

CCP Synching With Metron Dashboard 2.0.1

Synching With Metron Dashboard

Date of publish: 2017-11-06

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

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

Create an Index Template.....	4
Configure the Metron Dashboard to View the New Data Source Telemetry Events.....	5

Create an Index Template

To work with a new data source data in the Metron dashboard, you must ensure that the data is sent to the search index (Solr or Elasticsearch) with the correct data types. You achieve this by defining an index template and configuring the Metron Dashboard to view the new data source telemetry events.

Before you begin

You must update the Index template after you add or change enrichments for a data source.

Procedure

1. Run a command similar to the following to create an index template for the new data source:

```
curl -XPOST $SEARCH_HOST:$SEARCH_PORT/_template/$DATASOURCE_index -d '
{
  "template": "sensor1_index*",
  "mappings": {
    "sensor1_doc": {
      "properties": {
        "timestamp": {
          "type": "date",
          "format": "epoch_millis"
        },
        "ip_src_addr": {
          "type": "ip"
        },
        "ip_src_port": {
          "type": "integer"
        },
        "ip_dst_addr": {
          "type": "ip"
        },
        "ip_dst_port": {
          "type": "integer"
        }
      }
    }
  }
}
```

This example shows an index template for a new sensor called sensor1.

- The template applies to any indices that are named sensor1_index*.
- The index has one document type that must be named sensor1_doc.
- The index is expected to contain timestamps.
- The properties section defines the types of each field.

This example defines the five common fields that most sensors contain.

- You can add fields following the five that are already defined.

By default, Elasticsearch attempts to analyze all fields of type string. This means that Elasticsearch tokenizes the string and performs additional processing to enable free-form text search. In many cases, you want to treat each of the string fields as enumerations. This is why most fields in the index template for Elasticsearch have the value not_analyzed.

2. Delete existing indices to enable updated replacements using the new template:

```
curl -XDELETE $SEARCH_HOST:9200/$DATASOURCE*
```

3. Wait for the new data source index to be re-created:

```
curl -XGET $SEARCH_HOST:9200/$DATASOURCE*
```

This might take a minute or two based on how fast the new data source data is being consumed in your environment.

Configure the Metron Dashboard to View the New Data Source Telemetry Events

After Cloudera Cybersecurity Platform (CCP) is configured to parse, index, and persist telemetry events and NiFi is pushing data to CCP, you can view streaming telemetry data in the Metron Dashboard.