CCP Synching With Metron Dashboard 2.0.0

Synching With Metron Dashboard

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

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 $SEARCH_HOST:9200/$DATSOURCE*
```

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.