Grok Integration with DataDog

Starting with Grok 1.3 we are excited to announce integration of Grok with DataDog.

Grok Anomaly scores can be exported and visualized in DataDog.
DataDog users can visualize Grok Anomaly scores combined with metric data and monitor the health of these metrics with the benefits of DataDog.

Setting up the Export to DataDog

A sample script to send Metric and Anomaly data from Grok to DataDog is available on Github and PyPI. You can install it via pip:

```
%> pip install grokcli
```

Please follow the instructions in https://github.com/GrokSolutions/grok-cli to ensure grokcli is setup correctly and that you have the correct Grok API key. Once grokcli is setup, the following example will send the last twelve records (one hour) of data from Grok to Datadog for the specified metric.

```
%> python –m grokcli.datadog --datadogApiKey=<datadog-api-key> --
grokServer=<Grok server URL> --grokApiKey=<Grok server API key> --
numRecords=12 <Metric ID>
```

The Grok values and anomaly scores will be sent to Datadog as two separate metrics with their names appended with ".value" and ".anomalyScore", respectively. The Datadog metrics will have the host attribute set as the Grok server value.

Please note that you can get the metric ID from Grok using the Grok command-line tool. An example to list all monitored metrics:

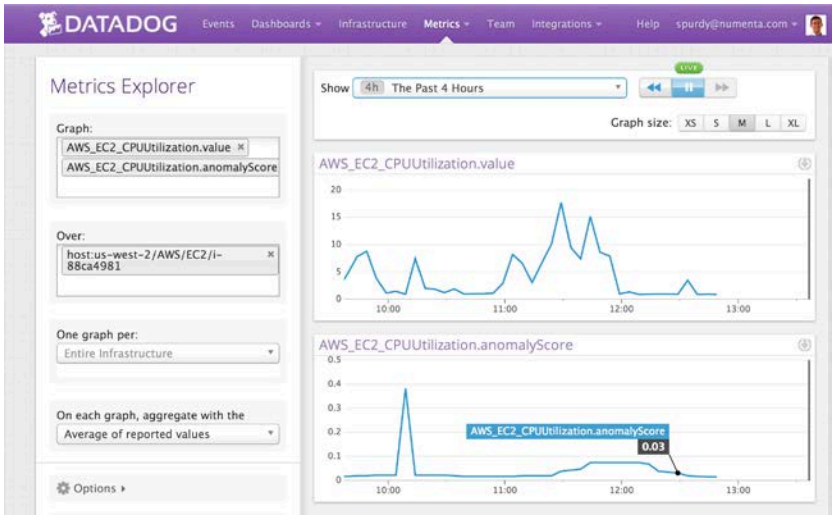
grok metrics list <Grok server URL> <Grok API key>

In order to see continuously updated information in DataDog, these commands should be run as a cron job. Due to DataDog requirements, this script should be run at least once every 3 hours. We recommend running it every 5 minutes – this will ensure that DataDog notifications have minimal latency. Sending data multiple times will not cause problems as long as you use average for the aggregation option in charts.

What you can do with this Integration

1. Visualization in DataDog

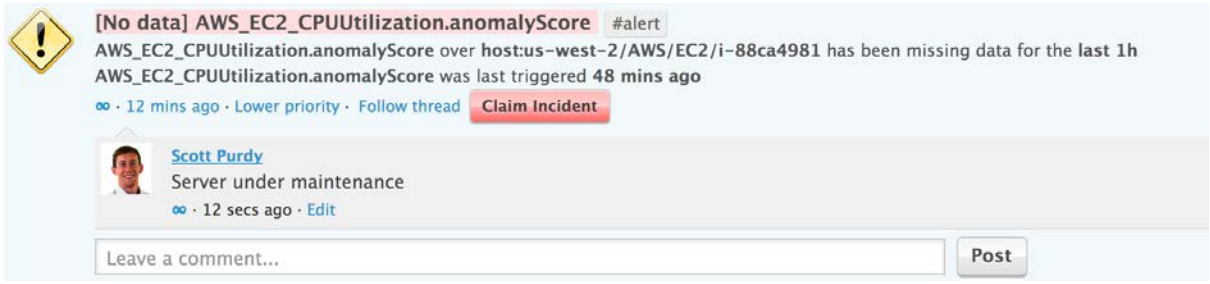
Below are some examples of Grok Anomaly scores being visualized in DataDog. In the screenshot below, we are using the **Metric Explorer View** with the **Average** function to aggregate.



You can use a similar procedure to visualize data in a DataDog Custom Dashboard.

2. Labeling Events

You can set thresholds to create an Event around a high Anomaly score. You should use a fixed threshold of Anomaly Score >= 0.5. Anomalies and other events such as servers being down can be labeled in DataDog



3. Grok Notifications in DataDog

Once you have anomaly scores in DataDog you can set up a threshold to create a DataDog event. You should use a fixed threshold of Anomaly Score >= 0.5 to re-create Grok anomalies exactly as they appear in the Grok mobile client. There is no need to change this threshold value.