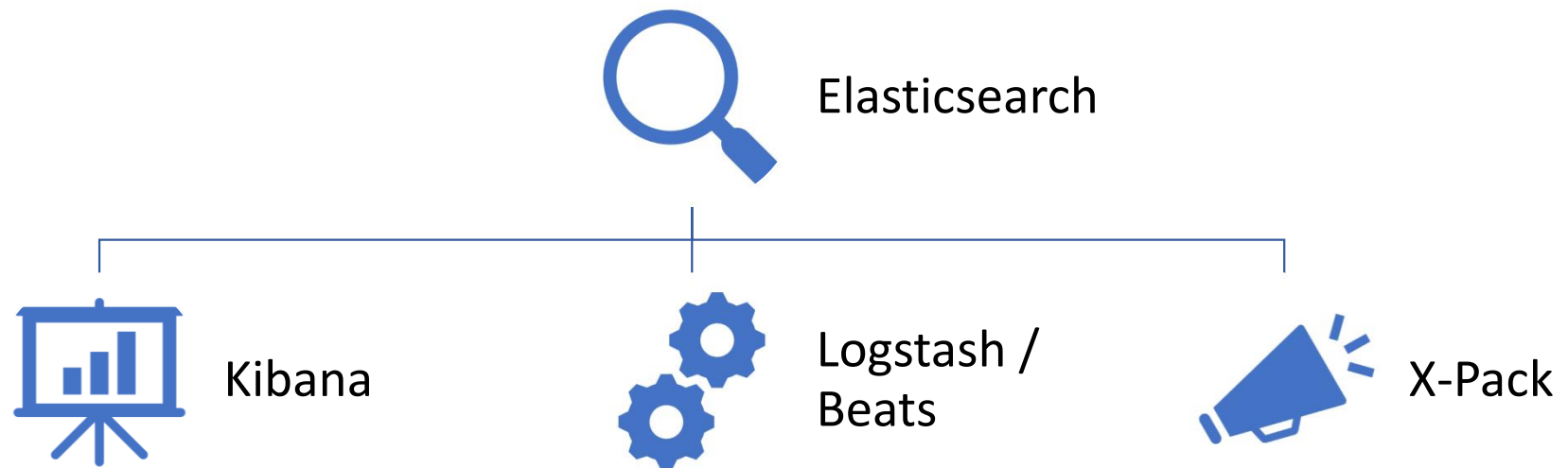
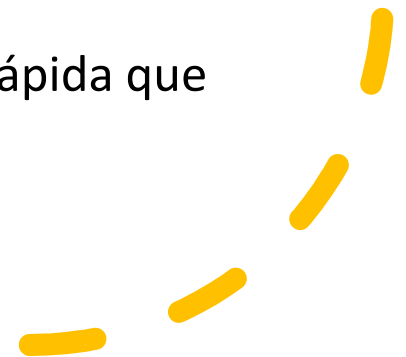


Elastic Stack



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

```
fkane@ubuntu: ~  
fkane@ubuntu:~$ curl -XGET 127.0.0.1:9200/tags/_search?pretty  
{  
  "took" : 9,  
  "timed_out" : false,  
  "shards" : {  
    "total" : 5,  
    "successful" : 5,  
    "failed" : 0  
  },  
  "hits" : {  
    "total" : 1296,  
    "max_score" : 1.0,  
    "hits" : [  
      {  
        "_index" : "tags",  
        "_type" : "tag",  
        "_id" : "AVvzNI_ifWhgHdc161jS",  
        "_score" : 1.0,  
        "_source" : {  
          "title" : "Swimming to Cambodia (1987)",  
          "movie_id" : 7478,  
          "user_id" : 15,  
          "timestamp" : 1170560997,  
          "tag" : "Cambodia"  
        }  
      }  
    ]  
  }  
}
```

Kibana



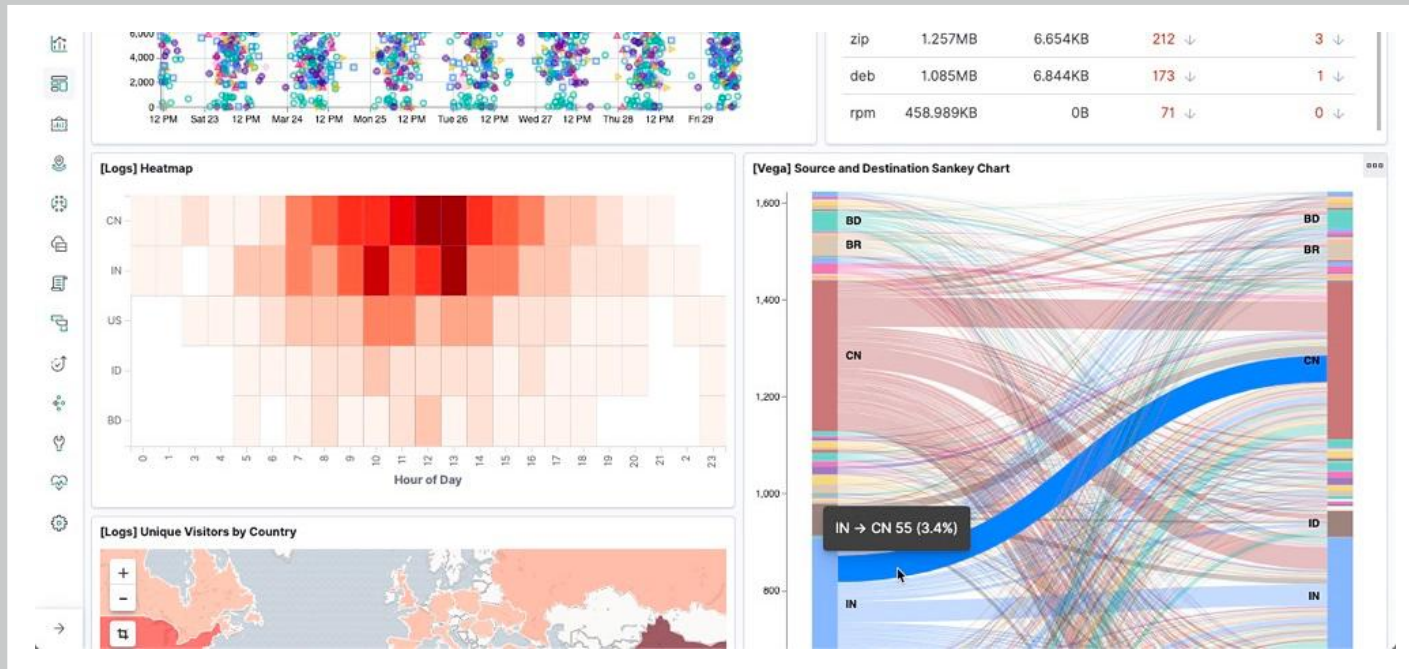
Interface Web para busca e visualização



Agregações complexas, grafos, gráficos, dashboards

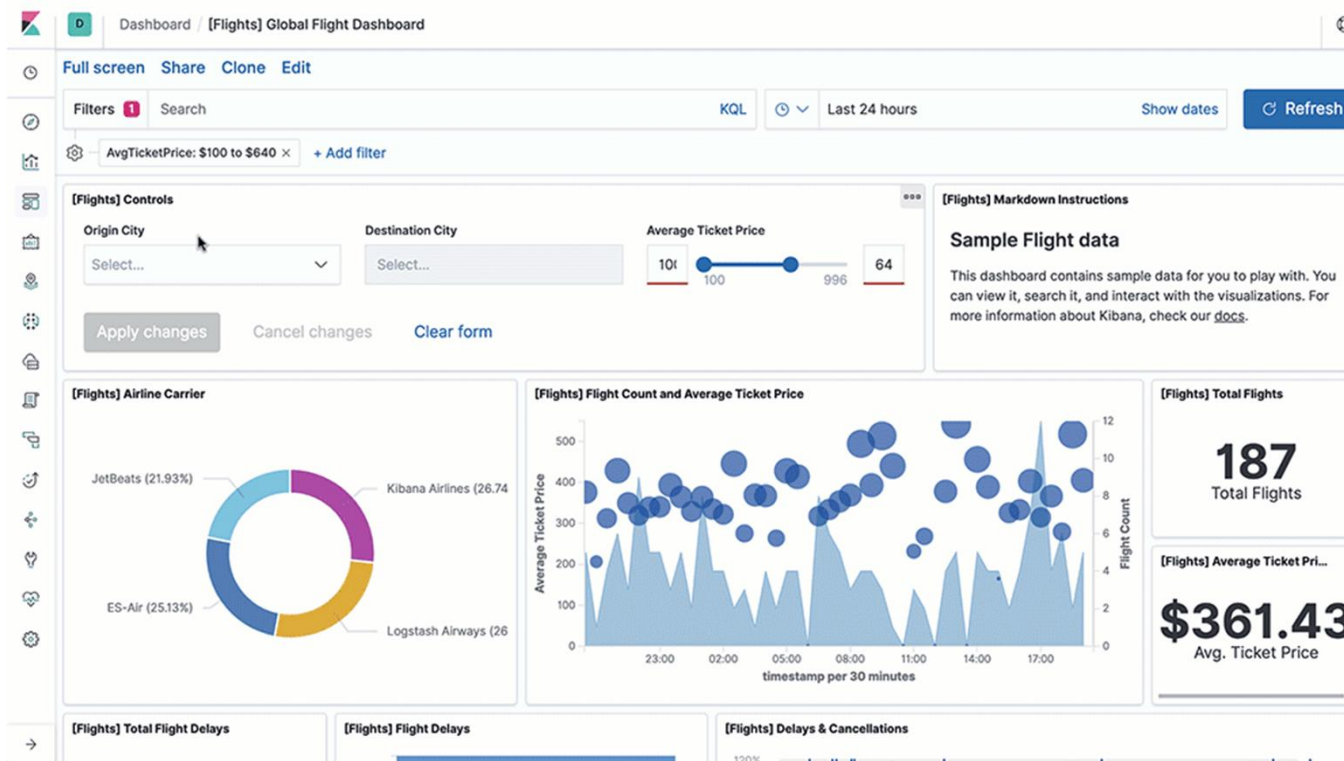


Muito utilizado para análise de logs



Kibana

Kibana



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

X-Pack

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

