Vancouver Meetup:

Beginner's Crash Course to the Elastic Stack Series

Part 1: Intro to Elasticsearch and Kibana

Lisa Jung
Developer Advocate @Elastic

Connect with the Elastic Community

Find your local User Group:

- https://community.elastic.co/

Virtual User Group:

https://community.elastic.co/amer-virtual/

Connect with the Elastic Community

Community Slack Workspace:

https://join.slack.com/t/elasticstack/shared_invite/zt-an1h0etg-04FI2hA9vvASBkYPe~QZmw

Vancouver Meetup:

Beginner's Crash Course to the Elastic Stack Series

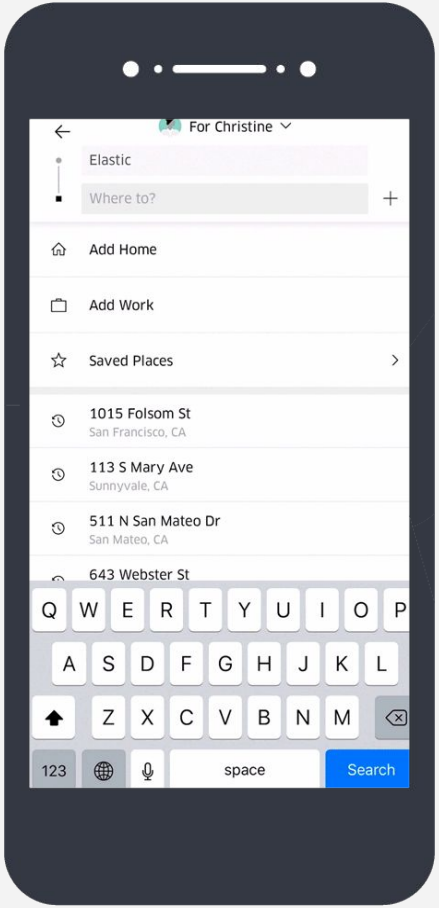
Part 1: Intro to Elasticsearch and Kibana

Lisa Jung
Developer Advocate @Elastic

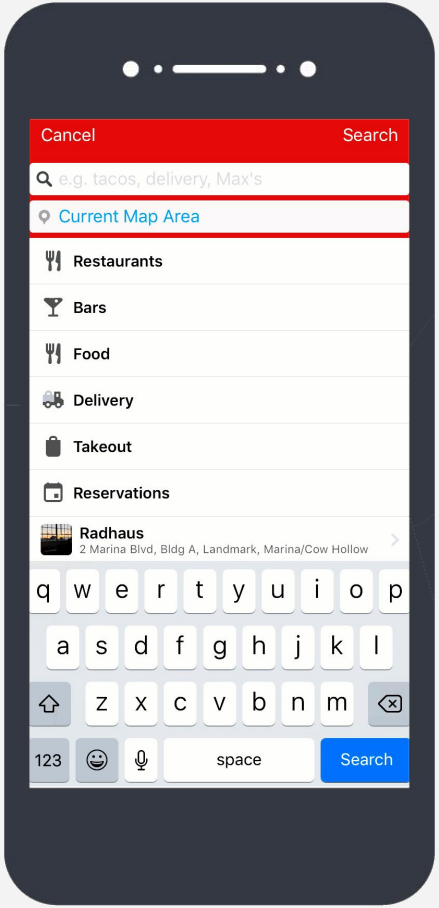
Have you ever used the Elastic Stack before?

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

elastic



Searching for **Rides**

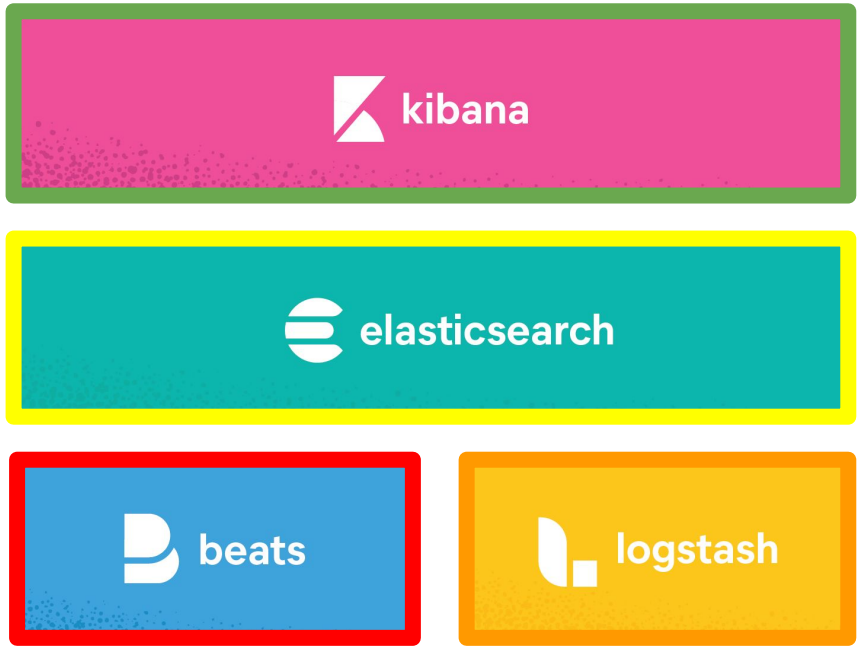


Searching for Restaurants

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

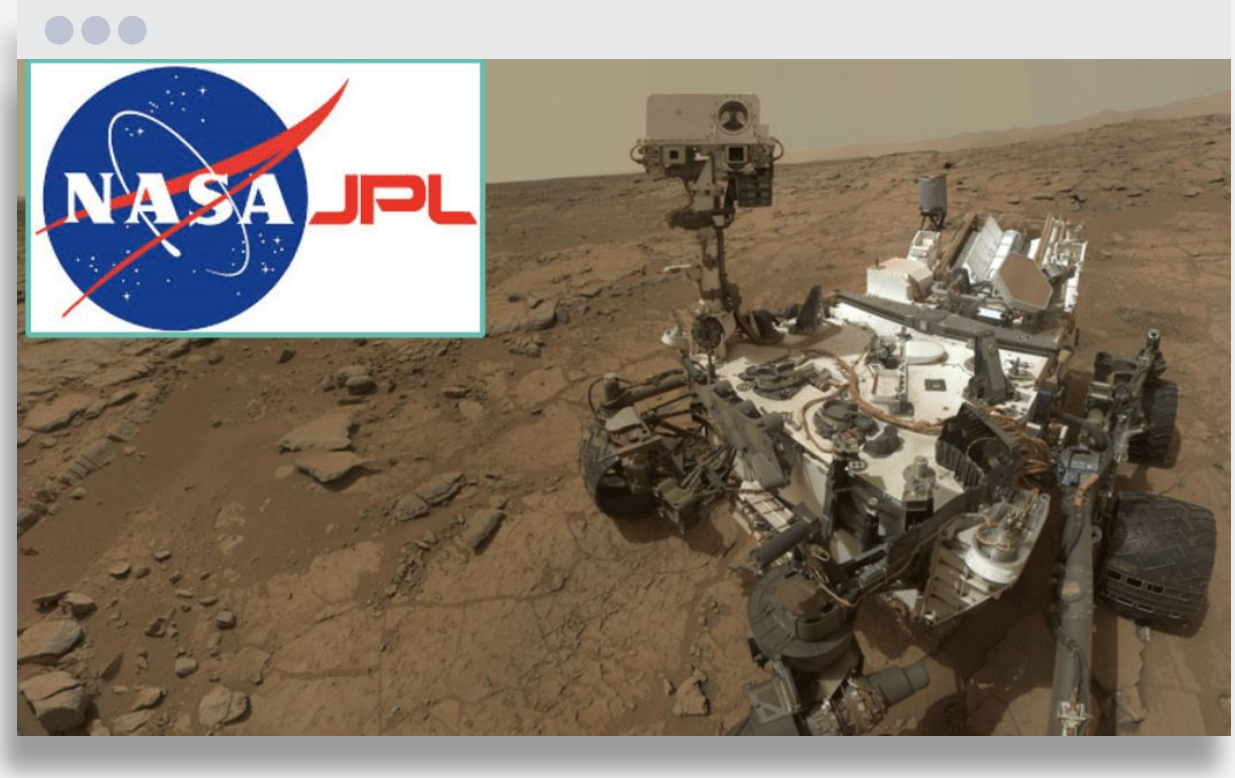
Use Case: Logging

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

ACTIVISION BLIZZARD

elastic

Use Case: Metrics

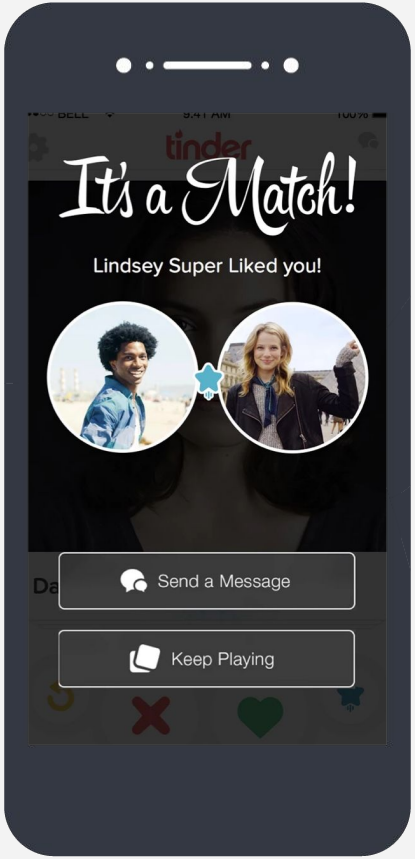


elastic

Use Case: Security Analytics

elastic

Use Case: Business Analytics

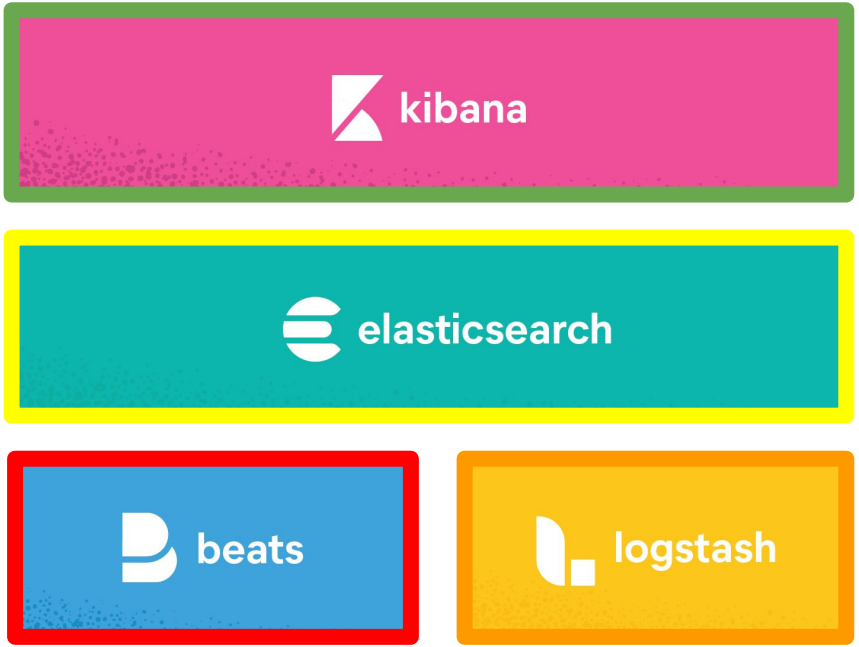


tinder™

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 the Elastic Stack Series

Part 1.1: Intro to Elasticsearch and Kibana

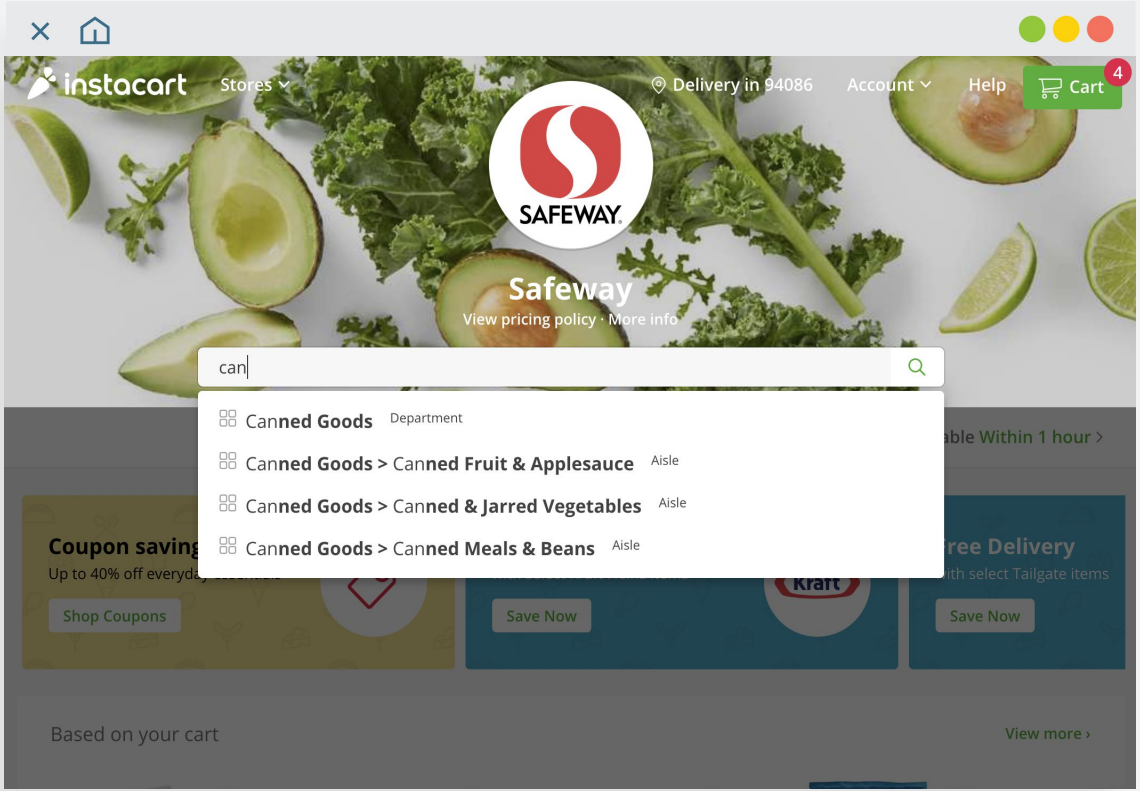
By the end of this workshop, you will be able to:

- 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

Elasticsearch

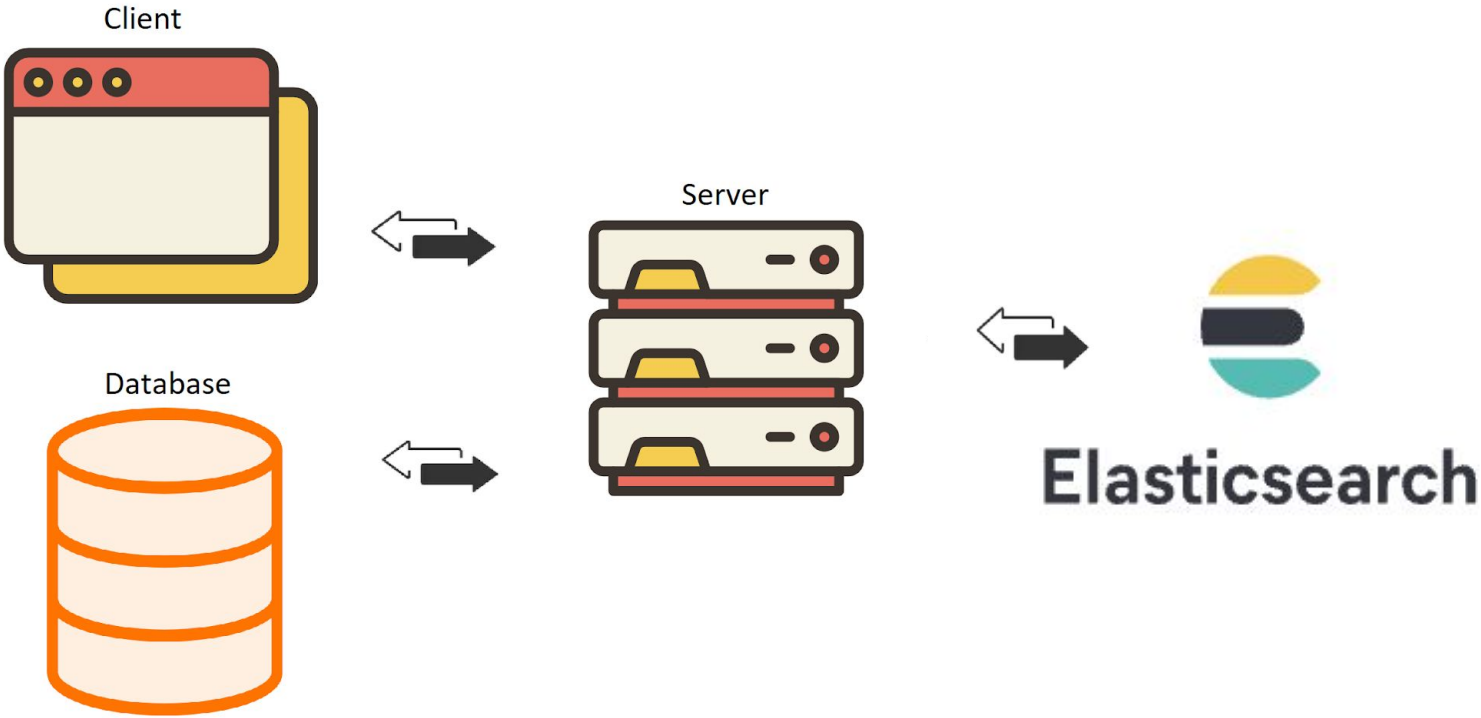
Store | Search | Analyze

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



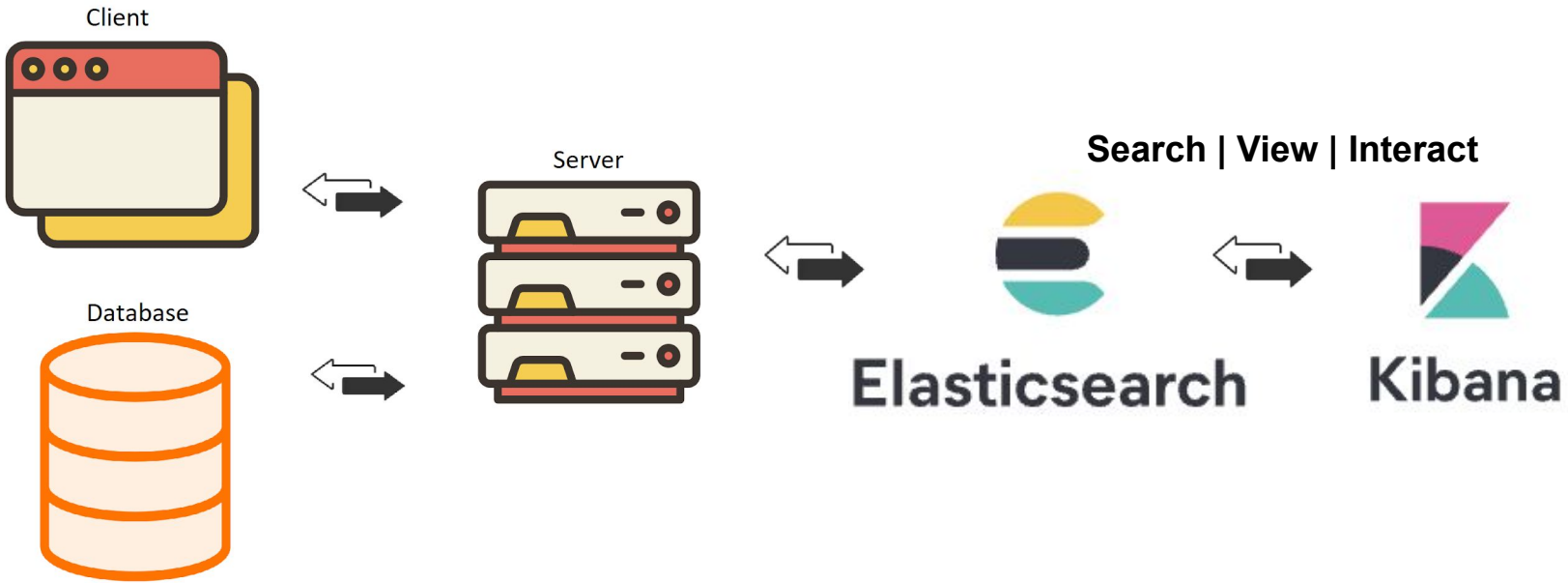
Find me a list of peanut butter brands. I want highest rated brands at the top.

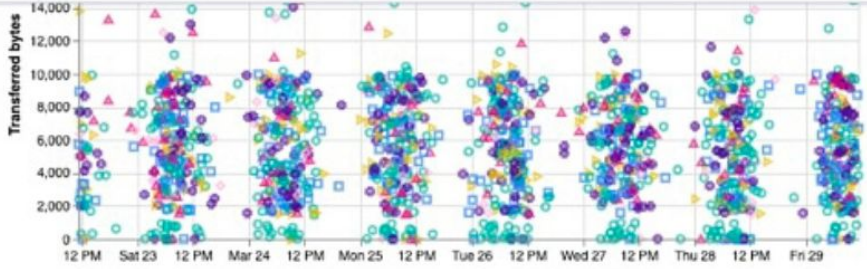
Find me a hot sauce named uh… I think it is spelled Sriracha? Maybe it's spelled Srirracah? Srirracha?


Client
Server
Database
Elasticsearch

Elasticsearch

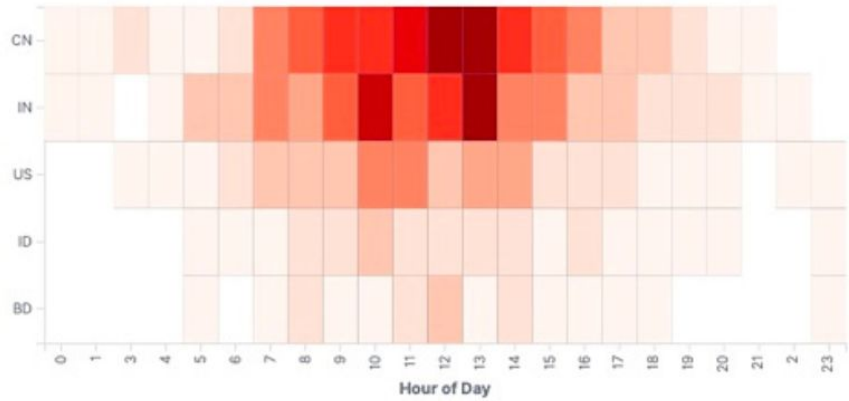
Store | Search | Analyze


Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana

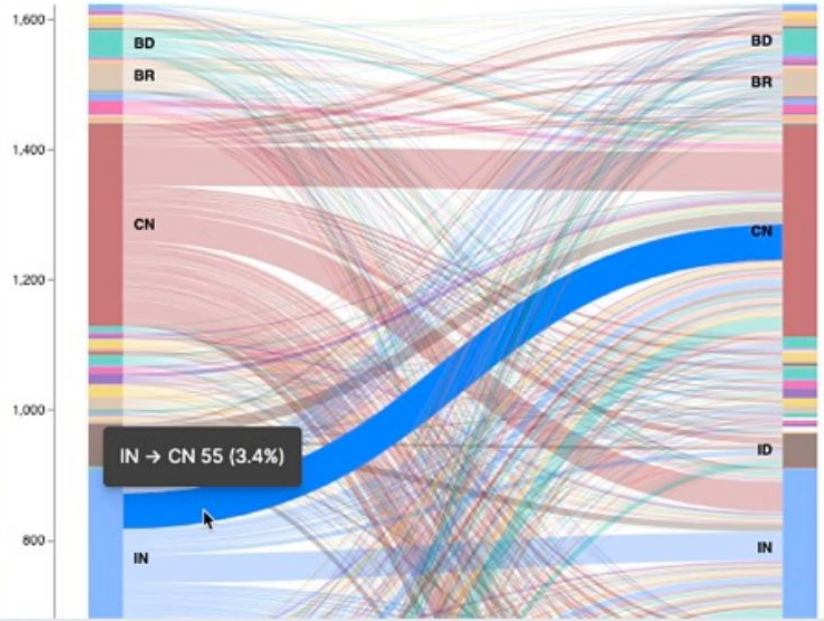


gz	1.594MB	34.493KB	283	7
css	1.385MB	12.378KB	270	2
zip	1.257MB	6.654KB	212	3
deb	1.085MB	6.844KB	173	1
rpm	458.989KB	0B	71	0

[Logs] Heatmap



[Vega] Source and Destination Sankey Chart



[Logs] Unique Visitors by Country

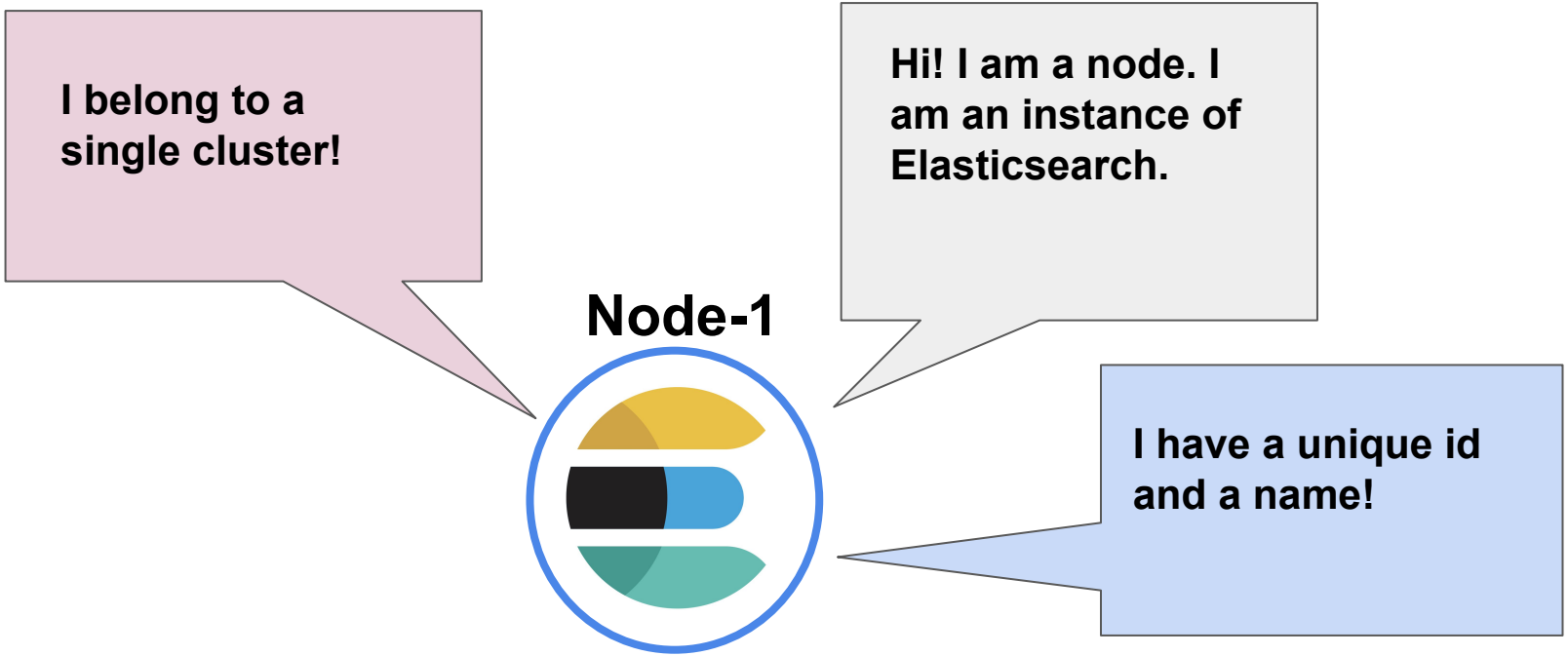
By the end of this workshop, you will be able to:

- 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

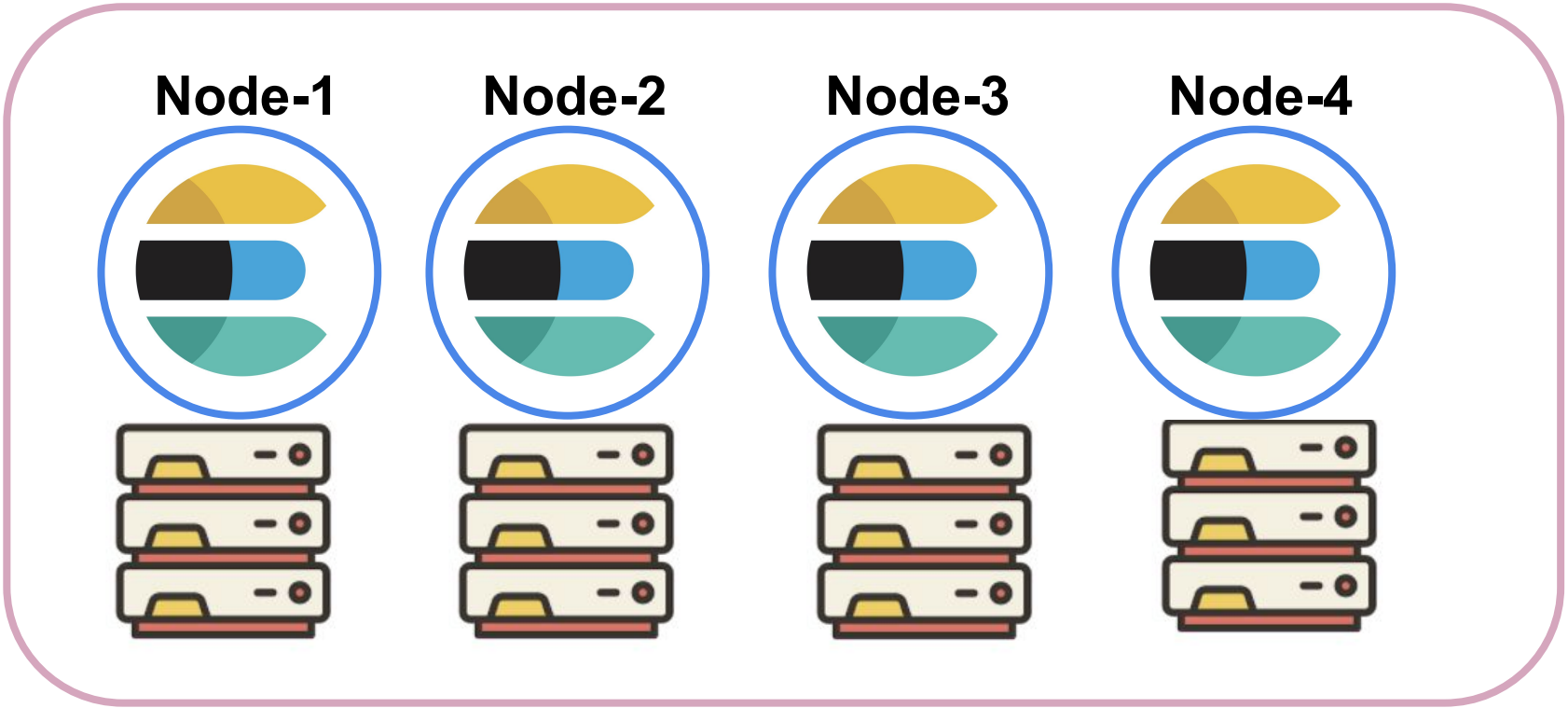
Elasticsearch

Store | Search | Analyze

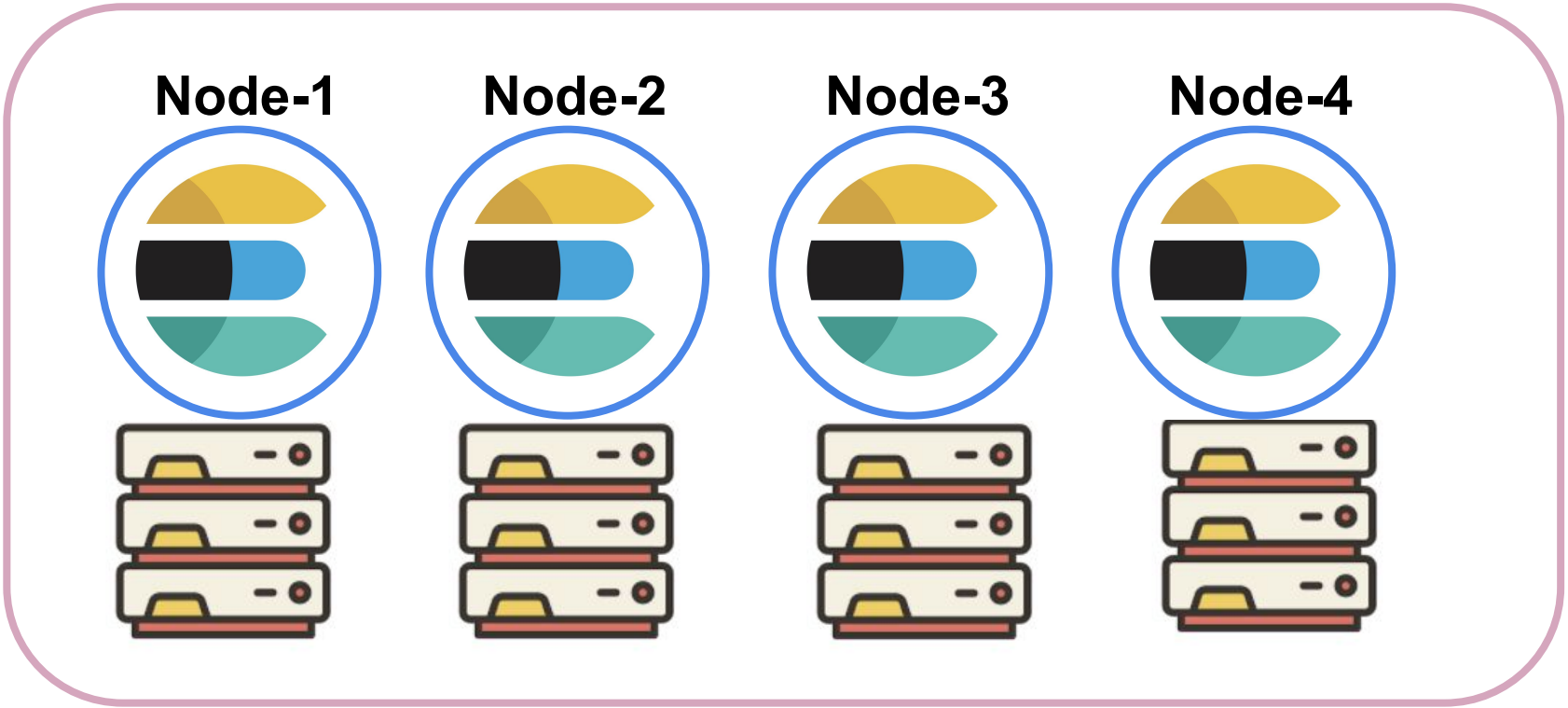
Cluster


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 in Elasticsearch!

```
{
"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!

elastic

Documents are grouped into an index!

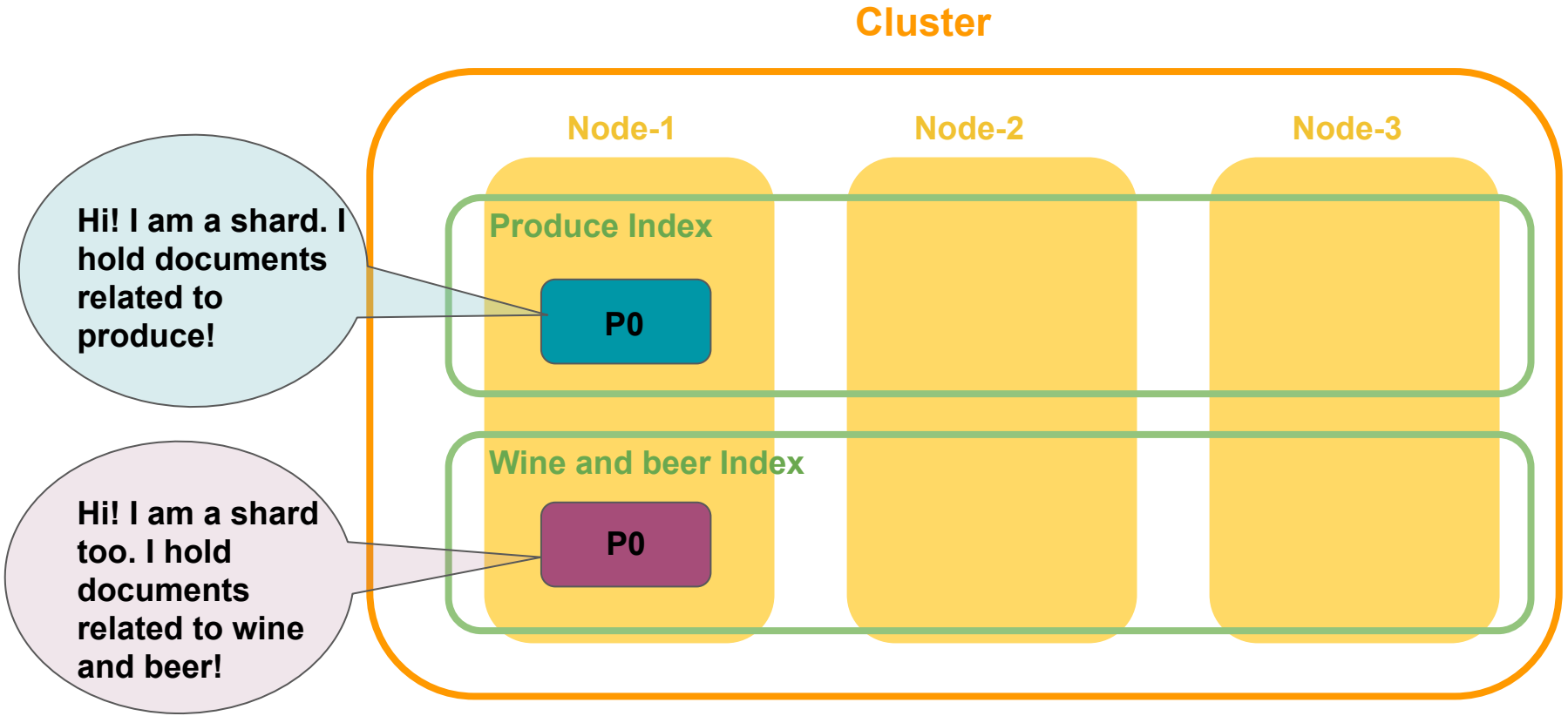
Produce Index


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

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

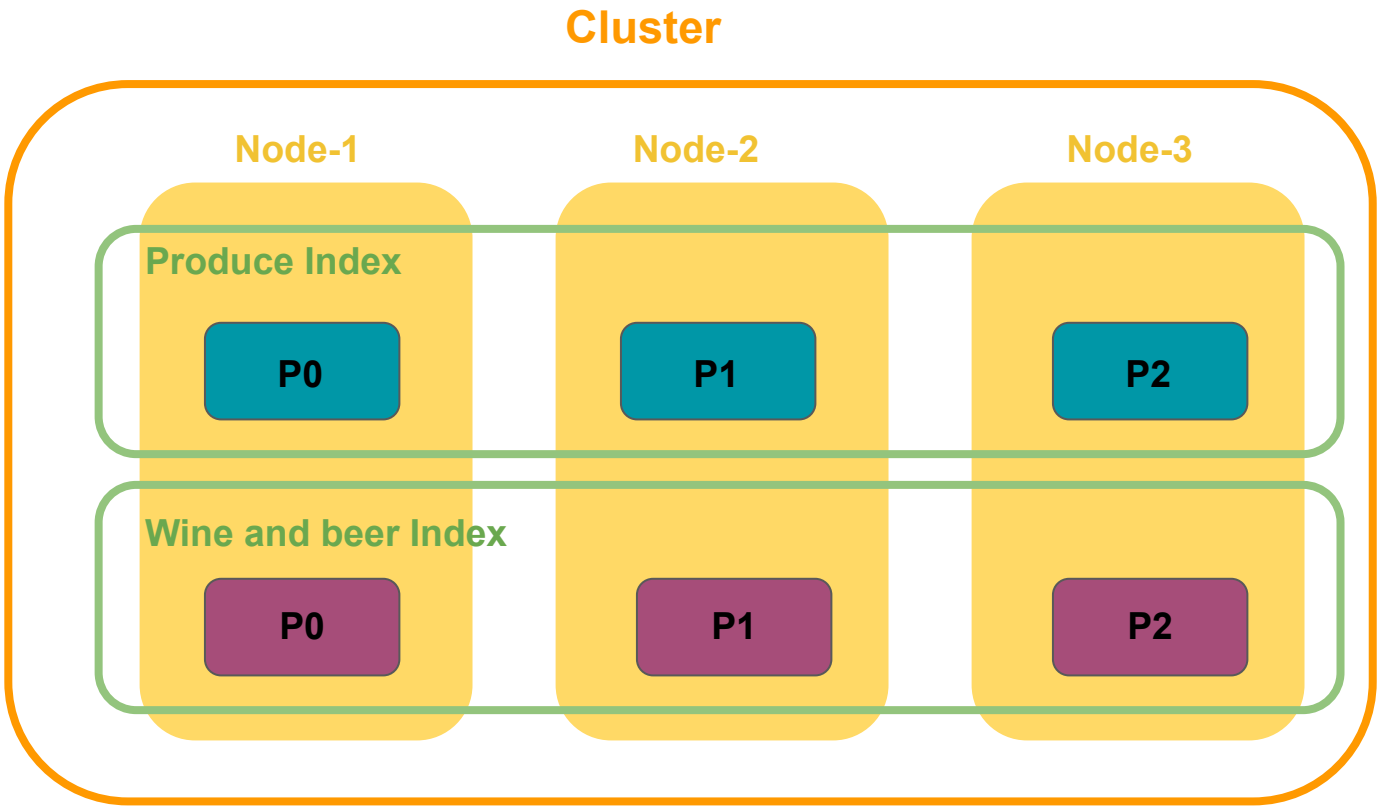

Wine & Beer Index


```
{
"name": "Unanime Malbec(750ml)",
"brand": "Mascota Vineyards",
"country": "Argentina",
"region": "Mendoza",
"wine_type": "Red Wine",
"ABV": "14%",
"price": "$22.99"
}

{
"name": "Hazy Little Thing IPA(750ml)",
"country": "US",
"state": "California",
"beer_type": "Ale",
"beer_style": "India Pale Ale",
"ABV": "6.7%",
"price": "$14.99"
}
```

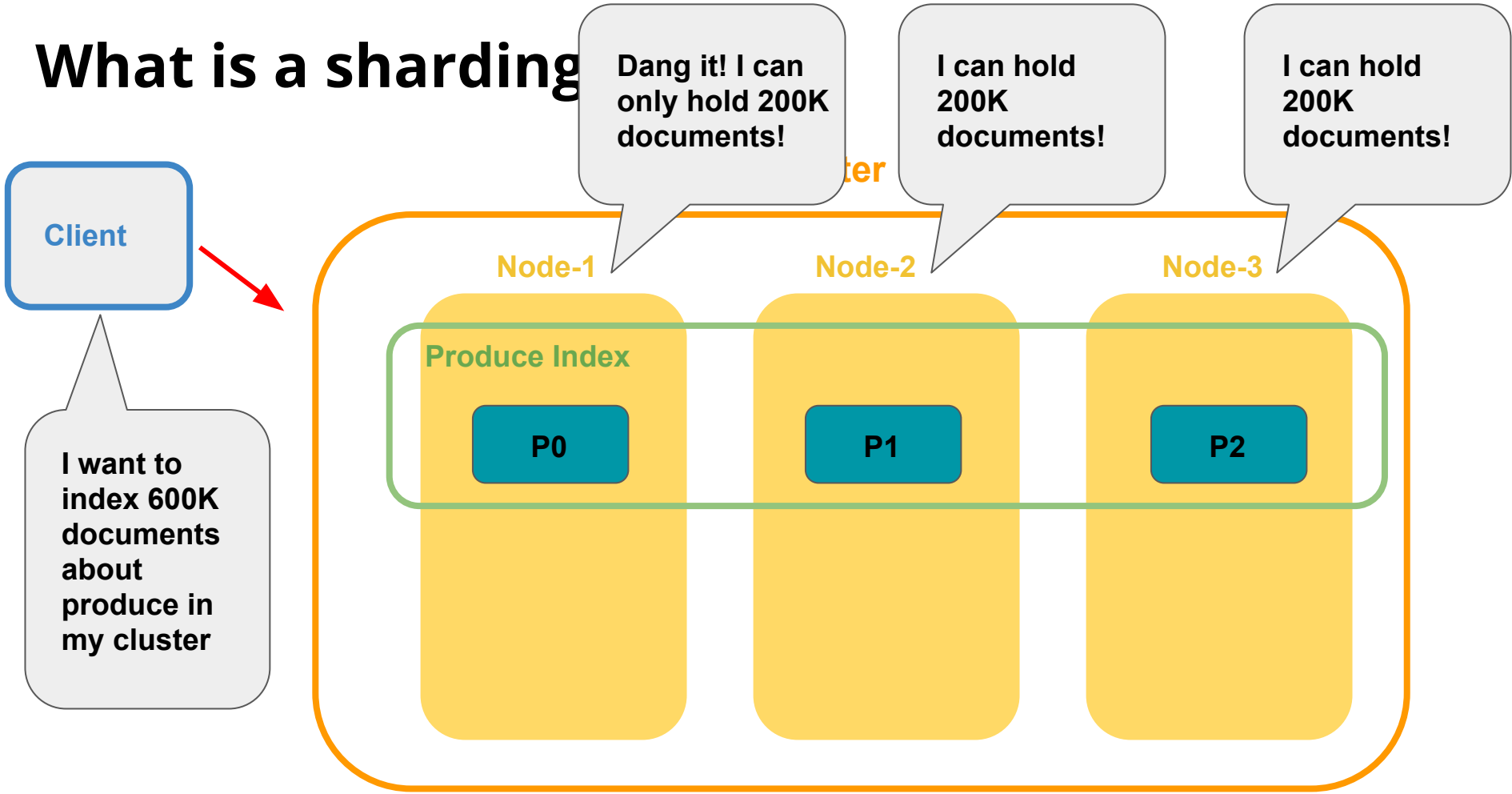
What is a shard?



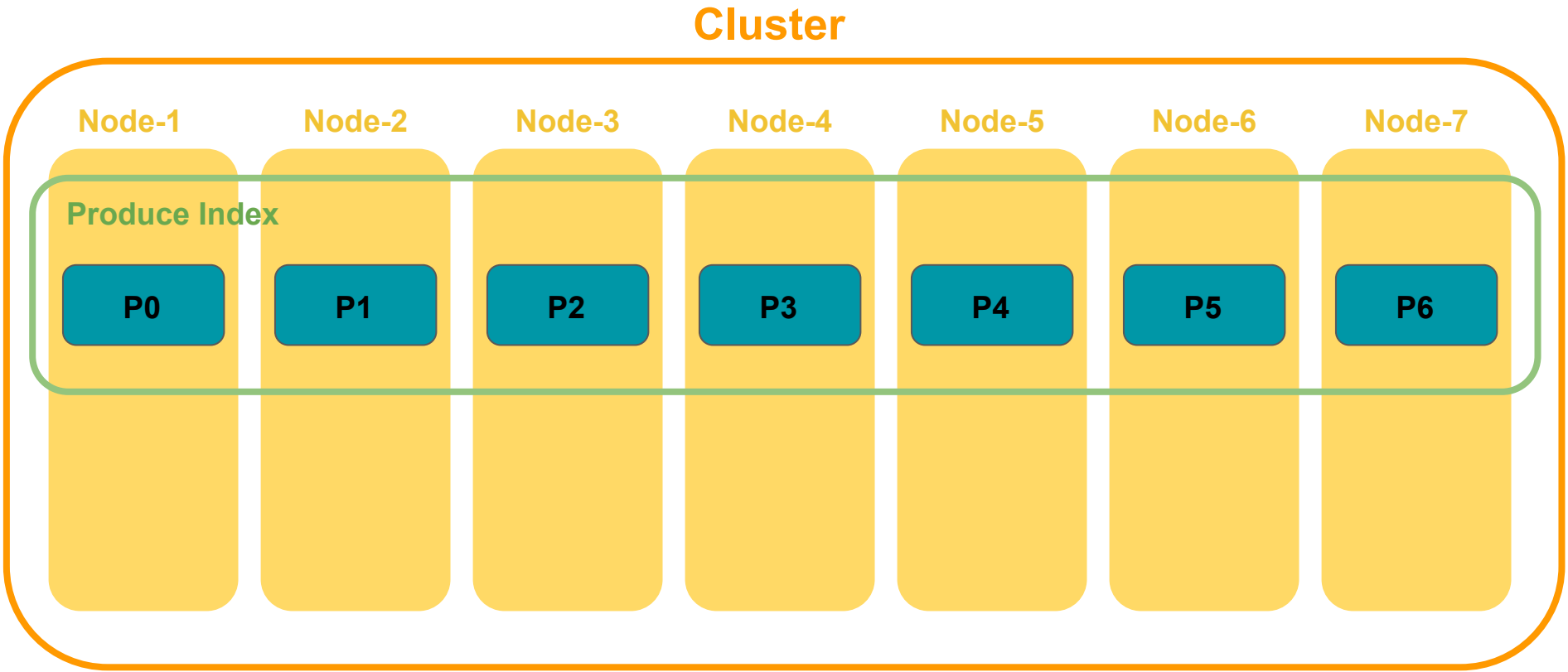
What is a sharding?



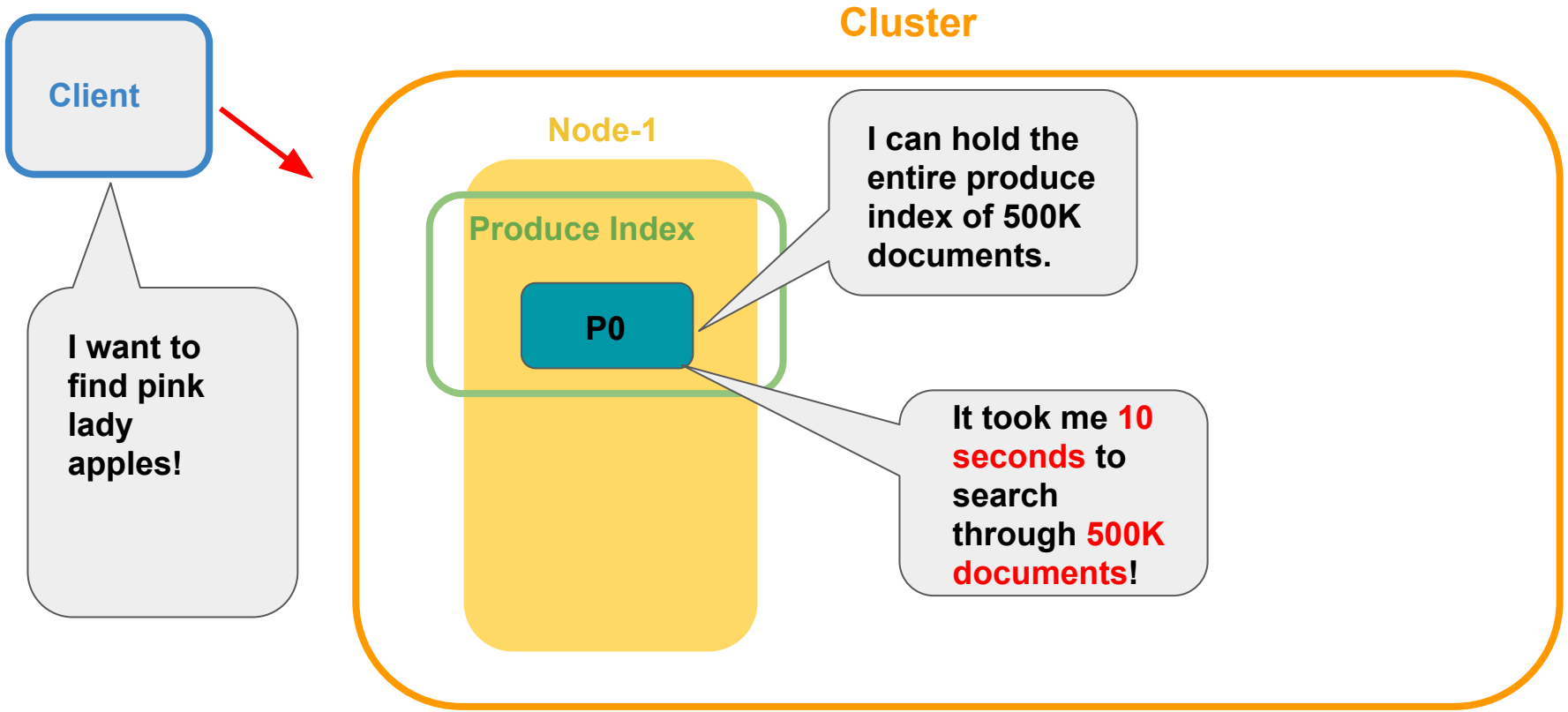
What is a sharding



What is a sharding?



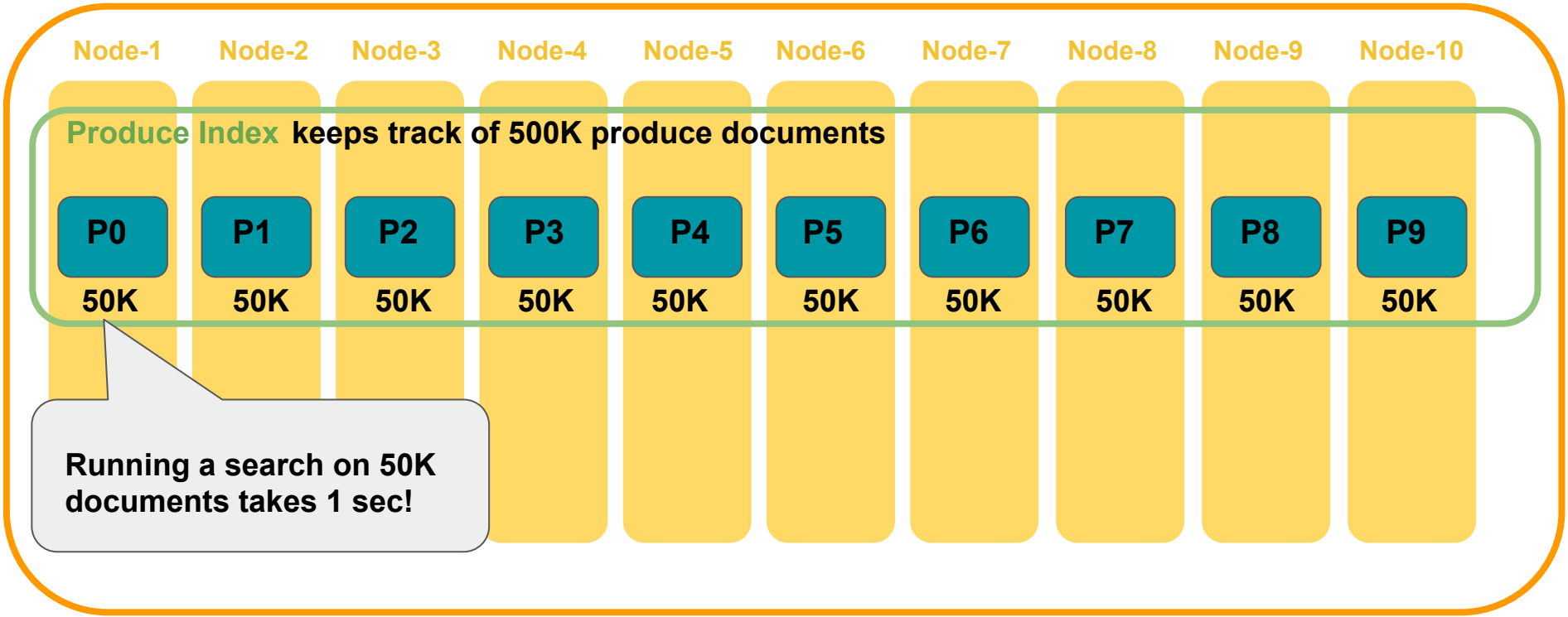
What is a sharding?



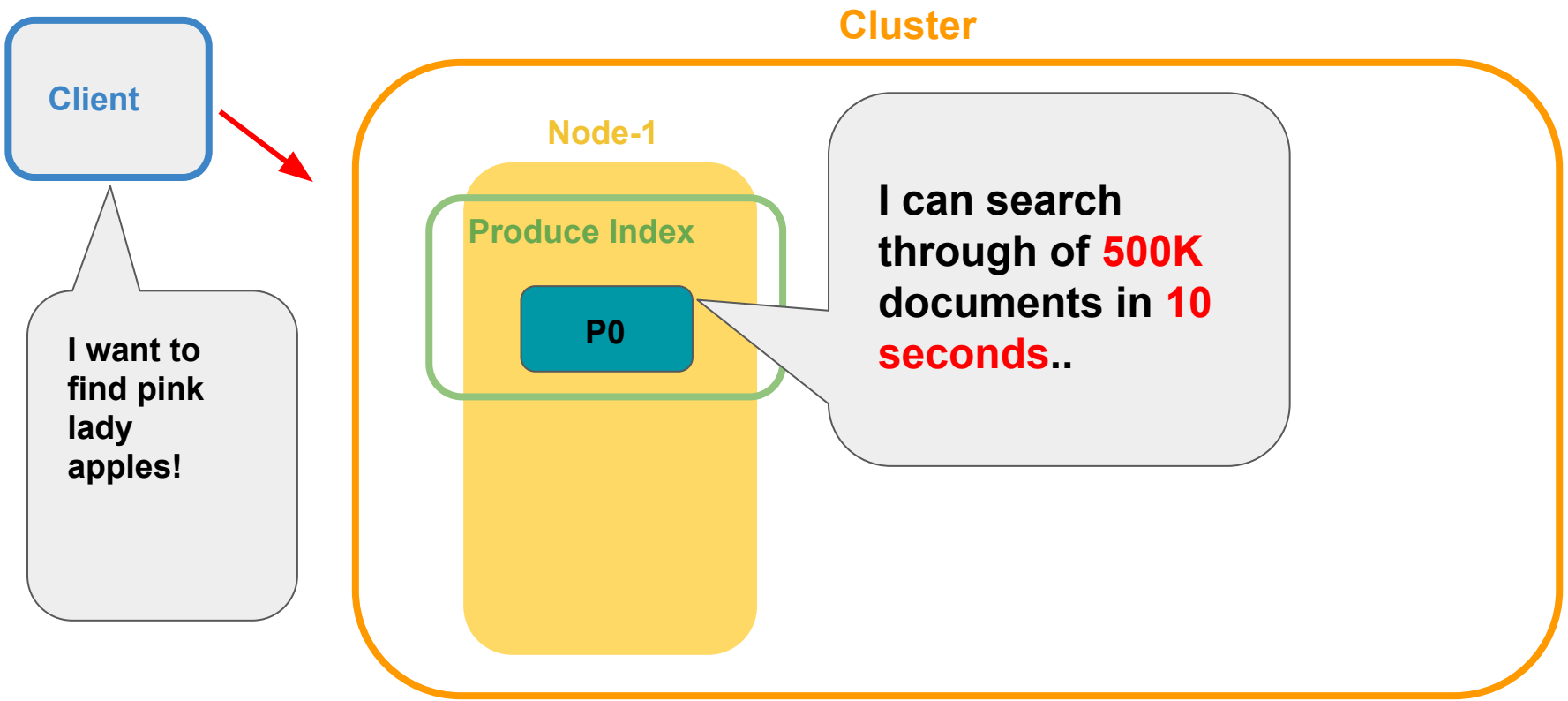
Sharding speeds up your search!

We can search through 500K documents in 1 second!

Cluster



What is a sharding?



Sharding speeds up your search!

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

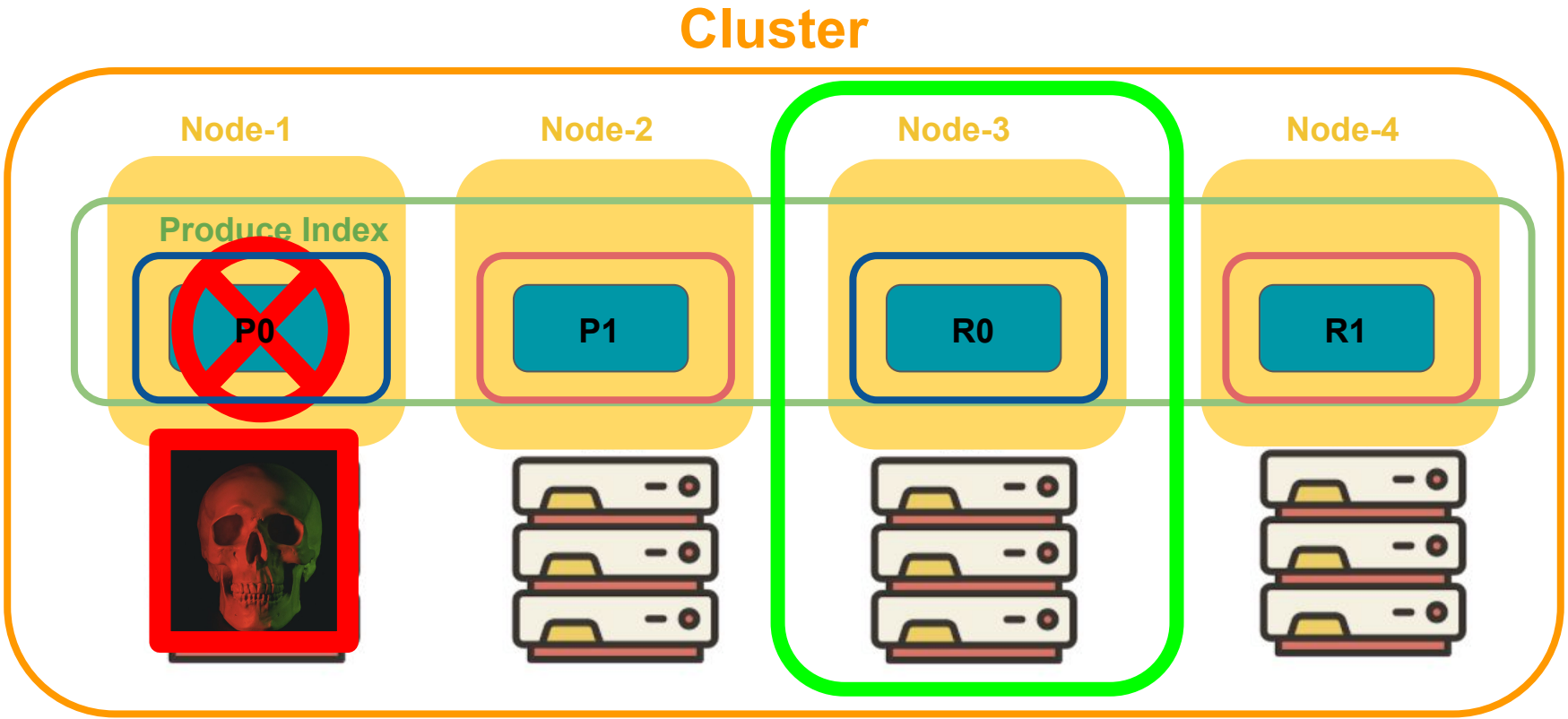
Produce Index

P0 P1 P2 P3 P4 P5 P6 P7 P8 P9

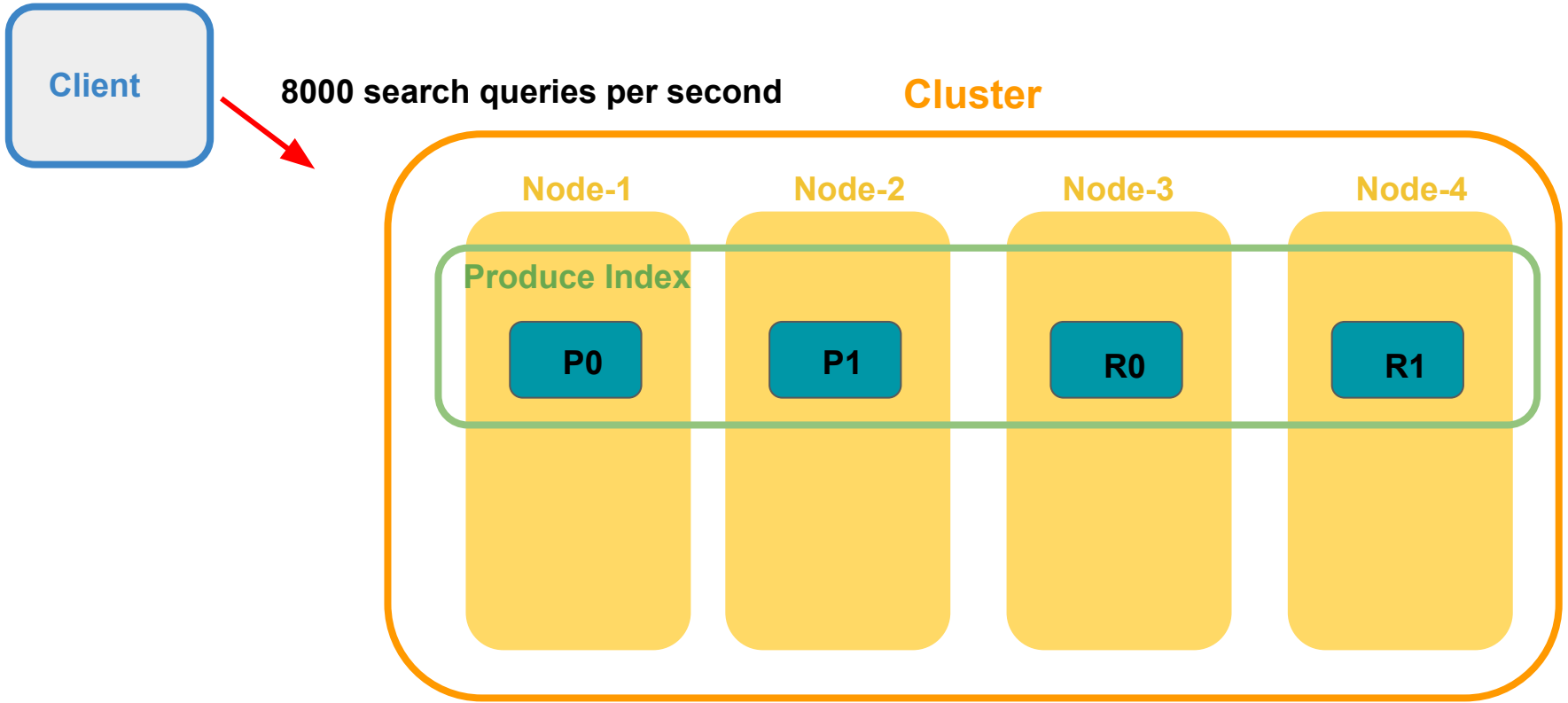
50K 50K 50K 50K 50K 50K 50K 50K 50K 50K


#SPONGEBOBMOVIE

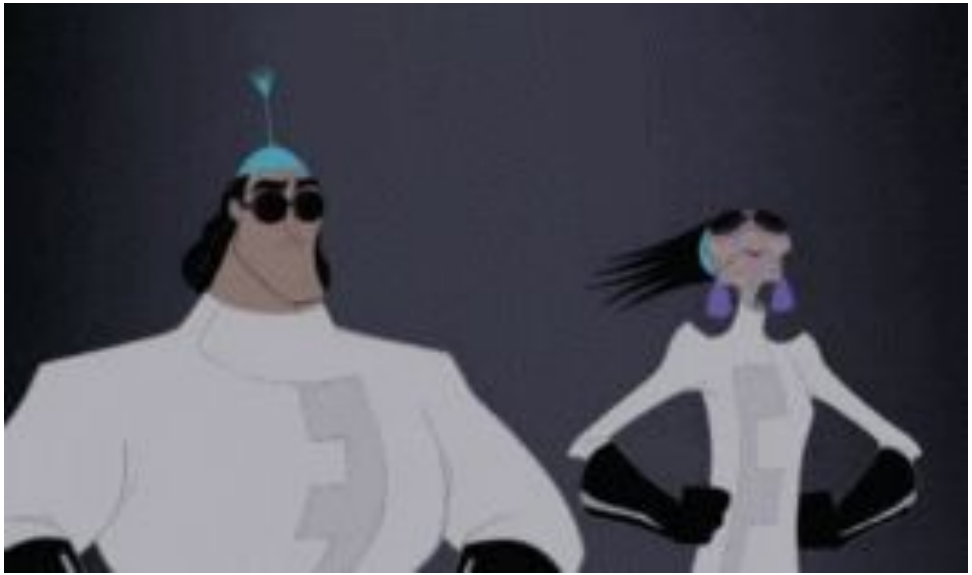
What are replica shards?



Replica shards can improve the performance of your search



Tutorial:
Performing CRUD Operations with Elasticsearch and Kibana



Click on the link to the tutorial repo.

https://ela.st/vancouver-workshop-1

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

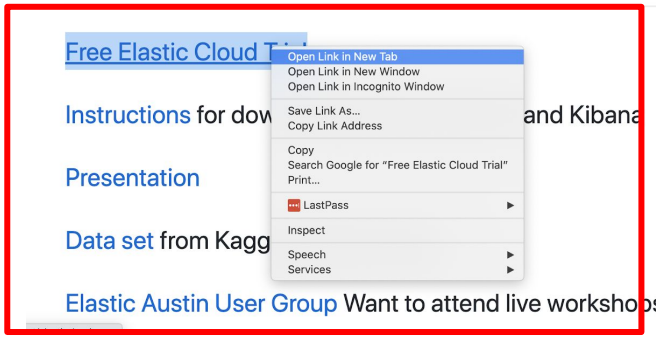
Beginner's Crash Course to the Elastic Stack Series

Part 1.2: Understanding the relevance of your search with Elasticsearch and Kibana

Welcome to the Beginner's Crash Course to the Elastic Stack!

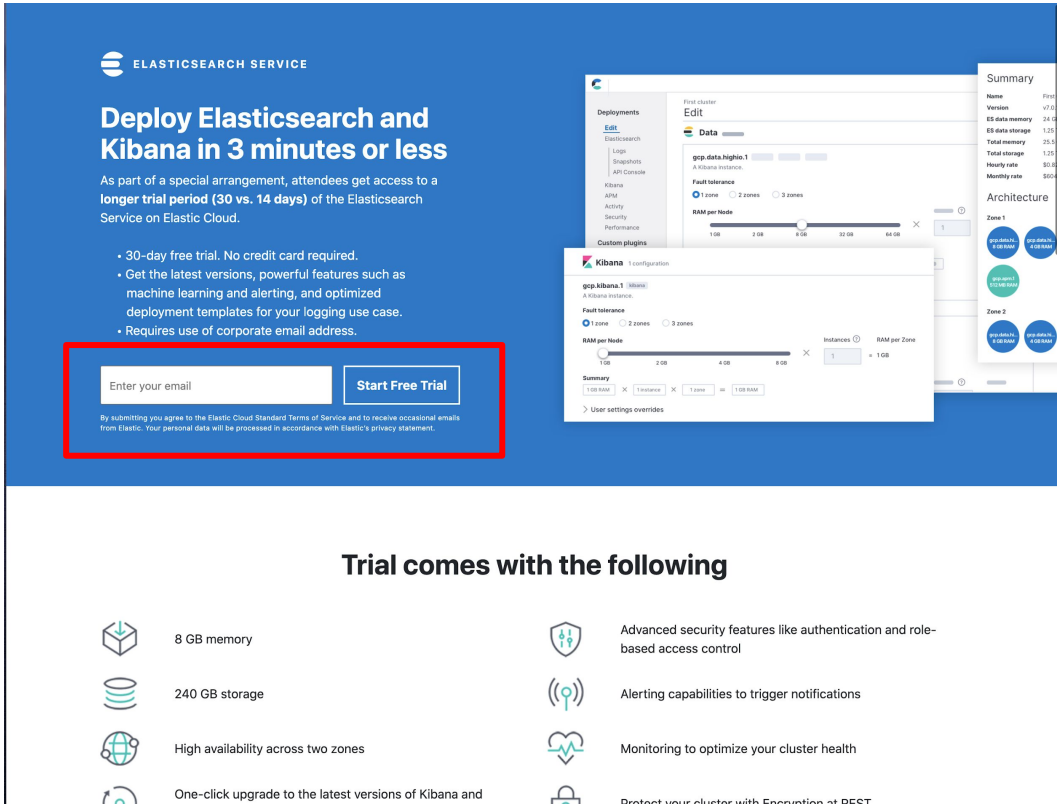
This repo contains all resources shared during the workshop 1.2: Understanding the relevance of your search with Elasticsearch and Kibana.

Resources



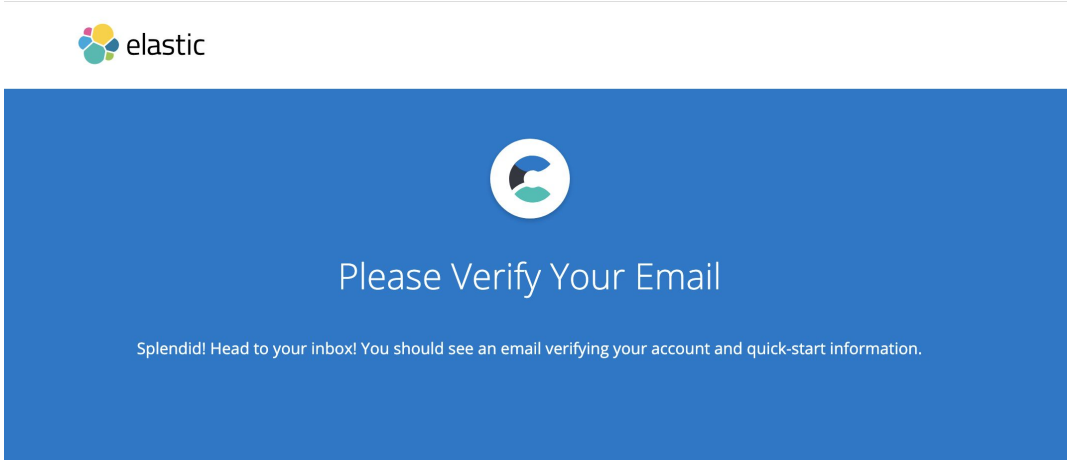
elastic

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

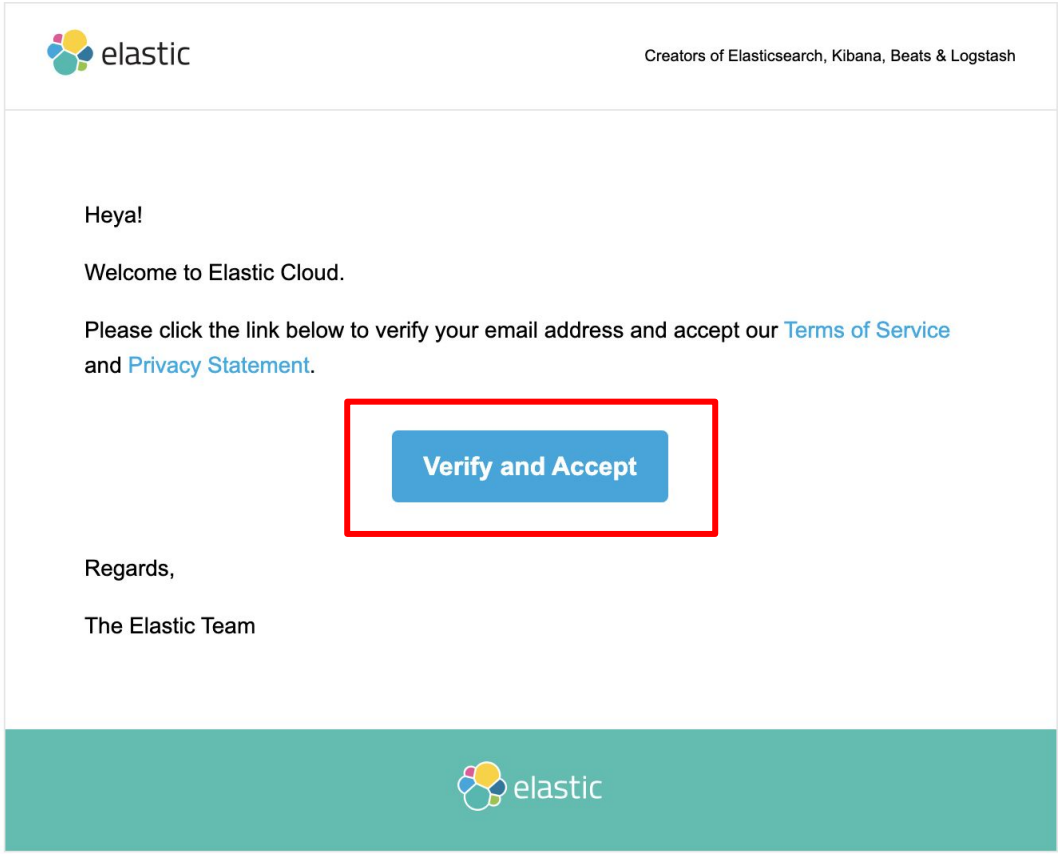


elastic

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

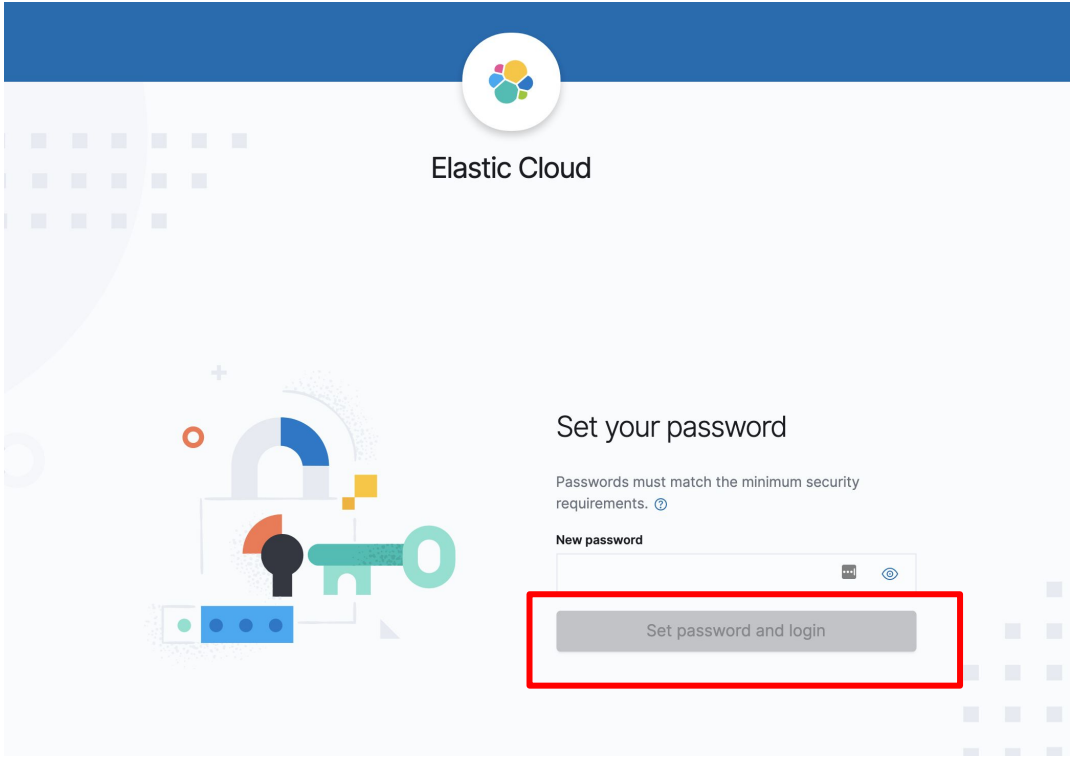


Open email from Elastic. Click on verify and accept button.



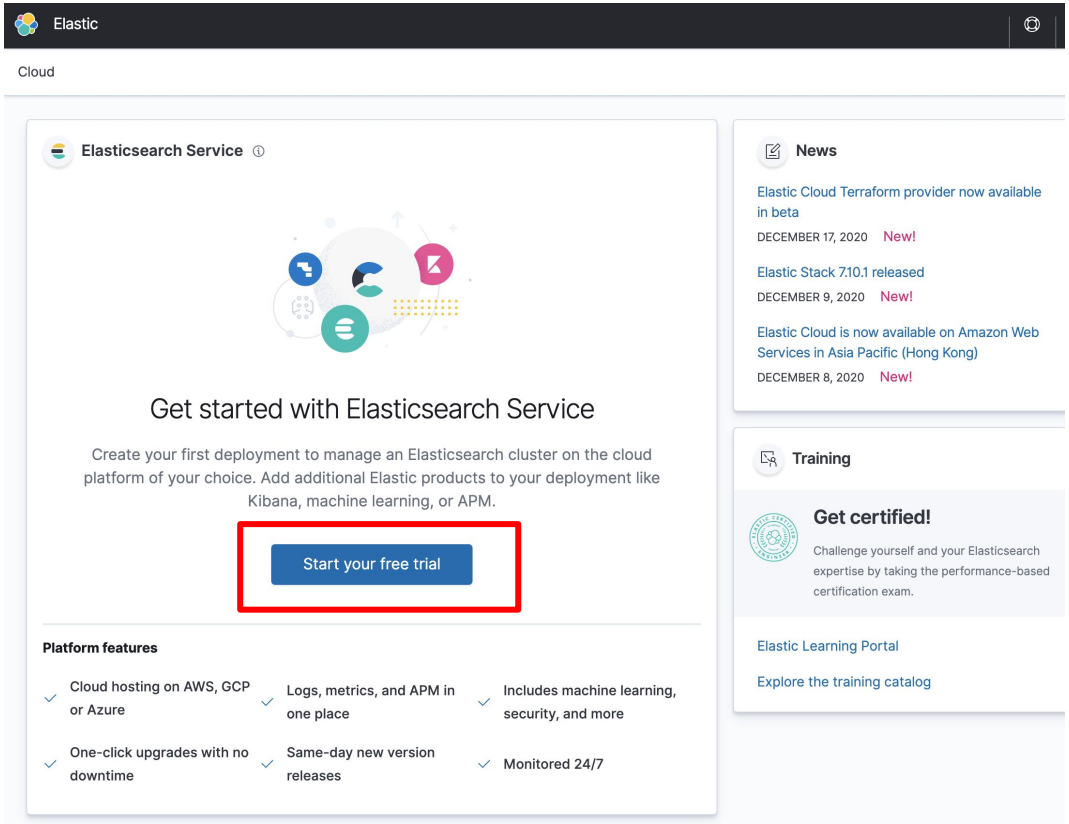
elastic

Enter your password.



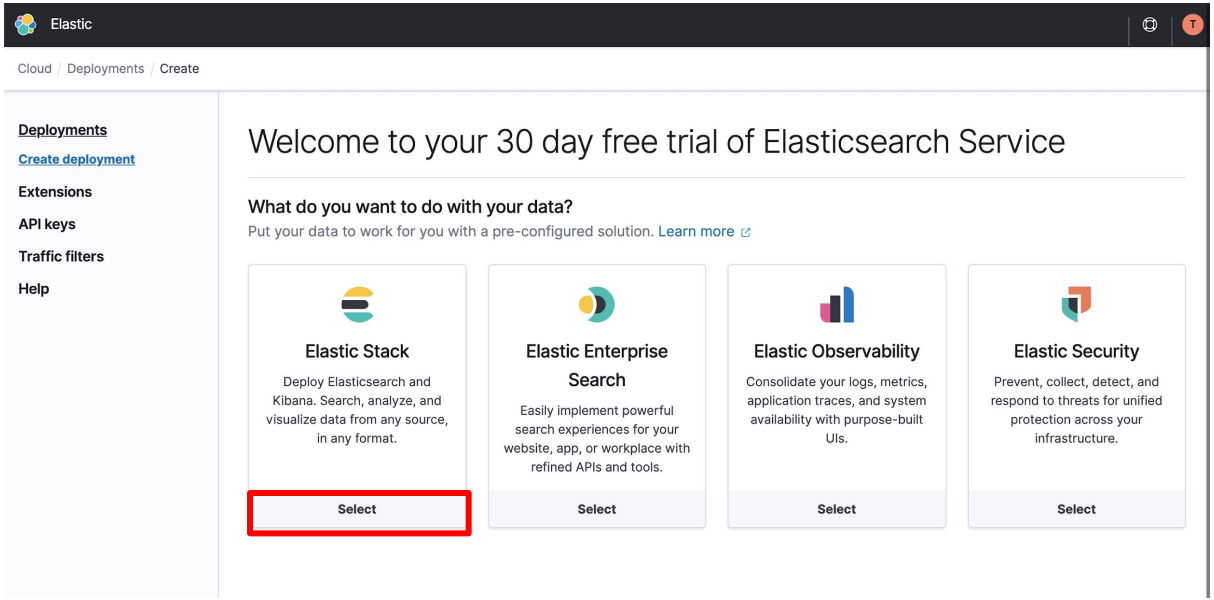
elastic

Click on start your free trial.



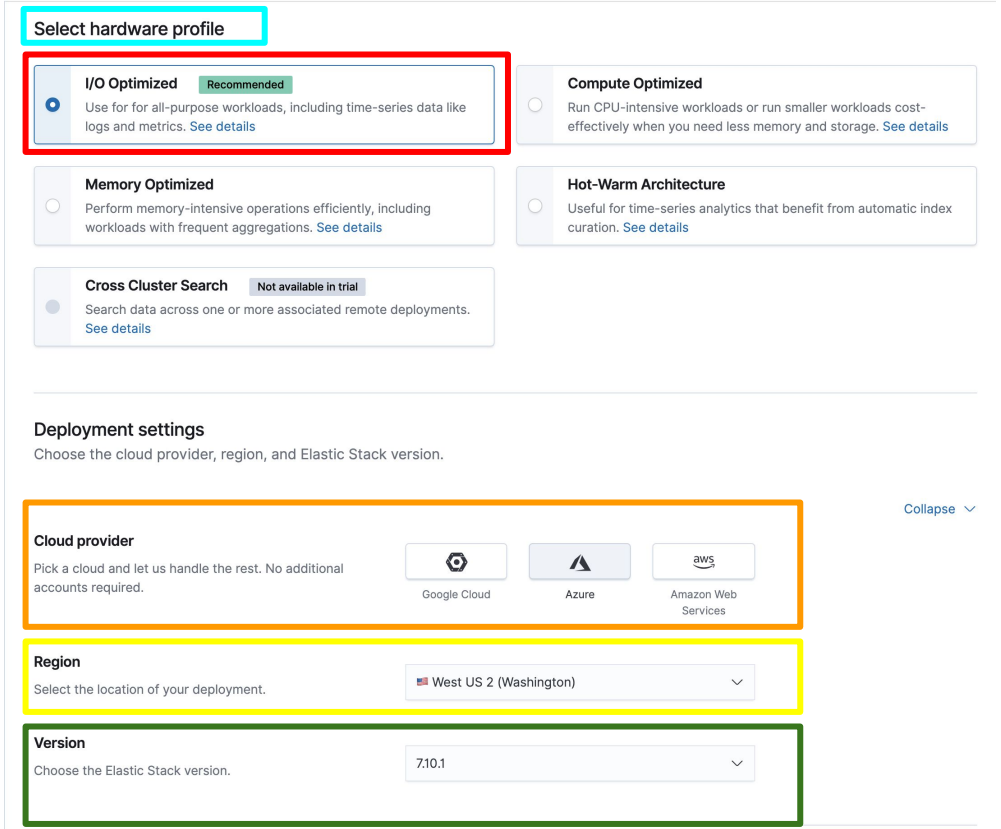
elastic

Select the Elastic Stack.



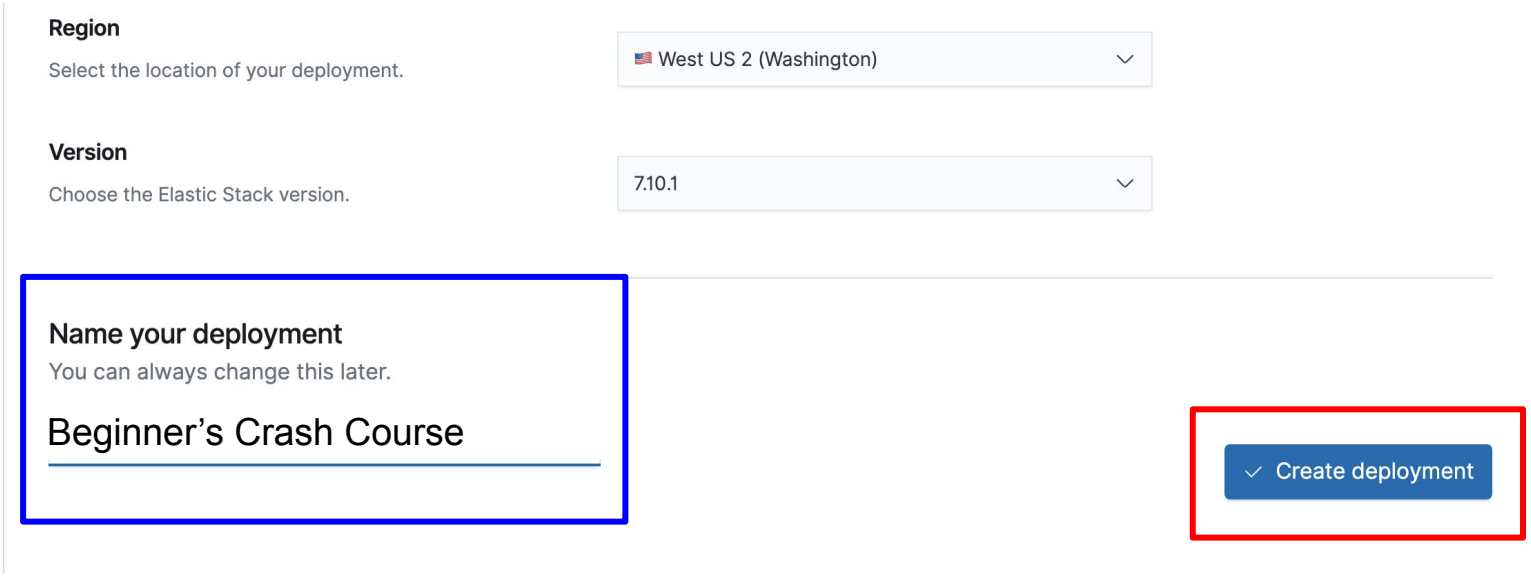
elastic

Configure your settings.

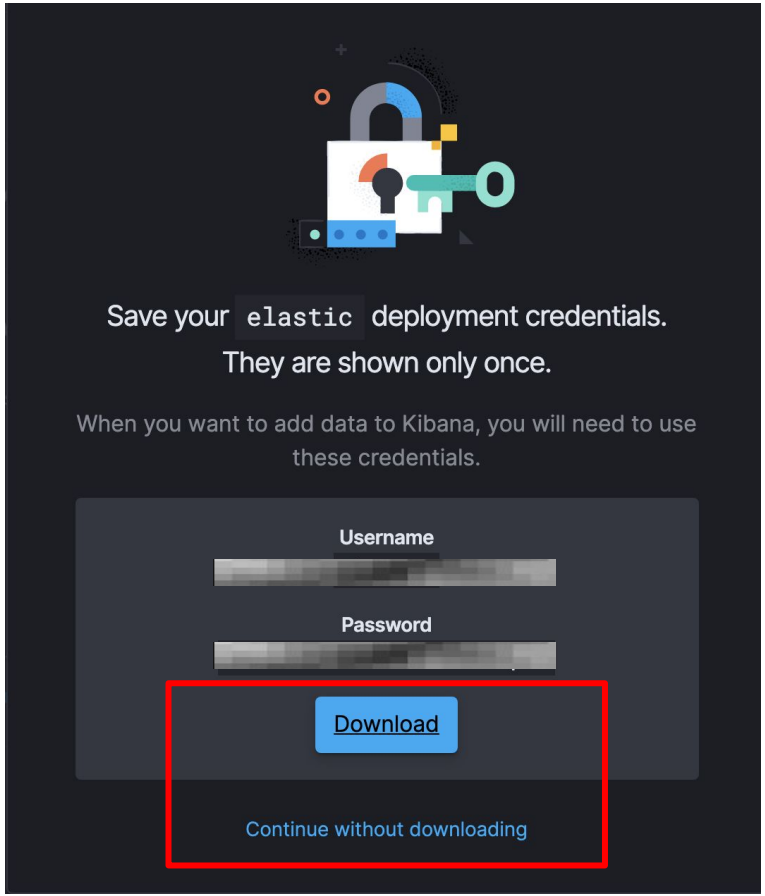


elastic

Name your deployment then create deployment.

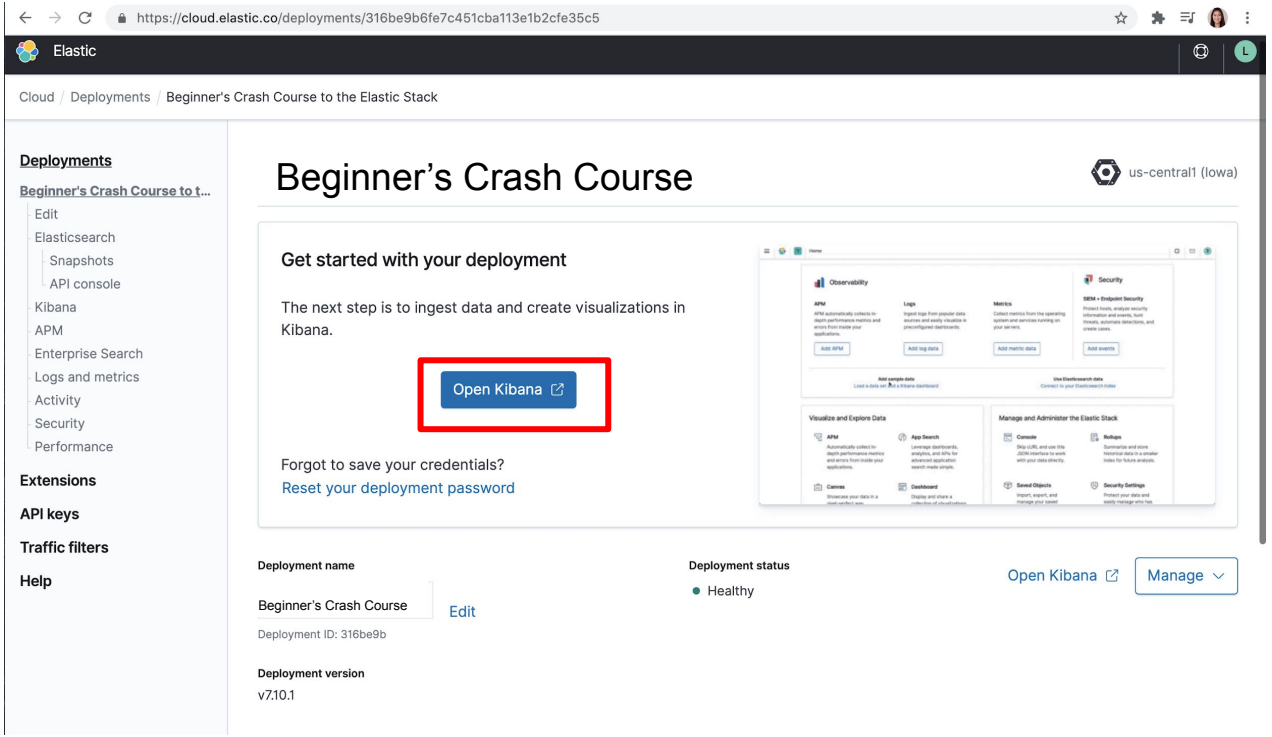


Save your deployment credentials.

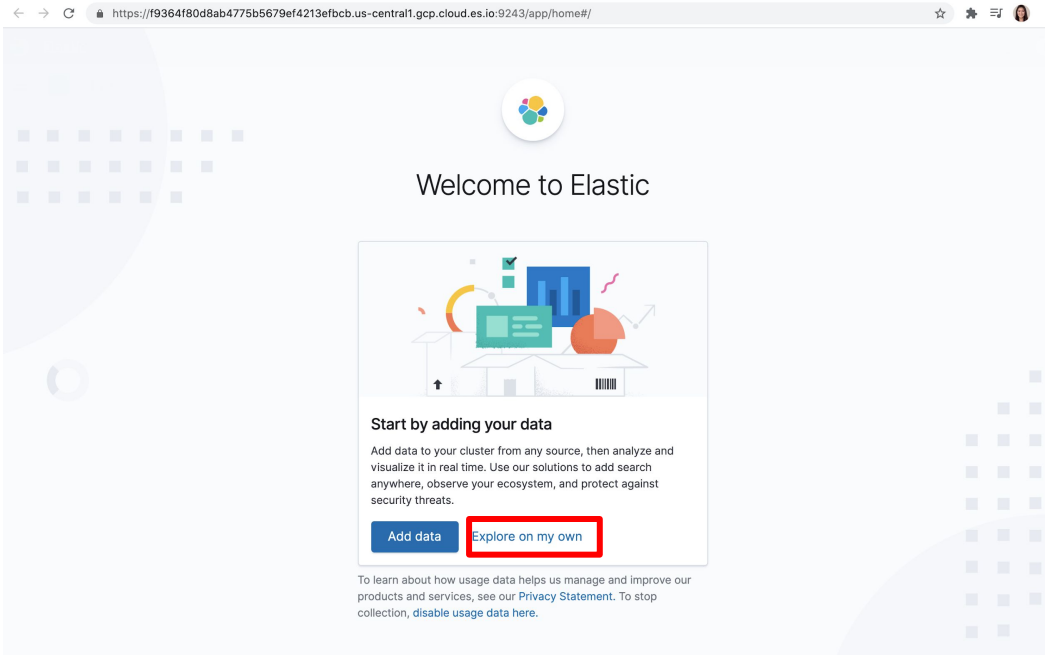


elastic

Open Kibana.

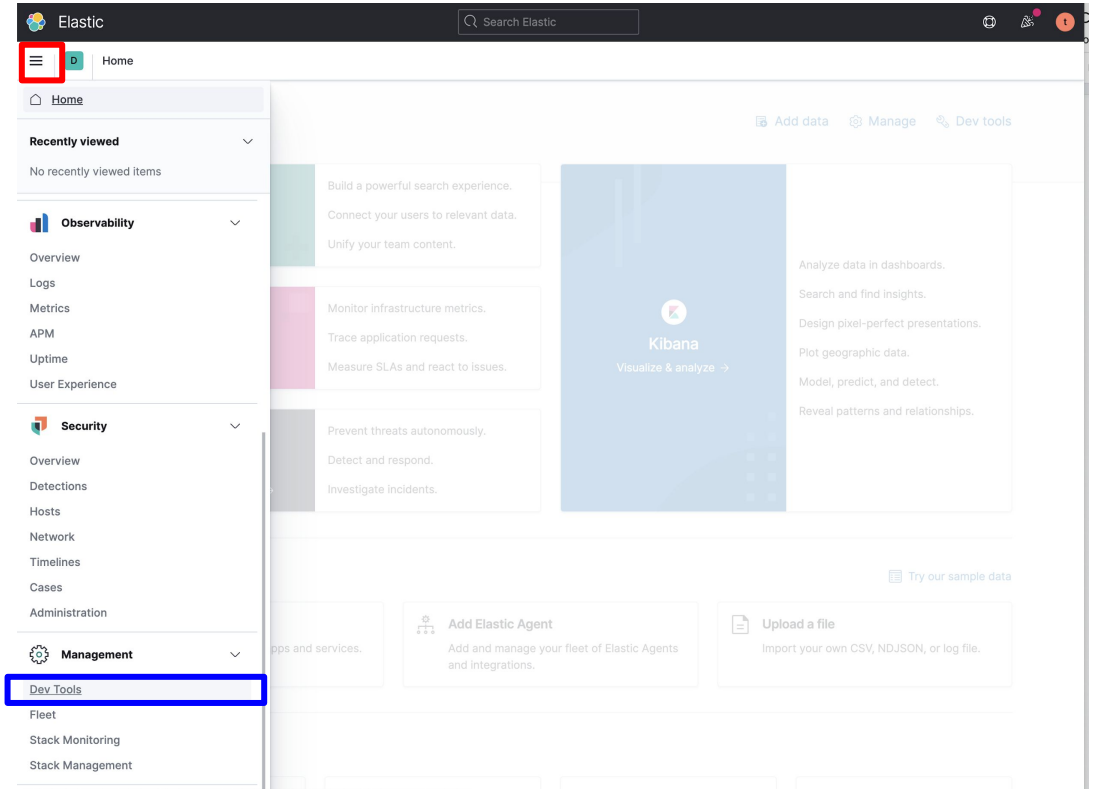

https://cloud.elastic.co/deployments/316be9b6fe7c451cba113e1b2cfe35c5
Elastic
Cloud / Deployments / Beginner's Crash Course to the Elastic Stack
Deployments
Beginner's Crash Course to t...
Edit
Elasticsearch
Snapshots
API console
Kibana
APM
Enterprise Search
Logs and metrics
Activity
Security
Performance
Extensions
API keys
Traffic filters
Help
Beginner's Crash Course
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
Beginner's Crash Course
Edit
Deployment ID: 316be9b
Deployment version
v7.10.1
Deployment status
Healthy
Open Kibana
Manage

Click on Explore on my own option.

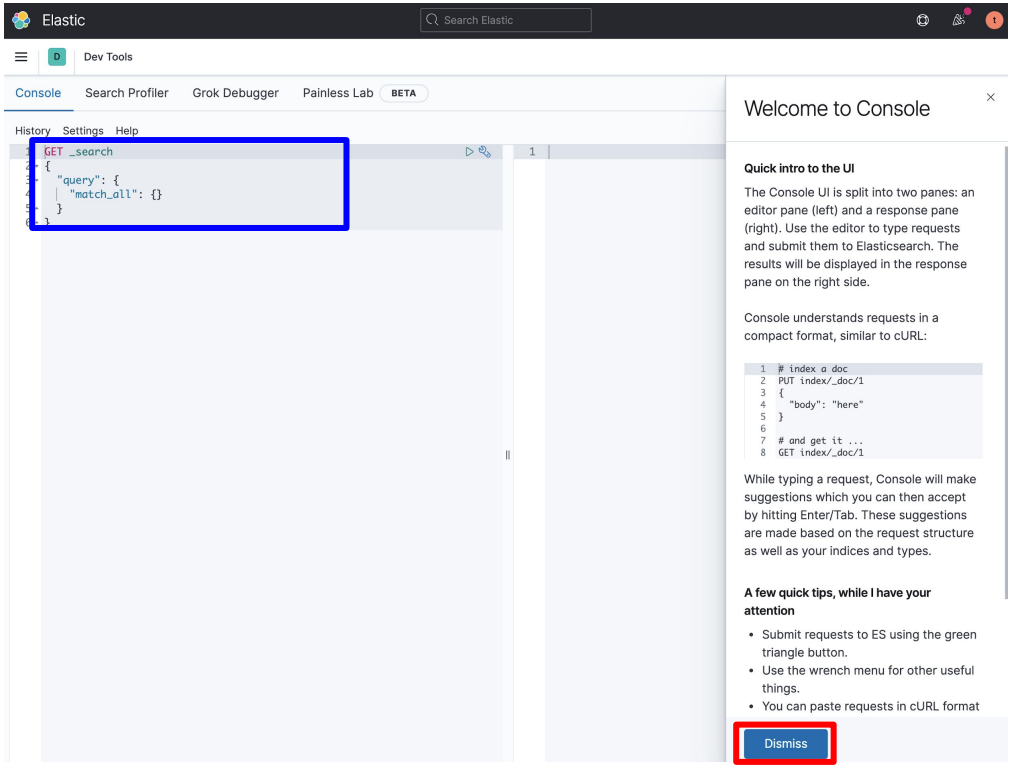


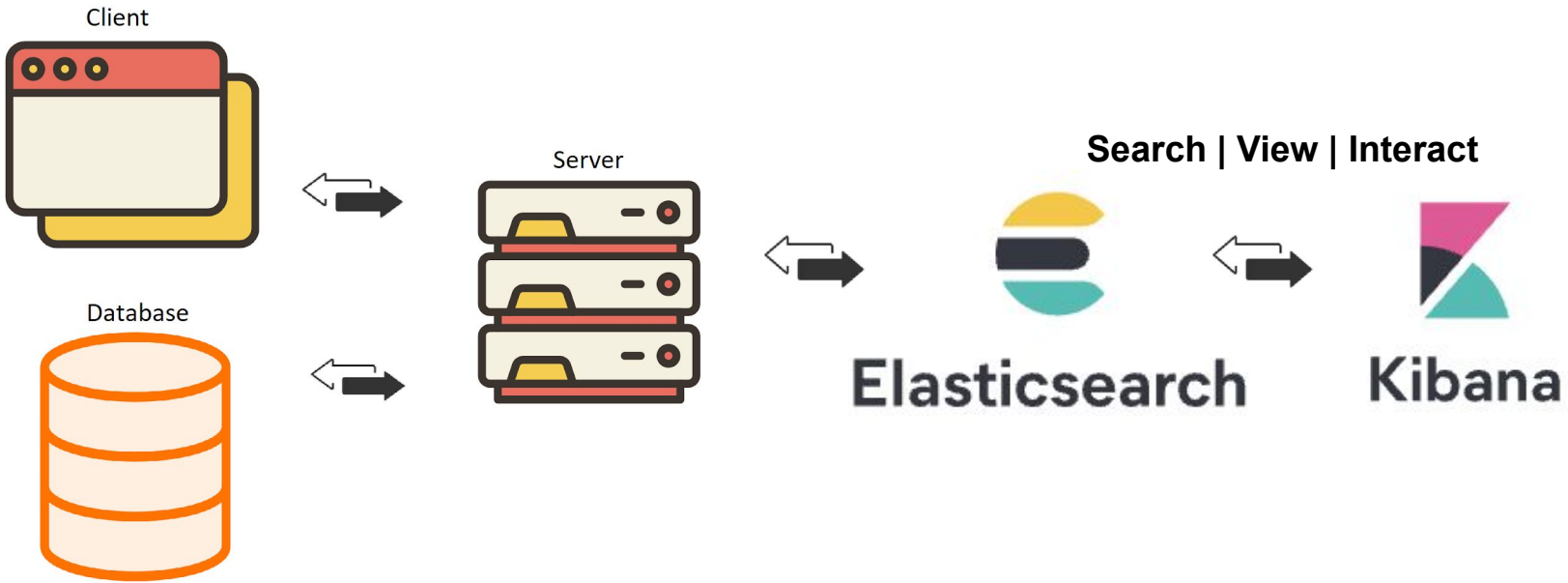
elastic

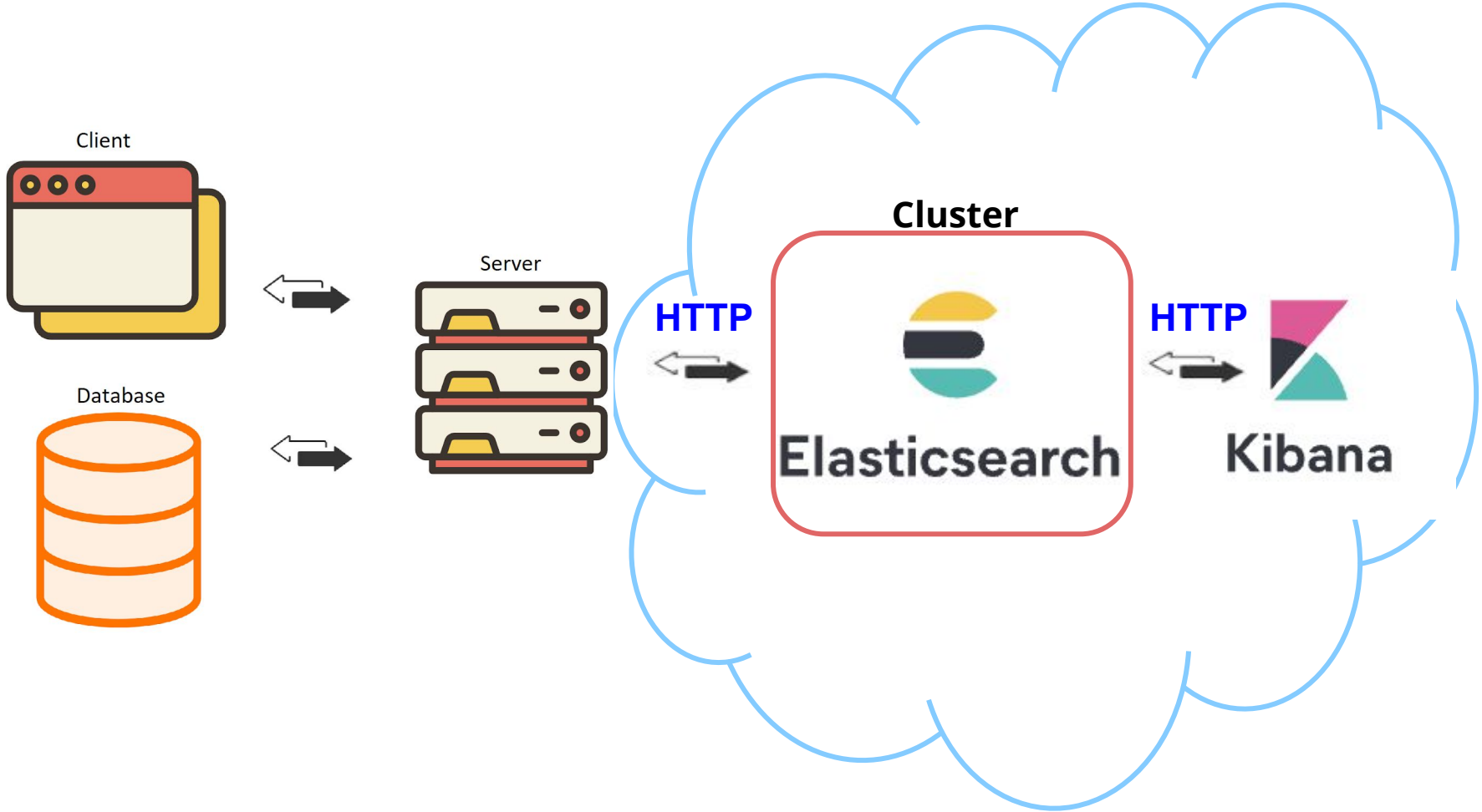
Click on menu icon, and open Dev Tools.



Click on dismiss and delete the default query.




Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana


Client
Database
Server
HTTP
Cluster
Elasticsearch
HTTP
Kibana

Questions?

Join us for part 2 of the Beginner's Crash Course series!


Lisa Jung

Developer Advocate @Elastic

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

Blog: https://dev.to/lisahjung

Twitter: @LisaHJung