splunk>

TECH BRIEF

ACCELERATE TIME TO INSIGHTS WITH METRICS AND SPLUNK

METRICS

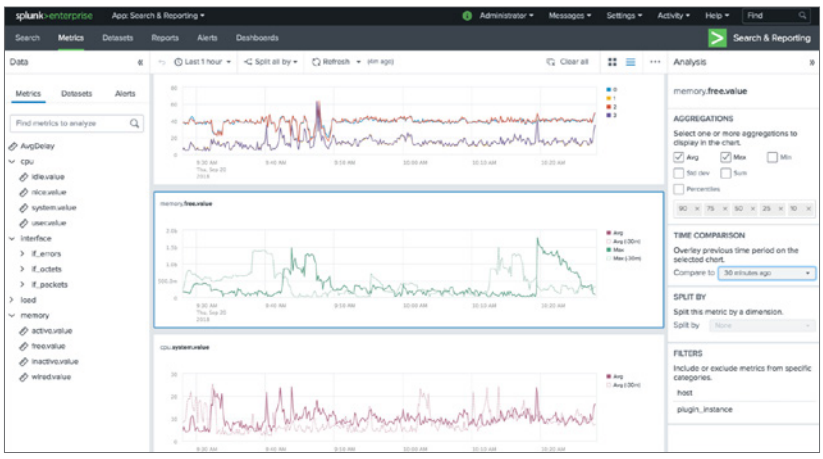
Breaking Down the Small Datatype With an Outsized Performance Boost

Metrics are numerical data points captured over time that can be compressed, stored, processed and retrieved far more efficiently than events. While metrics data can be found in many places, it can be a challenge to leverage effectively. With Splunk, you can easily correlate metrics data with other event data to be alerted to 'what' just happened (metrics), 'why' it happened (logs), and then act (fast).

The speed in which you're able to act can be a game changer for your organization. Using metrics as part of your data ingestion strategy can boost the speed of monitoring and alerting significantly.

Where can you find metrics data?

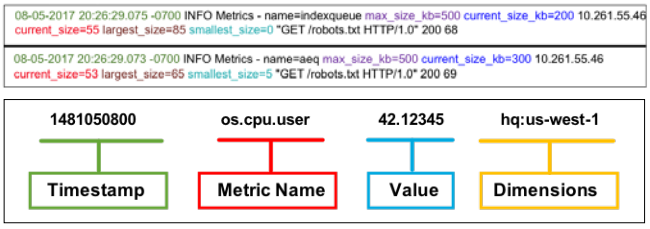
Metrics can come from servers, your applications, IoT sensors or just about any machine data-generating object containing numerical, time-series data points. Time-series data is produced at regular (and non-regular) time intervals. Common examples of metrics that you may be familiar with are system measurements like CPU, memory or disk space; infrastructure measurements from AWS CloudWatch; and measurements from IoT devices like temperature readings or GPS location (e.g. latitude-longitude pairs over time).



Screenshot of Metrics Workspace

How are metrics different than logs?

Metrics differ from log data in that they can be stored and optimized more efficiently for querying. They don't contain the rich information of a log, but they *do* present a specific measurement of a system over time. The structure of a metric consists of the following 4 elements: (1) timestamp, (2) metric name, (3) a measurement (a numerical data point), and (4) dimensions (which often describe where the metric is coming from or other descriptive attributes). While Splunk has always had the capability to store and query metrics data, its expression in a log format did not take advantage of metrics' compression, storage and processing advantages. Starting with Splunk Enterprise 7.0 and Splunk Cloud 7.0, Splunk now handles metrics in its native, lightweight format which directly contributes to providing 2000x performance increases over traditional log queries.



Log vs. Metric

METRICS AND SPLUNK

What You Can Do With Metrics in Splunk

In addition to the ability to natively ingest metrics data, Splunk has several capabilities that allow for easy configuration and analysis of metrics data. The **Metrics Workspace** is an interface within the Search and Reporting app that allows for the monitoring, analysis, and creation of alerts and dashboards on metrics data *without* using SPL. This GUI-based way to explore metrics enables the creation of sophisticated, metrics-focused alerts and dashboards.

After configuring your Splunk environment to ingest metrics effectively, you may want to consider converting logs to metrics in order to take advantage of metrics' inherent performance benefits and augment your ability to extract more rapid feedback from log data. With the aptly named **Logs to Metrics** feature, convert logs to metrics in a user interface to configure monitoring and alerting on these transformed metrics datasets. You can even configure and ingest multiple metrics from a single log.

SUCCESS METRICS

Unlocking Metrics Success

Freewire Technologies has used the Splunk Metrics Workspace and its interface to configure real-time monitoring of their customers' onsite battery systems for proactive maintenance.

"We chose Splunk to help us monitor and manage our mobile battery systems in the field. We receive metrics in real time which enable us to make faster decisions. Splunk Metrics Workspace - with its easy and intuitive interface - helps us discover and visualize patterns in these metrics. Now we can proactively maintain our battery systems on customer sites which enables us to improve the overall customer experience."

— David Lee, Technical Architect

FREEWIRE TECHNOLOGIES

MONITORING AND ALERTING PERFORMANCE INCREASED

200x
faster in Splunk 7.0
(as compared to Splunk 6.6)

2000x
faster in Splunk 7.1

USE METRICS IN YOUR DEPLOYMENT

Begin Using Metrics in Your Own Organization

For deeper instruction on metrics, see Splunk Docs where we breakdown how to begin ingesting metrics data from StatsD, collectd and other sources. It also includes step-by-step guides on how to convert logs to metrics and best practices for optimizing metrics to enhance the performance of your Splunk deployment.

Want some extra help? Contact our customer success managers to start accelerating your decision-making speed with metrics.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

TB-Splunk-Accelerate-Time-to-Insights-with-Metrics-101