# • kibana

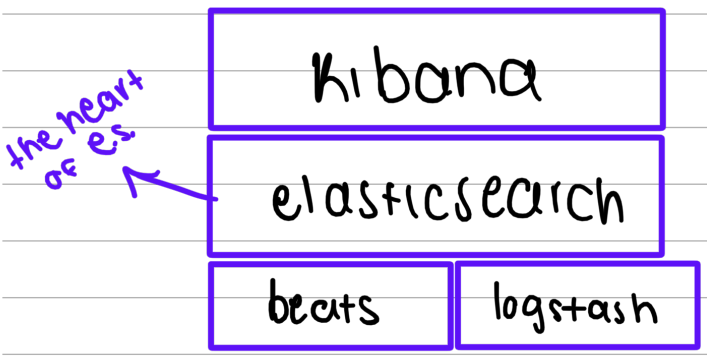
- UI to analyze elasticsearch data

## ¿ What can I do ?

- visualizations → build dashboards (dynamic)
- create users, roles, privileges
- exporting and share data
- set Alerts

* requires elasticsearch cluster

* It's easier to run the elastic cloud instead of installing it on our machine.




elastic Stack ↓ take data from any source in any format. search, analyze and visualize

## ◦ Use cases

- logging
- metrics
- security analytics
- business analytics

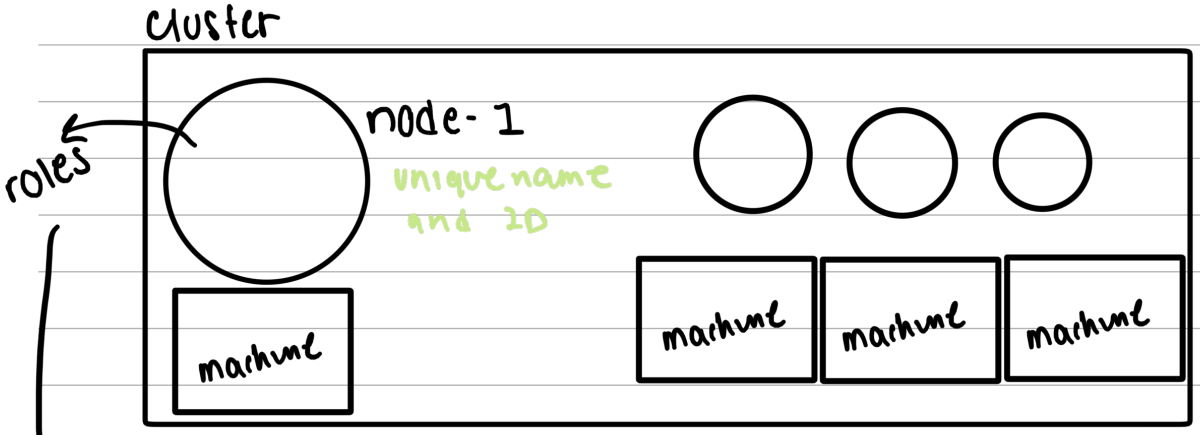
## Elastic Search

store | search | analyze

request → server → elasticsearch
← server ←

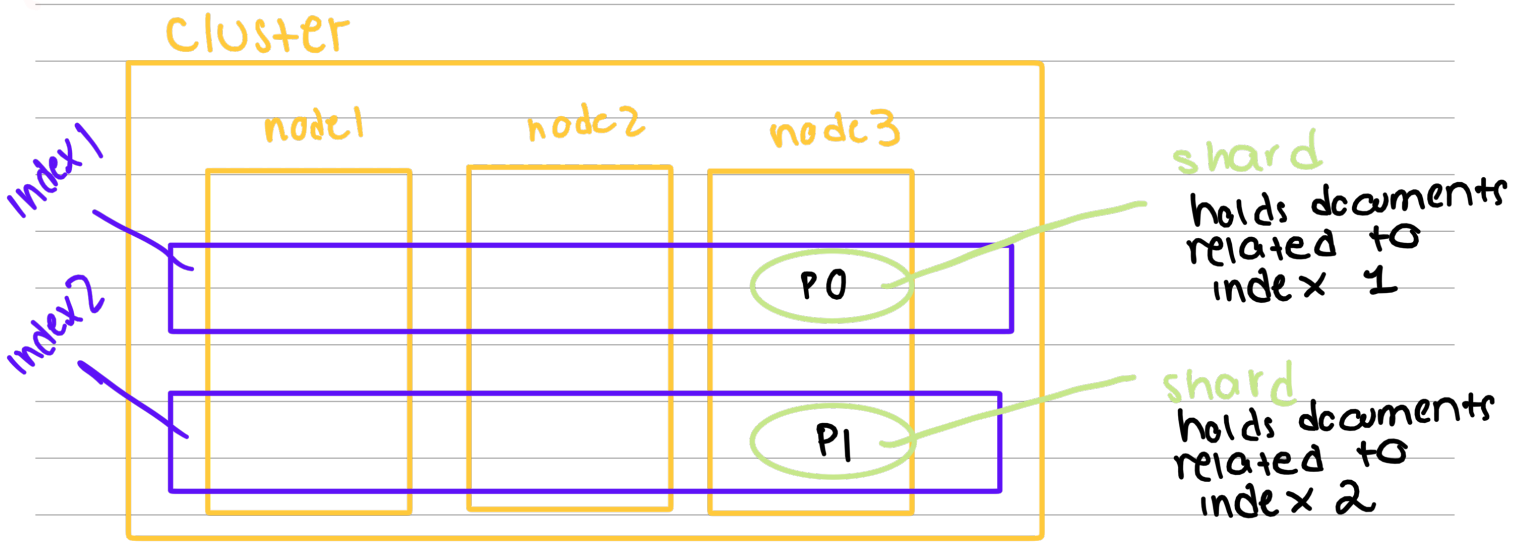
↳ kibana helps to visualize this
( search | view | interact )

## Elastic Search Arquitecture



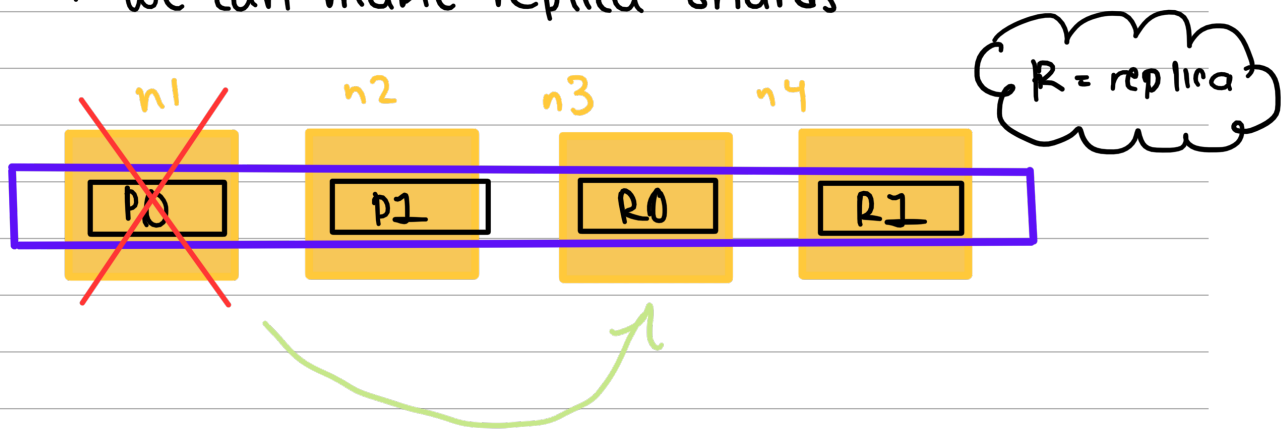

one of them is hold data (document) JSON
↓
grouped into indexes

* nodes use cache for searching




**Sharding:**
- shards are assigned to nodes.
- we can add more nodes to add more shards to an index.
- searchs can be parallel (faster)

* we can make replica shards




* replica shards can improve performance of searchs

* not recommended to have many shards in one node

# • Kibana – CRUD Operations

1. run bin\elasticsearch
2. cmd: curl https://localhost:9200
3. run bin\kibana

## – Create Index:

↳ PUT name-of-index

– index a document:

POST name-of-index/_doc/id-you-want

PUT

autogenerates id

```
{
  "field": "value"
}
```

JSON data

* use PUT when you use data with an specific id. Ex: patients
* this can update

if we don't want to overwrite:

– Create Endpoint

PUT name-of-index/_create/id-you-want

If it exists it conflicts

```
{
  "field": "value"
}
```

- **Read a document:**
  - ↳ GET name-of-index | id-of-document

- **Update a document**
  - ↳ POST name-of-index | _update | id-of-doc

```
{
    "doc": {
        "field": "value"
    }
}
```

updates only this

- **Delete a document**
  - ↳ DELETE name-of-index | _doc | id-of-doc