Moar Logs:
Logging on Linux using the ELK Stack

Jurgens du Toit

jrgns

EagerELK

What is it?

elastic

elasticsearch.
distributed restful search and analytics

kibana

Use cases

Search

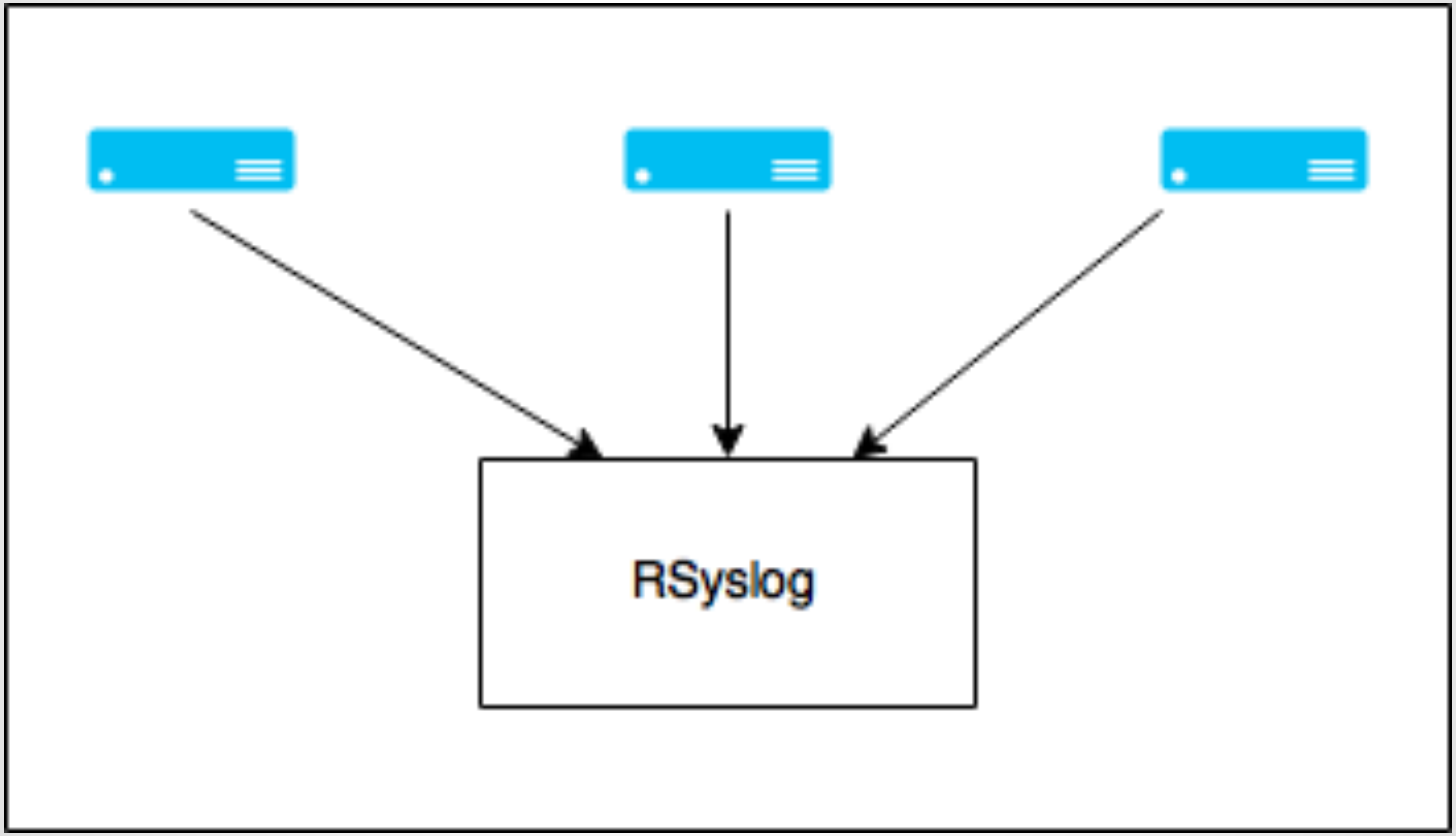
Time Series & Log Analysis

Application Database

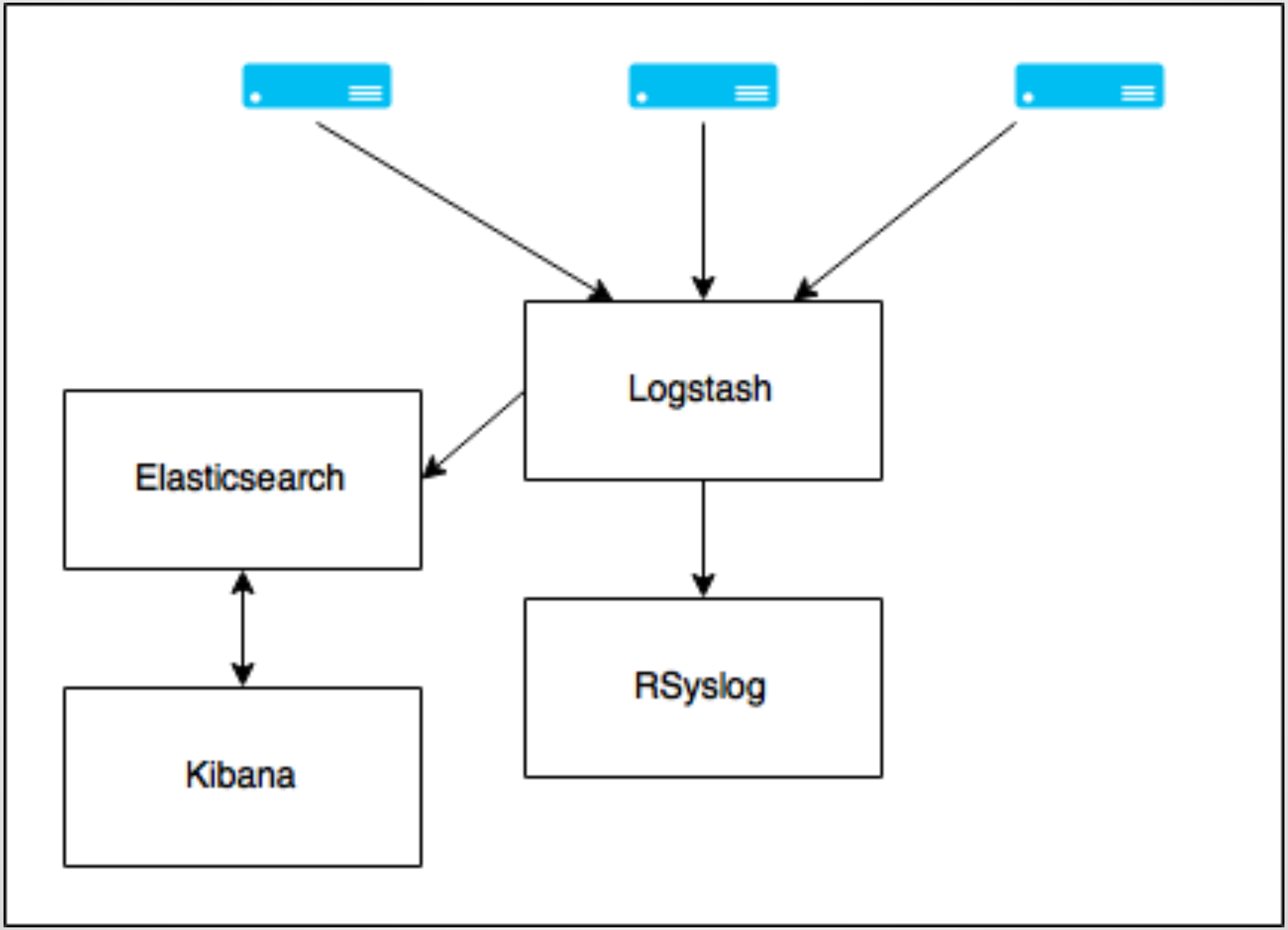
Installation

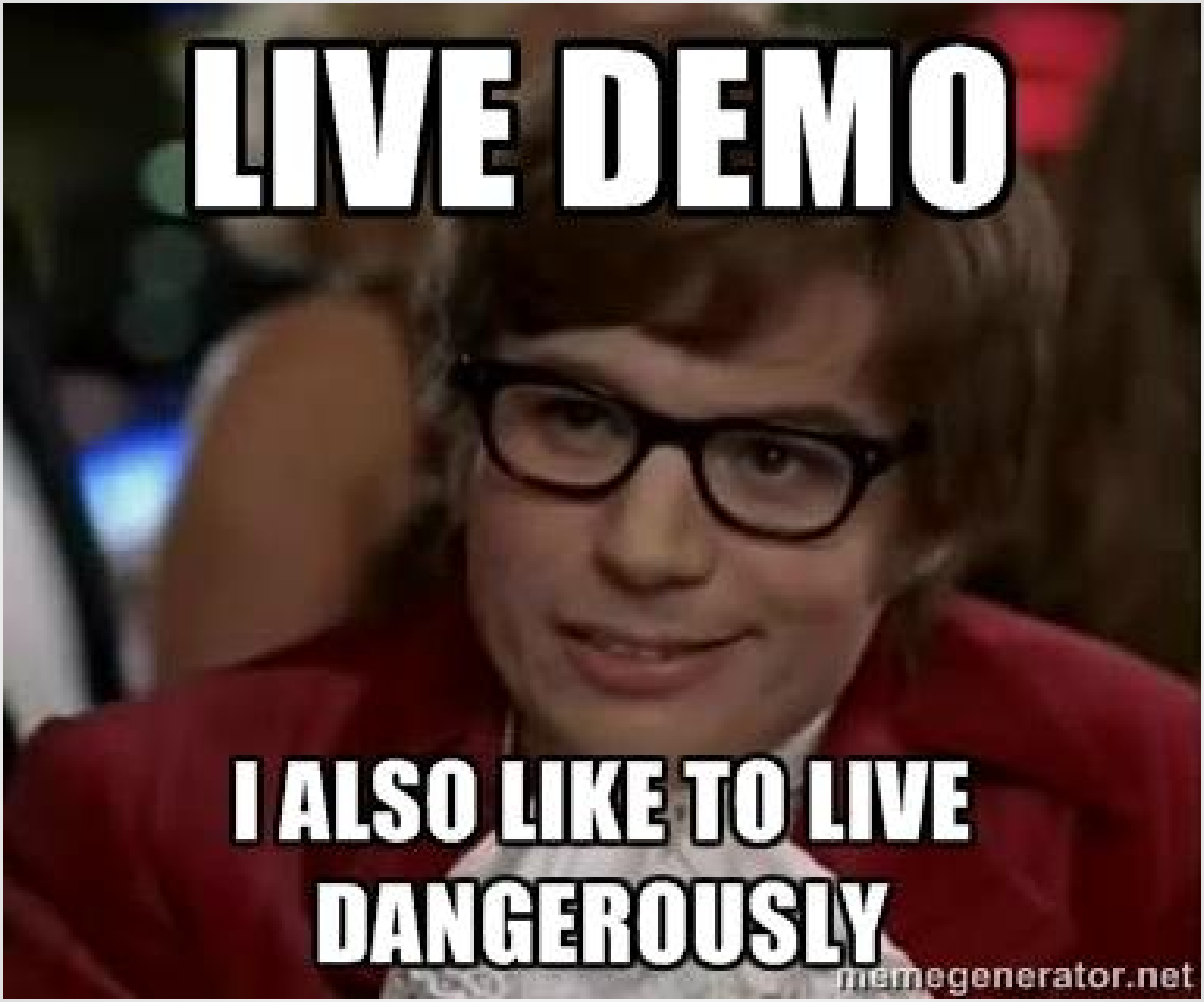
- Java is Required
- Official Elastic repositories
- Download
- Ansible
- Ready made VMs

Setup



Setup




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?