Instrumenting Linux Servers

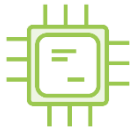
JP Toto
INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

Beats for Linux

Metricbeat

RAM



CPU

Disk

Filebeat

Filebeat

Built for consuming and shipping text-based logs and data

Outputs to Elasticsearch or Logstash

Most Linux logs are text-based so it's a good fit for monitoring

Demo

Download, install, and configure Filebeat

Setup Filebeat to read syslog files and forward to Logstash

Add a filter configuration to Logstash for syslog

Demo

Verify data is arriving in Elasticsearch from Filebeat

Setup first Linux dashboard

Summary

Instrumented our first “client” Linux server with Filebeat and Metricbeat

Added complex filtering to Logstash and setup a Kibana dashboard for Linux

Next: Packetbeat