

Collecting and Analyzing the Logs



Piotr Gaczkowski

IT CONSULTANT

@doomhammerng doomhammer.info



Overview



Visualizing and querying log information

**Looking for insights and debugging
application through logs**



Log Management



Statistics



User analytics



Compliance



Debugging



Insight into the system



Unified Logging Layer



Collects logs from different sources



Filters the logs



Translates the logs



Forwards logs to the appropriate location



Unified Logging Layer Tools

Logstash

Filebeat

Fluentd

Vector



Logstash



The former de facto standard

The “L” in ELK Stack (now Elastic Stack)

Resource intensive

Exotic configuration syntax

Filebeat



The new approach from Elastic

Dedicated to log collection

Lightweight



Fluentd



Cloud Native Computing Foundation
graduated project

Recommended by cloud providers

Numerous integrations



Vector



Focused on performance and correctness
Collects logs, metrics, and events
Still under development



Log Aggregation



Stores logs in a centralized place



Allows easy querying



Manages data retention



Integrates with alerting



Log Aggregation Tools

Elasticsearch

Loki



Elasticsearch



The “E” in ELK Stack (now Elastic Stack)

De facto standard for log aggregation

Great search engine

Numerous integrations

Loki



Focused on horizontal scalability and high availability

Inspired by Prometheus

Not yet as mature as Elasticsearch

Log Visualization



Helps with analyzing the logs



Allows creating visual dashboards



Simplifies querying



Log Visualization Tools

Kibana

Grafana (with Loki)



Kibana



The “K” in ELK Stack (now Elastic Stack)

Provides an additional query language on top of Elasticsearch

Focused on logs



Grafana



Pluggable backends (Prometheus, Graphite, InfluxDB, Loki)

Allows interactive graphs

Focused on time-series data

Integrated Solutions

Splunk

Datadog



Splunk



Software-as-a-Service

**Integrated solution for logs, metrics,
events, and performance data**

Operational Intelligence

Datadog



Software-as-a-Service

Integrated solution for logs, metrics, events, and performance data

Performance monitoring

Debugging with Logs

What is the high-level performance?

How did we end up in that state?

Is the problem localized to a single machine or pod?

When did the problem start?

How often do we see the problem?

Is it correlated to other events?



Demo



Deploy Elastic Stack

Point Fluentd to Elastic Stack

Use the Carved Rock Fitness application

Analyze the results



Summary



There are several solutions for log collection and analysis

Choose the one that fits your needs

Unified approach to logging helps with log management

