**Use Grok\_Exporter for Translating Log Events in Log Files into Prometheus Metrics**

**Purpose**

Research how Spring Boot Actuator or Prometheus can be used to analyze log files.

**Technologies and Tools**

Spring Boot Actuator is a sub-project of the Spring Boot Framework. Spring Boot Actuator provides several features like health check-up, request traffic, auditing JVM metrics, log information, caching statics, database state etc. It provides HTTP end points to manage and monitor applications on the production environment. Actuator endpoints can display system metrics and application information in JSON format. Metrics can be exported in various formats so that different monitoring tools can retrieve and visualize them. Spring Boot Actuator has an end point named “loggers”, which provides access to the Spring Boot application’s loggers and the configuration of their levels. To access it, just type <http://host:port/actuator/loggers> in the URL address of a browser. However, it only provides overview information about the configured loggers and their logging levels. It lacks the capability for analyzing and displaying detailed logged events. It is also unable to aggregate logged events into metrics.

Prometheus is an open-source systems monitoring and alerting toolkit, and it collects and stores application metrics as time series data. Application metrics are numeric measurements about health, performance, and certain events about the application. For example, for a web server, it might be request times; for a database, it might be number of active connections or number of active queries etc. A Prometheus server can act as a central server that scrapes various application metrics from different web applications. All metrics can be queried by PromQL, the Prometheus query language that retrieves, filters, and aggregates metrics data. Prometheus provides user interface that user can access metrics information and dashboard through a browser.

Micrometer is a metrics library for Java-based applications that provides a simple and unified way to record and expose metrics to various monitoring systems, such as Prometheus, Graphite, and InfluxDB. With the help of Micrometer library, Spring Boot Actuator can generate metrics in the format that Prometheus understands, so metrics of a Spring Boot application can be monitored by Prometheus. Furthermore, Micrometer library provides API for developers to instrument application source code and generate custom metrics. However, Micrometer library does not have API to directly extract events from existing log files and generate event metrics.

Grok\_exporter is a tool that enables the parsing and transformation of unstructured log data into structured data that can be easily queried and analyzed using tools such as Elasticsearch and Prometheus. Grok Exporter is based on the Grok library, which provides a way to match text patterns and extract fields from log messages. Its configuration file specifies what log files it should process, the text patterns used for extracting log events, and the types and structures of generated metrics based on the extracted log events. Grok\_exporter can run as a server or service to constantly processing log files and translate useful log messages into metrics. Prometheus then can be configured to scraping the metrics generated by grok\_exporter to analyze and display the metrics.

**Use Case**

Suppose we have a log file named activity.log containing user log-in and log-out events.

Text

Description automatically generated

We want to constantly monitor and count how many times a user has logged in and logged out from the application. We can configure grok\_exporter to parse the activity.log by using regular expression patterns and construct a user\_activity\_metrics. The config\_activity\_log.yml is shown as below:

Graphical user interface, text, application

Description automatically generated

Then we start the grok\_exporter server by typing the following command:

grok\_exporter -config C:\Projects\LogGenerator\Config\config\_activity\_log.yml

To access the metrics generated by the grok\_exporter, type the URL <http://localhost:9144/user_activity_metrics> in a browser, then the browser should display the metrics like the below:

Text

Description automatically generated

To enable Prometheus server to scrape user\_activity\_metrics from grok\_exporter, we need to configure Prometheus in prometheus.yml:

Text

Description automatically generated

Then we start the Prometheus server by typing the following command:

prometheus --config.file=C:\Projects\LogGenerator\Config\prometheus.yml

To access Prometheus web user interface, type <http://localhost:9090> in the URL field of a browser. Then type “user\_activity” in the search field of the metrics form.

Click “Execute” button to display the user\_activity metrics in the table format:

Graphical user interface

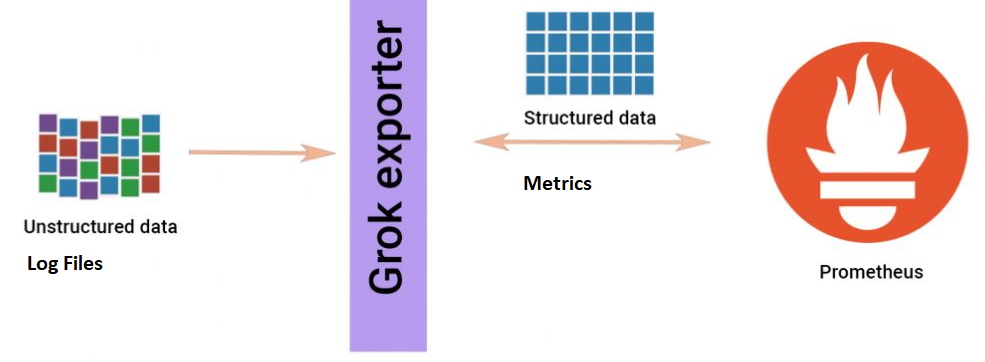
Description automatically generated with medium confidence

Click “Graph” link to visualize the metrics:

Chart, line chart

Description automatically generated

**Summary**



Grok\_exporter constantly parses log files by applying regular expression patterns and then constructs and emits metrics that Prometheus understands. Prometheus periodically scrapes and pulls the metrics for further displaying and analysis.

**Alternatives**

Loki and Grafana

**References**

Grok\_Exporter:

<https://github.com/fstab/grok_exporter>

Prometheus:

[Prometheus - Monitoring system & time series database](https://prometheus.io/)