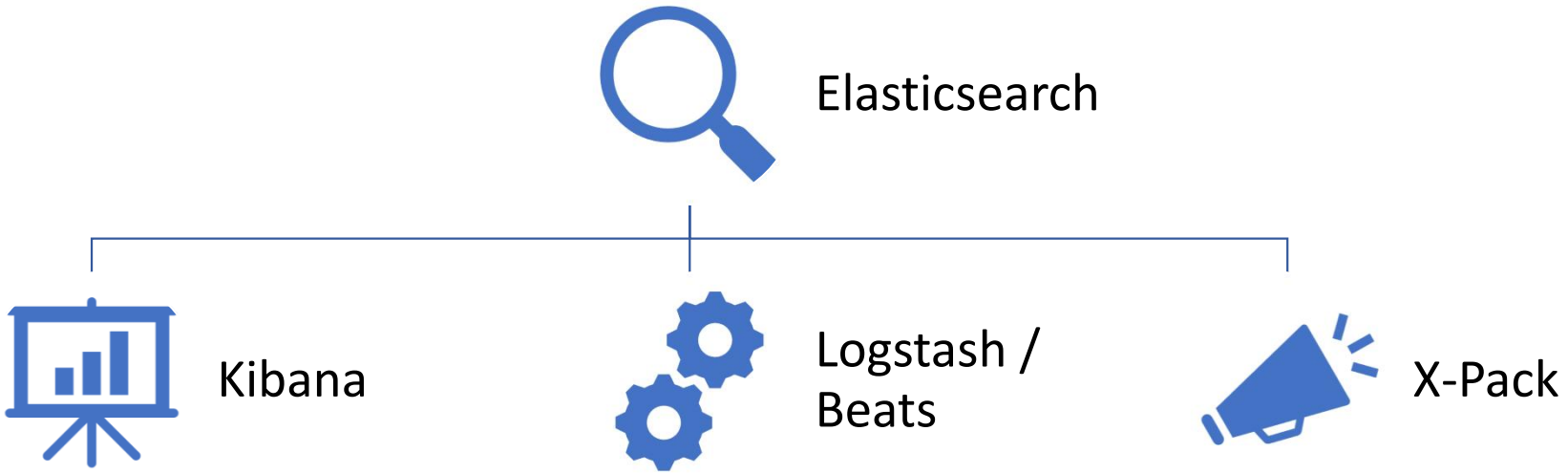
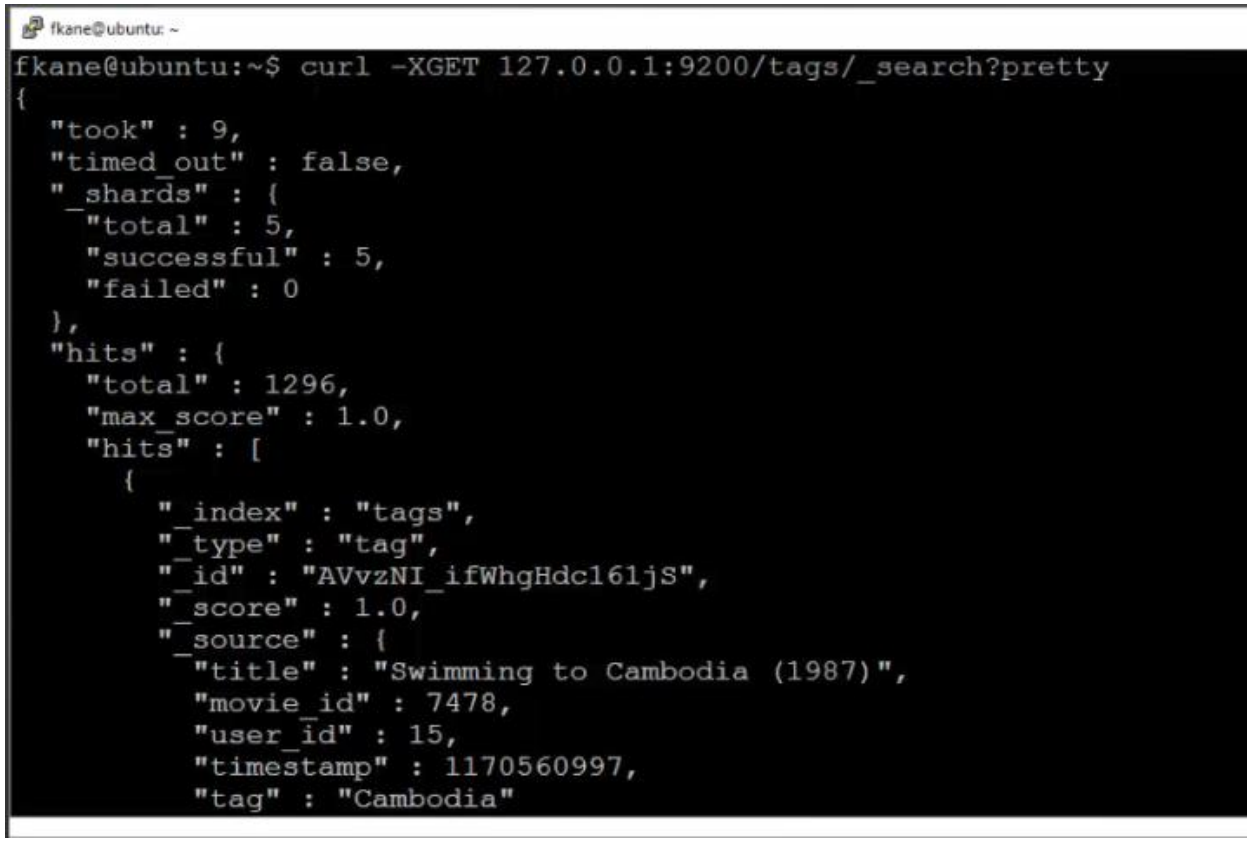
Elastic Stack



Sundog Education
Coralogix
PROF. FERNANDO AMARAL

Elasticsearch

- Versão escalável do Lucene
- Mecanismo de busca escalável horizontalmente
- Cada Shard é um índice invertido de documentos
- Além de busca:
  - Suporta dados estruturados
  - Pode agregar dados rapidamente
  - Normalmente uma solução mais rápida que Hadoop/Spark/Flink



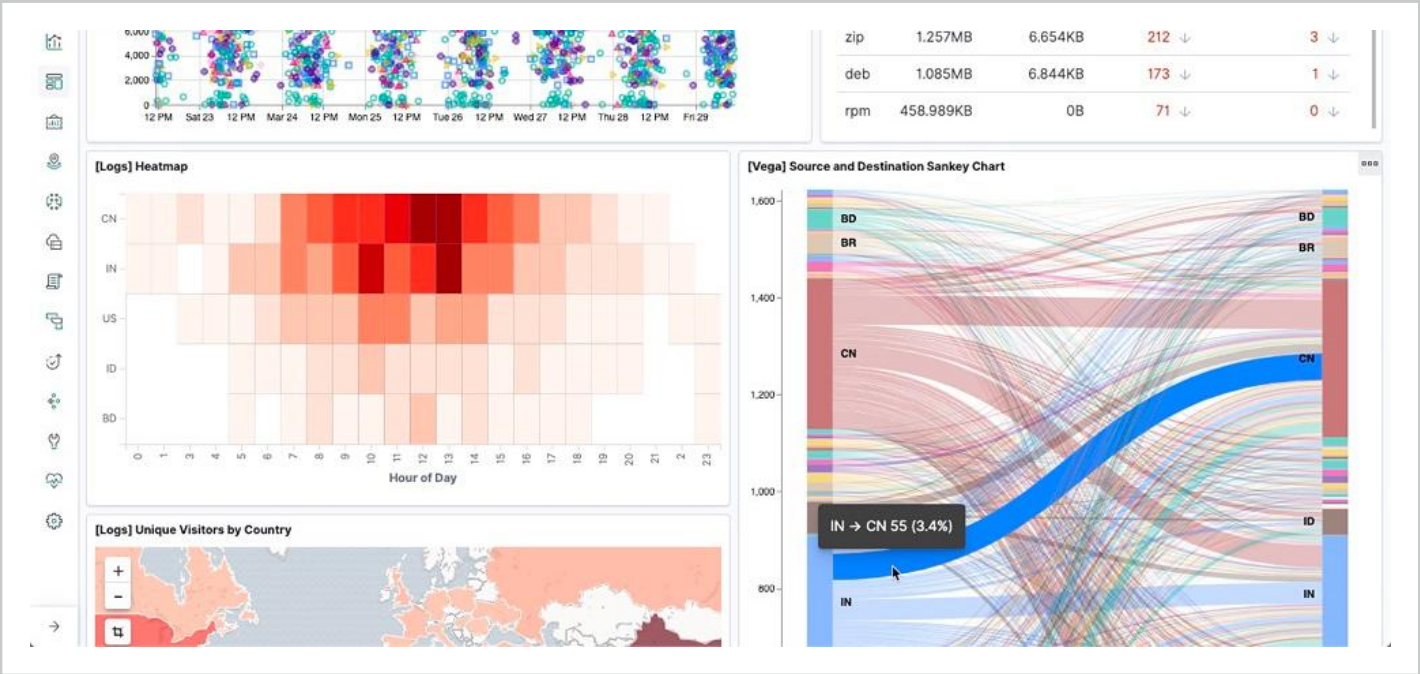
Elasticsearch

Kibana

Interface Web para busca e visualização

Agregações complexas, grafos, gráficos, dashboards

Muito utilizado para análise de logs



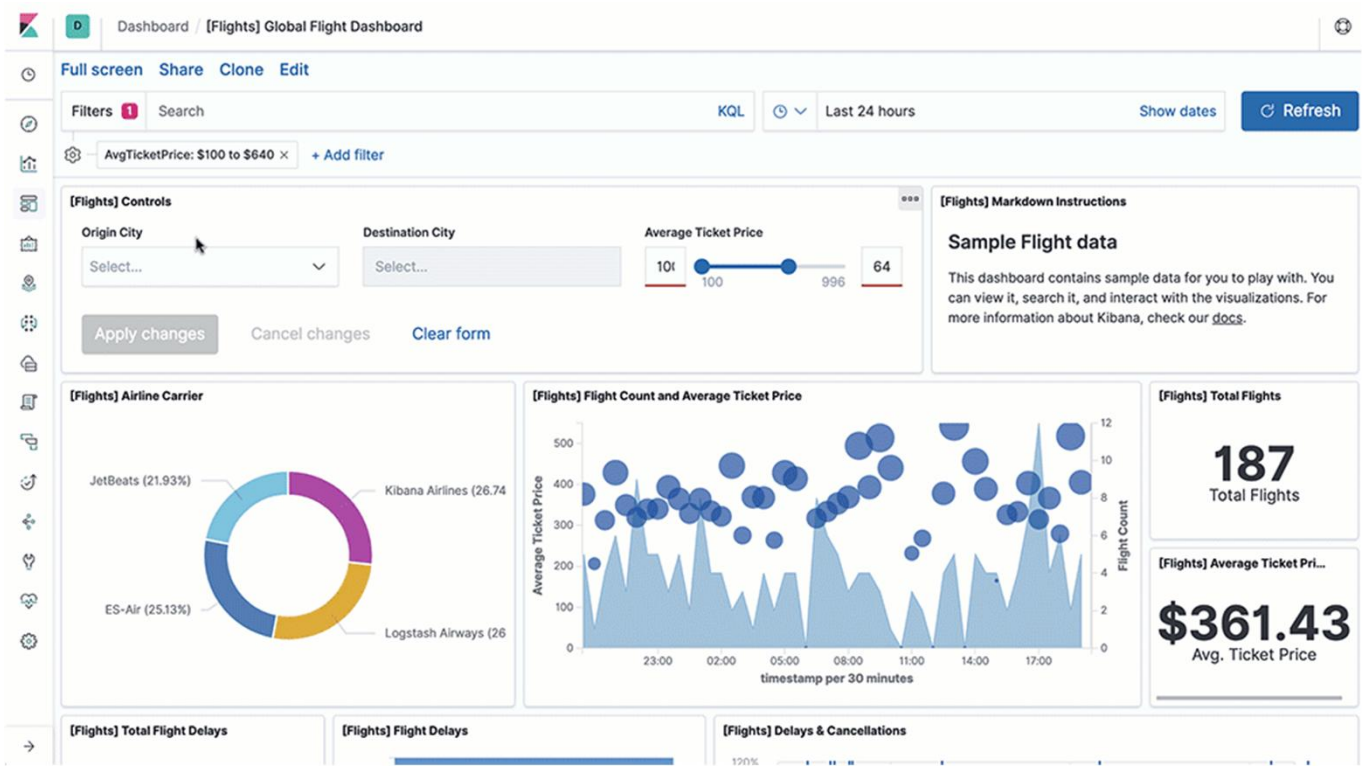
Kibana

Sundog Education

Coralogix

PROF. FERNANDO AMARAL

Kibana



Sundog Education

Coralogix

PROF. FERNANDO AMARAL

Logstash /Beats

Ingestão de dados no Elasticsearch

Filebeat pode monitorar arquivos de Log, analisar e importar para o Elasticsearch near-real-time

Logstash pode importar dados de vários computadores

Não são usados apenas para dados de log

Sundog Education

Coralogix

PROF. FERNANDO AMARAL

X-Pack

- Segurança
- Alertas
- Monitoramento
- Relatórios
- Machine Learning
- Grafos