# Elasticsearch

# Content

- What is Elasticsearch?
- What is Kibana?
- What is the Elastic stack?
- History of the Elastic Stack
- Why Elasticsearch?
- Key concepts of Elasticsearch
- Use cases of Elasticsearch
- Companies using Elasticsearch
- Queries
- Differences between Relational Database and Elasticsearch
- How to get started with Elasticsearch?

# What is Elasticsearch?


- Real-time distributed and open source full-text search and analytics engine
- developed in Java
- Based on the Lucene search engine
- Interaction through RESTful API
- uses schema less JSON documents to store data

# What is Kibana?

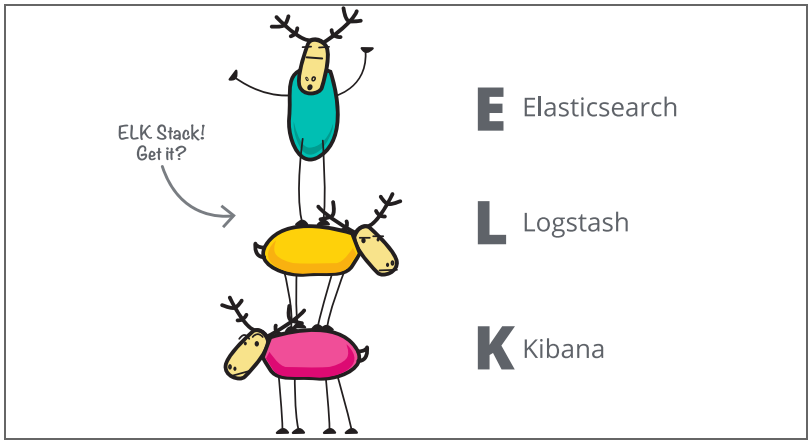

- open source browser visualisation tool
- to visualize large amounts of data

# What is the Elastic stack?


- combination of the open source projects Elasticsearch, Logstash, Kibana and Beats

# History of the Elastic Stack

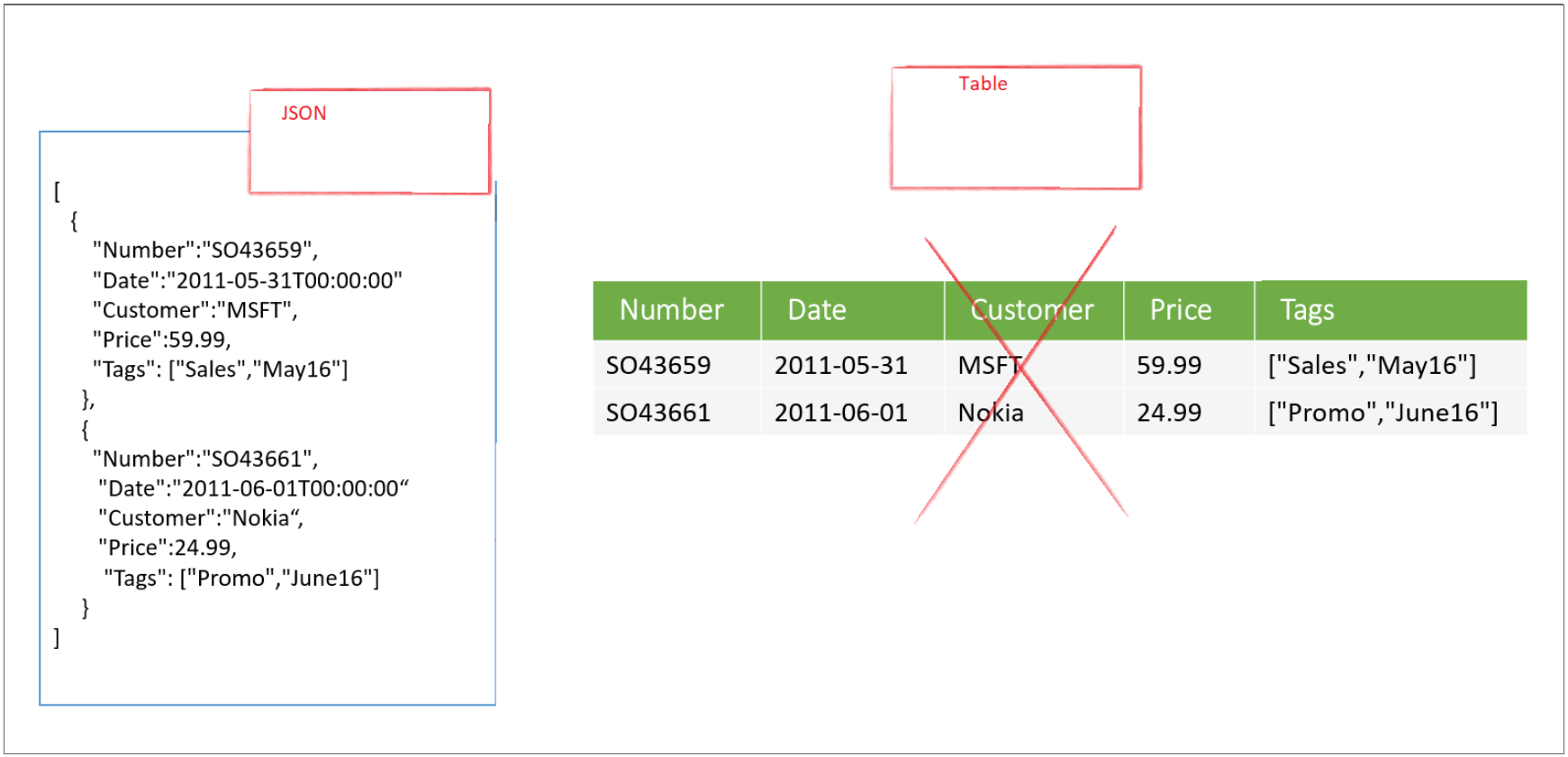
1. Elasticsearch developed as RESTful open source serach engine
2. Due to Elasticsearch being used more and more for log data, ingesting data and visualizing it became important so Logstash and Kibana were developed.
3. Beats added due to user suggestion



# Why Elasticsearch?

- compatible to run on every platform due to the development in java
- real time: newly added documents are directly searchable
- Handles multi-tenancy easily
- Scalability
- Performance
- Multilingual
- Document oriented -> json is easy to integrate
- autocompletion & instant search

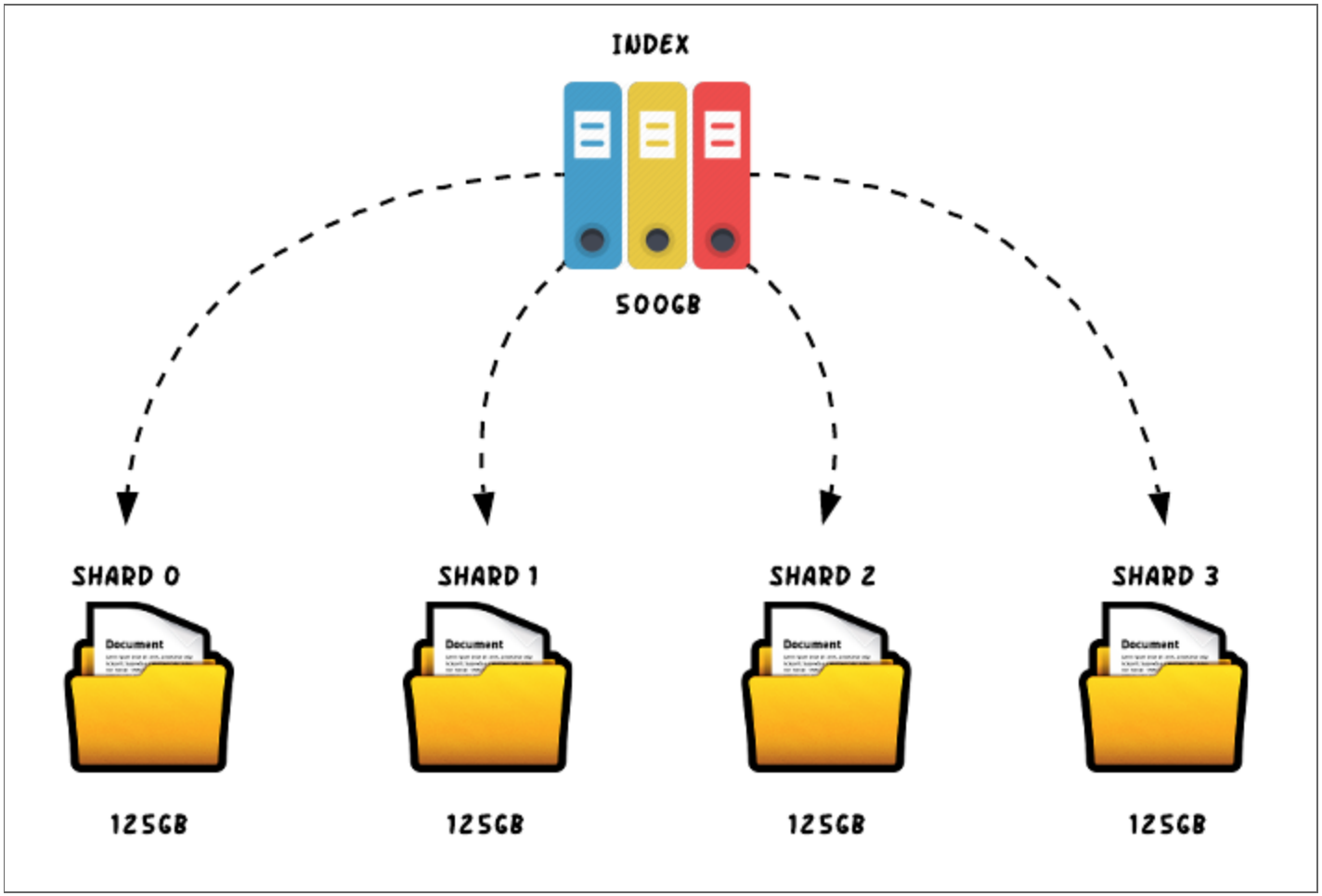
# Key concepts of Elasticsearch



# Key concepts of Elasticsearch

- Document
- Index
- Shards
- Cluster
- Replica shards
- Node
- Type
- Mapping

# Index and shards



## Use cases of Elasticsearch

- Full-text search
- Logging and Log Analysis
- Data visualization
- Scarping and combining public data
- Event data and metrics

# Elasticsearch Users

## Companies using Elasticsearch

- Airbus (Elasticsearch For Real-Time Access to Aircraft Technical Documents)
- Netflix (integrated into their messaging platform that delivers messages to customers)
- slack (Monitor for malicious activity)

## Alternatives to Elasticsearch

- Apache Solr (open source based on Lucene)
    - queries can return in JSON, XML and CSV
    - Scalable only with help of SolrCloud
    - focused on text-based searching

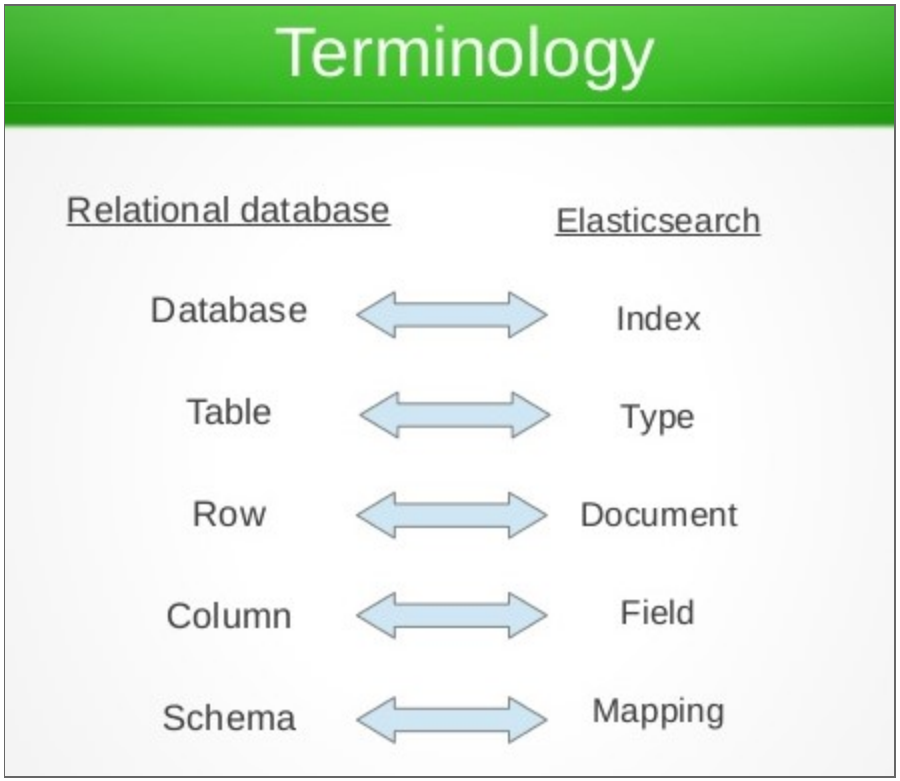
# Queries

- Elasticsearch Query DSL
- Match All Query : "query": {

```
"match_all": { }
```

- Full-text queries: Match, multi_match

# Differences between Relational Database and Elasticsearch



## Solution Using Relational Database Query

select * from product where name like '%Red%' or name like '%Shirt%';

```
name        | id
------------+----
Shirt       |  1
Red Shirt   |  2
```

- Elasticsearch Solution

```
POST test/product/_search
{       "query": {
          "match": {
            "name": "Red Shirt"   } } }
```

# Conclusion

```
"hits": [
  {
     "_index": "test",
     "_type": "product",
     "_id": "AVzglFomaus3G2tXc6sB",
     "_score": 1.2422675,              ===> Notice this
     "_source": {
        "id": 2,
        "name": "Red Shirt"
     }
  },
  {
     "_index": "test",
     "_type": "product",
     "_id": "AVzglD12aus3G2tXc6sA",
     "_score": 0.25427115,             ===> Notice this
     "_source": {
        "id": 1,
        "name": "Shirt"
     }
  }
```

```
]
```

- The differences will be in the result where Relational Database will return results in some random order while Elasticsearch returns results in decreasing order of _score which is calculated on the basis of relevancy.

# How to get started with Elasticsearch?

- Is the Elasticsearch Alive?
- you can access it at **http://localhost:9200** on your web browser, which returns this:


```
{
  "name" : "53c0837774f8",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "5__fv9BzSuSaGMB51gDS5Q",
  "version" : {
    "number" : "7.15.0",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "79d65f6e357953a5b3cbcc5e2c7c21073d89aa29",
    "build_date" : "2021-09-16T03:05:29.143308416Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

## Elasticsearch

- Elasticsearch hides the complexities behind a REST API POST (create) GET (read) PUT (update) DELETE (delete)
- and curl can work fine as the following example:
- `curl –X PUT http://localhost:9200/newindex`

Thank you for your attention