elastic

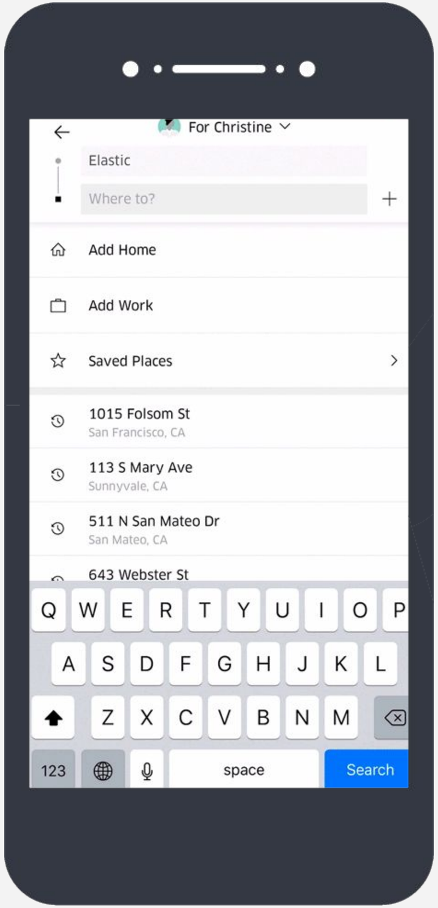
Beginner's Crash Course to Elastic Stack

Part 1.1: Intro to Elasticsearch and Kibana

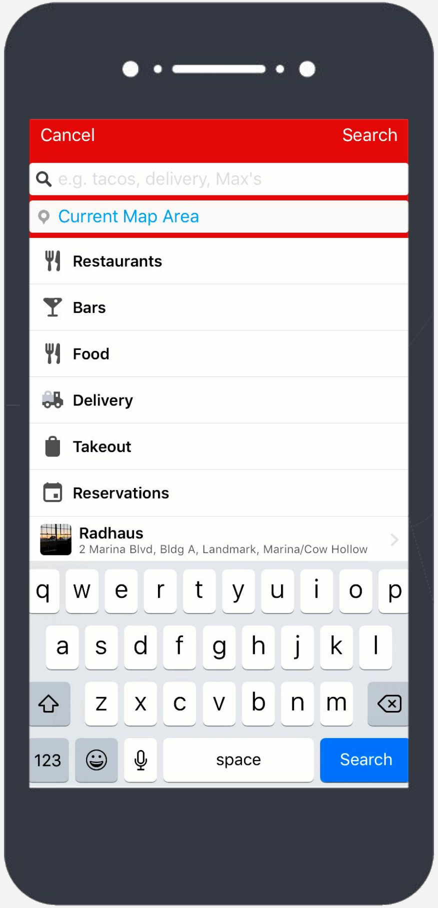
Lisa Jung
Developer Advocate @Elastic

Have you ever used the Elastic Stack before?

- In the chat window
  - Type YES if you have used it before
  - Type NO if you have never used it before



Searching for Rides

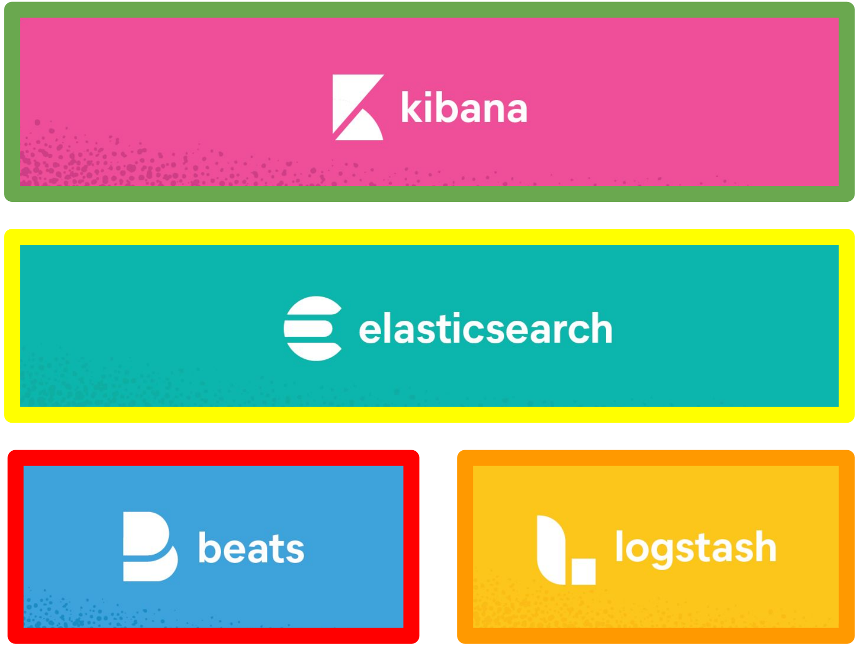


Searching for Restaurants

Searching for **Rides**

The Elastic Stack

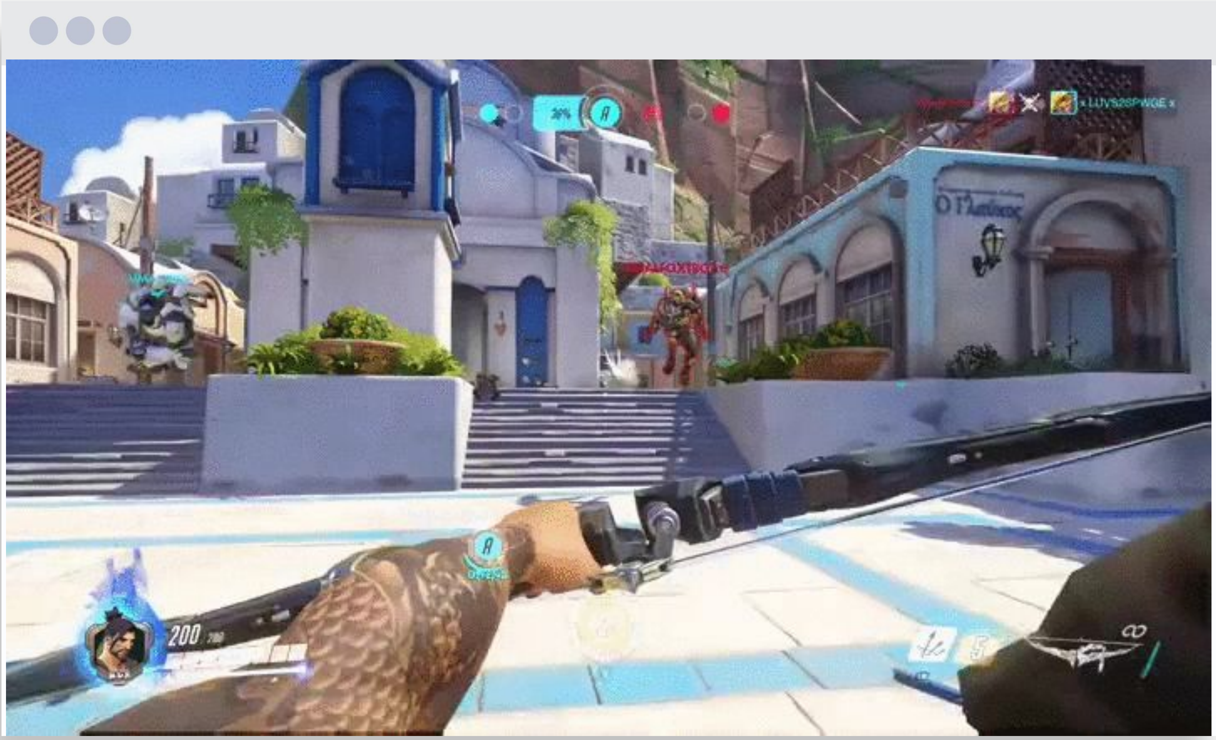
Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

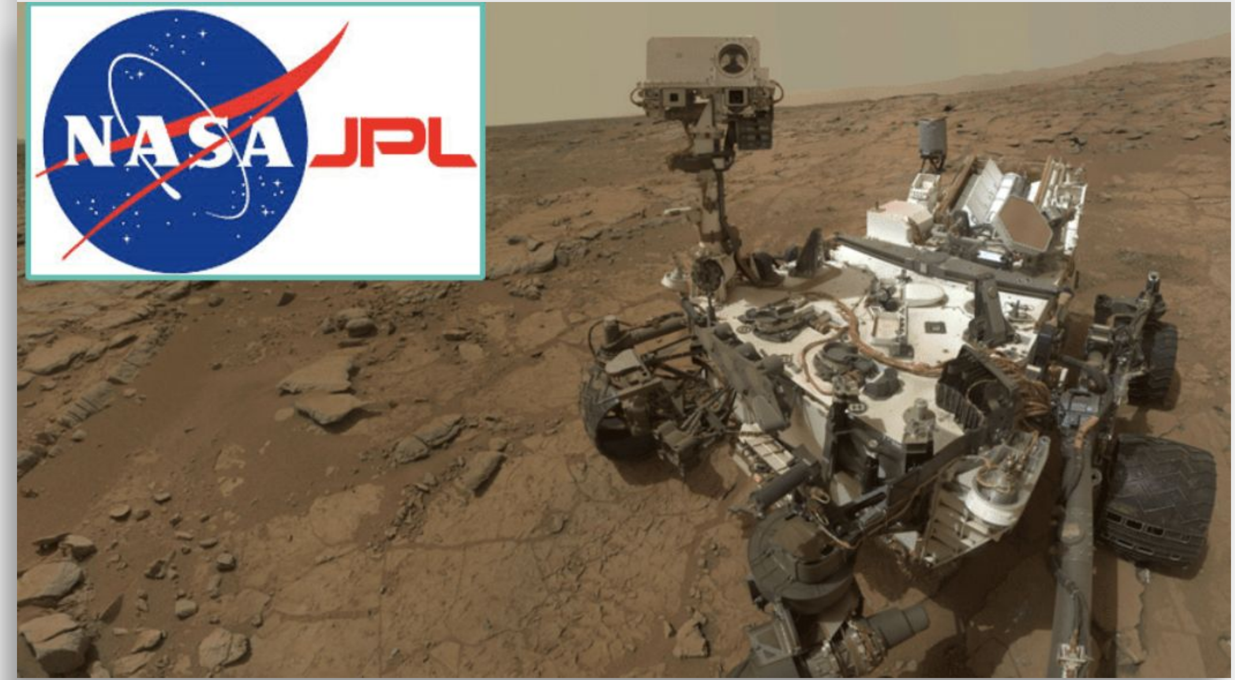
Use Case: Logging



https://www.reddit.com/r/gaming/comments/4lhm69/overwatch_blocked_pharahs_rocket_with_hanzos_arrow/

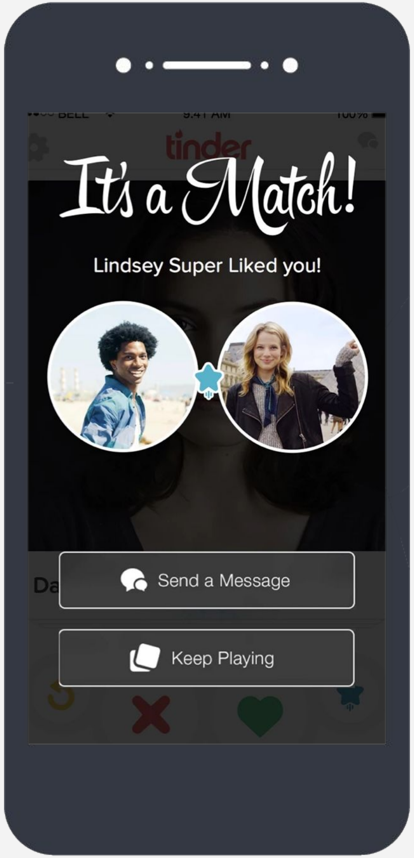
ACTIVISION BLIZZARD

Use Case: Metrics



Use Case: Security Analytics

Use Case: Business Analytics

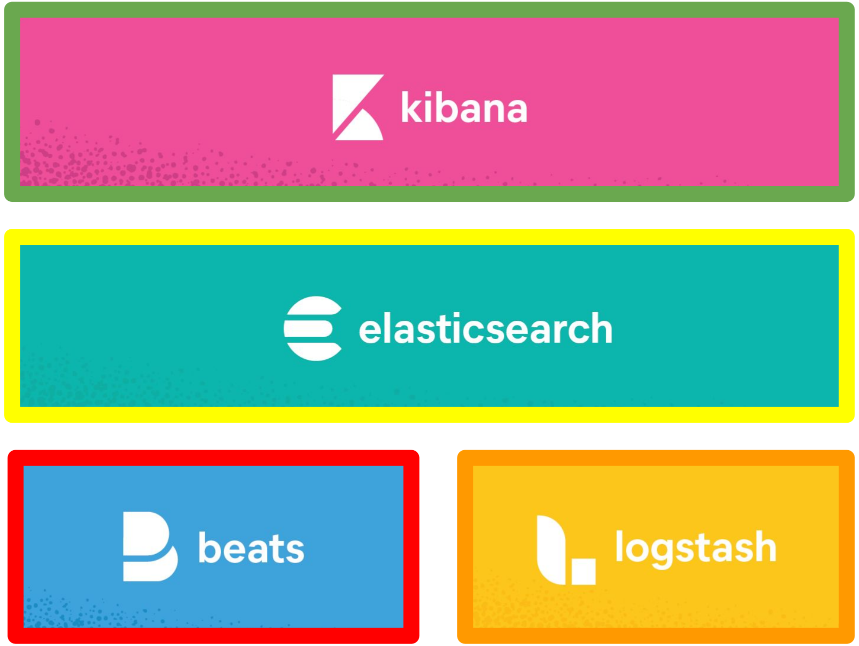


tinder™

elastic

The Elastic Stack

Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



Beginner’s Crash Course to Elastic Stack

Part 1.1: Intro to Elasticsearch and Kibana

By the end of this workshop, you will be able to:

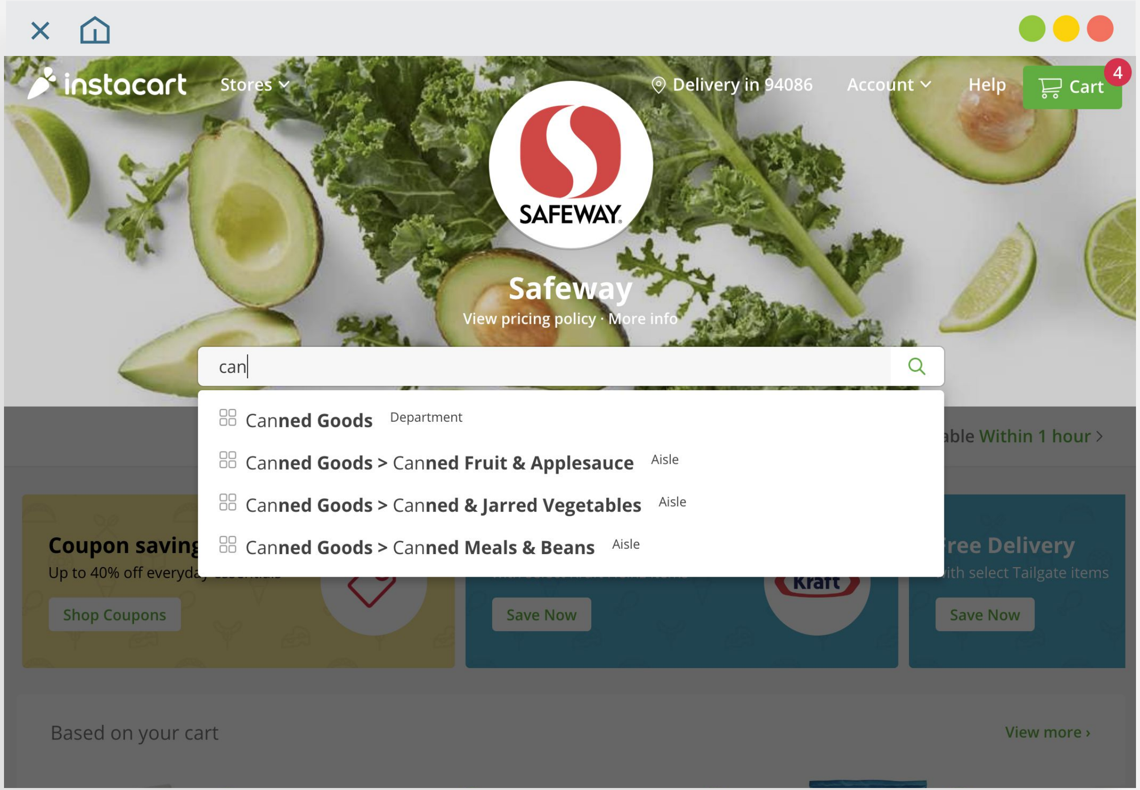
- understand a use case of Elasticsearch and Kibana
- understand the basic architecture of Elasticsearch
- Perform CRUD(Create, Read, Update, Delete) operations with Elasticsearch and Kibana

elastic

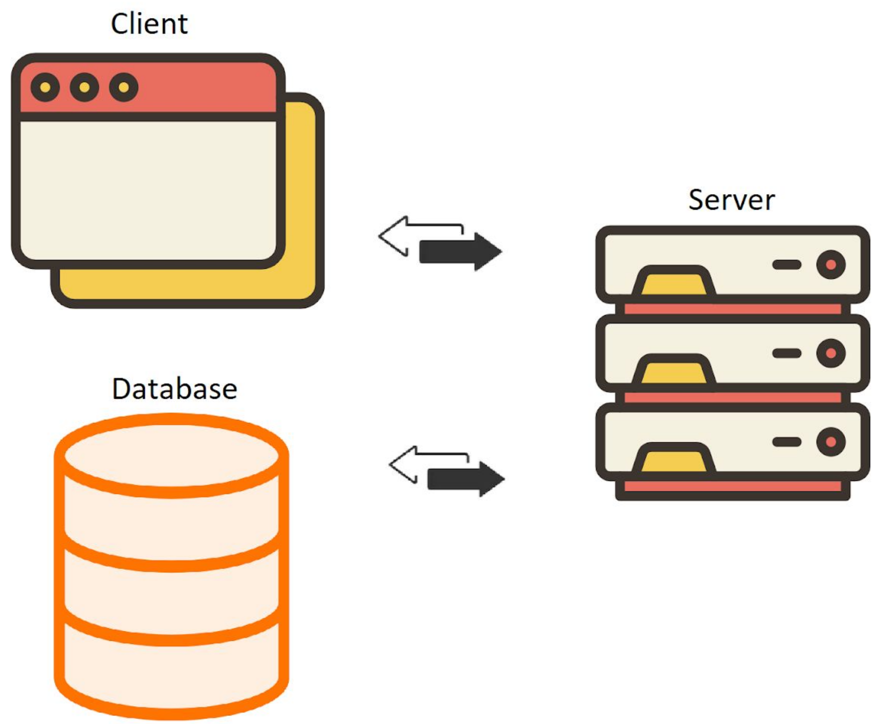
Elasticsearch

Store | Search | Analyze

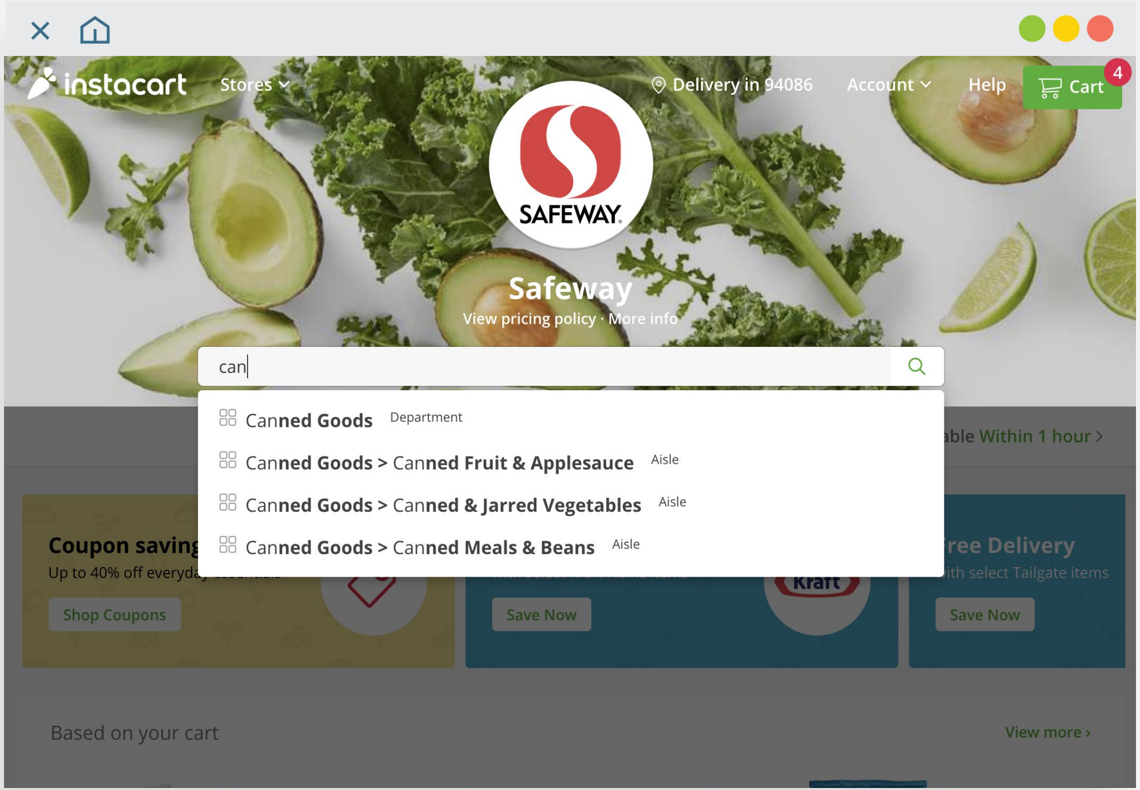
instacart



instacart
Stores
Delivery in 94086
Account
Help
Cart
4
SAFEWAY
Safeway
View pricing policy · More info
can
Canned Goods
Department
Canned Goods > Canned Fruit & Applesauce
Aisle
Canned Goods > Canned & Jarred Vegetables
Aisle
Canned Goods > Canned Meals & Beans
Aisle
able Within 1 hour
Coupon saving
Up to 40% off everyda
Shop Coupons
Save Now
Kraft
ree Delivery
ith select Tailgate items
Save Now
Based on your cart
View more ›

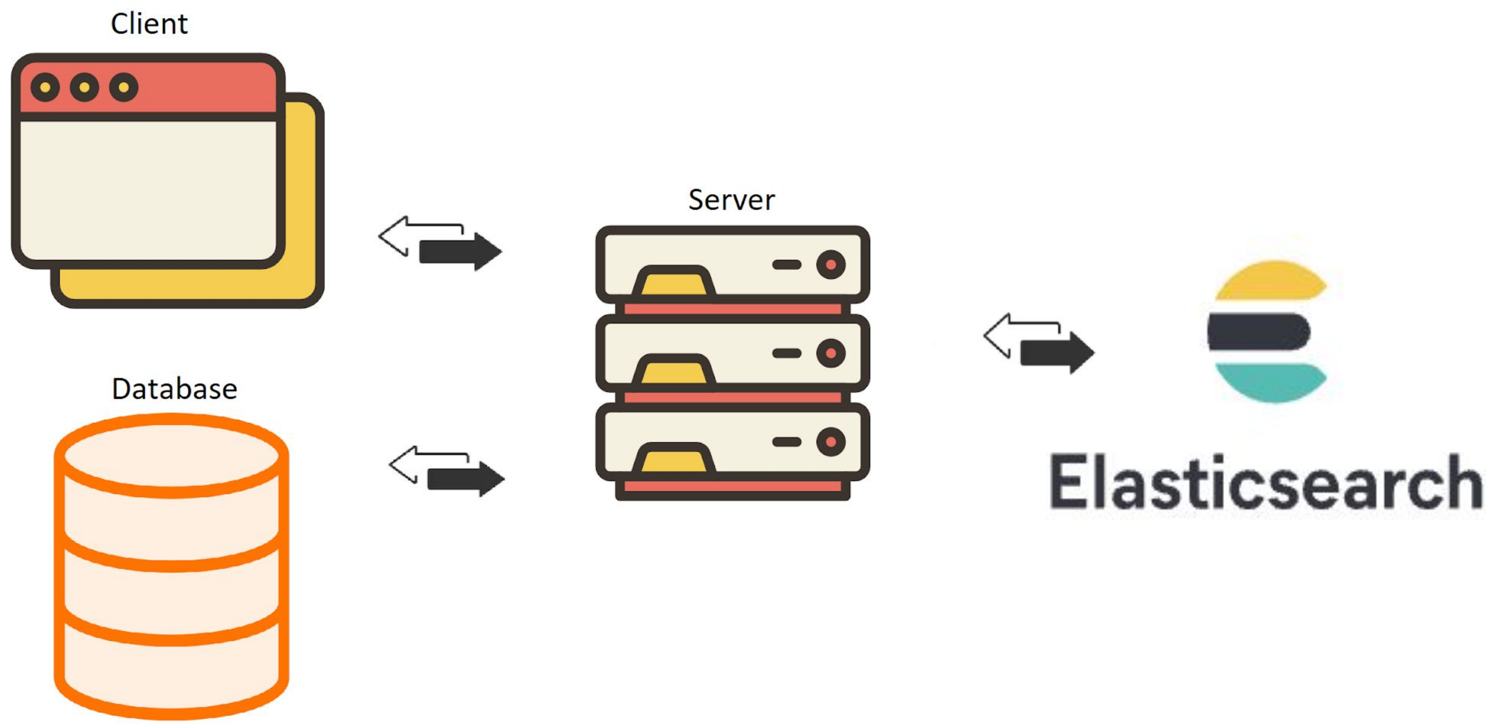

Client
Server
Database

Great Search Experience = Get fast and relevant results, no matter the scale.



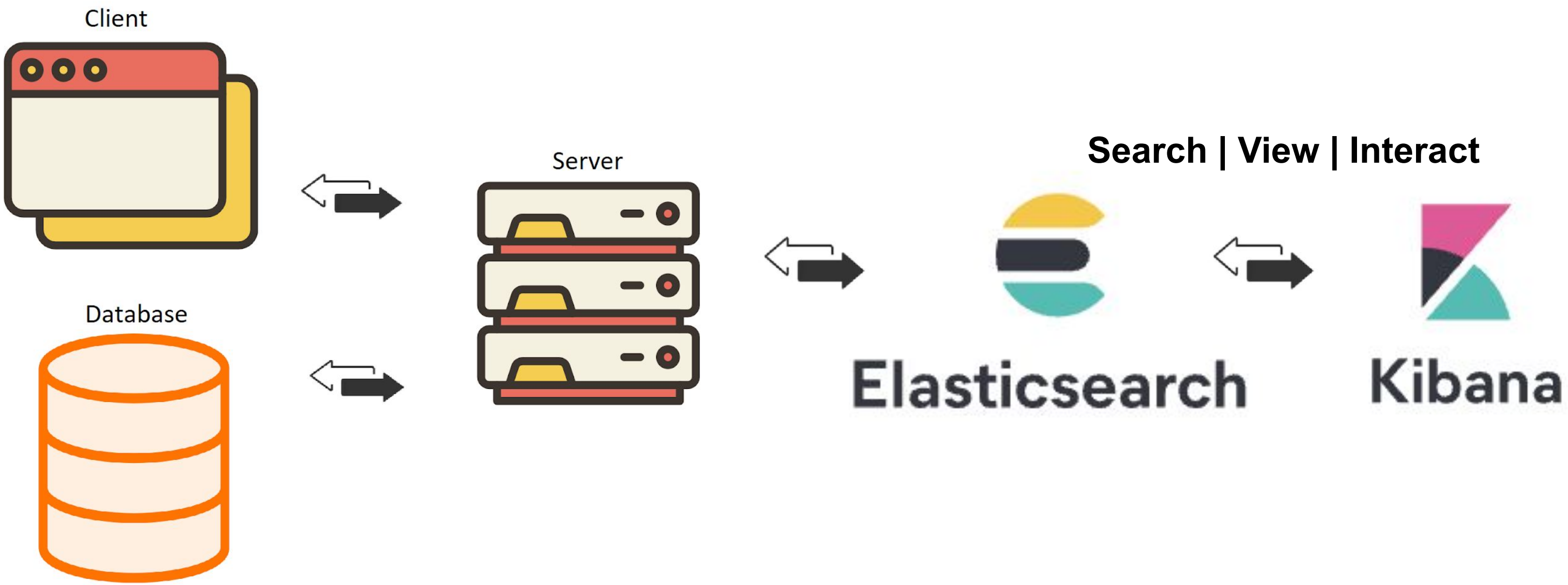
Find me a list of peanut butter brands. I want highest rated brands at the top.

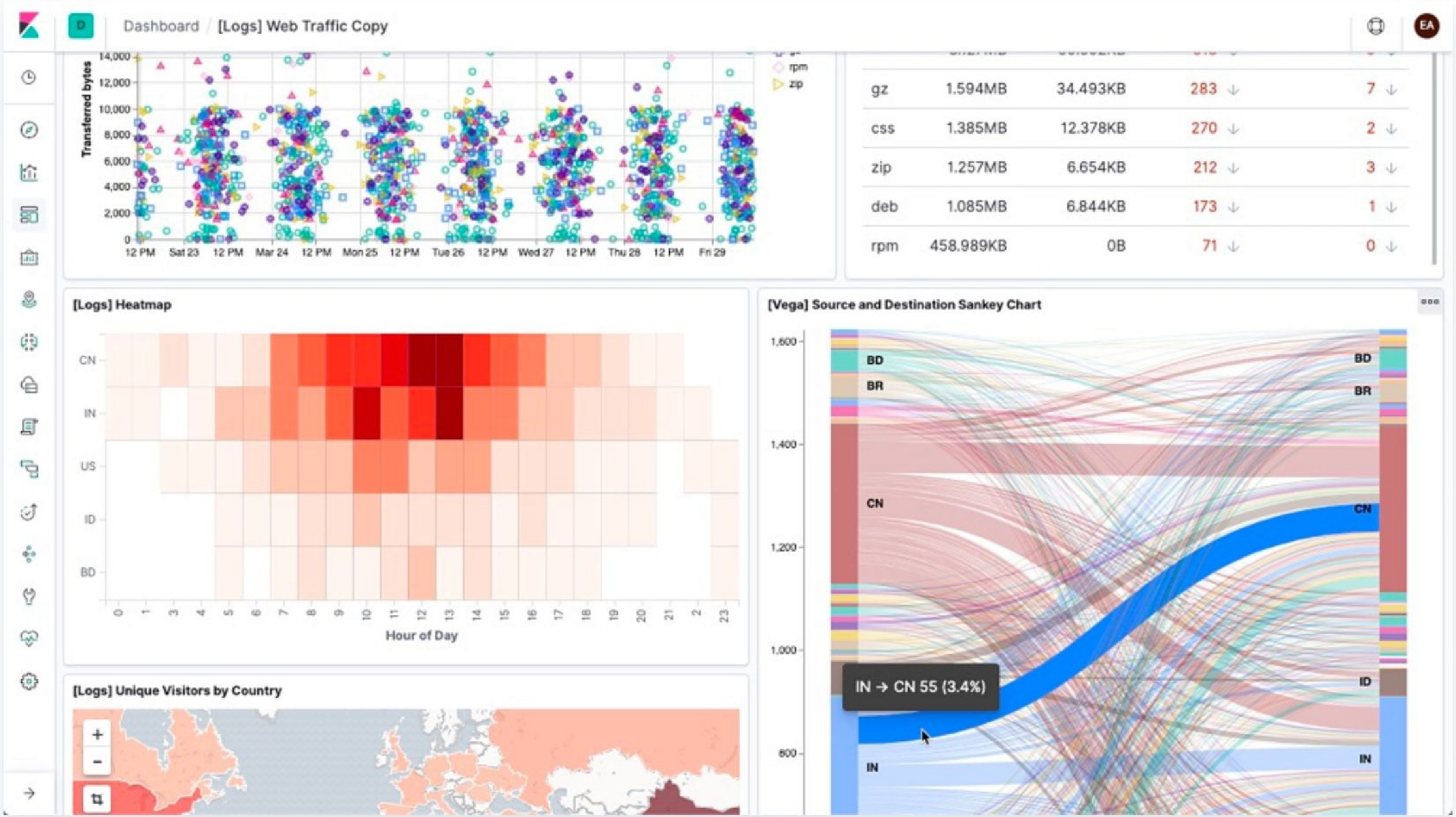
Find me a hot sauce named uh… I think it is spelled Sriracha? Maybe it's spelled Srirracah? Srirracha?


Client
Server
Database
Elasticsearch

Elasticsearch

Store | Search | Analyze


Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana


Dashboard / [Logs] Web Traffic Copy
EA
Transferred bytes
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
12 PM
Sat 23
12 PM
Mar 24
12 PM
Mon 25
12 PM
Tue 26
12 PM
Wed 27
12 PM
Thu 28
12 PM
Fri 29
rpm
zip
gz 1.594MB 34.493KB 283 7
css 1.385MB 12.378KB 270 2
zip 1.257MB 6.654KB 212 3
deb 1.085MB 6.844KB 173 1
rpm 458.989KB 0B 71 0
[Logs] Heatmap
CN
IN
US
ID
BD
0 1 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 2 23
Hour of Day
[Vega] Source and Destination Sankey Chart
1,600
1,400
1,200
1,000
800
BD
BR
CN
IN
ID
IN → CN 55 (3.4%)
[Logs] Unique Visitors by Country

By the end of this workshop, you will be able to:

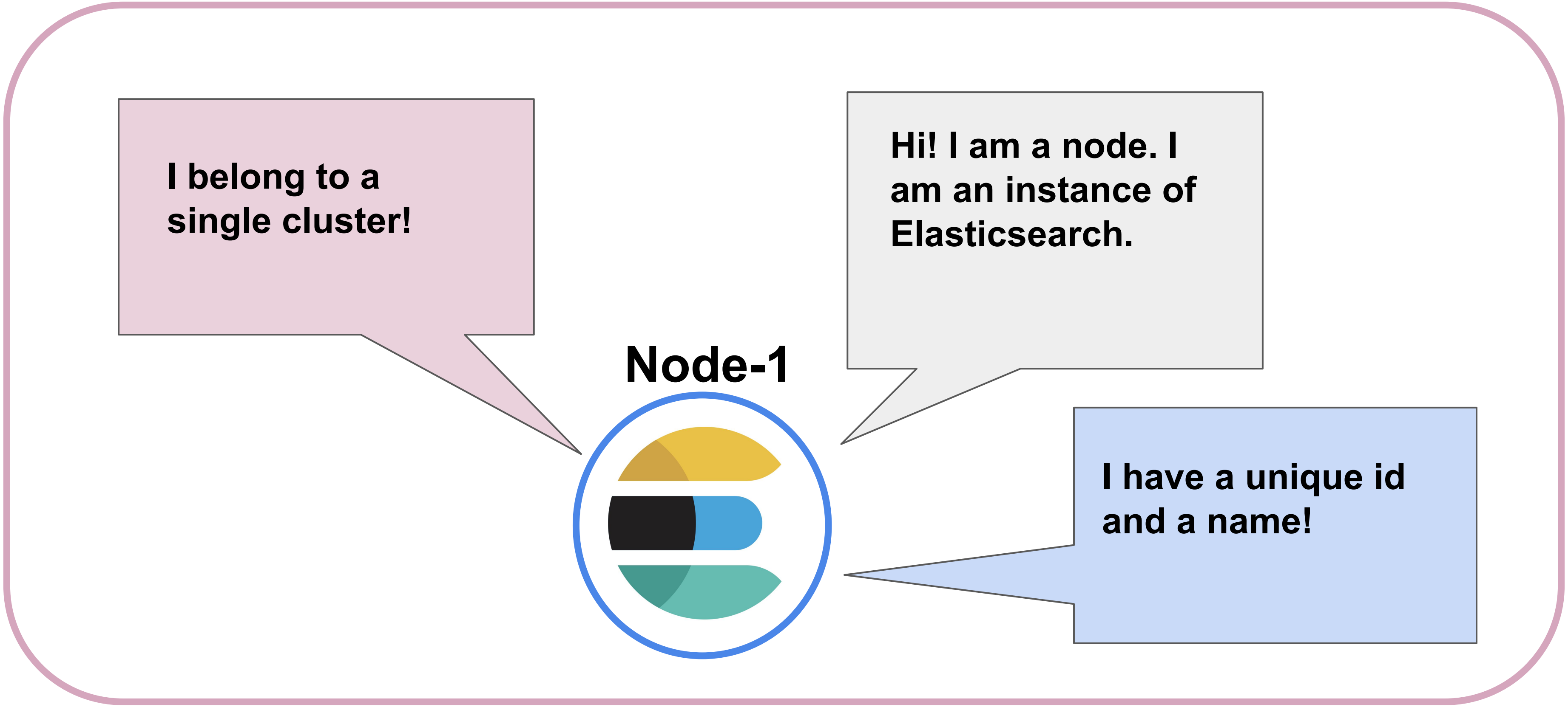
- understand a use case of Elasticsearch and Kibana
- **understand the basic architecture of Elasticsearch**
- Run CRUD (Create, Read, Update, Delete) Operations using Elasticsearch and Kibana

elastic

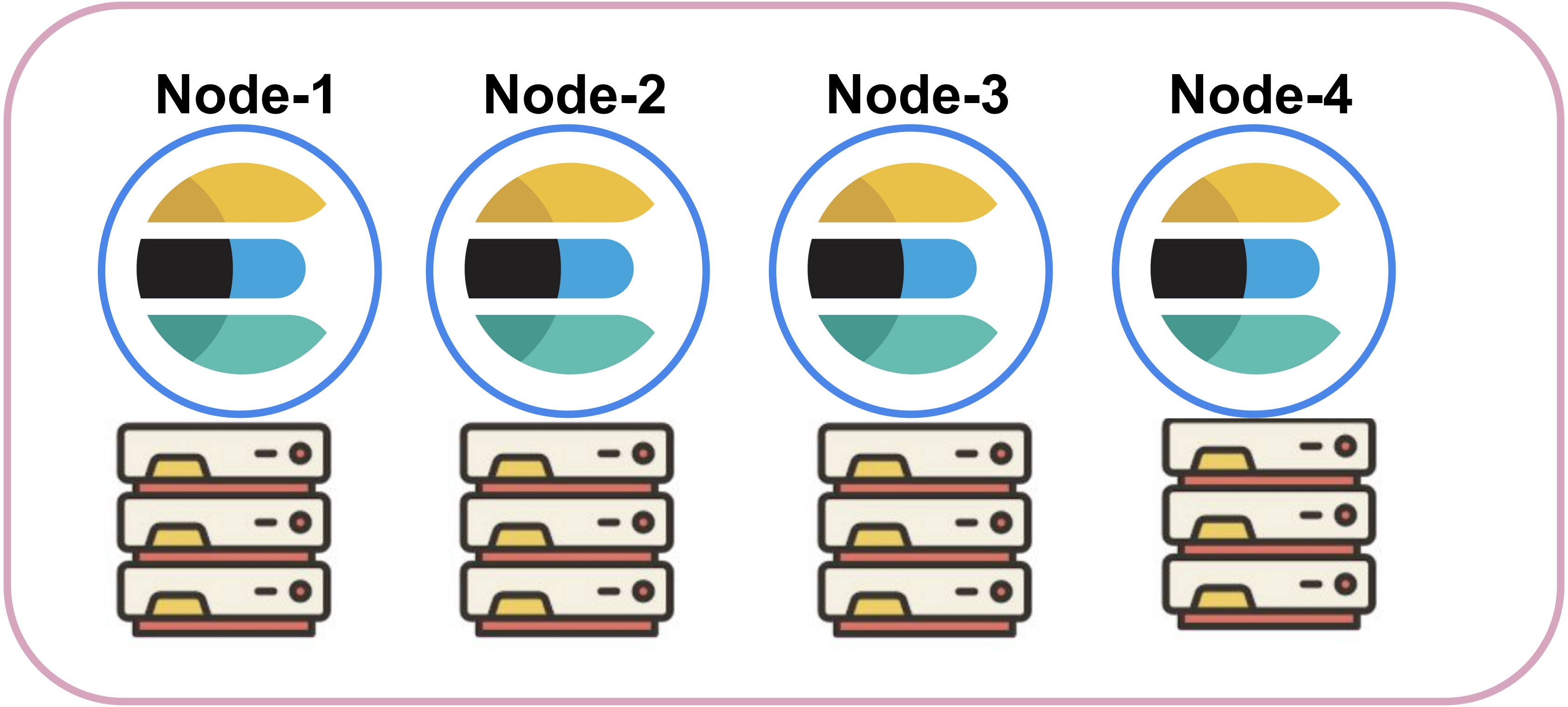
Elasticsearch

Store | Search | Analyze

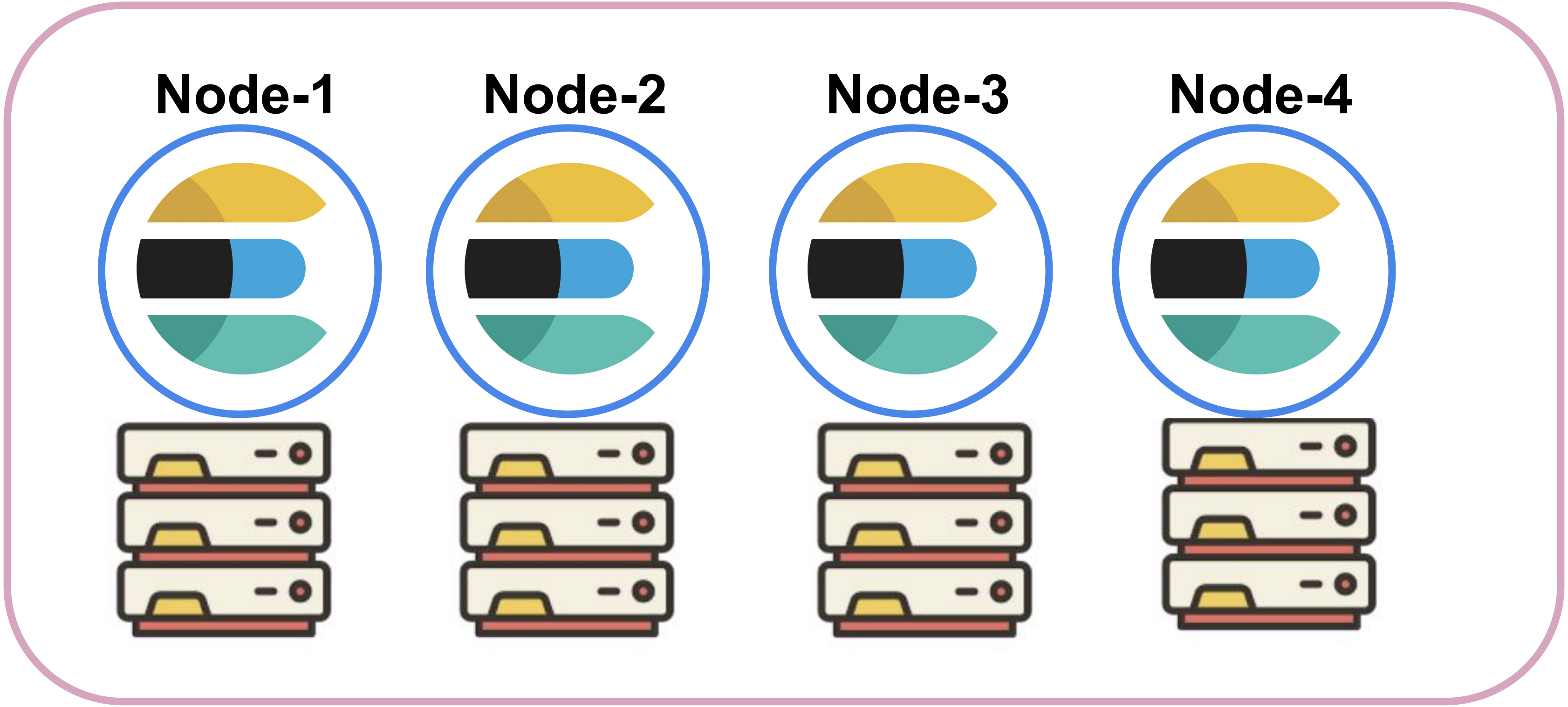
Cluster


I belong to a single cluster!
Hi! I am a node. I am an instance of Elasticsearch.
Node-1
I have a unique id and a name!

Cluster



Cluster



Data is stored as documents!

```
{
  "name": "Baby Carrots(1lb bag)",
  "category": "Vegetables",
  "brand": "365",
  "price": "$0.99"
}
```

I am a document, a JSON object that is stored in Elasticsearch under a unique ID!

Documents are grouped into an index!

Produce Index

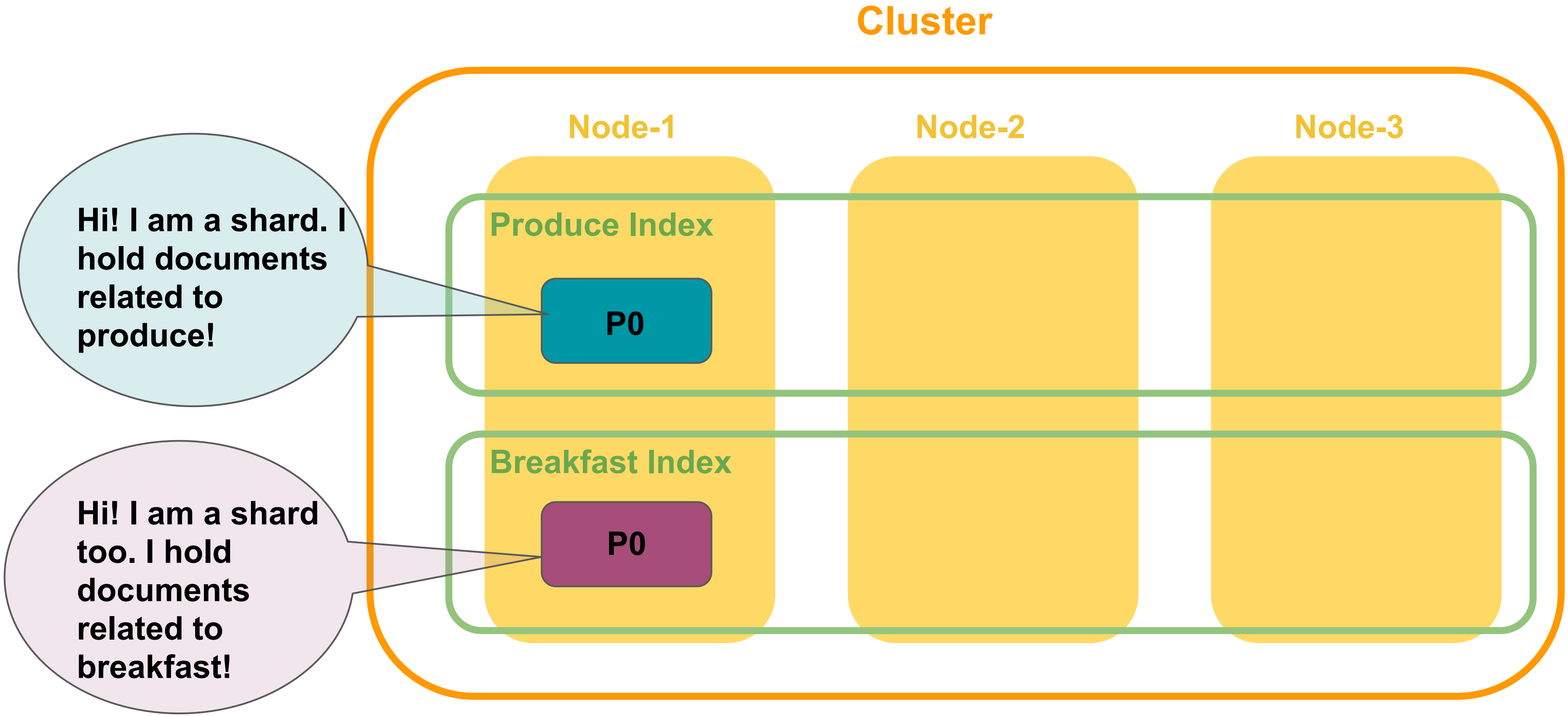
```
{
  "name": "Baby Carrots(1lb bag)",
  "category": "Vegetables",
  "brand": "365",
  "price": "$0.99"
}

{
  "name": "Clementines(3lb bag)",
  "category": "Fruits",
  "brand": "Cuties",
  "price": "$4.29"
}
```

Breakfast Index

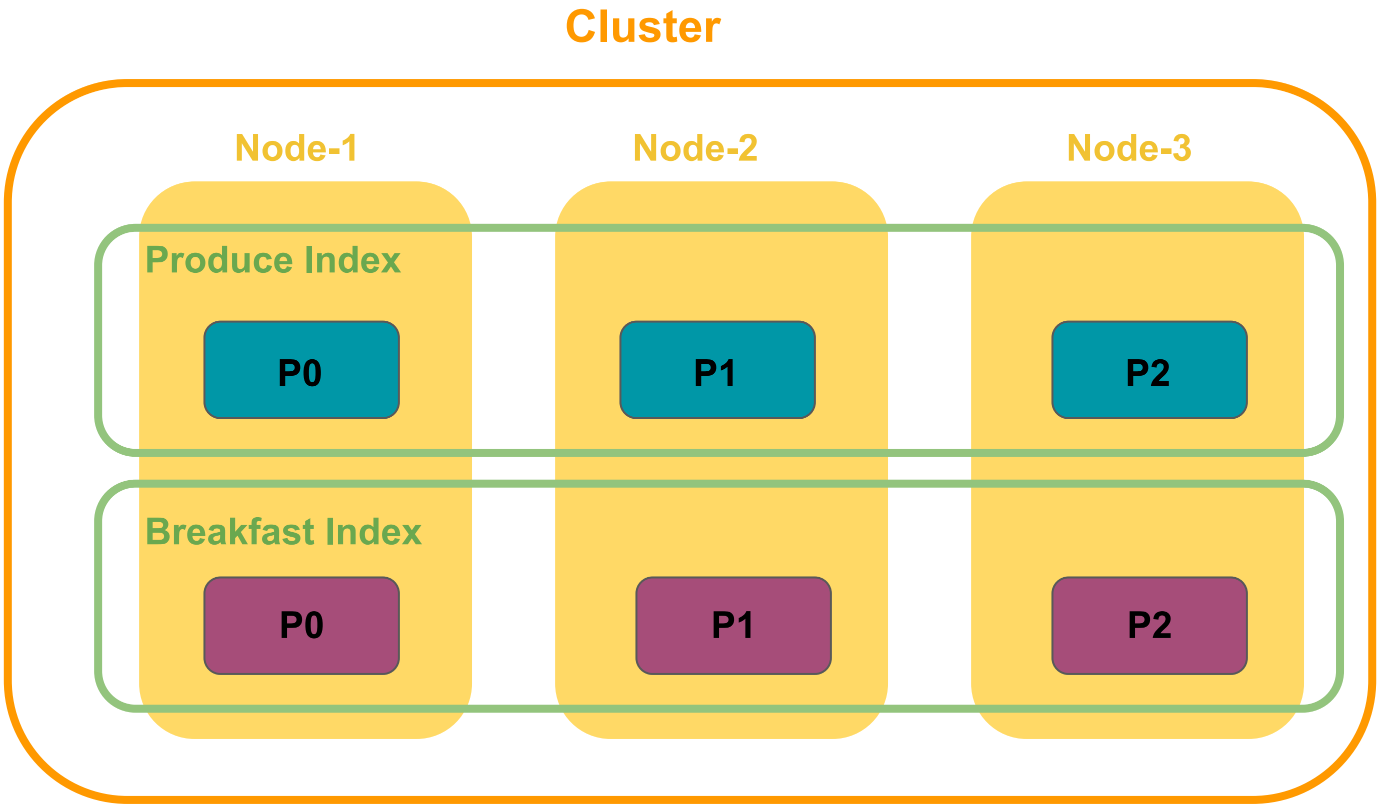
```
{
  "name": "Instant Oatmeal Brown Sugar",
  "category": "Breakfast",
  "brand": "Quaker",
  "price": "$3.59"
}

{
  "name": "Pop-Tarts Brown Sugar Cinnamon",
  "category": "Breakfast",
  "brand": "Kellogg's",
  "price": "$2.99"
}
```

elastic

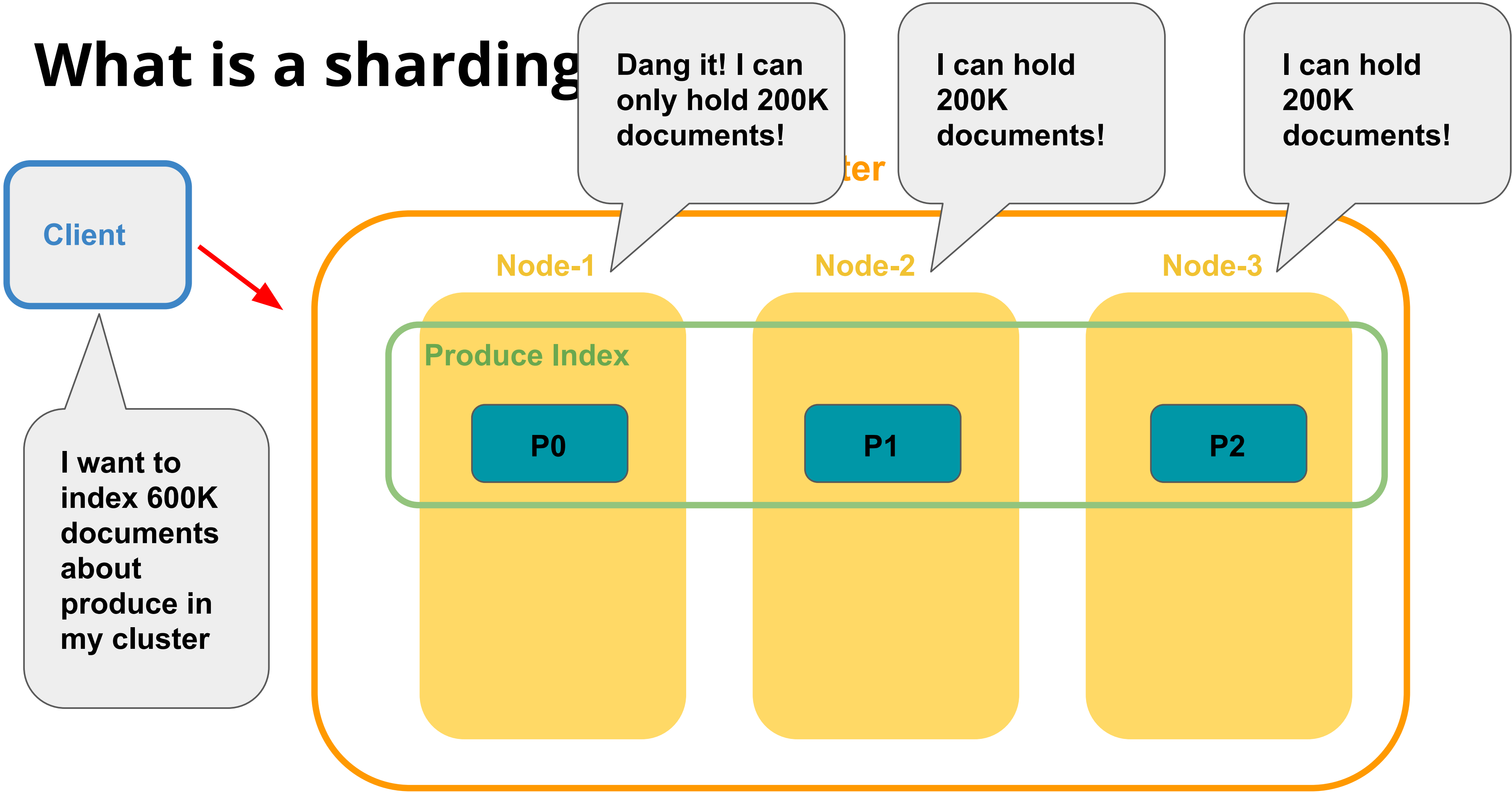
What is a shard?



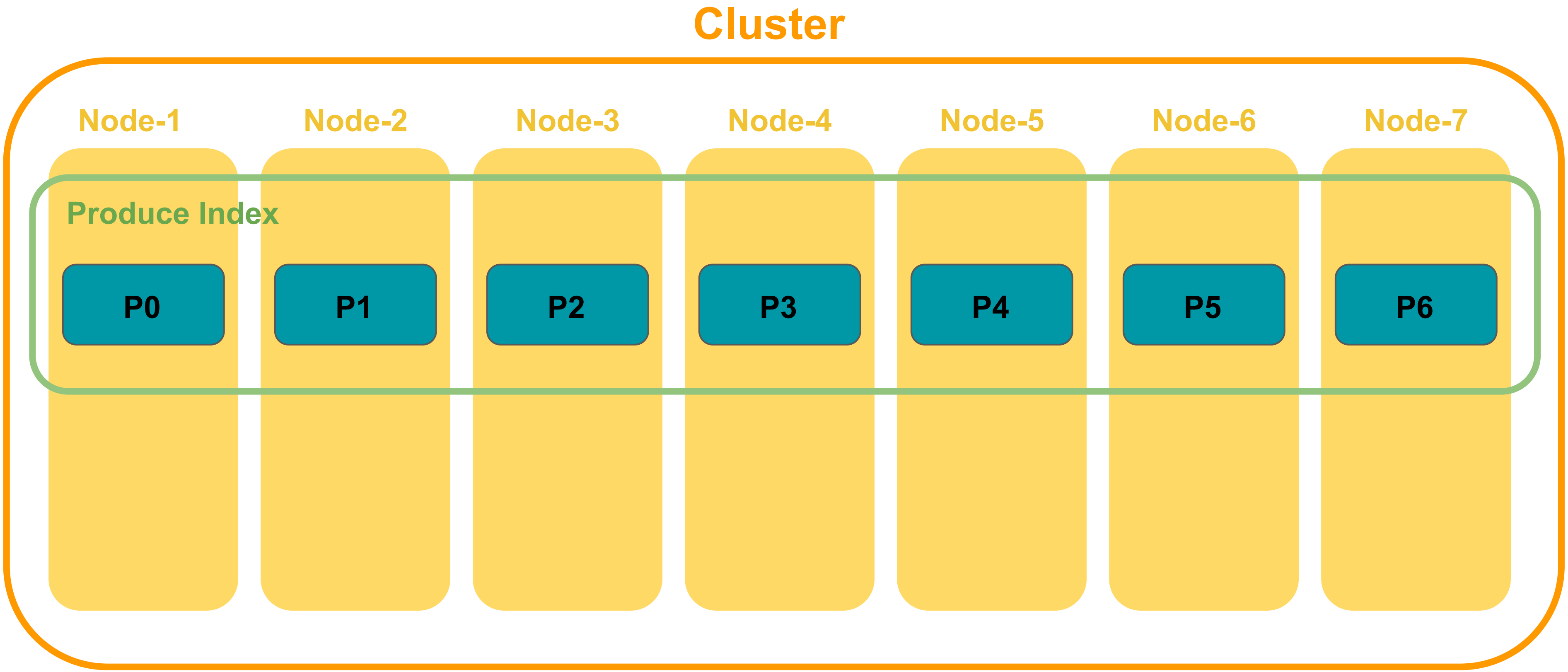
What is a sharding?



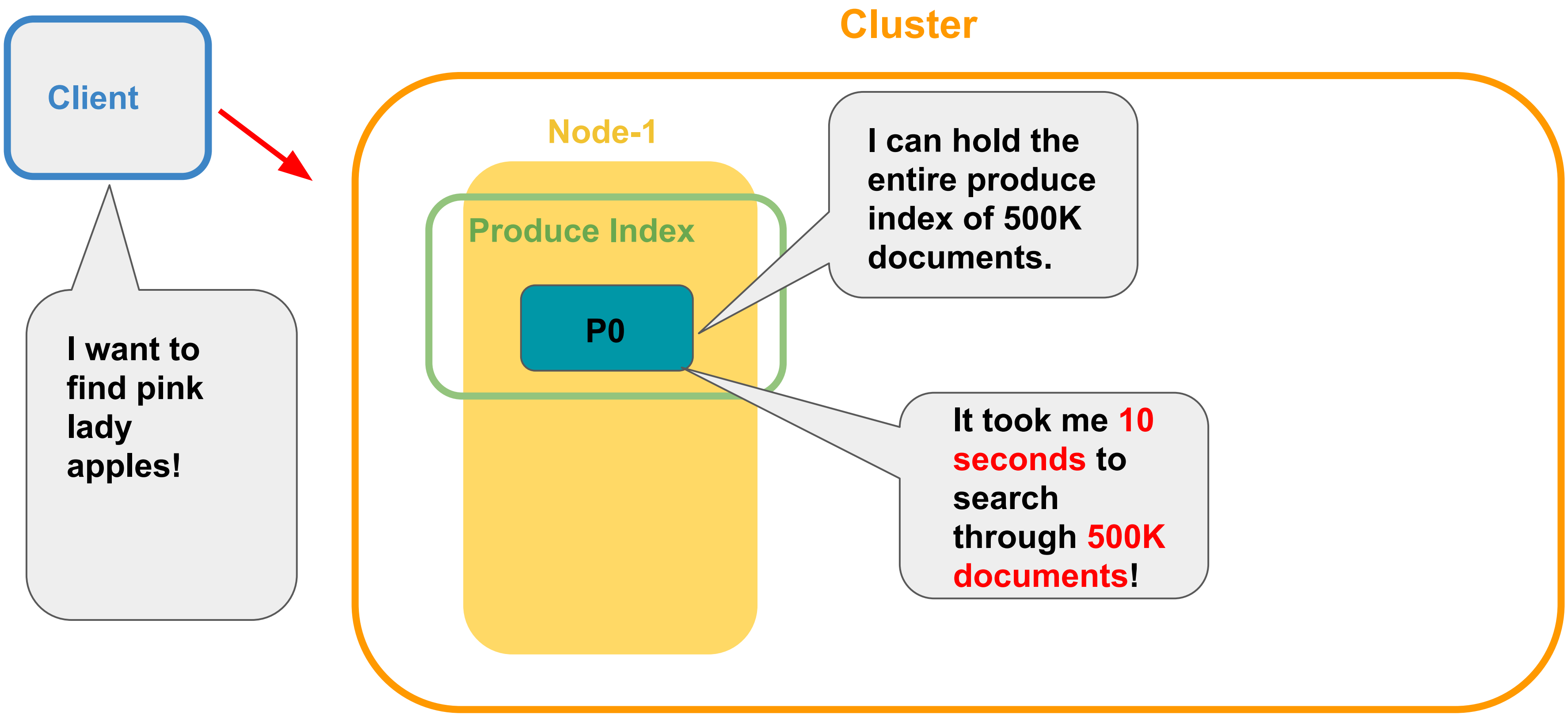
What is a sharding



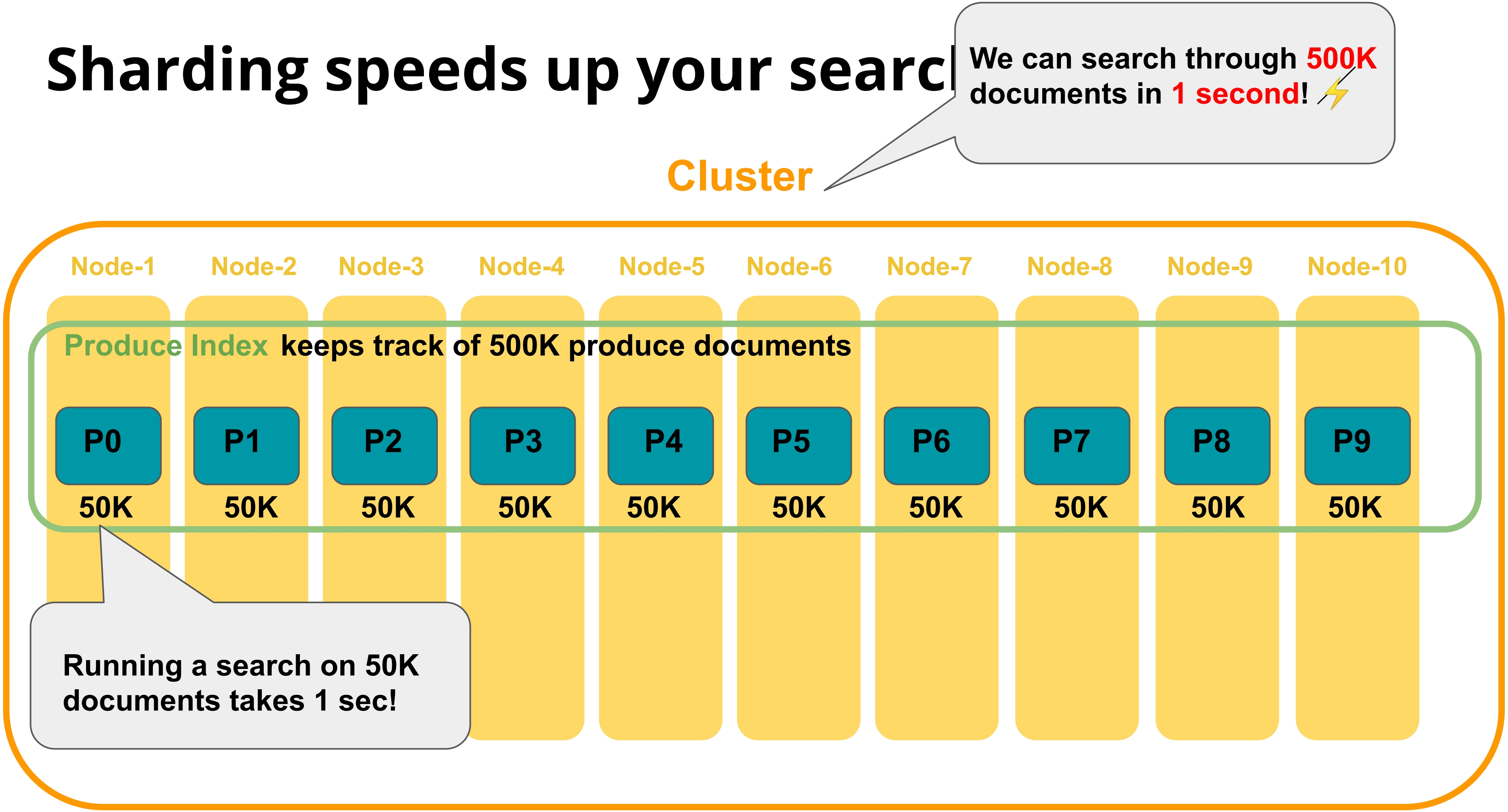
What is a sharding?



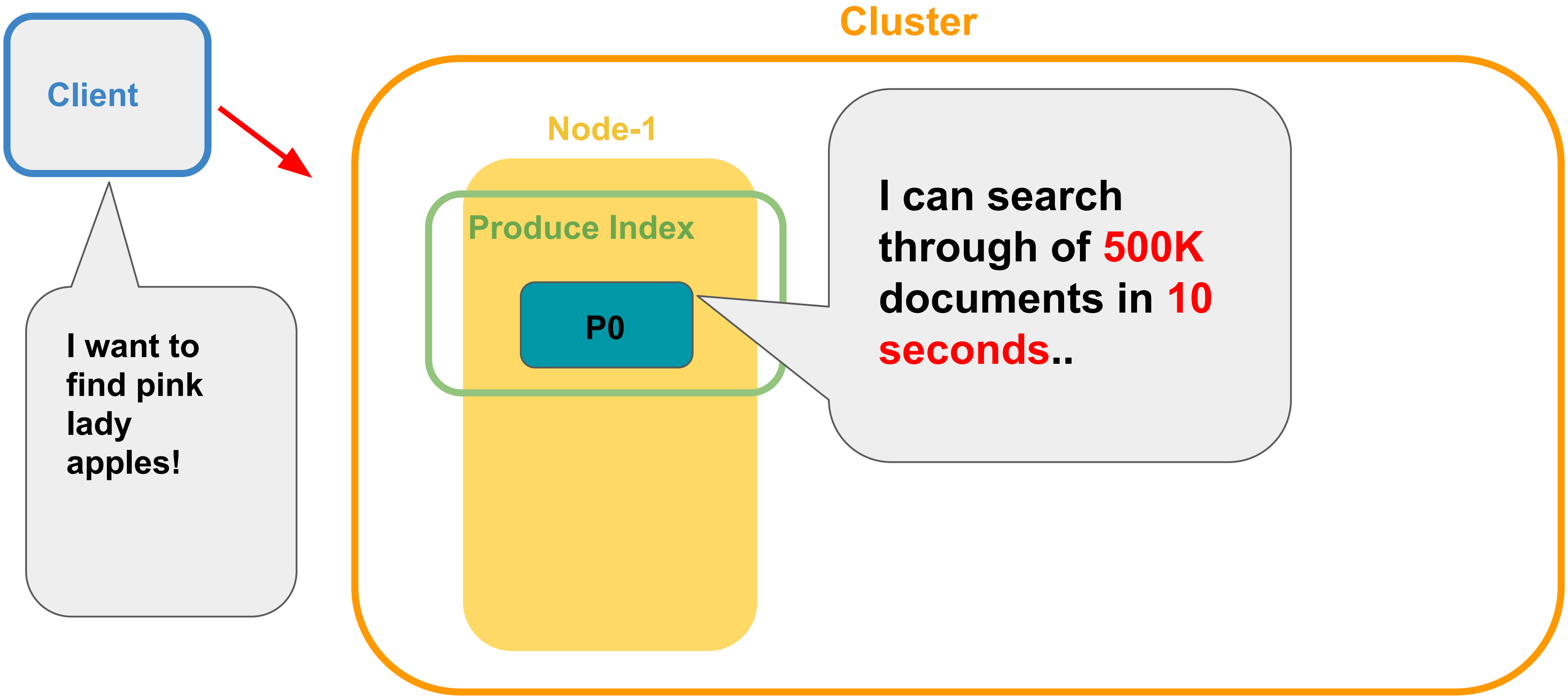
What is a sharding?



Sharding speeds up your searc



What is a sharding?



Sharding speeds up your searc

We can search through 500K documents in 1 second! ⚡

Cluster

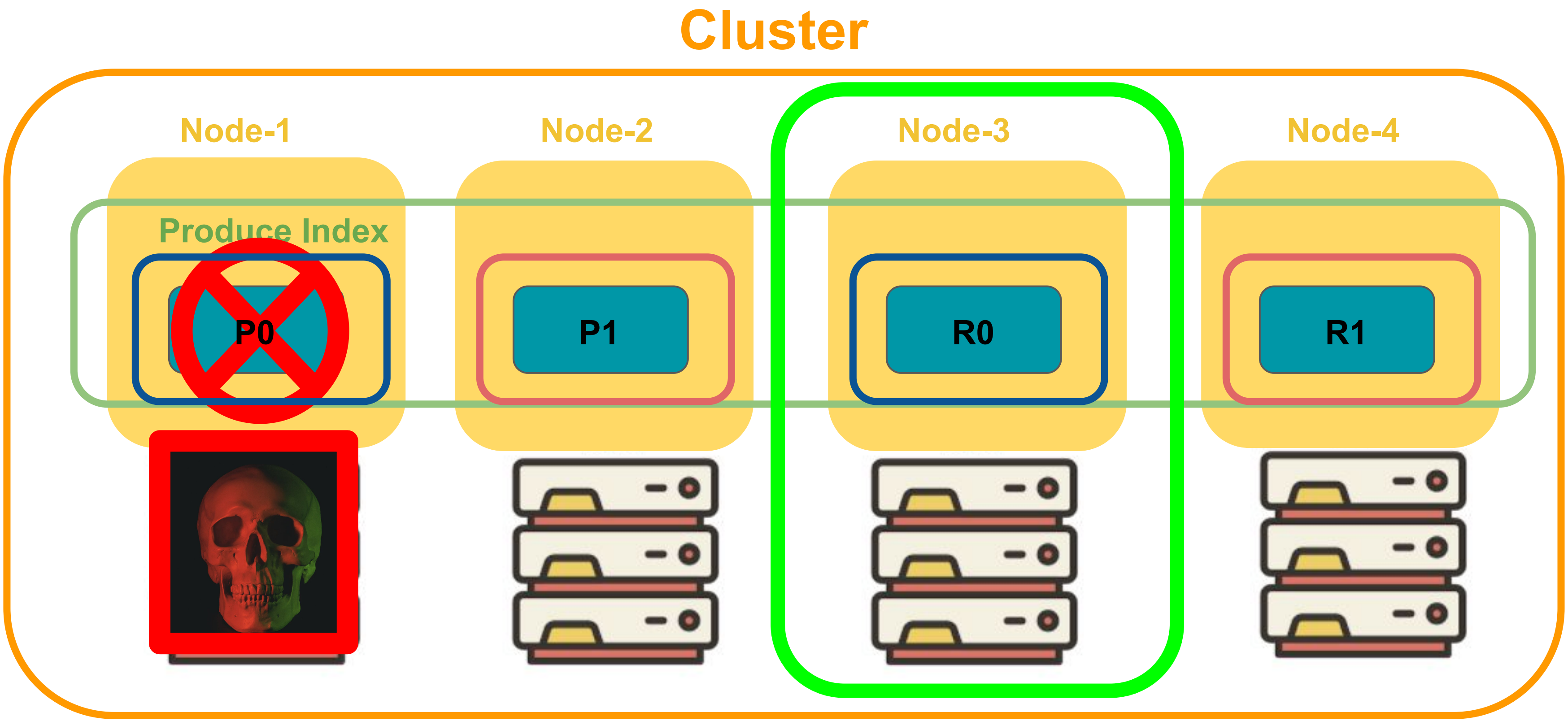
Node-1 Node-2 Node-3 Node-4 Node-5 Node-6 Node-7 Node-8 Node-9 Node-10

Produce Index

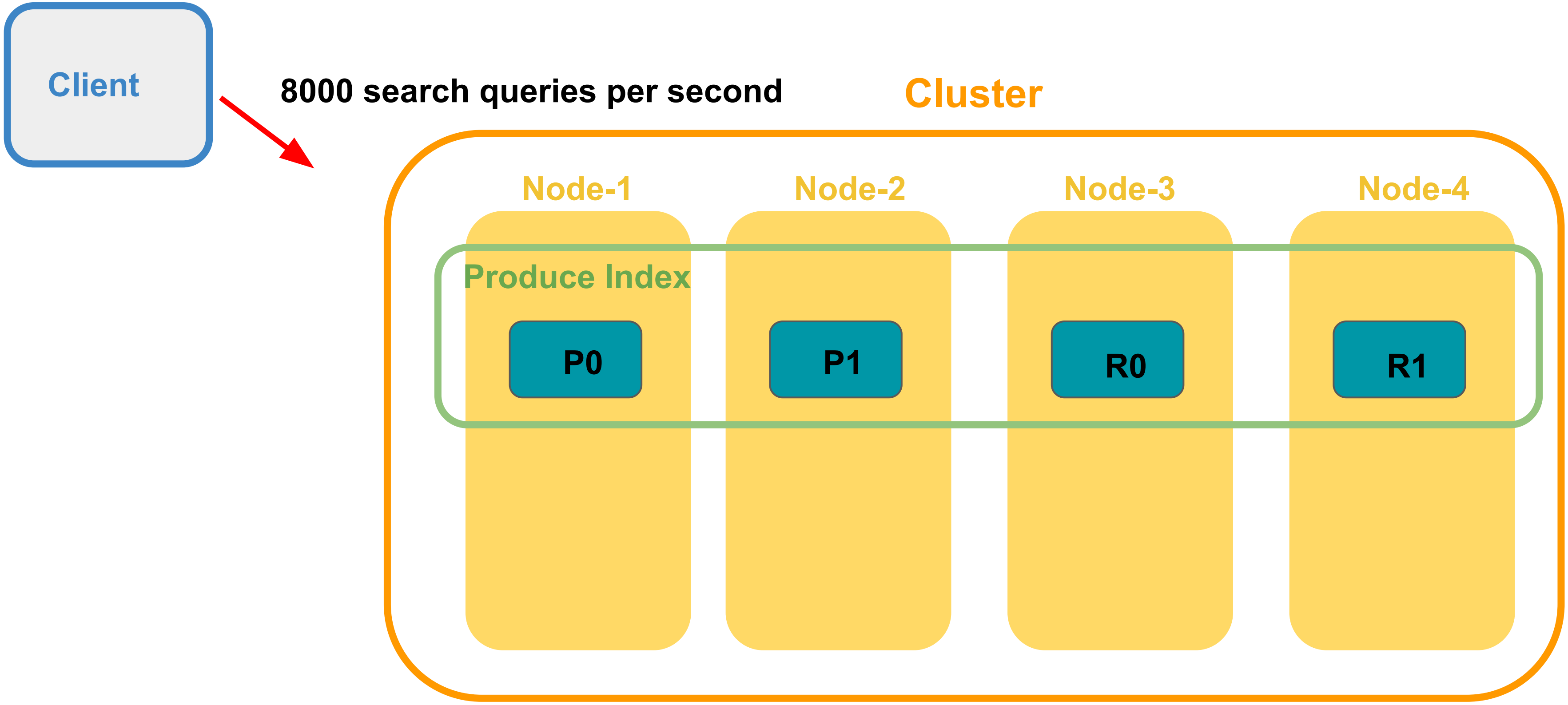
P0	P1	P2	P3	P4	P5	~~P6~~	P7	P8	P9
50K	50K	50K	50K	50K	50K	~~50K~~	50K	50K	50K


#SPONGEBOBMOVIE

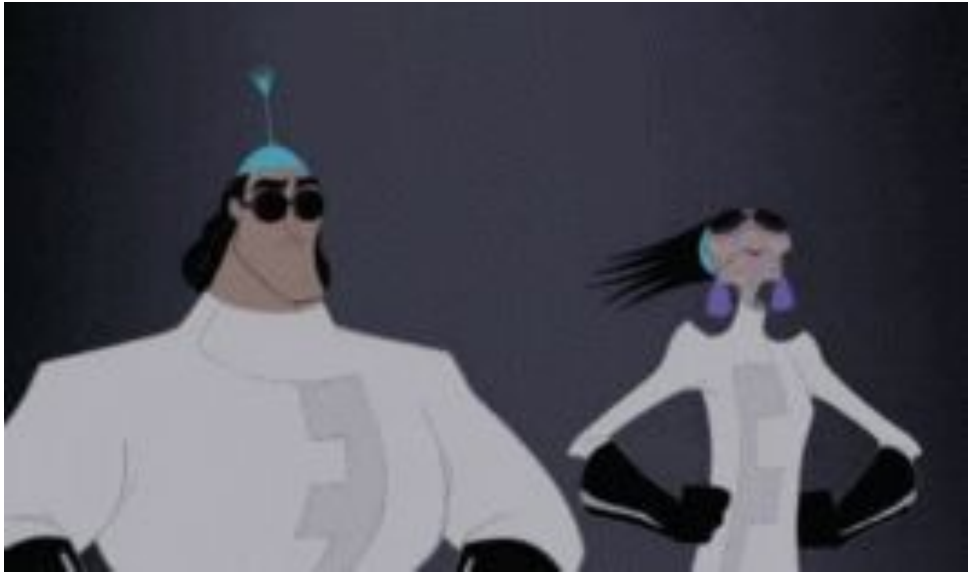
What are replica shards?



Replica shards can improve the performance of your search



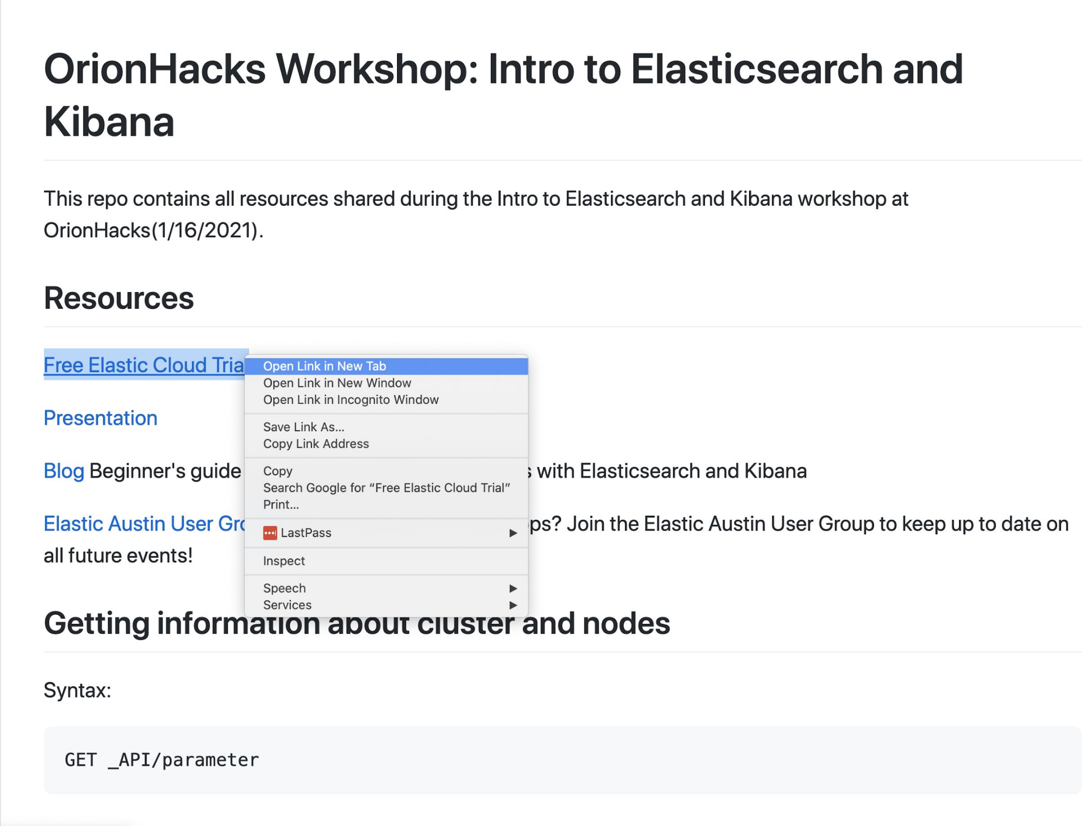
Hands-on Lab:
Performing CRUD Operations with Elasticsearch and Kibana



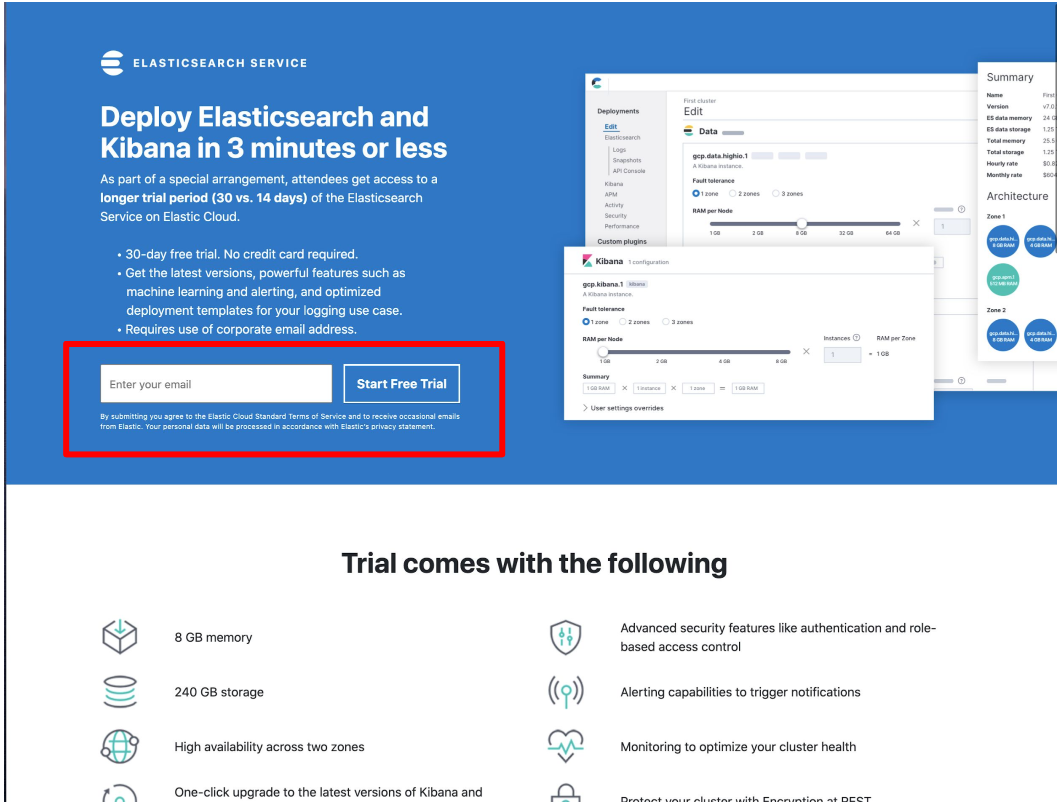
Click on the link to the workshop repo.

https://ela.st/orionhacks-elastic

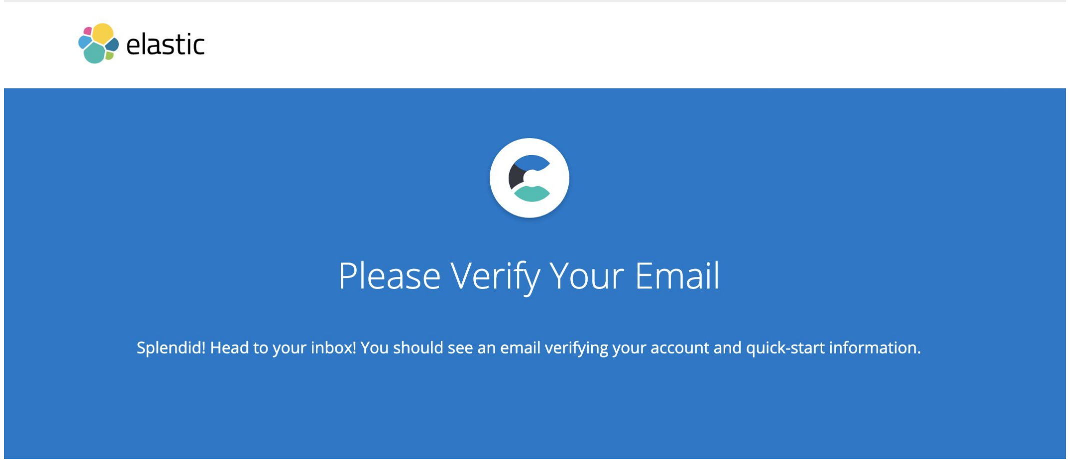
Scroll down to the Resources section & open Free Elastic Cloud Trial link in a new tab.



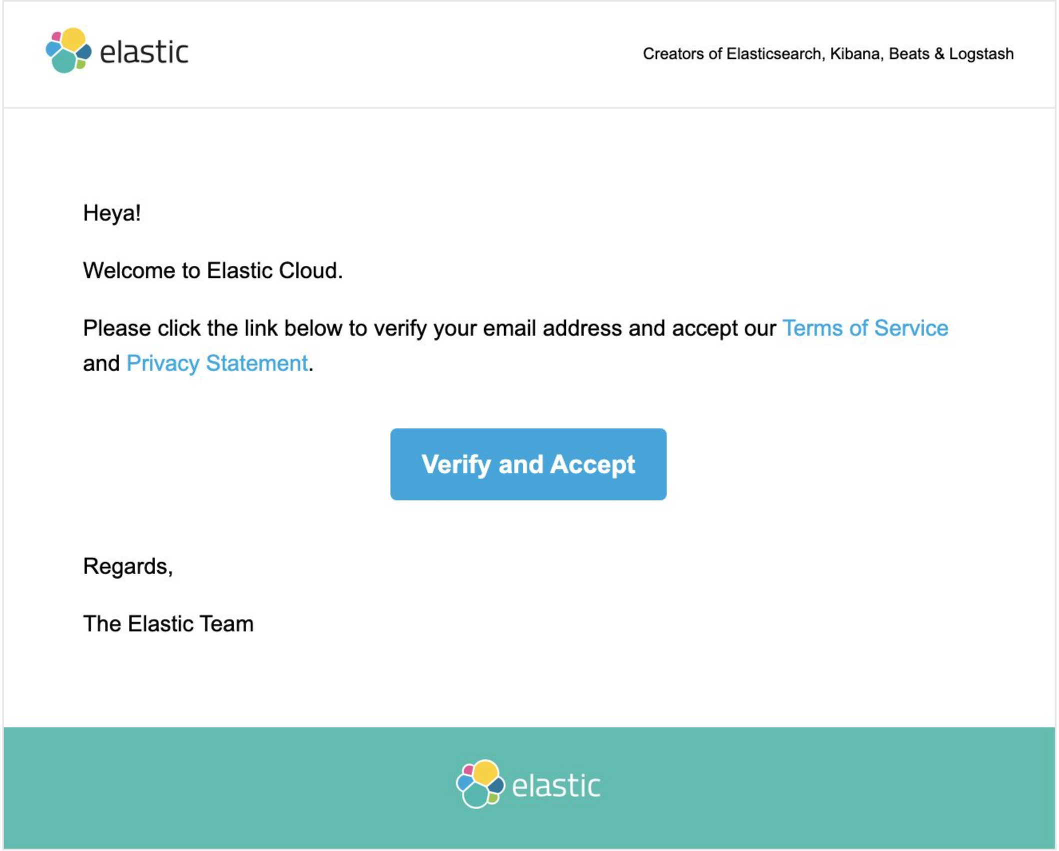
Scroll down to the Resources section & open Free Elastic Cloud Trial link in a new tab.



Go to the email account you signed up with and verify your email.



Click on verify and accept.


elastic

Creators of Elasticsearch, Kibana, Beats & Logstash

Heya!

Welcome to Elastic Cloud.

Please click the link below to verify your email address and accept our Terms of Service and Privacy Statement.

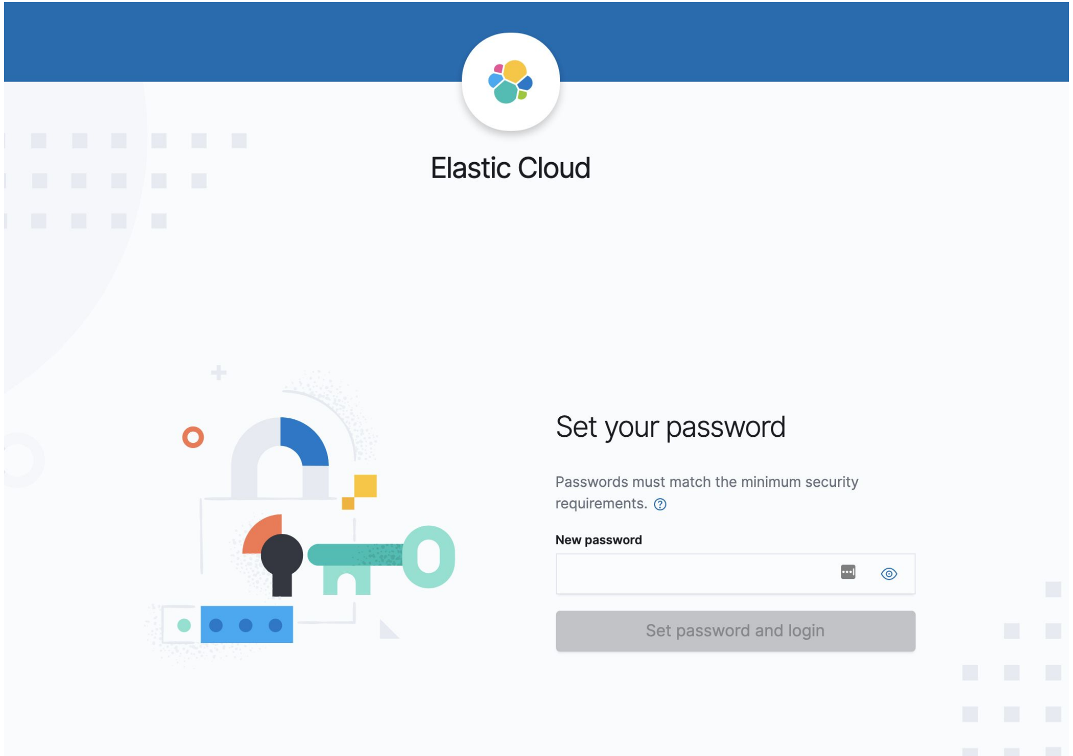
Verify and Accept

Regards,

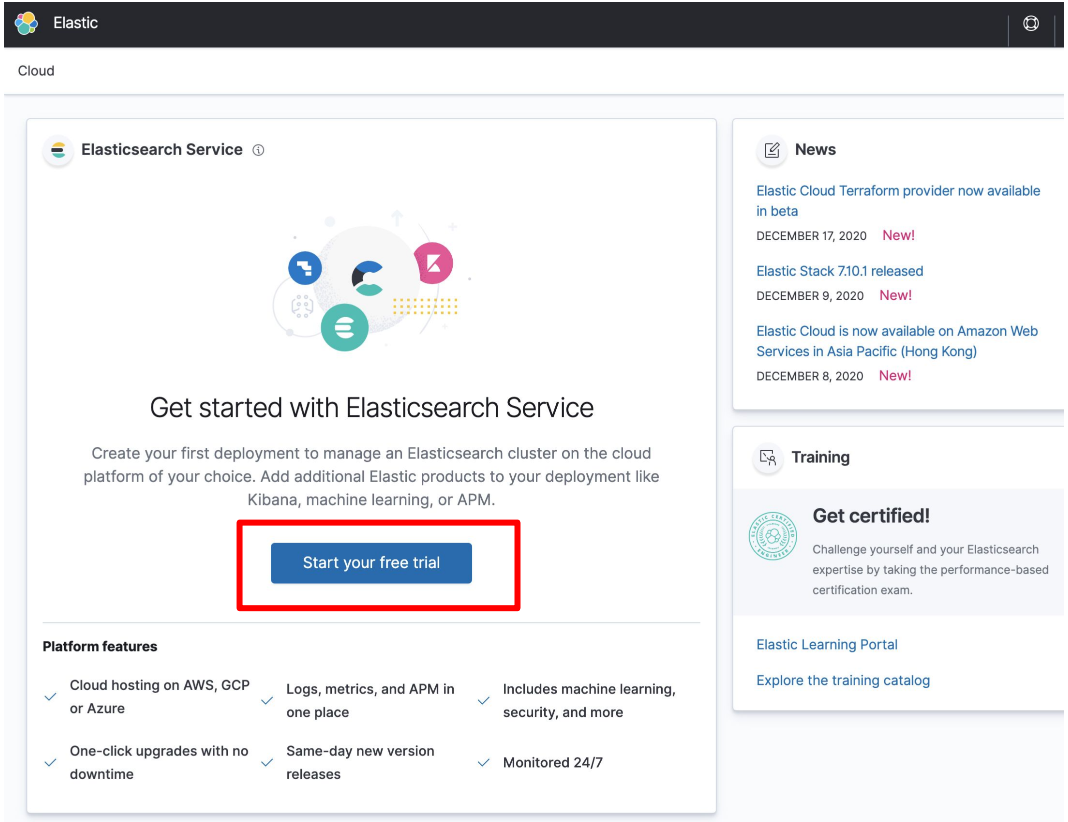
The Elastic Team

elastic

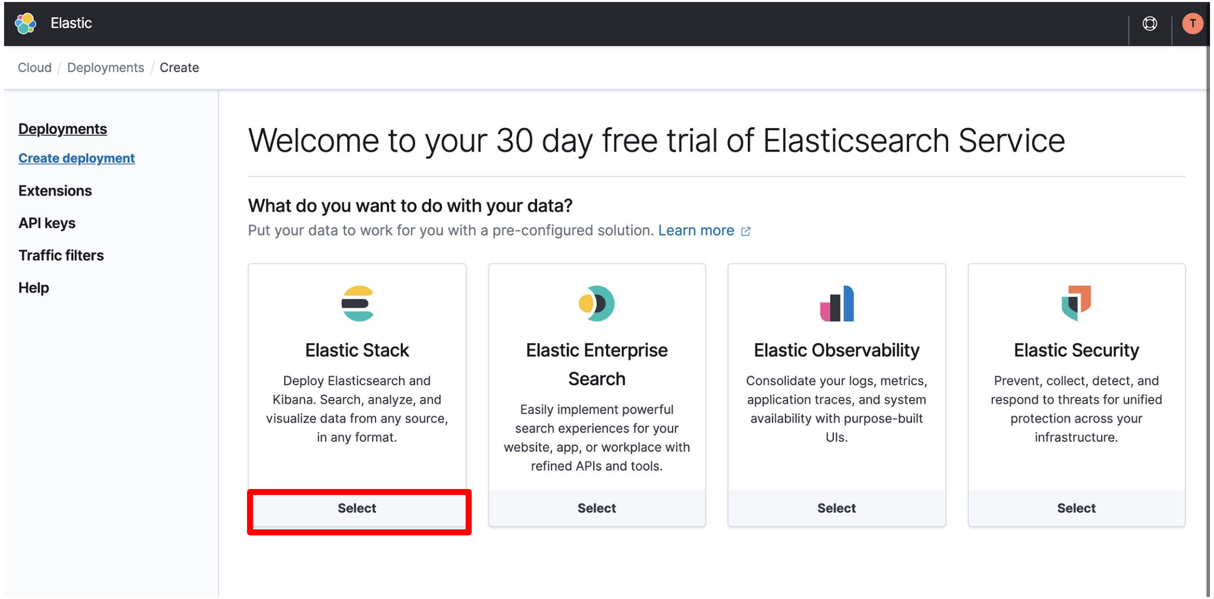
Enter your password.



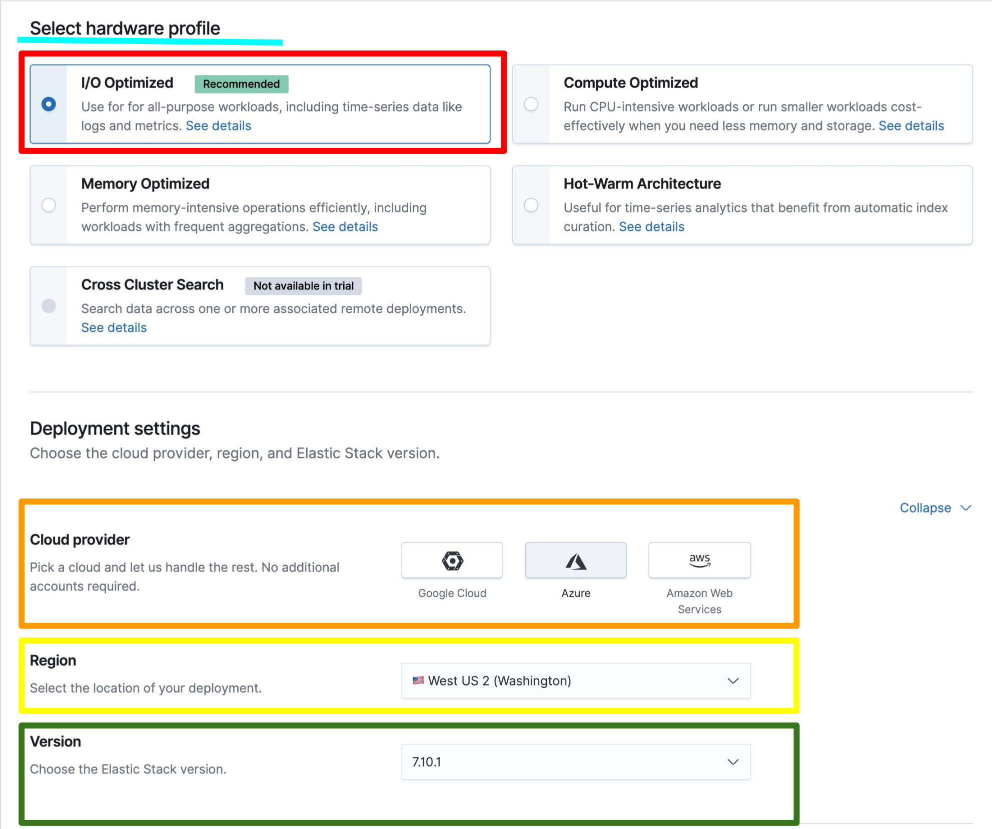
Click on start your free trial.



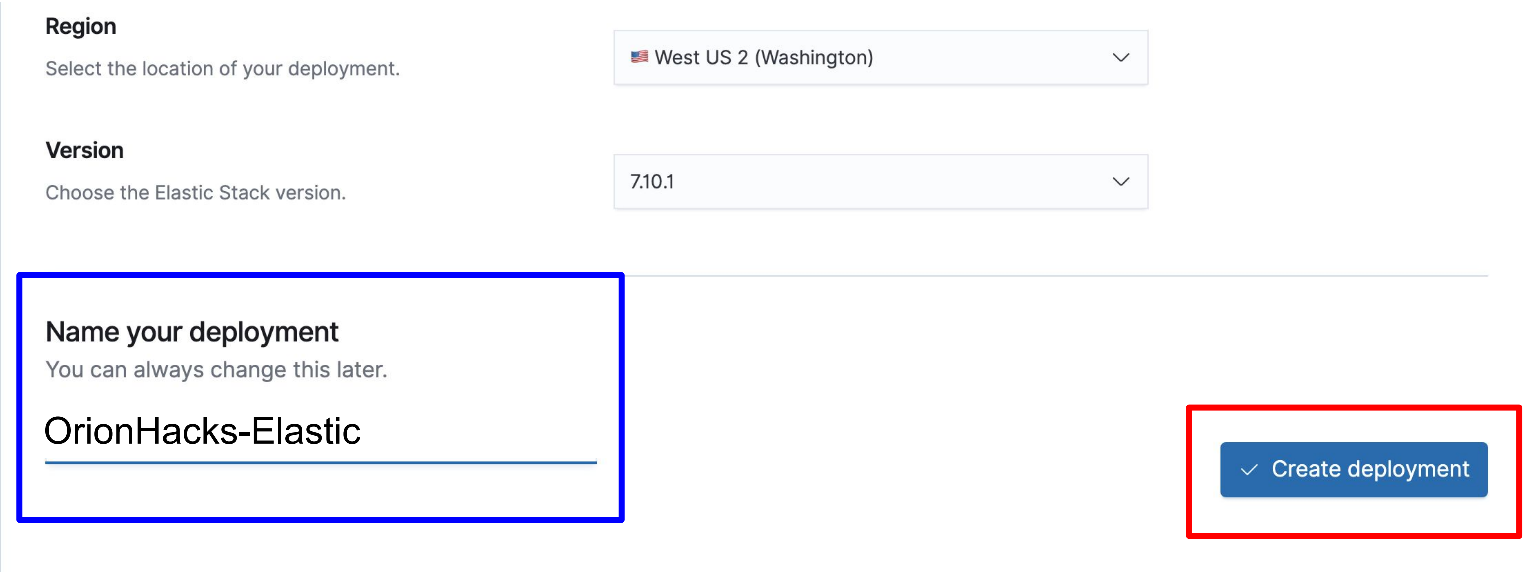
Select the Elastic Stack.



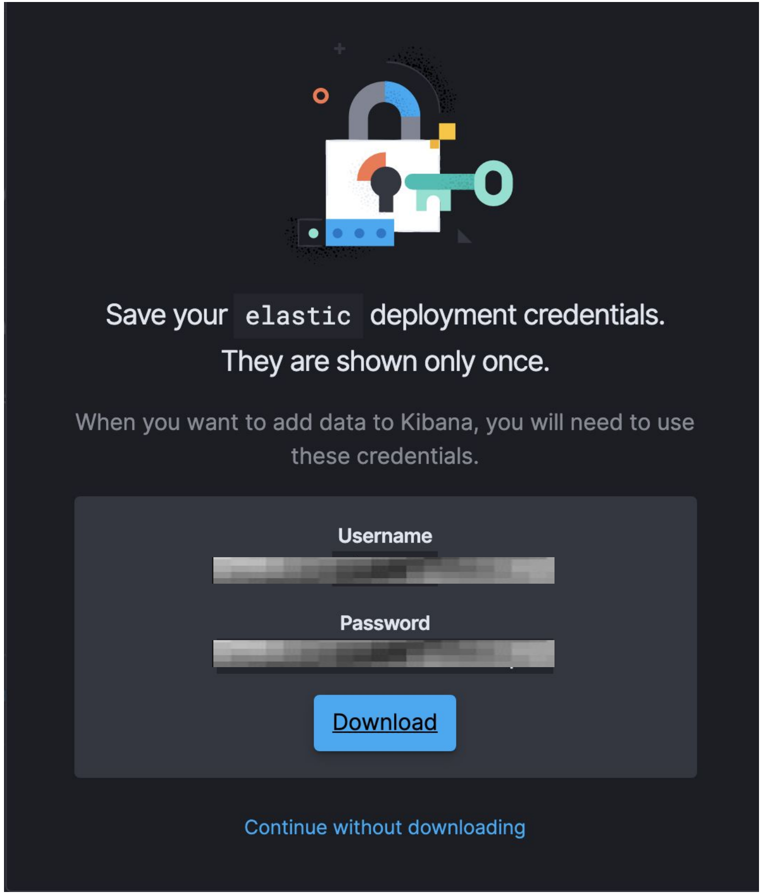
Configure your settings.



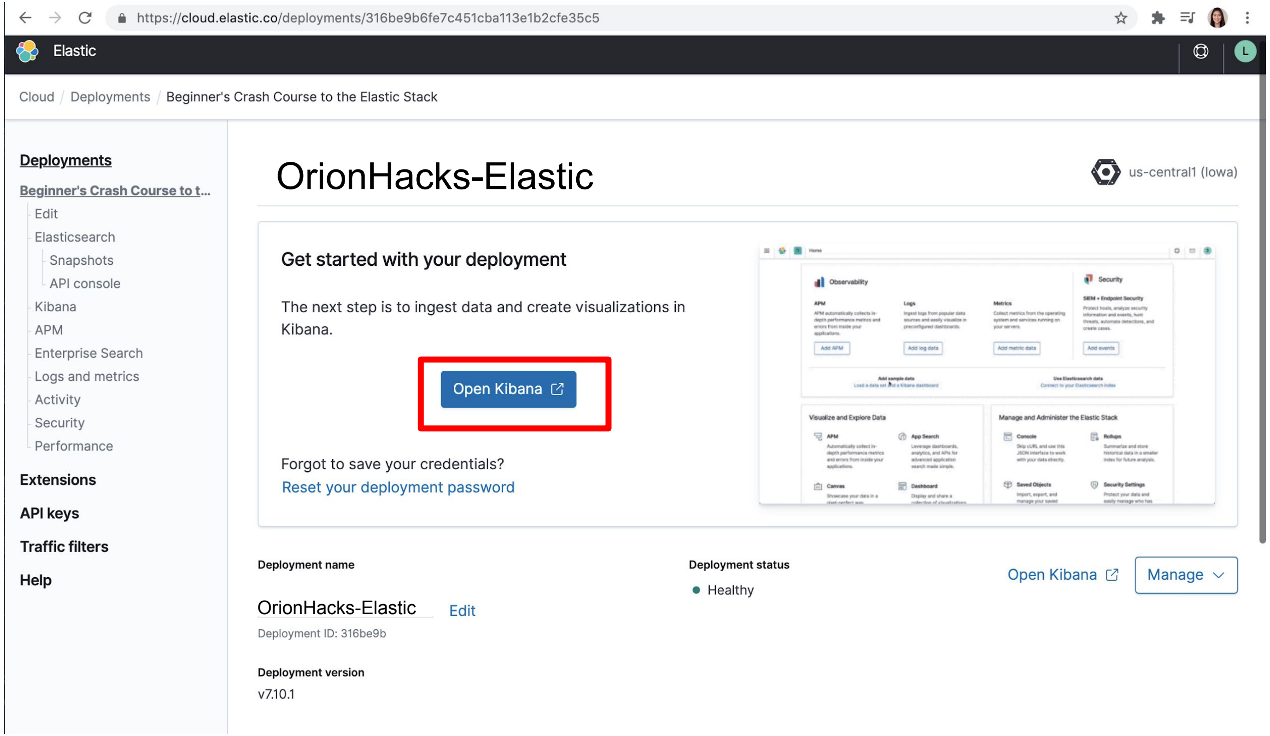
Name your deployment then create deployment.



Save your deployment credentials.

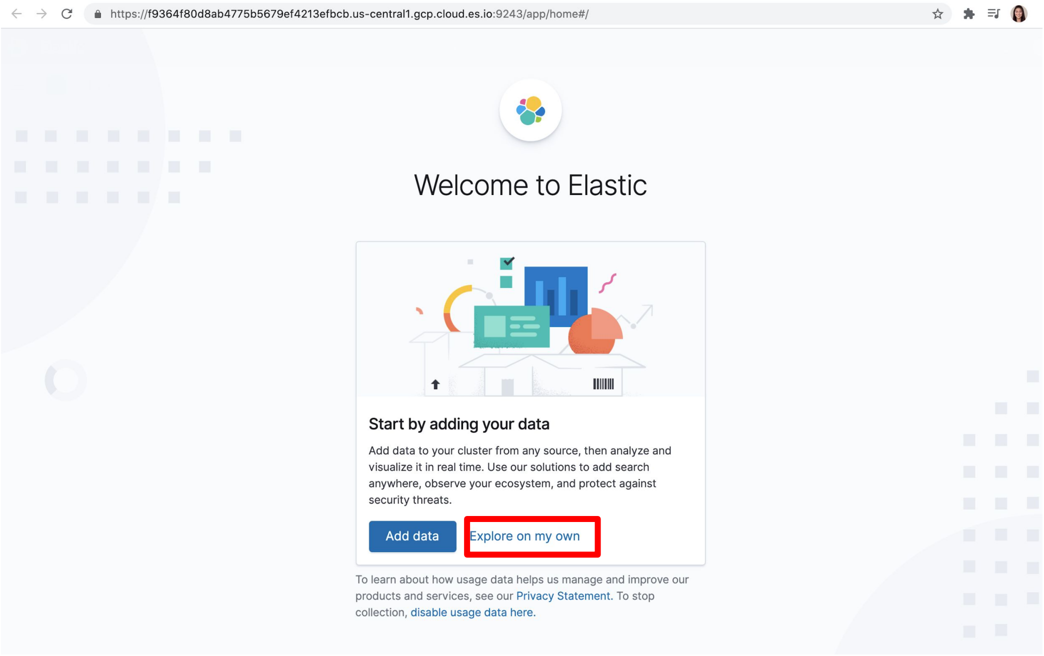


Open Kibana.

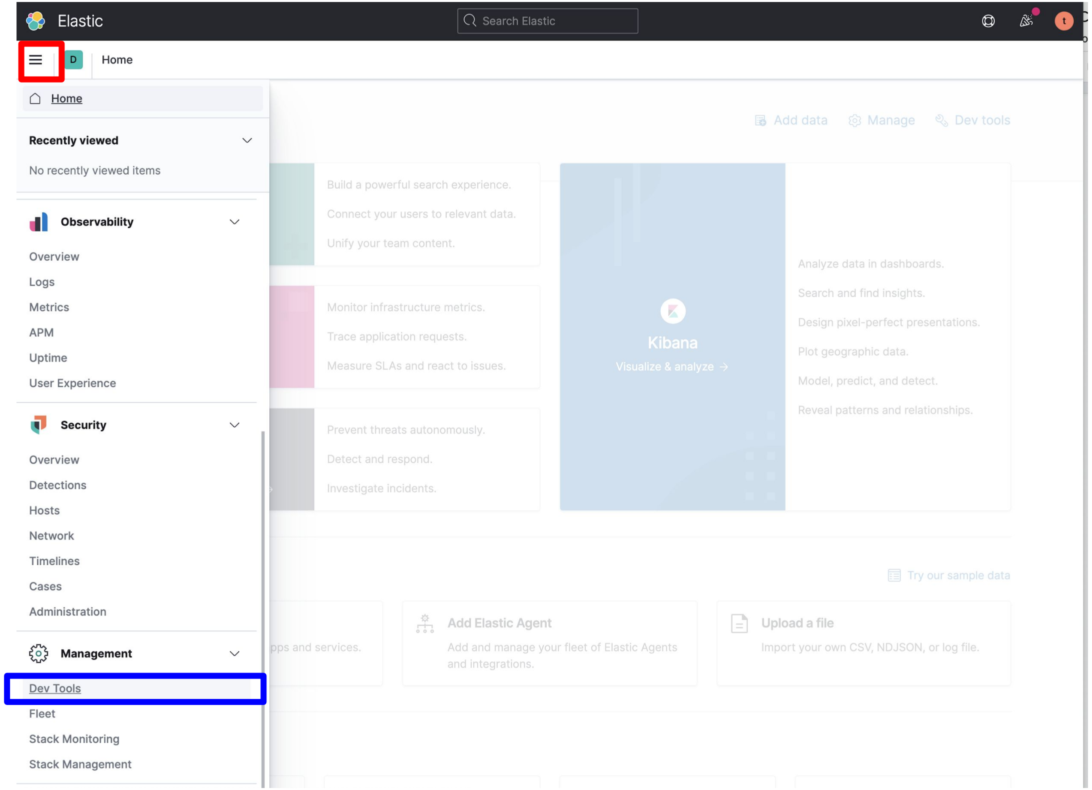


https://cloud.elastic.co/deployments/316be9b6fe7c451cba113e1b2cfe35c5
Elastic
Cloud / Deployments / Beginner's Crash Course to the Elastic Stack
Deployments
Beginner's Crash Course to t...
Edit
Elasticsearch
Snapshots
API console
Kibana
APM
Enterprise Search
Logs and metrics
Activity
Security
Performance
Extensions
API keys
Traffic filters
Help
OrionHacks-Elastic
us-central1 (Iowa)
Get started with your deployment
The next step is to ingest data and create visualizations in Kibana.
Open Kibana
Forgot to save your credentials?
Reset your deployment password
Deployment name
OrionHacks-Elastic
Edit
Deployment ID: 316be9b
Deployment version
v7.10.1
Deployment status
Healthy
Open Kibana
Manage

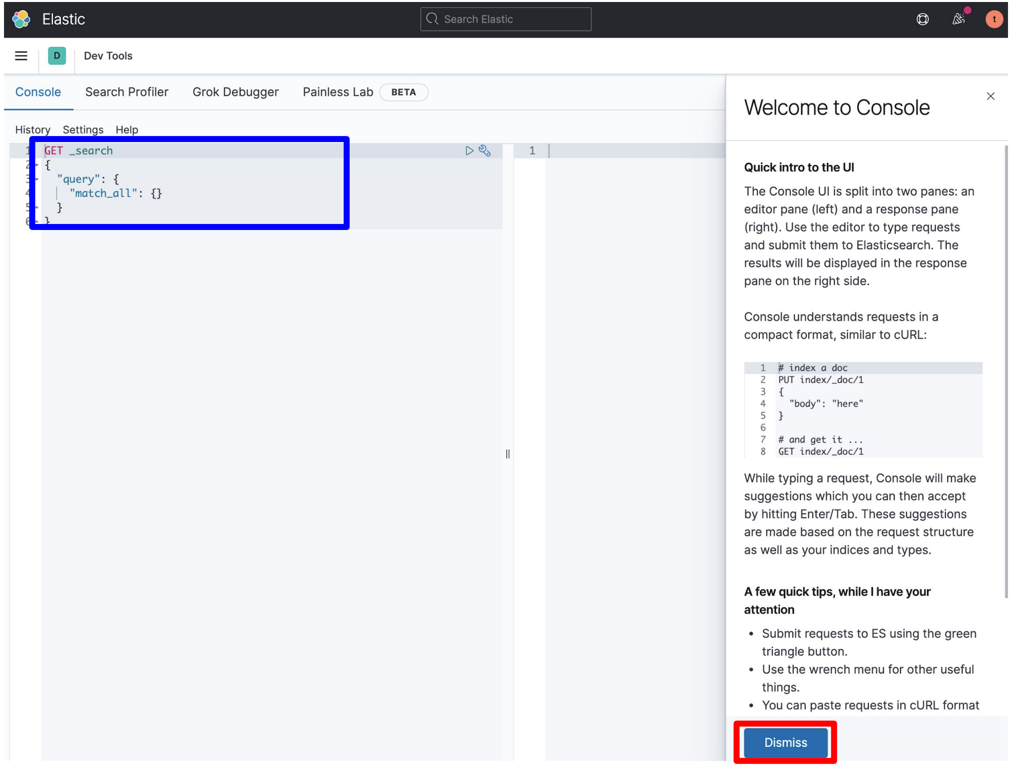
Click on Explore on my own option.

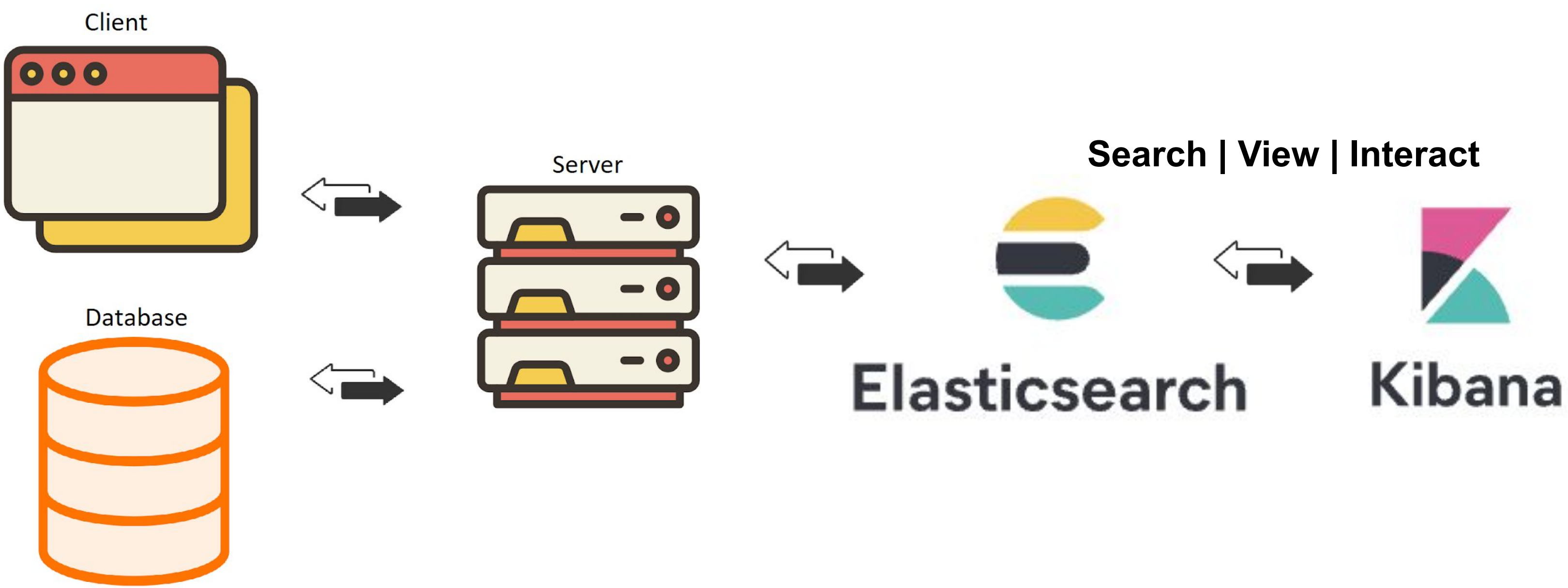


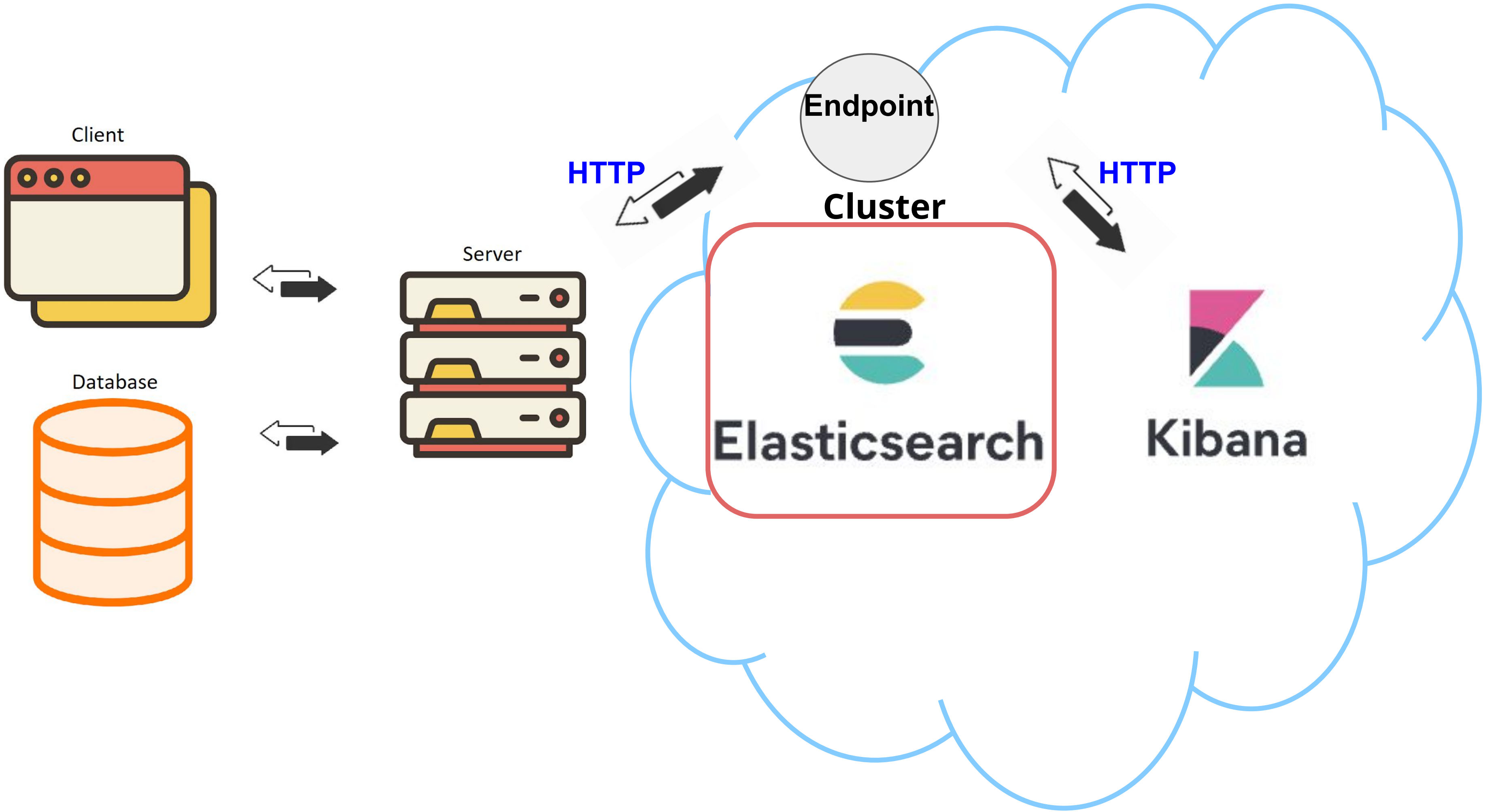
Click on menu icon, and open Dev Tools.



Click on Explore on my own option.

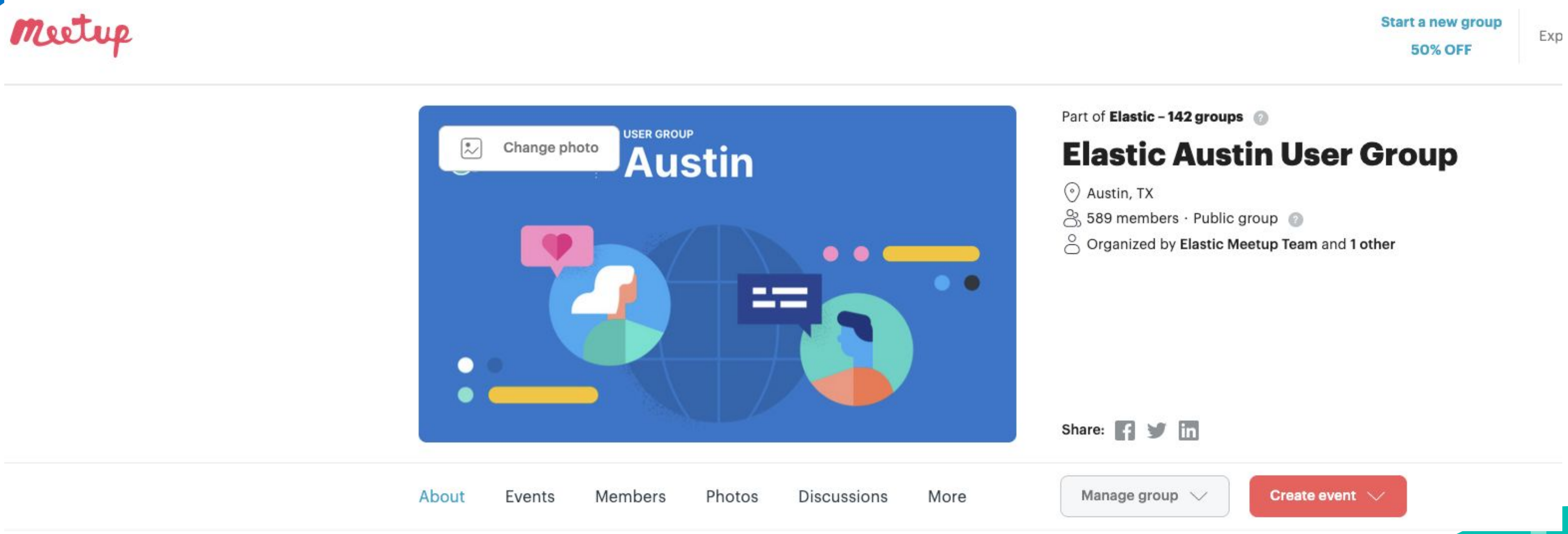



Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana


Client
Database
Server
HTTP
Endpoint
Cluster
HTTP
Elasticsearch
Kibana

Questions?

Join the Elastic Austin User Group for updates on future workshops!



Lisa Jung

Developer Advocate @Elastic

E-mail: lisa.jung@elastic.co

Discussion forum: https://discuss.elastic.co/

Blog: https://dev.to/lisahjung

Twitter: @LisaHJung

SCAN ME