

A gentle introduction into Elasticsearch

Jurgens du Toit

jrgns

EagerELK

What is it?



elasticsearch.

distributed restful search and analytics



elastic

Use cases

Search

Time Series Analysis

Application Database

Elasticsearch as a Service

- Found.no (Official)
- QBox
- Bonsai
- ???



Installation

- Java is Required
- Official Elastic repositories
- Download
- Ansible
- Ready made VMs

Architecture



Configuration

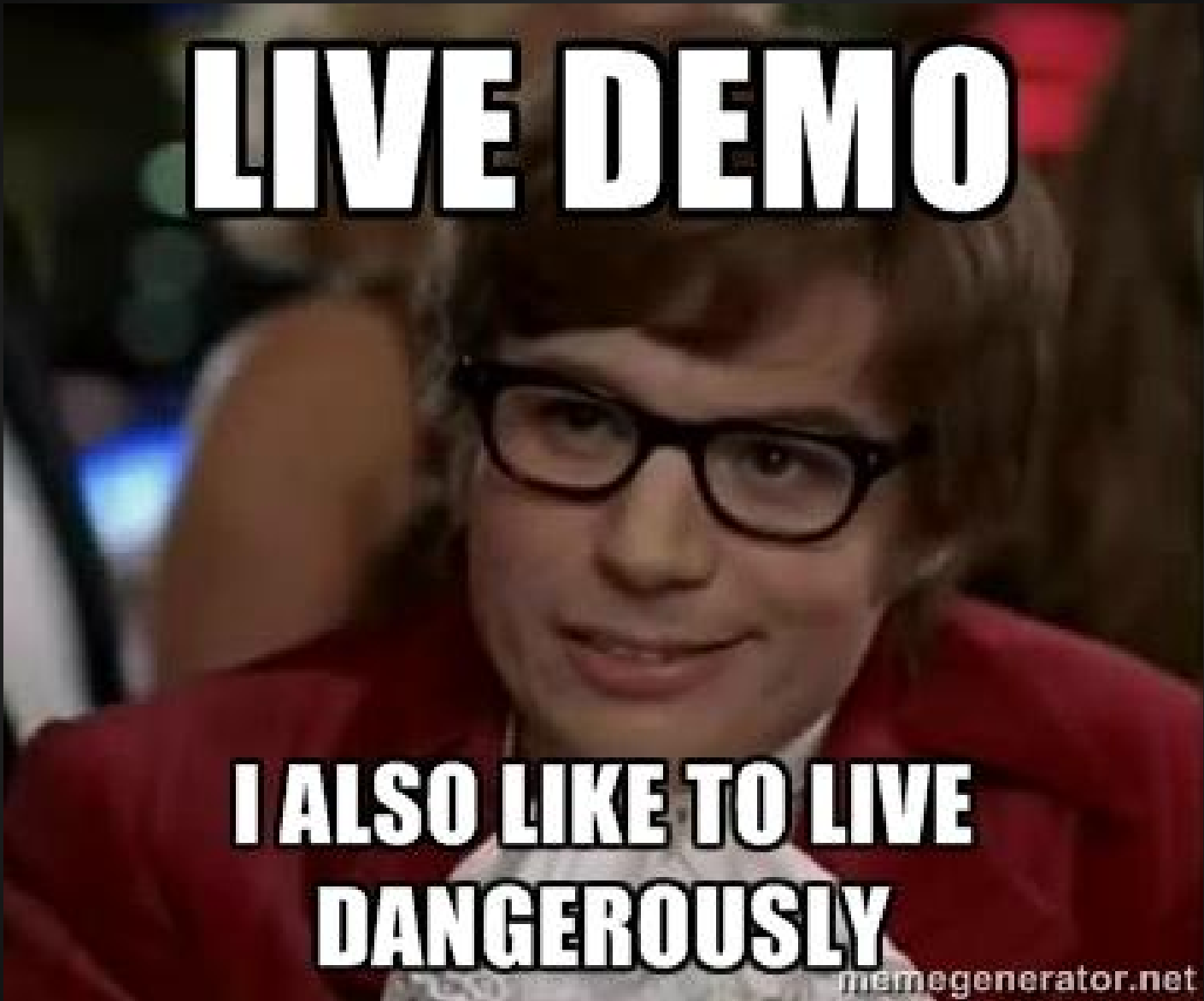
- **`/etc/default/elasticsearch`**
 - `ES_HEAP_SIZE`
 - `DATA_DIR`
 - `LOG_DIR`
 - `CONF_FILE`
- **`/etc/elasticsearch/elasticsearch.yml`**
 - `cluster.name`
 - `node.name`
 - `data / client / master`
 - `shards / replicas`
 - `network.bind_host`
 - `CORS`
 - And many more...

Plugins

- Shield
- Watcher
- Marvel
- Head
- And many more

Features

- Search
- Filters
- Aggregations
- Routing
- Percolators
- Parent / Child
- Versioning

A close-up of a man with curly brown hair and black-rimmed glasses, wearing a red blazer. He is looking slightly to the right with a faint, knowing smile. The background is blurred, showing other people and lights, suggesting a crowded event or conference.

LIVE DEMO

**I ALSO LIKE TO LIVE
DANGEROUSLY**

memegenerator.net

Resources

- **Reference Guide**

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

- **The Definitive Guide**

<https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html>

- **Resiliency Status**

<https://www.elastic.co/guide/en/elasticsearch/resiliency/current/index.html>

Questions?