Cloudera Navigator Data Management
Using Policies to Automate Metadata Tagging

Lineage

Cloudera Navigator Business Metadata

Administration (Navigator Console)
# Navigator Configuration and Management

- Accessing Navigator Data Management Logs ......................................................... 76
- Accessing Navigator Logs from Cloudera Manager .................................................. 76
- Accessing Navigator Logs from the Command Line .................................................. 76
- Backing Up Cloudera Navigator Data ........................................................................ 77
- Authentication and Authorization............................................................................. 77
- Configuring Cloudera Navigator to work with Hue HA ............................................. 78
- Cloudera Navigator support for Virtual Private Clusters ........................................... 79
- Navigator Auditing in Virtual Private Compute Clusters ............................................ 79
- Navigator Metadata and Lineage Extraction in Virtual Private Compute Clusters ...... 79
- Encryption (TLS/SSL) and Cloudera Navigator ........................................................................ 80
- Limiting Sensitive Data in Navigator Logs ................................................................. 80
- Preventing Concurrent Logins from the Same User ................................................... 81
- Navigator Audit Server Management ...................................................................... 81
- Navigator Auditing Architecture ............................................................................. 81
- Setting Up Navigator Audit Server .......................................................................... 82
- Enabling Audit and Log Collection for Services ....................................................... 85
- Configuring Service Auditing Properties .................................................................. 87
- Adding Audit Filters ............................................................................................... 91
- Monitoring Navigator Audit Service Health ............................................................ 93
- Publishing Audit Events ......................................................................................... 95
- Maintaining Navigator Audit Server ...................................................................... 97
- Navigator Metadata Server Management ............................................................... 99
- Navigator Metadata Architecture ............................................................................ 99
- Setting Up Navigator Metadata Server ................................................................... 104
- Navigator Metadata Server Tuning ......................................................................... 110
- Configuring and Managing Extraction .................................................................... 112
- Hive and Impala Lineage Configuration .................................................................. 115
- Configuring the Server for Policy Messages ............................................................ 117

# Cloudera Navigator and the Cloud

- Using Cloudera Navigator with Altus Clusters ....................................................... 119
- How it Works: Background to the Setup Tasks ....................................................... 120
- Configuring Extraction for Altus Clusters on AWS ............................................... 120
- Using Cloudera Navigator with Amazon S3 ............................................................ 125
- Amazon S3 Storage Characteristics ......................................................................... 126
- Cloudera Navigator and Amazon S3 ....................................................................... 126
- Configuring Extraction for Amazon S3 .................................................................. 130

# Cloudera Navigator APIs

- .......................................................................................................................... 139
About Cloudera Navigator Data Management

This guide shows you how to use Cloudera Navigator Data Management component for data governance, compliance, data stewardship, and other metadata management tasks.
Cloudera Navigator Overview

Cloudera Navigator Data Management component is a complete solution for data governance, auditing, and related data management tasks that is fully integrated with CDH, and that collects governance artifacts—lineage, metadata, and auditing—automatically. Cloudera Navigator lets compliance groups, data stewards, administrators, and others work effectively with data at scale. Working "effectively with data at scale" means that finding specific data entities—to prove to regulators that deposit reserves have not been artificially manipulated, for example—is easier when the data entities in multi-hundred-gigabyte (or terabyte, and beyond) clusters have been cataloged.

An effective catalog of cluster data supports self-service data discovery for an organization. For example, business users can find all the data associated with particular projects by looking for meaningful labels without needing to know the low-level structures within the cluster. Finding all the tables or files relevant for a specific project in a given department can be as simple as applying filters to the Search page. For example, to start exploring the finance team’s data stored in an organization’s Amazon Simple Storage Service (S3), authorized users can select the source type and the tag filters:

Cloudera Navigator enables the cataloging function for Hadoop clusters thanks to its metadata architecture, which lets organizations devise comprehensive metadata models and apply them automatically as data is ingested into the cluster. Using the Cloudera Navigator console, data stewards and other business users can get an at-a-glance view of cluster data through charts, graphs, and histograms that allow further drill-down into all the details, including displaying lineage diagrams that capture transformations to data entities that may have occurred since origination. By tracing data entities back to their source, lineage diagrams show an entity’s provenance and can be used to authenticate values by rendering precisely the transformations that may have occurred.

In addition to its metadata infrastructure, Cloudera Navigator also provides auditing infrastructure. Finding the data needed to pull together reports for regulators using standard Hadoop tools can take days but Cloudera Navigator lets organizations find needed information easily and quickly, from menu selectable reports, dashboards, and the like. Using the analytics feature to look at HDFS utilization, system administrators can glean meaningful information about data operations that might be tying up system resources and many other details. With further drill-down, administrators can identify root causes of issues and can also pro-actively monitor and pre-empt potential issues that could occur due to poor organization or consumption of data resources.

Navigator Console

The Cloudera Navigator console provides a unified view of auditing, lineage, and other data management capabilities across all clusters managed by a given Cloudera Manager instance. It organizes metadata collected through both the Navigator Audit Server and the Navigator Metadata Server.
Note: The Cloudera Navigator console invokes the REST APIs exposed by the web service on the host supporting the Navigator Metadata Server role instance. The APIs can be called directly by in-house, third-party, and other developers who want to automate tasks or implement functionality not currently provided by the Cloudera Navigator console. See Cloudera Navigator APIs for an overview and other details.

Assuming that the Cloudera Navigator data management component is running, that you have a login account for Cloudera Navigator, and that you know the host name and port of Navigator Metadata Server role (or have been given this information by your system administrator), follow the steps below to access the Cloudera Navigator console.

Accessing the Cloudera Navigator Console

The Cloudera Navigator console can be accessed from the Cloudera Manager Admin Console or directly on the Navigator Metadata Server instance. Only Cloudera Manager users with the role of Navigator Administrator (or Full Administrator) can access Cloudera Navigator console from the Cloudera Manager Admin Console.

From the Cloudera Manager Admin Console:

1. Open your browser.
2. Navigate to the Cloudera Manager Admin Console.
3. Log in as either Navigator Administrator or Full Administrator.
4. From the menu, select Clusters > Cluster-n.
5. Select Cloudera Navigator from the menu.
6. Log in to the Cloudera Navigator console.

To access the Cloudera Navigator console directly:

1. Open your browser.
2. Navigate to the host within the cluster running the Cloudera Navigator Metadata Server role.

http://fqdn-1.example.com:7187/login.html

In this example, node 1 of the cluster is running the Navigator Metadata Server role, hosted on the default port 7187. The login page displays.

3. Log in to the Cloudera Navigator console using the credentials assigned by your administrator.

If your Cloudera Navigator instance has been configured to integrate with your organization's Active Directory (or other LDAP instance) for authentication, your credentials may be simply the same user account and password you use every day for your other production systems.

Navigator Guide

This Cloudera Navigator Data Management guide contains information needed by data stewards, compliance teams, and business users to solve business problems using cluster metadata. The guide also includes information for administrators to configure and manage Cloudera Navigator servers and users. The table lists other documentation for Cloudera Navigator:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td><a href="#">Cloudera Navigator Data Management Overview</a> provides brief overview of common Cloudera Navigator data management functionality for data stewards, governance and compliance teams, data engineers, and administrators. Includes FAQs and an introduction to the Cloudera Navigator APIs with some resources for more information.</td>
</tr>
<tr>
<td>Installation</td>
<td><a href="#">Installing the Cloudera Navigator Data Management Component</a> provides all the details about installing and setting up Cloudera Navigator Data Management component. Cloudera Navigator requires a Cloudera Enterprise license. See <a href="#">Managing Licenses</a> for details.</td>
</tr>
</tbody>
</table>
## Cloudera Navigator Overview

<table>
<thead>
<tr>
<th>Upgrade</th>
<th><strong>Upgrading Cloudera Manager</strong> guides administrators through the upgrade process for Cloudera Manager, including Cloudera Navigator. Be sure to read the <a href="#">Cloudera Navigator 6 Data Management Release Notes</a> before starting an upgrade.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Notes</td>
<td><strong>Cloudera Navigator 6 Data Management Release Notes</strong> includes new features, changed features, known issues, and resolved issues for each release. Always read the <a href="#">Cloudera Navigator Data Management Release Notes</a> before upgrading.</td>
</tr>
</tbody>
</table>
Finding Specific Entities by Searching Metadata

When you enter search terms in Cloudera Navigator, you are looking up names, types, descriptions and other metadata collected by Navigator Metadata Server. The search index includes metadata (not data) about your cluster data assets and operations. You can make the search more powerful by associating your own information (business metadata) to the entities that Navigator stores.

Tip: Search data does not overlap with audit data. To access audit events, use the Audit tab in the Navigator Console.

Required Role: Metadata Viewer (or Metadata Administrator, Full Administrator)

You can find entities matching selected criteria using the Cloudera Navigator console, as detailed below.

Searching Metadata

1. Open your browser.
2. Navigate to the host within the cluster running the Cloudera Navigator Metadata Server role.
   
   http://fqdn-1.example.com:7187/login.html

   In this example, node 1 of the cluster is running the Navigator Metadata Server role, hosted on the default port 7187. The login page displays.
3. Log in to the Cloudera Navigator console using the credentials assigned by your administrator. The Cloudera Navigator console opens to the Search tab.
4. To display all entity types in the search results, click Clear all filters. Or, limit search results to specific source types, entity types, or other characteristics by applying filters.
5. Enter the search strings in the Search box.

Filter Example

The following filter example demonstrates how to narrow search results by selecting a built-in Source Type filter set to HDFS and the technical property PERMISSIONS with the value rwxrwxrwx. Breadcrumbs for each filter value show above the results. The "Deleted = Do not show Deleted" breadcrumb is included in the filter by default.

When you select a property value, a filter breadcrumb shows above the search results. Click the "x" in the breadcrumb to remove that criteria from the filter.
Viewing Search Results

The Search Results pane displays the number of matching entries in pages listing 25 entities per page. You can view the pages using the page control at the bottom of each page.

Each entry in the result list contains:

- Source type
- Name - A link to a page that displays the entity details and lineage diagram
- Properties
- If Hue is running, a link at the far right labeled View in Hue that opens the Hue browser for the entity. For example:

Displaying Entity Details

The entity Details page displays all three types of metadata for an entity—technical, managed, and user-defined—and entity type-specific information:

- HDFS directories - Directory contents
- HDFS datasets and fields - Schema
- Hive and Impala databases - Tables and views
- Hive tables - Extended attributes, table schema, partitions
- Impala tables - Table schema
- MapReduce, YARN, and Spark operations - Instances
- Pig operation executions - Tables
- S3 buckets and folders - Folder contents

All entity types can display inputs and outputs. See Enabling Inputs and Outputs to Display.

If managed properties have been defined for a particular entity type, the Show All checkbox in the Managed Properties pane displays all properties that can be assigned values for the selected entity. To display only those properties that have values, clear the checkbox. If all properties have values, the checkbox has no effect.

To display entity details:

1. Perform a search.
2. In the search results, click an entity name link. The Details tab displays.

Hive Table Entity Details

For example, if you click the Hive table web_logs link in the search result displayed in preceding example, you see the following details:
The caret > indicates fields with content; click to expand them. In addition to managed properties, user-defined properties, and technical metadata, you can view the names of the columns and the inputs and outputs.

**Managed Properties Example**

The following account table entity has two managed properties in the realestate namespace: Department and AccessAttempts.

**Filtering Search Results**

To filter search results, choose filter values in the Filters pane or type search strings in the Search box.

The Filters pane lists default properties (source type, type, owner, cluster, and tags) and their values. You can add or remove properties from this list: click Add Filters... and choose from the defined technical and metadata properties. To remove non-default filter properties, click the x in the filter.

Note that when filter values are timestamps, the server stores the timestamp in UTC, and the UI displays the timestamp converted to the local timezone.
Finding Specific Entities by Searching Metadata

The number to the right a property value is the number of extracted entities that have that property value:

```
<table>
<thead>
<tr>
<th>SOURCE TYPE</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>415,301</td>
</tr>
<tr>
<td>SIZE (MIB)</td>
<td></td>
</tr>
<tr>
<td>CREATED</td>
<td></td>
</tr>
<tr>
<td>GROUP</td>
<td></td>
</tr>
<tr>
<td>YARN</td>
<td>1,084</td>
</tr>
<tr>
<td>STARTED</td>
<td></td>
</tr>
<tr>
<td>ENDED</td>
<td></td>
</tr>
<tr>
<td>Hive</td>
<td>239</td>
</tr>
<tr>
<td>STARTED</td>
<td></td>
</tr>
<tr>
<td>ENDED</td>
<td></td>
</tr>
<tr>
<td>Pig</td>
<td>18</td>
</tr>
<tr>
<td>Impala</td>
<td>5</td>
</tr>
</tbody>
</table>
```

Facet values with the count 0 are not displayed.

When you enter values, the value is enclosed in quotes; the value inside the quotes must match the metadata exactly. For example:

- Typing "sample_*" in the `originalName` property returns only entities whose names match that exact string.
- To perform a wildcard search, type the wildcard string in the Search box. For example, typing the string "sample_*" in the Search box returns all entities with "sample_" at the beginning of their original name.

When you construct search strings with filters, use parentheses () to specify multiple values of a property. Add multiple properties by using the + operator. For example, entities of type HDFS or Hive that are of type file or directory:

```
+(sourceType:hdfs sourceType:hive) +(type:file type:directory)
```

and:

```
((+sourceType:hdfs +created:[NOW/DAY-30DAYS TO NOW/DAY+1DAY]) sourceType:hive)
```

Grouping Search Results Using Metadata

Using the Group by option, you can organize the search results into groups based on the common properties of the entities in your search, including managed, user-defined, and some technical metadata. When you choose a group by property, the search panel lists the property values and shows how many search results correspond to that value.
From the Group by view, you can:

- Click the number for a group to show the search results for that group.

<table>
<thead>
<tr>
<th>Group</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RK</td>
<td>19</td>
</tr>
<tr>
<td>OX</td>
<td>11</td>
</tr>
<tr>
<td>ST</td>
<td>7</td>
</tr>
<tr>
<td>AK</td>
<td>3</td>
</tr>
<tr>
<td>CF</td>
<td>2</td>
</tr>
<tr>
<td>JM</td>
<td>2</td>
</tr>
<tr>
<td>BL</td>
<td>1</td>
</tr>
</tbody>
</table>

- Click the "x" on the Group by breadcrumb to remove the groupings.

When you group results by a numeric or date property, you can also choose to "drill down" into a single group: the results from that group are grouped into smaller buckets. Hover over the group row to show the Drill into group control.
The Group by view shows at most 50 values of a property.

**Saving Searches**

1. Specify a search string or set of filters.
2. To the right of the Search box, select **Actions > Save**, **Actions > Save Search_name**, or **Actions > Save As**.
3. If you have not previously saved the search, specify a name and click **Save**.

**Reusing a Saved Search**

1. To the right of the Search box, select **Actions > View saved searches**. A label with the saved search name is added under the Search box.
2. Click the saved search name. The breadcrumbs and full query if displayed are updated to reflect the saved search, and the search results are refreshed immediately.

**Performing Actions on Entities**

**Required Role:** **Policy Editor** (or Full Administrator)

**Moving an HDFS Entity and Moving an HDFS Entity to Trash**

You can move an HDFS entity to another HDFS location, and to **HDFS trash**. To perform such actions, you must be a member of a user group that has the appropriate access to HDFS files.
Finding Specific Entities by Searching Metadata

Note: To move HDFS entities to another file system such as S3, consider designating an HDFS directory as an archive location, define a Navigator policy to move the HDFS entities to that directory, and define a CRON job or other process to regularly move the content of the archive directory to the non-HDFS location.

You can also schedule a move or move to trash in a policy.

1. Open your browser.
2. Navigate to the host within the cluster running the Cloudera Navigator Metadata Server role using the correct host name and port for your instance:

   http://fqdn-1.example.com:7187/login.html

   The login prompt displays.

3. Log in to the Cloudera Navigator console using the credentials assigned by your administrator.
4. Run a search in the Cloudera Navigator console.
5. Click an HDFS entity link returned in the search. The entity Details tab displays.
6. To the left of the Details tab, select Actions > Move... or Actions > Move to Trash....
7. For a move, specify the target path.
8. Click Run Action. When you delete a file, after a short delay the file displays a Deleted badge.

Viewing Command Action Status

1. Access the Cloudera Navigator console using the correct host name and port for your instance:

   http://fqdn-1.example.com:7187/login.html

   The login prompt displays.

2. Log in to the Cloudera Navigator console using the credentials assigned by your administrator.
3. In the top right, click username > Command Actions. The Command Actions status page displays with a list of actions performed and the policy that caused the action, if applicable.
4. If an action failed, a View Log button displays, which you can click to view the error message associated with the failure.

Viewing an Entity in Hue

If the Hue component is running on the cluster view some entities using Hue and related tools, as follows:

<table>
<thead>
<tr>
<th>File Browser</th>
<th>HDFS directories and files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hive Metastore Manager (HMS)</td>
<td>Hive database and tables</td>
</tr>
<tr>
<td>Job Browser</td>
<td>YARN, Oozie</td>
</tr>
</tbody>
</table>

1. Access the Cloudera Navigator console using the correct host name and port for your instance:

   http://fqdn-1.example.com:7187/login.html

   The login prompt displays.

2. Log in to the Cloudera Navigator console using the credentials assigned by your administrator.
3. Run a search in the Cloudera Navigator console.
4. Do one of the following:
   - Search results
     1. Click the View in Hue link in a search result entry.
   - Entity details
Finding Specific Entities by Searching Metadata

1. Click an entity link returned in the search. The entity Details tab displays.
2. To the left of the Details tab, select Actions > View in Hue.

The entity displays in the supported Hue application.
Cloudera Navigator Auditing

Cloudera Navigator auditing has been designed to meet demanding corporate governance and compliance requirements, especially for organizations in regulated industries. The Navigator Audit Server collects audit events from selected cluster services, including those running on a Compute cluster in a Cloudera Virtual Private Cluster configuration. Authorized users can use the Cloudera Navigator console to display audit event reports, create reports, and export audit details as CSV or other file formats. They can also search using configurable filters—a specific user name, IP address, or service name, for example—to quickly obtain answers to a variety of questions (see Using Audit Events to Understand Cluster Activity on page 21 for details).

Audit details for HDFS, the distributed storage layer that underlies any Hadoop cluster, are also characterized using histograms and other graphical charts that can be seen in the analytics area of the Cloudera Navigator console.

Events are the activities that occur during regular operations within the cluster. Events often result in messages that record the success or failure of activity along with other relevant details about the specific internal process, such as a hostname, IP address, or service name. Event messages from various services are typically sent to local log files, and from there, the Cloudera Manager Agent process sends them to the Navigator Audit Server (see Navigator Auditing Architecture on page 81 for details).

In addition to individual service events audited by Cloudera Navigator, Cloudera Manager Server records lifecycle events at the cluster, host, role, service, and user level, and records actions that involve licenses and parcels. For example, starting up the cluster is a lifecycle event captured by Cloudera Manager, as is downloading a parcel to update software. Cloudera Manager also captures security-related events, such as adding users, deleting users, login failures, and login successes. For more information about Cloudera Manager auditing capabilities, see Lifecycle and Security Auditing.

Cloudera Navigator tracks and coalesces events collected by Cloudera Manager and generates some of its own events as well. Audit events are viewable in the Cloudera Navigator console. Several pre-configured reports are available from the Audit tab of the Cloudera Navigator console, where you can also filter for specific types of events, create new reports, and export detailed audit reports as CSV or JSON. For example, here is a partial export of Recent Denied Accesses—user accounts without sufficient privileges (user roles) that attempted to log in to Cloudera Navigator but were prevented from doing so:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Username</th>
<th>IP Address</th>
<th>Service Name</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 23, 2017 8:57:01 AM</td>
<td>admin</td>
<td>172.21.2.218</td>
<td>Navigator</td>
<td>authentication</td>
</tr>
<tr>
<td>Jun 23, 2017 8:56:43 AM</td>
<td>rogue-user</td>
<td>172.21.2.218</td>
<td>Navigator</td>
<td>authentication</td>
</tr>
<tr>
<td>Jun 23, 2017 8:56:23 AM</td>
<td>nav-admin</td>
<td>172.21.2.218</td>
<td>Navigator</td>
<td>authentication</td>
</tr>
<tr>
<td>Jun 23, 2017 8:56:11 AM</td>
<td>kell</td>
<td>172.21.2.218</td>
<td>Navigator</td>
<td>authentication</td>
</tr>
</tbody>
</table>

Viewing Audit Analytics

**Required Role:** Auditing Viewer (or Full Administrator)

1. Log in to the Cloudera Navigator console.
2. Click the **Analytics** tab and select HDFS from the menu. The Audit tab displays. The Metadata tab may also display if the account has the appropriate permissions. The **Source** button displays in the banner section of the console if the Cloudera Navigator instance supports multiple clusters.

![Cloudera Navigator](image)

- Click the **Source** button (if it displays, meaning more than one instance) and select an HDFS instance from those available.

3. The Activity tab displays a bar graph that lists the number of files that have been read the number of times listed in the x-axis.

- To display at the right the directories containing the files that have been read, click an activity bar. This draws a blue selection outline around the bar and selects the Activity checkbox.
- To select more than one value, grab a bar edge and brush a range of values.
- To change a range, click a bar, drag to a different range of values, and drop.
- To reduce a range, grab a bar edge and contract the range.
- To clear Activity, clear the checkbox. The previous selection is indicated with a gray outline.
- When you select Activity and the graph had a previous selection, the previous selection is reused. For example, if you had previously selected values spanning six through nine for the number of times files have been read, and you select the checkbox, six through nine will be reselected.

4. In the directory listing on the right:

- Filter the directories by typing directory strings in the search box and pressing **Enter** or **Return**.

**Required Role:** Metadata & Lineage Viewer (or Managed & Custom Metadata Editor, or Full Administrator)

Add selected directories to a search query and display the Search tab by doing one of the following:

- Clicking a directory name link.
- Selecting one or more directory checkboxes and selecting **Actions** > **Show selection in search**.

**Required Role:** Metadata & Lineage Viewer (or Managed & Custom Metadata Editor, or Full Administrator)

Add selected directories to the search query of a new policy and display the Policies tab by selecting one or more directory checkboxes and selecting **Actions** > **Create a policy from selection**.
For example, the following screenshot shows files that have been accessed once and match the string staging. Each directory has six files that has been accessed.

Using Audit Events to Understand Cluster Activity

Actions performed on the cluster by users and by services are tracked by Cloudera Navigator. Using the filters available on the Audit page of the Cloudera Navigator console lets you quickly find answers to a variety of questions such as:

- **What Did a Specific User Do on a Specific Day?** on page 21
- **Who Deleted Files from Hive Warehouse Directory?** on page 23
- **What Happened to Data in the Database?** on page 24
- **Who ran which operation on a table?**

The examples below step through these common use cases.

To work with Audit Events in the Cloudera Navigator console, you must have an account with the user role of Auditing Viewer or Navigator Administrator.

To view Audit Events in the Cloudera Navigator console and apply filters:

1. Log in to the Cloudera Navigator console.
2. Click the Audits tab. The default view displays a list of all Audit Events for the past hour (note the date range field above the listing, below the Actions button).
3. Configure and apply filters as needed to find specific events by username, by source, for selected time frames, and so on.

**What Did a Specific User Do on a Specific Day?**

A data engineer complains that a job was not running as well as expected one afternoon and wants to find out what might have occurred.

To filter the audit details to these specifics, you need only the user name and the time frame. The example isolates actions by the user name cmjobuser for a one-hour period on November 3, 2016:

1. Limit the list of audit events to those for a specific user by defining a username filter:
   a. Click Filters to open the filter selector.
b. Select **Username** from the Select Property... drop-down selector.

c. Set the evaluation operator (=, like, !=) to = (equals sign).

d. Type the username (**cmjobuser** for this example).

```
<table>
<thead>
<tr>
<th>Username</th>
<th>=</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmjobuser</td>
<td></td>
</tr>
</tbody>
</table>
```

e. Click **Apply**. The filter is applied to the audit events and the list displays only those events for the selected username.

2. Limit the Audit Events list for the selected username to only those events that occurred on a specific date at a specific time:

   a. Click the arrow next to the current date range field to open the date and time range options selector. Time frame options range from the last 2, 6, 12, or 24 hours to the last 7 or last 30 days, but also let you set a custom range.

   b. **Click the Custom Range** link to open the date and time range selector.

   c. Use the field controls to set the start date and time and the end date and time for your custom time frame, as shown in this example:

   ```
<table>
<thead>
<tr>
<th>Selected Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/21/2017, 11:06 AM - 09/21/2017, 12:06 PM</td>
</tr>
</tbody>
</table>
   ```

   d. **Click Apply**.

The date and time range is applied to the Audit Events filtered by username and displays the resulting list in reverse chronological order (end date and time at the top of the list). The Audit Events for username **cmjobuser** during the one-hour period from 3:00 to 4:00 PM on November 3, 2016 are shown below.
Who Deleted Files from Hive Warehouse Directory?

A data steward is wondering what happened to some critical files in the data warehouse—they seem to have been deleted. The organization uses the Hive warehouse located in the default directory:

- `/user/hive/warehouse`

To find out who deleted files from this directory, create a filter that uses the Source property in conjunction with the Delete operation.

1. Limit the list of Audit Events to only those for the `/user/hive/warehouse` directory:
   a. Click Filters.
   b. Select Source from the Select Property... drop-down selector.
   c. Set the evaluation operator to like.
   d. Type `/user/hive/warehouse` in the entry field for the Source property.
   e. Click Apply. The source filter added to the list of filters and applied to Audit Events, returning an updated Audit Events list.

2. Find all delete operations that occurred on the source (the Hive warehouse directory, in this example):
   a. Click Filters. The Source filter displays the filter previously configured. Click the plus sign (+) at the end of the filter definition to add new filter setting fields.
   b. Select Operation from the Select Property... drop-down selector.
   c. Set the evaluation operator to =.
   d. Type delete in the entry field for Operation property.
   e. Click Apply. The filter to select delete operations is added to the list of filters and applied to Audit Events. An updated Audit Events list is returned, showing only delete operations for sources similar to `/user/hive/warehouse`.

The results show both completed and attempted delete operations (attempted but unsuccessful are in red). All these events are associated with username `navigator_user` from the same IP address and using the same service (hdfs) over the course of a day (June 9, 2016).
With this information, a Navigator Administrator can go to the Administration tab of the Cloudera Navigator console and find out who is associated with the navigator_user account.

- Log in to the Cloudera Navigator console.
- Click the Administration tab.
- Click the Role Management tab.

What Happened to Data in the Database?

The data files associated with a database are typically partitioned into files or directories by date, often by year. The system admin discovers that the data from 2015 is missing from the production database—only data prior to 2010 has been archived off the system, so data from 2015 should still be there.

Files for data created in 2015 include 2015 in their filenames.

To determine what happened to the data stored in folders and files in the year 2015, do the following:

1. Filter the list of events for sources containing 2015:
   a. Click Filters.
   b. Select Source from the Select Property... drop-down selector. Sources can be paths to HDFS files or directories.
   c. Set the evaluation operator to like.
   d. Type 2015 in the entry field for the Source property.
   e. Click Apply. The source filter added to the list of filters and applied to Audit Events, returning an updated Audit Events list.

2. Filter the list of events for the delete operation:
   a. Click Filters. The Source filter displays the filter previously configured. Click the plus sign (+) at the end of the filter definition to add new filter setting fields.
   b. Select Operation from the Select Property... drop-down selector.
   c. Set the evaluation operator to =.
   d. Type delete in the entry field for the Operation property.
   e. Click Apply. The operation filter added to the list of filters and applied to Audit Events, returning an updated list containing Audit Events for delete operations from sources like 2015.

3. Set the date range to one year:
   a. Click the date-time field at the top right of the Audit Events page.
   b. To set the range to be the last year, click Custom Range. The Selected Range field is enabled for input.
c. In the left date field, use the field controls to specify a date one year ago.

d. Click Apply.

The result of all filters and the selected time frame reveals that the hdfs username deleted directories containing 2015 in their names:

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Username</th>
<th>IP Address</th>
<th>Service Name</th>
<th>Operation</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 13 2016 11:45 AM</td>
<td>hdfs</td>
<td>10.17.207.26</td>
<td>hdfs</td>
<td>delete</td>
<td>/user/navigator_user/2015_11_21</td>
</tr>
<tr>
<td>Jun 13 2016 11:45 AM</td>
<td>hdfs</td>
<td>10.17.207.26</td>
<td>hdfs</td>
<td>delete</td>
<td>/user/navigator_user/2015_11_20</td>
</tr>
<tr>
<td>Jun 13 2016 11:45 AM</td>
<td>hdfs</td>
<td>10.17.207.26</td>
<td>hdfs</td>
<td>delete</td>
<td>/user/navigator_user/2015_11_19</td>
</tr>
<tr>
<td>Jun 13 2016 11:45 AM</td>
<td>hdfs</td>
<td>10.17.207.26</td>
<td>hdfs</td>
<td>delete</td>
<td>/user/navigator_user/2015_11_18</td>
</tr>
</tbody>
</table>

Who ran which operation against a table?

When a change occurs to a data asset, it can cause problems to reports or other processes that use the data asset. You can use the Audit events to find when and what caused a change in a data asset. This example describes how to use audits to determine what caused a schema change to a table so you can identify the user or process that may be causing unwanted changes.

To find all operations against a specific table in a general time range:

1. Filter the list of events for the table.
   a. Click Filters.
   b. Select Table Name from the Select Property... drop-down selector.
   c. Set the evaluation operator to like.
   d. Type the part or all of the table name in the entry field for the Table Name property.
   e. Click Apply. The source filter added to the list of filters and applied to Audit Events, returning an updated Audit Events list.

2. Set the date range to the general time frame where the change occurred:
   a. Click the date-time field at the top right of the Audit Events page.
   b. To set the range, click Custom Range. The Selected Range field is enabled for input.
   c. In the left date field, use the field controls to specify the earliest date where the change may have occurred.
      To include the entire day, set the time to indicate the beginning of the day, such as 12:01 AM.
   d. In the right date field, specify the latest date where the change may have occurred.
      To include the entire day, set the time to indicate the end of the day, such as 11:59 PM.
   e. Click Apply.

3. Review the results, looking at both the operation and the service name.

4. If the results are too large, consider adding additional filters:
   - **By Service Name.** For example, to show all Hive operations, use Service Name like hive.
   - **By Operation.** For example, to show only Hive operations that change the table metadata, use Operation like alter.
Exploring Audit Data

Required Role: **Auditing Viewer** (or Full Administrator)

Viewing Audit Events

1. Click the **Audits** tab. By default, the Audit Events report opens, listing all events that occurred within the last hour, with the most recent at the top:

The Audit Events and Recent Denied Accesses reports are available by default. You create your own reports and apply a variety of filters as detailed in the next section.

Filtering Audit Events in the Console

You filter audit events by specifying a time range or adding one or more filters containing an audit event field, operator, and value.

Specifying a Time Range

1. Click the date-time range at the top right of the Audits tab to open a range selector.
2. Select one of the pre-defined ranges.
   To enter a specific time range, choose **Custom range** and use the controls in **Selected Range** to specify start and end dates and times.

3. Click **Apply**.

**Adding a Filter Field**

1. Click the **Filters** link.

The Filters pane displays.

2. Click + if a filter field is not already open.

3. Choose a field in the **Select Property** drop-down list.
   The properties correspond to the audit fields listed in **Service Audit Events** on page 162.

4. Choose an operator in the operator drop-down list.
   - Choose from = (equals), != (not equals), like, and not like. The like operator matches to substrings. For example, to see all the audit events for files created in the folder /user/joe/out, specify **Source like /user/joe/out**.
   - Use **not like** to filter out events based on a partial string match. For example, to show audit events for a set of IP addresses that start with the same sequence 172.39.109, you can specify **IP Address not like 172.39.109**.

5. Type a field value in the value text field.
   For example, to see the events listed for Navigator, enter **Service Name = Navigator**.

6. To specify an additional filter, click + and define the new criteria.
   Audit events show that match all filters (AND).

7. Click **Apply**.
A filter breadcrumb appears above the list of audit events and the list of events displays all events that match all the filter criteria.

Removing a Filter Field

1. Click the x next to the filter breadcrumb.

You can also click Filters and modify or remove filter criteria.

Cloudera Navigator Audit Event Reports

Required Role: Auditing Viewer (or Full Administrator)

Cloudera Navigator console provides two default reports for display by default:

- Audit Events listing, which displays all recent events in reverse chronological order
- Recent Denied Accesses, which displays all accesses within the cluster and highlights denied access attempts in red, for easy identification.

These two default reports are starting points. Use the Audit Report and define filters to create new reports can be created by defining and applying filters to fine-tune the selected results. Give the filtered report specifications for future use, and export (download) any report to CSV and JSON file formats.

In addition, the metadata about the audit reports you create and save is recorded by the Navigator Metadata Server. This section shows you how to use the Cloudera Navigator console to create audit reports.

**Note:** All steps below start from the Cloudera Navigator console.

Creating Audit Event Reports

Selecting the Audit menu in the Cloudera Navigator console displays the Audit Events report. This report displays all audit events captured in the last 1 hour. You can modify the filters configured for this report and save it, giving it a new name, as follows.

1. To save a filtered version of the Audit Events report:
   a. Optionally specify filters (see Filtering Audit Events in the Console on page 26).
   b. Click Save As Report.
2. Enter a report name.
3. In the Default time range field, specify a relative time range. If you had specified a custom absolute time range before selecting Save As Report, the custom absolute time range is discarded.
4. Optionally add filters (see Filtering Audit Events in the Console on page 26).
5. Click Save.

Editing Audit Event Reports

1. In the left pane, click a report name.
2. Click Edit Report.
3. In the Default time range field, specify a relative time range. If you had specified a custom absolute time range before selecting Save As Report, the custom absolute time range is discarded.
4. Optionally add filters (see Filtering Audit Events in the Console on page 26).
5. Click Save.

Downloading Audit Event Reports

You can download audit event reports in the Cloudera Navigator console or using in CSV and JSON formats. An audit event contains the following fields:

- timestamp
- service
- username
- ipAddress
- command
- resource
- allowed
- [operationText]
- serviceValues

The values for resource and serviceValues fields depend on the type of the service. In addition, Hive, Hue, Impala, and Sentry events have the operationText field, which contains the operation string. See Service Audit Events on page 162 for details.

In addition to downloading audit events, you can configure the Navigator Audit Server to publish audit events to a Kafka topic or syslog. See Publishing Audit Events.

Downloading Audit Event Reports from

1. Do one of the following:
   - Add filters (see Filtering Audit Events in the Console on page 26).
   - In the left pane, click a report name.
2. Select Export > format, where format is CSV or JSON.

Downloading Audit Events Using the Audit API

You can filter and download audit events using the Cloudera Navigator APIs.

Hive Audit Events Using the Audit API

To use the API to download the audits events for a service named hive, use the audits endpoint with the GET method:

```
http://fqdn-n.example.com:port/api/APIversion/audits/?parameters
```

where fqdn-n.example.com is the host running the Navigator Metadata Server role instance listening for HTTP connections at the specified port number (7187 is the default port number). APIversion is the running version of the
API as indicated in the footer of the API documentation (available from the Help menu in the Navigator console) or by calling `http://fqdn-n.example.com:port/api/version`.

For example:

```
curl http://node1.example.com:7187/api/v13/audits/?query=service%3D%3Dhive&
&startTime=1431025200000&endTime=1431032400000&limit=5&offset=0&format=JSON&attachment=false
-X GET -u username:password
```

The `startTime` and `endTime` parameters are required and must be specified in `epoch time` in milliseconds.

The request could return the following JSON items:

```
[
  {
    "timestamp": "2015-05-07T20:34:39.923Z",
    "service": "hive",
    "username": "hdfs",
    "ipAddress": "12.20.199.170",
    "command": "QUERY",
    "resource": "default:sample_08",
    "operationText": "INSERT OVERWRITE \n  TABLE sample_09 \nSELECT \n  sample_07.code,sample_08.description 
  FROM sample_07 
  JOIN sample_08 
  WHERE
  sample_08.code = sample_07.code",
    "allowed": true,
    "serviceValues": {
      "object_type": "TABLE",
      "database_name": "default",
      "operation_text": "INSERT OVERWRITE \n  TABLE sample_09 \nSELECT \n  sample_07.code,sample_08.description 
  FROM sample_07 
  JOIN sample_08 
  WHERE
  sample_08.code = sample_07.code",
      "resource_path": "/user/hive/warehouse/sample_08",
      "table_name": "sample_08"
    }
  },
  {
    "timestamp": "2015-05-07T20:33:50.287Z",
    "service": "hive",
    "username": "hdfs",
    "ipAddress": "12.20.199.170",
    "command": "SWITCHDATABASE",
    "resource": "default:",
    "operationText": "USE default",
    "allowed": true,
    "serviceValues": {
      "object_type": "DATABASE",
      "database_name": "default",
      "operation_text": "USE default",
      "resource_path": "/user/hive/warehouse",
      "table_name": ""
    }
  },
  {
    "timestamp": "2015-05-07T20:33:23.792Z",
    "service": "hive",
    "username": "hdfs",
    "ipAddress": "12.20.199.170",
    "command": "CREATETABLE",
    "resource": "default:",
    "operationText": "CREATE TABLE sample_09 (code string,description string) ROW FORMAT DELIMITED FIELDS TERMINATED BY '\t' STORED AS TextFile",
    "allowed": true,
    "serviceValues": {
      "object_type": "DATABASE",
      "database_name": "default",
      "operation_text": "CREATE TABLE sample_09 (code string,description string) ROW FORMAT DELIMITED FIELDS TERMINATED BY '\t' STORED AS TextFile",
      "resource_path": "/user/hive/warehouse",
      "table_name": ""
    }
  }
]
```
Analytics: Data Stewardship Dashboard

The Cloudera Navigator Data Stewardship dashboard captures a variety of information about data, metadata, and user jobs that process the data. The Data Stewardship dashboard provides information and metrics to help you understand the state of the data and data usage, and lets you visualize trends and averages for a variety of data sources and actions.

For example, system administrators use the Dashboard (Analytics > Data Stewardship Dashboard) to look at the Activity Summary page, which provides a comprehensive overall view—databases created, tables created, tables dropped, SQL queries started, and so on.

Administrators can look for trends, the administrator navigates to the Data Explorer tab, makes two selections to filter for the past several weeks on SQL Queries Started as source type and gleans some clues about a rogue SQL query.

Access the dashboard by clicking Analytics and then choosing Data Stewardship on the navigation bar. Specify the source clusters by clicking Source and clicking a cluster name or All Clusters.

On the Data Stewardship dashboard, select a tab for the information you want to view:

- Dashboard. Provides "at-a-glance" information about databases, tables, operations, and files and directories
- Data Explorer. Lets you select cluster actions to view and compare for specific time periods, in conjunction with charts that show averages and trend lines.

The dashboard is divided into the following major information areas:

- Activity Summary
- Databases
- Hive Tables
- Files and Directories
- Operations and Operation Executions
Each tile in the Activity Summary section provides summary information for actions on a particular entity type and includes the following:

- The name of the activity
- The number of occurrences for that activity for a time period that you select (daily, weekly, monthly, quarterly, all time)
- A line graph showing activity trends based on the time period that you select

A graphical representation of the time-lapse summary for each activity tile is located at the bottom of the tile. Hovering over a point displays the value for that entity on a particular date. For example, if you select Daily Trend, the number in the graph shows number of occurrences for the day so far (since midnight), and hovering over a graph point shows the number of occurrences for that full day as well as the average for the 20-day period represented by the graph.

The Activity Summary area includes the following information:

<table>
<thead>
<tr>
<th>Activity Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases Created</td>
<td>Number of new databases that were added to the cluster.</td>
</tr>
<tr>
<td>Tables Created</td>
<td>Number of new tables that were added to the cluster. Click the value to link to the Search page that shows the search results of the query defined. You can apply filters to narrow the search results and perform any other search actions.</td>
</tr>
<tr>
<td>Tables Altered</td>
<td>Number of tables that were changed.</td>
</tr>
<tr>
<td>Tables Populated</td>
<td>Number of tables that were populated with data. Note that these counts reflect the number of times that a table has been loaded with data, such as through INSERT and UPDATE statements—not the number of unique tables loaded. For example, a single table to which data is added (through 6 INSERT statements) and that has also had 4 UPDATE statements submitted in the same period would report Tables Populated as 10.</td>
</tr>
<tr>
<td>Tables Dropped</td>
<td>Number of tables that were deleted.</td>
</tr>
<tr>
<td>Partitions Created</td>
<td>Number of partitions added. You can apply filters to narrow the search results and perform any other search actions.</td>
</tr>
<tr>
<td>HDFS Files Created</td>
<td>Files that were created. Click the new files value to link the Search page that shows the results of the query defined. You can apply filters to narrow the search results and perform any other search actions.</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SQL Queries Started</td>
<td>Number of SQL queries that were run.</td>
</tr>
<tr>
<td>Accesses Denied</td>
<td>Number of access attempts by users that were denied.</td>
</tr>
</tbody>
</table>

### Databases

**114 Databases**

#### Top Databases by Table Count

<table>
<thead>
<tr>
<th>Database</th>
<th>Table Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>clusterstats</td>
<td>2K</td>
</tr>
<tr>
<td>netsuite</td>
<td>1.2K</td>
</tr>
<tr>
<td>support</td>
<td>1K</td>
</tr>
<tr>
<td>jira</td>
<td>626</td>
</tr>
<tr>
<td>sfdc</td>
<td>434</td>
</tr>
<tr>
<td>warehouse_main</td>
<td>374</td>
</tr>
<tr>
<td>moodle</td>
<td>340</td>
</tr>
<tr>
<td>as_adventure</td>
<td>258</td>
</tr>
<tr>
<td>default</td>
<td>167</td>
</tr>
<tr>
<td>w_house_satellite</td>
<td>141</td>
</tr>
</tbody>
</table>

The Databases area of the Dashboard shows the total number of databases in the source clusters. The top 10 databases, by table count, are displayed in the bar graph.

Click the value next to the Database heading (in this case, 1.5K) to open a Search page showing results from the query "Deleted=Do not show deleted" "Type=Database". Apply or remove filters to refine or broaden the results.
Hover over the bar in the graph to see information about that database, and click the bar to open the Details page for that database. The following figure shows the Details page for the database `nav_policy_db`.
Hive Tables

**8.2K Hive Tables and Views**

### Top Tables by Partition Count

<table>
<thead>
<tr>
<th>Table</th>
<th>Database</th>
<th>Partition Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_logs</td>
<td>default</td>
<td>120.8K</td>
</tr>
<tr>
<td>metrics_production</td>
<td>default</td>
<td>98.1K</td>
</tr>
<tr>
<td>usage_scrapes</td>
<td>product_usage</td>
<td>77.7K</td>
</tr>
<tr>
<td>metrics_staging</td>
<td>default</td>
<td>23.1K</td>
</tr>
<tr>
<td>clusterid_mostrecentcollection...</td>
<td>u.mulyadi</td>
<td>10.4K</td>
</tr>
<tr>
<td>opportunity_history</td>
<td>sfdc</td>
<td>7.7K</td>
</tr>
<tr>
<td>usage_final</td>
<td>product_usage</td>
<td>7K</td>
</tr>
<tr>
<td>distats_parquet</td>
<td>default</td>
<td>6.2K</td>
</tr>
<tr>
<td>case_history</td>
<td>sfdc</td>
<td>5.2K</td>
</tr>
<tr>
<td>jira___c_history</td>
<td>sfdc</td>
<td>4.9K</td>
</tr>
</tbody>
</table>

The Tables area of the dashboard shows the total number of Hive tables in the cluster. The top 10 tables, by partition count, are displayed in the bar graph.

Click the value next to the Hive Tables heading (in this case, 103.9K) to view matching tables in Search.

Click the bar to open the Details page for that table.

Files and Directories

### 802 Files  168 Directories

<table>
<thead>
<tr>
<th>File</th>
<th>Path</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>access.log</td>
<td>/datacore/web_logs</td>
<td>106.3M</td>
</tr>
<tr>
<td>ad.data1.txt</td>
<td>/datacore/ad</td>
<td>31.5M</td>
</tr>
<tr>
<td>part-m-00000</td>
<td>/datacore/part</td>
<td>28.1M</td>
</tr>
<tr>
<td>ad.data2.txt</td>
<td>/datacore/ad</td>
<td>23.6M</td>
</tr>
<tr>
<td>part-r-00000</td>
<td>/datacore/part</td>
<td>22.4M</td>
</tr>
<tr>
<td>hive-exec.jar</td>
<td>/user/oozie/shares/lib/20170509205421/Hive</td>
<td>10.5M</td>
</tr>
<tr>
<td>hive-exec.jar</td>
<td>/user/oozie/shares/lib/20170509205421/Hive2</td>
<td>10.5M</td>
</tr>
<tr>
<td>hive-exec.jar</td>
<td>/user/oozie/shares/lib/20170509205421/spark</td>
<td>10.5M</td>
</tr>
<tr>
<td>hive-exec.jar</td>
<td>/user/oozie/shares/lib/20170509205421/epoop</td>
<td>10.5M</td>
</tr>
<tr>
<td>part-m-00001</td>
<td>/datacore/orders</td>
<td>15.8M</td>
</tr>
</tbody>
</table>

The Files and Directories area of the Dashboard shows the total number of files and directories in the cluster.

Clicking the value next to the Files or Directory heading (in this case, 64.6M or 16.2M, respectively) to show matching files or directories in Search.
The bar graph displays the top 20 files, based on size. Hover over the bar in the graph to see information about that file. Click the bar to open the Details page for that file.

**Operations and Operation Executions**

<table>
<thead>
<tr>
<th>Service</th>
<th>Operations</th>
<th>Operation Executions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octie</td>
<td>1.4M</td>
<td>2.7M</td>
</tr>
<tr>
<td>Yarn</td>
<td>280.5K</td>
<td>1.8M</td>
</tr>
<tr>
<td>Hive</td>
<td>796.1K</td>
<td>697K</td>
</tr>
<tr>
<td>Sqoop</td>
<td>5.3K</td>
<td>60.8K</td>
</tr>
<tr>
<td>Impala</td>
<td>10.9K</td>
<td>31.2K</td>
</tr>
<tr>
<td>Mapreduce</td>
<td>3.3K</td>
<td>5.9K</td>
</tr>
<tr>
<td>Pig</td>
<td>166</td>
<td>576</td>
</tr>
</tbody>
</table>

The Operations and Operation Executions area of the Dashboard shows the total number of operations and operation executions that occurred in the cluster for the specified period of time.

Click the value next to the Operations or Operations Executions for a service to view matching operations or operation executions in Search.

**Data Explorer**
Using Policies to Automate Metadata Tagging

Cloudera Navigator lets you automate the application of metadata to specific entity classes using the policies you define. The policy specifies the actions to be performed by Navigator Metadata Server and the conditions under which to apply them. For data stewards who want to facilitate self-service discovery in their organizations, Cloudera Navigator’s metadata policy feature provides a robust mechanism for streamlining the metadata management tasks. For example, you can define policies that:

- Add managed properties or tags to entities as they are ingested by the cluster
- Move entities of specific class to a specific target path, or to the trash
- Send messages to a JMS message queue for notifications. This requires configuring the JMS server on the Cloudera Management Service. See Configuring a JMS Server for Policy Messages for details.

Messages sent to JMS queues are formatted as JSON and contain the metadata of the entity to which the policy should apply and the policy’s specified message text. For example:

```json
{
    "entity": entity_property,
    "userMessage": "some message text"
}
```

Policies are executed in the home directory of their creator and can only take actions (run commands) for which the creator has privileges. At runtime, a policy fails if the user account of the policy creator does not have privileges to perform all the commands specified in the policy.

Policy ownership can be changed by cloning the policy:

- Log in to the Cloudera Navigator console using the account name to which you want to transfer ownership.
- Clone the policy.
- Log out from this account, and then log in again using account identity of original policy owner.
- Delete or disable the original policy.

**Note:** To ensure that command actions do not fail, policies containing command actions should be created by data stewards who are members of a user group that has the appropriate access to HDFS files.

Certain actions can be specified using Java expressions. See Metadata Policy Expressions on page 168 for details.

Creating Policies

**Required Role:** Policy Editor (or Full Administrator)

These steps begin from the Cloudera Navigator console.

1. Click the Policies tab.
2. Click the New Policy button.
3. Click the **Enable** checkbox.
4. Enter a meaningful name for the policy.
5. In the **Search Query** field, specify the search query that defines the class of entities to which the policy should apply.
6. Click the **Test Query** link to see a list of results based on the query and revise the query as needed.
7. Enter a **Policy Description** to document some of the functional aspects of this policy in the context of your organization. This field is optional but it is recommended for use especially if your organization has many policies defined for use by different teams, departments, and so on.
8. For a policy that includes Java expressions, enter the classes that the expressions will use in the **Import Statements** field. See [Metadata Policy Expressions](#) on page 168 for details, including examples and a class reference.
9. Choose the schedule for applying the policy:
   - **On Change** - When the entities matching the search string change.
   - **Immediate** - When the policy is created.
   - **Once** - At the time specified in the Start Time field.
   - **Recurring** - At recurring times specified by the Start and End Time fields at the interval specified in the Interval field.

   For Once and Recurring fields, specify dates and times using the calendar, time, and date tools available for the setting.
10. Follow the appropriate procedure for the actions performed by the policy:
    - **Metadata Assignments**: Specify the [user-defined or managed properties](#) to be assigned. Optionally, you can define Java expressions for fields in the policy that support them. Check the **Expression** checkbox to select this capability. The following fields support expressions:
      - Name
      - Description
      - Managed Properties (Key-Value Pairs)
      - User-defined Properties (Key-Value Pairs)
    - **Command Actions**: Select Add Action > Move to Trash or Add Action > Move. For a move, specify the location to move the entity to in the Target Path field. If you specify multiple actions, they are run in the order in which they are specified.
Command actions are supported only for HDFS entities. If you configure a command action for unsupported entities, a runtime error is logged when the policy runs.

See Viewing Command Action Status on page 17.

- **JMS Notifications**: If not already configured, configure a JMS server and queue. Specify the queue name and message. Optionally, check the Expression checkbox and specify a policy expression for the message.

11. Click Save.

**Viewing Policies**

**Required Role:** Policy Viewer (or Policy Editor, or Full Administrator)

1. Log in to the Cloudera Navigator console.
2. Click the Policies tab.
3. In a policy row, click a policy name link or select Actions > View. The policy detail page is displayed.

You can also edit, copy, or delete a policy from the policy details page by clicking the Actions button.

<table>
<thead>
<tr>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdfsImmediatePolicy</td>
</tr>
<tr>
<td>Status:</td>
</tr>
<tr>
<td>Search Query:</td>
</tr>
<tr>
<td>Policy Description:</td>
</tr>
<tr>
<td>Last Run On:</td>
</tr>
</tbody>
</table>

**Enabling and Disabling Policies**

As a policy administrator, you can manage access to policies by enabling and disabling them.

**Required Role:** Policy Editor (or Full Administrator)

1. Log in to the Cloudera Navigator console.
2. Click the Policies tab.
3. In a policy row, click a policy name link or select Actions > Enable or Actions > Disable.

**Copying and Editing a Policy**

If you have an existing policy that you want to use as a template for another similar property, you can copy it and then make any required adjustments. You can also edit existing policies if you need to make changes to it.

**Required Role:** Policy Editor (or Full Administrator)

1. Log in to the Cloudera Navigator console.
2. Click the Policies tab.
3. In a policy row, select Actions > Copy or Actions > Edit. You can also click the policy row and then on the policy details page, select Actions > Copy or Actions > Edit.
4. Edit the policy name, search query, or policy actions.
5. Click Save.

**Deleting Policies**

**Required Role:** Policy Editor (or Full Administrator)

1. Log in to the Cloudera Navigator console.
2. Click the Policies tab.
3. In a policy row, select Actions > Delete and OK to confirm.
Lineage

When it comes to making important business decisions, filing financial records, or complying with all manner of regulations, organizations need **verifiable** data. Public corporations in the United States must be able to prove to the IRS or to the SEC that values supplied in balance sheets and income statements are legitimate, for example. In pharmaceuticals research, data collected over multi-year clinical trials that may be combined with anonymous patient statistics must be able to be traced to data sources.

Cloudera Navigator lineage diagrams are designed to enable this type of verification. Lineage diagrams can reveal the **provenance** of data entities—the history of the data entity, back to its source with all changes along the way to its present form.

A **lineage diagram** is a directed graph that shows how data entities are related and how an entity may have changed over its lifetime in the cluster. Cloudera Navigator uses the metadata associated with entities contained in the cluster to render lineage diagrams that can trace data sources back to the column level and show relations and the results of transformations. See **Lineage Diagram icons** on page 153 for details about the line colors, styles, and icons used to render lineage diagrams, some of which are explained in the context of the examples below.

Using the Lineage View

For information about how lineage relationships are formed, see **Generating Lineage Diagrams** on page 49.

Exploring Lineage Diagrams

**Required Role:** [Metadata & Lineage Viewer](#) (or [Managed & Custom Metadata Editor](#), or Full Administrator)

Lineage diagrams are accessible in various ways in the Cloudera Navigator console. This example uses Search to first find a specific entity and then display its lineage diagram. Use this approach if you know the name, data type, source type, or another property value for a specific entity. The example uses the Hive sample data warehouse (installed by default) and assumes the following query has been run:

```sql
SELECT sample_07.description, sample_07.salary FROM sample_07
WHERE (sample_07.salary > 100000)
ORDER BY sample_07.salary DESC LIMIT 1000
```

The query returns values from `description` and `salary` columns for salaries over 100,000 from the `sample_07` table. Because Cloudera Navigator automatically collects metadata from entities, it can render lineage diagrams on any data contained in the cluster, including operations, such as the SELECT query of the example.

To display the lineage diagram based on this query in Cloudera Navigator console:

- Click the **Search** tab.
- Click **Hive** and **Operation** filters limit the scope of the search.
- Type the word `salary` or `sample_07` to find the query created above.
- Find the returned entity that contains the query and click on it to display its Details page.
- Click the query and then click the **Lineage** tab to display the lineage diagram.
The columns identified in the `select` clause use solid directed lines to the source table (shown with the Hive Table icon) and a dashed line to the source column of the `where` clause (shown with the Operation icon).

Expanding Entities

The example shows how one lineage diagram can expand to another. The first image shows a YARN operation (PigLatin:DefaultJobName) that runs an associated Pig script of the same name (DefaultJobName). The solid lines represent data flow relationships, from the source file (in the `ord_us_gcb_crd_crs-fdr-sears` folder) through the script execution, to the destination (in folder `tmp137071676`). The YARN operation PigLatin:DefaultJobName is rendered using a dashed (rather than solid) line because it is the starting point for this particular lineage diagram. In lineage diagrams, lines change to the color blue when they are selected. Containment is signalled using the plus icon:

Click the plus icon to expand a parent entity and display child entities. For example, expanding the Pig script reveals the two Pig tables (ACT_FILE, ACT_FILE_COL_CNT_ERR_ROWS) referenced by the script. The solid directional line between the two tables indicates the data flow relationship between these two tables.

Adjusting the Lineage Layout for Readability

Lineage diagrams displayed in the Cloudera Navigator console can be manipulated by as follows:

- Click and drag entities outside their parent boxes.
- Use the plus-minus control displayed in the lineage diagram or the mouse scroll wheel to expand and shrink (zoom in, zoom out) the image size
- Relocate the lineage diagram within the pane using click-hold-drag gesture.
Filtering Lineage Diagrams

Lineage diagrams can render faster when filters are applied. Filters can limit or specify the entities displayed.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Lineage Options default selection applies the Latest Partition and Operation filter, which displays only the most recent partitions and operations. For example, if Hive partitions are created daily, the filter displays only the latest partition.</td>
<td><img src="image" alt="Lineage Options" /></td>
</tr>
</tbody>
</table>

**Note:** This filter applies only to metadata collected with Navigator Metadata Server installed with Cloudera Manager version 5.12 or later. Operations against multiple partitions that were collected by earlier versions will not collapse into a single partition.

![Lineage diagram of the sample_09 table filtering deleted items only.](image)  

**Control Flow Relations.** The operation is collapsed and control flow links are hidden.

![Control Flow Relations](image)
<table>
<thead>
<tr>
<th>Filter</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Only Upstream</strong> filter displays only input (upstream) entities and links. The <strong>Only Downstream</strong> filter displays only output (downstream) entities and links. The operation is collapsed and only upstream (or downstream) entities and links display. The output table is hidden.</td>
<td></td>
</tr>
<tr>
<td><img src="image1" alt="Diagram" /></td>
<td><img src="image2" alt="Diagram" /></td>
</tr>
<tr>
<td>Here, the operation is collapsed and only downstream entities and links are shown. The input tables are hidden.</td>
<td><img src="image3" alt="Diagram" /></td>
</tr>
<tr>
<td>The <strong>Operations</strong> filter collapses operations into green links between entities.</td>
<td><img src="image4" alt="Diagram" /></td>
</tr>
<tr>
<td>The <strong>Deleted Entities</strong> filter displays entities that have been deleted but maintains relations to other entities.</td>
<td><img src="image5" alt="Diagram" /></td>
</tr>
</tbody>
</table>
Exploring Hidden Entities in a Lineage Diagram

Lineage diagrams use the **hidden icon** to indicate areas in the diagram available for further exploration. The basic mouse gestures to use to traverse a lineage diagram with hidden information are as follows (there are many alternative approaches, including simply double-clicking the hidden icon):

1. Hover over the hidden icon (note the hand floating at the top of the hidden icon) to display an information text (box, upper-right) with the link that provides access to lineage for the additional entities.

2. Click the hidden icon to select it.
3. Click the **view the lineage** link to display a new lineage diagram contained at that intersect point. The green line is a summary line that contains

   ![Lineage Diagram Example](image)

   This shows that the **sample_08** table is actually contained in a folder, **sample_08**.

Finding Specific Entities in Lineage Diagrams

Cloudera Navigator’s Search function can be used in the context of an open lineage diagram. This is useful especially when lineage diagrams have hidden entities that are may not be visible.

1. In the **Search** box at the right of the diagram, type an entity name. A list of matching entities displays below the box.
2. Click an entity in the list. A blue box is drawn around the entity and its details display in a box below the Search box.
3. Click the **Show** link next to the entity. The selected entity moves to the center of the diagram.

4. To view the lineage of the selected entity, click the **View Lineage** link in the entity details box.

---

**Displaying a Template Lineage Diagram**

A **template lineage diagram** contains template entities, such as jobs and queries, that can be instantiated, and the input and output entities to which they are related.

To display a template lineage diagram:

1. Perform a metadata search.
2. In the list of results, click an entity. The entity Details page displays. For example, when you click the **sample_09** result entry:

![Hive sample_09](image)

the Search screen is replaced with a Details page that displays the entity property sheet:

- **Technical Metadata**
  - Source Type: Hive
  - Type: Table
  - Parent Path: /default
  - Path: `https://nightly1-1.gos.cloudera.com:8020/user/hive/warehouse/sample_09`
  - Compressed: true
  - SerDe Library: org.apache.hadoop.hive.serde2.jaxb.La...
  - Input Format: org.apache.hadoop.hive.serde2.TsvInputF...
  - Output Format: org.apache.hadoop.hive.serde2.HiveRowSer...
  - Owner: admin
  - Created: Mar 18 2016 10:15 AM
  - Source: Hive
  - Class Name: hive.table
  - Package Name: new

- **Managed Metadata**
  - No metadata available

- **Custom Metadata**
  - No metadata available

3. Click the **Lineage** tab. For example, clicking the Lineage tab for the sample_09 table displays the following lineage diagram:

![Lineage Diagram](image)

This example shows the relations between a Hive query execution entity and its source and destination tables:

- **Click the plus icon to display the columns and lines connecting the source and destination columns display:**
Displaying an Instance Lineage Diagram

An instance lineage diagram displays instance entities, such as job and query executions, and the input and output entities to which they are related. To display an instance lineage diagram:

1. Perform a search and click a link of type Operation.
2. Click a link in the Instances box.
3. Click the Lineage tab.

Displaying the Template Lineage Diagram for an Instance Lineage Diagram

To browse from an instance diagram to its template:

1. Display an instance lineage diagram.
2. Click the Details tab.
3. Click the value of the Template property to go to the instance’s template.

Using Lineage to Display Table Schema

Required Role: Metadata & Lineage Viewer (or Managed & Custom Metadata Editor, or Full Administrator)

A table schema contains information about the names and types of the columns of a table.

Displaying Hive, Impala, and Sqoop Table Schema

1. Use the Cloudera Navigator console to search for entities of source type Hive and type Table.
2. In the list of results, click a result entry. The table schema displays in the Details tab.

Displaying Pig Table Schema

1. Use the Cloudera Navigator console to search for entities of source type Pig.
2. In the list of results, click a result entry of type Table. The table schema displays in the Details tab.
Generating Lineage Diagrams

Navigator Metadata Server uses the metadata it collects to generate lineage graphs. These graphs tell you what data and processes were used to generate a given data asset.

This documentation describes

- Where the lineage information comes from
- How the lineage varies based on the source of the metadata
- Life cycle of lineage info as assets change on the cluster

Lineage Generation Architecture

Navigator Metadata Server collects metadata from CDH services, creates records in Solr for each of the data assets and operations, then uses the operation metadata to build relations among the data assets. You see the relations among data assets in the Navigator Console as a lineage graph. Here’s the process in a little more detail:

1. Extractors collect metadata from services in the cluster.

   The extractors are components within Navigator that communicate with each service that Navigator supports. For example, for Navigator Metadata Server to collect HDFS metadata, the Navigator HDFS extractor talks to the namenode to request file system information.

   There are two types of extractors:

   - Pull extractors (CDX, HDFS, YARN, Oozie, HMS). The extractor requests metadata from the service about every 10 minutes, assuming there is not already an extraction in progress. The CDX extractor pulls metadata from S3.
   - Push extractors (Spark, Impala, Hive Server 2, Sqoop). The service saves metadata to the local file system for every operation; the Cloudera Manager agent running on the same host passes the metadata to Navigator Metadata Server about every five seconds.

   For more information about how the timing of push and pull extractors affects when lineage appears in the Navigator console, see Metadata Extraction Timing on page 101.
2. Navigator indexes each data asset and operation.
   For each new data asset and operation it finds in the extracted metadata, Navigator Metadata Server creates an entry in its Solr index. These entries appear in nav_elements core. The most recently extracted metadata is always used to update any existing entity entry. In addition, Navigator Metadata Server creates a nav_relation entry in the Solr index to store relationship information, such as between a directory and a file or subdirectory or between a table and the directory backing it. Navigator saves a variety of relationship information:
   - Logical - physical: Hive table and the HDFS directory that contains the data.
   - Instance of: Operation and operation execution.
   - Data flow: Query operation that refers to input or output tables.
   - Control flow: Column level details in an operation that refers to specific column or field details in a table, view, or file.
   If Navigator doesn’t have all the information it needs to fill in both ends of a relationship, it creates an "unlinked" relation. For example, when an HMS table is extracted, but the corresponding HDFS directory is not already in the index, Navigator will create an unlinked relation for the table that will be filled in later with the directory metadata.

3. Linker fills in missing relation endpoints.
   After it receives metadata from an extraction, Navigator Metadata Server runs a process ("linker") that uses the new metadata to fill in unlinked relations.

4. Navigator console displays the relations as a lineage diagram.
   The Navigator console reads nav_relation to show entity relationships in a directed graph, where the graph flows from input to output, left to right. You can choose how much detail you want to see in the graph, including showing the operations that give details on how data was transformed.

   The entities shown in a lineage picture are determined by the service where the metadata came from. The lineage for data assets includes other data assets and the operations that relate them; lineage for query and compute operations include existing data assets used as inputs or outputs.

   For more about how to use the lineage view to show more information, see Exploring Lineage Diagrams on page 41.

Lineage Life-cycle
   The contents of a lineage diagram are determined by what metadata is extracted from services. If an object doesn't exist when the extraction occurs, it will not be reflected in the lineage diagram.

Metadata extraction timing
   For pull extractors, Navigator triggers metadata extraction for each type of extractor every 10 minutes. Push extractors work differently: instead of waiting for Navigator to ask for the metadata, the services write out metadata when an event occurs; the Cloudera Manager agent on the host polls every 5 seconds and forwards whatever metadata it finds.
to Navigator Metadata Server. The extractor operations run until the extractor processes all the metadata provided by the service; an extraction could be running for minutes or hours depending on the volume of metadata being extracted.

Navigator runs the linking process after each extractor completes processing an extraction. The linking process can also take minutes or hours, depending on the volume of data being processed.

**Deleted data assets**

Each metadata extraction from a service is a snapshot of the objects managed by that service at a given time. If one extraction includes a reference to a specific table and the following extraction does not, Navigator Metadata Server flags the entity for that table as deleted. These relations are hidden in lineage diagrams. You can show them again by enabling the Deleted Entities in the lineage view options. The deleted entities are indicated with a line through their name.

**Metadata Purge and Lineage**

Metadata purge reviews lineage relations where at least one endpoint of the relation is a candidate for removal. A data asset entity would be flagged as deleted; operation executions would have to have been executed earlier than the purge threshold date. What gets purged is slightly different among the different types of objects. See [What Metadata is Purged?](#) on page 72 for purge details. Here’s how purge affects lineage:

- "Instance of" relations between operation and operation executions are removed when the operation execution was executed earlier than the threshold date for purge.
- Data flow relations for operations are removed when:
  - The operation doesn't have an output entity; that is, the operation does not produce a table or view or other entities produced by Sqoop jobs or associated with Pig tables.
  - The associated operation executions are older than the purge threshold date.
- Parent child relations between HDFS files and their parent directory are only removed when the directory has been flagged as deleted longer than the purge threshold date.

The following items are not affected by purge:

- Hive tables and the operations that produce them are never removed, even if the tables were deleted before the purge threshold date.
- Logical-physical relations between Hive tables and HDFS directories are not removed, even if the tables were deleted before the purge threshold date.

**Temporary data assets**

Sometimes operations include data assets that are created and then deleted as part of the operation (or as part of a series of operations that occur close together in time). These temporary objects may or may not be captured as part of a Navigator pull extraction. The operation that produced the object is likely be extracted through a push extractor. When temporary objects are not captured, Navigator Metadata Server produces an unlinked relation based on the operation metadata. The technical metadata for the operation, such as query text, includes a reference to the temporary object; the object itself will not be listed in the Navigator console and will not appear in lineage diagrams.

For example, consider a Hive pipeline that writes data to a table, transforms the data and writes it to a second table, then removes the first table. The lineage content is different depending on whether or not metadata extraction captured the temporary table before it was dropped.

If the Navigator-HMS extractor runs when the first table was present, Navigator will create a metadata entity for the first table. When Navigator links the details of the operation with known entities, it will translate the operation details into a lineage diagram including the first and second tables. After the table is deleted and when the next extraction
runs, Navigator Metadata Server flags the entity for the first table as deleted. The lineage diagram for the second table shows the first table as deleted (you may have to enable Deleted Entities in the lineage view options). The operation and operation executions still show in the lineage diagram.

**If the first table is created and deleted between Navigator-HMS extractions,** no metadata entity is created for the table, and the operation details don't link up to an existing entity as an operation input (unlinked relation). If you look at the lineage diagram for the second table and turn on the option to show operations, you'll see the operation that created the second table, but you won't see the first table. In the lineage view, you can see the query run by the operation. That query text shows the first table in the FROM clause.

**Example of lineage across temporary tables**

This example shows how the lineage diagram changes depending on whether a temporary table was included in a metadata extraction. The following Impala queries were run in Hue to create temporary tables (temp_sample_07 and temp_sample_08), then use those tables to load data into a third table (sample_merge):

```
1 CREATE TABLE temp_sample_07 AS SELECT * FROM sample_07;
2 CREATE TABLE temp_sample_08 AS SELECT * FROM sample_08;
3 CREATE TABLE merge_sample AS SELECT * FROM temp_sample_07;
4 INSERT INTO merge_sample SELECT * FROM temp_sample_08;
5 DROP TABLE temp_sample_08;
6 /* delay until after Navigator metadata extraction occurs */
7 DROP TABLE temp_sample_07;
```

Assume that the temp_sample_08 table was created and dropped between two metadata extractions and that the temp_sample_07 DROP TABLE command is run only after metadata extraction occurred.

After extractions are run and linking occurs, the lineage picture for the sample_merge table shows an "upstream" relationship with sample_07.

After turning on the option for **Deleted Entities**, the temporary table temp_sample_07 appears. It exists in the system because it was captured by the first metadata extraction and then it was deleted by the second extraction.
Turning on the option for **Operations** shows the queries that created and inserted rows into the `sample_merge` table. Note in particular that the operation shows for inserting data into the `sample_merge` table from the temporary table `temp_sample_08` even though the table was not captured by a metadata extraction.

If you select the insert operation, you can see the query details to identify the operation input.
If you wanted to further trace the origin of the temporary table, you can use the table name to search for operations that affected the temporary table by searching on the query text:

```markdown
queryText:*temp_sample_08*
```

**Lineage Behavior by Service**

Lineage graphs follow some rules based on the kinds of metadata provided by services. This section describes how the metadata is formed into relations; the conventions for how the relations are displayed on the lineage diagram as listed in [Lineage Diagram Icons](#) on page 153. For a list of the specific operations that produce entities in Navigator, see [Service Metadata Entity Types](#) on page 167.

**Hive, Impala**

Lineage is generated for (most) operations against the Hive Metastore that create data assets or modify data, including operations from HiveServer2, Impala, and Impala queries on Kudu tables. Lineage is not produced for operations performed using the Hive Server 1 CLI. For a list of the specific operations captured by Navigator extractors, see [Hive Operations and Cloudera Navigator Support Matrix](#) on page 167.

For each query operation, a relation is created for each data asset referenced as an input or output (or both) in the query. The lineage diagrams include tables, views, and operations. The metadata indicates whether the data asset is an input or output.
Figure 1: Impala Lineage

The query information provided by Hive Metastore (HMS) includes query information that allows Navigator to show data assets referenced in joins or lookups. You can see these tables when you turn on Control Flow Relations.

Figure 2: Lineage Showing Control Flow Relations

When Navigator has column level information, the lineage diagram shows a + next to the name of the object. Opening the column level information shows you how columns in source tables contribute to columns in the destination tables. Columns referenced in joins or lookups are indicated with dashed lineage relations and appear when the view includes control flow information. (Move the cursor over a column to highlight only that column’s lineage through all the objects.) Because the information is generated by HMS, column-level tracing is available regardless of the underlying compute engine.
Only database-layer objects appear in the lineage for query services: Navigator doesn’t show the logical-to-physical relationships such as the backing HDFS directory for each Hive table. If you want to know the location of the underlying HDFS files for a table, you can see this information in the `Path` property of the technical metadata for the table. Note that lineage shown for an HDFS file or directory, you will see the logical-to-physical relationship to Hive tables or views.

Only operations that include output appear in lineage for tables and views. To see a lineage diagram for operations such as SELECT that do not produce a data asset, view lineage for the operation. To see all such activity run against a specific table, you may find it useful to go the `Audits` tab in the Navigator console and filter on the table name.

Lineage for query services does not expose the compute engine used to perform the query; Hive operations appear the same whether they are run on MapReduce or Spark. This information is available in the technical metadata for the operation execution. Note that queries run directly in Spark are different because Spark provides different metadata than HMS.

**HDFS, S3**

Navigator collects metadata for file system entities. It does not collect metadata for file-system level operations, such as moves or copies. Lineage metadata appears when applications perform operations against file-system entities. For example, when a Spark job copies an HDFS directory, the lineage diagrams show the relationship between the source directory and the copied directory as connected by the Spark operation.

When HDFS directories are used as backing data for tables managed in Hive Metastore (including Impala tables), the lineage for the directory and any of the files included in the directory will show a logical-physical relation to the table.

**Figure 4: Logical Physical Relationship between HDFS File and Hive Table**

**MapReduce, Spark, Sqoop**

Navigator shows lineage diagrams for operations performed by compute engines such as MapReduce v1, YARN (MRV2), or Spark (all Spark 1 versions and Spark 2 starting with version 2.3). Lineage reflects data processed using Spark SQL, including the Datasets/Dataframe APIs. Other services such as Apache Sqoop contribute metadata that Navigator can use to create lineage diagrams as well.

For compute operations, a relation is created for each data asset referenced as an input or output (or both) in the operation. As in this image, the input and output relations are shown with arrows.
Data assets that are used for both output from and input to stages of the operation appear with two lineage lines, one with an arrow pointing into the entity; another pointing out. In the Navigator lineage diagram, entities that are both input and output to the same operation may be shown parallel to the operation rather than on the left or right.

The Navigator extractors for MapReduce and Spark services trace data lineage at the application level only. The result is that when you show the lineage diagram for a single column in a table that is affected by a Spark operation, the diagram shows other data assets that contribute to the column, but how the specific columns inside those assets contribute to the selected column is not shown.

Navigator shows all the lineage information available for Spark operations, but does not include SQL statements executed in Spark. This limitation is because Spark does not keep the SQL statement: the Spark parser creates the plan from the SQL statement and, from that point on, the SQL statement provided by the client is not retained as part of the metadata associated with the Spark job. For many Spark operations, SQL isn't part of the original request. For example: `spark.read.parquet("/input").write.parquet("/output")` generates lineage, but there is no SQL statement used at all.
Lineage diagrams differ slightly between Spark 1 and Spark 2 operations. In Spark 1, table creation commands are not captured as a lineage relation: when a table is created and then used by another command, the table appears only as an input to the operation. In Spark 2, table creation commands are captured: the table shows as an output (creation) and an input to the operation.

YARN, Oozie

Lineage for resource management operations, such as YARN and Oozie, include lineage relations to other operations; the metadata for YARN and Oozie entities does not reveal specific data assets touched by the processing.

Navigator shows lineage diagrams for operations performed by resource management tools such as Oozie and YARN. Relations are created for each operation controlled by job managers. These lineage diagrams show processing stages, but do not show the individual data assets affected by the operations.

When a YARN job runs a Hive query, the Navigator lineage diagram exposes the logical-to-physical relationships between Hive tables and the backing HDFS directories. The resource management through YARN appears in parallel to the data flow for Hive.

As described for compute services, jobs that run MapReduce or Spark operations report different metadata to Navigator, so the lineage diagrams look different from query processing.
Troubleshooting Lineage

When you don't see the lineage relations you expect, look for the following possible issues:

**Give time for extractors to run**

Pull extractors run every ten minutes assuming the previous run completed. For large data sets, the extractor process may require more time to run. In addition, if there are connectivity issues or if the corresponding service is busy or not available, the extraction time can lengthen. For HMS in particular, the actual time required to extract all the metadata required to draw new lineage relations can be as much as an hour if the multiple extractors involved run offset from each other.

**View lineage from the appropriate entity**

If you want to see a logical-physical relation between an HDFS directory and a Hive table, you need to access lineage from the HDFS directory.

If you want to see all the times a query is run against a Hive table you may not see it in the Hive table lineage; if the operation doesn't produce output, access the lineage from the operation, not the Hive table.

**Are extractors running successfully?**

Navigator won't show lineage information if it's not receiving it. Check to make sure that the extractor is running properly:

- Check the Navigator Metadata Server log for errors that would indicate that an extractor isn't running.

  You can access Navigator Metadata Server logs from Cloudera Manager or from the command line on the host where the service is running. See Accessing Navigator Data Management Logs on page 76.

  Extractor status messages include the word "extractor", such as com.cloudera.nav.hive.extractor.HiveOperationExtractor.

- Check Cloudera Manager agent log to find out more detail about an error.

  If you find an error in the Navigator Metadata Server log that indicates a problem with one of the push extractors, go to the Cloudera Manager agent log for the host indicated by the log error.
Cloudera Navigator Business Metadata

Cloudera Navigator lets organizations catalog data contained in Hadoop clusters. With data entities in the cluster tagged with relevant metadata properties, data stewards can provide curated datasets, business users can do their own self-service discovery, and system administrators can develop effective archival strategies.

The Navigator Metadata Server is the role instance that provides the metadata definition, tagging, and management system. Any given entity can be identified by one or more of the three different classes of metadata.

Cloudera Navigator console lets you view metadata through various dashboards, such as the Data Stewardship Dashboard and Data Explorer, that provide at-a-glance views of cluster assets.

This section focuses on the HDFS Analytics menu of the Cloudera Navigator console.

Three Different Classes of Metadata

Cloudera Navigator supports extraction of three different types of metadata from the data contained in the cluster. The characteristics of each type are summarized in the table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Usage Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Metadata</td>
<td>Characteristics inherent to the entity that are obtained when extracted.</td>
<td>Not modifiable.</td>
</tr>
<tr>
<td>Managed Properties</td>
<td>Key-value pairs that can be defined once and applied globally to specific entity types. Properties are defined within namespaces, and values can be constrained by type (such as Text, Number, Boolean, Date, Enumeration).</td>
<td></td>
</tr>
<tr>
<td>User-defined Properties</td>
<td>Tags and key-value pairs that can be added to entities before or after extraction. When users create these properties, they are one-off instances of metadata for an entity. If your organization finds these properties useful, consider defining a managed property instead and take advantage of the structure provided by that metadata type.</td>
<td>Recommended that you use managed properties.</td>
</tr>
</tbody>
</table>

The screenshot below (from the Cloudera Navigator console) shows the details of a web log saved to HDFS as a comma-separated value (CSV) file. This particular entity has all three types of metadata associated with it:

- The technical metadata was extracted from the source system, in this example, HDFS.
- The managed properties were defined by a data steward from the Finance department to augment entities processed by the system with properties that enable self-service data discovery for cluster data. That is, business users looking for data handled by the Finance department can more easily locate files that have been labeled with these properties.
- Tags have also been applied to this file.
Technical metadata is obtained from the source entity and cannot be modified. Common examples of technical metadata include an entity's name, type (directory or file, for example), path, creation date and time, and access permissions. For entities created or managed by cluster services, technical metadata may include the name of the service that manages or uses that entity and relations—parent-child, data flow, and instance of—between entities.

For example, for Hive entities, Cloudera Navigator extracts the extended attributes added by Hive clients to the entity. As another example, technical metadata for an Amazon S3 bucket includes Bucket name, Region (AWS Region, such as us-west-1), S3 Encryption, S3 Storage Class, S3 Etag, Source (S3), and so on. Technical metadata is simply whatever metadata is provided for the entity by the system that created the entity.

### Viewing Metadata Analytics

**Required Role:** [Metadata & Lineage Viewer](#) and [Policy Editor](#) (or Full Administrator)

1. Open your browser.
2. Navigate to the host within the cluster running the Navigator Metadata Server role as shown in this example (7187 is the default port for Navigator Metadata Server):

   ```
   http://fqdn-1.example.com:7187/login.html
   ```

   The login page displays.
3. Log in to the Cloudera Navigator console using the credentials assigned by your administrator.
4. Click the Analytics tab. The Metadata analytics tab displays.
5. Click the Source button and select an HDFS service instance from the drop-down list.
6. The Metadata tab displays a set of bar graphs that list the number of files that satisfy groups of values for last access time, created time, size, block size, and replication count.
   - To display the files at the right, click a bar. This draws a blue selection outline around the bar and selects the property checkbox.
   - To select more than one value, grab a bar edge and brush a range of values.
   - To change a range, click a bar, drag to a different range of values, and then drop.
   - To reduce a range, grab a bar edge and contract the range.
   - To clear a property, clear the checkbox. The previous selection is indicated with a gray outline.
   - When you select a previously selected property, the previous selection is reused. For example, if you had previously selected one and three for replication count, and you reselect the replication count checkbox, the values one and three are reselected.
   - To clear all current and past selections, click Clear all selections.
7. In the listing on the right, select an option to display the number of files by directory, owner, or tag. In the listing:
   - Filter the selections by typing strings in the search box and pressing Enter or Return.
   - Add categories (directory, owner, or tag) to a search query and display the Search tab by doing one of the following:
     - Clicking a directory, owner, or tag name link.
     - Selecting Actions > Show in search. To further refine the query, select one or more checkboxes, and select Actions > Show selection in search.
   - Required Role: Policy Editor (or Full Administrator)
   Add categories to the search query of a new policy and display the Policies tab by selecting Actions > Create a policy. To further refine the query, select one or more checkboxes, and select Actions > Create a policy from selection.

Defining Managed Properties

Required Role: Metadata Administrator (or Full Administrator)

You can add metadata to classes of entities as managed properties. A namespace is a container for properties. Four namespaces are reserved:

- nav for Navigator metadata classes (for example, fselement and user-defined fields)
- up (user-defined properties)
- tp (technical properties)
- xt (partner applications)

The combination of namespace and property name must be unique.

Note: The Cloudera Navigator console cannot delete namespaces. Empty namespaces can be deleted using the Cloudera Navigator APIs.

A property can be one of the following types:

- Boolean
- date
- integer
- long
- float
A property can be single-valued or assume multiple values.

After metadata properties have been assigned to specific entities in the cluster, the property types and values can be used as filters for Cloudera Navigator Search, to find specific entities.

Creating User-defined Properties with the Cloudera Navigator Console

To create user-defined properties:

1. Log in to the Cloudera Navigator console.
2. Click the Administration link in the upper right. The Managed Properties tab displays the list of namespaces and the properties defined in the namespaces.
3. Click the New Property... button.
4. In the Classes field, click the filter icon ( ) or start typing one of the Cloudera Navigator entity built-in class names.
5. Select the class of entities to which the property applies. To clear the field, hover over the field and click the delete icon (x) that displays at the right of the field.
6. Click the Namespace field and select a namespace. If the Namespace drop-down list is empty, click Create Namespace....
   a. Specify a namespace name and optional description.
   b. Click Continue.
7. Add the name for the property.
   The name can contain letters, numbers, underscores, and hyphens and can be up to 50 characters long.
8. Specify an optional description.
9. Select the Multivalued Enable checkbox if the property can have more than one value. For example, an emailFrom property should accept only one value, but an emailTo property could accept more than one value.
10. In the Type drop-down list, select the property type and specify constraints on the value.
    • Boolean - Boolean: true or false.
    • Date - Date and time.
    • Enumeration - A set of values. In the Enumeration field, type valid enumeration values and press Enter or Tab.
    • Number - A number. In the Number Type field, select the type of the number: Integer, Long, Float, Double.
    • Text - A string.
      – Maximum Length - The maximum length of the string.
      – Regular Expression - A regular expression that determines whether a string is a valid value. You can test the expression by clicking Show regex tester and entering input that you expect to match the expression.

If you change the regular expression, click outside the field to trigger the tester to re-evaluate the expression.
11. Click **Continue to Review**. The Review screen displays.
12. Click **Create** to create the property, **Cancel** to return to the Properties page, or **Back to Edit Property** to continue editing the property.

**Example Properties**

The following figure shows two properties in the namespace MailAnnotation that apply to entities of the HDFS Entity class (HDFS files and directories). The emailFrom property is of type TEXT and can be assigned a single value. The MailTo property is also of type TEXT but can have multiple values.

**Properties**

See the documentation before creating or modifying properties.

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Type</th>
<th>Classes</th>
<th>Multivalued</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MailAnnotation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EmailFrom</td>
<td>Active</td>
<td>Text</td>
<td>HDFS Entity</td>
<td>No</td>
<td>Actions</td>
</tr>
<tr>
<td>EmailTo</td>
<td>Active</td>
<td>Text</td>
<td>HDFS Entity</td>
<td>Yes</td>
<td>Actions</td>
</tr>
</tbody>
</table>

**Using Cloudera Navigator Console to Manage Properties**

You can view managed property summary details by clicking property name in the Properties table, or from Actions > View.

You can also edit some aspects of a property, delete and restore a property, and purge deleted properties.

**Editing a Property**

After a property is created, you can edit property data in the following ways:

- Add **classes** to which the property applies
- Add and remove enumeration values
- Change the description
- Change the maximum length
- Change the regex pattern

1. Log in to the Cloudera Navigator console using administrator credentials roles:
   - Cloudera Manager Full Administrator
   - Cloudera Manager Navigator Administrator
   - Cloudera Navigator Full Administrator
   - Cloudera Navigator Metadata Administrator

2. Click the Administration link in the upper right. The Managed Metadata tab displays the list of namespaces and the properties defined in the namespaces.

3. Open the property Edit page by clicking the Actions box in the property row and then clicking **Edit** in the dropdown.

4. In the Additional Class field, click the or type the name of a Cloudera Navigator **class**. For example, start typing "Hive.." to see

5. Select the class of entities to which the property applies. To clear the field, hover over the field and click the delete icon (x) that displays at the right of the field.

6. In the Description field, add a description or edit an existing description.

7. If the property is of the Enumeration type, you can add or remove values in the Enumeration field.
8. For Text properties:
   - In the Maximum Length field, add or change the value for the maximum length.
   - In the Regular Expression field, edit the expression. Click Show regex tester to test input against any changes you make.

9. Click **Continue to Review**. The Review screen displays.
10. Click **Update** to commit the change or **Back to Edit Property** to continue editing the property, or **Cancel** to return to the Properties page.

Deleting, Restoring, and Purging Managed Properties

After a property is deleted, it cannot be assigned to entities. However, the property still exists and the entities that have already been associated with the property retain the property (and value) until the Purge Deleted Properties operation is run.

Deleted properties display status as Deleted in the Cloudera Navigator console (on the Managed Properties tab of the Administration menu). For example, the EmailFrom property has been deleted:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Type</th>
<th>Classes</th>
<th>Multivalued</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailFrom</td>
<td>Deleted</td>
<td>Text</td>
<td>HDFS Entity</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>EmailTo</td>
<td>Active</td>
<td>Text</td>
<td>HDFS Entity</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

The Status displays only to users with the Navigator Administrator or Managed & User-defined Properties Editor user roles.

The Cloudera Navigator Purge Deleted Properties operation permanently removes the deleted properties and their values from all entities. Policies that assign metadata using a property that has been purged will fail the next time they are run. Because deleted properties are not removed from the system until they have been purged, the name of any deleted property cannot be re-used until after purging deleted properties.

Deleting a Property

1. In the Properties table, for the property that you are deleting, click the **Actions** button, and then click **Delete** in the drop-down menu.
2. In the Delete Property dialog box, review the property deletion information. If any entities are affected, you see a **View affected entities** link; click to see all entities that use the property.
3. Click **Confirm Delete** to delete the property, or click **Cancel**.

Restoring a Property

If you have not yet purged a deleted property, you can restore it.

- In the Properties table, for the property that you are restoring, click **Actions** > **Restore**.

Purging a Property

You can permanently remove deleted properties by running the Purge Deleted Properties operation. Purging permanently removes all properties marked as Deleted in the Status column. It removes the property and its value(s) from any entity it has been associated with. Other metadata for the entities are not affected.
Note: When you run a Purge Deleted Properties operation, it stops all other non-purge Navigator tasks and runs immediately. Tasks that are stopped are restarted from the beginning when the purge operation completes. Navigator is unavailable to users or API calls until the purge operation completes.

1. In the Properties table, click Purge Deleted Properties. The Purge all Deleted Properties dialog box opens, describing the effects of the purge and reporting the number of entities that use the property.

   If the Purge Deleted Properties option isn't available, it may be that there is already a purge task running, such as a scheduled metadata purge operation. When the currently running purge task completes, the option will be available again.

2. In the Purge all Deleted Properties dialog box, click Confirm Purge to permanently remove all deleted properties, or click Cancel to return to the Properties page.

### Navigator Built-in Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS Dataset</td>
<td>Logical dataset backed by a path in HDFS.</td>
</tr>
<tr>
<td>HDFS Dataset Field</td>
<td>Field in an HDFS dataset.</td>
</tr>
<tr>
<td>HDFS Entity</td>
<td>HDFS file or directory.</td>
</tr>
<tr>
<td>Hive Column</td>
<td>Column in a Hive table.</td>
</tr>
<tr>
<td>Hive Database</td>
<td>Hive database.</td>
</tr>
<tr>
<td>Hive Partition</td>
<td>Partition of a Hive table.</td>
</tr>
<tr>
<td>Hive Query</td>
<td>Hive query template.</td>
</tr>
<tr>
<td>Hive Query Execution</td>
<td>Instance of a Hive query.</td>
</tr>
<tr>
<td>Hive Query Part</td>
<td>Component of a Hive query that maps specific input columns to output columns.</td>
</tr>
<tr>
<td>Hive Table</td>
<td>A Hive table.</td>
</tr>
<tr>
<td>Hive View</td>
<td>View on one or more Hive tables.</td>
</tr>
<tr>
<td>Impala Query</td>
<td>Impala query template.</td>
</tr>
<tr>
<td>Impala Query Execution</td>
<td>Instance of an Impala query.</td>
</tr>
<tr>
<td>Impala Query Part</td>
<td>Component of an Impala query that maps specific input columns to output columns.</td>
</tr>
<tr>
<td>Job Instance</td>
<td>Instance of a MapReduce, YARN, or Spark job.</td>
</tr>
<tr>
<td>Job Template</td>
<td>Template for a MapReduce, YARN, or Spark job.</td>
</tr>
<tr>
<td>Oozie Workflow</td>
<td>Template for an Oozie workflow.</td>
</tr>
<tr>
<td>Oozie Workflow Instance</td>
<td>Instance of an Oozie workflow.</td>
</tr>
<tr>
<td>Pig Field</td>
<td>Field for a relation in Pig; similar to a column in a Hive table.</td>
</tr>
<tr>
<td>Pig Operation</td>
<td>Template for a Pig transformation.</td>
</tr>
<tr>
<td>Pig Operation Execution</td>
<td>Instance of a Pig transformation.</td>
</tr>
<tr>
<td>Pig Relation</td>
<td>Pig relation; similar to a Hive table.</td>
</tr>
<tr>
<td>S3 Bucket</td>
<td>A bucket in S3.</td>
</tr>
</tbody>
</table>
### Defining Metadata with the Navigator API and Navigator SDK

In addition to accessing and defining metadata with the Cloudera Navigator console, you can also use the Cloudera Navigator API and the Navigator SDK.

For information on the Navigator API, see Cloudera Navigator APIs on page 139.

The Navigator SDK is a client library that can be used to extract metadata directly from Navigator Metadata Server or to enrich metadata with managed property models, user-defined properties and tags, entities, and relationships. The SDK is located in Github in the cloudera/navigator-sdk repository.

### Adding and Editing Metadata

**Required Role:** Metadata Administrator (or Full Administrator)

Cloudera Navigator provides two different types of metadata that can be applied to entities extracted from the cluster:

- **Managed properties** consists of the comprehensive organization-wide labeling scheme typically set up by data stewards to provide centralized, curated data sets. Different namespaces can be created for different departments, functional groups, or data type, or any categorization scheme needed, and each namespace contains the key-value pairs that are used to tag entities. Values can be constrained by data type (text, number, boolean, date, enumeration, for example). Values for managed properties can be applied to entities after extraction (not before), and can be applied automatically by using the API or configuring the Navigator Metadata Server to apply policies.

- **User-defined properties and tags** consists of key-value pairs or labels (tags) that users define on an ad hoc basis. These unmanaged properties can be applied to entities before and after extraction. Because this kind of metadata is not centrally managed for content and consistency, we recommend that you use managed properties as often as possible and leave user-defined metadata for individual or occasional use.

### Editing Metadata Using the Cloudera Navigator Console

1. Log in to the Cloudera Navigator console.
2. Search for any entity in the Cloudera Navigator console.
3. Click an entity link returned in the search. The Details tab displays.
4. Access the metadata you want to edit:

   You can view and change all of the business metadata from Actions > Edit Properties... at the top of the Details tab.
   Alternatively, click Edit in one of the metadata sections lower in the page.
5. Add metadata fields:

- In the Name field, type a new display name. This change does not modify the physical name of the data asset.
- In the Description field, type a description (500 characters maximum).
- Select a Managed Property to add the value appropriate for this entity. Click the plus icon (+) to add another managed property key-value pair or another value for a given key.
- Enter a User-defined Property or Tag.

You can specify special characters (for example, ",", "$") in the property name or tag, but it makes searching for the entity more difficult because some characters collide with special characters in the search syntax.

User-defined Properties

In the following example, the tag `archive_personal` and the property `year` with value `2015` are added to the HDFS directory `2015_11_20`:

After you save, the metadata appears in the User-defined Property pane:

Managed Properties

The following example shows the Department and Retain Until managed properties for the customers Hive table entity:
After you specify the values and save, the properties display in the Managed Properties pane:
Administration (Navigator Console)

The Cloudera Navigator console provides an Administration menu for several different tasks, including setting up a schedule to remove stale and deleted metadata from the system ("purge"), setting up users and groups, and defining managed properties.

For information on defining managed properties, see Defining Managed Properties on page 62.

Managing Metadata Storage with Purge

The volume of metadata maintained by Navigator Metadata Server can grow quickly and reduce the efficiency of the Solr instance that processes the index, which can affect search results speed and time to display data lineage. In addition, stale metadata may show relationships that no longer exist, or the lineage may take longer to display than necessary as the system processes extraneous details.

Cloudera Navigator’s purge function removes metadata for files that have been deleted or for operations that are older than the specified timeframe. The result is faster search and more precise (up-to-date) lineage diagrams.

Note: Metadata for deleted files are only purged when the containing directory is also deleted.

In addition, clearing metadata before upgrading Cloudera Navigator to a new release can speed-up the upgrade process and reduce the chance of out-of-memory errors.

There are three ways to clear metadata:

- After deleting managed metadata properties, as detailed in Purging a Property.
- By using the Cloudera Navigator APIs, as detailed in Using the Purge APIs for Metadata Maintenance Tasks.
- By using the Cloudera Navigator console and scheduling a regular weekly Purge, as detailed below.

Best Practices for Clearing Metadata using Purge

When a purge job runs, any running Navigator tasks—extractions, policy application, or other background tasks—are stopped so that the purge can run immediately. When the purge task completes, the tasks that were stopped are restarted from the beginning. The interruption for the purge task may delay collecting new audits and metadata but does not affect what content is collected.

A purge task won’t stop another purge task: if a purge task if already running when a new purge task is triggered, the new purge task will be ignored. For example, if the scheduled metadata purge is running, an administrator won’t be able to kick off a purge task for deleting managed metadata properties; if a scheduled metadata purge is still running when the next scheduled purge starts, the new task is ignored.

Based on the purge behavior, consider the following recommendations to make sure that Navigator purge tasks don’t conflict with extraction tasks:

- **Purge Timing.** Because purge tasks stop extraction and other Navigator jobs, it’s important to schedule the purge task when it will cause the least disruption: users and processes will be unable to use Cloudera Navigator until the purge process completes.

- **First Time Purge Runs.** For new installations of Navigator or installations starting with a fresh storage directory, schedule purge jobs after you’ve seen the HDFS and Hive HMS extractions shift from bulk extraction to incremental extraction. The first extractions of metadata from HDFS run against every HDFS directory in the cluster and can run for many hours. Subsequent extractions run incrementally, only extracting metadata for new and changed entities. If the initial extractions are never allowed to complete, the shorter, faster incremental extractions don’t begin. The same is true for HMS extractions.
To avoid a purge task from stopping the initial bulk extraction, avoid scheduling purge tasks until after extraction has shifted to the incremental mode.

**Scheduling the Purge Process**

Use the Cloudera Navigator console to configure a schedule for a regular weekly purge of deleted and stale metadata from the Navigator Metadata Server and its associated database.

**Required Role:** Metadata Administrator (or Full Administrator)

To configure the automated purge schedule:

1. [Log in to the Cloudera Navigator console](#) using an account with Full Administrator privileges.
2. Go to **Administration > Purge Settings** tab.

The current Metadata and Lineage purge schedule displays, along with lists of up to five upcoming scheduled purges and a list of up to five most recent completed purges.

To change the existing schedule:

1. **Click Edit.**
2. **Set the purge process options.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Range of selectable values and usage note</th>
</tr>
</thead>
<tbody>
<tr>
<td>How often</td>
<td>Weekly</td>
<td>Not configurable. The purge runs weekly per your specifications for Day and Time. It is enabled by default.</td>
</tr>
<tr>
<td>Day</td>
<td>Saturday</td>
<td>Select a day for the purge that will have minimal impact to your user community.</td>
</tr>
<tr>
<td>Time</td>
<td>12 Midnight</td>
<td>Hourly time, from 12 Midnight through 11 PM. Select a time that will have minimal impact on production.</td>
</tr>
<tr>
<td>Maximum purge duration</td>
<td>12 hours</td>
<td>Set the amount of time you want to allow for the purge process to run. If not already complete, the HDFS purge process will not add any new items to purge after your specified duration. Entities purged to that point remain purged. All non-HDFS purge processes will run without limit. If set to 0, the purge is disabled. No other Cloudera Navigator operations, including through the console, can occur during the purge process.</td>
</tr>
</tbody>
</table>
Range of selectable values and usage note

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge HDFS entities deleted more than*</td>
<td>60 days</td>
<td>The number of days after an entity is deleted that elapse until the purge process removes its metadata. For example, a setting of 1 day purges entities deleted before two days ago but retains entities deleted yesterday.</td>
</tr>
<tr>
<td>Purge SELECT operations*</td>
<td>Enabled</td>
<td>Hive and Impala SELECT operations older than days specified in <strong>Only Purge SELECT operations older than</strong> will be purged.</td>
</tr>
<tr>
<td>Purge operations older than*</td>
<td>60 days</td>
<td>Yarn, Sqoop, and Pig operations older than the specified date will be purged. If <strong>Purge SELECT Operations</strong> is enabled, Hive and Impala SELECT operations older than the specified date will also be purged.</td>
</tr>
</tbody>
</table>

3. Click **Save** when finished.

Here is an example of a revised schedule:

<table>
<thead>
<tr>
<th>How often</th>
<th>Weekly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day*</td>
<td>Sunday</td>
</tr>
<tr>
<td>Time*</td>
<td>2 AM</td>
</tr>
<tr>
<td>Maximum purge duration*</td>
<td>5 hours</td>
</tr>
<tr>
<td>Purge HDFS entities deleted more than*</td>
<td>60 days</td>
</tr>
<tr>
<td>Purge SELECT operations*</td>
<td>Enable</td>
</tr>
<tr>
<td>Purge operations older than*</td>
<td>90 days</td>
</tr>
</tbody>
</table>

**Note:** If no schedules appear after you configure the purge process, your environment may not have automated purge enabled. To check if the automated purge is enabled, add `/debug` to the Navigator URL (http://fqdn-a.example.com:7187/debug), click **Configuration**, and check the value of `nav.purge.enabled`. If the property is set to false, you can enabled it in the debug page for this Navigator session; **change the property in Cloudera Manager** by adding `nav.purge.enabled=true` to the **Navigator Metadata Server Advanced Configuration Snippet (Safety Valve)** for `cloudera-navigator.properties`.

What Metadata is Purged?

Purge processes look for metadata that is associated with deleted files and tables and with operation executions that are older than the configured threshold date.

**Hive Metadata**

- Hive operations
  - That don’t produce output
  - That have all operation executions that were executed earlier than the threshold date
- Hive operation executions
  - Associated with Hive operations that don’t produce output
  - That were executed earlier than the threshold date
- Hive sub-operations
  - Associated with Hive operations that were purged
- All relations associated with the purged entities

**Impala Metadata**
- Impala operations
  - That don't produce output
  - That have all operation executions that were executed earlier than the threshold date
- Impala operation executions
  - Associated with Impala operations that don't produce output
  - That were executed earlier than the threshold date
- Impala sub-operations
  - Associated with Impala operations that were purged
- All relations associated with the purged entities

**Sqoop Metadata**
- Sqoop import and export operations
  - That have all operation executions that were executed earlier than the threshold date and no existing downstream entities
- Sqoop operation executions
  - That were executed earlier than the threshold date
- All relations associated with the purged entities

**YARN Metadata**
- YARN operations
  - That have all operation executions that were executed earlier than the threshold date
- YARN operation executions
  - That were executed earlier than the threshold date
- All relations associated with the purged entities

**Pig Metadata**
- Pig operations
  - That have all operation executions that were executed earlier than the threshold date and don't apply to tables connected to existing HDFS files
- Pig operation executions
  - That were executed earlier than the threshold date
- Pig tables
  - That were created by an operation execution executed earlier than the threshold date and also not connected to an existing HDFS file
- Pig fields
  - Fields in purged tables
- All relations associated with the purged entities
HDFS Metadata

- HDFS directories
  - That have been deleted longer than the configured threshold
  - AND don't have a logical-physical relation with another entity (such as a Hive table)
  - AND don't have children (sub directories or files) that aren’t ready to be purged
  - AND aren’t an endpoint in a data flow relation
- HDFS files
  - Deleted file metadata are purged only when the containing directory is purged
- All relations that have both endpoints associated with purged entities

Administering Navigator User Roles

Cloudera Navigator user roles can be assigned to groups that are managed by an external LDAP-compliant identity/authentication system (Active Directory, OpenLDAP) using the Role Management tab of the Cloudera Navigator console. The Role Management feature only becomes available in the Cloudera Navigator console after the external system has been successfully configured for use by Cloudera Navigator. See Authentication for Cloudera Navigator for configuration details.

Assigning User Roles to Groups

Cloudera Navigator user roles determine the Cloudera Navigator features and functions available to the logged in account holders. Data stewards, auditors, and other business users log in to the Cloudera Navigator console and have available only those menu selections and options appropriate for the user role (or roles) granted to group of which they are a member. The groups are defined in an external LDAP service that has been configured for use by Cloudera Navigator. See Authentication for Cloudera Navigator for details.

For example, a user belonging to a group granted only the Policy Editor role is limited to the Search, Analytics (metadata), and Policies tabs of the Cloudera Navigator console and to the features and functions available from those menus. See User Roles and Privileges Reference on page 176 for details about each Cloudera Navigator user role. Assigning or editing user roles requires logging in to the Cloudera Navigator console with an account having one of the following roles:

- Cloudera Manager Full Administrator or Navigator Administrator, or Cloudera Navigator User Administrator.

To assign Cloudera Navigator user roles to a group:

1. Log in to Cloudera Navigator console.
2. Click the Administration menu.
3. Click the Role Management tab.
4. Select Search for groups to search among all groups in the external directory.
   - The Groups with Navigator roles choice shows groups that have already been assigned one or more Cloudera Navigator user roles.
5. Enter the name of the specific group in the search field.
6. Select the group from among those returned in the list.
   - The details list any existing roles associated with this group. For example:
7. Click **Manage Role Assignment** in the upper right corner.
8. Select each user role you want to assign to the group.
9. Click **Save**.

Changes to user role assignments take effect the next time users in the group log in to Cloudera Navigator.

**Displaying Roles for Current User Account Login**

From the Cloudera Navigator console, you can verify the user roles associated with your current login by selecting **My Roles** from the account drop-down menu.
Navigator Configuration and Management

Cloudera Navigator runs as two discrete roles—Navigator Audit Server and Navigator Metadata Server—in the context of Cloudera Manager Server. Features and configuration options available for these server-side processes are managed using the Cloudera Manager Admin Console. Management tasks include configuring filters to fine-tune audit event collection, tuning the Navigator Metadata Server for optimal performance, and configuring auditing for select services.

Management tasks also include implementing a backup system for Navigator metadata, and configuring security features, such as TLS/SSL to support HTTPS and client-server encrypted communications over the network.

Topics in this section apply to Navigator in general or to either Navigator Audit Server or Navigator Metadata Server specifically.

Accessing Navigator Data Management Logs

You can access Navigator Metadata Server and Navigator Audit Server logs from Cloudera Manager or from the command line on the host where each server is running.

Accessing Navigator Logs from Cloudera Manager

To access Navigator Metadata Server Logs from Cloudera Manager:

1. Select Clusters > Cloudera Management Service.
2. In the Status Summary, click Navigator Audit Server or Navigator Metadata Server.
3. Choose Log Files > Role Log File.

A new browser tab opens with a page of the most recent log. This example shows the audit server log; the metadata server log behaves the same.

Accessing Navigator Logs from the Command Line

By default, the Navigator server logs are located in /var/log on the host where the server is running. The host name is part of the log file name:

Audit Server: /var/log/cloudera-scm-navigator/mgmt-cmf-mgmt-NAVIGATOR-host.log.out
Metadata Server: /var/log/cloudera-scm-navigator/mgmt-cmf-mgmt-NAVIGATORMETASERVER-host.log.out

Figure 8: Navigator Audit Server Log in Cloudera Manager
Backing Up Cloudera Navigator Data

Backups of Cloudera Manager include the data stored for Navigator Audit Server and Navigator Metadata Server data, as described in Backing Up Cloudera Manager. Follow these steps if you need to back up either storage independently from Cloudera Manager:

Backup Navigator Audit Server Data

Navigator Audit Server stores audit information in a database instance. The audit metadata does not need to be backed up at the same time as the Navigator Metadata Server metadata.

1. Confirm the Navigator Audit Server database location and connection information.
   
   To locate this information, log in to the Cloudera Manager Admin Console and go to Clusters > Cloudera Management Service. Click the Configuration tab. Select Scope > Navigator Audit Server and Category > Database. The results indicate the type, host, database name, and login account.

2. Using the appropriate tool for the database instance (such as MySQL), backup the database. See Back Up the Cloudera Manager Databases.

Backup Navigator Metadata Server Data

Navigator Metadata Server stores metadata in an embedded Solr data directory and in a database instance. Back up these locations together so the backups describe the same metadata state.

1. Shut down the Navigator Metadata Server role.

2. Backup the data directory.
   
   The Navigator Metadata Server default directory is /var/lib/cloudera-scm-navigator. To confirm that this is the path your deployment uses, log in to the Cloudera Manager Admin Console and search for the Navigator Metadata Server Storage Dir property (nav.data.dir).

3. Backup the database instance.
   
   • Confirm the Navigator Metadata Server database location and connection information.
     
     To locate this information, log in to the Cloudera Manager Admin Console and go to Clusters > Cloudera Management Service. Click the Configuration tab. Select Scope > Navigator Metadata Server. Select Category > Database. The results indicate the type, host, database name, and login account.

   • Using the appropriate tool for the database instance (such as MySQL), backup the database. See Back Up the Cloudera Manager Databases.

4. Start the Navigator Metadata Server role.

Authentication and Authorization

To support its user role-based authorization scheme, Cloudera Navigator integrates with external authentication mechanisms. External authentication mechanisms include:

- LDAP-compliant identity/authentication services, such as Active Directory and OpenLDAP
- SAML-based SSO solutions, such as Shibboleth and SiteMinder

Cloudera Manager Server has its own internal authentication mechanism, a database repository of user accounts. However, the user accounts defined in the internal Cloudera Manager account repository cannot be assigned Cloudera Navigator user roles. The only Cloudera Navigator user role that can be effectively applied to an account created in the Cloudera Manager internal repository is that of Navigator Administrator.

In other words, assigning Cloudera Navigator user roles to user accounts requires using an external authentication mechanism, such as Active Directory or OpenLDAP. See the following topics in the Cloudera Security guide for details:
Configuring Cloudera Navigator to work with Hue HA

Cloudera Navigator Search results include links to open data assets in Hue. No special configuration is required to enable these links.

However, for multiple Hue instances deployed behind external load-balancers such as in certain Hue high availability configurations, the links are properly generated only if the host name of the external load-balancer is set as the preferred URL, by configuring the Advanced Configuration Property (Safety Valve) as follows:

1. Log in to Cloudera Manager Admin Console using an account with Full Administrator privileges.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
5. Under the Category filter, click Advanced.
6. Scroll to the property Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties.
7. Replace the cluster name and set the nav.hue.preferred_baseurl.<clusterName> to the fully-qualified domain name (FQDN) or specific URL of your Hue load-balancer using one of the following formats:

   nav.hue.preferred_baseurl.<clusterName>=<FQDN>

   or

   nav.hue.preferred_baseurl.<clusterName>=https://<FQDN>::<port>

   Use the full URL format when Hue is configured to use TLS/SSL; indicate https and the secure port number for the load balancer.

   For example, if a load-balancer for multiple Hue services is setup on host hue_lb_nginx.example.com and configured for TLS/SSL on port 8889, the entry would be as follows:

   

   nav.hue.preferred_baseurl.myCluster=https://hue_lb.example.com:8889


8. Click Save.
9. Restart the Navigator Metadata Server role.

   Links to Hue will now be properly created and available in the Search results lists in the Cloudera Navigator console.
Cloudera Navigator support for Virtual Private Clusters

Cloudera Manager supports deploying workloads in virtual private compute clusters, allowing administrators to access resources for high-demand times or to isolate workloads. In this environment Cloudera Navigator continues to extract metadata and track audit events from services running on the Base cluster and track audit events from services running on the Compute cluster. Navigator does not extract metadata from services running on the Compute cluster.

When you use Compute clusters, you define a data context to control how data is shared between a Compute cluster and the Base cluster. The interaction between the Compute clusters and the Base clusters through the data context means that some of the activity that occurs on Compute clusters does affect the metadata collected in Navigator. For example, if you create Hive data assets using HiveServer2 or SparkSQL on the Compute cluster and you have Hive in your data context, you will see entities for the new Hive data assets in Navigator. You won't see lineage for how these assets were created because the operations on the Compute cluster are not extracted. You will see audits for the events that created the assets. The following tables describe the behavior of Navigator metadata and audit collection in Base and Compute clusters for the services Navigator supports.

Navigator Auditing in Virtual Private Compute Clusters

Audits appear in Navigator for events that occur on a Compute cluster. Note that there can be latency between an event occurring and the audit reaching Navigator on the base cluster. Be aware of this possible delay when terminating a compute cluster: audit events from the Compute cluster may be lost if they have not been processed when the cluster is terminated.

Table 1: Audit Behavior in Virtual Private Clusters

<table>
<thead>
<tr>
<th>Audited Service</th>
<th>Base Cluster</th>
<th>Compute Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBase</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>HDFS</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HiveServer2</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Hue</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Impala</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Sentry</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Solr</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Navigator Metadata and Lineage Extraction in Virtual Private Compute Clusters

No metadata is extracted from services running on a Compute cluster. However, if HDFS or Hive is included in the data context for a Compute cluster, Navigator shows entities created or updated on a Compute cluster and stored in HDFS or Hive Metastore on the Base cluster. For example, when directories or files are created from actions on a Compute cluster with HDFS in its data context, the directories and files are stored on the HDFS in the Base cluster. Navigator collects the metadata from the Base cluster HDFS and creates entities for the directories and files. Similarly, when Hive databases, tables, views, or partitions are created or modified by HiveServer2, Impala, or SparkSQL operations on a Compute cluster and Hive is included in the data context for that cluster, the updated metadata is extracted from HMS on the Base cluster and collected by Navigator. Because Navigator does not extract metadata directly from the Compute cluster, the operations and operation executions that created the data assets are not collected; therefore, Navigator does not calculate lineage for these data assets.
### Encrypted (TLS/SSL) and Cloudera Navigator

Cloudera Navigator supports TLS/SSL encryption for network communications between the Navigator Metadata Server and clients, such as the web browser used for Cloudera Navigator console, and between RPC client and server processes for Navigator Metadata Server and Navigator Audit Server. See Cloudera Security for configuration details, specifically:

- Configuring TLS/SSL for Cloudera Navigator Audit Server
- Configuring TLS/SSL for Cloudera Navigator Metadata Server

### Limiting Sensitive Data in Navigator Logs

Cloudera Navigator collects metadata for cluster activities and assets; typically, this information does not include data and therefore doesn’t provide an opportunity to expose sensitive data through the user interface. However, there could be sensitive data exposed the Navigator logs: queries from Impala or Hive may include a specific data value, such as a phone number or US social security number.

To guard against sensitive data exposures through Navigator logs, you can use Cloudera Manager’s log redaction feature to filter out string patterns using regular expressions. For example, you could mask all quoted strings, social security numbers, and phone numbers.

The log redaction rules can apply across all cluster services.

For details, see the Cloudera Security guide, specifically Log and Query Redaction.
Preventing Concurrent Logins from the Same User

You can configure a limit to the number of simultaneous sessions authenticated against the same user name. The property `nav.max.concurrent.sessions` takes an integer value as a limit; set the value to -1 (default) to turn off the limit. To change the default behavior, in Cloudera Manager, add the property with a new value to the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for `cloudera-navigator.properties`. Restart the Navigator Metadata Server to apply the change.

Navigator Audit Server Management

The Navigator Audit Server tracks and coalesces events from Cloudera Manager and stores them in the Navigator Audit database. This section provides a high level view of the auditing architecture and shows administrators how to use Cloudera Manager Admin Console to add the Navigator Audit Server to an existing cluster, how to configure some of its features.

Navigator Auditing Architecture

The figure below shows a high level view of the Cloudera Navigator auditing architecture:

During system setup, plug-ins for the various services—HDFS, HBase, and Hive (HiveServer2, Beeswax servers) services, for example—are enabled. These plug-ins work with the service to collect and filter events emitted by the respective service, writing the events to an audit log on the local filesystem. Impala, Sentry, and the Cloudera Navigator Metadata Server also collect and filter events and write them to their respective audit log files.

Note: When upgrading Cloudera Navigator, always check the requirements for any preliminary tasks or constraints due to service plug-ins.
Auditing Architecture In More Detail: How It Works

Here is some more detail about the auditing architecture and interaction among Cloudera Manager Agent, local log file, and Navigator Audit Server.

The Cloudera Manager Agent process on each host in the cluster:

- Monitors local audit log files
- Sends events captured in the logs to the Navigator Audit Server
- Retries sending any event that fails to transmit successfully
- Keeps track of successfully transmitted events from the log file (offset position in the file) to prevent re-sending any already processed events after a system failure and restart
- Deletes old audit logs after successful transmission to the Navigator Audit Server

After any event is written to the audit log file (and assuming space available on the filesystem), its delivery is guaranteed. In other words, transient (in-memory) buffer handling is not involved in this part of the process. Audit logs are rotated and the Cloudera Manager Agent follows the rotation of the log.

The plug-in for each of the various services effectively writes the events to the audit log file. A plug-in that fails to write an event to the audit log file can either drop the event or can shut down the process in which it is running depending on the configured queue policy.

The Navigator Audit Server performs the following functions:

- Tracks and coalesces events obtained from Cloudera Manager
- Stores events to the Navigator Audit database

Auditing can be enabled for the core services listed in the table. Use the Cloudera Manager Admin Console to change the configuration details and to create whitelists and blacklists for better control over audit details collected by Navigator Audit Server. See Configuring Audit and Log Properties for details.

<table>
<thead>
<tr>
<th>Audited Service</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBase</td>
<td>hbase-MASTER, hbase-REGIONSERVER</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs-NAMENODE</td>
</tr>
<tr>
<td>Hive</td>
<td>Hive Server 2 only (hive-HIVESERVER2). Command line <code>beeline</code> (not <code>hive</code>).</td>
</tr>
<tr>
<td>Hue</td>
<td></td>
</tr>
<tr>
<td>Impala</td>
<td>impala-IMPALAD (Auditing data and lineage data both collected by Cloudera Manager Agent).</td>
</tr>
<tr>
<td>Navigator Metadata Server</td>
<td></td>
</tr>
<tr>
<td>Sentry</td>
<td></td>
</tr>
<tr>
<td>Solr</td>
<td></td>
</tr>
</tbody>
</table>

Setting Up Navigator Audit Server

The steps below show you how to add the Navigator Audit Server role to an existing Cloudera Manager cluster.

The Navigator Audit Server role runs on the Cloudera Management Service. By default, the installation process installs both Navigator Audit Server and Navigator Metadata Server roles on the same Cloudera Management Service instance, but that may not be optimal, especially for very large clusters.

Adding the Navigator Audit Server Role

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

The steps below assume that an external database is running and available to be used with the Navigator Audit Server role. Before adding this role, gather the configuration details about the external database instance so you can enter them when needed during this process.
To add the Navigator Audit Server role to the cluster:

1. Log in to the Cloudera Manager Admin Console.
2. From the menu, select Clusters > Cloudera Management Service.
3. Click the Instances tab.
4. Click Add Role Instances. The Customize Role Assignments page displays and lists the nodes available to support additional roles, assuming the cluster has available resources. Reassign and customize role instances as needed.
5. Select the Navigator Audit Server role and assign it to appropriate host for your cluster.
6. When finished, click Continue. The Database Setup page displays.
7. Click Use Custom Database.
8. In the Navigator Audit Server section, enter the details of your database instance:
   - Database host name
   - Database type
   - Database name
   - Username
   - Password

   Note: For non-production use only, you can select Use Embedded Database. Cloudera Manager creates and configures the databases for you. Make a note of the generated passwords.

Here is an example of a configured external database instance:

<table>
<thead>
<tr>
<th>Navigator Audit Server Database Type</th>
<th>Navigator Audit Server Default Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigator.db.type</td>
<td>MySQL</td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
</tr>
<tr>
<td></td>
<td>PostgreSQL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Navigator Audit Server Database Hostname</th>
<th>Navigator Audit Server Default Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigator.db.host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fqdn-1.example.com:3306</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Navigator Audit Server Database Name</th>
<th>Navigator Audit Server Default Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigator.db.name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nae-db</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Navigator Audit Server Database Username</th>
<th>Navigator Audit Server Default Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigator.db.user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Navigator Audit Server Database Password</th>
<th>Navigator Audit Server Default Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>navigator.db.password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>.......</td>
</tr>
</tbody>
</table>

9. Click Test Connection to verify the communication between the cluster and the external database. If the test fails, check the database settings and try again. If you selected embedded database, a message displays regarding database creation.
10. Click Continue.
12. Click Finish.
Starting, Stopping, and Restarting the Navigator Audit Server

1. Log in to the Cloudera Manager Admin Console.
2. From the menu, select Clusters > Cloudera Management Service.
3. Click the Instances tab.
4. Click the link for the Navigator Audit Server from the Role Type list. The Actions for Selected button activates and displays (1) for the selected role.
5. From the Actions for Selected (1) menu, select the Action you want to perform on this role instance:
   - Start
   - Stop
   - Restart
   - Enter Maintenance Mode
   - Exit Maintenance Mode
   - Delete

   A confirmation message displays prompting you to Cancel or complete the specified Action.
6. Click Cancel to abandon the process, or click Action to execute the action.

Configuring the Navigator Audit Server Data Expiration Period

By default, the Navigator Audit Server keeps 90 days worth of audit events in its database. The setting can be changed to a shorter timeframe by configuring the number of hours or days of audit events to keep in the Navigator Audit Server database as follows:

1. Log in to the Cloudera Manager Admin Console.
2. From the menu, select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Select Navigator Audit Server from the Scope filter.
5. For the Navigator Audit Server Data Expiration Period, enter the number of days or hours of audit events that should be retained in the database before purging and select either day(s) or hour(s) from the drop-down to label the value accordingly.
6. Restart the Navigator Audit Server role.

Review the Navigator Audit Server Filters

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

By far, HDFS produces the largest volume of audit events. Many of these events are caught and discarded by audit filters, particularly events that don’t uniquely describe activity on the cluster or are produced only by controlled service users. Many of the default HDFS audit filters assume default service role names. To get value from the default filters, be sure to review them to make sure that the role names referenced match those used in your environment.

See Customizing the Default Audit Filters on page 91 for more information about the provided filters and their use.

You can review and possibly change the filters as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select an HDFS service. Select Cluster > HFDS Service-Name
3. Click the Configuration tab.
4. Filter the properties on “audit”.
5. Review the list of filters in the property Audit Event Filter.
6. Make changes to the filters as appropriate.
7. Restart the Navigator Audit Server role.

Setting the Navigator Audit Server Java Heap Size

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)
The Navigator Audit Server performance is typically bound by the performance of the database. With that in mind, consider increasing the Navigator Audit Server Java heap to as much as 4 GB; increasing heap beyond this point is unlikely to change the server performance. The default Java heap is set to 1.5 GiB.

You can change the setting as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Select Scope > Navigator Audit Server.
5. For Filter Category, click Resource Management to display the Java Heap Size property.

   ![Java Heap Size of Auditing Server in Bytes](image)

6. Use the drop-down selector to change the unit scale to B (Bytes), KiB, MiB, or GiB and set your preferred heap size.
7. Click Save Changes.
   
   The setting takes effect only after restarting the role. Restart the Navigator Metadata Server role now or make other configuration changes and restart after you are finished with all changes.

8. Restart the Navigator Audit Server role.

Configuring the Navigator Audit Server Log Directory

The default location for the Navigator Audit Server logs is:

```
/var/log/cloudera-scm-navigator
```

To change the location for the log directory:

1. Log in to the Cloudera Manager Admin Console.
2. From the menu, select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Select Category > Logs.
5. Enter the path for the Navigator Audit Server Log Directory property.
6. Restart the Navigator Audit Server role.

Enabling Audit and Log Collection for Services

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

Auditing of every service and role in the cluster may not be necessary and may degrade performance, which is why auditing is not always enabled by default. In addition, auditing can be configured to capture only specific events, as detailed in Configuring Service Auditing Properties.

Enabling Audit Collection

Any service or role instance that can be audited by Cloudera Navigator has an Enable Audit Collection property. When enabled, the Cloudera Manager Agent process on the node monitors the audit log file (or files) and sends collected audit records to the Navigator Audit Server.

1. Log in to Cloudera Manager Admin Console
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Select ServiceName (Service-Wide) for the Scope filter.
5. Select Navigator Metadata Server for the Category filter.
6. Click the Enable Audit Collection checkbox to activate auditing for the service.
7. Click **Save Changes**.
8. Restart the service.

**Configuring Impala Daemon Logging**

To enable logging for the Impala Daemon role.

1. Log in to Cloudera Manager Admin Console
2. Select **Clusters > Cloudera Management Service**.
3. Click the **Configuration** tab.
4. Select **Impala Daemon** for the **Scope** filter.
5. Select **Logs** for the **Category** filter.
6. Edit the **Enable Impala Audit Event Generation**.
7. Click **Save Changes**.
8. Restart the Impala daemon.

To set the log file size:

1. Click the Impala service.
2. Select **Scope > Impala Daemon**.
3. Select **Category > Logs**.
4. Set the **Impala Daemon Maximum Audit Log File Size** property.
5. Click **Save Changes**.
6. Restart the Impala service.

**Enabling Solr Auditing**

Solr auditing is disabled by default. To enable auditing:

1. Enable Sentry authorization for Solr following the procedure in [Configuring Sentry Authorization for Cloudera Search](#).
2. Go to the Solr service.
3. Click the **Configuration** tab.
4. Select **Scope > Solr Service (Service-Wide)**
5. Select **Category > Policy File Based Sentry** category.
6. Select or clear the **Enable Sentry Authorization** checkbox.
7. Select **Category > Cloudera Navigator** category.
8. Select or clear the **Enable Audit Collection** checkbox. See [Configuring Service Audit Collection and Log Properties](#).
9. Enter a **Reason for change**, and then click **Save Changes** to commit the changes.
10. Restart the service.

**Configuring Audit Logs**

The following properties apply to an audit log file:

- **Audit Log Directory** - The directory in which audit log files are written. By default, this property is not set if Cloudera Navigator is not installed.

  A validation check is performed for all lifecycle actions (stop/start/restart). If the Enable Collection flag is selected and the Audit Log Directory property is not set, the validator displays a message that says that the Audit Log Directory property must be set to enable auditing.

  If the value of this property is changed, and service is restarted, then the Cloudera Manager Agent will start monitoring the new log directory for audit events. In this case it is possible that not all events are published from the old audit log directory. To avoid loss of audit events, when this property is changed, perform the following steps:

  1. Stop the service.
2. Copy audit log files and (for Impala only) the impalad_audit_wal file from the old audit log directory to the new audit log directory. This needs to be done on all the hosts where Impala Daemons are running.

3. Start the service.

- **Maximum Audit Log File Size** - The maximum size of the audit log file before a new file is created. The unit of the file size is service dependent:
  - HDFS, HBase, Hive, Hue, Navigator Metadata Server, Sentry, Solr - MiB
  - Impala - lines (queries)

- **Number of Audit Logs to Retain** - Maximum number of rolled over audit logs to retain. The logs will not be deleted if they contain audit events that have not yet been propagated to the Audit Server.

To configure audit logs do the following:

1. Do one of the following:
   - Service - Go to a supported service.
   - Navigator Metadata Server
     - Do one of the following:
       - Select Clusters > Cloudera Management Service.
       - On the Home > Status tab, in Cloudera Management Service table, click the Cloudera Management Service link.

2. Click the Configuration tab.

3. Select the scope according to the service:
   - All services except Impala - **Scope > ServiceName (Service-Wide)**.
   - Impala - **Scope > Impala Daemon**.
   - Navigator Metadata Server - **Scope > Navigator Metadata Server**.

4. Select **Category > Logs**.

5. Configure the log properties. For Impala, preface each log property with **Impala Daemon**.

6. Click **Save Changes**.

7. Restart the service.

**Configuring Service Auditing Properties**

Set auditing properties for a service in the service’s configuration settings in Cloudera Manager.

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)

**Setting Audit Properties**

To review or update audit properties for a service:

1. Log in to the Cloudera Manager Admin Console.
2. Select select any service that supports auditing. Select **Cluster > Service-Name**
3. Click the Configuration tab.
4. Select **Service (Service-Wide)** for the Scope filter.
5. Select **Cloudera Navigator** for the Category filter.
6. Edit the properties.
7. Enter a **Reason for change**, and then click **Save Changes** to commit the changes.
8. Restart the service if needed.

It is not necessary to restart the service if you are updating an audit filter.
In addition, for Impala and Solr auditing, perform the steps in Configuring Impala Daemon Logging on page 86 and Enabling Solr Auditing on page 86 and for all services perform the steps in Configuring Audit Logs on page 86.

Operations within Navigator are also audited. To update Navigator’s audits:

1. Select Clusters > Cloudera Management Service. 
2. Click the Configuration tab. 
4. Select Category > Cloudera Navigator category. 
5. Edit the properties. 
6. Enter a Reason for change, and then click Save Changes to commit the changes. 
7. Restart the service if needed. 

It is not necessary to restart the service if you are updating an audit filter.

Service-level Audit Properties

Each service (with exceptions noted) that supports auditing has the following properties:

- **Enable Audit Collection** - See Enabling Audit Collection on page 85 and Enabling Solr Auditing on page 86. 
- **Audit Log properties** - See Configuring Audit Logs on page 86 and Configuring Impala Daemon Logging. 
- **Audit Event Filter** - A set of rules that capture properties of auditable events and actions to be performed when an event matches those properties. The Cloudera Manager Agent uses this property to filter events out before they are sent to Cloudera Navigator. The default filter settings discard the following events:
  - **HDFS**
    - Generated by the internal Cloudera and Hadoop users (cloudera-scm, hbase, hive, impala, mapred, solr, spark, and dr.who) 
    - Generated by the hdfs user running the listStatus, listCachePools, listCacheDirectives, and getfileinfo operations
    - That affect files in the /tmp directory
  - **HBase** - That affect the -ROOT-, .META., and acl tables
  - **Hive** - Generated by Hive MapReduce jobs in the /tmp directory
  - **Impala, Solr, Solr, Navigator Metadata Server** - No default filter

See also

- **Audit Event Tracker** - A set of rules for tracking and coalescing events. This feature is used to define equivalency between different audit events. Tracking works by keeping a reference to events when they first appear, and comparing other incoming events against the tracked events according to the rules defined. When events match, according to a set of configurable parameters, only one entry in the audit list is generated for all the matching events. This property is not supported for the Navigator Metadata Server.

- **Audit Queue Policy** - The action to take when the audit event queue is full. The options are Drop or Shutdown. When a queue is full and the queue policy of the service is Shutdown, before shutting down the service, N audits will be discarded, where N is the size of the Cloudera Navigator Audit Server queue. 

**Note:** If the queue policy is Shutdown, the Impala service is shut down only if Impala is unable to write to the audit log file. It is possible that an event may not appear in the audit event log due to an error in transfer to the Cloudera Manager Agent or database. In such cases Impala will not shut down and will keep writing to the log file. When the transfer problem is fixed the events will be transferred to the database.

This property is not supported for Hue or the Navigator Metadata Server.
Finding Audit Filter Properties for Each Service

For information on the structure of the objects, and the properties for which you can set filters, display the description on the configuration page as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select any service that supports auditing. Select Cluster > Service-Name
3. Click the Configuration tab.
4. Select Service (Service-Wide) for the Scope filter.
5. Select Cloudera Navigator for the Category filter.
6. Click for Audit Event Tracker to open the property description.

For example, the Hive properties are:

- operation: the Hive operation being performed.
- userName: the user performing the action.
- ipAddress: the IP from where the request originated.
- allowed: whether the operation was allowed or denied.
- databaseName: the databaseName for the operation.
- tableName: the tableName for the operation.
- objectType: the type of object affected by the operation.
- resourcePath: the path of the resource affected by the operation.

Entering Audit Filter Properties

The Audit Event Filter and Audit Event Tracker rules for filtering and coalescing events are expressed as JSON objects. You can edit these rules using a rule editor. The username filters shown here include an optional phrase (?:/.+)? to filter events where the user name is constructed with a slash as part of the name, such as a Kerberos principal (username/instance@REALM). It applies only if the regular expression matches one of the usernames listed in the first phrase. The src filter shows a similar optional phrase (?:/.*?) that filters for subdirectories under the /tmp directory. The regular expression looks for occurrences of slash followed by zero or more characters; this makes sure that subdirectories are included but other directories whose name starts with “tmp” are not included in the filter.

HDFS-1 (Service-Wide)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Action</th>
<th>Fields</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>discard</td>
<td>username</td>
<td>(?cloudera-scm</td>
</tr>
<tr>
<td>Rule</td>
<td>discard</td>
<td>username</td>
<td>(?hdfs)(?/.+)?, operation: (?listStatus</td>
</tr>
<tr>
<td>Rule</td>
<td>discard</td>
<td>src</td>
<td>/tmp(?/.*)?</td>
</tr>
</tbody>
</table>

or in a JSON text field:
Audit Filter Examples

Use audit filters to control what information is collected by Navigator Audit Server. The following sections describe cases where a filter can allow you to remove noise from the audit events or otherwise improve the quality of the audit trail.

Removing audit events for automated tasks

If you find that the audit events include references to automated tasks against HDFS or other services that you don’t want to include in your audit, you can include the tasks in a "discard" filter. For example, to discard all tasks performed against HDFS by the user under which the automated tasks are performed, create an HDFS filter:

```json
    "rules": [  
      {  
        "action": "discard",  
        "fields": [  
          {  
            "name": "username",  
            "match": "(?<cloudera-scm|hbase|mapred|hive|dr,who|soir|impala|spark)?/\.+?"  
          }  
        ]  
      },  
      {  
        "action": "discard",  
        "fields": [  
          {  
            "name": "username",  
            "match": "(?<hdfs)?/\.+?"  
          }  
        ]  
      },  
      {  
        "action": "discard",  
        "fields": [  
          {  
            "name": "src",  
            "match": "tmp/\.+?"  
          }  
        ]  
      }  
    ],  
    "defaultAction": "accept",  
    "comment": "Default filter for HDFS services.",  
    "Discards events generated by the internal Cloudera and/or HDFS users",  
    "[cloudera-scm, hbase, mapred, hive, dr,who, soir, impala, and spark]",  
    "[ks] actions performed by the hdfs user",  
    "and events that affect files in the /tmp directory."
```
Removing audit events for low priority operations

You may find that your audit log includes reference to events that you are not interested in tracking. You can prevent these events from being included in the audit log by filtering them out by operation. For example, if the audit event that you don’t want to track looks like this:

```
2170816, hdfs, 1, someuser@MYREALM.COM, null, 192.168.12.18, 1477605498525, getfileinfo, /user/someuser/.staging/jobx/status, null, null, null
```

where the HDFS operation `getfileinfo` ran against the file `status` for the user `someuser` on a node in the cluster. The user account is indicated with a Kerberos realm.

To remove the HDFS `getfileinfo` accesses by this user, the audit filter would reference the user (by itself or with a Kerberos realm name) and the `getfileinfo` operation:

```
Action: Discard
Fields: username: (?:username|username@MYREALM.com)
        operation: (?:getfileinfo)
```

As a performance optimization, the expressions are included in parentheses with `?:` to indicate that the matched values are not retained.

To include more than one operation in the same filter, include both operations with an OR operator `|`: 

```
Action: Discard
Fields: username: (?:username|username@MYREALM.com)
        operation: (?:getfileinfo|liststatus)
```

Adding Audit Filters

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)

Audit filters control what information Navigator Audit Server collects. The following sections describe cases where a filter can allow you to remove noise from the audits or otherwise improve the quality of the audit trail.

The components of audit events differ based on the service that produces the event. See Service Audit Events on page 162 for a list of the event fields. You can modify audit filters for services in the Cloudera Manager configuration property `Audit Event Filter` located in the Cloudera Navigator configuration page. See Configuring Service Auditing Properties on page 87.

Customizing the Default Audit Filters

Cloudera Manager includes audit filters for HDFS, HBase, Hive by default. It may be possible to improve the effectiveness of these audit filters by using information you know about your system. You can check the Audits tab in the Navigator console to verify the exact text of the fields to ensure your filters match the right events. For example, check usernames for specific syntax such as when using Kerberized names.

There are two changes that can potentially have vast improvements for the effectiveness of the default audit filters:

- **Default system usernames**
  
  If your system uses other usernames for key system users, you can improve the default filters by replacing the generic user names with the specific names used in your environment. For example, if you have a system user that performs HDFS operations that is named something other than `hdfs`, modify the default filters to use the specific name.

- **Events from unneeded operations**
  
  You can improve the default filters by adding system events that don’t add value to your audit tracking.

**HDFS Audit Filters**

The default HDFS filters are the following:
• Excludes events produced by typical system user roles.

Action: discard
Fields: username: (?:cloudera-scm|dr.who|hbase|hive|impala|mapred|solr|spark)(?:/.+)?

• Excludes common events that don't add value to an audit log.

Action: discard
Fields: username: (?:hdfs)(?:/.+)?,
          operation: (?:listStatus|listCachePools|listCacheDirectives|getfileinfo)

• Excludes activity in /tmp and Hue system directories

Action: discard
Fields: src: /user/hue/\cloudera_manager_hive_metastore_canary(?:/.*)?

Action: discard
Fields: src:/user/hue/\Trash/Current/user/hue/\cloudera_manager_hive_metastore_canary(?:/.*)?

Action: discard
Fields: src: /tmp(?:/.*)?

HBASE Audit Filters
The default HBase filter is the following

• Excludes activity on the HBase system tables

Action: discard
Fields: tableName: (?:-ROOT-|.META.|_acl_|hbase:meta|hbase:acl)

Hive Audit Filters
The default Hive filter is the following:

• Excludes queries against the internal Hive /tmp data

Action: discard
Fields: operation: QUERY,
          objectType: DFS_DIR,
          resourcePath: /tmp/hive-(?:.+)?/hive_(?:.+)?/-mr-.*

Safeguarding Audit Events for Important Operations
To make sure your audit history includes the critical events that you want to track such as HDFS delete or rename operations, consider setting the first filter in the list for a service to something like the following:

Action: accept
Fields: operation: delete|rename

This filter ensures that any delete or rename operation gets accepted, irrespective of other filters.
Removing Audit Events for Automated Tasks

If you find that the audit events include references to automated tasks against HDFS or other services that you don't want to include in your audit, you can include the tasks in a "discard" filter. For example, to discard all tasks performed against HDFS by the user under which the automated tasks are performed, create an HDFS filter:

| Action: Discard |
| Fields: username: (?:automationuser|automationuser@realm.example.com) |

This rule would discard any event performed by the automationuser account, where the user is specified by itself or with a Kerberos realm designation. Note that the filter is not case sensitive. As a performance optimization, the expression is included in parentheses with ?: to indicate that the matched values are not retained.

Removing Audit Events for Low Priority Operations

You may find that your audit log includes reference to events that you are not interested in tracking. You can prevent these events from being included in the audit log by filtering them out by operation. For example, if the audit event that you don't want to track looks like this:

```
2170816,hdfs,1,someuser@MYREALM.COM,null,192.168.12.18,1477605498525,getfileinfo,
/user/someuser/.staging/jobx/status,null,null,null
```

where the HDFS operation getfileinfo ran against the file status for the user someuser on a node in the cluster. The user account is indicated with a Kerberos realm.

To remove the HDFS getfileinfo accesses by this user, the audit filter would reference the user (by itself or with a Kerberos realm name) and the getfileinfo operation:

| Action: Discard |
| Fields: username: (?:username|username@MYREALM.com) operation: (?:getfileinfo) |

As a performance optimization, the expressions are included in parentheses with ?: to indicate that the matched values are not retained.

To include more than one operation in the same filter, include both operations with an OR operator |.

```
Action: Discard
Fields: username: (?:username|username@MYREALM.com) operation: (?:getfileinfo|liststatus)
```

Monitoring Navigator Audit Service Health

Cloudera recommends monitoring the Navigator Audit Service to ensure that it is always running. This is especially important to ensure that complete and immutable audit records will be available when needed for corporate governance and compliance purposes.

The Navigator Audit Service has a self-check mechanism, the Audit Pipeline Health Check, that generates warning messages when the system slows down or fails. The health check determines failures and slow downs by keeping track of the number of bytes of audit data sent, bytes unsent, or failures during the send process that occur within the monitoring window. Healthy state for a given monitoring period results when all audit data is sent (no data remaining), with error-free transmission from agent to server.

The health check can be run for each service role instance (daemon) that can generate events. By default, all service role groups are selected when you enabled the health check, and the default monitoring period is 20 minutes. Thresholds for warning messages and the monitoring period are configurable using the Cloudera Manager Admin, as detailed below.

Configuring the Audit Pipeline Health Check

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)
Log in to the Cloudera Manager Admin Console. For each service that you want to enable the health check, follow the steps below.

1. Select Clusters > service-name.
2. Click the Configuration tab.
3. In the Search field, type mgmt.navigator to display the health check configuration properties for the service:

   ![mgmt.navigator](image)

   **Navigator Audit Pipeline Health Check**
   
   mgmt.navigator.status.check.enabled

   **Monitoring Period For Audit Failures**
   
   mgmt.navigator.failure.window

   **Navigator Audit Failure Thresholds**
   
   mgmt.navigator.failure.thresholds

4. Modify the settings to shorten (or lengthen) the monitoring period as needed for your system and set bytes for Warning and Critical thresholds.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigator Audit Pipeline Health Check</td>
<td>Check the box to enable the health check. Health check can be enabled for specific groups. By default, the health check is enabled for all groups.</td>
</tr>
<tr>
<td>Monitoring Period for Audit Failures</td>
<td>Default is 20 minutes. The amount of time to process audit events (count processed and evaluate other metrics before generating warnings.</td>
</tr>
<tr>
<td>Navigator Audit Failure Thresholds</td>
<td>Size (in bytes) of failures that will trigger messages.</td>
</tr>
<tr>
<td></td>
<td>• Warning—Default is Never. Set this to an amount of bytes and condition (which to trigger a warning message.</td>
</tr>
<tr>
<td></td>
<td>• Critical—Default is Any, meaning that any amount of failed audit data sent from Cloudera Manager to the server will trigger a critical message.</td>
</tr>
</tbody>
</table>

5. Click Save Changes.

For example, as shown in the Cloudera Manager Admin Console, the pipeline health check is enabled for all groups in the service. The failure period is set to 15 minutes, and the health check sends a warning for failures of any size and a critical error when 2 KiB of audit events have not been sent.
Publishing Audit Events

Minimum Required Role: Navigator Administrator (also provided by Full Administrator)

Audit events can be published to a Kafka topic or to the system log (syslog). After configuring Cloudera Navigator to send audit events, failures to send events are logged to the Audit Server log.

Publishing Audit Events to Kafka

Navigator can stream audit events to a Kafka topic so the events can be used by another application or archived outside of the Navigator Audit Server database. To configure Navigator to stream audits to a Kafka topic:

1. Create the topic in Kafka.

   If the Kafka instance is configured with Topic Auto Creation enabled, you can skip this step. The topic will be created when the first event is sent to Kafka.

   For steps for creating a Kafka topic, see the Kafka kafka-topics command in Commands for Client Interactions.

2. Log in to Cloudera Manager Admin Console using either Navigator Administrator or Full Administrator privileged account.


4. Click the Configuration tab.

5. If Kafka is managed by the same Cloudera Manager instance as Navigator:

   a. In the Search field, type "kafka" to display the configurable settings.

   b. For the Kafka Service property, select the Kafka service to which Cloudera Navigator will publish audit events.

   c. For the Kafka Topic property, enter the name of the topic to which Cloudera Navigator will publish the audit events.

6. If Kafka is not managed by the same Cloudera Manager instance as Navigator, add properties to accommodate logging for Kafka:

   a. In the Search field, type "logging" to display the configurable settings.
b. For the **Navigator Audit Server Logging Advanced Configuration Snippet (Safety Valve)** property, insert the following logging properties, inserting the brokerList and topic values with the values for your system:

```log4j
log4j.logger.kafkaAuditStream=TRACE,KAFKA
log4j.appender.KAFKA=org.apache.kafka.log4jappender.KafkaLog4jAppender
log4j.additivity.kafkaAuditStream=false
log4j.appender.KAFKA.layout=org.apache.log4j.PatternLayout
log4j.appender.KAFKA.layout.ConversionPattern=%m%n
log4j.appender.KAFKA.syncSend=false
log4j.appender.KAFKA.brokerList=<comma-separated list of brokers as host:port>
log4j.appender.KAFKA.topic=<topic>
```

If Kafka is managed using Cloudera Manager, you can find the broker host names in the **Instances** tab for the Kafka service. List the host and port numbers in a comma-separated list without spaces. For example:

```log4j
kafka-dedicated-1.example.com:9092,kafka-dedicated-2.example.com:9092,kafka-dedicated-3.example.com:9092
```

c. If Kafka is not managed by the same Cloudera Manager instance as Navigator and Kerberos is enabled in the Kafka cluster, there are additional configuration steps.

These steps are described in the Kafka client documentation for security, [Enabling Kerberos Authentication](#).

- Include the following additional properties in the **Navigator Audit Server Logging Advanced Configuration Snippet (Safety Valve)**, inserting the truststore location and truststore password with the values from your system:

```log4j
log4j.appender.KAFKA.SaslKerberosServiceName=kafka
log4j.appender.KAFKA.clientJaasConfPath=navigator.jaas.conf
log4j.appender.KAFKA.SecurityProtocol=SASL_SSL
log4j.appender.KAFKA.SaslTruststoreLocation=/path/to/truststore
log4j.appender.KAFKA.SaslTruststorePassword=<password>
```

- For the Navigator Kafka client create a jaas.conf file with keytabs.

  To generate keytabs, see [Step 6: Get or Create a Kerberos Principal for Each User Account](#).

  Insert the keyTab and principal with the values from your system.

```java
KafkaClient {
  com.sun.security.auth.module.Krb5LoginModule required
  useKeyTab=true
  keyTab="/etc/security/keytabs/mykafkaclient.keytab"
  principal="mykafkaclient/clients.hostname.com@EXAMPLE.COM";
};
```

- Set the location of the jaas.conf in the Navigator host environment.

```sh
export KAFKA_OPTS="-Djava.security.auth.login.config=/home/user/jaas.conf"
```

7. Add a description of the changes and click **Save Changes**.

8. Restart the role.

9. You can validate that events are published to the topic using the Kafka **kafka-console-consumer** command as described in [Commands for Client Interactions](#).

### Publishing Audit Events to Syslog

The Audit Server logs all audit records into a **Log4j** logger called **auditStream**. The log messages are logged at the TRACE level, with the attributes of the audit records. By default, the auditStream logger is inactive because the logger level is set to FATAL. It is also connected to a **NullAppender**, and does not forward to other appenders (additivity set to false).
To record the audit stream, configure the auditStream logger with the desired appender. For example, the standard SyslogAppender allows you to send the audit records to a remote syslog.

The Log4j SyslogAppender supports only UDP. An example syslog configuration would be:

```
$ModLoad imudp
$UDPServerRun 514
# Accept everything (even DEBUG messages)
local2.* /my/audit/trail.log
```

Other appenders can be attached to the auditStream to implement other integration behaviors.

Audit events published to syslog can be formatted as JSON or RSA EnVision. To configure audit logging to syslog:

1. Log in to Cloudera Manager Admin Console using either Navigator Administrator or Full Administrator privileged account.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Locate the Navigator Audit Server Logging Advanced Configuration Snippet property by typing its name in the Search box.
5. Depending on the format type, enter:

   - For JSON:
     ```
     log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender
     log4j.appender.SYSLOG.SyslogHost = hostname
     log4j.appender.SYSLOG.Facility = Local2
     log4j.appender.SYSLOG.FacilityPrinting = true
     log4j.logger.auditStream = TRACE,SYSLOG
     log4j.additivity.auditStream = false
     ```

   - For RSA EnVision:
     ```
     log4j.logger.auditStreamEnVision = TRACE,SYSLOG
     log4j.additivity.auditStreamEnVision = false
     ```

6. Click Save Changes.
7. Restart the role.

Maintaining Navigator Audit Server

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)

When you have Cloudera Navigator running, Navigator Audit Server is enabled by default. Audits are enabled for all supported services, including HDFS, Hive, Impala, Hue, HBase, Sentry, and Solr as well as Cloudera Manager and Navigator itself. Events are retained for 90 days with some default filters defined.

Because the default settings may not work for all environments, we recommend that you review your Navigator Audit Server setup to review these three areas:

- **What events are collected?**
  Default filters remove some service-to-service events. However, you should check to make sure that the role names used in the filters match what's used in your system.

- **How long are events retained?**
  To determine the best expiration period for events in your audit system, consider the volume of incoming events, the disk space available for the audit database, and how your organization is using the audits from the Navigator console or API.

- **How are events archived?**
  Most organizations keep audit events in storage well after they are useful for casual queries through the Navigator console. Your archiving solution should balance the effort required to access archived audit data with the cost of
implementing your archiving system. Be sure that whatever system you design can handle the volume of audits you intend to maintain.

This Navigator YouTube video gives an overview of the audit tuning process and some database queries and other techniques that will help you make sure your audit system is working well.

Reviewing Navigator Audits for Unproductive Events

You can use the Navigator console, Audit tab to get a general feel for what events are audited and if you are seeing too many audit events that don't add value. In addition, here are some queries you can run against the audit database itself to identify users or operations that produce more events than expected or needed.

Review Audited Operations

1. Log into the database as a privileged user.
   For example for MySQL:
   ```
   $ mysql -u user_name -p
   
   You are prompted for a password.
   ```

2. Show the databases and look for the Navigator database.
   ```
   mysql> show databases;
   mysql> use navigator audit server database
   
   If you aren’t sure of the name, you can check the Navigator Audit Server Database Name in Cloudera Manager.
   ```

3. List the tables to see that the table names show the service and the day the audits are from.
   ```
   mysql> show tables;
   ```

4. Pick a table and run a query to show the events recorded by user.
   ```
   mysql> select username, operation, count(*) as usercount from audit table group by username order by usercount DESC;
   
   If you find that a relatively large number of events were collected for a single user, it may be that this user is a system user. The default filters discard events performed by the HDFS superuser, but only if the role name is hdfs. You may need to add another audit filter to discard events by this additional system user name.

5. Pick a table and run a query to show the events recorded by operation.
   ```
   mysql> select operation, username, count(*) as opcount from audit table group by operation order by opcount DESC;
   
   This query may indicate that your audit system includes large numbers of events that you may not care to track. In that case, consider adding an audit filter to discard the unneeded events by operation.

Reviewing Default Audit Filters

To see the default Navigator Audit Filters:

1. Log in to the Cloudera Manager Admin Console.
2. Select the service you want to review. Select **Cluster > Service-Name**
3. Click the **Configuration** tab.
4. Select Service (Service-Wide) for the **Scope** filter.
5. Select Cloudera Navigator for the **Category** filter.
6. Click for Audit Event Tracker to open the property description.

The make sure the default filters are doing what they are designed to do, check that the user names in the filters correspond to the role names in your environment. For example, one default filter is configured to discard redundant audit events produced in HDFS when operations are performed in Hive or other services. This filter is configured for the user hdfs. If your environment uses other names for HDFS superusers, consider creating additional filters to discard the same operations performed under the other superuser names.

Review and Predict Audit Volume

One way to calculate the volume of disk space you’ll need for the Navigator Audit Server database is to look at the event count for a single day or average of days and multiply that volume by the number of days in the audit event expiration period. You can modify the expiration period in Cloudera Manager, in the Navigator Audit Server Data Expiration Period property. The default value is 90 days.

Calculate Audit Volume

1. To see the size of all audit tables for a given date, query against a set of tables. For example, in MySQL:

```
mysql> SELECT table_name AS `Table`, round(((data_length + index_length) / 1024 / 1024), 2)  
2) `Size in MB` FROM information_schema.TABLES WHERE table_schema = "navigator audit  
database" and table_name like "%YYYY_MM_DD%";
```

Insert your Navigator Audit Database name and a valid audit date (YYYY_MM_DD format) in the query.

2. To see the total size of audits for each day for a give year of audits, query against the event tables in the database for a given year:

```
SELECT sum(round(((data_length + index_length) / 1024 / 1024), 2)) `Size in MB across  
all audits`, right(table_name,10) as dateset FROM information_schema.TABLES WHERE  
table_schema = "navigator audit database" and table_name like "%YYYY_%" group by dateset;
```

Insert your Navigator Audit Database name and a valid audit year (YYYY format) in the query.

3. Calculate the expected size of your audit database by selecting a representative size for a day of audit data and multiplying that value by the number of days in the expiration period.

For example, if your system is generating about 5 GB of events per day and you are keeping the default 90 days of audits, you’ll need about 450 GB of space for the audit database.

Navigator Metadata Server Management

The Navigator Metadata Server is one of the two roles that provides Cloudera Navigator data management functionality. The Navigator Metadata Server manages, indexes, and stores entity metadata extracted from cluster services. Using policies defined by data stewards and others, the Navigator Metadata Server can tag entities with metadata or take other actions during the extraction process. It is the metadata that enables data discovery and data lineage functions for Cloudera Navigator.

This section starts with an overview of the Navigator Metadata Server system architecture and then covers administrator tasks that require Cloudera Manager Admin Console such as adding the Navigator Metadata Server role to an existing cluster, tuning for optimal performance, and setting up the LDAP or Active Directory groups to use Cloudera Navigator role-based access privileges.

Navigator Metadata Architecture

The figure below shows a high-level view of the key components that make up the Cloudera Navigator Metadata Architecture. Extracting, indexing, and storing metadata from cluster entities, both on-premises and in the cloud, are some of the important processes implemented by this architecture. As shown in the figure below, Cloudera Navigator can also extract metadata from entities stored on cloud services (Amazon S3) and from clusters running on Amazon EC2 or Cloudera Altus.
Organizations use the Cloudera Navigator console to define their own managed properties to apply to entities contained in the cluster. The Navigator Metadata Server periodically connects to the Cloudera Manager Server and extracts metadata from the entities CDH services (HDFS, Hive, Impala, and so on).

**Note:** Not all services are shown in the image above (for example, Sqoop1, Spark 2).

As it extracts metadata, the Navigator Metadata Server can also apply any policies that have been configured.

For example, a policy may specify that all Hive table entities with table name `budget_2017` be tagged with the managed property name `finance-team`, or that any entities with a file creation date (technical metadata) prior to 2014 be labeled with the prefix `archive-yyyy`, with the specific year obtained from the file creation date and applied to the label.

Extracted metadata is then indexed for later search using the embedded Solr instance. Solr Documents that comprise the index are stored on disk in the storage directory at the location configured in Cloudera Manager Admin Console for the Navigator Metadata Server datadir. See Services Supported for Metadata Extraction on page 101 for more detail.

The Navigator Metadata Server also:
- Manages authorization data for Cloudera Navigator users
- Manages audit report metadata
- Generates metadata and audit analytics
- Exposes the Cloudera Navigator APIs
- Hosts the web server that provides the Cloudera Navigator console. (The web server and the console are also used to support the Cloudera Navigator Auditing services.)

The Navigator Database stores policies, user authorization and audit report metadata, and analytic data. Extracted metadata and the state of extractor processes is kept in the storage directory.
Services Supported for Metadata Extraction

The Navigator Metadata Server extracts metadata for the resource types listed in the table. Metadata is "pulled" by Navigator Metadata Server or "pushed" from the service through the Cloudera Manager agent on the host where the service is running.

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Metadata Extracted</th>
<th>Extraction Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>HDFS metadata at the next scheduled extraction run after an HDFS checkpoint. If the cluster is configured for high availability (HA), metadata is extracted at the same time it is written to the JournalNodes.</td>
<td>Pull</td>
</tr>
<tr>
<td>Hive Server 2</td>
<td>Query metadata is pushed to Navigator as queries occur. See Managing Hive and Impala Lineage Properties.</td>
<td>Push</td>
</tr>
<tr>
<td>Hive Metastore</td>
<td>Database asset metadata (database, tables, views, partitions, columns). See Managing Hive and Impala Lineage Properties. HMS entities include tables that result from Impala queries and Sqoop jobs.</td>
<td>Pull</td>
</tr>
<tr>
<td>Impala</td>
<td>Query metadata is pushed to Navigator from the Impala Daemon lineage logs. See Managing Hive and Impala Lineage Properties. When using Hue to perform Impala queries, after running the query, the lineage won’t show up in Navigator until Impala determines that the query is complete (Hue gives users the opportunity to pull another set of results on the same query). Lineage metadata is sent after Impala reaches its configured query timeout or an event such as another query or logging out of Hue. To reduce the timeout, see: • For impalad Setting the Idle Query and Idle Session Timeouts for impalad • In Hue: IDLE_SESSION_TIMEOUT Query Option (or higher only) and QUERY_TIMEOUT_S Query Option (or higher only)</td>
<td>Push</td>
</tr>
<tr>
<td>MapReduce</td>
<td>Job metadata from the JobTracker. The default setting in Cloudera Manager retains a maximum of five jobs; if you run more than five jobs between Navigator extractions, the Navigator Metadata Server extracts the five most recent jobs.</td>
<td>Pull</td>
</tr>
<tr>
<td>Oozie</td>
<td>Oozie workflows from the Oozie Server.</td>
<td>Pull</td>
</tr>
<tr>
<td>Pig</td>
<td>Pig script runs from the JobTracker or Job History Server.</td>
<td>Pull</td>
</tr>
<tr>
<td>S3</td>
<td>Bucket and object metadata.</td>
<td>Pull</td>
</tr>
<tr>
<td>Spark</td>
<td>Query metadata is pushed to Navigator as queries occur. Spark job metadata from YARN logs is pulled as part of the YARN extractor. Note that Spark 1.6, which is included with CDH, and CDS 2 Powered by Apache Spark include integration with Navigator. Third-party versions of Spark do not produce metadata for Navigator lineage.</td>
<td>Push</td>
</tr>
<tr>
<td>Sqoop 1</td>
<td>Query metadata is pushed to Navigator as queries occur. Database and table metadata comes from the HMS extraction.</td>
<td>Push</td>
</tr>
<tr>
<td>YARN</td>
<td>Job metadata from the ResourceManager.</td>
<td>Pull</td>
</tr>
</tbody>
</table>

Metadata Extraction Timing

The two types of Navigator extractors have different timing: Push extractors send metadata to Navigator after each event that generates metadata (Hive Server 2, Impala, Spark, Sqoop). Pull extractors run about every 10 minutes, when Navigator Metadata Server triggers them (Oozie, YARN, HDFS, HMS, S3). When the 10 minute mark comes around for a given service, Navigator checks to see if an extraction process is already running; if one is, Navigator resets the wait
time without starting another extraction. Extractors for different services typically run simultaneously, inserting new metadata into Navigator in a regular cadence. However, extractor behavior and timing for HMS and HDFS can be more complicated because of the volume of metadata they collect in a single extractor run.

**HMS Extraction**

Navigator extracts metadata from Hive Metastore (HMS) through a pull extractor where Navigator Metadata Server triggers the extraction. Every time Navigator extracts HMS metadata, it reviews all databases for all data assets: tables, views, partitions, etc. There is no incremental extraction from HMS. When your HMS includes many databases and lots of assets, the extraction can take a long time: certainly more than the 10 minute extraction interval.

As it progresses through the extraction, Navigator creates new entities for any data assets that aren’t already represented in Navigator.

**HDFS Extraction**

Navigator extracts metadata for HDFS from the namenode. After the initial extraction, Navigator users iNotify to extract changes to HDFS contents rather than re-extracting all entities again. The initial HDFS extraction process still requires a long period; subsequent extractions may be more likely to conform to the 10-minute pattern. If Navigator encounters an a iNotify failure, it will fall back to bulk extraction.

**Calculating Lineage from Metadata**

As described in detail in Lineage Generation Architecture on page 49, lineage is generated when Navigator combines the metadata for data assets (such as file, tables, views) with the metadata for operation executions (queries and jobs). Tables and views come from HMS extraction, while operation executions come from push extractors for Impala, Hive Server 2, Spark, YARN, and Sqoop. If any of the metadata is missing (not extracted yet), lineage relationships aren’t calculated or displayed. For lineage relationships to be displayed completely, Navigator must have completed extraction from each of the services involved and then it must run a lineage calculation process called "linking."

To understand the timing of how metadata and lineage relationships become available in the Navigator console, consider the pull extractor for HMS and a push extractor from Hive Server 2 as they run independently. Lineage metadata, which requires metadata from both HMS and a query engine, appears in the Navigator console only after both extraction operations are complete and the linker process runs. The following illustration describes the timing for each of the processes that must complete for lineage to appear in the console:

1. HMS Extraction is a long-running process that steps through HMS one database at a time.
2. Query engines such as Hive Server 2 push metadata updates to Navigator as soon as an event occurs: In this example, a query that creates table X is pushed to Navigator and Navigator creates an operation entity and an
operation execution entity to represent the query. Navigator creates lineage relationship entities for the new
table, but the relationships are left "unlinked" because the new table doesn't yet exist in Navigator.

3. The HMS extraction gets to the database where the table was created and passes the metadata to Navigator,
which creates a new entity for the table.

4. After the HMS extraction finishes, Navigator triggers a linker process that reviews the "unlinked" lineage relations
and connects them to the correct entities. Now the table created in step 2 is included in the lineage relationship
created to describe the query.

5. Lineage for the new table appears in the Navigator console.

Note that step 3 is a variable here: it’s possible that the HMS extraction run may have already processed the relevant
database (1) before the query occurred (2). In that case, the HMS extraction would complete and linking would run
(3), but there would not be an entity in place for the new table. Lineage for the new table doesn’t appear until the next
HMS extraction run reaches the relevant database (4) to create the table entity; then linking runs at the end of the
HMS extraction (5) and adds the correct lineage information (6).

Troubleshooting

If Navigator is missing entities for:

- Queries: check the push extractor processing. The Navigator logs won’t show any problems in this case. Instead,
  check the Cloudera Manager agent log on the host where the suspect service is running.
- Data asset entities: check the HMS pull extractor processing in the Navigator Metadata Server log.
- Filesystem entities: check the HDFS or S3 extractor processing in the Navigator Metadata Server log.

If Navigator is missing lineage, make sure that Navigator shows the entities for both the data assets and the queries
that describe the lineage; then give enough time for the lineage processing to complete. If you are running Impala
queries from Hue, Hue doesn’t close out the query right away, giving you a chance to show additional pages or results.
Impala doesn’t send metadata to Navigator until that query is complete, so you may have to wait until the Impala
query timeout is past, exit Hue, or trigger a new query to close the current query. If you still don’t see lineage relations,
check to make sure the linker is running (in the Navigator Metadata Server log). If HMS extraction never completes,
you may see metadata for some data assets, but the linking process may not have been triggered. Check the Navigator
Metadata Server log.

The pull extraction frequency can be configured using nav.extractor.poll_period in the Navigator Metadata
Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties in Cloudera Manager. Note
that lowering the polling period won’t affect latency if your system has one of the problems described here.

To find pull extractor events in the Navigator Metadata Server log, look for "extraction tasks for service", then filter
further on the specific services you are interested in. For example:

```
[[ExtractorServiceExecutor-3] Cluster 1::HIVE-1]: Enqueuing 6 extraction tasks for
service 'Cluster 1::HIVE-1'...
```

```
```
In this example, it took 10 minutes to finish the first extraction (20:26:00 - 20:15:58). Navigator waited 10 minutes to start the second extraction (20:35:58). The second extraction took 20 minutes to finish (20:56:00 - 20:35:58). The third extraction started 10 minutes after the second one finished (21:05:59), a total of 30 minutes after the start time of the second extraction.

Metadata Indexing

After metadata is extracted, the embedded Solr engine indexes it and makes it available for searching. The Solr instance indexes entity properties and the relations among entities. Relationship metadata is implicitly visible in lineage diagrams and explicitly available by downloading the lineage using the Cloudera Navigator APIs.

Data stewards and other business users explore entities of interest using the Cloudera Navigator console. Metadata and lineage that has been extracted, linked, and indexed can be found using Search. See Lineage, Metadata and other sections in this guide for Cloudera Navigator console usage information. The following sections focus on using the Cloudera Manager Admin Console for systems management tasks.

Setting Up Navigator Metadata Server

In addition to the basic configuration topics discussed below, see Navigator Metadata Server Tuning for memory sizing and other considerations.

Setting up Navigator Role Instances on Different Hosts

By default, the Cloudera Manager installation wizard assigns the Navigator Audit Server and Navigator Metadata Server roles to the same Cloudera Management Service host. This configuration can support small clusters but larger production clusters often need these roles distributed to different nodes for better performance. You can distribute these roles to different nodes at install time or you can move the Navigator Metadata Server later if necessary.

Adding the Navigator Metadata Server Role

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

1. Configure the database where policies, roles, and audit report metadata is stored. For production environments, Cloudera supports only external databases. The internal PostgreSQL database should be used for non-production clusters only, such as proof-of-concept.
   - For external databases (production environments): The database should be up and running before you add the Navigator Metadata Server role to the cluster. You must have the database schema name (user name), password, and other details to provide when adding the role. When you have these ready, you can proceed.
   - For internal databases (non-production environments): No additional preliminary information is needed. You can proceed.

2. Log in to the Cloudera Manager Admin Console.
4. Click the Instances tab.
5. Click the Add Role Instances button. The Customize Role Assignments page displays and lists the nodes available to support additional roles, assuming the cluster has available resources. Reassign and customize role instances as needed.
6. Select the Navigator Metadata Server role and assign it to appropriate host for your cluster.
7. When finished, click Continue. The Database Setup page displays.
8. Click Use Custom Database.
9. In the **Navigator Metadata Server** section, enter the details of your database instance:
   
   - Database host name
   - Database type
   - Database name
   - Username
   - Password

   **Note:** Do not use the embedded database for production deployments. It is not a supported configuration. For non-production environments only you can select Use Embedded Database to have Cloudera Manager create and configure the database for you. Make a note of the generated passwords.

Here is an example of a configured custom (external) database instance that uses MySQL for the Navigator Metadata Server database:

10. Click **Test Connection** to verify the communication between the cluster and the external database. If the test fails, check the database settings and try again. If you selected embedded database, a message displays regarding database creation.

11. Click **Continue**.
12. The **Cluster Setup Review Changes** page displays.
13. Click **Finish**.

**Removing the Navigator Metadata Server Role**

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the **Instances** tab.
4. Select the Navigator Metadata Server role type.
5. If the Navigator Metadata Server role is not already stopped, choose Actions for Selected > Stop. Click Stop to confirm the action.

6. Select the Navigator Metadata Server role type.
7. Choose Actions for Selected > Delete. Click Delete to confirm the action.

Starting, Stopping, and Restarting a Navigator Metadata Server Role Instance

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Instances tab.
4. Click the link for the Navigator Metadata Server from the Role Type list. The Actions for Selected button activates and displays (1) for the selected role.
5. From the Actions for Selected (1) menu, select the Action you want to perform on this role instance:
   - Start
   - Stop
   - Restart
   - Enter Maintenance Mode
   - Exit Maintenance Mode
   - Delete

   A confirmation message displays giving you the option to Cancel or complete the specified Action.
6. Click Cancel to abandon the process, or click Action to execute the action.

Backup Navigator Metadata Server Data

Navigator Metadata Server stores metadata in an embedded Solr data directory and in a database instance. Back up these locations together so the backups describe the same metadata state.

1. Shut down the Navigator Metadata Server role.
2. Backup the data directory.

   The Navigator Metadata Server default directory is `/var/lib/cloudera-scm-navigator`. To confirm that this is the path your deployment uses, log in to the Cloudera Manager Admin Console and search for the Navigator Metadata Server Storage Dir property (`nav.data.dir`).
3. Backup the database instance.
   - Confirm the Navigator Metadata Server database location and connection information.

   To locate this information, log in to the Cloudera Manager Admin Console and go to Clusters > Cloudera Management Service. Click the Configuration tab. Select Scope > Navigator Metadata Server. Select Category > Database. The results indicate the type, host, database name, and login account.

   - Using the appropriate tool for the database instance (such as MySQL), backup the database. See Back Up the Cloudera Manager Databases.

4. Start the Navigator Metadata Server role.

Moving the Navigator Metadata Server to a New Host

**Cloudera Manager Required Role:** Navigator Administrator (or Full Administrator)
When resources become tight on the host where Navigator servers are installed, one solution is to move one or both servers to another host or hosts. These instructions describe moving only the Navigator Metadata Server. Be sure to stop the Navigator Metadata Server before backing up the storage directory.

1. **Stop the Navigator Metadata Server role.**
2. **Backup the Navigator Metadata Server database and storage directory.**
3. **Delete the Navigator Metadata Server role** from the existing host.
4. If the storage directory is not on NFS/SAN, move the data to the same path on the new host.

By default, the Navigator Metadata Server storage directory is `/var/lib/cloudera-scm-navigator`. This value is set in the Cloudera Manager **Navigator Metadata Server Storage Dir** property (`nav.data.dir`). If you want to put the directory in a different location, change the property when you reconfigure the Navigator Metadata Server role and before you restart the role.

5. **Add the role to a new host.**

This step includes configuring the new storage directory location and specifying the database connection information. See **Adding the Navigator Metadata Server Role** on page 104 for details.

6. Make sure the Navigator Metadata Server storage directory is configured correctly for the new host. See **Configuring the Navigator Metadata Server Storage Directory** on page 108.

**Important:** Make sure that the storage directory is in place and the Cloudera Manager configuration is correct before starting the Navigator Metadata Server role on the new host. If Navigator Metadata Server starts without finding the storage directory, it will create a new one, which will not be synchronized with the database and the move will fail. If this happens, stop the server, replace the newly created storage directory with the backup from step 2 and restart the server.

7. **Start the Navigator Metadata Server.**

**Setting the Navigator Metadata Server Java Heap Size**

**Cloudera Manager Required Role:** **Navigator Administrator** (or **Full Administrator**)

Use the formula discussed in **Memory Sizing Considerations for Navigator Metadata Server** to calculate optimal Java heap size:

\[
((\text{num}_\text{nav}_\text{elements} + \text{num}_\text{nav}_\text{relations}) \times 200 \text{ bytes}) + 2 \text{ GB}
\]

Briefly, the total of `num_nav_elements` and `num_nav_relations` is the number of Solr documents (per the Navigator Metadata Server log file) that comprise the index. See **sizing guidelines** for complete details. If you are just starting your Navigator deployment, set the Java heap size to at least 10 GB and as much as 30 GB if you have the memory available on the Navigator host.

After you have determined an appropriate Java heap setting using this or another technique, you can change the setting as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select **Clusters > Cloudera Management Service**.
3. Click the **Configuration** tab.
4. Select **Scope > Navigator Metadata Server**.
5. For Filter **Category**, click **Resource Management** to display the Java heap size property. The default value is 1.5 GiB (specified in **binary units**).
6. Use the drop-down selector to change the unit scale to B (Bytes), KiB, MiB, or GiB and set your preferred heap size.

7. Click Save Changes. The setting takes effect only after restarting the role. Restart the Navigator Metadata Server role now or make other configuration changes and restart after you are finished with all changes. To restart the role:

8. Click the Instances tab to display list the list of instances of each role type.

9. Click the link for the Navigator Metadata Server to select it.

10. From the Actions for Selected (1) menu, select Restart to restart the Navigator Metadata Server role instance using the new Java heap size.

Configuring the Navigator Metadata Server Storage Directory

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

Navigator Metadata Server uses a Solr instance (a search engine) to index extracted metadata for fast search and retrieval. The searchable Solr documents are stored in a directory on the host on which the Navigator Metadata Server runs. The default location for the directory is /var/lib/cloudera-scm-navigator.

To change the location of the storage directory:

1. Log in to the Cloudera Manager Admin Console.

2. Select Clusters > Cloudera Management Service.

3. Click the Instances tab.

4. Click the link for the Navigator Metadata Server to select it.

5. From the Actions for Selected (1) menu, select Stop.

6. Open a terminal session and log in to the host configured to run Navigator Metadata Server.

7. Copy the contents of the current storage directory to the new location. When copying is complete, return to the Cloudera Manager Admin Console.

8. Click the Configuration tab.


10. Enter the directory path in the Navigator Metadata Server Storage Dir property. The property applies to the default role group, but you can apply to other role groups as needed. See Modifying Configuration Properties Using Cloudera Manager for details.

11. Click Save Changes. This change does not take effect until the Navigator Metadata Server role is restarted.

12. Click the Instances tab.

13. Click the link for the Navigator Metadata Server from the list of instances.

14. From the Actions for Selected menu, select Restart to restart the Navigator Metadata Server role instance.

Configuring the Navigator Metadata Server Port

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

The Cloudera Navigator console is accessed at port 7187 by default, on the host supporting the Navigator Metadata Server role. Follow the steps below to change setting.

1. Log in to the Cloudera Manager Admin Console.

2. Select Clusters > Cloudera Management Service.

3. Click the Configuration tab.

4. In the Search box, type the word "ports" to display properties.

5. Specify the port in the Navigator Metadata Server Port property. The property applies to the default role group, but you can apply to other role groups as needed. See Modifying Configuration Properties Using Cloudera Manager for details.

6. Click Save Changes.

7. Click the Instances tab.

8. Restart the Navigator Metadata Server role.
Configuring the Navigator Metadata Server Log Directory

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

The default location of the Navigator Metadata Server logs is /var/log/cloudera-scm-navigator, but you can change to a different location, as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
5. Under Filter Category, click Logs.
6. Set the Navigator Metadata Server Log Directory property. The property applies to the default role group, but you can apply to other role groups as needed. See Modifying Configuration Properties Using Cloudera Manager for details.
7. Click Save Changes.
8. Restart the Navigator Metadata Server role instance.

Configuring the Navigator Metadata Server Session Timeout

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

The default session timeout is 30 minutes (1800 seconds). To change the timeout period:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
5. For Filter Category, click Advanced. Scroll to find the Advanced Configuration Snippet (Safety Valve) entry field for cloudera-navigator.properties.
6. Set the value for the nav.max_inactive_interval property to the number of seconds that can elapse before system times out:

   nav.max_inactive_interval=num-seconds-until-timeout

   This example reduces the timeout period from the default of 30 minutes to 15 minutes:

7. Click Save Changes.
8. Restart the Navigator Metadata Server role instance.

Disabling Anonymous Usage Collection

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

Cloudera Navigator by default sends anonymous usage information to Cloudera for analysis. The usage information helps Cloudera improve Cloudera Navigator functionality and pro-actively identify areas of the product to enhance. The information is completely anonymous and cannot be traced to any customer installation.

To disable anonymous usage information collection:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
4. Under the Filter for **Scope**, click **Navigator Metadata Server**.
5. Click the **Allow Usage Data Collection** to clear the checkbox.
6. Click **Save Changes**.
7. Restart the Navigator Metadata Server role instance.

Cloudera Navigator stops emitting anonymous usage information.

This capability can be re-enabled at any time by clicking the Allow Usage Data Collection box that has been cleared.

**Configuring Navigator Metadata Server for Kerberos and Custom Keytab Retrieval**

If Navigator is running on a Kerberized cluster and the cluster is set up to use a custom keytab retrieval script, you need to manually put keytabs for HDFS and Hue principals into the Navigator home directory (typically `/var/lib/cloudera-scm-navigator`) for use by the Navigator web server.

If the keytabs are not available, you'll see Navigator Metadata Server log errors such as the following:

```plaintext
Error running extraction task.
java.lang.RuntimeException: java.util.concurrent.ExecutionException:
java.lang.RuntimeException: java.io.IOException: Login failure for
hdfs/node.example.com@EXAMPLE.COM from keytab
/var/lib/cloudera-scm-navigator/temp/1234/hadoop1234.keytab:
javax.security.auth.login.LoginException: Unable to obtain password from user
```

**Navigator Metadata Server Configuration Settings Summary**

Access to the Cloudera Manager Admin Console and the ability to change any of the settings in the table below requires the Cloudera Manager user role of Navigator Administrator or Full Administrator.

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigator Metadata Storage Dir</td>
<td>/var/lib/cloudera-scm-navigator</td>
<td>Change to another path if you like. Be sure to move existing content from the default directory to the new directory to maintain state. Offload content from this directory prior to upgrading for faster upgrades.</td>
</tr>
<tr>
<td>Cloudera Navigator Server Port</td>
<td>7187</td>
<td>Change to another port if necessary. This is the port used to access Cloudera Navigator console.</td>
</tr>
<tr>
<td>Navigator Metadata Server Log Directory</td>
<td>/var/log/cloudera-scm-navigator</td>
<td>Examine the log to find out how many documents the Solr index contains, and use that count to estimate Java heap size needed for normal operations and for upgrades. Use the log to troubleshoot issues.</td>
</tr>
<tr>
<td>Server Session Timeout</td>
<td>30 minutes (1800 seconds)</td>
<td>Timeout is specified in number of seconds that must elapse before the system generates a timeout event.</td>
</tr>
<tr>
<td>Allow Usage Data Collection</td>
<td>enabled</td>
<td>Cloudera Navigator uses Google Analytics to anonymous usage data to Cloudera for product enhancement. Disable this setting if you do not want to send usage data.</td>
</tr>
</tbody>
</table>

**Navigator Metadata Server Tuning**

This page can help you tune your Navigator Metadata Server instance for peak performance. See also Setting up Navigator Role Instances on Different Hosts.
Memory Sizing Considerations for Navigator Metadata Server

Unlike Navigator Audit Server for which configured Java heap size is rarely an issue, Navigator Metadata Server encompasses two processes that have a direct impact on memory, specifically:

- Extracting metadata from the cluster and creating relationships among the metadata entities (facilitating lineage)
- Querying to find entities

Navigator Metadata Server uses Solr to index, store, and query metadata. Indexing occurs during the extraction process, with the resulting Solr documents—data structure used by Solr for index and search—stored in the specified Navigator Metadata Server Storage Dir. Because the metadata is indexed, querying is fast and efficient. However, Solr indexing runs in-process with Navigator Metadata Server, so the amount of memory configured for the Java heap is critical.

There is a direct correlation between the number of Solr documents contained in the index and the size of the Java heap required by Navigator Metadata Server, so this setting may need to be changed over time as the number of Solr documents making up the index increases. To calculate optimal Java heap setting for your system, see Estimating Optimal Java Heap Size Using Solr Document Counts.

Estimating Optimal Java Heap Size Using Solr Document Counts

Each time it starts up, Navigator Metadata Server counts and logs the number of Solr documents in the datadir (the Navigator Metadata Server storage directory), as shown below:

```
```

These counts can be used to estimate optimal Java heap size for the server, as detailed below. If your normal setup provides less than 8 GB for the Navigator Metadata Server heap, consider increasing the heap before performing an upgrade. See Setting the Navigator Metadata Server Java Heap Size for details about using Cloudera Manager Admin Console to modify this setting when needed.

**Note:** If your system has been running without interruption for awhile, the data in the log may be stale. Restart the Navigator Metadata Server when it is convenient and then look at the log to find the current number of documents to use in the calculation.

To estimate the Java heap size:

1. Open the log file for Navigator Metadata Server. By default, logs are located in /var/log/cloudera-scm-navigator.
2. Find the number of documents in solr core nav_elements line in the log.
3. Find the number of documents in solr core nav_relations line in the log.
4. Multiply the total number of documents by 200 bytes per document and add to a baseline of 2 GB:

\[(\text{num}\_\text{nav}\_\text{elements} \times 200 \text{ bytes}) + 2 \text{ GB}\]

For example, using the log shown above, the recommended Java heap size is ~14 GiB:

\[(68813088 \times 200) + 2 \text{ GB} \]

\[13762617600 \text{ bytes} = ~12.8 \text{ GiB} + 2 \text{ GB} (-1.8 \text{ GiB}) = ~14-15 \text{ GiB}\]
Important: If you are upgrading to a Cloudera Manager version 5.10.0 or later, you'll need considerably more Java heap to perform the upgrade. Upgrading to the 5.10 release includes the unusual performance of a schema change in Solr. This operation requires additional Java heap for the duration of the upgrade process. To calculate the recommended Java heap for the upgrade, multiply the total number of documents by 200 bytes per document and add to a baseline of 2 GB:

\[
\text{((num\_nav\_elements + num\_nav\_relations) * 200 \text{ bytes}) + 2 \text{ GB}}
\]

For example, using the log shown above, the recommended Java heap size is ~31 GiB:

\[
((\text{68813088 + 78813930}) * 200) + 2 \text{ GB} \\
29525403600 \text{ bytes} = \sim 29.5 \text{ GiB + 2 GB (1.8 GiB)} = \sim 31.3 \text{ GiB}
\]

Purging the Navigator Metadata Server of Deleted and Stale Metadata

In addition to adjusting the Java heap size, administrators can also clear the Navigator Metadata Server of stale and deleted metadata prior to an upgrade or whenever system performance seems slow. Purging stale and deleted metadata also helps speed up display of lineage diagrams. Purge fully removes metadata that has been deleted.

Cloudera Navigator console (Administration tab) provides a fully configurable Purge Settings page. See Managing Metadata Storage with Purge for details. You can also invoke purge capability using the Cloudera Navigator APIs. See Using the Purge APIs for Metadata Maintenance Tasks for details.

Configuring and Managing Extraction

Entities extracted from cluster services and the metadata that is applied to them supports Cloudera Navigator features, such as the ability to trace entities to their source in lineage diagrams, search for specific entities, and so on. Extraction is enabled for some services by default, while for other services, extraction must be specifically enabled. For example, extraction is enabled for Spark by default. Extraction consumes computing resources, such as memory and storage, so administrators may want to disable extraction for some services entirely, or configure more selective extraction for specific services.

In addition to configuring extraction for specific services, specific filters can be configured to blacklist specific HDFS paths to remove them from the extraction process which both speeds up the process and cuts down on indexing time, as well as the amount of storage consumed by the datadir. Filters can also be configured to blacklist or whitelist Amazon S3 buckets.

Note: Make sure to configure the metadata purge function, which cleans the Solr storage directory of documents that describe the deleted entities. Using purge on a regular basis facilitates fast search and noise-free lineage diagrams. See Managing Metadata Storage with Purge on page 70.

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

Enabling Hive Metadata Extraction in a Secure Cluster

To extract entities from Hive, the Navigator Metadata Server authenticates to the Hive metastore using the hue user account. By default the hue user has privileges and can log in to the Hive metastore for authentication. That means that if the Hive metastore configuration was changed from the defaults, user hue may not be able to authenticate and the Navigator Metadata Server will be prevented from extracting from Hive. The specific configuration properties are the following two, which work together for authentication for Hive:

- Hive Metastore Access Control and Proxy User Groups Override (Inherits from Hive Proxy User Groups when left empty (the default))
- Hive Proxy User Groups

1. Log in to Cloudera Manager Admin Console.
2. Select Clusters > Hive-1.
3. Click the Configuration tab.
4. Select **Proxy** for the **Category** filter.

5. Add **hue** to the **Hive Metastore Access Control and Proxy User Groups Override** list if necessary:
   - Click the plus icon to open an entry field to add a row to the property.
   - Type **hue** in the entry field.

6. Click **Save Changes**, and repeat the process to add the Hive Proxy User Groups property on the HDFS server:
   - Select **Clusters** > **Hive-1**.
   - Click the **Configuration** tab.
   - Select **Proxy** for the **Category** filter.
   - Add **hue** to the **Hive Proxy User Groups** list by adding a row and typing **hue** in the entry field.

7. Click **Save Changes**.

8. Restart the Hive service.

**Disabling Spark Metadata Extraction**

Metadata and lineage for Spark is extracted by default (see [Apache Spark Known Issues](#) for limitations). To disable Spark metadata extraction:

1. Log in to Cloudera Manager Admin Console.
2. Select **Clusters** > **Spark_on_YARN-1**.
3. Click the **Configuration** tab.
4. Select **Cloudera Navigator** for the **Category** filter. The state of the Enable Lineage Collection feature displays, as in this example:

   ![Enable Lineage Collection](image)

5. To disable lineage collection, click the checked box.

**Editing MapReduce Custom Metadata**

You can associate metadata with arbitrary configuration parameters to MapReduce jobs and job executions. The configuration parameters to be extracted by Cloudera Navigator can be specified statically or dynamically.

To specify configuration parameters statically for all MapReduce jobs and job executions, do the following:

1. Log in to Cloudera Manager Admin Console.
2. Select **Clusters** > **Cloudera Management Service**.
3. Click the **Configuration** tab.
4. Select **Navigator Metadata Server** for the **Scope** filter.
5. Select **Advanced** for the **Category** filter.
6. Scroll to find the **Navigator Metadata Server Advanced Configuration Snippet for cloudera-navigator.properties**.
7. Specify values for the following properties:
   - **nav.user_defined_properties** - A comma-separated list of user-defined property names.
   - **nav.tags** - A comma-separated list of property names that serve as tags. The property **nav.tags** can point to multiple property names that serve as tags, but each of those property names can only specify a **single** tag.

8. Click **Save Changes**.

9. Click the **Instances** tab.

10. Restart the role.
In the MapReduce job configuration, set the value of the property names you specified in step 7.

To specify configuration parameters dynamically:

1. Specify one or more of the following properties in a job configuration:
   - **Job properties (type:OPERATION)**
     - nav.job.user_defined_properties - A comma-separated list of user-defined property names
     - nav.job.tags - A comma-separated list of property names that serve as tags
   - **Job execution properties (type:OPERATION_EXECUTION)**
     - nav.jobexec.user_defined_properties - A comma-separated list of user-defined property names
     - nav.jobexec.tags - A comma-separated list of property names that serve as tags

   The properties nav.job.tags and nav.jobexec.tags can point to multiple property names that serve as tags, but each of those property names can only specify a single tag.

2. In the MapReduce job configuration, set the value of the property names you specified in step 1.

Setting Properties Dynamically

Add the tags onetag and twotag to a job:

1. Dynamically add the job_tag1 and job_tag2 properties:

   ```java
   conf.set("nav.job.tags", "job_tag1, job_tag2");
   ```

2. Set the job_tag1 property to onetag:

   ```java
   conf.set("job_tag1", "onetag");
   ```

3. Set the job_tag2 property to twotag:

   ```java
   conf.set("job_tag2", "twotag");
   ```

Add the tag atag to a job execution:

1. Dynamically add the job_tag property:

   ```java
   conf.set("nav.jobexec.tags","job_exec_tag");
   ```

2. Set the job_exec_tag property to atag:

   ```java
   conf.set("job_exec_tag", "atag");
   ```

Add the user-defined key key with the value value:

1. Dynamically add the user-defined key bar:

   ```java
   conf.set("nav.job.user_defined_properties", "key");
   ```

2. Set the value of the user-defined key key to value:

   ```java
   conf.set("key", "value")
   ```

Enabling Inputs and Outputs to Display

The Cloudera Navigator console displays a Details page for selected entities. Details include an entity's type and can optionally include table inputs and operation inputs and outputs. The inputs and outputs are not displayed by default.
because rendering them can slow down the display. Enabling the display of inputs and outputs in the Details page requires changing the `nav.ui.details_io_enabled` on the Navigator Metadata Server to `true`, as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click the Configuration tab.
5. Select Advanced for the Category filter.
6. In the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for `cloudera-navigator.properties`, enter the following:

   ```
   nav.ui.details_io_enabled=true
   ```

7. Click Save Changes.
8. Restart the Navigator Metadata Server role.

### Hive and Impala Lineage Configuration

**Cloudera Manager Required Role:** Configurator (or Cluster Administrator, or Full Administrator)

Unlike for other services running in the cluster (such as Pig), lineage data from Hive and Impala queries is not extracted by Navigator Metadata Server. Instead, these two services write query data to log files collected in a specific directory on the cluster node. The Cloudera Manager Agent process running on that node monitors the directory and routinely sends the log files to the Navigator Metadata Server, where the query data is coalesced with other metadata collected by the system.

Lineage collection from Hive and from Impala log files is enabled by default—each of these services has its own Enable Lineage Collection property and some related configuration properties, which can be disabled or reconfigured as detailed below.

#### Modifying Lineage Collection Settings for Hive

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Lineage Collection</td>
<td>Enabled for Hive, Service-Wide</td>
<td>Enable collection of lineage from the service’s roles.</td>
</tr>
<tr>
<td>Hive Lineage Log Directory</td>
<td>/var/log/hive/lineage</td>
<td>Directory in which Hive lineage log files are written.</td>
</tr>
<tr>
<td>(lineage_event_log_dir)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hive Maximum Lineage Log File</td>
<td>100 MiB</td>
<td>Maximum size (MiB, GiB) of Hive lineage log file before a new file is created.</td>
</tr>
<tr>
<td>Size (max_lineage_log_file_size)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To disable Hive lineage collection:

control whether the Impala Daemon role logs to the lineage log and whether the Cloudera Manager Agent collects the Hive and Impala lineage entries:

1. Log in to Cloudera Manager Admin Console.
2. Select Clusters > Hive.
3. Click the Configuration tab.
4. Type `lineage` in the Search box.
5. Click the Enable Lineage Collection check-box to deselect it and disable lineage collection.
6. Click Save Changes.
7. Restart the Hive service.
Modifying Lineage Collection Settings for Impala

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Impala Lineage Generation (enable_lineage_log)</td>
<td>Enabled for the Impala daemon default group</td>
<td>When enabled, Impala daemon process creates a logfile containing lineage data and stores it in the directory specified by the Impala Daemon Log Lineage Directory property.</td>
</tr>
<tr>
<td>Enable Lineage Collection</td>
<td>Enabled for Impala Service-Wide</td>
<td>Enable collection of lineage from the service’s roles.</td>
</tr>
<tr>
<td>Impala Daemon Lineage Log Directory in which Impala daemon lineage log files are written. When Impala Lineage Generation property is enabled, Impala generates its lineage logs in this directory.</td>
<td>/var/log/impalad/lineage</td>
<td></td>
</tr>
<tr>
<td>Impala Daemon Maximum Lineage Log File Size (max_lineage_log_file_size)</td>
<td>5000</td>
<td>Maximum number of Impala daemon lineage log file entries (queries) written to file before a new file is created.</td>
</tr>
</tbody>
</table>

The Enable Lineage Collection property determines whether lineage logs should be collected by the Cloudera Manager Agent. To control whether the Impala Daemon role logs to the lineage log and whether the Cloudera Manager Agent collects the Hive and Impala lineage entries:

To disable lineage collection for Impala queries:

1. Log in to Cloudera Manager Admin Console.
2. Select Clusters > Impala.
3. Click the Configuration tab.
4. Type lineage in the Search box.
5. Click the Enable Lineage Collection check-box to deselect it and disable lineage collection.
6. Click the Enable Impala Lineage Generation check-box to deselect it.
7. Click Save Changes.
8. Restart the Impala service.

De-selecting either Enable Lineage Collection or Enable Impala Lineage Generation disables lineage collection for Impala.

Configuring Hive on Spark and Impala Daemon Lineage Logs

If the value of a log directory property is changed, and service is restarted, the Cloudera Manager Agent starts monitoring the new log directory. In this case it is possible that not all events are published from the old directory. To avoid losing lineage information when this property is changed, perform the following steps:

1. Stop the affected service.
2. Copy the lineage log files and (for Impala only) the impalad_lineage_wal file from the old log directory to the new log directory. This needs to be done on the HiveServer2 host and all the hosts where Impala Daemon roles are running.
3. Start the service.

To edit lineage log properties:

1. Go to the service.
2. Click the Configuration tab.
3. Type lineage in the Search box.
4. Edit the lineage log properties.
5. Click Save Changes.
6. Restart the service.
Configuring the Server for Policy Messages

Cloudera Navigator can send notifications to a JMS message queue whenever entities change as a result of policies set for that class of entity. To use this capability, an administrator must setup a JMS server with a queue for the messages and then configure the JMS server using the Cloudera Manager Admin Console, as detailed below.

In addition to setting up and configuring the server side components, the policies (that include notifications about changes) are defined using the Cloudera Navigator console. See Using Policies to Automate Metadata Tagging for details about defining policies.

Configuring a JMS Server for Policy Messages

Cloudera Manager Required Role: Navigator Administrator (or Full Administrator)

Only the JMS URL, JMS User, and JMS Password settings are required to set up the JMS Server. Enable Expression Input only if you want to use Java expressions to define your policies. See Metadata Policy Expressions on page 168 for details about using Java expressions in your policy definitions.

These steps begin from the Cloudera Manager Admin Console home page.

1. Select Clusters > Cloudera Management Service.
2. Click the Configuration tab.
3. For choice of Filters, select Category > Policies. The configurable properties display:

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMS URL</td>
<td>tcp://localhost:61616</td>
<td>The URL of the JMS server. Notifications of changes to entities affected by policies you define are sent to this URL.</td>
</tr>
<tr>
<td>JMS User</td>
<td>admin</td>
<td>The JMS user to which notifications of changes to entities affected by policies are sent.</td>
</tr>
<tr>
<td>JMS Password</td>
<td>admin</td>
<td>The password of the JMS user to which notifications of changes to entities affected by policies are sent.</td>
</tr>
<tr>
<td>JMS Queue</td>
<td>Navigator</td>
<td>The JMS queue to which notifications of changes to entities affected by policies are sent.</td>
</tr>
<tr>
<td>Enable Expression Input</td>
<td>Disabled.</td>
<td>Click the box to enable if you want to use Java expressions to define policies. See Metadata Policy Expressions on page 168 for details.</td>
</tr>
</tbody>
</table>

4. Set the following properties for each role group
<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>When enabled, feature applies to the Navigator Metadata Server Default Group. If this configuration should apply to another role group (or groups), edit the value for the appropriate role group. See Modifying Configuration Properties Using Cloudera Manager.</td>
</tr>
</tbody>
</table>

5. Click **Save Changes**.
6. Restart the Navigator Metadata Server role instance.
Cloudera Navigator and the Cloud

Market-leading organizations today are deploying clusters to the cloud to increase efficiency and reduce costs. Using public cloud infrastructure lets companies create optimal solutions that combine both on-premises and cloud clusters in persistent or transient deployment model. With Cloudera Altus, transient clusters are provisioned quickly, expand and shrink in response to varying workloads, and can be terminated just as easily when no longer needed. See Cloudera Enterprise in the Cloud for an overview.

In addition to full-scale cluster deployments to the cloud, on-premises Cloudera clusters can leverage cloud resources, such as Amazon Simple Storage Service (S3). For example, an Amazon S3 storage bucket can be used as the source or target for BDR (backup and disaster recovery), enabling organizations to replicate HDFS files and Hive data to and from the S3 bucket. As another example, an S3 bucket is often used as a persistent data store, with data copied to HDFS on a transient cluster for interactive or iterative workloads. Other supported cloud-based functionality includes using Amazon Simple Queue Service (SQS) to support notification from changes to Amazon S3 bucket objects.

Cloudera Navigator can collect metadata from clusters running on Cloudera Altus and from objects stored on Amazon S3. That means that the entities resulting from Hive jobs, for example, running on clusters instantiated by Cloudera Altus users can be seen in lineage diagrams in a centralized on-premises Cloudera Navigator instance running on a persistent or long-running Cloudera Manager cluster.

**Hotel Cust Books Props**

hotel_cust_bookings_props

```
hdfs://ip-10-175-168-69.us-west-2.compute.internal:8020/user/hive/warehouse/hotel_altus.db/hotel_cust_books_props
```

**Note:** The Cloudera Navigator instance runs in an on-premises or persistent cluster.

This chapter provides the details for setting up Cloudera Navigator to extract from cloud-based resources, including Cloudera Altus clusters and Amazon S3 buckets. After configuring support, data stewards, data engineers, and others use the Cloudera Navigator console to explore metadata, relationships, and trace data lineage to its source as with any other type of entity.

**Using Cloudera Navigator with Altus Clusters**

Cloudera Navigator can extract metadata and lineage from Cloudera Altus clusters. That means that data engineers running jobs on transient clusters and processing jobs using Hive on Altus clusters can view metadata and lineage in...
Cloudera Navigator. Because Cloudera Navigator identifies cluster, cluster group, and other properties related to Altus deployed clusters, data engineers can use the lineage diagrams available in the Cloudera Navigator console to trace data back to its source, even when data processing spans different clusters.

Support for Cloudera Altus metadata and lineage extraction from Cloudera Navigator is not enabled by default. Configuration tasks must be completed in the Cloudera Altus console and in the Cloudera Manager Admin Console to enable this capability. Completing the configuration tasks requires your organization to have a Cloudera Altus account, and assume that you are successfully running jobs on clusters according to the processes detailed in the Cloudera Altus documentation.

**Important:** Altus exchanges metadata with Cloudera Navigator using an S3 bucket. Altus uses AWS IAM roles configured with policies to access the bucket; Navigator uses AWS Access Key Credentials to access the S3 bucket. Be sure that you can use access key credentials before you enable Navigator in your Altus environment.

### How it Works: Background to the Setup Tasks

Every cluster deployed using Cloudera Altus is deployed as a Cloudera Manager cluster, that is, it has its own Cloudera Manager Server. This Cloudera Manager Server instance is read-only, but an Altus user—for example, a data engineer developing a new Hive or MapReduce2 script—can use Cloudera Manager to view execution and other details. This Cloudera Manager Server also includes the Telemetry Publisher role instance (daemon) that publishes data from the transient cluster to other systems. The Telemetry Publisher stores metadata and lineage details from the running transient cluster to a cloud-based storage location (for example, an Amazon S3 bucket) specified in the Altus Environment used to instantiate the cluster.

It is the Telemetry Publisher role instance running in the Cloudera Manager Server of a Cloudera Altus cluster and the cloud-based storage mechanism that enables Cloudera Navigator to obtain metadata and lineage information from single-user transient clusters. Before the cluster shuts down, an internal process checks to ensure that all metadata and lineage from that transient cluster has been successfully published to the specified cloud-based storage resource.

Meanwhile, the on-premises Cloudera Navigator instance has been collecting the metadata and lineage information by reading from the same cloud-based storage location. Because cloud storage is a persistent store that runs independently and is not part of the transient cluster, it remains a viable source of data for Cloudera Navigator.

These system interactions are all but transparent to both Cloudera Altus users and Cloudera Navigator data stewards and other users. However, enabling the interaction involves several preliminary tasks across both Cloudera Altus and Cloudera Navigator. The specifics vary, depending on the cloud provider.

### Configuring Extraction for Altus Clusters on AWS

Follow the steps below to configure Cloudera Navigator to extract metadata and lineage from single-user transient clusters deployed to Amazon Web Services using Cloudera Altus. The Cloudera Navigator extraction process for clusters launched by Cloudera Altus works as follows:

- Any HDFS paths in a job, query, or data entity are extracted as proxy entities for the path, similar to how Hive entities are extracted. That means that HDFS is not bulk extracted from an Altus cluster.
- Hive Metastore (HMS) entities are also not bulk extracted. Cloudera Navigator extracts Hive entities used in queries that generate lineage, such as databases, tables, and so on.

### Requirements

Cloudera Navigator collects metadata and lineage entities from transient clusters deployed to AWS by Cloudera Altus users. The metadata and lineage data is not collected directly from the transient clusters but rather from an Amazon S3 bucket that serves as the storage mechanism for the Telemetry Publisher running in the cluster (see How it Works: Background to the Setup Tasks on page 120 for details).

Integration of Cloudera Navigator and Cloudera Altus clusters depends on:

- Identifying an Amazon S3 bucket for storing metadata
• Configuring access permissions to the S3 bucket from Cloudera Altus (IAM role with access policy) and Cloudera Navigator (AWS access key credentials). Transient clusters instantiated by Altus users must have read and write permissions to the Amazon S3 bucket used by Telemetry Publisher. The on-premises centralized Cloudera Navigator instance must have read permissions on the same Amazon S3 bucket.

- Altus user account (with cross-account privileges to AWS account). Privileges to launch EC2 clusters and use other AWS resources, including Amazon S3 buckets identified in the Altus environment (data input, data output, logs, and the S3 bucket for Telemetry Publisher).

- Read and write privileges to the Amazon S3 bucket configured in the Altus environment assigned to the Altus user.

- AWS access key ID and AWS secret key for the AWS account associated with the Amazon S3 bucket.

The steps below assume that you have:

• An Amazon Web Services account.

• A Cloudera Altus account.

• A Cloudera Altus user account that can run jobs on transient clusters deployed to AWS.

• An AWS IAM user account.

• An Amazon S3 bucket to use as the storage location for metadata and lineage.

• AWS Credentials for the AWS account hosting the S3 bucket.

• Access to the on-premises or persistent Cloudera Manager cluster running Cloudera Navigator. The Cloudera Manager user role of Full Administrator and the ability to log in to the Cloudera Manager Admin Console is required.

Obtaining AWS Access Key Credentials for the Amazon S3 Bucket

AWS Access Keys are available to be downloaded whenever you create an IAM user account through the AWS Management Console. If you are configuring an existing Amazon S3 bucket and you do not have the AWS Access Keys for it, you can generate new AWS Access Keys from the AWS account using either the AWS Management Console or the AWS CLI.

**Important**: The AWS account where the access keys are generated must have read and write access to the Amazon S3 bucket.

Generating new AWS access keys deactivates any previously issued credentials and makes the newly generated credentials Active for the AWS account. Keep that in mind if you obtain new AWS access keys to use for the Cloudera Navigator-Cloudera Altus integration.
Note: If you have the AWS access keys obtained when the account was created, do not regenerate a new set of AWS access keys unless you want to change the credentials.

- Log in to the AWS Management Console using the account associated with the Amazon S3 bucket.
- Navigate to the Security credentials section of the Users page in IAM for this account. For example:

  ![AWS Management Console](image)

  - Click the Create access key button to generate new AWS access keys. Extract the credentials (the Access Key Id and Secret Key) from the user interface or download the credentials.csv for later use.

Cloudera Altus Configuration

Cloudera Altus instantiates single-user transient clusters focused on data engineering workloads that use compute services such as Hive or MapReduce2. The typical deployment scenario involves running scripts that invoke the Cloudera Altus CLI to instantiate the cluster, in this case, using Amazon Web Services according to the details specified in the Altus environment. An Altus environment specifies all resources needed by the cluster, including the AWS account that will be used to instantiate the cluster. The Cloudera Altus user account is configured to provide cross-account access to the AWS account that has permissions to launch AWS Elastic Compute Cloud (EC2) instances and use other AWS resources, including Amazon S3 buckets.

Use the Environment Wizard to specify the Amazon S3 bucket that clusters will use to store metadata and lineage information for collection by Cloudera Navigator. Specifically, the Instance Profile Role page of the Configuration Wizard lets you enable integration with Cloudera Navigator and specify the Amazon S3 bucket that will hold collected metadata and lineage information.

On the Instance Profile Role page of the Configuration Wizard, complete the following steps:

- Click the Enable checkbox for Cloudera Navigator Integration.
- In the Cloudera Navigator S3 Data Bucket field, enter the path to the Amazon S3 bucket, including the final /, which identifies the target as an S3 bucket. For example:

  ```
  s3a://cluster-lab.example.com/cust-input/
  ```

To provide the correct access to the S3 bucket from Altus, you must also create the appropriate policy in the AWS Management Console and apply the policy to the Amazon S3 bucket. To provide the correct access to the S3 bucket from Navigator, follow the steps in Cloudera Navigator Configuration on page 123.

For more information about using Cloudera Altus, see the Cloudera Altus documentation.
Cloudera Navigator Configuration

The Cloudera Navigator runs in the context of Cloudera Manager Server. Its two role instances, the Navigator Audit Server and Navigator Metadata Server, run on the Cloudera Management Service. The Navigator Metadata Server role instance is the component that extracts metadata and lineage from the Amazon S3 bucket using the AWS Credentials configured for connectivity in the steps below:

- Follow the steps in Adding AWS Credentials and Configuring Connectivity on page 123 to add new or regenerated AWS access keys to the Cloudera Manager Server and then configure connectivity.
- Follow the steps in Configuring Connectivity for AWS Credentials on page 124 to configure connectivity for AWS access keys that are already available to be used for the Amazon S3 bucket but have not yet been configured for connectivity.

Important: Cloudera Navigator extracts metadata and lineage for clusters deployed using Altus from one Amazon S3 bucket only. In addition, for any given Amazon S3 bucket collecting metadata and lineage from Altus clusters, configure only one Cloudera Navigator instance to extract from that Amazon S3 bucket. Using multiple Cloudera Navigator instances to extract from the same Amazon S3 bucket is not supported and has unpredictable results.

Adding AWS Credentials and Configuring Connectivity

Cloudera Manager Required Role: Full Administrator

The AWS access keys must be added to the Cloudera Manager Server for use by Cloudera Navigator. These credentials must be from the AWS account hosting the Amazon S3 bucket that is configured in the Altus environment.

Note: The AWS account associated with these credentials must have cross-account access permissions from the Altus user account that will launch clusters on AWS and run jobs. These credentials must also have read and write permissions on the S3 bucket because the clusters launched must be able to write metadata and lineage information to the Amazon S3 bucket as jobs run.

1. Log in to the Cloudera Manager Admin Console.
2. Select Administration > External Accounts.
3. In the AWS Credentials tab, click Add Access Key Credentials.
   a. Enter a meaningful name for the AWS Credential, such as the type of jobs the associated clusters will run (for example, etl-processing). This name is for your own information and is not checked against any Cloudera Altus or AWS attributes.
   b. Enter the AWS Access Key ID and the AWS Secret Key.

4. Click Add to save the credentials. The S3Guard option page displays, reflecting the credential name (for example, Edit S3Guard: etl-processing). Disregard this option.
5. Click **Save**. The Connect to Amazon Web Services page displays, showing the options available for this specific AWS credential.

6. Click **Enable Metadata and Lineage Extraction from Cloudera Altus**. The Metadata and Lineage Extraction Configuration setting page displays a field for specifying the Amazon S3 bucket name.

7. Enter the name of the Amazon S3 bucket. For example:

8. Click **OK**. The AWS Credentials page re-displays, and the newly added AWS Access Key Credential is listed with any other AWS Credentials held by the Cloudera Manager Server.

9. Restart the Cloudera Management Service.

When the service restarts, the AWS access key will be used by Cloudera Navigator to authenticate to the AWS account and extract metadata and lineage stored on the specified S3 bucket.

**Configuring Connectivity for AWS Credentials**

If the AWS Credentials are available for the Amazon S3 bucket, you can configure them as follows:

1. Log in to the Cloudera Manager Admin Console.
2. Select **Administration > External Accounts**.
3. In the AWS Credentials tab, find the available AWS Access Key Credentials that provide access to the Amazon S3 bucket used to collect metadata and lineage from transient clusters.
4. Select Actions > Edit Connectivity. The Connect to Amazon Web Services page displays the three sections of possible configurations.

5. In the Cloudera Navigator section, click the Enable Metadata and Lineage Extraction from Cloudera Altus link. The Metadata and Lineage Extraction Configuration page displays.

6. Enter the name of the Amazon S3 bucket in the S3 Bucket Name field.

7. Click OK.

8. Restart the Cloudera Management Service.

This completes the setup process. After the restart, metadata and lineage for transient clusters deployed using Cloudera Altus should be available in the Cloudera Navigator console.

Note: See Troubleshooting to identify possible issues if metadata and lineage do not display in the Cloudera Navigator console after completing the configuration and restarting the system.

Technical metadata specific to clusters deployed using Altus include the following property names and types:

- Cluster (Source Type)
- Cluster-name (Cluster Group)
- Transient (Deployment Type)
- Cluster Template, Cluster Instance (Classname)

For example:

See Search Syntax and Properties on page 156 and Cloudera Navigator Business Metadata on page 60 for more information.

Using Cloudera Navigator with Amazon S3

Amazon Simple Storage Service (S3) is a storage solution offered by Amazon Web Services (AWS) that provides highly available storage in the cloud. Clusters deployed not only in the AWS cloud but also on-premises are using Amazon S3.
as persistent storage. Common use cases include BDR (backup and disaster recovery) and persistent storage for transient clusters deployed to the cloud, such as storage for ETL workload input and output.

As with data stored on HDFS and processed using compute engines like Hive and Impala, Cloudera Navigator can obtain metadata and lineage from Amazon S3 storage. There are some limitations and constraints as discussed below, and some setup is required to enable this capability (see Configuring Extraction for Amazon S3 on page 130).

Note: Cloudera Navigator does not audit Amazon S3 storage buckets. Only Cloudera Navigator metadata and lineage are supported.

This section provides conceptual information about Amazon S3 storage and shows you how to configure Cloudera Navigator to extract metadata and lineage from an Amazon S3 bucket.

Continue reading:

- Amazon S3 Storage Characteristics on page 126
- Cloudera Navigator and Amazon S3 on page 126
  - Extraction from Unnamed Directories on page 127
  - Object Lifecycle Rules Constraints on page 127
  - Amazon SQS and Amazon SNS Constraints on page 127
  - Object Storage Hierarchy on page 128
- Overview of Amazon S3 Extraction Processes on page 129
  - API Usage and Setting Limits on page 129

Amazon S3 Storage Characteristics

Amazon S3 is an object store rather than a file store or block store. It does not have the hierarchy found in typical filesystems. Amazon S3 uses the construct of a *bucket* as a container for *objects*. An object can be any kind of file—text file, image, photo, graphic, video, an ETL bundle to be ingested into a cluster, and so on.

Files can be added to Amazon S3 through the AWS Management Console, by using the AWS CLI, or by using scripts that invoke the CLI.

Amazon S3 storage is highly available because Amazon replicates data across multiple servers within its data centers and uses an *eventual consistency* model—not all accesses of an object on Amazon S3 may be reflected concurrently or instantaneously. However, eventually, all updates to data across servers are synchronized. The eventual consistency model can result in a short delay between the time objects are uploaded to Amazon S3 and the time their metadata is available in Cloudera Navigator. This is expected behavior and simply how eventual consistency works.

Note: The eventual consistency model of Amazon S3 can be augmented by using S3Guard, which leverages Amazon DynamoDB to provide support for transactions. See Configuring and Managing S3Guard in the Cloudera Administration guide for details.

For more information about Amazon S3, see Amazon S3 documentation.

Cloudera Navigator and Amazon S3

Cloudera Navigator collects metadata for Amazon S3 entities in much the same way as for HDFS entities, with some exceptions shown in the table below.

Note: In addition to metadata, Cloudera Navigator extracts lineage from Hive, Impala, and MapReduce (except for MapReduce Glob paths) on Amazon S3.

The following table lists some differences between object types and supported features offered by Amazon S3 and how those are supported by Cloudera Navigator:
### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Amazon S3</th>
<th>Cloudera Navigator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User-defined metadata</strong> consists of custom key-value pairs (in which each key is prefixed with <code>x-amz-meta-</code>) that can be used to describe objects on Amazon S3.</td>
<td>✔</td>
<td>☐</td>
</tr>
<tr>
<td><strong>System-defined metadata</strong> includes properties such as <code>Date</code>, <code>Content-Length</code>, <code>Last-Modified</code>. Some system-defined properties comprise the Technical Metadata for the object in Cloudera Navigator.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Tags for buckets and objects</td>
<td>✔</td>
<td>☐</td>
</tr>
<tr>
<td>Versioning is not supported. Cloudera Navigator extracts metadata and lineage from the latest version only.</td>
<td>✔</td>
<td>☐</td>
</tr>
<tr>
<td>Unnamed directories. See Extraction from Unnamed Directories on page 127 for details.</td>
<td>✔</td>
<td>☐</td>
</tr>
<tr>
<td><strong>Object lifecycle rules</strong>. See Object Lifecycle Rules Constraints on page 127 for more information.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Amazon Simple Queue Service</strong> (SQS). See Amazon SQS and Amazon SNS Constraints for usage limitations and requirements.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Amazon Simple Notification Service</strong> (SNS). See Amazon SQS and Amazon SNS Constraints for usage limitations and requirements.</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Hierarchy in object storage. See Object Storage Hierarchy on page 128 for more information and behavior.</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

### Refreshing AWS Credentials

After configuring Cloudera Navigator with a specific set of AWS Credentials for Amazon S3, future changes to the credentials, such as when credentials are rotated regularly, must be for the same AWS account (IAM user). If a new key is provided to Navigator, the key must belong to the same AWS account as the original key.

### Extraction from Unnamed Directories

Unnamed folders on Amazon S3 are not extracted by Navigator, but the content of the folders is extracted. For example, a top-level folder the top level folder in the bucket has no name (for example, `/bucket//folder/file`), it is extracted as `/bucket/folder/file`.

### Object Lifecycle Rules Constraints

Cloudera Navigator does not support lifecycle rules that remove objects from Amazon S3. For example, an object lifecycle rule that removes objects older than `n` days deletes the object from Amazon S3 but the event is not tracked by Cloudera Navigator. This limitation applies to removing objects only. Using lifecycle rules requires using bulk-only extraction. See Custom Configurations on page 133 for details about configuring the necessary AWS Policy and applying it to the Amazon S3 bucket for use by Cloudera Navigator.

### Amazon SQS and Amazon SNS Constraints

**Amazon Simple Queue Service** (SQS) is a distributed, highly scalable hosted queue for storing messages. **Amazon Simple Notification Service** (SNS) is publish-subscribe notification service that coordinates message delivery. Both services can be configured for use with Amazon S3 storage buckets. For example, Amazon S3 storage buckets can send notification messages to one or more queues or to email addresses whenever specified events occur, such as creating, renaming, updating, or deleting data on the Amazon S3 bucket.

During the default configuration process, Cloudera Navigator transparently sets up an Amazon SQS queue and configures Amazon S3 event notification for each bucket. The queue is used to hold event messages that are subsequently collected by the Cloudera Navigator S3 extractor process, for incremental extracts. Use the default configuration process only for Amazon S3 buckets that do not have existing queues or notifications configured.
For Amazon S3 buckets that are already configured for queues, use the custom configuration process—sometimes referred to as "Bring Your Own Queue" (BYOQ)—to manually configure queues for Cloudera Navigator. For Amazon S3 buckets that are already configured for notifications, use the BYOQ custom configuration in conjunction with Amazon SNS in a fan-out configuration. In a fan-out scenario, an Amazon SNS message is sent to a topic and then replicated and pushed to multiple Amazon SQS queues, HTTP endpoints, or email addresses. See Common Amazon SNS Scenarios for more information about fan-out configuration, and see Custom Configurations on page 133 for details about configuring Cloudera Navigator when the Amazon S3 bucket is already set up for either Amazon SQS or Amazon SNS.

Object Storage Hierarchy

Amazon S3 storage does not use a directory structure or other hierarchy as found in a traditional file system. Each object has an object key name that identifies the object by its S3 URI location—the path to the object. This path includes the object, prefix if any, and bucket name. Including the S3 protocol specifier, the pattern is as follows:

`s3://bucketname/prefix/objectkey`

There can be more than one prefix in an object key name. Prefixes are separated by the forward slash character (/).

Although Amazon S3 provides a folder metaphor for organizing objects in an S3 bucket, the folder does not provide actual containment or structure: it is the object key name and its S3Uri location that identifies the object.

Cloudera Navigator mimics file system behavior by mapping elements of the object key name to implicit folders. For example, for an Amazon S3 file with the object key name `2017/08_AUG/data-raw.csv`, Cloudera Navigator creates an entity with the path `2017/08_AUG/data-raw.csv` and also creates two directories: `2017` and `2017/08_AUG`.

Cloudera Navigator console Lineage tab for the file with object key `2017/08_AUG/data-raw.csv` shows it in the context of implicit folders:
Cloudera Navigator has some limitations specifically for deleted objects and implicit folders as follows:

- Cloudera Navigator does not mark an implicit folder as deleted even after all its child objects have been deleted.
- Cloudera Navigator does not mark as deleted any objects and folders deleted using Amazon S3 tools, such as the AWS CLI (`aws s3` commands) or the AWS Management Console.

**Note:** To filter out implicit folders from the S3 entities displayed, enter `implicit:false` in the Search field. Conversely, to find implicit entities enter `implicit:true` in the Search field.

For more details about the properties shown by Cloudera Navigator, see [S3 Properties](#) on page 161 in the Reference section of this guide.

Despite the differences between an object store and a hierarchical store, data engineers can work with Amazon S3 using the Cloudera Navigator in much the same way as for HDFS and other entities.

**Overview of Amazon S3 Extraction Processes**

By default, Cloudera Navigator uses combined bulk and incremental extraction processes. An initial bulk process extracts all metadata from an Amazon S3 bucket during the configuration process. Subsequent extracts are incremental. Changes are collected from an Amazon SQS queue created by Cloudera Navigator during the default configuration process.

Note that when Cloudera Navigator extraction encounters inconsistencies in AWS (for example, due to eventual consistency), it can delay Navigator extraction of metadata and lineage from Amazon S3. When Navigator detects an inconsistency, extraction may stop until the inconsistency is resolved in AWS. Navigator will retry at the next scheduled extraction.

This bulk-plus-incremental extraction combination provides the optimal performance for production systems and is also the most cost-effective in terms of Amazon API usage:

- For the bulk extract, Cloudera Navigator invokes the Amazon S3 API.
- For the incremental extract, Cloudera Navigator invokes the Amazon SQS API.

Amazon meters usage and charges differently for each of these APIs.

**API Usage and Setting Limits**

Amazon bills on a monthly basis and resets the billing cycle each month. To help manage the monthly cost of using these APIs, Cloudera Navigator provides a safety valve property that can be set to limit its use of the AWS APIs. If you decide to configure this property to set a limit on API usage, keep the following in mind:

- If the limit is set is reached in any given 30-day interval, Cloudera Navigator suspends extraction from the configured Amazon S3 buckets until the next 30-day interval begins.
- When the new 30-day interval begins, Cloudera Navigator extracts any data that was not extracted while extraction was suspended.

To set a limit on the AWS API usage:

- Use Cloudera Manager Admin Console to access the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties.
Set the value of `any_int` to your chosen limit.

```
nav.aws.api.limit=any_int
```

See [Setting Properties with Advanced Configuration Snippets](#) for details about using Cloudera Manager Admin Console for this task.

**Note:** Cloudera Navigator does not notify you if extraction is ever suspended due to the limit you have set in the safety valve. Cloudera recommends setting a billing alarm in the AWS Management Console to get notified by Amazon when your monthly use of the APIs exceeds the limit you have set in the safety valve.

## Configuring Extraction for Amazon S3

Depending on the specifics of the Amazon S3 bucket targeted for extraction by Cloudera Navigator, the configuration process follows one of two alternative paths:

- **Default configuration** — The default configuration is available for Amazon S3 buckets that have no existing Amazon SQS or Amazon SNS services configured. During configuration, Cloudera Navigator accesses the configured AWS account, performs an initial bulk extract from the Amazon S3 bucket, sets up Amazon SQS queues in each region with buckets, and sets up event notifications for each bucket for subsequent incremental extracts—all transparently to the Cloudera Manager administrator handling the configuration process.

- **Custom configuration** — Custom configuration is required for any Amazon S3 bucket that is currently using Amazon SQS (has queues set up for other applications, for example) or is setup for notifications using Amazon’s SNS. In these cases you must manually configure a new queue—`bring your own queue`—and in some cases, additionally configure Amazon SNS for `fanout`.

Continue reading:

- [AWS Credentials Requirements](#) on page 130
- [Default Configuration](#) on page 131
- [Custom Configurations](#) on page 133
  - Configuring Your Own Queues on page 133
    - Configure the Queue for Cloudera Navigator on page 133
    - Configure Event Notification for the Queues on page 134
    - Configuring Amazon SNS Fan-out on page 135
  - Defining and Attaching Policies on page 135
    - Event Notification Policy for Custom Queues on page 135
    - Extraction Policies for Custom Queues on page 135
    - Extraction Policies JSON Reference on page 136
  - Setting Properties with Advanced Configuration Snippets on page 137
- [Cloudera Navigator Extraction Behavior for Amazon S3](#) on page 137
- [Cloudera Navigator Properties for Amazon S3](#) on page 137

### AWS Credentials Requirements

Cloudera Manager can have multiple AWS credentials configured for various purposes at any given time. These are listed by name on the AWS Credentials page which is accessible from the Cloudera Manager Admin Console, under the Administration menu. However, there are specific constraints on AWS credentials for Cloudera Navigator as follows:

- Navigator supports a single key for authentication; only one AWS credential can be used for a given Navigator instance. Navigator can extract metadata from any number of S3 buckets, assuming the buckets can be accessed with the configured credential.
• An AWS credential configured for connectivity from one Cloudera Navigator instance cannot be used by another Cloudera Navigator instance. Configuring the same AWS credentials for use with different Cloudera Navigator instances can result in unpredictable behavior.

• Cloudera Navigator requires an AWS credential associated with an IAM user identity rather than an IAM role.

• Any changes to the AWS credentials (for example, if you rotate credentials on a regular basis) must be for the same AWS account (IAM user). Changing the AWS credentials to those of a different IAM user results in errors from the Amazon Simple Queue Service (used transparently by Cloudera Navigator). If a new key is provided to Cloudera Navigator, the key must belong to the same AWS account as the prior key.

• For the default configuration, the account for this AWS credential must have administrator privileges for:
  – Amazon S3
  – Amazon Simple Queue Service (SQS)

• For the custom configurations, the account needs privileges for Amazon S3, Amazon SQS, and for Amazon Simple Notification Service (SNS).

Default Configuration

The steps below assume that you have the required AWS credentials for the IAM user with the Amazon S3 bucket. Amazon Web Services (AWS) account (an IAM user account) and that you can use the AWS Management Console.

The AWS credentials for the IAM user are configured for Cloudera Navigator using the Cloudera Manager Admin Console during the configuration process below.

Important: If the Amazon S3 bucket is already configured for queuing or notification, do not follow the steps in this section. See Custom Configurations on page 133 instead.

Configuring Cloudera Navigator for Amazon S3

At the end of the configuration process detailed below, Cloudera Navigator authenticates to AWS using the credentials and performs an initial bulk extract of entities from the Amazon S3 bucket. It also sets up the necessary Amazon SQS queue (or queues, one for each region) to use for subsequent incremental extracts.

The steps below assume you have the required AWS credentials available.

1. Log in to the Cloudera Manager Admin Console.
2. Click Administration > AWS Credentials. The AWS Credentials page displays, listing any existing credentials that have been setup for the Cloudera Manager cluster.
3. Click the Add Access Key Credentials button. In the Add Access Key Credentials page:
   a. Enter a Name for the credentials. The name can contain alphanumeric characters and can include hyphens, underscores, and spaces but should be meaningful in the context of your production environment. Use the name of the Amazon S3 bucket or its functionality, for example, cust-data-raw or post-proc-results.
   b. Enter the AWS Access Key ID.
   c. Enter the AWS Secret Key.
4. Click *Add*. The *Edit S3Guard:aws-cred-name* page displays, giving you the option to enable S3Guard for the S3 bucket.
   - Click the Enable S3Guard box only if the AWS credential has privileges on Amazon DynamoDB and if the preliminary S3Guard configuration is complete. See *Cloudera Administration* for details about Configuring and Managing S3Guard.

5. Click *Save*.

   **Note:** Cloudera Manager stores the AWS credential securely in a non-world readable location. The access key ID and secret values are masked in the Cloudera Manager Admin Console, encrypted before being passed to other processes, and redacted in the logfiles.

The Connect to Amazon Web Services page displays the credential name and services available for its use:

6. Click the *Enable S3 Metadata Extraction* link in the Cloudera Navigator section of the page. A Confirm prompt displays, notifying you that Cloudera Navigator must be manually restarted after this change.
7. Click OK to enable the connection.
8. At the top of the Cloudera Manager Admin Console, click the Stale Configuration restart button when you are ready to restart Cloudera Navigator.

Metadata and lineage for Amazon S3 buckets will be available in the Cloudera Navigator console along with other sources, such as HDFS, Hive, and so on. It may take several minutes to complete the initial extraction depending on the number of objects stored on the Amazon S3 bucket.

Custom Configurations

Follow these steps for Amazon S3 buckets that are already configured with queues or event notifications. Custom configurations include configuring your own queue (BYOQ) and BYOQ with Fan-out, as detailed below.

Configuring Your Own Queues

Sometimes referred to as Bring Your Own Queue (BYOQ), configuring your own queue is required if the Amazon S3 bucket being targeted for extraction by Cloudera Navigator already has existing queues or is configured for notifications. The process involves stopping Cloudera Navigator and then using the AWS Management Console for the following tasks:

- Creating and configuring an Amazon Simple Queue Service (SQS) queue for Cloudera Navigator for each region in which the AWS (IAM user) account has Amazon S3 buckets.
- Configuring Amazon Simple Notification Service (SNS) on each bucket to send Create, Rename, Update, Delete (CRUD) events to the Cloudera Navigator queue.
- Configuring the bucket for Notification Fan-Out if needed to support existing notifications configured for other applications.
- Adding a Policy for the appropriate extraction process (Bulk + Incremental, Bulk Only) to the IAM user account.
- Adding the Policy for event notifications to the IAM user account.

**Important:** Always make sure any newly created Amazon S3 buckets are configured for event notifications before adding data so the queues are properly updated.

Configure the Queue for Cloudera Navigator

This manual configuration process requires stopping Cloudera Navigator. You must create a queue for each region that has S3 buckets.

1. Log in to Cloudera Manager Admin Console and stop Cloudera Navigator:
   - Select Clusters > Cloudera Management Service
   - Click the Instances tab.
   - Click the checkbox next to Navigator Audit Server and Navigator Metadata Server in the Role Type list to select these roles.
   - From the Actions for Selected (2) menu button, select Stop

2. Log in to the AWS Management Console with AWS account (IAM user) and open the Simple Queue Service setup page (select Services > Messaging > Simple Queue Service. Click Create New Queue or Get Started Now if region has no configured queues.)

3. For each region that has Amazon S3 buckets, create a queue as follows:
   a. Click the Create New Queue button. Enter a Queue Name, click the Standard Queue (not FIFO), and then click Configure Queue. Configure the queue using the following settings:

| Default Visibility Timeout | 10 minutes |
| Message Retention Period   | 14 days    |
| Delivery Delay             | 0 seconds  |
| Receive Message Wait Time  | 0 seconds  |
b. Select the queue you created, click the **Permissions** tab, click **Add a Permission**, and configure the following in the **Add a Permission to...** dialog box:

<table>
<thead>
<tr>
<th>Effect</th>
<th>Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal</td>
<td>Everybody</td>
</tr>
<tr>
<td>Actions</td>
<td>SendMessage</td>
</tr>
</tbody>
</table>

c. Click the **Add Conditions (optional)** link open the condition fields and enter the following values:

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>ArnLike</td>
</tr>
<tr>
<td>Key</td>
<td>aws:SourceArn</td>
</tr>
<tr>
<td>Value</td>
<td>arn:aws:s3::<em>:</em></td>
</tr>
</tbody>
</table>

d. Click **Add Condition** to save the settings.
e. Click **Add Permission** to save all settings for the queue.

![SQS Queue selected](image)

Repeat this process for each region that has Amazon S3 buckets.

**Configure Event Notification for the Queues**

After creating queues for all regions with Amazon S3 buckets, you must configure event notification for each Amazon S3 bucket. Assuming you are still logged into the AWS Management Console:

1. Navigate to the Amazon S3 bucket for the region (**Services > Storage > S3**).
2. Select the bucket.
3. Click the **Properties** tab.
4. Click the **Events** settings box.
5. Click **Add notification**.
6. Configure event notification for the bucket as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>nav-send-metadata-on-change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>• ObjectCreated(All)</td>
</tr>
<tr>
<td></td>
<td>• ObjectRemoved(All)</td>
</tr>
<tr>
<td>Send to</td>
<td>SQS Queue</td>
</tr>
<tr>
<td>SQS queue</td>
<td>Enter the name of your queue</td>
</tr>
</tbody>
</table>

**Important:** Cloudera Navigator extracts metadata from one queue only for each region.
Configuring Amazon SNS Fan-out

Configure SNS fanout if you have existing S3 event notification. For more information about SNS fanout, see Amazon documentation for Common SNS Scenarios.

1. Add the following to the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties. See Setting Properties with Advanced Configuration Snippets on page 137 for details about using Cloudera Manager Admin Console if necessary.

```
nav.s3.extractor.incremental.enable=true
nav.s3.extractor.incremental.auto_setup.enable=false
nav.s3.extractor.incremental.queues=queue_json
```

Specify the queue properties using the following JSON template (without any spaces). Escape commas (,) by preceding them with two backslashes (\), as shown in the template:

```
[{"region":"us-west-1","queueUrl":"https://sqs.aws_region.amazonaws.com/account_num/queue_name"},{queue_2},...,{queue_n}]
```

2. Restart Cloudera Navigator.

Defining and Attaching Policies

Event Notification Policy for Custom Queues

To enable event notification for a custom queue, create the following policy by copying the policy text and pasting it in the policy editor, and then attaching it to the Cloudera Navigator user in AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1481678612000",
      "Effect": "Allow",
      "Action": [
        "sqs:DeleteMessage",
        "sqs:DeleteMessageBatch",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Stmt1481678744000",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Extraction Policies for Custom Queues

Custom configurations require a valid extraction policy be defined and attached to the AWS user account associated with the Amazon S3 bucket. The policy is a JSON document that specifies the type of extraction. As mentioned in Overview of Amazon S3 Extraction Processes on page 129, the two types of extraction are as follows:
• Bulk + Incremental—This is the recommended approach for both cost and performance reasons and is used by the Default Configuration process automatically.
• Bulk Only—This approach is recommended for proof-of-concept deployments. It is required for the BYOQ with Fan-out configuration. In addition to applying the policy as detailed below, this approach also requires setting the nav.s3.extractor.incremental.enable property to false. See Setting Properties with Advanced Configuration Snippets on page 137 and the Cloudera Navigator Properties for Amazon S3 on page 137 for details.

To configure the policy:
• Log in to the AWS Management Console using the IAM user account associated with the target Amazon S3 bucket.
• Copy the appropriate JSON text from the table below Extraction Policies JSON Reference on page 136 and paste into the AWS Management Console policy editor for the Navigator user account on (the IAM user) through the AWS Management Console.

Extraction Policies JSON Reference

<table>
<thead>
<tr>
<th>Bulk + Incremental (Recommended)</th>
<th>Bulk Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial bulk process extracts all metadata.</td>
<td></td>
</tr>
<tr>
<td>Subsequent incremental process extracts changes only (CRUD).</td>
<td></td>
</tr>
<tr>
<td>Cannot be used with Amazon S3 buckets that use event notification.</td>
<td></td>
</tr>
<tr>
<td>Must be used for Amazon S3 buckets configured for event notifications.</td>
<td></td>
</tr>
</tbody>
</table>

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1481678612000",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "Stmt1481678744000",
            "Effect": "Allow",
            "Resource": ["arn:aws:s3:::*"]
        }
    ]
}
```
### Setting Properties with Advanced Configuration Snippets

Certain features require additional settings or changes to the Cloudera Navigator configuration. For example, configuring BYOQ queues to use bulk-only extraction requires not only creating and attaching the extraction policy but also adding the following snippet to the Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties setting:

```property=nav.s3.extractor.incremental.enable=false```

To change property values by adding an advanced configuration snippet:

1. Log in to the Cloudera Manager Admin Console.
2. Select Clusters > Cloudera Management Service.
3. Click Configuration.
4. Click Navigator Metadata Server under the Scope filter, and click Advanced under the Category filter.
5. Enter Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties in the Search field to find the property.
6. Enter the property and its setting as a key-value pair, for example:

```
property=your_setting
```

in:

1. Click Save Changes.
2. Restart the Navigator Metadata Server instance.

### Cloudera Navigator Extraction Behavior for Amazon S3

Objects from S3 buckets appear as you would expect directories and files to appear in Navigator. However, there are some behaviors that are specific to S3 source types:

- **Unnamed directories**
  
  It is possible to place files in unnamed directory in an S3 bucket, such as `s3://mybucket//myfile`. Navigator does not extract files inside unnamed directories.

- **Deleted implicit directories**

  When adding files to an S3 bucket, S3 may create implicit directories for the file if the directories specified in the file path do not already exist. When a file is deleted and its implicit directories are also removed on S3, Navigator will show the file as deleted but will not delete the implicit directories. You can filter these directories from the Navigator search results by setting `implicit:false` in the search query.

- **Inconsistency delays**

  Inconsistencies that occur in AWS can delay Navigator extraction of metadata and lineage from Amazon S3. When Cloudera Navigator detects an inconsistency, extraction may stop until the inconsistency is resolved in AWS. Cloudera Navigator will retry at the next scheduled extraction.

### Cloudera Navigator Properties for Amazon S3

The table below lists the Navigator Metadata Server properties (cloudera-navigator.properties) that control extraction and other features related to Amazon S3. These properties can be set using the Cloudera Manager Admin Console to set properties in the advanced configuration settings.

Changing any of the values in the table requires a restart of Cloudera Navigator.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nav.aws.api.limit</td>
<td>Default is 5,000,000. Maximum number of Amazon Web Services (AWS) API calls that Cloudera Navigator can make per month.</td>
</tr>
<tr>
<td>nav.sqs.max_receive_count</td>
<td>Default is 10. Number of retries for inconsistent SQS messages (inconsistent due to eventual consistency).</td>
</tr>
<tr>
<td>nav.s3.extractor.enable</td>
<td>Default is true when an AWS credential has been configured to extract metadata from Amazon S3.</td>
</tr>
<tr>
<td>nav.s3.extractor.incremental.auto_setup.enable</td>
<td>Default is true. Enables Cloudera Navigator to set up Amazon SQS queues to receive notifications from Amazon S3 events. Set to false to disable the automatic setup and custom configure your own queue (BYOQ with Fan-out).</td>
</tr>
<tr>
<td>nav.s3.extractor.incremental.batch_size</td>
<td>Default is 1000. Number of messages held in memory during the extraction process.</td>
</tr>
<tr>
<td>nav.s3.extractor.incremental.enable</td>
<td>Default is true. Enables incremental extraction. Setting to false disables incremental extraction and effectively enables bulk-only extraction.</td>
</tr>
<tr>
<td>nav.s3.extractor.incremental.event.overwrite</td>
<td>Default is false. Prevents any existing event notifications from being overwritten by Cloudera Navigator auto-generated queues created during default configuration process. <strong>Important:</strong> Do not set to true unless you fully understand the impact of overwriting event notifications. Setting to true may overwrite critical existing business logic.</td>
</tr>
<tr>
<td>nav.s3.extractor.incremental.queues</td>
<td>No default queue. Used by the custom configuration only. Specify a list of queues for the custom configuration using the JSON template. The list of queues should include the existing queues already in use and the newly configured queue that Cloudera Navigator will use for incremental extracts.</td>
</tr>
<tr>
<td>nav.s3.extractor.max_threads</td>
<td>Default is 3. The number of extractors (worker processes) to run in parallel.</td>
</tr>
<tr>
<td>nav.s3.home_region</td>
<td>Default is us-west-1. AWS region closest to the cluster and the Cloudera Navigator instance. Select the same AWS region (or the nearest one geographically) to minimize latency for API requests.</td>
</tr>
<tr>
<td>nav.s3.implicit.batch_size</td>
<td>Default is 1000. Number of Solr documents held in memory when updating the state of implicit directories.</td>
</tr>
</tbody>
</table>
Cloudera Navigator APIs

Cloudera Navigator exposes REST APIs on the host running the Navigator Metadata Server role instance. In-house, third-party, and other developers can use the APIs to provide functionality not currently available through the Cloudera Navigator console or to customize behavior.

The APIs are used by the Cloudera Navigator console at runtime as users interact with the system. The Cloudera Navigator console has a debug mode that captures API calls and responses to a file that can then be downloaded and analyzed, not only for development projects but also for troubleshooting. Several examples of direct use of the APIs are included in this section.

Navigator APIs Overview

Documentation and a brief tutorial for the Navigator APIs are available on the same node of the cluster that runs the Navigator Metadata Server role. These are also accessible from the Cloudera Navigator console. Example pathnames for direct access (outside the Cloudera Navigator console) are shown in the table.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>APIs</td>
<td><a href="http://fqdn-n.example.com:port/api/vn/operation">http://fqdn-n.example.com:port/api/vn/operation</a></td>
</tr>
<tr>
<td>API Documentation</td>
<td><a href="http://fqdn-n.example.com:port/api-console/index.html">http://fqdn-n.example.com:port/api-console/index.html</a></td>
</tr>
<tr>
<td>API Usage Tutorial</td>
<td><a href="http://fqdn-n.example.com:port/api-console/tutorial.html">http://fqdn-n.example.com:port/api-console/tutorial.html</a></td>
</tr>
</tbody>
</table>

Operations on the API are invoked using the following general pattern:

http://fqdn-n.example.com:port/api/vn/operation

The $n$ in $vn$ for the APIs represents the version number, for example, v11 for the Cloudera Navigator version 2.11.x. The API version number is located at the bottom of the Cloudera Navigator API documentation page.

The API uses HTTP Basic Authentication and accepts the same users and credentials that have access to the Cloudera Navigator console.

The resources listed in the table are aimed at technical and general audiences for Cloudera Navigator Data Management. The GitHub repository is aimed at developers.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>GitHub cloudera/navigator-sdk</td>
<td>Cloudera Navigator SDK is a client library that provides functionality to help users extract metadata from Navigator and to enrich the metadata in Navigator with custom metadata models, entities, and relationships.</td>
</tr>
<tr>
<td>Cloudera Community Data Management forum</td>
<td>Cloudera Community &gt; Data Management &gt; Data Discovery, Optimization forum for Cloudera Navigator users and developers.</td>
</tr>
<tr>
<td>Cloudera Engineering Blog</td>
<td>In-depth technical content provided by Cloudera engineers about components and specific subject areas.</td>
</tr>
</tbody>
</table>

Accessing API Documentation

The API documentation is available from the Cloudera Navigator console from a menu selection that navigates to the same URL listed in the table above.

To access the API documentation and tutorial:
Cloudera Navigator APIs

1. Click Help.
2. Select **API Documentation**. The interactive API documentation page displays in a new window.
3. Click the Tutorial link near the top of the page to view the Cloudera Navigator API Usage Tutorial to learn about the APIs.

Locating the Version Information for the Navigator API

1. Click Help.
2. Select **API Documentation** to display the API documentation.
3. Scroll to the bottom of the page. The version number is the last item on this page:

   ```
   [ BASE_URL: http://node-5.example.com:7187/api/api-docs, API VERSION: v10 ]
   ```

The API is structured into resource categories. Click a category to display the resource endpoints.

Mapping API Versions to Product Versions

The following table identifies the compatibility between API versions and Cloudera Manager and Cloudera Navigator product versions.

<table>
<thead>
<tr>
<th>Cloudera Manager</th>
<th>Cloudera Navigator</th>
<th>Navigator API</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>6.2</td>
<td>v14</td>
</tr>
<tr>
<td>6.0 – 6.1</td>
<td>6.0 – 6.1</td>
<td>v13</td>
</tr>
<tr>
<td>5.14 – 5.16 and later</td>
<td>2.13 – 2.15 and later</td>
<td>v13</td>
</tr>
<tr>
<td>5.13</td>
<td>2.12</td>
<td>v12</td>
</tr>
<tr>
<td>5.12</td>
<td>2.11</td>
<td>v11</td>
</tr>
<tr>
<td>5.10 – 5.11</td>
<td>2.9 – 2.10</td>
<td>v10</td>
</tr>
<tr>
<td>5.7 – 5.9</td>
<td>2.6 – 2.8</td>
<td>v9</td>
</tr>
<tr>
<td>5.6</td>
<td>2.5</td>
<td>v8</td>
</tr>
</tbody>
</table>

Using Debug Mode

Cloudera Navigator console debug mode captures API responses and requests during interaction with the server. Use debug mode to facilitate development efforts or when asked by Cloudera Support to troubleshoot issues.

**Tip:** Exploring debug files can be a good way to learn about the APIs.

The general process for obtaining debug files to send to Cloudera Support is as follows:

1. Navigate to the Cloudera Navigator console menu item or page for which you want to obtain debug information.
2. Enable debug mode.
3. Reload the page and perform the specific action. For example, if you need to send a debug file to Cloudera Support for an error message that displays when you click on an entity in one of the charts, perform that action to raise the error message.
4. Download the debug file or files. Each time the counter changes, the content of the debug file content changes, so you should download each time the counter updates.
5. Disable debug mode.

To follow these steps you must be logged in to the Cloudera Navigator console.

Enable Debug Mode

The Enable Debug Mode menu selection is effectively a toggle. In other words, when you Enable Debug Mode, the menu selection changes to Disable Debug Mode. To enable debug mode:
1. Click the user_name from the menu to open the drop-down menu.
2. Select Enable Debug Mode. The Cloudera Navigator console displays a notification message in the bottom right of the page:

   ![Debug mode enabled. Captured 0 calls. Disable Download debug file](image)

   Notice the links to Disable and Download debug file, which you can use at any time to do either. Do not disable debug mode until you have downloaded the debug file you need.
3. Reload the browser page.

   The counter $n$ displays the number of API calls captured in the debug file for the current session interaction. Here is an example from a downloaded debug file showing one of the responses after reloading the page:

   ```
   {
   "type": "GET",
   "url": "/api/v10/dashboard/clusters",
   "status": 200,
   "responseText": "{"\n   "clusterInfos": [{"\n   "clusterId": "Cluster 1",
   "clusterDisplayText": "Cluster 1\n   }],
   "pages": "https://fqdn-1.example.com:7187/dashboard.html",
   "timestamp": "2017-06-15T09:00:32Z"
   }
   },
   ```

**Download Debug File or Files**

As you perform actions with the Cloudera Navigator console, the counter refreshes and keeps track of current calls only (stateless nature of REST). In other words, download the debug file for any given action or selection that you want to examine.

**To download the debug file:**

- Click the Download debug file link in the debug-enabled notification message.
- Save the file to your local workstation.

Debug files use a naming convention that includes the prefix "api-data" followed by the name of the host and the UTC timestamp of the download time and the JSON file extension. The pattern is as follows:

   api-data-fqdn-yyyymm-ddThh-mm-ss.json

   For example:

   api-data-fqdn-2.example.com-2017-06-15T09-00-32.json

**Disable Debug Mode**

When you are finished capturing and downloading debug files, you can disable debug mode.

- Click the Disable debug mode link in the notification message box.

   The message box is dismissed and debug mode is disabled.

   Or, use the Cloudera Navigator console menu:

   - Select user_name > Disable Debug Mode.

**Set Debug Logging Levels**

The Cloudera Navigator Debug Mode allows you to configure the logging levels for individual methods in the application code. For example, to increase the logging detail for API calls, you would set the logging level for the org.apache.cxf.interceptor class to "DEBUG" level. If you are collecting debugging information for a specific issue, Cloudera support will provide the class name.

To set the logging level for a Cloudera Navigator application class:
1. **Log in to the Cloudera Navigator console.**
2. Add `/debug` to the Navigator URL:

   http://navigator-host:7187/debug

   The debugging console appears.

3. **Click Configure Logging.**
4. In the **Logger** drop-down menu, select a Navigator class, such as `org.apache.cxf.interceptor` for API calls.
5. **Set the logging level for the class.**
   
   For example, for the API call logging, select **DEBUG**.
6. **Click Submit.**

   When changed in Debug Mode, logging levels will return to their default values after restarting the Navigator Metadata Server. To permanently change the logging levels, use Cloudera Manager to add an entry in the Navigator Metadata Server Logging Advanced Configuration Snippet. Create the entry as follows:

   ```
   log4j.logger.<classname>=<level>
   ```

   For example, to set the API logging level to "DEBUG", include the following string in the Advanced Configuration Snippet:

   ```
   log4j.logger.org.apache.cxf.interceptor=DEBUG
   ```

   See **Modifying Configuration Properties Using Cloudera Manager.**

---

### Applying Metadata to HDFS and Hive Entities using the API

Using the Navigator API and JSON formatted metadata definition files, entities can be assigned properties in bulk, prior to extraction.

### Applying HDFS and Hive Metadata

The Navigator APIs can be used modify metadata of HDFS or Hive entities, such as databases, tables, and operations, before or after entity extraction. There are three methods to apply or update entity metadata:

- Pre-register metadata for an asset that isn’t yet in Navigator. (POST /entities)
- Apply new or update metadata for a single entity. (PUT /entities/{id})
- Apply new or update metadata for a set of entities. (PUT /entities/bulk)

The Navigator SDK includes examples of pre-registering entities. For example, see this example of creating a Hive operation, which will allow you to see lineage for pre-registered entities.

### Retrieving Existing Metadata for Entities: GET /entities

When you call an API to update or add metadata to existing Navigator entities, the call replaces the metadata of a given type with the metadata provided in the API call. Therefore when you update an entity, you must supply the existing metadata as well as the new metadata in the call payload.

Typically, you would call the GET /entities API to retrieve the existing metadata for the entities you want to update. The GET call returns a JSON object that includes all the metadata for the entities you request. You can then strip the technical metadata from the JSON, augment the remaining metadata with the values you want to update, then use the JSON as the payload for the PUT or POST call.

The GET /entities API allows you to retrieve entity metadata using an entity identifier or by using a search query. The search query uses the same syntax and field names as the full query text in the Navigator console Search tab. There are many examples of useful GET /entity calls in **GET Existing Metadata Examples** on page 147.
Pre-registering Navigator Entities: POST /entities

Navigator provides an API to create new entities without a metadata extraction process. Use this API to insert entities in Navigator from sources that do not have an extractor plugin or when you want to store metadata during ingest or other processes that occur before extraction would run. The API generates the appropriate internal identifier for the entity. If you call the API before the metadata for an entity is extracted, the user-defined metadata is stored with the following entity properties:

- Identity
- Source ID
- Metadata fields (name, description, tags, properties)
- Fields relevant to the identifier

Other fields (attributes) for the entity, such as Type, are not present when the entity is generated and are filled in later by an automated metadata extraction process.

If the entity already exists in Navigator, the POST /entities call updates the existing entity with the provided metadata.

Use the following cURL syntax to call the POST /entities API:

```
POST curl http://fqdn-n.example.com:port/api/APIversion/entities/ \
-u username:password \
-X POST \
-H "Content-Type: application/json" \
-d '{properties}'
```

where properties are:

- **sourceId** (required) — The identifier value from an existing source entity. See the GET /entities example to find the existing sources.
- **parentPath** — The path of the parent entity, defined as:
  - HDFS file or directory — `fileSystemPath` of the parent directory. (Do not provide this field if the entity affected is the root directory.) The parentPath for `/user/admin/input_dir` is `/user/admin`.
  - If you add metadata to a directory, the metadata does not propagate to any files or folders in that directory.
  - Hive database — If you are updating database metadata, do not specify this field.
  - Hive table or view — The name of database containing the table or view. The parentPath for a table in the default database is default.
  - Hive column — `database name/table name/view name`. The parentPath for a column in the `sample_07` table is `default/sample_07`.
- **originalName** (required) — The name as defined by the source system.
  - HDFS file or directory — Name of file or directory (ROOT if the entity is the root directory). The originalName for `/user/admin/input_dir` is `input_dir`.
  - Hive database, table, view, or column — The name of the database, table, view, or column.
    - Example for default database: `default`
    - Example for `sample_07` table: `sample_07`
- Metadata fields (name, description, tags, user-defined properties, managed properties) that describe the final entity, including existing metadata.

All existing naming rules apply, and if any value is invalid, the entire request is denied. The call adds the entity to Navigator with the provided metadata and generates the entity identity:

- **identity** — The ID assigned to an entity by Navigator. This value is generated by Navigator based on the originalName, parentPath, and sourceId.
Cloudera Navigator APIs

Updating Metadata for a Single Entity: PUT /entities/{id}

You can use the PUT /entity/{id} API to update the metadata for a single entity.

User-defined metadata provided through the API overwrites existing metadata. In addition, null values for some metadata overwrites existing metadata. For example, passing empty or no name and description fields with an empty array for tags and empty property dictionary with the API call removes the existing metadata. If you omit the tags or properties fields, the existing tags or properties values remain unchanged. If you want to add a tag to a list of existing tags, you must include the existing tags in your update.

Use the following cURL syntax to make a PUT /entities call:

```bash
PUT curl http://fqdn-n.example.com:port/api/APIversion
/entities/identity \  
-u username:password \  
-X PUT \  
-H "Content-Type: application/json" \  
-d '{properties}'
```

where identity is an entity ID and properties are:

- name — The name for the entity. This "name" is used in Navigator and is distinct from the "originalName" that Navigator extracted from the source. If there is already a name applied, you must supply the existing name to prevent the call from overwriting the name with a null value.
- description — The description for the entity. If you are not updating the description, you must supply the existing description to avoid overwriting a description with a null value.
- tags — Tag metadata. If you provide any tags, you must also supply existing tags to avoid removing existing tags.
- properties — User-defined properties. The format is {key: value}. Again, if you are adding a user-defined property, you must also supply the existing user-defined properties associated with this entity to avoid overwriting them.
- customProperties — Managed properties. The format is {namespace: {key: value}}. If a property is assigned a value that does not conform to type constraints, the call returns an error. If you are associating a managed property with an entity, you must also supply the existing managed properties associated with this entity to avoid overwriting them.

If any value is invalid, the entity is not updated.

Updating Metadata for Entities in Bulk: PUT /entities/bulk

Use the PUT /entities/bulk/ API to update metadata for many entities in the same call. This API is faster than the single PUT API because it uses a single HTTP request to apply the metadata rather than an HTTP request for each entity.

Like the single PUT API, the call must supply the existing Navigator metadata for each entity being updated or the call will overwrite the existing metadata with null values. Typically, you would call the GET /entities API to retrieve the existing metadata for the entities you want to update. The GET call returns a JSON object that includes all the metadata for the entities you request. You can then strip the technical metadata from the JSON, augment the remaining metadata with the values you want to update, then use the JSON as the payload for the PUT /entities/bulk call. See GET Existing Metadata Examples on page 147. Note that the bulk update API is different from the single PUT call: the PUT call uses the long ID of an existing entity while the bulk update PUT uses a combination of source ID, original name, and parent path to identify the entity to update.

```bash
PUT curl http://fqdn-n.example.com:port/api/APIversion/entities/bulk?allOrNone=boolean  
-u username:password \  
-X PUT \  
-H "Content-Type: application/json" \  
-d '{properties}'
```

where the parameter is:

- allOrNone — True indicates that the call applies metadata updates only if all items in the payload can be successfully applied. If false, any items in the payload that can be applied, will be applied. Errors appear in the log to indicate which items were not updated. (Default: False)
where properties are:

- **sourceId** (required) — The identifier value from an existing source entity. See the GET /entities example to find the existing sources.
- **parentPath** — The path of the parent entity, defined as:
  - HDFS file or directory — fileSystemPath of the parent directory. (Do not provide this field if the entity affected is the root directory.) The parentPath for /user/admin/input_dir is /user/admin.
    If you add metadata to a directory, the metadata does not propagate to any files or folders in that directory.
  - Hive database — If you are updating database metadata, do not specify this field.
  - Hive table or view — The name of database containing the table or view. The parentPath for a table in the default database is default.
  - Hive column — database name/table name/view name. The parentPath for a column in the sample_07 table is default/sample_07.
- **originalName** (required) — The name as defined by the source system.
  - HDFS file or directory — Name of file or directory (ROOT if the entity is the root directory). The originalName for /user/admin/input_dir is input_dir.
  - Hive database, table, view, or column — The name of the database, table, view, or column.
    - Example for default database: default
    - Example for sample_07 table: sample_07
- Metadata fields (name, description, tags, user-defined properties, managed properties) that describe the final entity, including existing metadata.

### API Usage Examples

This section contains some examples, which include the URL that points to the Navigator Metadata Server host and port:

```
http://fqdn-n.example.com:port/api/APIversion/entities/
```

where *fqdn-n.example.com* is the host running the Navigator Metadata Server role instance listening for HTTP connections at the specified *port* number (7187 is the default port number). *APIversion* is the running version of the API as indicated in the footer of the API documentation (available from the Help menu in the Navigator console) or by calling `http://fqdn-n.example.com:port/api/version`.

To create an authorization token to use in subsequent calls:

This example makes a dummy call that saves an authentication token to the current location in a file named NavCookie. You can use the token in later calls to avoid having to specify the *username* and *password*.

```
curl https://node1.example.com:7187/api/v14/interactive/entities?limit=1&offset=0 -c NavCookie -u username:password -X GET
```
Note: These cURL examples use an authorization token and ASCII encoding for punctuation and spaces in the URLs. The encoding is necessary for some of the more complex queries; simple queries can be formatted without the ASCII codes. The characters replaced with codes are:

<table>
<thead>
<tr>
<th>Character</th>
<th>ASCII Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space</td>
<td>%20</td>
</tr>
<tr>
<td>Colon (:)</td>
<td>%3A</td>
</tr>
<tr>
<td>Double quotation mark (&quot;)</td>
<td>%22</td>
</tr>
<tr>
<td>Plus (+)</td>
<td>%2B</td>
</tr>
</tbody>
</table>

HDFS PUT Custom Metadata Example for /user/admin/input_dir Directory

```
curl http://node1.example.com:7187/api/v13/entities/e461de8de38511a3ac6740dd7d51b8d0 \
-u username:password \
-X PUT \
-H "Content-Type: application/json" \
-d '{"name":"my_name", "description":"My description", "tags":["tag1","tag2"], "properties":{"property1":"value1","property2":"value2"}}'
```

HDFS POST Custom Metadata Example for /user/admin/input_dir Directory

```
curl http://node1.example.com:7187/api/v13/entities/ \
-u username:password \
-X POST \
-H "Content-Type: application/json" \
-d '{"sourceId":"a09b0233cc58ff7d601ea68673a20c6", "parentPath":"/user/admin", "originalName":"input_dir", "name":"my_name", "description":"My description", "tags":["tag1","tag2"], "properties":{"property1":"value1","property2":"value2"}}'
```

Hive POST Custom Metadata Example for total_emp Column

```
curl http://node1.example.com:7187/api/v13/entities/ \
-u username:password \
-X POST \
-H "Content-Type: application/json" \
-d '{"sourceId":"4fbdadc6899638782fc8cb626176dc7b", "parentPath":"default/sample_07", "originalName":"total_emp", "name":"my_name", "description":"My description", "tags":["tag1","tag2"], "properties":{"property1":"value1","property2":"value2"}}'
```

HDFS PUT Managed Properties Example

This example adds a property and a tag to the entity identified as "14", which happens to be the Hive emailPreferences column in the customers sample table. The Approved property is a Boolean to indicate whether or not the metadata for this column was reviewed and approved. The ToBeReviewed tag marks the column temporarily so a data steward can easily find this column for review:

```
curl http://node1.example.com:7187/api/v13/entities/14 \
-u username:password \
-X PUT \
```

cloudera navigator data management
The server responds:

```json
{
  "originalName": "email_preferences",
  "originalDescription": null,
  "sourceId": "7",
  "firstClassParentId": "13",
  "parentPath": "/default/customers",
  "deleteTime": null,
  "extractorRunId": "7##1",
  "customProperties": {
    "Operations": {
      "Approved": true
    }
  },
  "name": null,
  "description": null,
  "tags": [ "ToBeReviewed" ],
  "properties": {
    "__cloudera_internal__hueLink": "https://node1.example.com:8889/hue/metastore/table/default/customers"
  },
  "technicalProperties": null,
  "dataType": "struct<email_format:string,frequency:string,categories:struct<promos:boolean,surveys:boolean>>",
  "type": "FIELD",
  "sourceType": "HIVE",
  "userEntity": false,
  "metaClassName": "hv_column",
  "deleted": false,
  "packageName": "nav",
  "identity": "14",
  "internalType": "hv_column"
}
```

GET Existing Metadata Examples

This section shows some examples of useful GET /entity calls:

To retrieve a specific entity:

Use the entity identifier that shows in the URL in the Navigator console. This example gets the metadata for the entity with identifier 21302.

```bash
curl https://node1.example.com:7187/api/v14/entities/21302 
-X GET -b NavCookie
```

To retrieve entities that describe the sources Navigator extracts data from:

```bash
curl https://node1.example.com:7187/api/v14/entities/?query=type%3ASOURCE 
- b NavCookie -X GET
```

To use the source in a query, find its identity: In the output, find the name of the source, then collect the identity for that entity. In this example, the HIVE-1 source has the identity "6".

```json
{
  "originalName": "HIVE-1",
  "originalDescription": null,
  "sourceId": null,
  "firstClassParentId": null,
  "parentPath": null,
  "deleteTime": null,
```
To retrieve all entities from a single source:

Run the previous call to determine the identity of the source, then use that value as the sourceId in the query. This example uses sourceId of 6.

```
curl https://node1.example.com:7187/api/v14/entities/?query=sourceId%3A6 \
  -b NavCookie -X GET
```

To retrieve all entities marked with a specific tag:

Use quotes around the tag name. This example retrieves metadata for entities tagged with "sensitive".

```
curl https://node1.example.com:7187/api/v14/entities/?query=tags%3A%22sensitive%22 \
  -b NavCookie -X GET
```

To retrieve all entities from a single source and marked with a tag:

This example includes a plus sign (+) before each of the query components to ensure they are treated as an AND relation. Note that this is a case where the query returns the correct results only with the ASCII codes.

```
curl https://node1.example.com:7187/api/v14/entities/?query=%2btags%3A%22sensitive%22%2bsourceId%3A6 \
  -b cookie -X GET
```

To search for pre-registered entities:

This example shows how to get metadata for pre-registered entities, which do not include an internal type:

```
curl http://node1.example.com:7187/api/v13/entities/?query=-internalType:* \
  -b cookie -X GET
```

To retrieve managed property definitions:

The /model API allows you to retrieve and to create managed properties. This example shows retrieving all defined managed properties:

```
curl http://node1.example.com:7187/api/v13/models/properties \
  -b cookie -X GET
```
This example shows retrieving a map of entity types and the managed properties that can be associated with them:

```
curl http://node1.example.com:7187/api/v13/models/properties/mappings
  -b cookie -X GET
```

Using the Cloudera Navigator SDK for Metadata Management

To help application developers work with metadata using the Cloudera Navigator APIs, Cloudera provides the Cloudera Navigator SDK. Cloudera Navigator SDK is a client library that provides functionality for extracting and enriching metadata with custom models, entities, and relationships. See GitHub cloudera/navigator-sdk for details.

Using the Purge APIs for Metadata Maintenance Tasks

**Required Role:** Cloudera Navigator Full Administrator

The volume of metadata maintained by Navigator Metadata Server can grow quickly and reduce the efficiency of the Solr instance that processes the index and supports the search capability. For faster search and cleaner lineage tracing, use the purge feature to routinely delete stale metadata from the system.

Purging stale metadata is also recommended prior to upgrading an existing Cloudera Navigator instance. See Purging the Navigator Metadata Server of Deleted and Stale Metadata on page 112 for details.

**Note:** The Cloudera Navigator console includes a configurable scheduling feature for Purge operations. Use the Cloudera Navigator console to purge deleted managed properties. See Deleting, Restoring, and Purging Managed Properties on page 65 and Defining Managed Properties on page 62.

See also What Metadata is Purged? on page 72

Purging Stale Entity Metadata

You can delete obsolete metadata using the purge method. Purge is a long-running task that requires exclusive access to the Solr instance and does not allow any concurrent activities, including extraction. When a purge job runs, any running Navigator tasks—extractions, policy application, or other background tasks—are stopped so that the purge can run immediately. When the purge task completes, the tasks that were stopped are restarted from the beginning. The interruption for the purge task may delay collecting new audits and metadata but does not affect what content is collected.

**Required Role:** Metadata Administrator (or Full Administrator)

To purge metadata, do the following:

1. Invoke the maintenance/purge endpoint with the POST method with a user with Full Administrator role:

   ```
   http://fqdn-n.example.com:port/api/APIversion/maintenance/purge?parameters
   ```

   where `fqdn-n.example.com` is the host running the Navigator Metadata Server role instance listening for HTTP connections at the specified `port` number (7187 is the default port number). `APIversion` is the running version of the API as indicated in the footer of the API documentation (available from the Help menu in the Navigator console) or by calling `http://fqdn-n.example.com:port/api/version`.

   **Table 3: Purge Parameters**

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>delete timed</td>
<td>After an HDFS entity is deleted, the amount of time that elapses before the</td>
</tr>
<tr>
<td></td>
<td>threshold</td>
<td>entity can be purged.</td>
</tr>
<tr>
<td></td>
<td>minutes</td>
<td>Default: 86400 minutes (60 days).</td>
</tr>
<tr>
<td>Metadata</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|          | runtimeCapMinutes | Amount of time allowed for the HDFS purge process to run. When specified time is reached, the state is saved and the purge process stops. Run purge again to remove any remaining items held in state.  
**Default:** 720 minutes (12 hours). Set to 0 to effectively disable purge for HDFS files and directories (none will be purged).  
**Default:** 720 minutes (12 hours). |
| Operations from all services | deleteSelectOperations | Set to true to enable purge for Hive and Impala SELECT queries, and to enable YARN, Sqoop, and Pig operations older than the staleQueryThresholdDays value to be purged.  
**Default:** false  
By default, does not purge Hive and Impala SELECT queries, nor are YARN, Sqoop, and Pig operations purged. |
|                      | staleQueryThresholdDays | Number of days at which operations will be identified as stale, effectively marking them 'ready for purge.' They will be purged automatically within hours of the value being reached.  
**Default:** 60 days. To disable marking entities as stale for the foreseeable future, set the value to very large number, such as 36500. |

For example, the following cURL call purges the metadata of all deleted HDFS entities (elapsed minutes value set to 0):

```
curl -X POST -u admin:admin "http://node1.example.com:7187/api/v14/maintenance/purge?deleteTimeThresholdMinutes=0"
```

Purge tasks do not start until all currently running extraction tasks finish.

2. When all tasks have completed, click **Continue** to return to the Cloudera Navigator console.

### Retrieving Purge Status

**Required Role:** Metadata Administrator (or Full Administrator)

To view the status of the purge process, invoke the `maintenance/running` endpoint with the `GET` method:

```
http://fqdn-n.example.com:port/api/APIversion/maintenance/running
```

For example:

```
curl -X GET -u admin:admin "http://node1.example.com:7187/api/v13/maintenance/running"
```

A result would look similar to:

```
[{
"id" : 5,
"type" : "PURGE",
"startTime" : "2016-03-10T23:17:41.884Z",
"endTime" : "1970-01-01T00:00:00.000Z",
"status" : "IN_PROGRESS",
"message" : "Purged 2661984 out of 4864714 directories. Averaging 1709 directories per minute.",
"username" : "admin",
"stage" : "HDFS_DIRECTORIES",
}
]```
Retrieving Purge History

Required Role: Metadata Administrator (or Full Administrator)

To view the purge history, invoke the `maintenance/history` endpoint with the GET method with parameters from the following table:

```
http://fqdn-n.example.com:port/api/APIversion/maintenance/history?parameters
```

where `fqdn-n.example.com` is the host running the Navigator Metadata Server role instance listening for HTTP connections at the specified `port` number (7187 is the default port number). `APIversion` is the running version of the API as indicated in the footer of the API documentation (available from the Help menu in the Navigator console) or by calling `http://fqdn-n.example.com:port/api/version`.

**Table 4: History Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offset</td>
<td>First purge history entry to retrieve. Default: 0.</td>
</tr>
<tr>
<td>limit</td>
<td>Number of history entries to retrieve from the offset. Default: 100.</td>
</tr>
</tbody>
</table>

For example:

```
curl -X GET -u admin:admin "http://node1.example.com:7187/api/v13/maintenance/history?offset=0&limit=100"
```

A result would look similar to:

```json
[
  {
    "id": 1,
    "type": "PURGE",
    "startTime": "2016-03-09T18:57:43.196Z",
    "endTime": "2016-03-09T18:58:33.337Z",
    "status": "SUCCESS",
    "username": "admin",
    "stagePercent": 0
  },
  {
    "id": 2,
    "type": "PURGE",
    "startTime": "2016-03-09T19:47:39.401Z",
    "endTime": "2016-03-09T19:47:40.841Z",
    "status": "SUCCESS",
    "username": "admin",
    "stagePercent": 0
  },
  {
    "id": 3,
    "type": "PURGE",
    "startTime": "2016-03-10T01:27:39.632Z",
    "endTime": "2016-03-10T01:27:46.809Z",
    "status": "SUCCESS",
    "username": "admin",
    "stagePercent": 0
  }
]
```
Stopping a Purge Operation

To stop a purge operation that is running too long and blocking user access to Navigator, restart the Navigator Metadata Server. To complete the operation, rerun the purge command at a later time.
This section provides the following reference information:

- Lineage Diagram Icons on page 153
- Search Syntax and Properties on page 156
- Service Audit Events on page 162
- Service Metadata Entity Types on page 167
- User Roles and Privileges Reference on page 176

## Lineage Diagram Icons

### Entity Types and Icons Reference

In lineage diagrams, entity types are represented by icons that vary depending upon the source system. The table below lists source system and shows the icons that can display in lineage diagrams.

Lineage diagrams are limited to 400 entities. After 400 entities, Cloudera Navigator lineage diagrams use the hidden icon to provide an entry point for exploring additional entities.

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Cluster group icon]</td>
<td>Cluster group</td>
</tr>
<tr>
<td>![Cluster instance icon]</td>
<td>Cluster instance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HDFS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![File icon]</td>
<td>File</td>
</tr>
<tr>
<td>![Directory icon]</td>
<td>Directory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hive and Impala</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Hive and Impala icon]</td>
<td>Hive entities include tables that result from Impala queries and Sqoop jobs.</td>
</tr>
<tr>
<td>![Table icon]</td>
<td>Table</td>
</tr>
<tr>
<td>![Field icon]</td>
<td>Field</td>
</tr>
<tr>
<td>![Operation icon]</td>
<td>Operation, sub-operation, execution</td>
</tr>
<tr>
<td>![Impala operation icon]</td>
<td>Impala operation, sub-operation, execution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MapReduce and YARN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![MapReduce operation icon]</td>
<td>MapReduce operation and operation execution</td>
</tr>
<tr>
<td>![YARN operation icon]</td>
<td>YARN operation and operation execution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oozie</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Oozie icon]</td>
<td></td>
</tr>
</tbody>
</table>
### Operation, operation execution

<table>
<thead>
<tr>
<th>Pig</th>
<th>Operation, execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td></td>
</tr>
<tr>
<td>Pig field</td>
<td></td>
</tr>
<tr>
<td>Pig operation, operation execution</td>
<td></td>
</tr>
</tbody>
</table>

### Spark

Spark lineage is rendered only for data that is read/written or processed using the Dataframe and SparkSQL APIs. Lineage is not available for data that is read/written or processed using Spark RDD APIs.

<table>
<thead>
<tr>
<th>Spark</th>
<th>Operation, operation execution. (Spark RDDs and aggregation operations are not included in the diagrams.)</th>
</tr>
</thead>
</table>

### Sqoop

<table>
<thead>
<tr>
<th>Sqoop</th>
<th>Operation, sub-operation, execution</th>
</tr>
</thead>
</table>

### S3

<table>
<thead>
<tr>
<th>S3</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File</td>
</tr>
<tr>
<td></td>
<td>S3 Bucket</td>
</tr>
</tbody>
</table>

### Other Icons and Visual Elements in Lineage Diagrams

- **Hidden** entities. Used in lineage diagrams containing more than 400 entities. Click this icon to display the hidden entity details. See [Exploring Hidden Entities in a Lineage Diagram](#) for more information.

- **Placeholder** for an entity that has not yet been extracted. This icon is replaced by the correct entity icon after Cloudera Navigator extracts and links the entity. Hive entities deleted from the system before extraction completes also use this icon, in which case, the icon remains in the lineage diagram.

- **Plus** icon. Click this icon in a lineage diagram to see more information about the entity.

See [Metadata Extraction and Indexing](#) for more information on the extraction process, including length of time to extract newly created entities.

### Types of Relations Shown in Lineage Diagrams

Lineage diagrams render relationships between entities using different line styles and colors. Arrows indicate data flow direction. Cloudera Navigator supports the following types of relations:
<table>
<thead>
<tr>
<th>Relation Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data flow</td>
<td>A relation between data and a processing activity, such as between a file and a MapReduce job or vice versa. Sometimes you may see a data flow relation without data assets. If that happens, it may be because they've been deleted. Turn on <strong>Deleted Entities</strong> in the lineage view to see the original data assets.</td>
</tr>
<tr>
<td>Parent-child</td>
<td>A parent-child relation. For example, the relation between a directory (parent) and a file (child).</td>
</tr>
<tr>
<td>Logical-physical</td>
<td>The relation between a logical entity and its physical entity. For example, between a Hive query and a MapReduce job.</td>
</tr>
<tr>
<td>Instance of</td>
<td>The relation between an operation execution and its operation. <strong>Instance of</strong> relations are not rendered in lineage diagrams.</td>
</tr>
<tr>
<td>Control flow</td>
<td>A relation in which a source entity controls the data flow of the target entity. For example, the relation between the columns of an <strong>insert</strong> clause and the <strong>where</strong> clause of a Hive query.</td>
</tr>
</tbody>
</table>

Lineage diagrams contain the line types shown in the table:

- A solid line depicts a **data flow** relationship, indicating that the columns appear (possibly transformed) in the output (when line has directional arrow) and logical-physical (when line does not have an arrow). For example, a solid line appears between the columns used in a **select** clause.
  - If you don't see the data assets involved, it may be because they've been deleted. Turn on **Deleted Entities** in the lineage view to see the original data assets.

- A dashed line depicts a **control flow** relationship, indicating that the columns determine which rows flow to the output. For example, a dashed line appears between the columns used in an **insert** or **select** clause and the **where** clause of a Hive query. Control flow lines are hidden by default. See **Filtering Lineage Diagrams** on page 43.

- A blue line depicts a link within the lineage diagram that has been selected.

- A green line depicts a summary link that contains operations. When clicked, the green line turns blue denoting it has been selected, and the nested operations display in a selected link summary.

**Selected Link Summary**

**Data Flow Summary**

```
Operations:
|   | INSERT OVERWRITE TABLE sample_09
|   | SELECT sample_07.co...

sample_09
```

Cloudera Navigator Reference
Search Syntax and Properties

Cloudera Navigator search uses an embedded Solr engine that follows the syntax specified for the LuceneQParserPlugin.

Search Syntax

Search strings are constructed by specifying a default property value and one of the four types of key-value pairs as follows:

- **Technical metadata key-value pairs** - `key : value`
  - `key` is one of the properties listed in Searchable Properties Reference on page 157.
  - `value` is a single value or range of values specified as `[value1 TO value2]`. In a value, * is a wildcard. In property values, you must escape special characters :, -, /, and * with the backslash character (\), or enclose the property value in quotes.

  Technical metadata key-value pairs are read-only and cannot be modified.

- **Hive extended attribute key-value pairs** - `tp_key : value`
  - `key` is an extended attribute set on a Hive entity. The syntax of the attribute is specific to Hive.
  - `value` is a single value supported by the entity type.

  Hive extended attribute key-value pairs are read-only and cannot be modified.

- **Managed properties (key-value pairs)** - `namespace .key : value`
  - `namespace` is the namespace containing the property. See Defining Managed Properties on page 62.
  - `key` is the name of a managed property.
  - `value` is a single value, a range of values specified as `[value1 TO value2]`, or a set of values separated by spaces. In a value, * is a wildcard. In property values, you must escape special characters :, -, /, and * with the backslash character (\), or enclose the property value in quotes.

  Only the values of managed properties can be modified.

- **User-defined properties (key-value pairs)** - `up_key : value`
  - `key` is a user-defined property.
  - `value` is a single value or range of values specified as `[value1 TO value2]`. In a value, * is a wildcard. In property values, you must escape special characters :, -, /, and * with the backslash character (\), or enclose the property value in quotes.

  User-defined properties key-value pairs can be modified.

- **S3 key-value pairs** - `tp_key : value`
  - `key` is the name of user-defined metadata.
  - `value` is a single value.
  - Only file metadata is extracted; bucket and folder metadata is not extracted.

Constructing Compound Search Strings

To construct compound search strings, you can join multiple property-value pairs using the Lucene Query Parser Boolean operators:

- `+`, `-`
- `OR`, `AND`, `NOT`

Both syntax types use ( ) to group multiple clauses into a single field and to form sub-queries.

When you filter Search results in the Cloudera Navigator console, the constructed search strings use the +, - syntax.
## Example Search Strings

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Search String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities in the path /user/hive that have not been deleted</td>
<td><code>+(&quot;/user/hive&quot;) +(-deleted:true)</code></td>
</tr>
<tr>
<td>Descriptions that start with the string &quot;Banking&quot;</td>
<td><code>description:Banking*</code></td>
</tr>
<tr>
<td>Entities of type MapReduce or entities of type Hive</td>
<td><code>sourceType:mapreduce sourceType:hive OR sourceType:mapreduce OR sourceType:hive</code></td>
</tr>
<tr>
<td>Entities of type HDFS with size equal to or greater than 1024 MiB or entities of type Impala</td>
<td><code>(+sourceType:hdfs +size:[1073741824 TO *]) sourceType:impala</code></td>
</tr>
<tr>
<td>Directories owned by hdfs in the path</td>
<td><code>/user/hdfs/input +owner:hdfs +type:directory +fileSystemPath:&quot;/user/hdfs/input&quot;</code> or <code>owner:hdfs AND type:directory AND fileSystemPath:&quot;/user/hdfs/input&quot;</code></td>
</tr>
<tr>
<td>Job started between 20:00 to 21:00 UTC</td>
<td><code>started:[2013-10-21T20:00:00.000Z TO 2013-10-21T21:00:00.000Z]</code></td>
</tr>
<tr>
<td>Technical key-value. In Hive, specify table properties like this:</td>
<td><code>tp_key1:value1</code></td>
</tr>
<tr>
<td>ALTER TABLE table_name SET TBLPROPERTIES ('key1'='value1');</td>
<td></td>
</tr>
<tr>
<td>Managed key-value with multivalued property</td>
<td><code>MailAnnotation.emailTo=&quot;dana@example.com&quot;</code></td>
</tr>
<tr>
<td></td>
<td><code>MailAnnotation.emailTo=&quot;lee@example.com&quot;</code></td>
</tr>
<tr>
<td>User-defined property value</td>
<td><code>project-customer1-up_project:customer1</code></td>
</tr>
</tbody>
</table>

### Note:
When viewing MapReduce jobs in the Cloudera Manager Activities page, the string that appears in a job Name column equates to the originalName property. To specify a MapReduce job name in a Navigator search, use the string (sourceType:mapreduce) and (originalName: *jobName*), where *jobName* is the value in the job Name column.

## Searchable Properties Reference

The following sections describe the categories (types) of properties that can be searched.

### Default Properties

The following properties can be searched by specifying a property value: `type`, `fileSystemPath`, `inputs`, `jobId`, `mapper`, `mimeType`, `name`, `originalName`, `outputs`, `owner`, `principal`, `reducer`, and `tags`.

### Common Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>text</td>
<td>Description of the entity.</td>
</tr>
<tr>
<td>group</td>
<td>caseInsensitiveText</td>
<td>The group to which the owner of the entity belongs.</td>
</tr>
<tr>
<td>name</td>
<td>ngramedText</td>
<td>The overridden name of the entity. If the name has not been overridden, this value is empty. Names cannot contain spaces.</td>
</tr>
<tr>
<td>operationType</td>
<td>ngramedText</td>
<td>The type of an operation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pig - SCRIPT</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>originalName</td>
<td>ngramedText</td>
<td>Entity name at extraction time.</td>
</tr>
<tr>
<td>originalDescription</td>
<td>text</td>
<td>Entity description at extraction.</td>
</tr>
<tr>
<td>owner</td>
<td>caseInsensitiveText</td>
<td>Entity owner.</td>
</tr>
<tr>
<td>principal</td>
<td>caseInsensitiveText</td>
<td>For entities with type OPERATION_EXECUTION, the initiator of the entity.</td>
</tr>
<tr>
<td>properties</td>
<td>string</td>
<td>Set of key-value pairs that describe the entity.</td>
</tr>
<tr>
<td>tags</td>
<td>ngramedText</td>
<td>Set of tags that describe the entity.</td>
</tr>
<tr>
<td>type</td>
<td>tokenizedCaseInsensitiveText</td>
<td>Entity type. Source type of entity determines set of types available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• hdfs - DIRECTORY, FILE, DATASET, FIELD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• hive - DATABASE, TABLE, FIELD, OPERATION, OPERATION_EXECUTION, SUB_OPERATION, PARTITION, VIEW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• impala - OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mapreduce - OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• oozie - OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• pig - OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• spark - OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sqoop - OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• yarn - OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
<tr>
<td>userEntity</td>
<td>Boolean</td>
<td>Indicates whether an entity was added using the Cloudera Navigator SDK.</td>
</tr>
<tr>
<td>Query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>queryText</td>
<td>string</td>
<td>The text of a Hive, Impala, or Sqoop query.</td>
</tr>
<tr>
<td>Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>clusterName</td>
<td>string</td>
<td>The name of the cluster in which the source is managed.</td>
</tr>
<tr>
<td>sourceId</td>
<td>string</td>
<td>The ID of the source type.</td>
</tr>
<tr>
<td>sourceType</td>
<td>caseInsensitiveText</td>
<td>The source type of the entity: hdfs, hive, impala, mapreduce, oozie,pig, spark, sqoop, or yarn.</td>
</tr>
<tr>
<td>sourceUrl</td>
<td>string</td>
<td>The URL of web application for a resource.</td>
</tr>
</tbody>
</table>

### Timestamps

Fields vary by source type:
- hdfs - created, lastAccessed, lastModified
- hive - created, lastModified
- impala, mapreduce, pig, spark, sqoop,

<table>
<thead>
<tr>
<th>date</th>
<th>Timestamps in the Solr Date Format. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• lastAccessed: [* TO NOW]</td>
</tr>
<tr>
<td></td>
<td>• created: [1976-03-06T23:59:59.999Z TO *]</td>
</tr>
<tr>
<td></td>
<td>• started: [1995-12-31T23:59:59.999Z TO 2007-03-06T00:00:00Z]</td>
</tr>
<tr>
<td></td>
<td>• ended: [NOW-1YEAR/DAY TO NOW/DAY+1DAY]</td>
</tr>
<tr>
<td></td>
<td>• created: [1976-03-06T23:59:59.999Z TO 1976-03-06T23:59:59.999Z+1YEAR]</td>
</tr>
</tbody>
</table>
### Entity Types

<table>
<thead>
<tr>
<th>Source</th>
<th>Entity Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdfs</td>
<td>DIRECTORY, FILE, DATASET, FIELD</td>
</tr>
<tr>
<td>hive</td>
<td>DATABASE, TABLE, FIELD, OPERATION, OPERATION_EXECUTION, SUB_OPERATION,</td>
</tr>
<tr>
<td></td>
<td>_PARTITION, RESOURCE, VIEW</td>
</tr>
<tr>
<td>impala</td>
<td>OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
<tr>
<td>mapreduce</td>
<td>OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td>oozie</td>
<td>OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td>pig</td>
<td>OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td>spark</td>
<td>OPERATION, OPERATION_EXECUTION</td>
</tr>
<tr>
<td>sqoop</td>
<td>OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
<tr>
<td>yarn</td>
<td>OPERATION, OPERATION_EXECUTION, SUB_OPERATION</td>
</tr>
</tbody>
</table>

### HDFS Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blockSize</td>
<td>long</td>
<td>The block size of an HDFS file.</td>
</tr>
<tr>
<td>deleted</td>
<td>Boolean</td>
<td>Indicates whether the entity has been moved to the Trash folder.</td>
</tr>
<tr>
<td>deleteTime</td>
<td>date</td>
<td>The time the entity was moved to the Trash folder.</td>
</tr>
<tr>
<td>fileSystemPath</td>
<td>path</td>
<td>The path to the entity.</td>
</tr>
<tr>
<td>mimeType</td>
<td>ngramedText</td>
<td>The MIME type of an HDFS file.</td>
</tr>
<tr>
<td>parentPath</td>
<td>string</td>
<td>The path to the parent entity of a child entity. For example: <code>parent path:/default/sample_07 for the table sample_07 from the Hive database default. </code></td>
</tr>
<tr>
<td>permissions</td>
<td>string</td>
<td>The UNIX access permissions of the entity.</td>
</tr>
<tr>
<td>replication</td>
<td>int</td>
<td>The number of copies of HDFS file blocks.</td>
</tr>
<tr>
<td>size</td>
<td>long</td>
<td>The exact size of the entity in bytes or a range of sizes. Range examples: <code>size:[1000 TO *],size: [* TO 2000], and size: [* TO *] to find all fields with a size value. </code></td>
</tr>
</tbody>
</table>

### Hive Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dataType</td>
<td>ngramedText</td>
<td>The type of data stored in a field (column).</td>
</tr>
<tr>
<td>fieldIndex</td>
<td>int</td>
<td>The ordinal value of the column, where indexing starts with zero.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>compressed</td>
<td>Boolean</td>
<td>Indicates whether a table is compressed.</td>
</tr>
<tr>
<td>serDeLibName</td>
<td>string</td>
<td>The name of the library containing the SerDe class.</td>
</tr>
<tr>
<td>serDeName</td>
<td>string</td>
<td>The fully qualified name of the SerDe class.</td>
</tr>
</tbody>
</table>

**Partition**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>partitionColNames</td>
<td>string</td>
<td>The table columns that define the partition.</td>
</tr>
<tr>
<td>partitionColValues</td>
<td>string</td>
<td>The table column values that define the partition.</td>
</tr>
<tr>
<td>technical_properties</td>
<td>string</td>
<td>Hive extended attributes.</td>
</tr>
<tr>
<td>clusteredByColNames</td>
<td>string</td>
<td>The column names that identify how table content is divided into buckets.</td>
</tr>
<tr>
<td>sortByColNames</td>
<td>string</td>
<td>The column names that identify how table content is sorted within a bucket.</td>
</tr>
</tbody>
</table>

**MapReduce and YARN Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inputRecursive</td>
<td>Boolean</td>
<td>Indicates whether files are searched recursively under the input directories, or only files directly under the input directories are considered.</td>
</tr>
<tr>
<td>jobId</td>
<td>ngramedText</td>
<td>The ID of the job. For a job spawned by Oozie, the workflow ID.</td>
</tr>
<tr>
<td>mapper</td>
<td>string</td>
<td>The fully qualified name of the mapper class.</td>
</tr>
<tr>
<td>outputKey</td>
<td>string</td>
<td>The fully qualified name of the class of the output key.</td>
</tr>
<tr>
<td>outputValue</td>
<td>string</td>
<td>The fully qualified name of the class of the output value.</td>
</tr>
<tr>
<td>reducer</td>
<td>string</td>
<td>The fully qualified name of the reducer class.</td>
</tr>
</tbody>
</table>

**Operation Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>inputFormat</td>
<td>string</td>
<td>The fully qualified name of the class of the input format.</td>
</tr>
<tr>
<td>outputFormat</td>
<td>string</td>
<td>The fully qualified name of the class of the output format.</td>
</tr>
<tr>
<td>Operation Execution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>inputs</td>
<td>string</td>
<td>The name of the entity input to an operation execution. For entities of resource type mapreduce, yarn, and spark, it is usually a directory. For entities of resource type hive, it is usually a table.</td>
</tr>
<tr>
<td>outputs</td>
<td>string</td>
<td>The name of the entity output from an operation execution. For entities of resource type mapreduce, yarn, and spark, it is usually a directory. For entities of resource type hive, it is usually a table.</td>
</tr>
<tr>
<td>engineType</td>
<td>string</td>
<td>The type of the engine used for an operation: MR or Spark.</td>
</tr>
</tbody>
</table>
### Oozie Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>string</td>
<td>The status of the Oozie workflow: RUNNING, SUCCEEDED, or FAILED.</td>
</tr>
</tbody>
</table>

### Pig Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scriptId</td>
<td>string</td>
<td>The ID of the Pig script.</td>
</tr>
</tbody>
</table>

### S3 Properties

**Object Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>region</td>
<td>string</td>
<td>The geographic region in which the bucket is stored</td>
</tr>
<tr>
<td>bucketName</td>
<td>string</td>
<td>The name of the bucket in which the object is stored</td>
</tr>
<tr>
<td>fileSystemPath</td>
<td>path</td>
<td>The key of the S3 object.</td>
</tr>
<tr>
<td>size</td>
<td>long</td>
<td>Object size in bytes.</td>
</tr>
<tr>
<td>lastModified</td>
<td>date</td>
<td>Object creation date or the last modified date, whichever is the latest.</td>
</tr>
<tr>
<td>etag</td>
<td>string</td>
<td>A hash of the object. The ETag reflects changes only to the contents of an object, not its metadata. The ETag may or may not be an MD5 digest of the object data.</td>
</tr>
<tr>
<td>storageClass</td>
<td>string</td>
<td>Storage class used for storing the object.</td>
</tr>
<tr>
<td>owner</td>
<td>string</td>
<td>Owner of the object.</td>
</tr>
<tr>
<td>sequencer</td>
<td>string</td>
<td>Latest S3 event notification sequencer. Used to order events.</td>
</tr>
<tr>
<td>parentPath</td>
<td>string</td>
<td>Parent of the S3 object.</td>
</tr>
<tr>
<td>technicalProperties</td>
<td>key-value pairs</td>
<td>User-defined properties for each S3 object.</td>
</tr>
</tbody>
</table>

**Bucket Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>region</td>
<td>string</td>
<td>Region for the bucket.</td>
</tr>
<tr>
<td>created</td>
<td>date</td>
<td>Date the bucket was created.</td>
</tr>
<tr>
<td>owner</td>
<td>string</td>
<td>Owner of the bucket.</td>
</tr>
</tbody>
</table>

### Sqoop Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbURL</td>
<td>string</td>
<td>The URL of the database from or to which the data was imported or exported.</td>
</tr>
<tr>
<td>dbTable</td>
<td>string</td>
<td>The table from or to which the data was imported or exported.</td>
</tr>
<tr>
<td>dbUser</td>
<td>string</td>
<td>The database user.</td>
</tr>
<tr>
<td>dbWhere</td>
<td>string</td>
<td>A where clause that identifies which rows were imported.</td>
</tr>
</tbody>
</table>
Service Audit Events

Service audit events are the events generated by a given service running on the cluster. Users with the appropriate permissions (Auditing Viewer, Full Administrator) can view audit events in the Cloudera Navigator console or by using the APIs. Audit events can include the fields listed in the tables below.

The Cloudera Navigator console Audits includes events collected by Cloudera Manager: service lifecycle events (activate, create, delete, deploy, download, install, start, stop, update, upgrade, and so on) and user security-related events (add and delete user, login failed and succeeded). See Lifecycle and Security Auditing for more details on Cloudera Manager audit events.

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Field in API</th>
<th>Field in Streaming</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Info</td>
<td>additional_info</td>
<td>additionalInfo</td>
<td>JSON text that contains more details about an operation performed in Metadata Server.</td>
</tr>
<tr>
<td>Allowed</td>
<td>allowed</td>
<td>allowed</td>
<td>Indicates whether the request to perform an operation failed or succeeded. A failure occurs if the user is not authorized to perform the action.</td>
</tr>
<tr>
<td>Collection Name</td>
<td>collection_name</td>
<td>collectionName</td>
<td>The name of the affected Solr collection.</td>
</tr>
<tr>
<td>Database Name</td>
<td>database_name</td>
<td>db databaseName</td>
<td>For Sentry, Hive, and Impala, the name of the database on which the operation was performed.</td>
</tr>
<tr>
<td>Delegation Token ID</td>
<td>delegation_token_id</td>
<td>delegationTokenId</td>
<td>Delegation token identifier generated by HDFS NameNode that is then used by clients when submitting a job to JobTracker.</td>
</tr>
<tr>
<td>Destination</td>
<td>dest</td>
<td>dst</td>
<td>Path of the final location of an HDFS file in a rename or move operation.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>entity_id</td>
<td>entityId</td>
<td>Identifier of a Navigator Metadata Server entity. The ID can be retrieved using the Navigator Metadata Server API.</td>
</tr>
<tr>
<td>Event Time</td>
<td>timestamp</td>
<td>time</td>
<td>Date and time an action was performed. The Navigator Audit Server stores the timestamp in the timezone of the Navigator Audit Server. The Cloudera Navigator console displays the timestamp converted to the local timezone. Exported audit events contain the stored timestamp.</td>
</tr>
<tr>
<td>Family</td>
<td>family</td>
<td>family</td>
<td>HBase column family.</td>
</tr>
<tr>
<td>Impersonator</td>
<td>impersonator</td>
<td>impersonator</td>
<td>Name of user (service) that invokes an action on behalf of another user (service). Impersonator field always displays values when Sentry is not used with the cluster. For clusters that use Sentry, the Impersonator field displays values for all services other than Hive.</td>
</tr>
<tr>
<td>IP Address</td>
<td>ipAddress</td>
<td>ip</td>
<td>The IP address of the host where an action occurred.</td>
</tr>
<tr>
<td>Object Type</td>
<td>object_type</td>
<td>objType</td>
<td>For Sentry, Hive, and Impala, the type of the object (TABLE, VIEW, DATABASE) on which operation was performed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbColumnExpression</td>
<td>string</td>
<td>An expression that identifies which columns were imported.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Field in API</td>
<td>Field in Streaming</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Operation</td>
<td>command</td>
<td>op</td>
</tr>
<tr>
<td>Operation Params</td>
<td>operation_params</td>
<td>operationParams</td>
</tr>
<tr>
<td>Operation Text</td>
<td>operation_text</td>
<td>opText</td>
</tr>
<tr>
<td>Permissions</td>
<td>permissions</td>
<td>perms</td>
</tr>
<tr>
<td>Privilege</td>
<td>privilege</td>
<td>privilege</td>
</tr>
<tr>
<td>Qualifier</td>
<td>qualifier</td>
<td>qualifier</td>
</tr>
<tr>
<td>Query ID</td>
<td>query_id</td>
<td>—</td>
</tr>
<tr>
<td>Resource</td>
<td>resource</td>
<td>—</td>
</tr>
<tr>
<td>Resource Path</td>
<td>resource_path</td>
<td>path</td>
</tr>
<tr>
<td>Service Name</td>
<td>service</td>
<td>service</td>
</tr>
<tr>
<td>Session ID</td>
<td>session_id</td>
<td>—</td>
</tr>
<tr>
<td>Solr Version</td>
<td>solr_version</td>
<td>solrVersion</td>
</tr>
<tr>
<td>Source</td>
<td>src</td>
<td>src</td>
</tr>
<tr>
<td>Status</td>
<td>status</td>
<td>status</td>
</tr>
<tr>
<td>Stored Object Name</td>
<td>stored_object_name</td>
<td>name</td>
</tr>
<tr>
<td>Sub Operation</td>
<td>sub_operation</td>
<td>subOperation</td>
</tr>
<tr>
<td>Table Name</td>
<td>table_name</td>
<td>table</td>
</tr>
<tr>
<td>Usage Type</td>
<td>objUsageType</td>
<td>—</td>
</tr>
<tr>
<td>Username</td>
<td>username</td>
<td>user</td>
</tr>
</tbody>
</table>
### Operations by Component

The Operation field of an audit event includes the actions taken (commands run) on the component. Operations for Cloudera Navigator (and sub-operations) are listed at Navigator Metadata Server Sub Operations on page 166.

#### Note:

Cloudera Navigator does not capture audit events for queries that are run on Spark or HiveServer1/Hive CLI. If you want to use Cloudera Navigator to capture auditing for Hive operations, upgrade to HiveServer2 if you have not done so already.

<table>
<thead>
<tr>
<th>Component</th>
<th>Action taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBase</td>
<td>addColumn, append, assign, balance, balanceSwitch, checkAndDelete, checkAndPut, compact, compactSelection, createTable, delete, deleteColumn, deleteTable, disableTable, enableTable, exists, flush, get, getClosestRowBefore, grant, increment, incrementColumnValue, modifyColumn, modifyTable, move, put, revoke, scannerOpen, shutdown, split, stopMaster, unassign.</td>
</tr>
<tr>
<td>HDFS</td>
<td>append, concat, create, createSymlink, delete, fsck, getfacl, getfileinfo, listEncryptionZones, listSnapshottableDirectory, listStatus, mkdirs, open, rename, setfacl, setOwner, setPermission, setReplication, setTimes</td>
</tr>
<tr>
<td></td>
<td>Erasure coding policy commands, including: addPolicies, disablePolicy, enablePolicy, getPolicy, listCodecs, listPolicies, setPolicy, unsetPolicy</td>
</tr>
<tr>
<td>HiveServer2/Beeline</td>
<td>ALTER_PARTITION_MERGE, ALTER_TABLE_MERGE, ALTERDATABASE, ALTERDATABASE_SET_OWNER, ALTERINDEX_PROPS, ALTERINDEX_REBUILD, ALTERPARTITION_FILEFORMAT, ALTERPARTITION_LOCATION, ALTERPARTITION_PROTECTMODE, ALTERPARTITION_SERDEPROPERTIES, ALTERPARTITION_SERIALIZER, ALTERTABLE_ADDCOLS, ALTERTABLE_ADDPARTS, ALTERTABLE_ARCHIVE, ALTERTABLE_CLUSTER_SORT, ALTERTABLE_DROPPARTS, ALTERTABLE_FILEFORMAT, ALTERTABLE_LOCATION, ALTERTABLE_PROPERTIES, ALTERTABLE_PROTECTMODE, ALTERTABLE_RENAME, ALTERTABLE_RENAMECOL, ALTERTABLE_RENAMEPART, ALTERTABLE_REPLACECOLS, ALTERTABLE_SERDEPROPERTIES, ALTERTABLE_SERIALIZER, ALTERTABLE_SET_OWNER, ALTERTABLE_TOUCH, ALTERTABLE_UNARCHIVE, ALTERVIEW_PROPERTIES, CREATEDATABASE, CREATEFUNCTION, CREATEINDEX, CREATEROLE, CREATETABLE, CREATEVIEW, DESCDATABASE, DESCFUNCTION, DESCTABLE, DROPPARTITION, DROPINDEX, DROPFILE, DROPPARTITION_FILEFORMAT, DROPTABLE, DROPVIEW, EXPLAIN, EXPORT, GRANT_PRIVILEGE, GRANT_ROLE, IMPORT, LOAD, LOCKTABLE, MSCK, QUERY, REVOKE_PRIVILEGE, REVOKE_ROLE, SHOW_GRANT, SHOW_ROLE_GRANT, SHOW_TABLESTATUS, SHOW_TBLPROPERTIES, SHOWDATABASES, SHOWFUNCTIONS, SHOWINDEXES, SHOWLOCKS, SHOWPARTITIONS, SHOWTABLES, SWITCHDATABASE, UNLOCKTABLE</td>
</tr>
<tr>
<td></td>
<td>See also <a href="#">Data Manipulation Language statements</a></td>
</tr>
<tr>
<td></td>
<td>Not supported: &quot;Shutdown&quot; option for the queue full policy.</td>
</tr>
<tr>
<td>Hue</td>
<td>ADD_LDAP_GROUPS, ADD_LDAP_USERS, CREATE_GROUP, CREATE_USER, DELETE_GROUP, DELETE_USER, DOWNLOAD, EDIT_GROUP, EDIT_PERMISSION, EDIT_USER, EXPORT, NAVIGATOR_ADD_TAG, NAVIGATOR_DELETE_TAG, SYNC_LDAP_USERS_GROUPS, USER_LOGIN, USER_LOGOUT</td>
</tr>
<tr>
<td>Impala</td>
<td>ALTER_DATABASE_SET_OWNER, ALTER_TABLE_SET_OWNER, ALTER_VIEW_SET_OWNER, CREATE_ROLE, DELETE, DROP_ROLE, GRANT privilege, GRANT_ROLE, INSERT, Query, REVOKE privilege, REVOKE ROLE, SHOW GRANT ROLE, SHOW ROLE GRANT, UPDATE, <a href="#">Hive DDL and DML Statements Support</a></td>
</tr>
<tr>
<td>Sentry</td>
<td>ADD_ROLE_TO_GROUP, ALTER_DATABASE_SET_OWNER, ALTER_TABLE_SET_OWNER, ALTER_VIEW_SET_OWNER, CREATE_ROLE, DELETE_ROLE_FROM_GROUP, DROP_ROLE, GRANT_PRIVILEGE, REVOKE_PRIVILEGE</td>
</tr>
</tbody>
</table>
HDFS Audit Logging for ACL Operations

HDFS audit logging for ACL operations has some variation based on the command options.

<table>
<thead>
<tr>
<th>Command</th>
<th>Option</th>
<th>Audit Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>getfacl</td>
<td>—</td>
<td>getAclStatus</td>
</tr>
<tr>
<td>setfacl</td>
<td>--b</td>
<td>removeAcl</td>
</tr>
<tr>
<td>setfacl</td>
<td>--k</td>
<td>removeDefaultAcl</td>
</tr>
<tr>
<td>setfacl</td>
<td>--m</td>
<td>modifyAclEntries</td>
</tr>
<tr>
<td>setfacl</td>
<td>--x</td>
<td>removeAclEntries</td>
</tr>
<tr>
<td>setfacl</td>
<td>--set</td>
<td>setAcl</td>
</tr>
</tbody>
</table>

There is a difference in audit logging behavior based on how the ACL operations are run:

- Over FileSystem ACL APIs, all `setfacl` and `getfacl` operations produce audit log events.
- Over FsShell (that is, `hadoop fs` or `hdfs dfs` command lines):
  - All `setfacl` operations produce audit log events.
  - `getfacl` operations produce audit log events only if the file has ACLs set.

That is, `setfacl` operations always produce audit log events and `getfacl` operations always produce audit log events when ACLs are set.

Hive DDL and DML Statements Support

The table below lists Hive DDL and DML statements and whether Cloudera Navigator supports the operation with metadata and lineage extraction. This list applies to Cloudera Navigator 2.12 (Cloudera Manager 5.13) and later releases.

<table>
<thead>
<tr>
<th>Hive operations</th>
<th>Cloudera Navigator Support</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort</td>
<td>🛑</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Alter Table/Partition/Column</td>
<td>🟢</td>
<td>Known Issue. ALTER TABLE RENAME TO does not create query entity. ALTER TABLE CHANGE column name does not create query operation entity.</td>
</tr>
<tr>
<td>Create Table</td>
<td>🟢</td>
<td></td>
</tr>
<tr>
<td>Create/Drop Macro</td>
<td>🛑</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Create/Drop/Alter Index</td>
<td>🛑</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Create/Drop/Alter View</td>
<td>🛑</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Create/Drop/Alter/Use Database</td>
<td>🛑</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Hive operations</td>
<td>Cloudera Navigator Support</td>
<td>Comment</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create/Drop/Grant/Revoke Roles and Privileges</td>
<td>☐</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Create/Drop/Reload Function</td>
<td>☐</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>DELETE</td>
<td>☐</td>
<td>Requires ACID support. <a href="#">Hive ACID not supported</a></td>
</tr>
<tr>
<td>Describe</td>
<td>☐</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>Drop/Truncate Table</td>
<td>☐</td>
<td></td>
</tr>
<tr>
<td>EXPORT</td>
<td>☐</td>
<td>Known Issue. External tables can be exported to HDFS but Cloudera Navigator does not create a query entity for the EXPORT.</td>
</tr>
<tr>
<td>IMPORT</td>
<td>☐</td>
<td>Known Issue. External tables can be imported from HDFS but Cloudera Navigator does not create a query entity for the IMPORT.</td>
</tr>
<tr>
<td>INSERT data into Hive Tables from queries</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>INSERT data into the file system from queries</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>INSERT values into tables from SQL</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>LOAD</td>
<td>☐</td>
<td>Known Issue. LOADING a CSV from HDFS into an existing Hive table does not generate lineage.</td>
</tr>
<tr>
<td>MERGE</td>
<td>☐</td>
<td>Requires ACID support. <a href="#">Hive ACID not supported</a></td>
</tr>
<tr>
<td>MSCK REPAIR</td>
<td>☐</td>
<td>Tables track their respective partitions. Queries to create or repair partitions using <a href="#">MSCK</a> are not captured as query entities.</td>
</tr>
<tr>
<td>Show</td>
<td>☐</td>
<td>Operation does not generate data flow lineage.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>☐</td>
<td>Requires ACID support. <a href="#">Hive ACID not supported</a></td>
</tr>
</tbody>
</table>

### Navigator Metadata Server Sub Operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Sub Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditReport</td>
<td>createAuditReport, deleteAuditReport, fetchAllReports, updateAuditReport</td>
</tr>
<tr>
<td>authorization</td>
<td>deleteGroup, fetchGroup, fetchRoles, searchGroup, updateRoles</td>
</tr>
<tr>
<td>metadata</td>
<td>fetchAllMetadata, fetchMetadata, updateMetadata</td>
</tr>
<tr>
<td>policy</td>
<td>createPolicy, deletePolicy, deletePolicySchedule, fetchAllPolicies, fetchPolicySchedule, updatePolicy, updatePolicySchedule</td>
</tr>
<tr>
<td>savedSearch</td>
<td>createSavedSearch, deleteSavedSearch, fetchAllSaved Searches, fetchSavedSearch, updateSavedSearch</td>
</tr>
</tbody>
</table>
Service Metadata Entity Types

Metadata entities are the data assets stored in and operations generated by services running on the cluster. Users with the appropriate permissions (Metadata and Lineage Viewer, Full Administrator) can view metadata entities in the Cloudera Navigator console or by using the APIs.

The Cloudera Navigator console includes entities extracted from services that are enabled for integration with Navigator Metadata Service.

Navigator creates the following entities from metadata extracted from these services:

<table>
<thead>
<tr>
<th>Service</th>
<th>Navigator Entity Types Created from Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>directory, file</td>
</tr>
<tr>
<td>HiveServer2</td>
<td>database, table, field, operation, operation_execution, sub_operation, partition, view</td>
</tr>
<tr>
<td>Impala</td>
<td>operation, operation_execution, sub_operation</td>
</tr>
<tr>
<td>Mapreduce (v1 and v2)</td>
<td>operation, operation_execution</td>
</tr>
<tr>
<td>Oozie</td>
<td>operation, operation_execution</td>
</tr>
<tr>
<td>Pig</td>
<td>operation, operation_execution</td>
</tr>
<tr>
<td>Spark (v1 and v2)</td>
<td>operation, operation_execution</td>
</tr>
<tr>
<td>Sqoop (v1)</td>
<td>operation, operation_execution, sub_operation</td>
</tr>
<tr>
<td>YARN</td>
<td>operation, operation_execution</td>
</tr>
<tr>
<td>Cluster</td>
<td>cluster_template,cluster_instance</td>
</tr>
<tr>
<td>S3</td>
<td>file, s3bucket</td>
</tr>
</tbody>
</table>

Hive Operations and Cloudera Navigator Support Matrix

The table below lists Hive DDL and DML statements and whether Cloudera Navigator supports the operation with metadata and lineage extraction.

<table>
<thead>
<tr>
<th>Hive operations</th>
<th>Cloudera Navigator Metadata Support</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Alter Table/Partition/Column</td>
<td>☑</td>
<td>ALTER TABLE RENAME TO does not create query entity. ALTER TABLE CHANGE column name does not create query entity.</td>
</tr>
<tr>
<td>Create Table</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Create/Drop Macro</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Create/Drop/Alter Index</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Create/Drop/Alter View</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Create/Drop/Alter/Use Database</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Create/Drop/Grant/Revoke Roles and Privileges</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Create/Drop/Reload Function</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Hive operations</td>
<td>Cloudera Navigator Metadata Support</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>DELETE</td>
<td>☒</td>
<td>Requires ACID support. <strong>Hive ACID not supported</strong>.</td>
</tr>
<tr>
<td>Describe</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>Drop/Truncate Table</td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>EXPORT</td>
<td>☒</td>
<td>Known Issue. External tables can be exported to HDFS but Cloudera Navigator does not create a query entity for the EXPORT.</td>
</tr>
<tr>
<td>IMPORT</td>
<td>☒</td>
<td>Known Issue. External tables can be imported from HDFS but Cloudera Navigator does not create a query entity for the IMPORT.</td>
</tr>
<tr>
<td>INSERT data into Hive Tables from queries</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>INSERT data into the filesystem from queries</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>INSERT values into tables from SQL</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>LOAD</td>
<td>☒</td>
<td>Known Issue. LOADING a CSV from HDFS into an existing Hive table does not generate lineage.</td>
</tr>
<tr>
<td>MERGE</td>
<td>☒</td>
<td>Requires ACID support. <strong>Hive ACID not supported</strong>.</td>
</tr>
<tr>
<td>MSCK REPAIR</td>
<td>☒</td>
<td>Tables track their respective partitions. Queries to create or repair partitions using <strong>MSCK</strong> are not captured as query entities.</td>
</tr>
<tr>
<td>Show</td>
<td>☒</td>
<td>Operation does not generate data flow.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>☒</td>
<td>Requires ACID support. <strong>Hive ACID not supported</strong>.</td>
</tr>
</tbody>
</table>

Cloudera Navigator extractor for Hive does not support all Hive statements, specifically these:

- Table-generating functions
- Lateral views
- Transform clauses
- Regular expressions (regex) in SELECT clause

Hive queries that include any of the above will prevent lineage diagrams from completing successfully.

**Metadata Policy Expressions**

A **metadata policy expression** is a Java expression that uses Java expressions instead of string literals to define properties for a metadata extraction policy. Properties that can be defined using Java expressions include entity names and descriptions, managed properties, user-defined properties, and JMS notification messages. Declare classes for the expression to use in the policy's **import** statement. The Java expressions defined to apply policies must evaluate to strings.

The Cloudera Navigator console displays an **Expression** check box near entities that can use Java expressions. Click the help icon for a pop-up example of an expression:
Expressions can support the following:

- Metadata Assignments
  - Name
  - Description
  - Managed Properties (Key-Value Pairs)
  - User-defined Properties (Key-Value Pairs)

- JMS Notification Messages

**Note:** Using Java expressions to define policies is not enabled by default. See [Configuring the Server for Policy Messages](#) to enable this feature.

### Including Entity Properties in Policy Expressions

To include entity properties in property expressions, use the `entity.get` method and pass the property and return type as follows:

```java
entity.get(EnumTypeProperties.PROPERTY, return_type)
```

The `EnumTypeProperties.PROPERTY` and respective values for `return_type` are detailed in full in the [Entity Property Enum Reference](#) below. The `EnumType` class names are:

- FSEntity
- HiveColumn
- HiveDatabase
- HivePartition
- HiveQueryExecution
- HiveQueryPart
- HiveQuery
- HiveTable
- HiveView
- JobExecution
- Job
- WorkflowInstance
- Workflow
- PigField
- PigOperationExecution
- PigOperation
- PigRelation
- SqoopExportSubOperation
- SqoopImportSubOperation
- SqoopOperationExecution
For any operation based on return type \( (\text{return\_type}) \), use the return type listed in Entity Property Enum Reference on page 170. Each \textit{PROPERTY} listed for a given \textit{EnumType} has its data type \( (\text{return\_type}) \) specified following the Java comment //.

For example, the return type for the \textit{ORIGINAL\_NAME} property of the \texttt{FSEntityProperties} class is \texttt{java.lang.String}, which means you can use \texttt{String} methods such as \texttt{toLowerCase()} to modify the returned value:

\[
\text{entity.get(FSEntityProperties.ORIGINAL\_NAME, String.class).toLowerCase()}
\]

\textbf{Note:} For expressions that do not require specific type, use \texttt{Object.class} as the return type.

**Metadata Policy Expression Examples**

Here are some short examples showing how to use Java expressions for metadata policies. The examples include the import statements to enter into the \textbf{Import Statements} field when creating policies in the Cloudera Navigator console.

- Set a filesystem entity name to the original name concatenated with the entity type:

  \[
  \text{entity.get(FSEntityProperties.ORIGINAL\_NAME, Object.class) + " " + entity.get(FSEntityProperties.TYPE, Object.class)}
  \]

  \textbf{Import Statements:}
  
  \[
  \text{import com.cloudera.nav.hdfs.model.FSEntityProperties;}
  \]

- Add the entity's creation date to the entity name:

  \[
  \text{entity.get(FSEntityProperties.ORIGINAL\_NAME, Object.class) + " - " + new SimpleDateFormat("yyyy-MM-dd").format(entity.get(FSEntityProperties.CREATED, Instant.class).toDate())}
  \]

  \textbf{Import Statements:}
  
  \[
  \text{import com.cloudera.nav.hdfs.model.FSEntityProperties; import java.text.SimpleDateFormat; import org.joda.time.Instant;}
  \]

- Set the key-value pair: retain_until-seven years from today's local time:

  \[
  \text{new DateTime().plusYears(7).toLocalDateTime().toString("MMM dd yyyy", Locale.US)}
  \]

  \textbf{Import statements:}
  
  \[
  \text{import org.joda.time.DateTime; import java.util.Locale;}
  \]

**Entity Property Enum Reference**

The Java enumerations for retrieving properties from each entity type are listed below.

\[
\text{com.cloudera.nav.hdfs.model.FSEntityProperties}
\]

\[
\text{public enum FSEntityProperties implements PropertyEnum \{}
\]

\[
\text{PERMISSIONS, // Return type: java.lang.String}
\]

\[
\}}
\]
public enum HiveColumnProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    DELETED, // Return type: java.lang.Boolean
    DATA_TYPE, // Return type: java.lang.String
    ORIGINAL_DESCRIPTION, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

public enum HiveDatabaseProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    ORIGINAL_DESCRIPTION, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    DELETED, // Return type: java.lang.Boolean
    FILE_SYSTEM_PATH, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

public enum HivePartitionProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    DELETED, // Return type: java.lang.Boolean
    FILE_SYSTEM_PATH, // Return type: java.lang.String
    CREATED, // Return type: org.joda.time.Instant
    LAST_ACCESSED, // Return type: org.joda.time.Instant
    COL_VALUES, // Return type: java.util.List
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

public enum HiveQueryExecutionProperties implements PropertyEnum {
com.cloudera.nav.hive.model.HiveQueryPartProperties
public enum HiveQueryPartProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.hive.model.HiveQueryProperties
public enum HiveQueryProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    INPUTS, // Return type: java.util.Collection
    OUTPUTS, // Return type: java.util.Collection
    QUERY_TEXT, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    WF_IDS, // Return type: java.util.Collection
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.hive.model.HiveTableProperties
public enum HiveTableProperties implements PropertyEnum {
    OWNER, // Return type: java.lang.String
    INPUT_FORMAT, // Return type: java.lang.String
    OUTPUT_FORMAT, // Return type: java.lang.String
    DELETED, // Return type: java.lang.Boolean
    FILE_SYSTEM_PATH, // Return type: java.lang.String
    COMPRESSED, // Return type: java.lang.Boolean
    PARTITION_COL_NAMES, // Return type: java.util.List
    CLUSTERED_BY_COL_NAMES, // Return type: java.util.List
    SORT_BY_COL_NAMES, // Return type: java.util.List
    SER_DE_NAME, // Return type: java.lang.String
    SER_DE_LIB_NAME, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    CREATED, // Return type: org.joda.time.Instant
    LAST_ACCESSED, // Return type: org.joda.time.Instant
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
}
com.cloudera.nav.hive.model.HiveViewProperties
public enum HiveViewProperties implements PropertyEnum {
    DELETED, // Return type: java.lang.Boolean
    QUERY_TEXT, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    CREATED, // Return type: org.joda.time.Instant
    LAST_ACCESSSED, // Return type: org.joda.time.Instant
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: org.joda.time.Instant
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.mapreduce.model.JobExecutionProperties
public enum JobExecutionProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    JOB_ID, // Return type: java.lang.String
    ENDED, // Return type: org.joda.time.Instant
    INPUT_RECURSIVE, // Return type: boolean
    TYPE, // Return type: java.lang.String
    INPUTS, // Return type: java.util.Collection
    OUTPUTS, // Return type: java.util.Collection
    STARTED, // Return type: org.joda.time.Instant
    PRINCIPAL, // Return type: java.lang.String
    WF_INST_ID, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.mapreduce.model.JobProperties
public enum JobProperties implements PropertyEnum {
    ORIGINAL_NAME, // Return type: java.lang.String
    INPUT_FORMAT, // Return type: java.lang.String
    OUTPUT_FORMAT, // Return type: java.lang.String
    OUTPUT_KEY, // Return type: java.lang.String
    OUTPUT_VALUE, // Return type: java.lang.String
    MAPPER, // Return type: java.lang.String
    REDUCER, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    WF_IDS, // Return type: java.util.Collection
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.oozie.model.WorkflowInstanceProperties
public enum WorkflowInstanceProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    CREATED, // Return type: org.joda.time.Instant
    JOB_ID, // Return type: java.lang.String
    STATUS, // Return type: java.lang.String
    ENDED, // Return type: org.joda.time.Instant
    INPUTS, // Return type: java.util.Collection
    OUTPUTS, // Return type: java.util.Collection
    STARTED, // Return type: org.joda.time.Instant
PRINCIPAL, // Return type: java.lang.String
WF_INST_ID, // Return type: java.lang.String
NAME, // Return type: java.lang.String
ORIGINAL_NAME, // Return type: java.lang.String
USER_ENTITY, // Return type: boolean
SOURCE_ID, // Return type: java.lang.String
EXTRACTOR_RUN_ID, // Return type: java.lang.String
PARENT_PATH; // Return type: java.lang.String

com.cloudera.nav.oozie.model.WorkflowProperties
public enum WorkflowProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.pig.model.PigFieldProperties
public enum PigFieldProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    INDEX, // Return type: int
    SOURCE_TYPE, // Return type: java.lang.String
    DATA_TYPE, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.pig.model.PigOperationExecutionProperties
public enum PigOperationExecutionProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    ENDED, // Return type: org.joda.time.Instant
    INPUTS, // Return type: java.util.Collection
    OUTPUTS, // Return type: java.util.Collection
    STARTED, // Return type: org.joda.time.Instant
    PRINCIPAL, // Return type: java.lang.String
    WF_INST_ID, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.pig.model.PigOperationProperties
public enum PigOperationProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    OPERATION_TYPE, // Return type: java.lang.String
    SCRIPT_ID, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    WF_IDS, // Return type: java.util.Collection
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
}
com.cloudera.nav.pig.model.PigRelationProperties
public enum PigRelationProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    FILE_SYSTEM_PATH, // Return type: java.lang.String
    SPRING_ID, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.sqoop.model.SqoopExportSubOperationProperties
public enum SqoopExportSubOperationProperties implements PropertyEnum {
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    INPUTS, // Return type: java.util.Collection
    FIELD_INDEX, // Return type: int
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.sqoop.model.SqoopImportSubOperationProperties
public enum SqoopImportSubOperationProperties implements PropertyEnum {
    DB_COLUMN_EXPRESSION, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    SOURCE_TYPE, // Return type: java.lang.String
    INPUTS, // Return type: java.util.Collection
    FIELD_INDEX, // Return type: int
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.sqoop.model.SqoopOperationExecutionProperties
public enum SqoopOperationExecutionProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    TYPE, // Return type: java.lang.String
    ENDED, // Return type: org.joda.time.Instant
    INPUTS, // Return type: java.util.Collection
    OUTPUTS, // Return type: java.util.Collection
    STARTED, // Return type: org.joda.time.Instant
    PRINCIPAL, // Return type: java.lang.String
    WF_INST_ID, // Return type: java.lang.String
    NAME, // Return type: java.lang.String
    ORIGINAL_NAME, // Return type: java.lang.String
    USER_ENTITY, // Return type: boolean
    SOURCE_ID, // Return type: java.lang.String
    EXTRACTOR_RUN_ID, // Return type: java.lang.String
    PARENT_PATH; // Return type: java.lang.String
}

com.cloudera.nav.sqoop.model.SqoopQueryOperationProperties
public enum SqoopQueryOperationProperties implements PropertyEnum {
    SOURCE_TYPE, // Return type: java.lang.String
    INPUTS, // Return type: java.util.Collection
}
User Roles and Privileges Reference

Cloudera Navigator lets authenticated users—those who have successfully logged in to Cloudera Navigator console—access features and functionality according to specifically assigned user roles. The Cloudera Navigator user role scheme requires the use of an external LDAP-compliant identity-directory service, such as OpenLDAP or Microsoft Server Active Directory. See Cloudera Navigator Authentication Overview for details.

After users have been assigned to various groups in the external LDAP-compliant identity-directory service, Cloudera Navigator administrators can grant user roles to various groups as needed. See Administering Navigator User Roles on page 74 for details.

Information about user roles and the specific privileges to Cloudera Navigator is contained in the high-level summary and detailed matrix below.
**Cloudera Navigator User Roles**

Cloudera Navigator provides the following user roles for organizing and applying user permissions:

- **Auditing Viewer**—View audit events, view audit analytics, and create audit reports.
- **Custom Business Metadata Editor**—Search for entities, view metadata, view lineage, view metadata analytics, edit user-defined properties and tags.
- **Managed and Custom Business Metadata Editor**—Search for entities, view metadata, view lineage, edit user-defined properties, edit managed properties, and define managed metadata models.
- **Metadata & Lineage Viewer**—Search for entities, view metadata, view lineage, and view metadata analytics such as the Data Stewardship Dashboard and the Data Explorer.
- **Policy Editor**—View, create, update, and delete metadata policies.
- **Policy Viewer**—View policies that can be applied to metadata. Note that this role needs to be combined with other roles to give view access to Navigator metadata.
- **User Administrator**—Assign user roles to groups. Requires the group (and the user accounts it contains) to exist in an LDAP-compliant directory service. See Configuring Navigator User Roles and Authentication and Cloudera Navigator for details.
- **Full Administrator**—All Navigator permissions.

Cloudera Manager provides the following user roles for managing Cloudera Manager and Cloudera Navigator.

- **Full Administrator**—Complete administrative and management access, including assigning user roles to groups. Required to install Cloudera Navigator. Users with this role are automatically assigned the Navigator Full Administrator role.
- **Navigator Administrator**—View data in Cloudera Manager, view service and monitoring information, administer Cloudera Navigator, view audit events. Users with this role are automatically assigned the Navigator Full Administrator role.

**Cloudera Navigator User Role Details**

The Cloudera Manager user roles **Full Administrator** and **Navigator Administrator** have the privileges listed for Full Administrator in the table below.

<table>
<thead>
<tr>
<th>Cloudera Navigator User Role</th>
<th>Auditing Viewer</th>
<th>Custom Business Metadata Editor</th>
<th>Managed and Custom Business Metadata Editor</th>
<th>Metadata &amp; Lineage Viewer</th>
<th>Policy Editor</th>
<th>Policy Viewer</th>
<th>User Administrator</th>
<th>Full Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-to-group mapping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define metadata models</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit entity name or description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit user-defined properties and tags</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit managed properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloudera Navigator User Role</td>
<td>Auditing Viewer</td>
<td>Custom Business Metadata Editor</td>
<td>Managed and Custom Business Metadata Editor</td>
<td>Metadata &amp; Lineage Viewer</td>
<td>Policy Editor</td>
<td>Policy Viewer</td>
<td>User Administrator</td>
<td>Full Administrator</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------</td>
<td>--------------</td>
<td>---------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Search for entities</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>Start maintenance job</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>View audit analytics</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>View audit events and create reports</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>View lineage</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>View maintenance history</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>View metadata analytics</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>View metadata policies</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Enable debugging tools</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☑</td>
</tr>
</tbody>
</table>
Troubleshooting Navigator Data Management

This page contains troubleshooting tips and workarounds for various issues that can arise.

Cloudera Navigator-Cloudera Altus

No metadata or lineage collected from an Altus deployed cluster.

**Symptom:** No metadata collected from a Cloudera Altus instantiated cluster. Although both the Cloudera Altus environment has been setup to use a given Amazon S3 bucket and the Cloudera Navigator instance has been configured to read from that same S3 bucket, no metadata is collected.

**Possible cause:** Permissions on the Amazon S3 bucket have not been applied correctly.

**Steps to resolve:** To determine the root cause of this issue:

- Check that permissions have been set properly on the Amazon S3 bucket.
- Verify that the Amazon S3 bucket name has not been changed.

To determine if the cause of the issue is misconfiguration, look at the Telemetry Publisher logs. A failure message in the log such as the following means that the Amazon S3 bucket has either not been properly identified, or that the correct permissions have not been set:

```plaintext
...Metadata export failed com.amazonaws.services.s3.model.AmazonS3Exception: The specified bucket does not exist
(Service: Amazon S3; Status Code: 404; Error Code: NoSuchBucket; Request ID: D28543E2494BD521), S3 Extended Request ID:
...
```

The 404 status code and "NoSuchBucket" in the error message indicate the Telemetry Publisher was unable to write to Amazon S3 bucket because the bucket was misidentified or that permissions were configured incorrectly.

Navigator Audit Server

"No serializer found" error

**Symptom:** Selecting an Audits page results in error message.

**Error message:**

```
No serializer found
```

**Possible cause:** Communication failure somewhere between Navigator Metadata Server and Cloudera Manager Server and its communication to Navigator Audit Server. This is an existing Known Issue that needs to be resolved so that the error message can be properly mapped.

**Workaround:** This workaround does not resolve the issue, but provides additional information as to the actual source of the underlying error.

1. Log in to the Cloudera Navigator console.
2. Enable Navigator API logging.
3. Perform your action on the Audits page that raised the error message and see if the underlying issue is caught in the API log. If the Navigator API logging reveals no additional information, turn on API logging for Cloudera Manager:
   - Log in to the Cloudera Manager Admin Console.
   - Select Administrator > Settings
• Select Advanced for the Category filter.
• Click the Enable Debugging of API check box to select it. The server log will contain all API calls. Try your request again and see if the source error message displays in the response.

Processing a backlog of audit logs

Problem: You have logs that include audit events that were not processed by the Cloudera Navigator Audit Server, such as logs for events that took place before audit server was online or during a period when audit server was offline.

Solution: A backlog of logs can be processed by audit server as follows:

1. Determine what days were not processed and will need to have partitions created for them. The audit log files have the UNIX epoch appended to their name:

   hdfs-NAMENODE-341ad9b94435839ce45b8b22e7c805b3-HdfsAuditLogger-1499844328581

   You want the dates from the oldest and newest files. You can do this by sorting the list and identifying the first and last files. For example, for HDFS audit files:

   The oldest: $ ls ./hdfs* | head -1

   The newest: $ ls ./hdfs* | tail -1

   Depending on your shell, you can convert the epoch value to a date using `date -r`.

2. Create partitions in the Navigator Audit Server database for days that have missing audits.

   Create a partition from an existing template table using SQL commands. Use `SHOW TABLES` to list the template tables. For example, the template table for HDFS is `HDFS_AUDIT_EVENTS`.

   Using MySQL as an example, if you have partitions up to March 31, 2017 and your audit logs include HDFS data for the first week of April, you would run the following SQL commands:

   ```
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_01 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_02 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_03 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_04 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_05 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_06 LIKE HDFS_AUDIT_EVENTS;
   CREATE TABLE HDFS_AUDIT_EVENTS__2017_04_07 LIKE HDFS_AUDIT_EVENTS;
   ```

3. Change the Navigator Audit expiration period to be longer than the time period of the logs you want to process.

   Set the expiration period in Cloudera Manager. Search for the property “Navigator Audit Server Data Expiration Period”.

4. Stop the Cloudera Manager agent on the host running the role for the service whose logs will be restored.

   For example, if the logs are for HDFS, stop the agent on the namenode. For HiveServer2, stop the Cloudera Manager agent on the node where HiveServer2 is running. See Starting, Stopping, and Restarting Cloudera Manager Agents.

   If you aren’t sure of which host is involved, the log files contain the UUID of the role which generated them. Go to the host defined for that role. For high-availability clusters, make sure that you stop the role on the active host.

5. On that host, copy the backed up audit logs to the audit directory.

   The location is typically `/var/log/service/audit`. For example, `/var/log/hadoop-hdfs/audit`. The specific locations are configured in the Cloudera Manager `audit_event_log_dir` properties for each service.

6. Move the WAL file out of this directory. (Back it up in a safe location.)

7. Restart the Cloudera Manager agent.

   On restart, Cloudera Manager agent will not find the WAL file and will create a new one. It will process the older audit logs one by one.
8. Verify that the audits appear in Navigator.
   You can also check the contents of the WAL file to see which logs were processed.

Navigator Metadata Server

Server restart needed

If you see the following errors in the Navigator Metadata Server log, it's highly likely that the server needs to be restarted.

Embedded Solr isn't running

The following error indicates that Solr isn't running. Restarting Navigator Metadata Server is the best way to make sure Solr is running in the correct context.

```
[CDHExecutor-0-CDHUrlClassLoader@4446b570]: Failed to extract table example_table from
database example_db
with error: org.apache.solr.client.solrj.SolrServerException: IOException occured when
talking to server at: https://localhost:7187/solr/nav_elements
java.lang.RuntimeException: org.apache.solr.client.solrj.SolrServerException: IOException
occured when talking to server at: https://localhost:7187/solr/nav_elements
```
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.


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.
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.
```