ELK: Data Visualization

David Soller

OSU OSC – 10/24/2016

What is the ELK or Elastic Stack?

- It’s a combination of the open source projects:
  -  Elasticsearch - github.com/elastic/elasticsearch/
  -  Logstash - github.com/elastic/logstash/
  -  Kibana – github.com/elastic/kibana/
  - Docs at - elastic.co/guide/index.html

How do they interact?

Data Parser & Shipper

Database

Data Viewer

Logstash

- Written in Ruby
- Run on JRuby
- Plugin architecture to create .conf files
- “The Lumbering Beast”

Elasticsearch

- Written in Java
- NoSQL
- Search Optimized (a nice interface for Apache Lucene)
- Web API, Sharding and Distribution
- “The Perfect Person”

Kibana

- Written in JavaScript
- Angular & Node.js
- Visualize what's going on in your Elasticsearch data
- "The Problem Child"

Demo 1 – Basic Data Input

- Goals:
  - Walk through the stack
  - Show data input & visualization

Demo 2 – CSV Data

- Goals:
  - Read in a dataset from a .csv file
  - Create a basic dashboard

What sucks about using the stack?

- Security! – Pay to keep your data safe :’(
- Kibana is getting better but…
  - There are major parts of Elasticsearch not supported
    - Nested Objects:

Replacements

No Logstash?
Try: Heka or Hindsight

- Heka (DEPRICATED):
  - github.com/mozilla-services/heka
  - By Mozilla
  - Written in Go & Lua
  - Performance
- Hindsight:
  - github.com/mozilla-services/hindsight
  - By Mozilla
  - Written in C & Lua
  - Performance

No Kibana?
Try: Grafana

- Grafana:
  - github.com/grafana/grafana
  - Supports multiple visualization platforms
  - Written in Go & TypeScript

Thanks!

:D