has been issued where you can address the issue. See Managing Services.</p>
 Restart Needed Refresh Needed	Configuration modified	<p>Indicates that at least one of a service's roles is running with a configuration that does not match the current configuration settings in Cloudera Manager.</p> <p>Click the indicator to display the Stale Configurations page. To bring the cluster up-to-date, click the Refresh or Restart button on the Stale Configurations page or follow the instructions in Refreshing a Cluster, Restarting a Cluster, or Restarting Services and Instances after Configuration Changes.</p>
	Client configuration redeployment required	<p>Indicates that the client configuration for a service should be redeployed.</p> <p>Click the indicator to display the Stale Configurations page. To bring the cluster up-to-date, click the Deploy Client Configuration button on the Stale Configurations page or follow the instructions in Manually Redeploying Client Configuration Files.</p>

- **Cloudera Management Service** - A table containing a link to the Cloudera Manager Service. The Cloudera Manager Service has a menu of actions that you select by clicking



- **Charts** - A set of charts ([dashboard](#)) that summarize resource utilization (IO, CPU usage) and processing metrics.

Click a line, stack area, scatter, or bar chart to expand it into a full-page view with a legend for the individual charted entities as well more fine-grained axes divisions.

By default the time scale of a dashboard is 30 minutes. To change the time scale, click a duration link

[30m](#) [1h](#) [2h](#) [6h](#) [12h](#) [1d](#) [7d](#) [30d](#) at the top-right of the dashboard.

To set the dashboard type, click



and select one of the following:

- **Custom** - displays a custom dashboard.
- **Default** - displays a default dashboard.
- **Reset** - resets the custom dashboard to the predefined set of charts, discarding any customizations.

All Health Issues

Displays all health issues by cluster. The number badge has the same semantics as the per service health issues reported on the Status tab.

- By default only Bad health test results are shown in the dialog. To display Concerning health test results, click the **Also show *n* concerning issue(s)** link.
- To group the health test results by entity or health test, click the buttons on the **Organize by Entity/Organize by Health Test** toggle.
- Click the link to display the Status page containing with details about the health test result.

All Configuration Issues

Displays all configuration issues by cluster. The number badge has the same semantics as the per service configuration issues reported on the Status tab. By default only notifications at the Error severity level are listed, grouped by service name are shown in the dialog. To display Warning notifications, click the **Also show *n* warning(s)** link. Click the message associated with an error or warning to be taken to the configuration property for which the notification has been issued where you can address the issue.

All Recent Commands

Displays all commands run recently across the clusters. A badge



indicates how many recent commands are still running. Click the command link to display details about the command and child commands. See also [Viewing Running and Recent Commands](#).

Displaying Cloudera Manager Documentation

To display Cloudera Manager documentation:

1. Open the Cloudera Manager Admin Console.
2. Select **Support > Help, Installation Guide, API Documentation, or Release Notes**. By default, the Help and Installation Guide files from the Cloudera web site are opened. This is because local help files are not updated after installation. You can configure Cloudera Manager to open either the latest Help and Installation Guide from the Cloudera web site (this option requires Internet access from the browser) or locally-installed Help and Installation Guide by configuring the **Administration > Settings > Support > Open latest Help files from the Cloudera website** property.

Displaying the Cloudera Manager Server Version and Server Time

To display the version, build number, and time for the Cloudera Manager Server:

1. Open the Cloudera Manager Admin Console.
2. Select **Support** > **About**.

Cloudera Manager API

The Cloudera Manager API provides configuration and service lifecycle management, service health information and metrics, and allows you to configure Cloudera Manager itself. The API is served on the same host and port as the [Cloudera Manager Admin Console](#) on page 29, and does not require an extra process or extra configuration. The API supports HTTP Basic Authentication, accepting the same users and credentials as the Cloudera Manager Admin Console.

Resources

- [Quick Start](#)
- [Cloudera Manager API tutorial](#)
- [Cloudera Manager API documentation](#)
- [Python client](#)
- [Using the Cloudera Manager Java API for Cluster Automation](#) on page 36

Obtaining Configuration Files

1. Obtain the list of a service's roles:

```
http://cm_server_host:7180/api/v10/clusters/clusterName/services/serviceName/roles
```

2. Obtain the list of configuration files a process is using:

```
http://cm_server_host:7180/api/v10/clusters/clusterName/services/serviceName/roles/roleName/process
```

3. Obtain the content of any particular file:

```
http://cm_server_host:7180/api/v10/clusters/clusterName/services/serviceName/roles/roleName/process/configFiles/configFileName
```

For example:

```
http://cm_server_host:7180/api/v10/clusters/Cluster%201/services/OOZIE-1/roles/OOZIE-1-OOZIE_SERVER-e121641328fcb107999f2b5fd856880d/process/configFiles/oozie-site.xml
```

Retrieving Service and Host Properties

To update a service property using the Cloudera Manager APIs, you'll need to know the name of the property, not just the display name. If you know the property's display name but not the property name itself, retrieve the documentation by requesting any configuration object with the query string `view=FULL` appended to the URL. For example:

```
http://cm_server_host:7180/api/v10/clusters/Cluster%201/services/service_name/config?view=FULL
```

Search the results for the display name of the desired property. For example, a search for the display name **HDFS Service Environment Advanced Configuration Snippet (Safety Valve)** shows that the corresponding property name is `hdfs_service_env_safety_valve`:

```
{
  "name" : "hdfs_service_env_safety_valve",
  "require" : false,
  "displayName" : "HDFS Service Environment Advanced Configuration Snippet (Safety
```

```

Valve)",
  "description" : "For advanced use only, key/value pairs (one on each line) to be
inserted into a roles
environment. Applies to configurations of all roles in this service except client
configuration.",
  "relatedName" : "",
  "validationState" : "OK"
}

```

Similar to finding service properties, you can also find host properties. First, get the host IDs for a cluster with the URL:

```
http://cm_server_host:7180/api/v10/hosts
```

This should return host objects of the form:

```

{
  "hostId" : "2c2e951c-aaf2-4780-a69f-0382181f1821",
  "ipAddress" : "10.30.195.116",
  "hostname" : "cm_server_host",
  "rackId" : "/default",
  "hostUrl" :
"http://cm_server_host:7180/cm/hosts/hostRedirect/2c2e951c-adf2-4780-a69f-0382181f1821",
  "maintenanceMode" : false,
  "maintenanceOwners" : [ ],
  "commissionState" : "COMMISSIONED",
  "numCores" : 4,
  "totalPhysMemBytes" : 10371174400
}

```

Then obtain the host properties by including one of the returned host IDs in the URL:

```
http://cm_server_host:7180/api/v10/hosts/2c2e951c-adf2-4780-a69f-0382181f1821?view=FULL
```

Backing Up and Restoring the Cloudera Manager Configuration

You can use the Cloudera Manager REST API to export and import all of its configuration data. The API exports a JSON document that contains configuration data for the Cloudera Manager instance. You can use this JSON document to back up and restore a Cloudera Manager deployment.

Minimum Required Role: [Cluster Administrator](#) (also provided by **Full Administrator**)

Exporting the Cloudera Manager Configuration

1. Log in to the Cloudera Manager server host as the `root` user.
2. Run the following command:

```
# curl -u admin_uname:admin_pass "http://cm_server_host:7180/api/v10/cm/deployment" >
path_to_file/cm-deployment.json
```

Where:

- `admin_uname` is a username with either the Full Administrator or Cluster Administrator role.
- `admin_pass` is the password for the `admin_uname` username.
- `cm_server_host` is the hostname of the Cloudera Manager server.
- `path_to_file` is the path to the file where you want to save the configuration.

Restoring the Cloudera Manager Configuration



Important: This feature is available only with a Cloudera Enterprise license; it is not available in Cloudera Express. For information on Cloudera Enterprise licenses, see [Managing Licenses](#).

Using a previously saved JSON document that contains the Cloudera Manager configuration data, you can restore that configuration to a running cluster.

1. Using the Cloudera Manager Administration Console, stop all running services in your cluster:

a. On the Home page, click



to the right of the cluster name and select **Stop**.

b. Click **Stop** in the confirmation screen. The **Command Details** window shows the progress of stopping services.

When **All services successfully stopped** appears, the task is complete and you can close the **Command Details** window.



Warning: If you do not stop the cluster before making this API call, the API call will stop *all* cluster services before running the job. Any running jobs and data are lost.

2. Log in to the Cloudera Manager server host as the `root` user.

3. Run the following command:

```
# curl --upload-file path_to_file/cm-deployment.json  
-u admin_username:admin_pass  
http://cm_server_host:7180/api/v10/cm/deployment?deleteCurrentDeployment=true
```

Where:

- *admin_username* is a username with either the Full Administrator or Cluster Administrator role.
- *admin_pass* is the password for the *admin_username* username.
- *cm_server_host* is the hostname of the Cloudera Manager server.
- *path_to_file* is the path to the file containing the JSON configuration file.

4. Restart the **Cloudera Manager Server**.

RHEL 7, SLES 12, Debian 8, Ubuntu 16.04

```
sudo systemctl restart cloudera-scm-server
```

RHEL 5 or 6, SLES 11, Debian 6 or 7, Ubuntu 12.04, 14.04

```
sudo service cloudera-scm-server restart
```

Using the Cloudera Manager Java API for Cluster Automation

One of the complexities of Apache Hadoop is the need to deploy clusters of servers, potentially on a regular basis. If you maintain hundreds of test and development clusters in different configurations, this process can be complex and cumbersome if not automated.

Cluster Automation Use Cases

Cluster automation is useful in various situations. For example, you might work on many versions of CDH, which works on a wide variety of OS distributions (RHEL 5 and RHEL 6, Ubuntu Precise and Lucid, Debian Wheezy, and SLES 11). You might have complex configuration combinations—highly available HDFS or simple HDFS, Kerberized or non-secure, YARN or MRv1, and so on. With these requirements, you need an easy way to create a new cluster that has the required setup. This cluster can also be used for integration, testing, customer support, demonstrations, and other purposes.

You can install and configure Hadoop according to precise specifications using the Cloudera Manager [REST API](#). Using the API, you can add hosts, install CDH, and define the cluster and its services. You can also tune heap sizes, set up HDFS HA, turn on Kerberos security and generate keytabs, and customize service directories and ports. Every configuration available in Cloudera Manager is exposed in the API.

The API also provides access to management functions:

- Obtaining logs and monitoring the system
- Starting and stopping services
- Polling cluster events
- Creating a disaster recovery replication schedule

For example, you can use the API to retrieve logs from HDFS, HBase, or any other service, without knowing the log locations. You can also stop any service with no additional steps.

Use scenarios for the Cloudera Manager API for cluster automation might include:

- OEM and hardware partners that deliver Hadoop-in-a-box appliances using the API to set up CDH and Cloudera Manager on bare metal in the factory.
- Automated deployment of new clusters, using a combination of Puppet and the Cloudera Manager API. Puppet does the OS-level provisioning and installs the software. The Cloudera Manager API sets up the Hadoop services and configures the cluster.
- Integrating the API with reporting and alerting infrastructure. An external script can poll the API for health and metrics information, as well as the stream of events and alerts, to feed into a custom dashboard.

Java API Examples

This example covers the Java API client.

To use the Java client, add this dependency to your project's `pom.xml`:

```
<project>
  <repositories>
    <repository>
      <id>cdh.repo</id>
      <url>https://repository.cloudera.com/groups/cloudera-repos</url>
      <name>Cloudera Repository</name>
    </repository>
    ...
  </repositories>
  <dependencies>
    <dependency>
      <groupId>com.cloudera.api</groupId>
      <artifactId>cloudera-manager-api</artifactId>
      <version>4.6.2</version>      <!-- Set to the version of Cloudera Manager you use -->
    </dependency>
    ...
  </dependencies>
  ...
</project>
```

The Java client works like a proxy. It hides from the caller any details about REST, HTTP, and JSON. The entry point is a handle to the root of the API:

```
RootResourceV10 apiRoot = new ClouderaManagerClientBuilder().withHost("cm.cloudera.com")
    .withUsernamePassword("admin", "admin").build().getRootV10();
```

From the root, you can traverse down to all other resources. (It's called "v10" because that is the current Cloudera Manager API version, but the same builder will also return a root from an earlier version of the API.) The tree view shows some key resources and supported operations:

- RootResourceV10
 - ClustersResourceV10 - host membership, start cluster
 - ServicesResourceV10 - configuration, get metrics, HA, service commands
 - RolesResource - add roles, get metrics, logs
 - RoleConfigGroupsResource - configuration

– `ParcelsResource` - parcel management

- `HostsResource` - host management, get metrics
- `UsersResource` - user management

For more information, see the [Javadoc](#).

The following example lists and starts a cluster:

```
// List of clusters
ApiClientList clusters = apiRoot.getClustersResource().readClusters(DataView.SUMMARY);
for (ApiClient cluster : clusters) {
    LOG.info("{}: {}", cluster.getName(), cluster.getVersion());
}

// Start the first cluster
ApiClient cmd = apiRoot.getClustersResource().startCommand(clusters.get(0).getName());
while (cmd.isActive()) {
    Thread.sleep(100);
    cmd = apiRoot.getCommandsResource().readCommand(cmd.getId());
}
LOG.info("Cluster start {}", cmd.getSuccess() ? "succeeded" : "failed " +
cmd.getResultMessage());
```

To see a full example of cluster deployment using the Java client, see [whirr-cm](#). Go to `CmServerImpl#configure` to see the relevant code.

Extending Cloudera Manager

In addition to the set of software packages and services managed by Cloudera Manager, you can also define and add new types of services using [custom service descriptors](#). When you deploy a custom service descriptor, the implementation is delivered in a Cloudera Manager [parcel](#) or other software package. For information on the extension mechanisms provided by Cloudera Manager for creating custom service descriptors and parcels, see [Cloudera Manager Extensions](#).

Cloudera Manager 5 Frequently Asked Questions

This guide answers frequently asked questions about Cloudera Manager.

General Questions

What are the new features of Cloudera Manager 5?

For a list of new features in Cloudera Manager 5, see [New Features and Changes in Cloudera Manager 5](#).

What operating systems are supported?

See [Supported Operating Systems](#) for more detailed information on which operating systems are supported.

What databases are supported?

See [Supported Databases](#) for more detailed information on which database systems are supported.

What version of CDH is supported for Cloudera Manager 5?

See [Supported CDH and Managed Service Versions](#) for detailed information.

What are the differences between the Cloudera Express and the Cloudera Enterprise versions of Cloudera Manager?

Cloudera Express includes a free version of Cloudera Manager. The Cloudera Enterprise version of Cloudera Manager provides additional functionality. Both the Cloudera Express and Cloudera Enterprise versions automate the installation,

configuration, and monitoring of CDH 4 or CDH 5 on an entire cluster. See the matrix at [Cloudera Express and Cloudera Enterprise Features](#) for a comparison of the two versions.

The Cloudera Enterprise version of Cloudera Manager is available as part of the Cloudera Enterprise subscription offering, and requires a license. You can also choose a Cloudera Enterprise Data Hub Edition Trial that is valid for 60 days.

If you are not an existing Cloudera customer, contact Cloudera Sales using this [form](#) or call 866-843-7207 to obtain a Cloudera Enterprise license. If you are already a Cloudera customer and you need to upgrade from Cloudera Express to Cloudera Enterprise, contact [Cloudera Support](#) to obtain a license.

Are there different types of Cloudera Enterprise licenses?

There are three editions of Cloudera Enterprise which enable you to manage clusters of the following services:

- **Basic Edition** - a cluster running core CDH services: HDFS, Hive, Hue, MapReduce, Oozie, Sqoop, YARN, and ZooKeeper.
- **Flex Edition** - a cluster running core CDH services plus one of the following: Accumulo, HBase, Impala, Navigator, Solr, Spark.
- **Data Hub Edition** - a cluster running core CDH services plus any of the following: Accumulo, HBase, Impala, Navigator, Solr, Spark.

Can I upgrade CDH using Cloudera Manager?

You can upgrade to CDH 4.1.2 or later from within the Cloudera Manager Admin Console using parcels. Furthermore, once you have installed or upgraded CDH using parcels, you can perform rolling upgrades on your CDH services. If you have HDFS High Availability configured and enabled, you can perform a rolling upgrade on your cluster without taking the entire cluster down.



Warning:

- Cloudera Manager 4 and CDH 4 have reached End of Maintenance (EOM) on August 9, 2015. Cloudera does not support or provide patches for Cloudera Manager 4 and CDH 4 releases.
- Cloudera Manager 3 and CDH 3 have reached End of Maintenance (EOM) on June 20, 2013. Cloudera does not support or provide patches for Cloudera Manager 3 and CDH 3 releases.

What version of CDH does Cloudera Manager 5 install?

Cloudera Manager 5 allows you to install any version of CDH 4 or CDH 5.

Where are CDH libraries located when I distribute CDH using parcels?

With parcel software distribution, the path to the CDH libraries is `/opt/cloudera/parcels/CDH/lib/` instead of the usual `/usr/lib/`.

What upgrade paths are available for Cloudera Manager, and what's involved?

For instructions about upgrading, see [Upgrading Cloudera Manager](#).

How do I install Cloudera Manager 5 in a walled-off environment (no Internet access)?

You can set up a local repository and use it in the installer. For instructions, see [Understanding Custom Installation Solutions](#).

Do worker hosts need access to the Cloudera public repositories for an install with Cloudera Manager?

You can perform an installation or upgrade using the parcel format and when using parcels, only the Cloudera Manager Server requires access to the Cloudera public repositories. Distribution of the parcels to worker hosts is done between

Cloudera Manager 5 Overview

the Cloudera Manager Server and the worker hosts. See [Parcels](#) for more information. If you want to install using the traditional packages, hosts only require access to the installation files.

For both parcels and packages, it is also possible to create local repositories that serve these files to the hosts that are being upgraded. If you have established local repositories, no access to the Cloudera public repository is required. For more information, see [Creating and Using a Package Repository for Cloudera Manager](#).

Can I use the service monitoring features of Cloudera Manager without the Cloudera Management Service?

No. To understand the desired state of the system, Cloudera Manager requires the global configuration that the Cloudera Management Service roles gather and provide. The Cloudera Manager Agent doubles as both the agent for supervision and for monitoring.

Can I run the Cloudera Management Service and the Hadoop services on the host where the Cloudera Manager Server is running?

Yes. This is especially common in deployments that have a small number of hosts.

Does Cloudera Manager Support an API?

Yes. A comprehensive set of APIs for the various features is supported in this version of Cloudera Manager. For more information about the Cloudera Manager API, see [Cloudera Manager API](#) on page 34. You can download this [Cloudera Manager API example](#) that shows how to integrate with Nagios or other systems.

Cloudera Navigator 2 Overview

Cloudera Navigator is a fully integrated data management and security tool for the Hadoop platform. Data management and security capabilities are critical for enterprise customers that are in highly regulated industries and have stringent compliance requirements.

Cloudera Navigator provides three categories of functionality:

- **Auditing data access and verifying access privileges** - The goal of auditing is to capture a complete and immutable record of all activity within a system. While Hadoop has historically lacked centralized cross-component audit capabilities, products such as Cloudera Navigator add secured, real-time audit components to key data and access frameworks. Cloudera Navigator allows administrators to configure, collect, and view audit events, to understand who accessed what data and how. Cloudera Navigator also allows administrators to generate reports that list the HDFS access permissions granted to groups.

Cloudera Navigator tracks access permissions and actual accesses to all entities in HDFS, Hive, HBase, Impala, Sentry, and Solr, and the Cloudera Navigator Metadata Server itself to help answer questions such as - who has access to which entities, which entities were accessed by a user, when was an entity accessed and by whom, what entities were accessed using a service, which device was used to access, and so on. Cloudera Navigator auditing supports tracking access to:

- HDFS entities accessed by HDFS, Hive, HBase, Impala, and Solr services
 - HBase and Impala
 - Hive metadata
 - Sentry
 - Solr
 - Cloudera Navigator Metadata Server
- **Searching metadata and visualizing lineage** - Cloudera Navigator metadata management features allow DBAs, data modelers, business analysts, and data scientists to search for, amend the properties of, and tag data entities.

In addition, to satisfy risk and compliance audits and data retention policies, it supports the ability to answer questions such as: where did the data come from, where is it used, and what are the consequences of purging or modifying a set of data entities. Cloudera Navigator supports tracking the lineage of HDFS files, datasets, and directories, Hive tables and columns, MapReduce and YARN jobs, Hive queries, Impala queries, Pig scripts, Oozie workflows, Spark jobs, and Sqoop jobs.

- **Securing data and simplifying storage and management of encryption keys** - Data encryption and key management provide a critical layer of protection against potential threats by malicious actors on the network or in the data center. It is also a requirement for meeting key compliance initiatives and ensuring the integrity of your enterprise data.

The following Cloudera Navigator components enable compliance initiatives that require at-rest data encryption and key management:

- [Cloudera Navigator Key Trustee Server](#) is an enterprise-grade virtual safe-deposit box that stores and manages cryptographic keys and other security artifacts.
- [Cloudera Navigator Key HSM](#) allows Cloudera Navigator Key Trustee Server to seamlessly integrate with a hardware security module (HSM).
- [Cloudera Navigator Encrypt](#) transparently encrypts and secures data at rest without requiring changes to your applications and ensures there is minimal performance lag in the encryption or decryption process.

Related Information

- [Installing the Cloudera Navigator Data Management Component](#)
- [Upgrading the Cloudera Navigator Data Management Component](#)
- [Cloudera Navigator Data Management Component Administration](#)

- [Cloudera Data Management](#)
- [Encryption](#)
- [Configuring Authentication in the Cloudera Navigator Data Management Component](#)
- [Configuring SSL for the Cloudera Navigator Data Management Component](#)
- [Cloudera Navigator Data Management Component User Roles](#)

Cloudera Navigator Data Management Component Overview

The section describes basic features of the Cloudera Navigator data management component.

Cloudera Navigator Data Management Component UI

The Cloudera Navigator data management component UI is the web-based UI that you use to:

- Create and view audit reports
- Search entity metadata, view entity lineage, and modify business metadata
- Define policies for modifying custom metadata when entities are extracted
- Assign user roles to groups

Navigator auditing, lineage, metadata, and policies all support multi-cluster deployments that are managed by a single Cloudera Manager instance. So if you have five clusters, all centrally managed by a single Cloudera Manager, you'll see all this information within a single Navigator data management component UI. In the metadata portion of the UI, Navigator also tracks the specific cluster the data comes from with the Cluster technical metadata property.

Starting and Logging into the Cloudera Navigator Data Management Component UI

1. Do one of the following:


- Enter the URL of the Navigator UI in a browser: `http://Navigator_Metadata_Server_host:port/`, where *Navigator_Metadata_Server_host* is the name of the host on which you are running the Navigator Metadata Server role and *port* is the port configured for the role. The default port of the Navigator Metadata Server is 7187. To change the port, follow the instructions in [Configuring the Navigator Metadata Server Port](#).
- Do one of the following:
 - Select **Clusters > Cloudera Management Service > Cloudera Navigator**.
 - Navigate from the Navigator Metadata Server role:
 1. Do one of the following:
 - Select **Clusters > Cloudera Management Service > Cloudera Management Service**.
 - On the Status tab of the Home page, in **Cloudera Management Service** table, click the **Cloudera Management Service** link.
 2. Click the **Instances** tab.
 3. Click the **Navigator Metadata Server** role.
 4. Click the **Navigator Web UI** link.

2. Log into Cloudera Navigator UI using the [credentials](#) assigned by your administrator.

Cloudera Navigator Data Management Component API

The Cloudera Navigator data management component API provides access to the same features as the UI.

The API available at `http://Navigator_Metadata_Server_host:port/api/v7`, where *Navigator_Metadata_Server_host* is the name of the host on which you are running the Navigator Metadata Server role and *port* is the port configured for the role. The default port of the Navigator Metadata Server is 7187. To change the port, follow the instructions in [Configuring the Navigator Metadata Server Port](#). The API supports HTTP Basic Authentication, accepting the same users and credentials as the UI.

For API documentation, select  > **API Documentation** or go to `Navigator_Metadata_Server_host:port/api-console/index.html`. The Cloudera Navigator API documentation displays in a new window.


Displaying the Cloudera Navigator Data Management Component Version

To display the version and build number for Cloudera Navigator data management component:

1. [Start and log into the Cloudera Navigator data management component UI](#).
2. Select  > **About**.

Displaying Cloudera Navigator Data Management Component Documentation

To display Cloudera Navigator data management component documentation:

1. [Start and log into the Cloudera Navigator data management component UI](#).
2. Select  > **Help**. The Cloudera Navigator online documentation displays in a new window.

Cloudera Navigator 2 Frequently Asked Questions

Is Cloudera Navigator a module of Cloudera Manager?

Cloudera Navigator sits side-by-side with and complements Cloudera Manager. What Cloudera Manager is to managing services, Cloudera Navigator is to managing all the data stored in those services. Cloudera Navigator provides three categories of functionality:

- Auditing data access and verifying access privileges - The goal of auditing is to capture a complete and immutable record of all activity within a system. While Hadoop has historically lacked centralized cross-component audit capabilities, products such as Cloudera Navigator add secured, real-time audit components to key data and access frameworks. Cloudera Navigator allows administrators to configure, collect, and view audit events, to understand who accessed what data and how. Cloudera Navigator also allows administrators to generate reports that list the HDFS access permissions granted to groups.
- Searching metadata and visualizing lineage - Cloudera Navigator metadata management features allow DBAs, data modelers, business analysts, and data scientists to search for, amend the properties of, and tag data entities.
- Securing data and simplifying storage and management of encryption keys - Data encryption and key management provide a critical layer of protection against potential threats by malicious actors on the network or in the data center. It is also a requirement for meeting key compliance initiatives and ensuring the integrity of your enterprise data.

The Cloudera Navigator data management component is implemented as two roles in the [Cloudera Management Service](#): Navigator Audit Server and Navigator Metadata Server. You can add Cloudera Navigator data management roles while installing Cloudera Manager for the first time or into an existing Cloudera Manager installation. For information on compatible Cloudera Navigator and Cloudera Manager versions, see the [Product Compatibility Matrix for Cloudera Navigator](#) product compatibility matrix.

Cloudera Navigator encryption is implemented as three services:

- [Cloudera Navigator Key Trustee Server](#) is an enterprise-grade virtual safe-deposit box that stores and manages cryptographic keys and other security artifacts.
- [Cloudera Navigator Key HSM](#) allows Cloudera Navigator Key Trustee Server to seamlessly integrate with a hardware security module (HSM).
- [Cloudera Navigator Encrypt](#) transparently encrypts and secures data at rest without requiring changes to your applications and ensures there is minimal performance lag in the encryption or decryption process.

Cloudera Navigator 2 Overview

Is Cloudera Navigator included with a Cloudera Enterprise Data Hub Edition license?

Yes. Cloudera Navigator is included with Cloudera Enterprise Data Hub Edition license and can be selected as a choice with a Cloudera Enterprise Flex Edition license.

Can Cloudera Navigator be purchased standalone, that is, without Cloudera Manager?

Cloudera Navigator components are managed by Cloudera Manager. Therefore, Cloudera Manager is a prerequisite for Cloudera Navigator.

What Cloudera Manager, CDH, and Cloudera Impala releases does Cloudera Navigator 2 work with?

See [Cloudera Navigator 2 Requirements and Supported Versions](#).

Is Cloudera Navigator open source or closed source?

Cloudera Navigator is a closed-source management tool that adds to the Cloudera suite of management capabilities for Hadoop.

How are Cloudera Navigator logs different from Cloudera Manager logs?

Cloudera Navigator tracks and aggregates only the accesses to the data stored in CDH services and used for audit reports and analysis. Cloudera Manager monitors and logs all the activity performed by CDH services that helps administrators maintain the health of the cluster. The target audiences of these logs are different but together they provide better visibility into both the data access and system activity for an enterprise cluster.

Cloudera Navigator Data Encryption Overview



Warning: Encryption transforms coherent data into random, unrecognizable information for unauthorized users. It is *absolutely critical* that you follow the documented procedures for encrypting and decrypting data, and that you regularly back up the encryption keys and configuration files. Failure to do so can result in irretrievable data loss. See [Backing Up and Restoring Key Trustee Server](#) for more information.

Do not attempt to perform any operations that you do not understand. If you have any questions about a procedure, contact Cloudera Support before proceeding.

Cloudera Navigator includes a turnkey encryption and key management solution for data at rest, whether data is stored in HDFS or on the local Linux filesystem. Cloudera Navigator encryption comprises the following components:

- [Cloudera Navigator Key Trustee Server](#)

Key Trustee Server is an enterprise-grade virtual safe-deposit box that stores and manages cryptographic keys. With Key Trustee Server, encryption keys are separated from the encrypted data, ensuring that sensitive data is protected in the event that unauthorized users gain access to the storage media.

- [Cloudera Navigator Key HSM](#)

Key HSM is a service that allows Key Trustee Server to integrate with a hardware security module (HSM). Key HSM enables Key Trustee Server to use an HSM as the root of trust for cryptographic keys, taking advantage of Key Trustee Server's policy-based key and security asset management capabilities while satisfying existing internal security requirements regarding treatment of cryptographic materials.

- [Cloudera Navigator Encrypt](#)

Navigator Encrypt is a client-side service that transparently encrypts data at rest without requiring changes to your applications and with minimal performance lag in the encryption or decryption process. Advanced key management with Key Trustee Server and process-based access controls in Navigator Encrypt enable organizations to meet compliance regulations and ensure unauthorized parties or malicious actors never gain access to encrypted data.

- Key Trustee KMS

For [HDFS Data At Rest Encryption](#), Cloudera provides Key Trustee KMS, a customized [Key Management Server](#) that uses Key Trustee Server for robust and scalable encryption key storage and management instead of the file-based Java KeyStore used by the default Hadoop KMS.

Cloudera Navigator encryption provides:

- High-performance transparent data encryption for files, databases, and applications running on Linux
- Separation of cryptographic keys from encrypted data
- Centralized management of cryptographic keys
- Integration with hardware security modules (HSMs) from Thales and SafeNet
- Support for Intel AES-NI cryptographic accelerator for enhanced performance in the encryption and decryption process
- Process-Based Access Controls

Cloudera Navigator encryption can be deployed to protect different assets, including (but not limited to):

- Databases
- Log files
- Temporary files
- Spill files

Cloudera Navigator Data Encryption Overview

- HDFS data

For planning and deployment purposes, this can be simplified to two types of data that Cloudera Navigator encryption can secure:

1. HDFS data
2. Local filesystem data

The following table outlines some common use cases and identifies the services required.

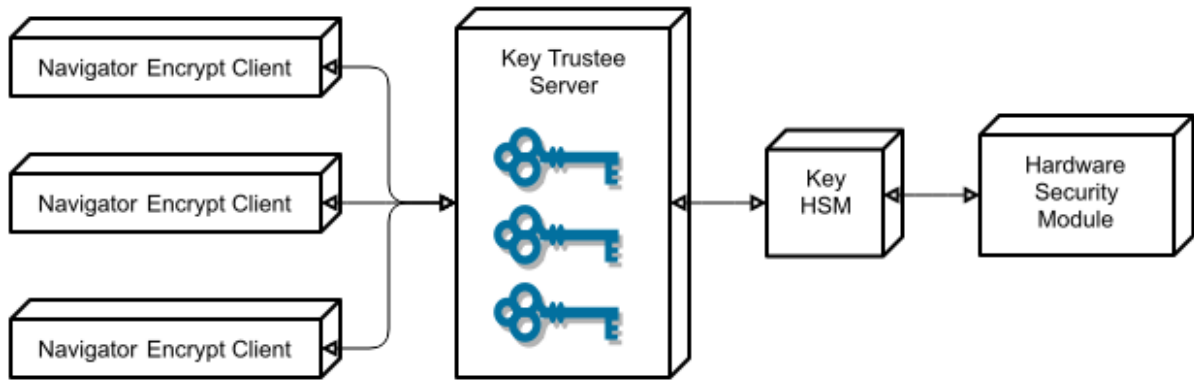
Table 2: Encrypting Data at Rest

Data Type	Data Location	Key Management	Additional Services Required
HDFS	HDFS	Key Trustee Server	Key Trustee KMS
Metadata databases, including: <ul style="list-style-type: none">• Hive Metastore• Cloudera Manager• Cloudera Navigator Data Management• Sentry	Local filesystem	Key Trustee Server	Navigator Encrypt
Temp/spill files for CDH components with native encryption: <ul style="list-style-type: none">• Impala• YARN• MapReduce• Flume• HBase• Accumulo	Local filesystem	N/A (temporary keys are stored in memory only)	None (enable native temp/spill encryption for each component)
Temp/spill files for CDH components without native encryption: <ul style="list-style-type: none">• Spark• Kafka• Sqoop2• HiveServer2	Local filesystem	Key Trustee Server	Navigator Encrypt
Log files	Local filesystem	Key Trustee Server	Navigator Encrypt Log Redaction

For instructions on using Navigator Encrypt to secure local filesystem data, see [Cloudera Navigator Encrypt](#).

Cloudera Navigator Encryption Architecture

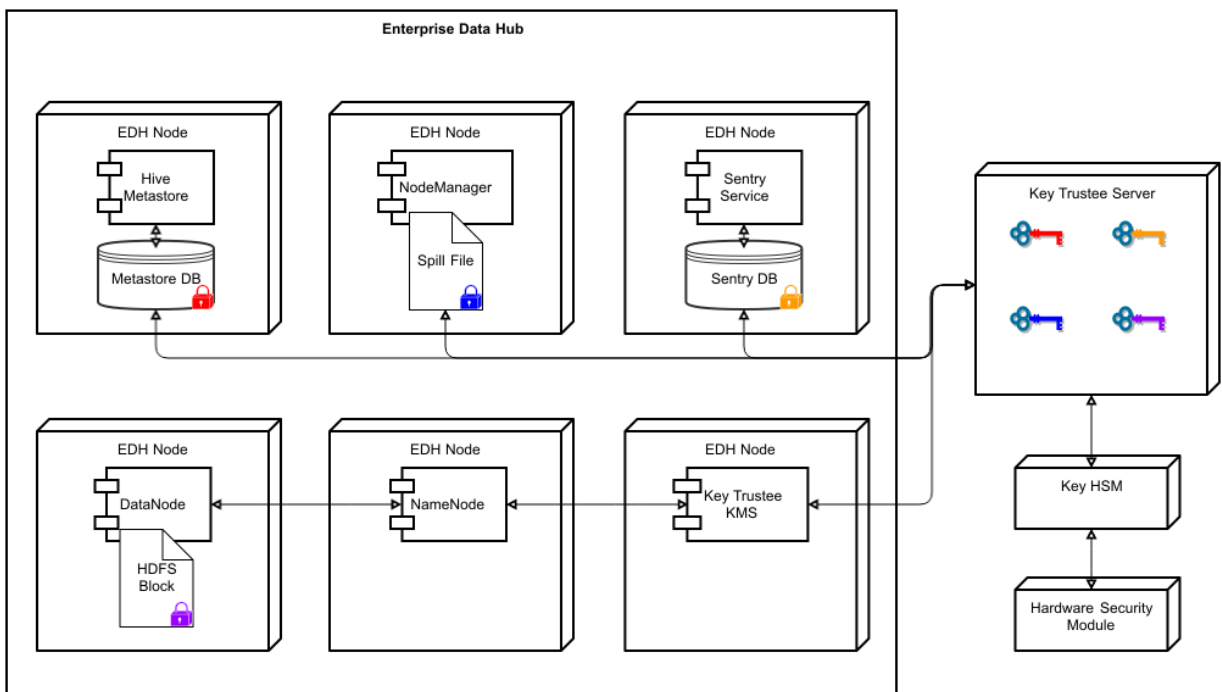
The following diagram illustrates how the Cloudera Navigator encryption components interact with each other:



Key Trustee clients include Navigator Encrypt and Key Trustee KMS. Encryption keys are created by the client and stored in Key Trustee Server.

Cloudera Navigator Encryption Integration with an EDH

The following diagram illustrates how the Cloudera Navigator encryption components integrate with an Enterprise Data Hub (EDH):



For more details on the individual components of Cloudera Navigator encryption, continue reading:

Cloudera Navigator Key Trustee Server Overview

Cloudera Navigator Key Trustee Server is an enterprise-grade virtual safe-deposit box that stores and manages cryptographic keys and other security artifacts. With Navigator Key Trustee Server, encryption keys are separated from the encrypted data, ensuring that sensitive data is still protected if unauthorized users gain access to the storage media.

Cloudera Navigator Data Encryption Overview

Key Trustee Server protects these keys and other critical security objects from unauthorized access while enabling compliance with strict data security regulations. For added security, Key Trustee Server can integrate with a [hardware security module \(HSM\)](#). See [Cloudera Navigator Key HSM Overview](#) on page 48 for more information.

In conjunction with the Key Trustee KMS, Navigator Key Trustee Server can serve as a backing key store for [HDFS Data At Rest Encryption](#), providing enhanced security and scalability over the file-based Java KeyStore used by the default Hadoop Key Management Server.

Cloudera Navigator Encrypt also uses Key Trustee Server for key storage and management.

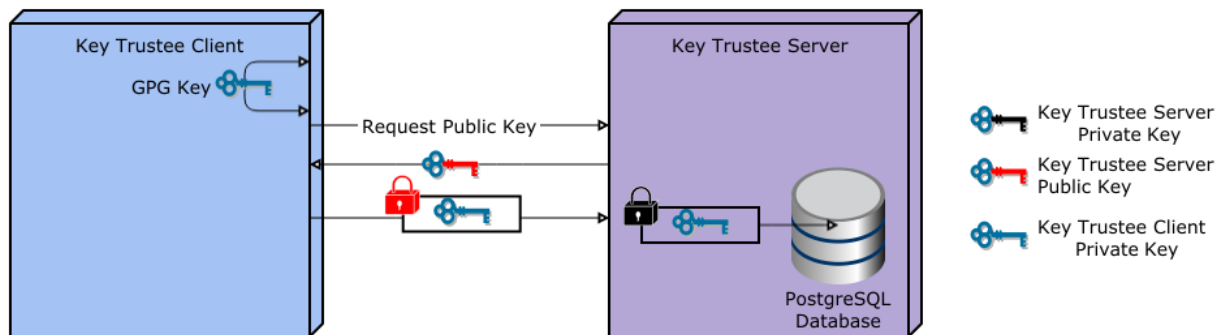
For instructions on installing Navigator Key Trustee Server, see [Installing Cloudera Navigator Key Trustee Server](#). For instructions on configuring Navigator Key Trustee Server, see [Initializing Standalone Key Trustee Server](#) or [Cloudera Navigator Key Trustee Server High Availability](#).

Key Trustee Server Architecture

Key Trustee Server is a secure object store. Clients register with Key Trustee Server, and are then able to store and retrieve objects with Key Trustee Server. The most common use case for Key Trustee Server is storing encryption keys to simplify key management and enable compliance with various data security regulations, but Key Trustee Server is agnostic about the actual objects being stored.

All interactions with Key Trustee Server occur over a TLS-encrypted HTTPS connection.

Key Trustee Server does not generate encryption keys for clients. Clients generate encryption keys, encrypt them with their private key, and send them over a TLS-encrypted connection to the Key Trustee Server. When a client needs to decrypt data, it retrieves the appropriate encryption key from Key Trustee Server and caches it locally to improve performance. This process is demonstrated in the following diagram:



The most common Key Trustee Server clients are Navigator Encrypt and Key Trustee KMS.

When a Key Trustee client registers with Key Trustee Server, it generates a unique fingerprint. All client interactions with the Key Trustee Server are authenticated with this fingerprint. You must ensure that the file containing this fingerprint is secured with appropriate Linux file permissions. The file containing the fingerprint is

`/etc/navencrypt/keytrustee/ztrustee.conf` for Navigator Encrypt clients, and

`/var/lib/kms-keytrustee/keytrustee/.keytrustee/keytrustee.conf` for Key Trustee KMS.

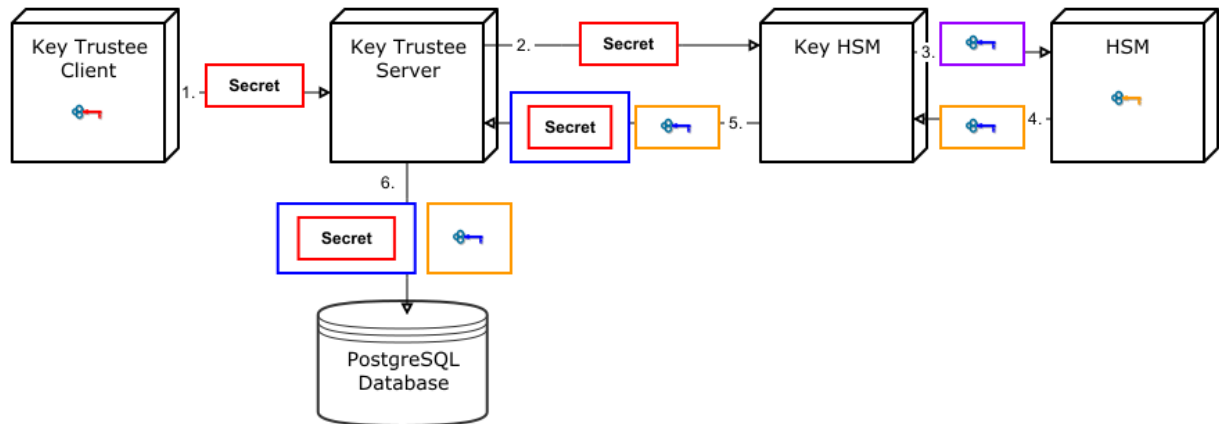
Many clients can use the same Key Trustee Server to manage security objects. For example, you can have several Navigator Encrypt clients using a Key Trustee Server, and also use the same Key Trustee Server as the backing store for Key Trustee KMS (used in HDFS encryption).

Cloudera Navigator Key HSM Overview

Cloudera Navigator Key HSM allows Cloudera Navigator Key Trustee Server to seamlessly integrate with a hardware security module (HSM). Key HSM enables Key Trustee Server to use an HSM as a root of trust for cryptographic keys, taking advantage of Key Trustee Server's policy-based key and security asset management capabilities while satisfying existing, internal security requirements for treatment of cryptographic materials.

Key HSM adds an additional layer of encryption to Key Trustee Server deposits, and acts as a root of trust. If a key is revoked on the HSM, any Key Trustee Server deposits encrypted with that key are rendered irretrievable.

The following diagram demonstrates the flow of storing a deposit in Key Trustee Server when Key HSM is used:



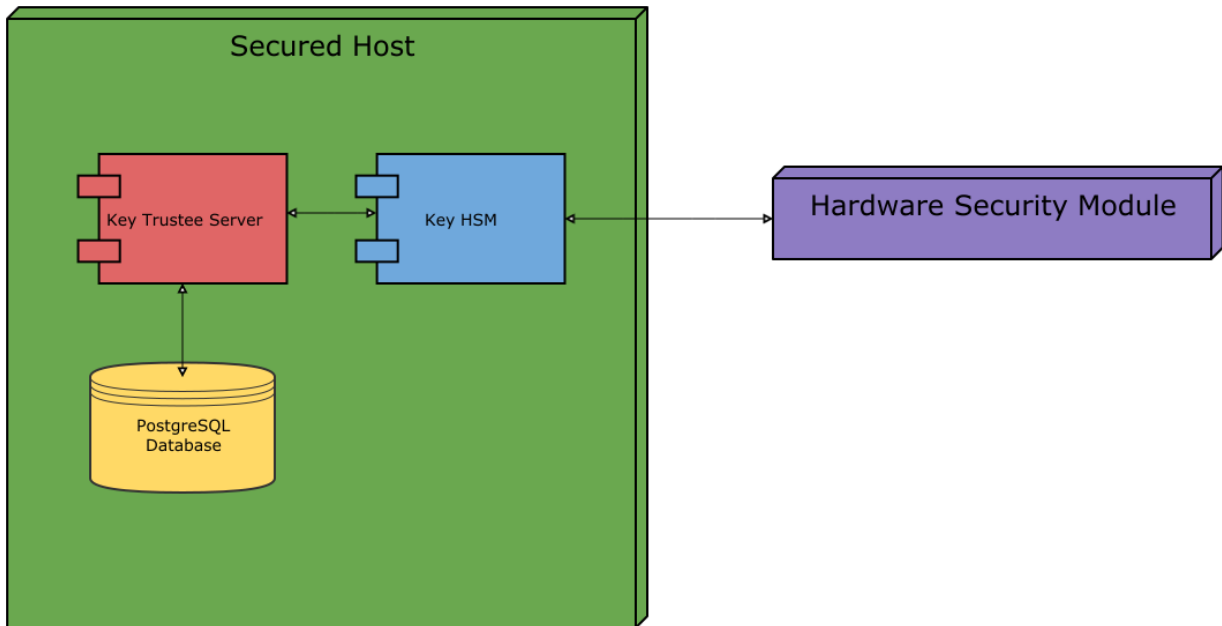
1. A Key Trustee client (for example, Navigator Encrypt or Key Trustee KMS) sends an encrypted secret to Key Trustee Server.
2. Key Trustee Server forwards the encrypted secret to Key HSM.
3. Key HSM generates a symmetric encryption key and sends it to the HSM over an encrypted channel.
4. The HSM generates a new key pair and encrypts the symmetric key and returns the encrypted symmetric key to Key HSM.
5. Key HSM encrypts the original client-encrypted secret with the symmetric key, and returns the twice-encrypted secret, along with the encrypted symmetric key, to Key Trustee Server. Key HSM discards its copy of the symmetric key.
6. Key Trustee Server stores the twice-encrypted secret along with the encrypted symmetric key in its PostgreSQL database.

The only way to retrieve the original encrypted secret is for Key HSM to request the HSM to decrypt the encrypted symmetric key, which is required to decrypt the twice-encrypted secret. If the key has been revoked on the HSM, it is not possible to retrieve the original secret.

Key HSM Architecture

For increased security, Key HSM should always be installed on the same host running the Key Trustee Server. This reduces the attack surface of the system by ensuring that communication between Key Trustee Server and Key HSM stays on the same host, and never has to traverse a network segment.

The following diagram displays the recommended architecture for Key HSM:



For instructions on installing Navigator Key HSM, see [Installing Cloudera Navigator Key HSM](#). For instructions on configuring Navigator Key HSM, see [Initializing Navigator Key HSM](#).

Cloudera Navigator Encrypt Overview

Cloudera Navigator Encrypt transparently encrypts and secures data at rest without requiring changes to your applications and ensures minimal performance lag in the encryption or decryption process. Advanced key management with [Cloudera Navigator Key Trustee Server](#) and process-based access controls in Navigator Encrypt enable organizations to meet compliance regulations and prevent unauthorized parties or malicious actors from gaining access to encrypted data.

For instructions on installing Navigator Encrypt, see [Installing Cloudera Navigator Encrypt](#). For instructions on configuring Navigator Encrypt, see [Registering Navigator Encrypt with Key Trustee Server](#).

Navigator Encrypt features include:

- Automatic key management: Encryption keys are stored in Key Trustee Server to separate the keys from the encrypted data. If the encrypted data is compromised, it is useless without the encryption key.
- Transparent encryption and decryption: Protected data is encrypted and decrypted seamlessly, with minimal performance impact and no modification to the software accessing the data.
- Process-based access controls: Processes are authorized individually to access encrypted data. If the process is modified in any way, access is denied, preventing malicious users from using customized application binaries to bypass the access control.
- Performance: Navigator Encrypt supports the Intel AES-NI cryptographic accelerator for enhanced performance in the encryption and decryption process.
- Compliance: Navigator Encrypt enables you to comply with requirements for HIPAA-HITECH, PCI-DSS, FISMA, EU Data Protection Directive, and other data security regulations.
- Multi-distribution support: Navigator Encrypt supports Debian, Ubuntu, RHEL, CentOS, and SLES.
- Simple installation: Navigator Encrypt is distributed as RPM and DEB packages, as well as SLES KMPs.
- Multiple mountpoints: You can separate data into different mountpoints, each with its own encryption key.

Navigator Encrypt can be used with many kinds of data, including (but not limited to):

- Databases
- Temporary files (YARN containers, spill files, etc.)

- Log files
- Data directories
- Configuration files

Navigator Encrypt uses `dmccrypt` for its underlying cryptographic operations. Navigator Encrypt uses several different encryption keys:

- **Master Key:** The master key can be a single passphrase, dual passphrase, or RSA key file. The master key is stored in Key Trustee Server and cached locally. This key is used when registering with a Key Trustee Server and when performing administrative functions on Navigator Encrypt clients.
- **Mount Encrypt Key (MEK):** This key is generated by Navigator Encrypt using `openssl rand` by default, but it can alternatively use `/dev/urandom`. This key is generated when preparing a new mount point. Each mount point has its own MEK. This key is uploaded to Key Trustee Server.
- **`dmccrypt` Device Encryption Key (DEK):** This key is not managed by Navigator Encrypt or Key Trustee Server. It is managed locally by `dmccrypt` and stored in the header of the device.

Process-Based Access Control List

The access control list (ACL) controls access to specified data. The ACL uses a process fingerprint, which is the SHA256 hash of the process binary, for authentication. You can create rules to allow a process to access specific files or directories. The ACL file is encrypted with the client master key and stored locally for quick access and updates.

Here is an example rule:

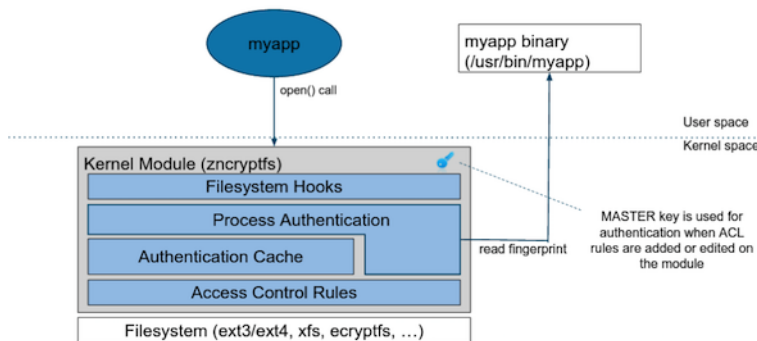
```
"ALLOW @mydata * /usr/bin/myapp"
```

This rule allows the `/usr/bin/myapp` process to access any encrypted path (*) that was encrypted under the category `@mydata`.

Navigator Encrypt uses a kernel module that intercepts any input/output (I/O) sent to an encrypted and managed path. The Linux module filename is `zncryptfs.ko` and it resides in the kernel stack, injecting filesystem hooks. It also authenticates and authorizes processes and caches authentication results for increased performance.

Because the kernel module intercepts and does not modify I/O, it supports any filesystem (`ext3`, `ext4`, `xfs`, etc.).

The following diagram shows `/usr/bin/myapp` sending an `open()` call that is intercepted by `zncrypt-kernel-module` as an `open` hook:

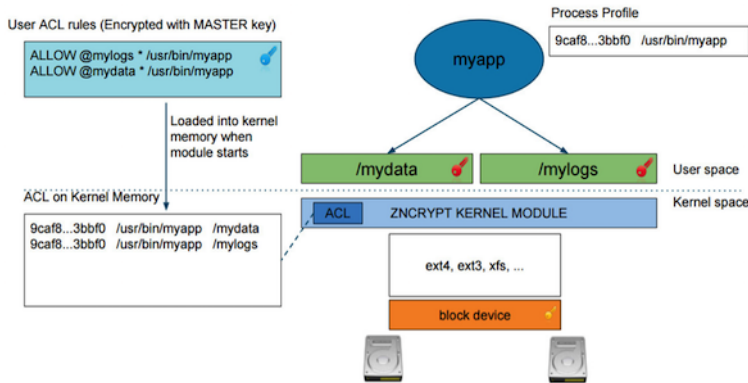


The kernel module calculates the process fingerprint. If the authentication cache already has the fingerprint, the process is allowed to access the data. If the fingerprint is not in the cache, the fingerprint is checked against the ACL. If the ACL grants access, the fingerprint is added to the authentication cache, and the process is permitted to access the data.

When you add an ACL rule, you are prompted for the master key. If the rule is accepted, the ACL rules file is updated as well as the `zncrypt-kernel-module` ACL cache.

The next diagram illustrates different aspects of Navigator Encrypt:

Cloudera Navigator Data Encryption Overview



The user adds a rule to allow `/usr/bin/myapp` to access the encrypted data in the category `@mylogs`, and adds another rule to allow `/usr/bin/myapp` to access encrypted data in the category `@mydata`. These two rules are loaded into the `zncrypt-kernel-module` cache after restarting the kernel module.

The `/mydata` directory is encrypted under the `@mydata` category and `/mylogs` is encrypted under the `@mylogs` category using `dmccrypt` (block device encryption).

When `myapp` tries to issue I/O to an encrypted directory, the kernel module calculates the fingerprint of the process (`/usr/bin/myapp`) and compares it with the list of authorized fingerprints in the cache.

Encryption Key Storage and Management

The master key and mount encryption keys are securely deposited in Key Trustee Server. One MEK per mount point is stored locally for offline recovery and rapid access. The locally-stored MEKs are encrypted with the master key.

The connection between Navigator Encrypt and Key Trustee Server is secured with TLS/SSL certificates.

The following diagram demonstrates the communication process between Navigator Encrypt and Key Trustee Server:



The master key is encrypted with a local GPG key. Before being stored in the Key Trustee Server database, it is encrypted again with the Key Trustee Server GPG key. When the master key is needed to perform a Navigator Encrypt operation, Key Trustee Server decrypts the stored key with its server GPG key and sends it back to the client (in this case, Navigator Encrypt), which decrypts the deposit with the local GPG key.

All communication occurs over TLS-encrypted connections.

Frequently Asked Questions About Cloudera Software

The following topics contain frequently asked questions about components and subsystems of the Cloudera Enterprise product:

- [Cloudera Manager 5 Frequently Asked Questions](#)
- [Cloudera Navigator Frequently Asked Questions](#)
- [Impala Frequently Asked Questions](#)
- [Cloudera Search Frequently Asked Questions](#)

Getting Support

This section describes how to get support.

Cloudera Support

Cloudera can help you install, configure, optimize, tune, and run CDH for large scale data processing and analysis. Cloudera supports CDH whether you run it on servers in your own datacenter or on hosted infrastructure services, such as Amazon Web Services, Microsoft Azure, or Google Compute Engine.

If you are a Cloudera customer, you can:

- Register for an account to create a support ticket at the [support site](#).
- Visit the [Cloudera Knowledge Base](#).

If you are not a Cloudera customer, learn how [Cloudera](#) can help you.

Information Required for Logging a Support Case

Before you log a support case, ensure you have either part or all of the following information to help Support investigate your case:

- If possible, provide a diagnostic data bundle following the instructions in [Collecting and Sending Diagnostic Data to Cloudera](#).
- Provide details about the issue such as what was observed and what the impact was.
- Provide any error messages that were seen, using screen capture if necessary & attach to the case.
- If you were running a command or performing a series of steps, provide the commands and the results, captured to a file if possible.
- Specify whether the issue took place in a new install or a previously-working cluster.
- Mention any configuration changes made in the follow-up to the issue being seen.
- Specify the type of release environment the issue is taking place in, such as sandbox, development, or production.
- The severity of the impact and whether it is causing outage.

Community Support

There are several vehicles for community support. You can:

- Register for the [Cloudera forums](#).
- If you have any questions or comments about CDH, you can visit the [Using the Platform forum](#).
- If you have any questions or comments about Cloudera Manager, you can
 - Visit the [Cloudera Manager forum](#) forum.
 - Cloudera Express users can access the Cloudera Manager support mailing list from within the Cloudera Manager Admin Console by selecting **Support > Mailing List**.
 - Cloudera Enterprise customers can access the [Cloudera Support Portal](#) from within the Cloudera Manager Admin Console, by selecting **Support > Cloudera Support Portal**. From there you can register for a support account, create a support ticket, and access the Cloudera Knowledge Base.
- If you have any questions or comments about Cloudera Navigator, you can visit the [Cloudera Navigator forum](#).

Get Announcements about New Releases

To get information about releases and updates for all products, visit the [Release Announcements](#) forum.

Report Issues

Your input is appreciated, but before filing a request:

- Search the [Cloudera issue tracker](#), where Cloudera tracks software and documentation bugs and enhancement requests for CDH.
- Search the [CDH Manual Installation](#), [Using the Platform](#), and [Cloudera Manager](#) forums.

Appendix: Apache License, Version 2.0

SPDX short identifier: Apache-2.0

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims

licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

1. You must give any other recipients of the Work or Derivative Works a copy of this License; and
2. You must cause any modified files to carry prominent notices stating that You changed the files; and
3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

Appendix: Apache License, Version 2.0

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

```
Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
```