CCP Monitoring 2.0.0

Monitoring

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Monitor Overview

Cloudera Cybersecurity Platform (CCP) powered by Apache Metron provides you with several options for monitoring your system. Before you perform any of these tasks, you should become familiar with CCP data throughput.

Understanding Throughput

Data flow for CCP occurs in real-time and involves Apache Kafka files ingesting raw telemetry data; parsing it into a structure that CCP can read; enriching it with asset, geo, and threat intelligence information; and indexing and storing the enriched data.

Depending on the type of data streaming into CCP, streaming occurs using Apache NiFi, performance networking ingestion probes, or real-time and batch threat intelligence feed loaders.

- Apache Kafka ingests information from telemetry data sources rough the telemetry event buffer.

  This information is the raw telemetry data consisting of host logs, firewall logs, emails, and network data. Depending on the type of data you are streaming into CCP, you can use one of the following telemetry data collectors to ingest the data:

  NiFi

  This type of streaming works for most types of telemetry data sources. See the NiFi documentation for more information,

  Performant network ingestion probes

  This type of streaming works for streaming high volume packet data.

  Real-time and batch threat intelligence feed loaders

  This type of streaming works for real-time and batch threat intelligence feed loaders.

- After the data is ingested into Kafka files, it is parsed into a normalized JSON structure that CCP can read. This information is parsed using a Java or general purpose parser and then it is uploaded to Apache ZooKeeper. A Kafka file containing the parser information is created for every telemetry data source.
- The information is enriched with asset, geo, and threat intelligence information.
- The information is indexed and stored, and any resulting alerts are sent to the Metron dashboard.

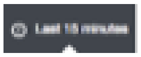
Display the Metron Error Dashboard

The Metron Error Dashboard displays information on all errors detected by CCP.

Before you begin

Prior to displaying the Metron Error Dashboard, ensure that you have created an index template.

Procedure

1. In the main Metron dashboard, click Dashboard in the upper left corner of the Metron dashboard.
2. Select **Metron-Error-Dashboard** from the list of dashboards.
3. Click  (timeframe tab) in the upper right corner of the Metron Error Dashboard to choose the timeframe you want to use.

Metron Error Dashboard Information

The Metron dashboard receives information from error messages.

The Metron Error dashboard receives the following information for all error messages:

- Exception
- Hostname - The machine on which the error occurred
- Stack trace
- Time - When the error occurred
- Message
- Raw Message - Original message
- Raw_message_bytes - The bytes of the original message
- Hash - Determines if there is a duplicate message
- Source_type - Identifies source sensor
- Error type - Defines the error type; for example parser error

Default Metron Error Dashboard Section Descriptions

The Metron dashboard uses a set of default fields that you can customize.

Total Error Messages

The total number of error messages received during an interim that you specify.

Unique Error Messages

The total number of unique error messages received during the interim that you have specified.

Errors Over Time

A **detailed message panel** that displays the raw data from your search query.

Error Source

When you submit a search query, the 500 most recent documents that match the query are listed in the **Documents** table.

Errors by Error Type

A list of all of the fields associated with a selected index pattern.

Error Type Proportion

Use the **line chart** when you want to display high density time series. This chart is useful for comparing one series with another.

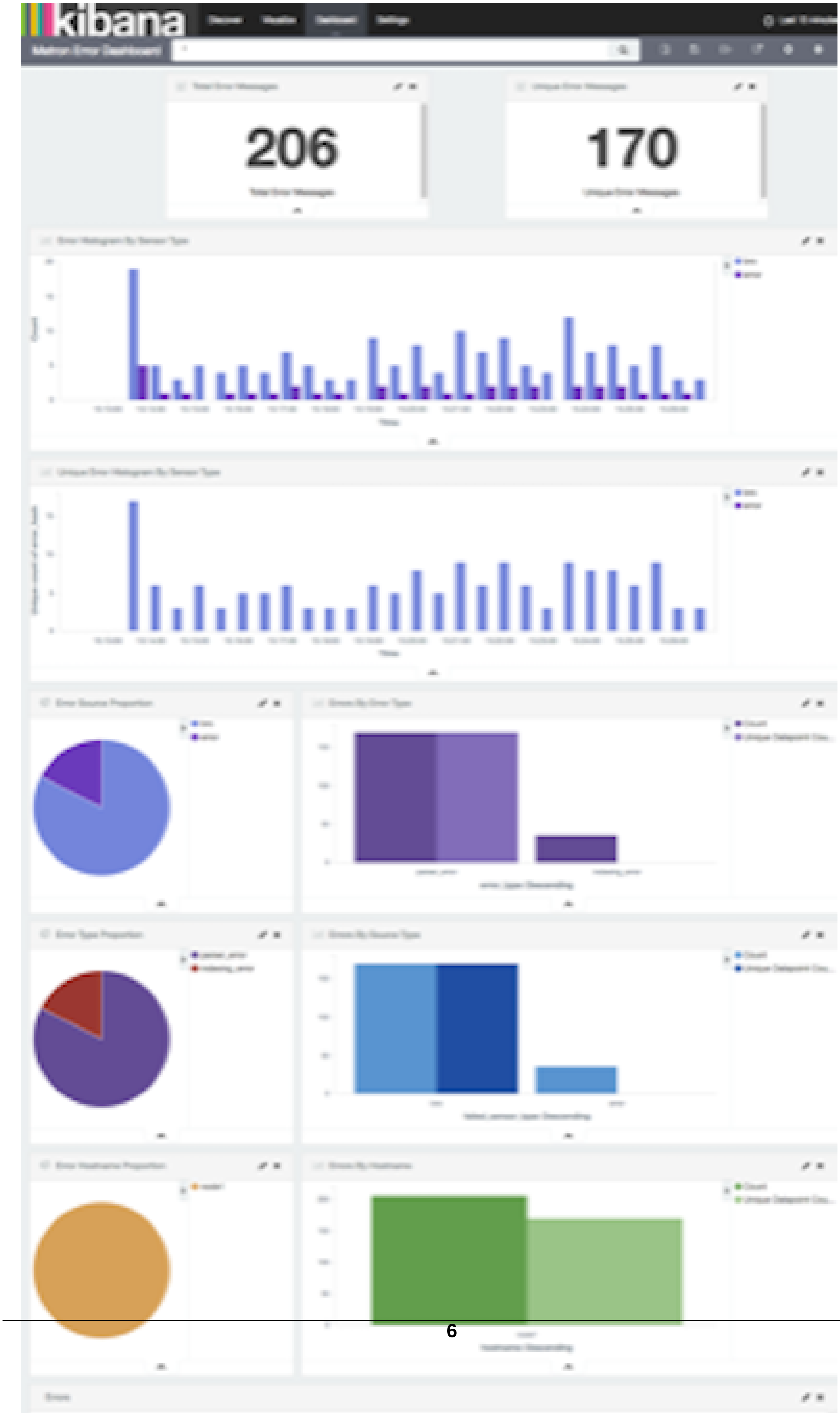
Errors by Type

You can use the **mark down widget panel** to provide explanations or instructions for the dashboard.

List of Errors

You can use a **metric panel** to display a single large number such as the number of hits or the average of a numeric field.

The default Error dashboard should look similar to the following:


kibana
206
170

Reload Metron Templates

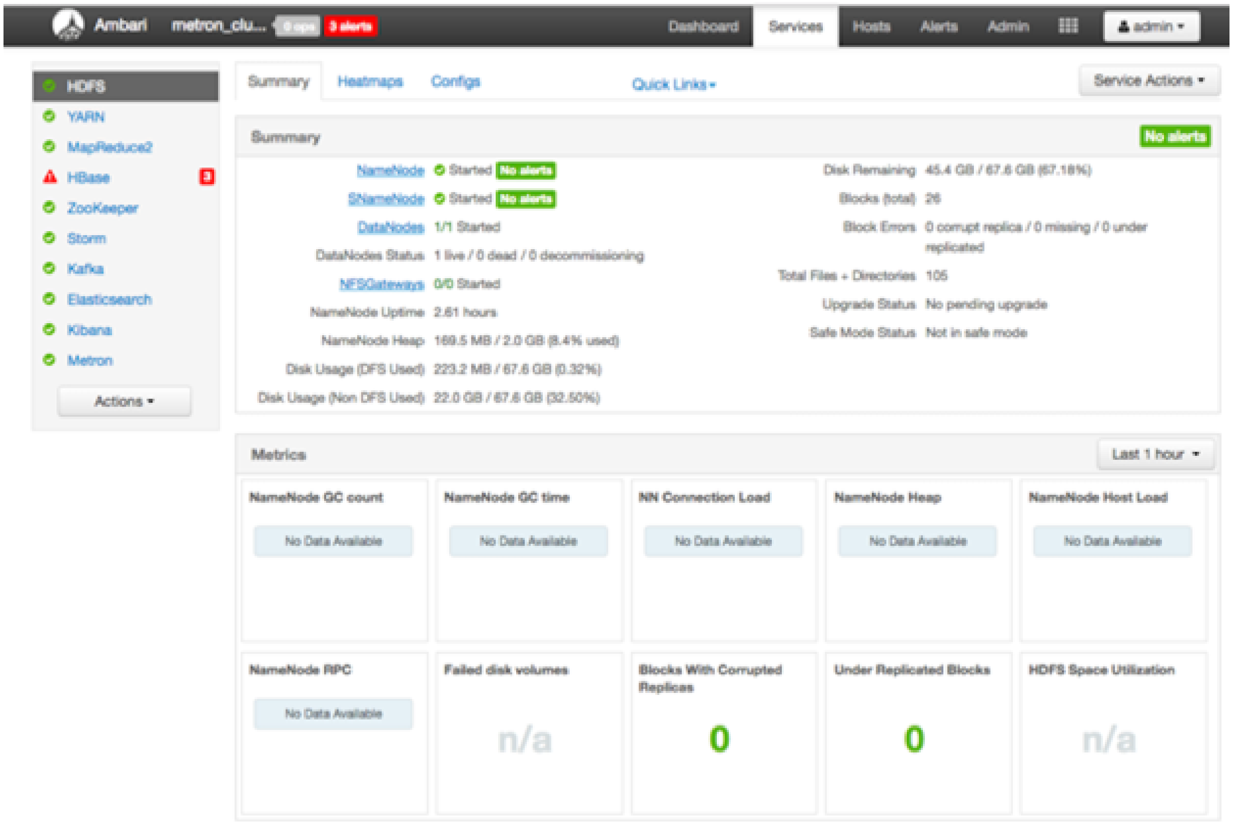
Cloudera Cybersecurity Platform (CCP) provides templates that display the default format for the Metron UI dashboards. You might want to reload these templates if the Metron UI is not displaying the default dashboard panes, or if you would like to return to the default format.

Procedure

1. From web browser, display the Ambari UI:

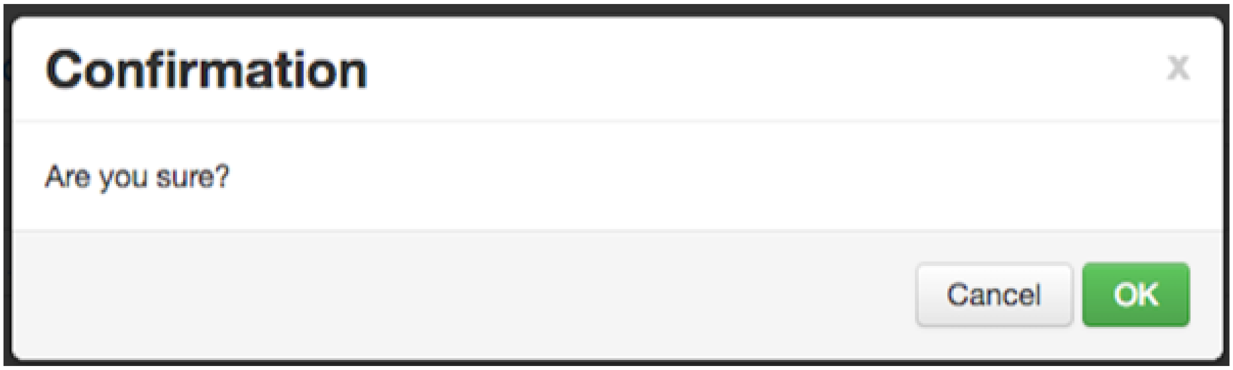
```
https://$METRON_HOME:8080
```

2. Click the **Services** tab.
3. Select Kibana in the left pane of the window.



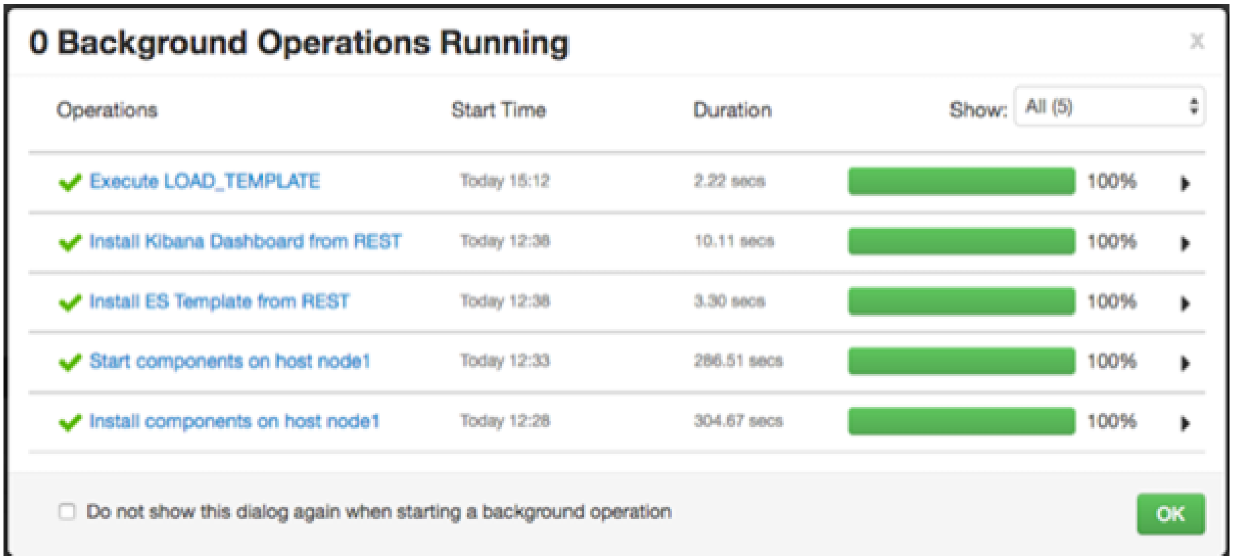
NameNode Started No alerts
SNameNode Started No alerts
DataNodes 1/1 Started
DataNodes Status 1 live / 0 dead / 0 decommissioning
NFSGateways 0/0 Started
NameNode Uptime 2.61 hours
NameNode Heap 169.5 MB / 2.0 GB (8.4% used)
Disk Usage (DFS Used) 223.2 MB / 67.6 GB (0.32%)
Disk Usage (Non DFS Used) 22.0 GB / 67.6 GB (32.50%)
Disk Remaining 45.4 GB / 67.6 GB (67.18%)
Blocks (total) 26
Block Errors 0 corrupt replica / 0 missing / 0 under replicated
Total Files + Directories 105
Upgrade Status No pending upgrade
Safe Mode Status Not in safe mode

4. From the **Service Actions** menu, select **Load Template**.
5. In the Confirmation dialog box, click the **OK**.



Are you sure?

Ambari displays a dialog box listing the background operations it is running.



0 Background Operations Running

Operations	Start Time	Duration	Show: All (5)
✓ Execute LOAD_TEMPLATE	Today 15:12	2.22 secs	100%
✓ Install Kibana Dashboard from REST	Today 12:38	10.11 secs	100%
✓ Install ES Template from REST	Today 12:38	3.30 secs	100%
✓ Start components on host node1	Today 12:33	286.51 secs	100%
✓ Install components on host node1	Today 12:28	304.67 secs	100%

□ Do not show this dialog again when starting a background operation

6. In the **Background Operation Running**dialog box, click **OK** to dismiss the dialog box.

   Ambari has completed loading the Metron template. You should be able to see the default formatting in the Metron dashboards.