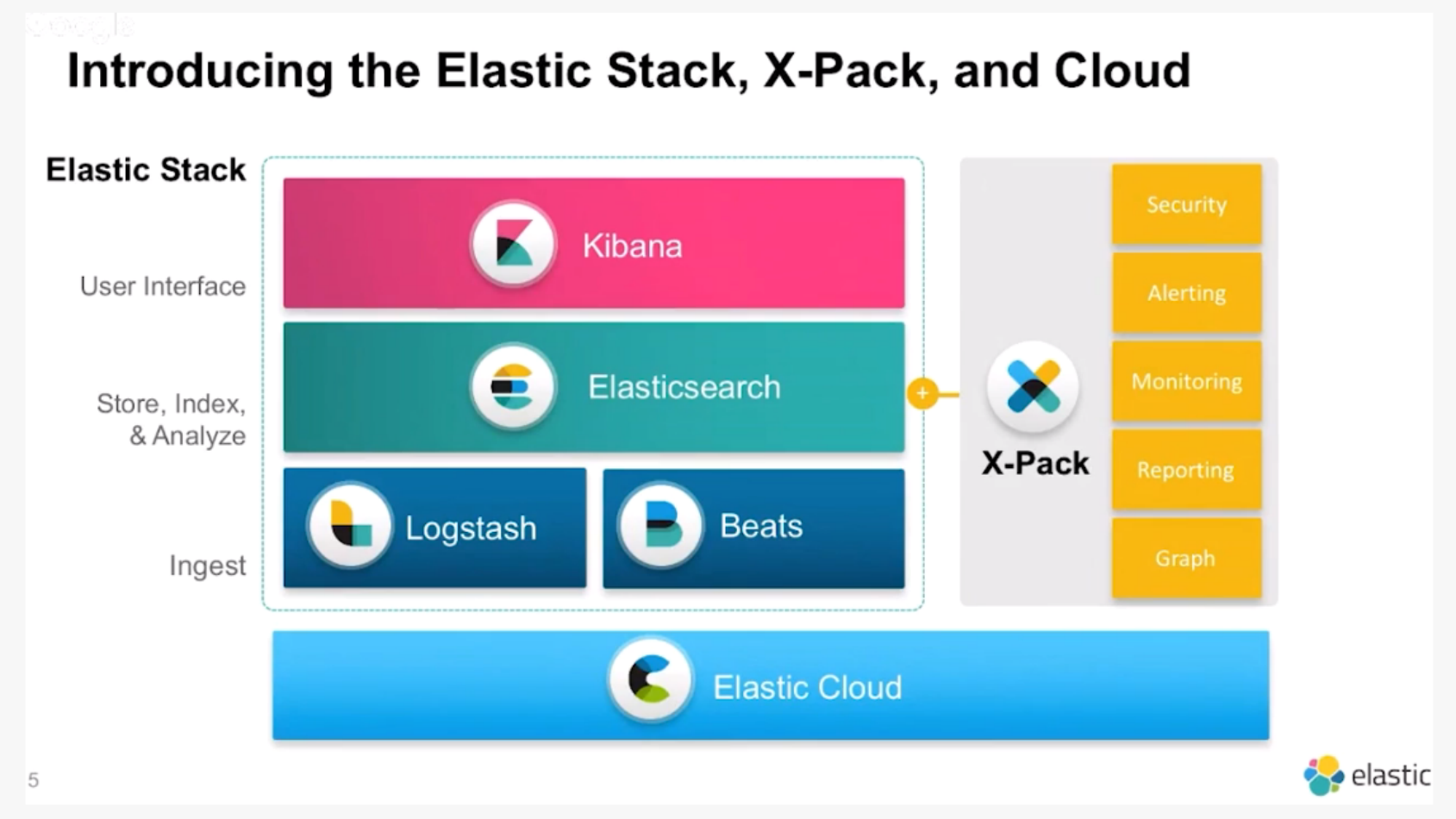
Análise de Logs de Apache com Elastic Stack

Ricardo Santos @ CERT-MZ TechTalk
ricardo@cert.mz - facebook.com/cert-mz - www.cert.mz

Elastic Stack



Elastic Stack: O quê?

- Storage Distribuído & Plataforma de Pesquisa de Informação
  - Motor de Pesquisa / Agregações
  - Sugestões / geo / highlithing
  - Armazenamento de documentos
  - Alta Disponibilidade
  - Pesquisa em (quase) tempo real
- Open Source
  - Licença Apache
  - Alguns plugins proprietários: Segurança, alarmística, machine learning
- corre em Java

Elastic Stack: Porquê?

- API muito simples
- Rapidez de pesquisa
- Muito versátil:
  - Análise de Logs
  - Análise de Eventos
  - Pesquisa de texto (com requintes bastante interessantes)
  - Agregações de informação
  - Visualização de Dados muito apelativa
  - Usado pelo Wikipedia, Netflix, Github.

Elastic Stack: Estrutura

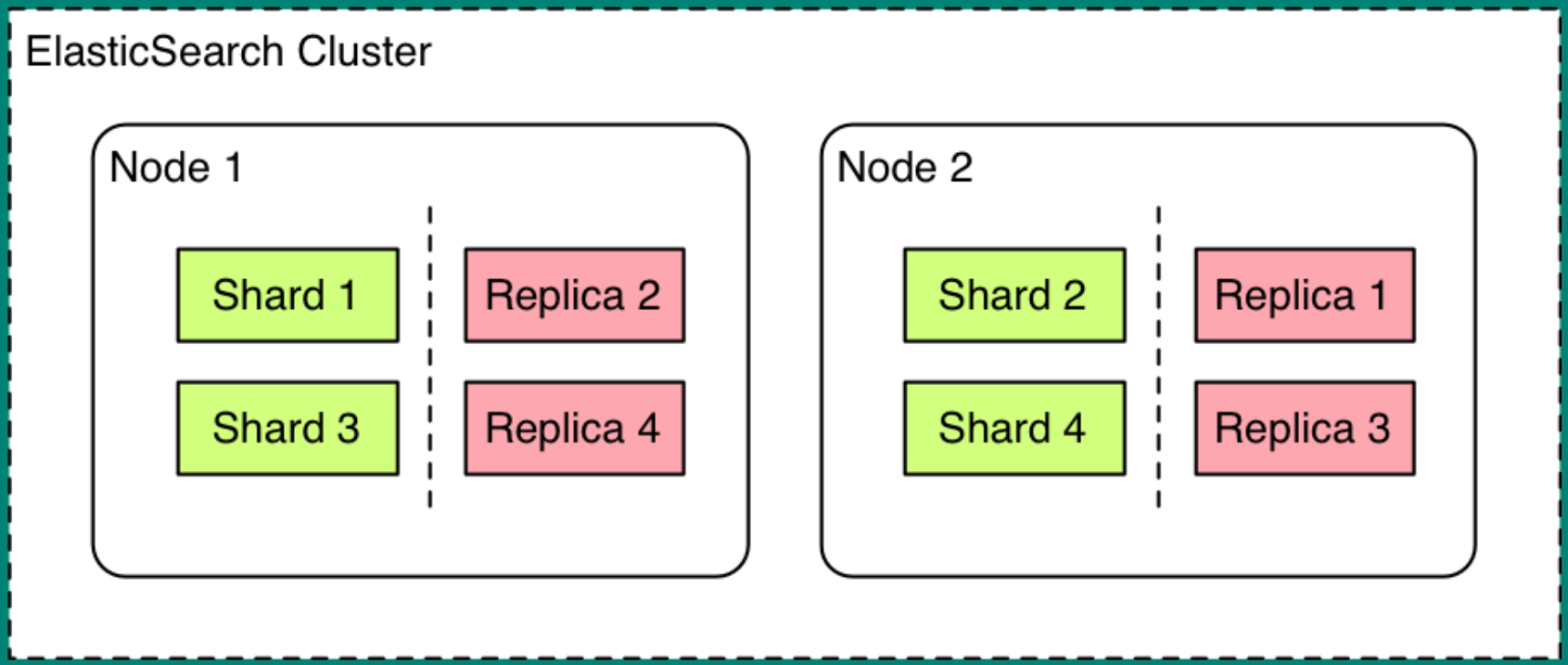
- Baseado em Apache Lucene
- Cada unidade de informação é um **documento**
- ... que existem em **índices**
- ... que são particionados por **shards**
- ... que são distribuídos pelos vários **nodes**
- ... que foram um **cluster**
- Documentos são objectos JSON

```
{ "name":"John", "age":30, "cars":[ "Ford", "BMW", "Fiat" ] }
```

Elastic Stack: Como escalar?

- Verticalmente:
  - Numa única máquina
  - Mais memória
  - Discos mais rápidos (SSD)
  - Tem limitações
- Horizontalmente
  - Scale out
  - Mais máquinas (nós) - escala linearmente
  - Processamento distribuído automaticamente
  - Permite um crescimento à medida das necessidades

Elastic Stack: Arquitectura



Análise de Logs Apache

Elastic Stack

Data Collection

Data Aggregation & Processing

Indexing & storage

Analysis & visualization

Ler o Log do Apache - Filebeat

`filebeat modules enable apache2`

indicar onde estão os logs (modules.d/apache2.yml)

`filebeat setup -e`

`filebeat`

```
./filebeat -e --modules=apache2 --setup
     -M "apache2.access.var.paths=
           [/vms/es-cert-mz/apache_logs*]
```

Visualizar o Dashboard

http://localhost:5601/app/kibana#/dashboards

QUESTÕES?!?!