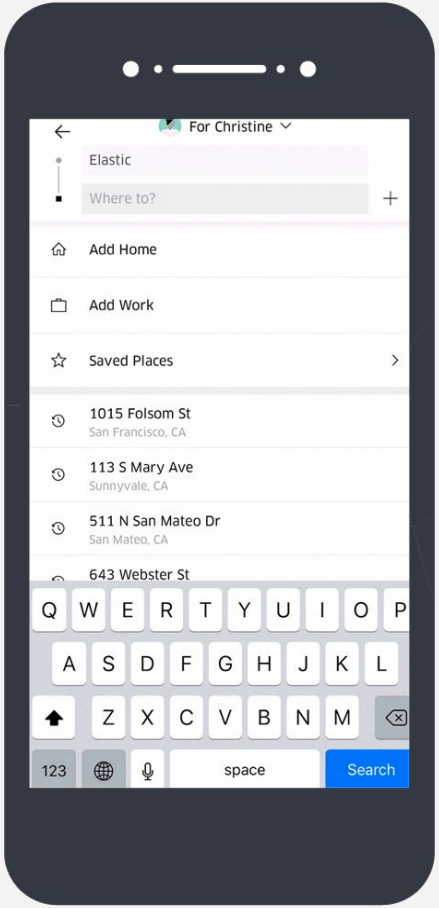

Introduction to
Elasticsearch and Kibana
Lisa Jung
Developer Advocate @ Elastic
elastic
@LisaHJung | Beginner's Crash Course to Elastic Stack

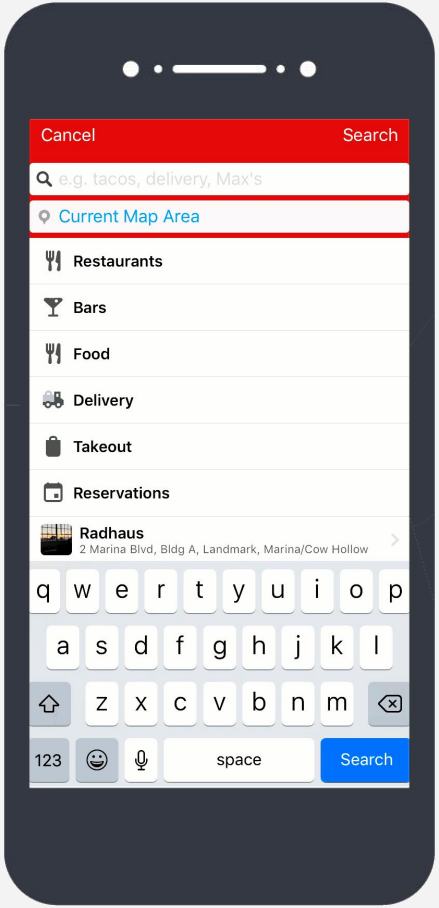
Have you ever used the Elastic Stack before?

Type **yes** in the chat if you have used it

Type **no** in the chat if you have never used it



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

elastic

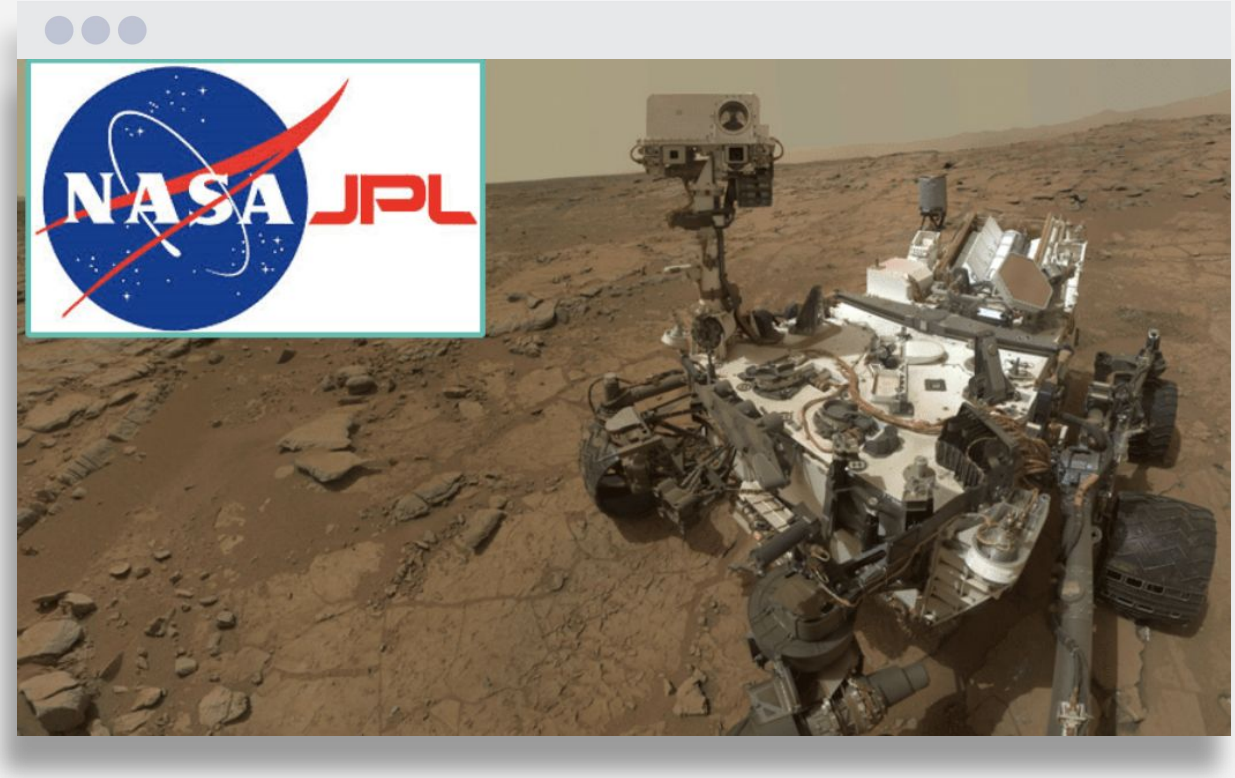
Use Case: Logging

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

ACTIVISION BLIZZARD

elastic

Use Case: Metrics

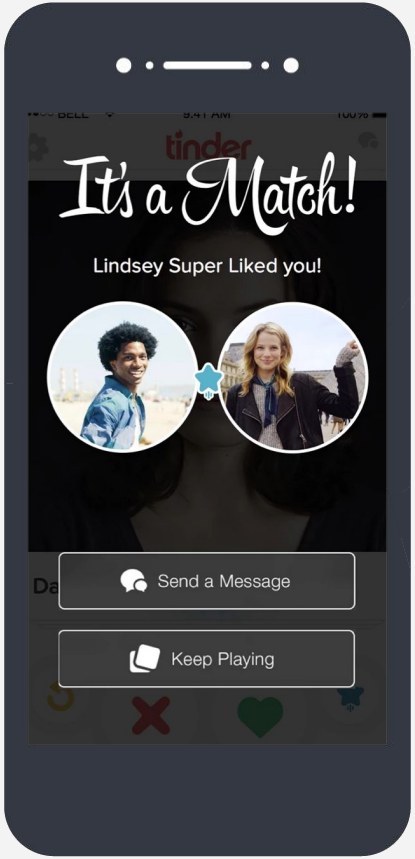


elastic

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.

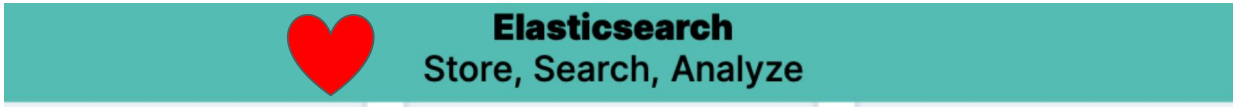

Introduction to
Elasticsearch and Kibana
Lisa Jung
Developer Advocate @ Elastic
elastic
@LisaHJung | Beginner's Crash Course to Elastic Stack

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

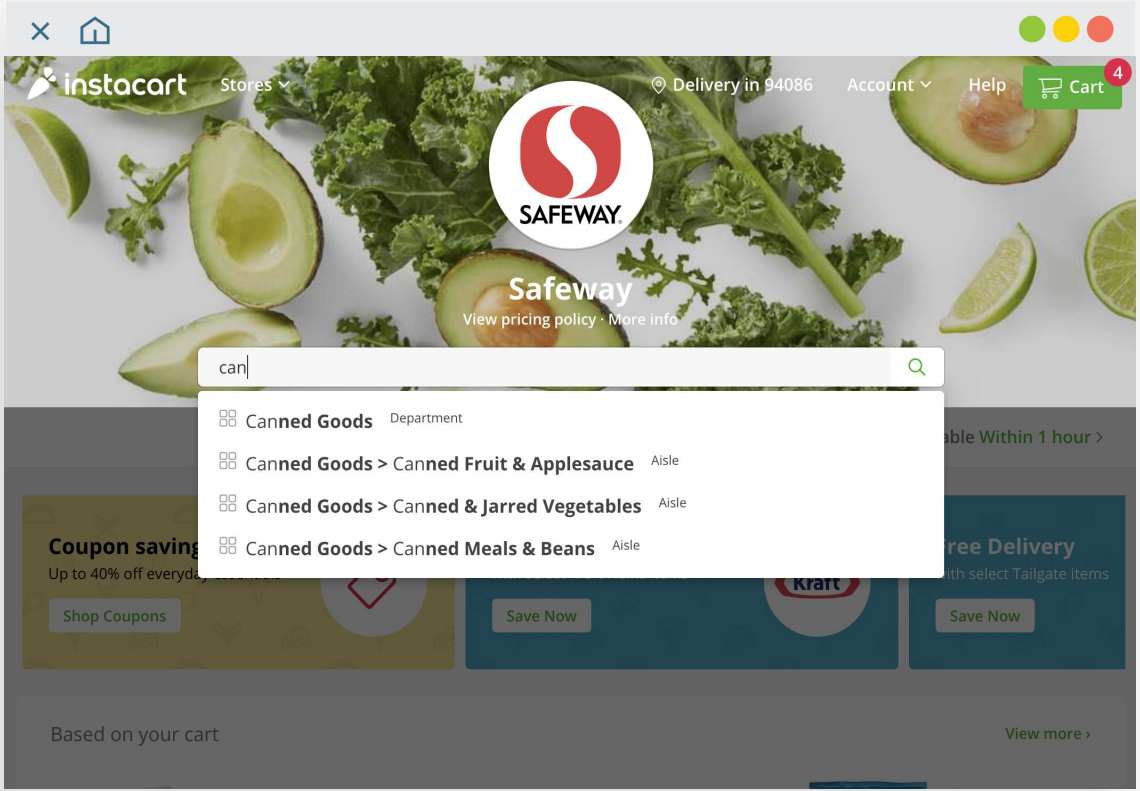
Elasticsearch

Store | Search | Analyze



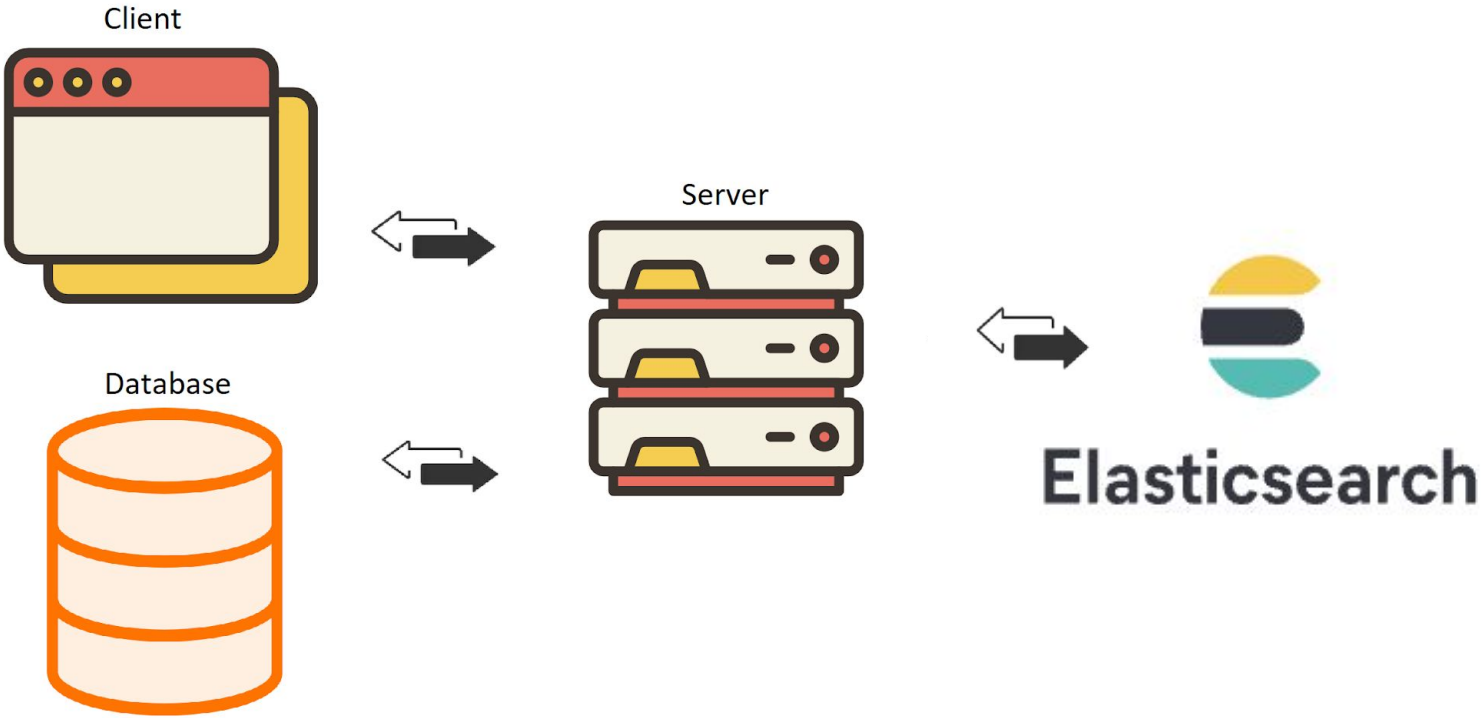
Great Search Experience = Get fast and relevant results, no matter the scale.

instacart



Find me a list of peanut butter brands. I want the 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?

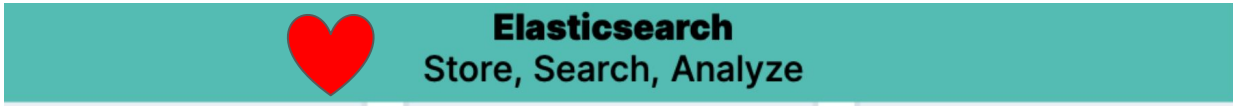

Client
Server
Database
Elasticsearch

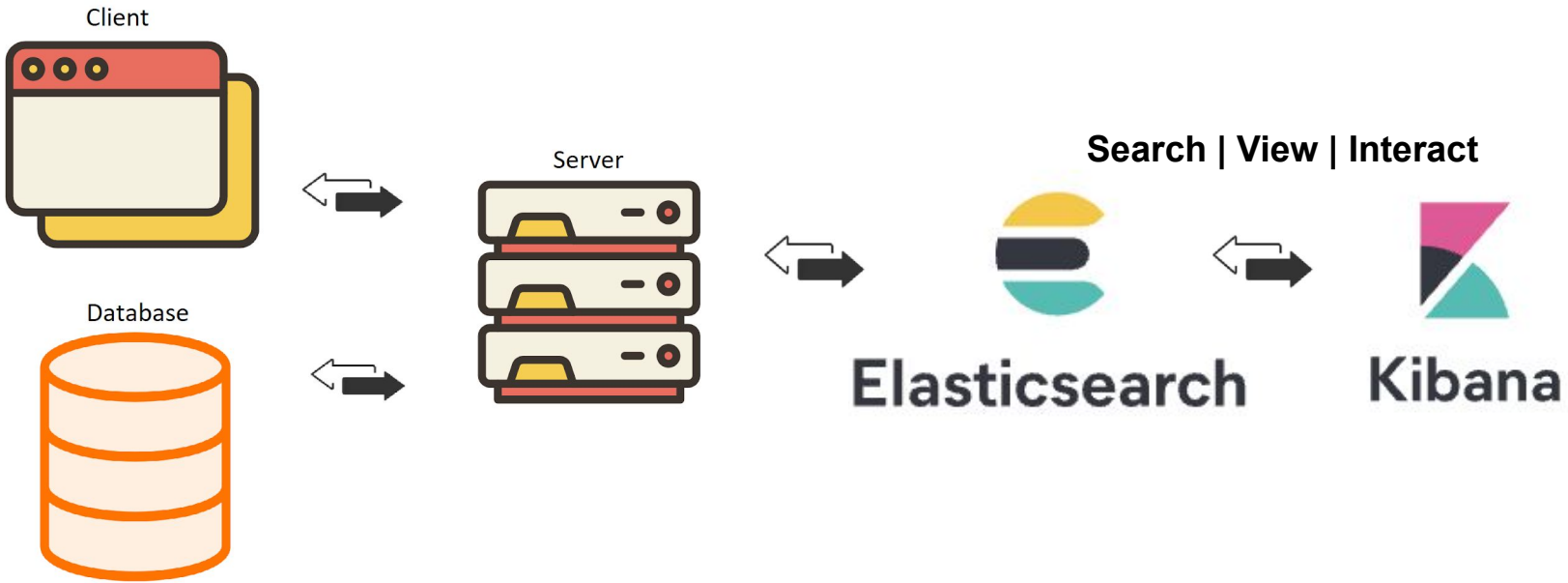
Kibana

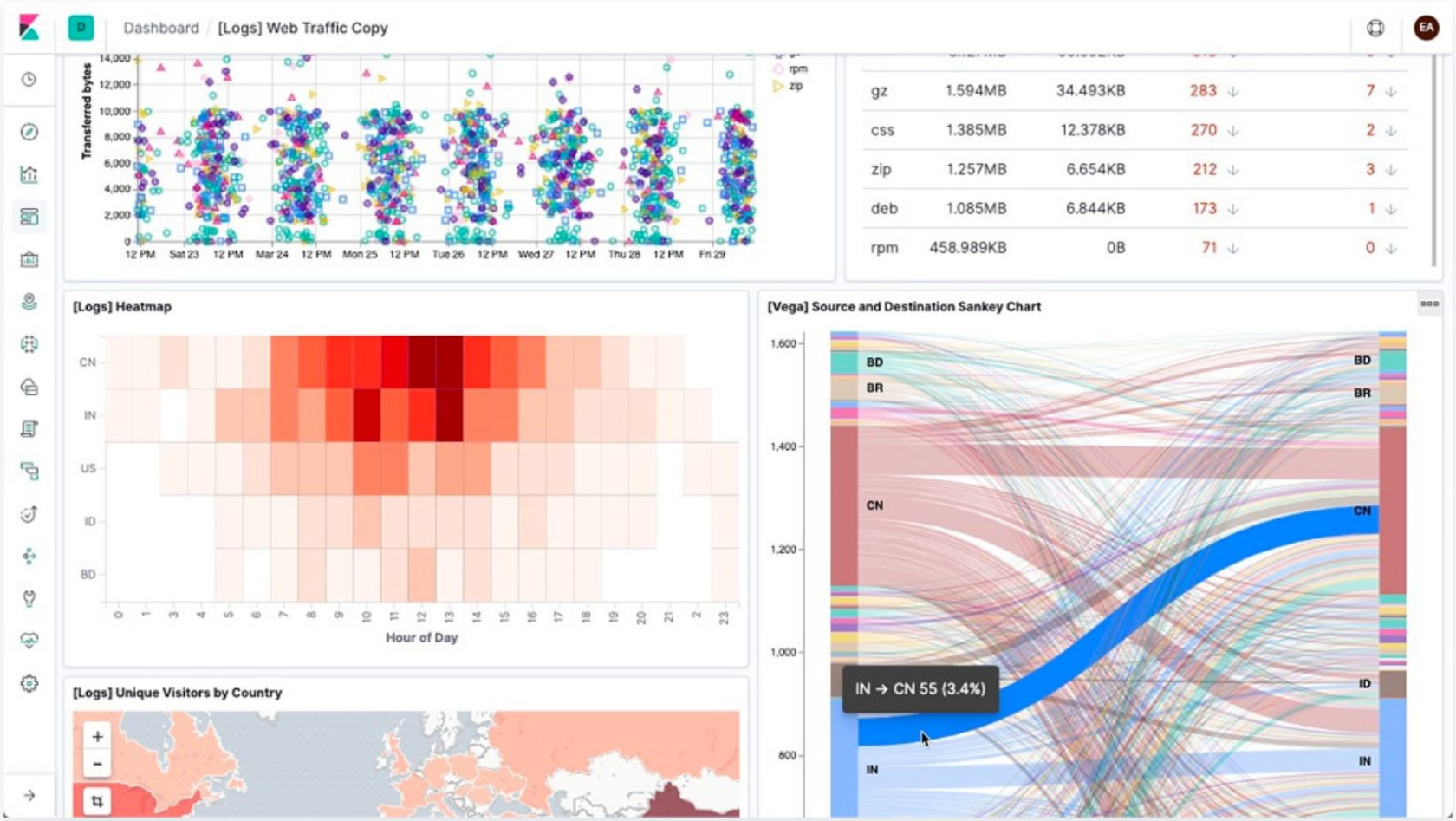
Visualize| Manage

Elasticsearch

Store | Search | Analyze




Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana

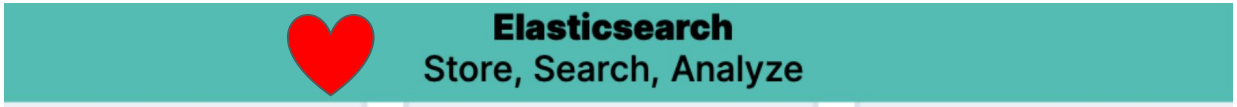

Dashboard / [Logs] Web Traffic Copy
Transferred bytes
rpm
zip
12 PM Sat 23 12 PM Mar 24 12 PM Mon 25 12 PM Tue 26 12 PM Wed 27 12 PM Thu 28 12 PM Fri 29
gz 1.594MB 34.493KB 283 7
css 1.385MB 12.378KB 270 2
zip 1.257MB 6.654KB 212 3
deb 1.085MB 6.844KB 173 1
rpm 458.989KB 0B 71 0
[Logs] Heatmap
CN
IN
US
ID
BD
Hour of Day
[Vega] Source and Destination Sankey Chart
BD
BR
CN
ID
IN
IN → CN 55 (3.4%)
[Logs] Unique Visitors by Country

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

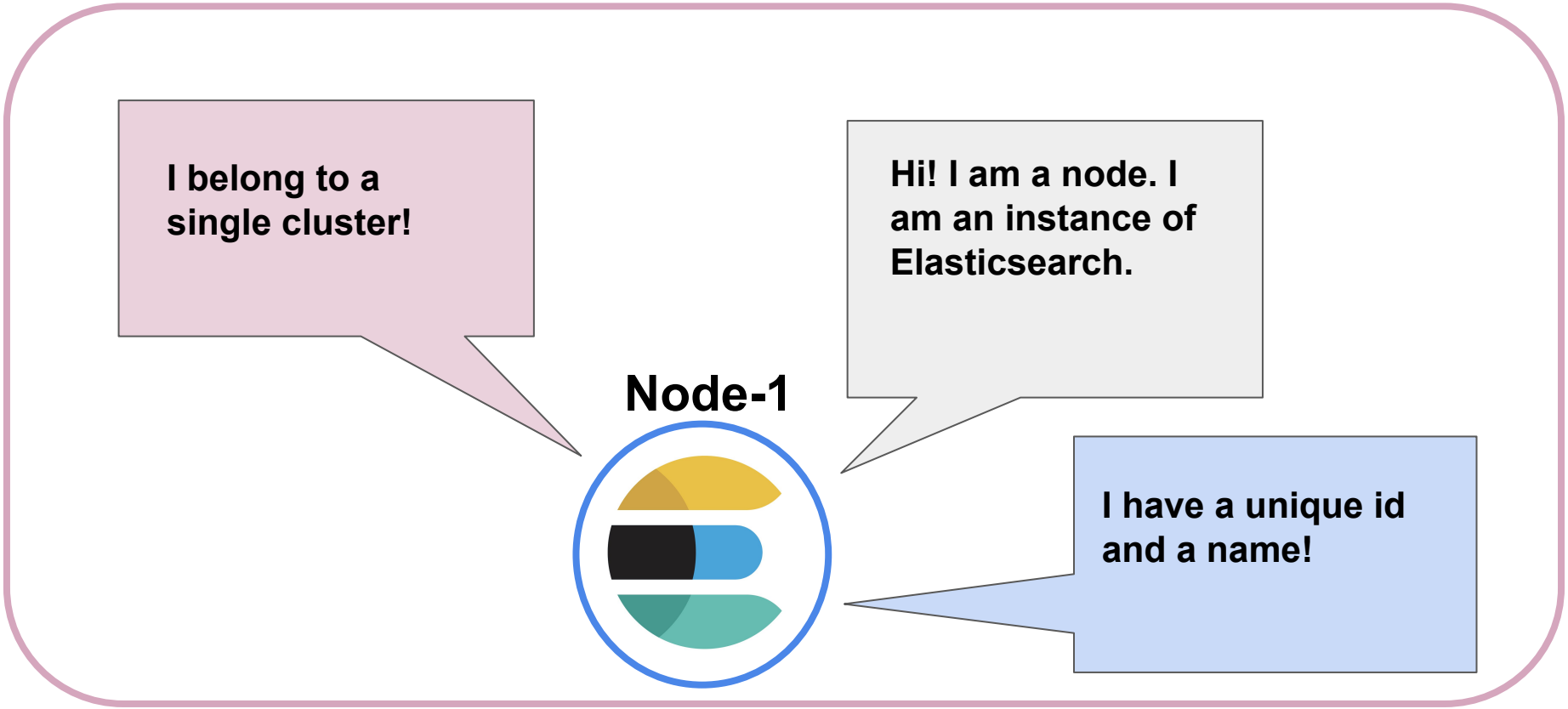
- understand a use case of Elasticsearch and Kibana
- **understand the basic architecture of Elasticsearch**
- Perform CRUD(Create, Read, Update, Delete) operations with Elasticsearch and Kibana

Elasticsearch

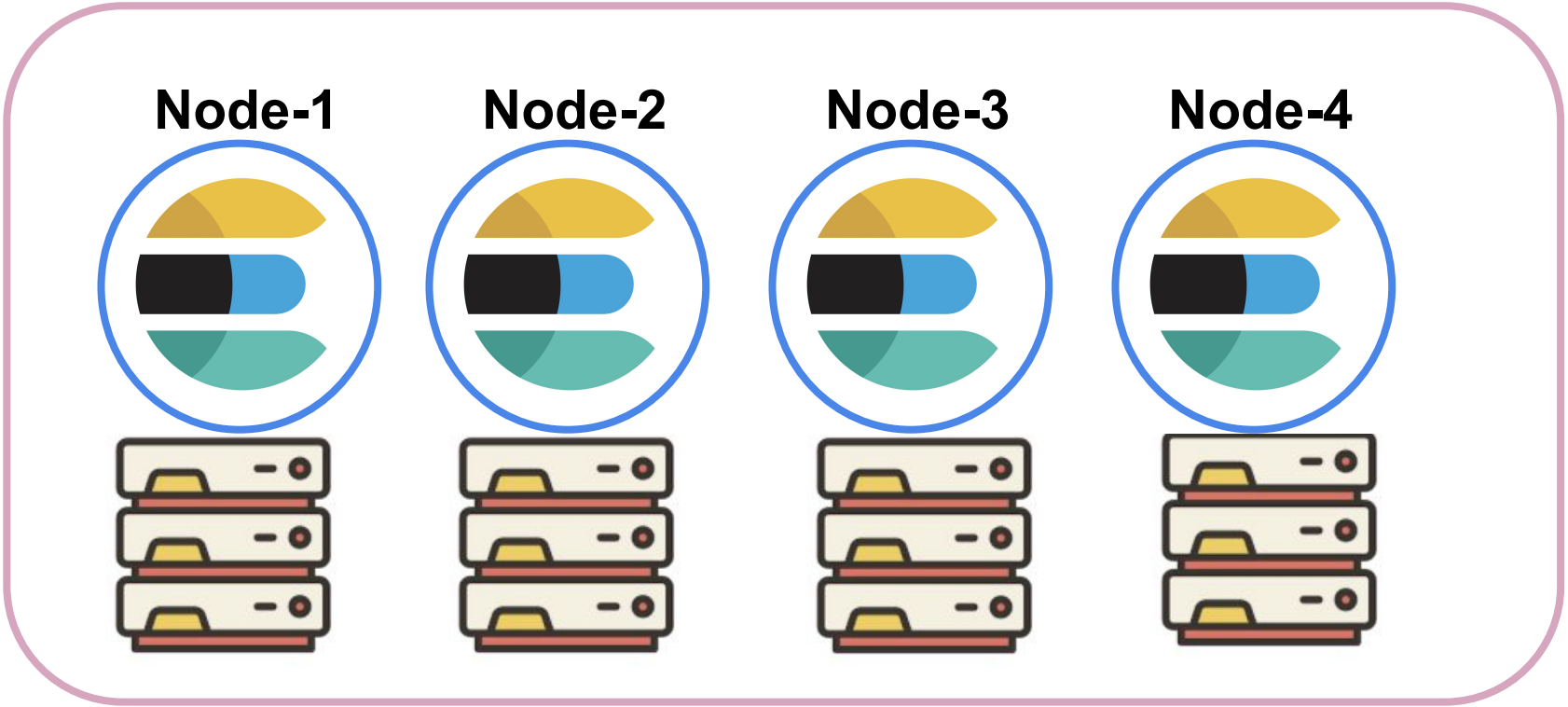
Store | Search | Analyze



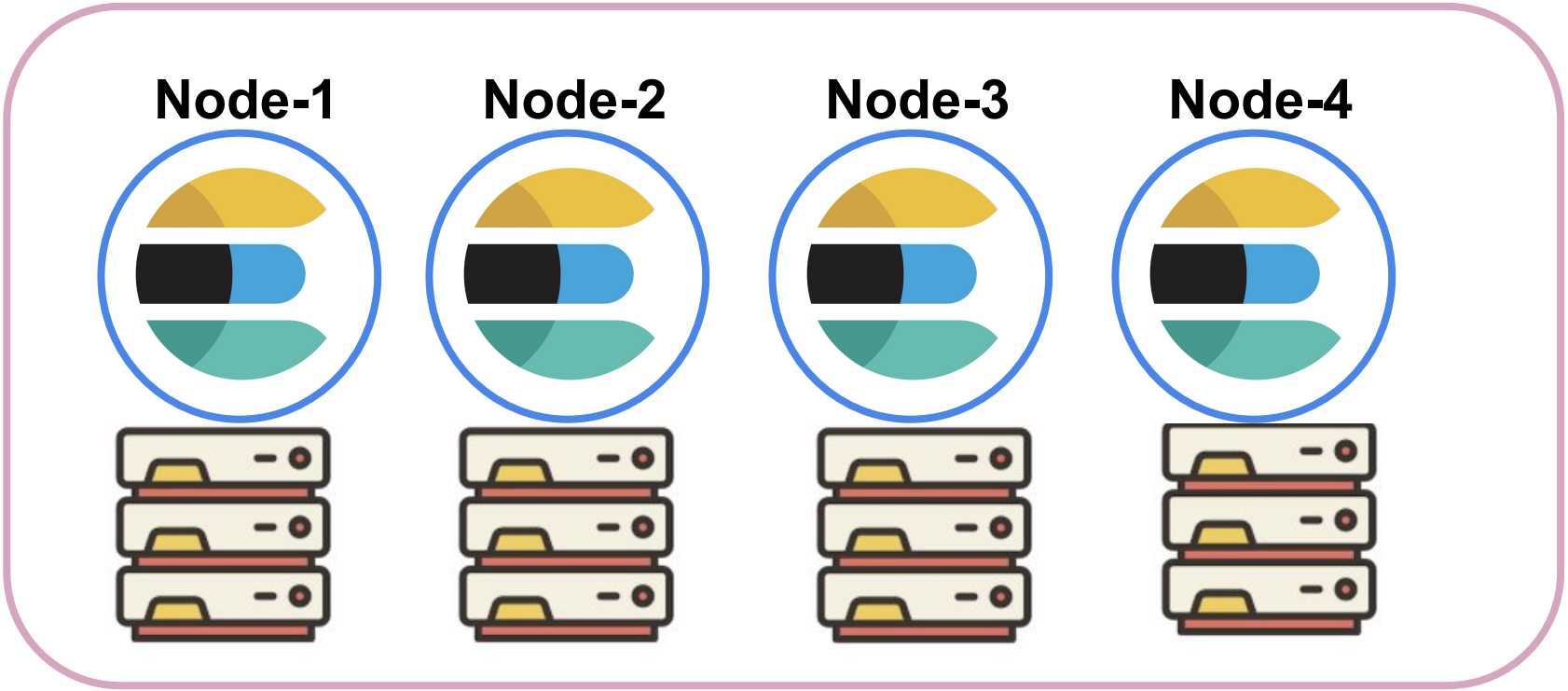
Cluster


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!

Documents are grouped into an index!

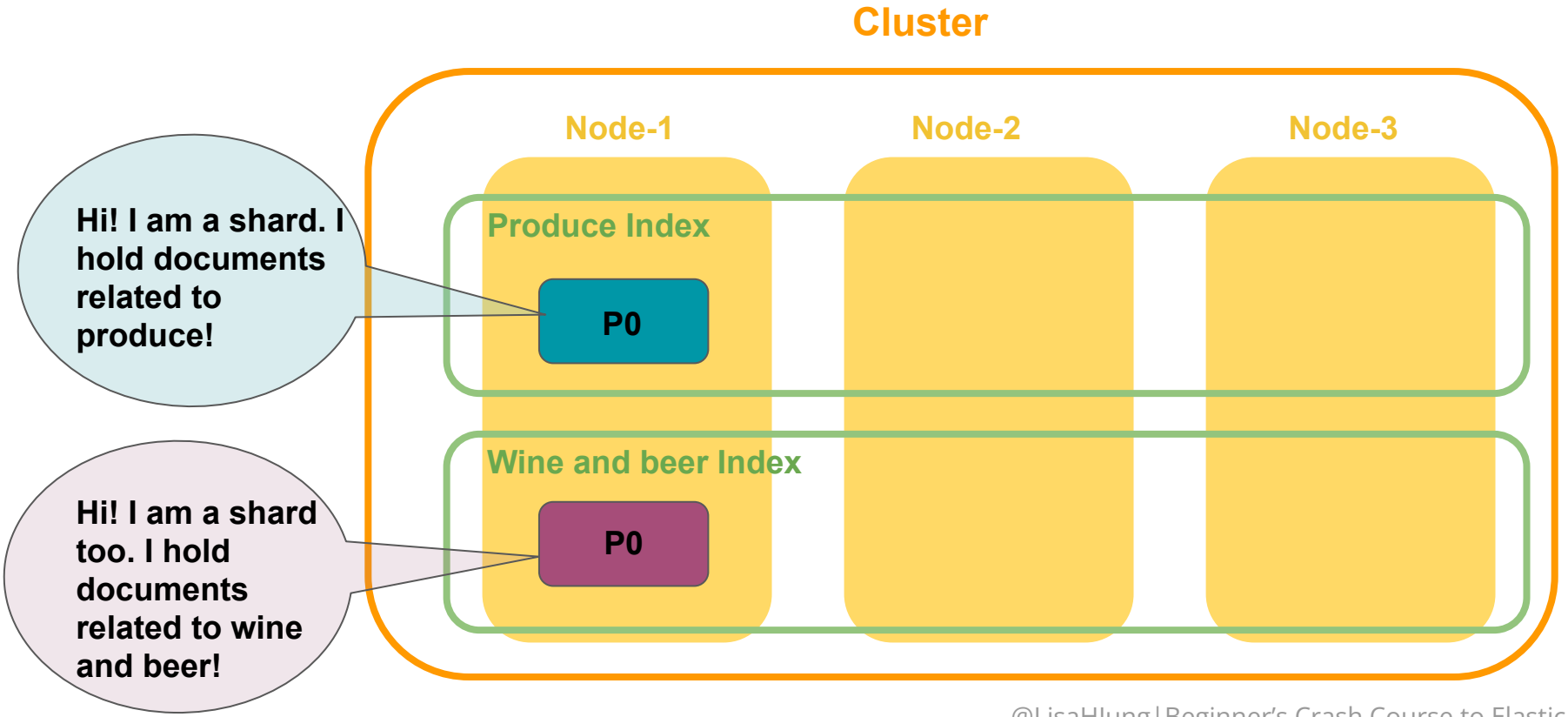
Produce Index


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

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

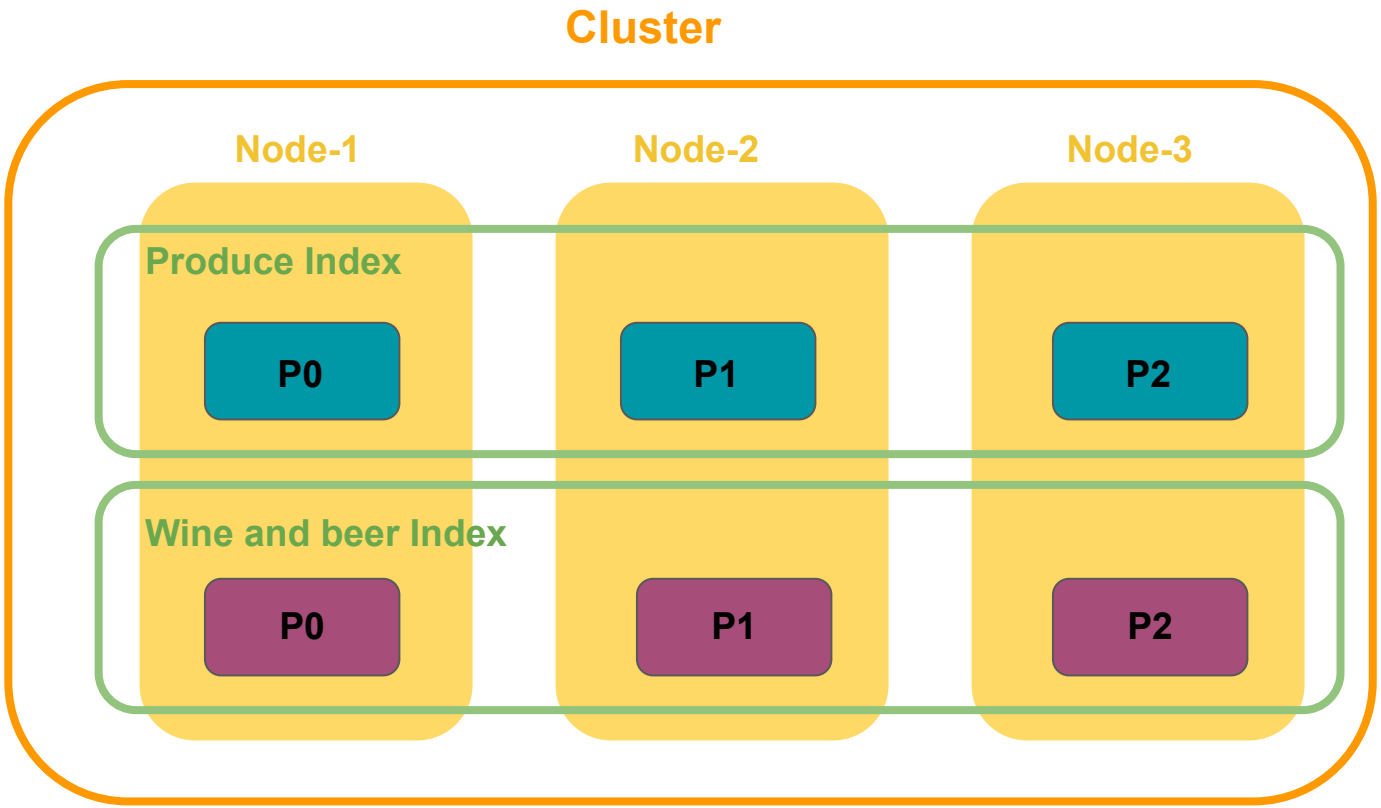

Wine & Beer Index


```
{
  "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",
  "brand": "US",
  "country": "California",
  "beer_type": "Ale",
  "beer_style": "India Pale Ale",
  "ABV": "6.7%",
  "price": "$14.99"
}
```

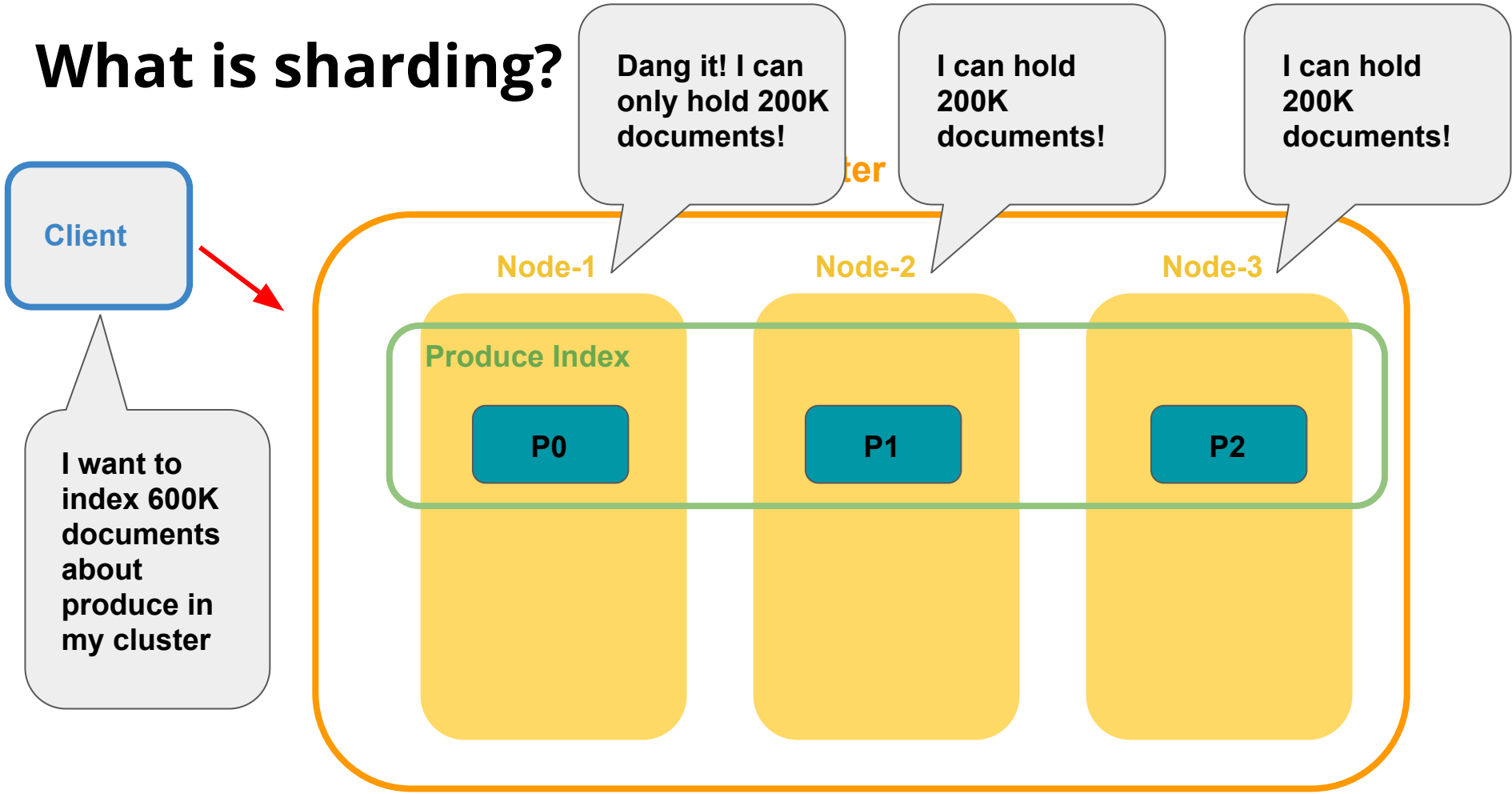
What is a shard?



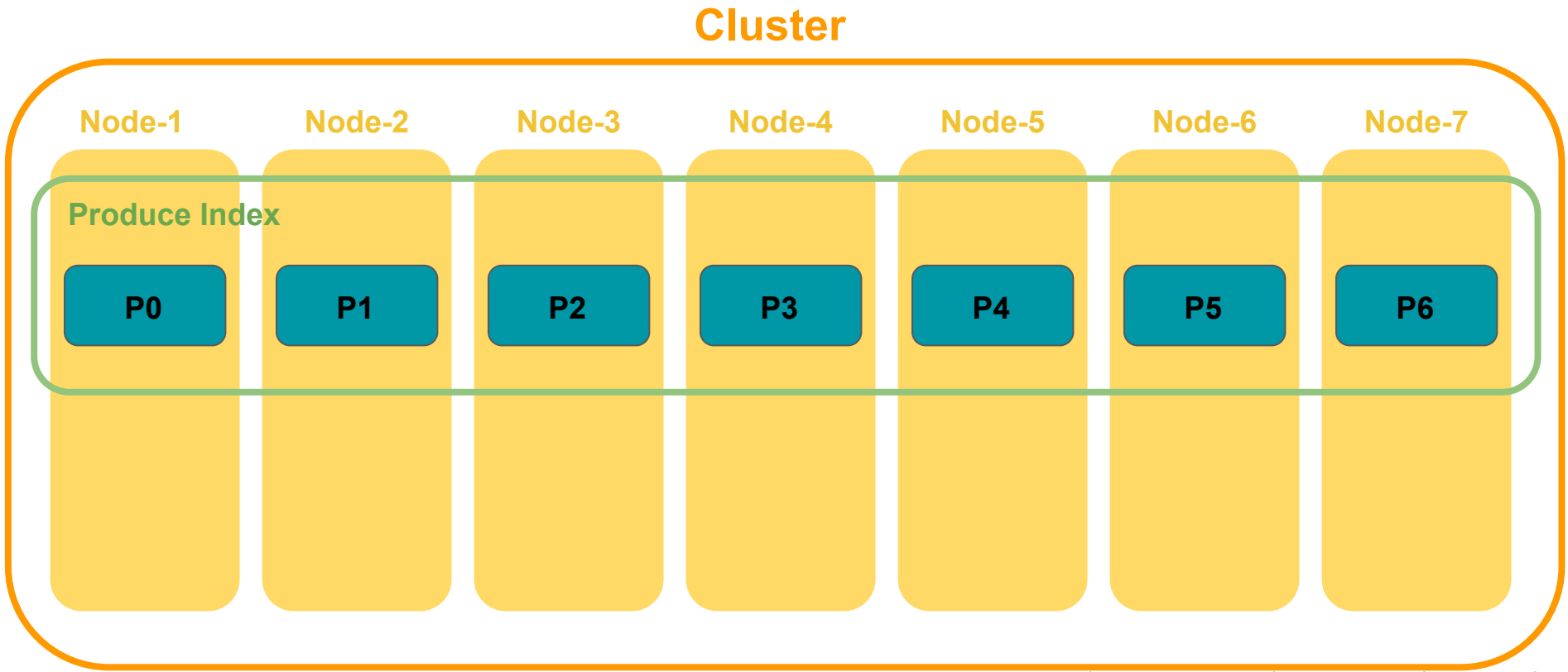
What is sharding?



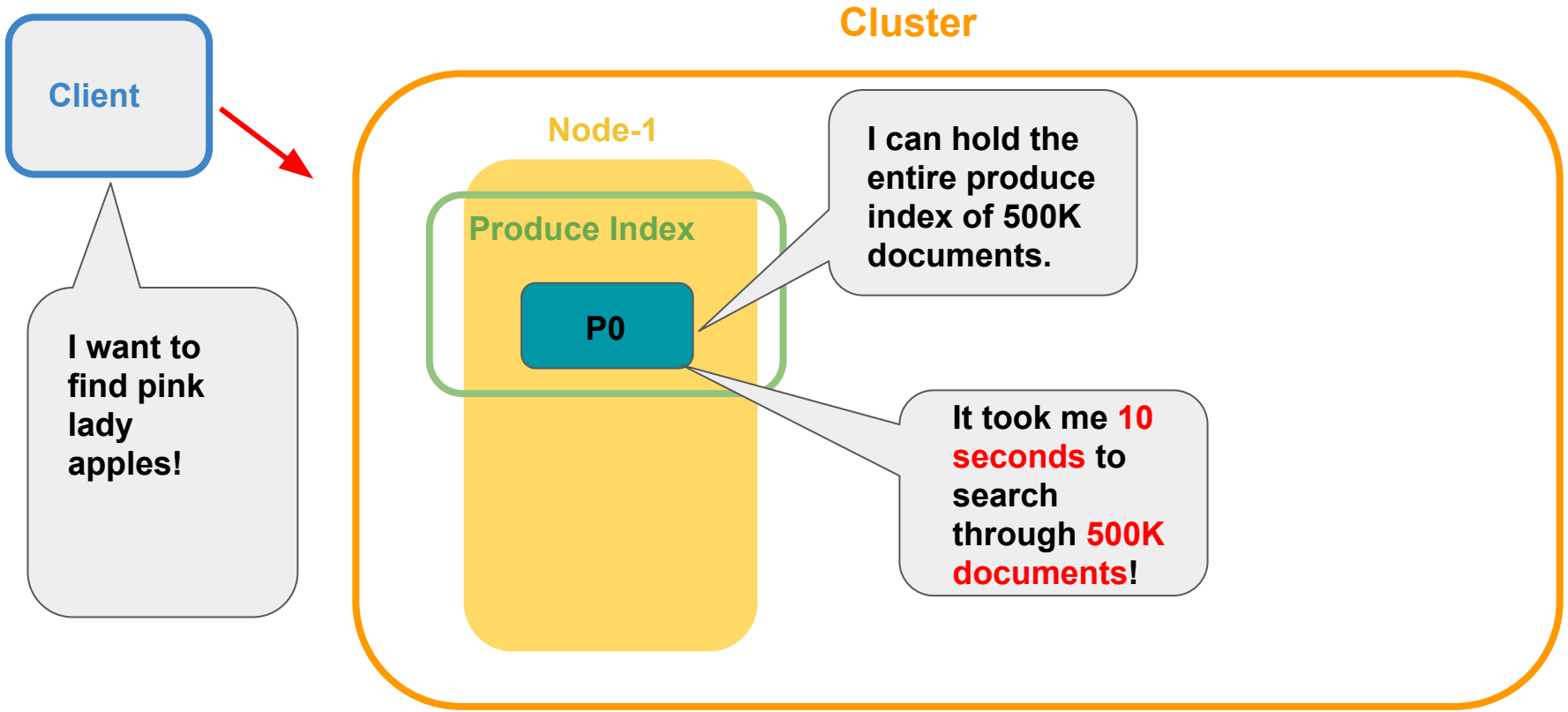
What is sharding?



What is sharding?



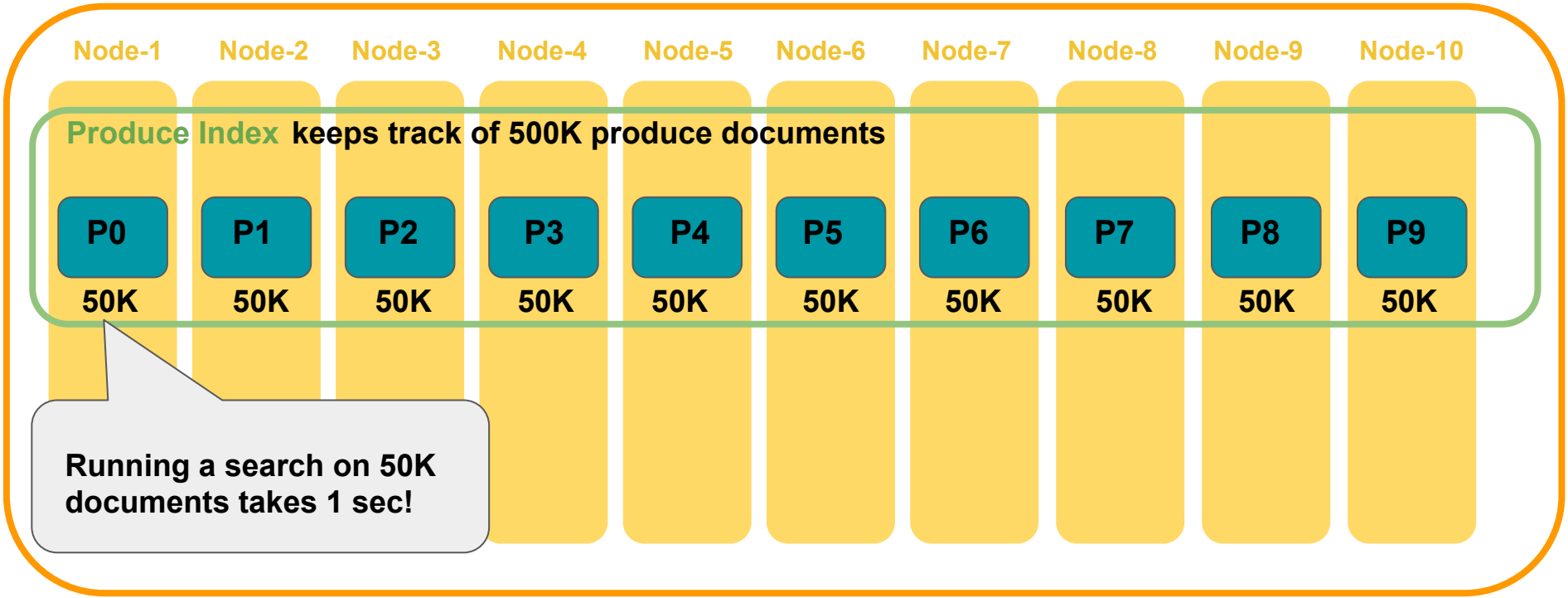
What is sharding?



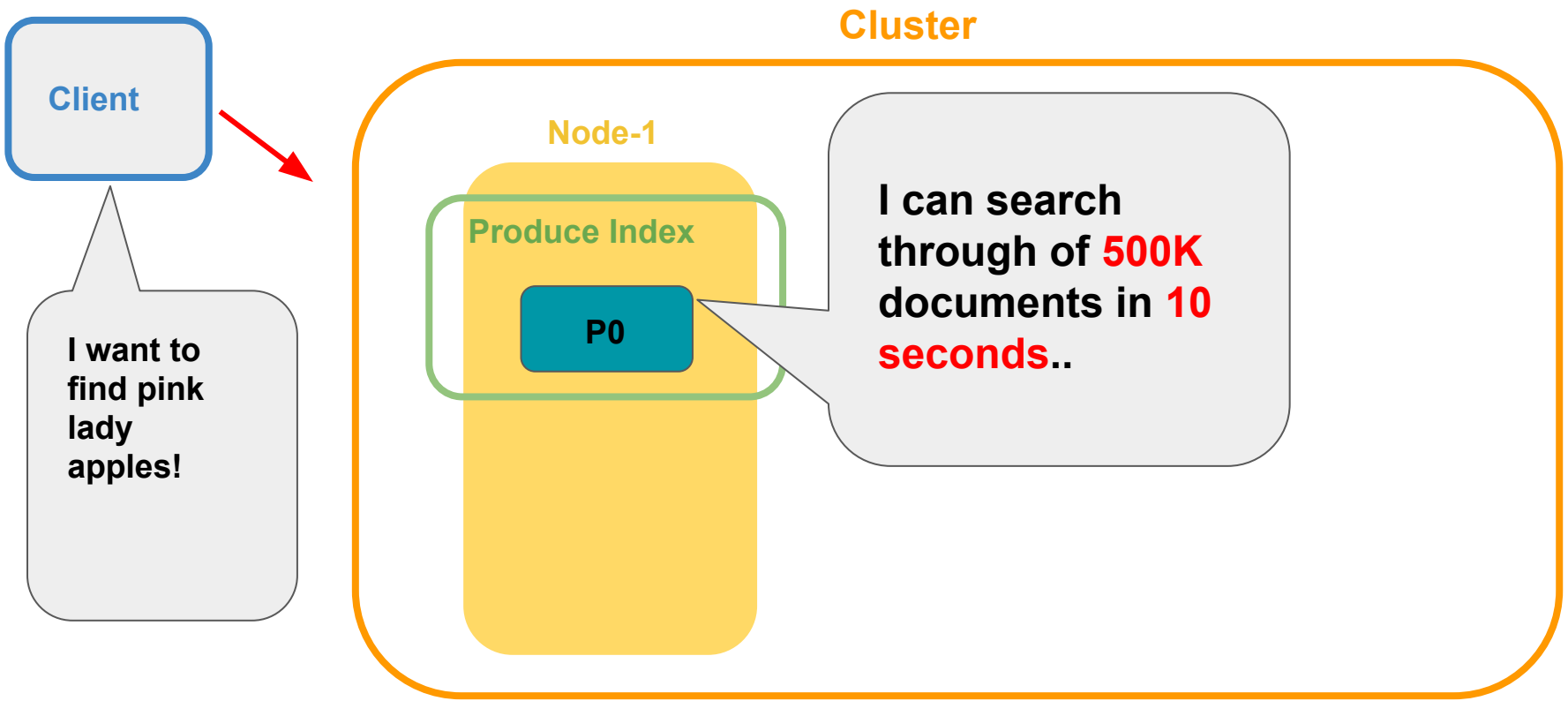
Sharding speeds up your search!

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

Cluster



What is 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

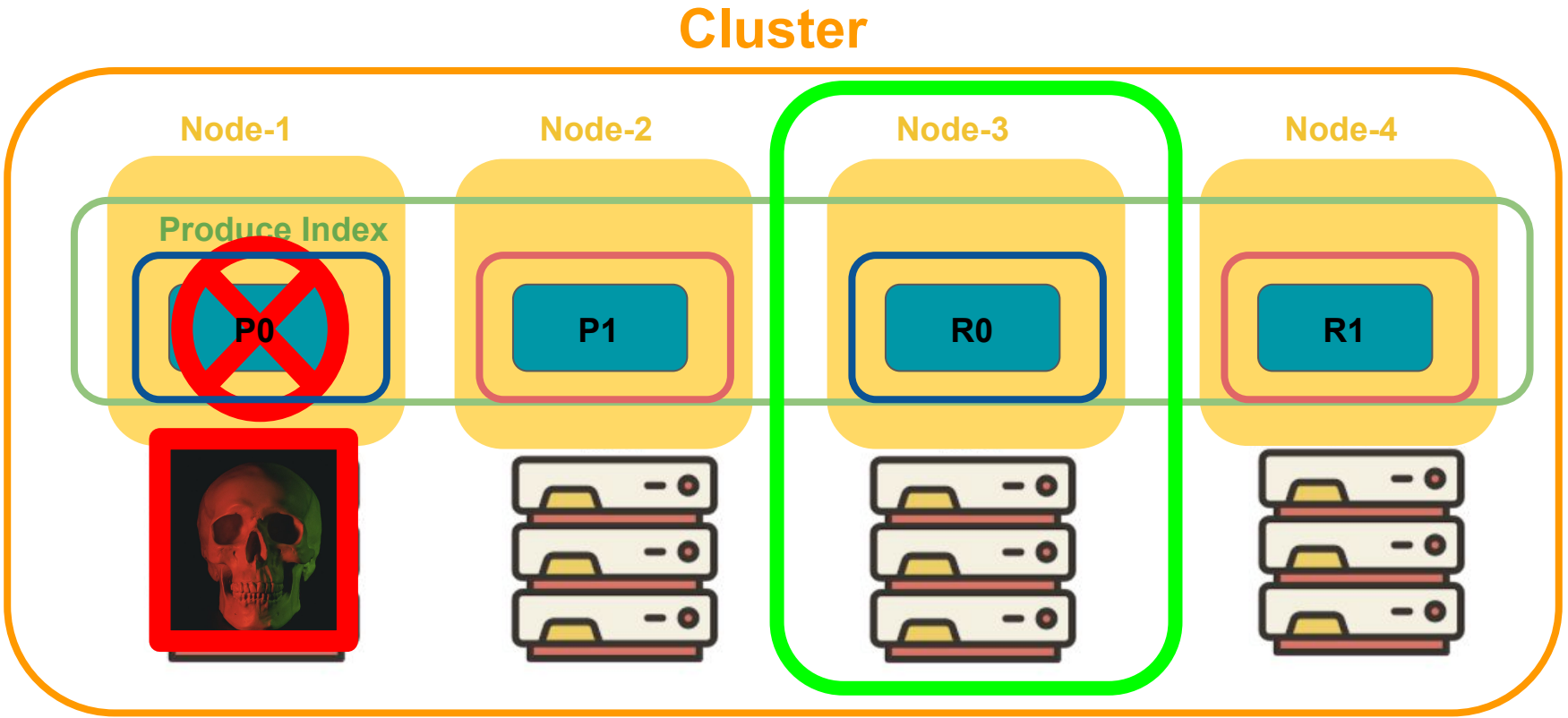
Produce Index

P0 P1 P2 P3 P4 P5 P6 P7 P8 P9

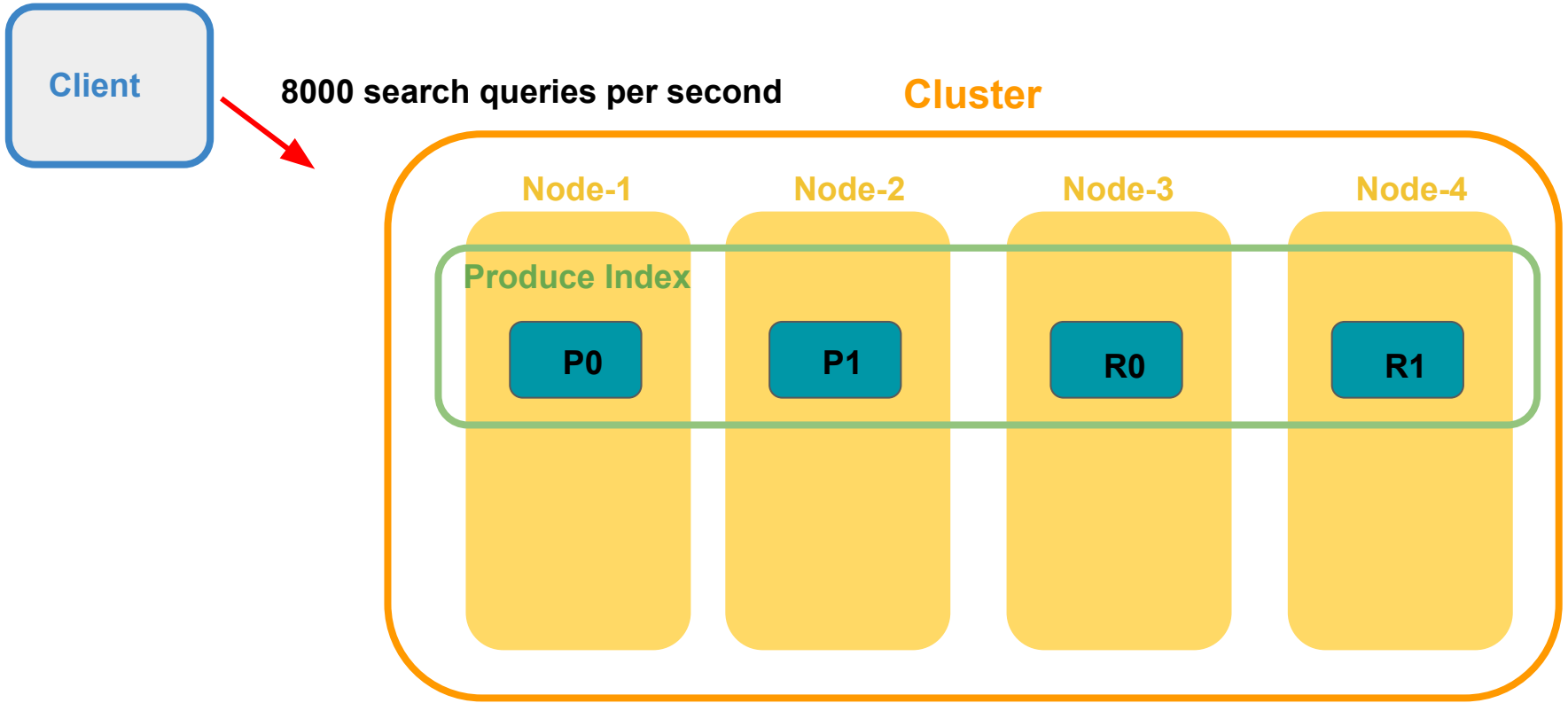
50K 50K 50K 50K 50K 50K 50K 50K 50K 50K


#SPONGEBOBMOVIE

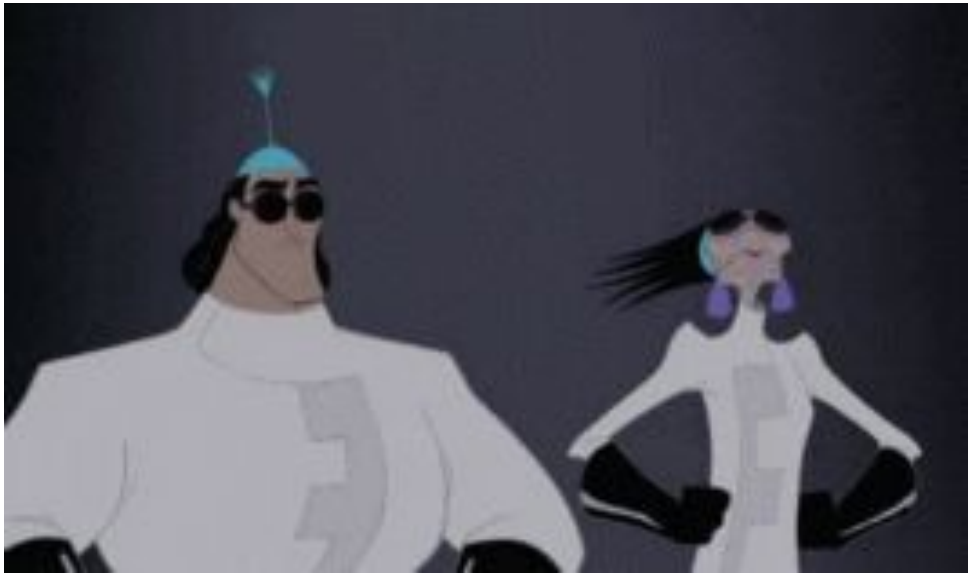
What are replica shards?



Replica shards can improve the performance of your search



Tutorial:
Performing CRUD Operations with Elasticsearch and Kibana



Deploy your way

Select a distribution model for your unique needs

Self-Managed

Install a single package

Elastic Cloud

Deploy instantly on AWS, Azure or Google Cloud

amazon web services™

Microsoft Azure

Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

Centrally manage multiple deployments on your infra

https://ela.st/beginners-table-of-contents

README.md

Table of Contents: Beginner's Crash Course to Elastic Stack Series

Who is this series for?

This series is open to all **developers** with little to no experience with the Elastic Stack or those who could use a refresher.

By the end of the series, you will be able to identify when to use Elasticsearch and Kibana and know how to get started with these products.

Table of contents for workshop repos

- Part 1: Intro to Elasticsearch and Kibana
- Part 2: Understanding the Relevance of Your Search with Elasticsearch and Kibana
- Part 3: Running Full Text Queries and Combined Queries with Elasticsearch and Kibana
- Part 4: Running Aggregations with Elasticsearch and Kibana
- Part 5: Understanding Mapping with Elasticsearch and Kibana
- Part 6: Troubleshooting Beginner Level Elasticsearch Errors

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

Beginner's Crash Course to Elastic Stack Series

Part 1: Intro to Elasticsearch & Kibana

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

This repo contains all resources shared during workshop Part 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, and Delete) operations with Elasticsearch and Kibana

Resources

Beginner's Crash Course to Elastic Stack Table of Contents This workshop is a part of the Beginner's Crash Course to Elastic Stack series. Check out this table contents to access all the workshops in the series thus far. This table will continue to get updated as more workshops in the series are released!

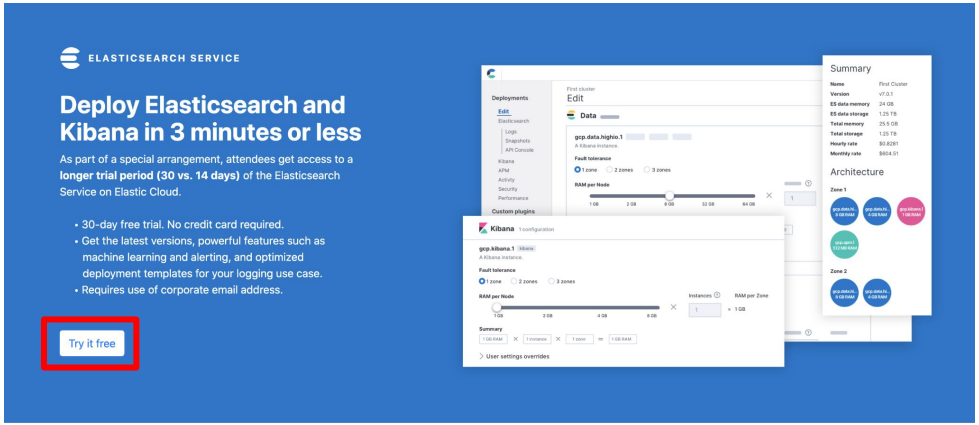
Free Elastic Cloud Trial

Instructions on how to access Elasticsearch and Kibana on Elastic Cloud

Instructions for downloading Elasticsearch and Kibana

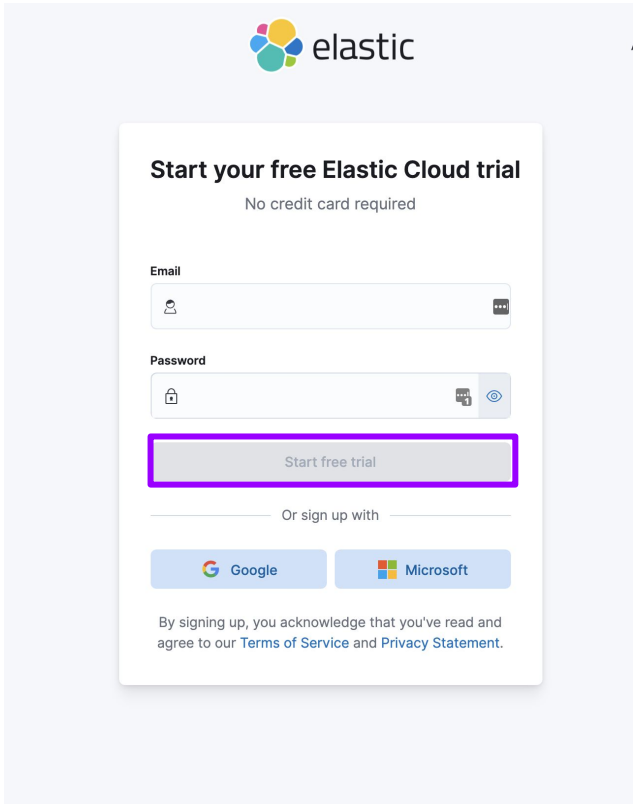
Presentation

Click on *Try it free* option

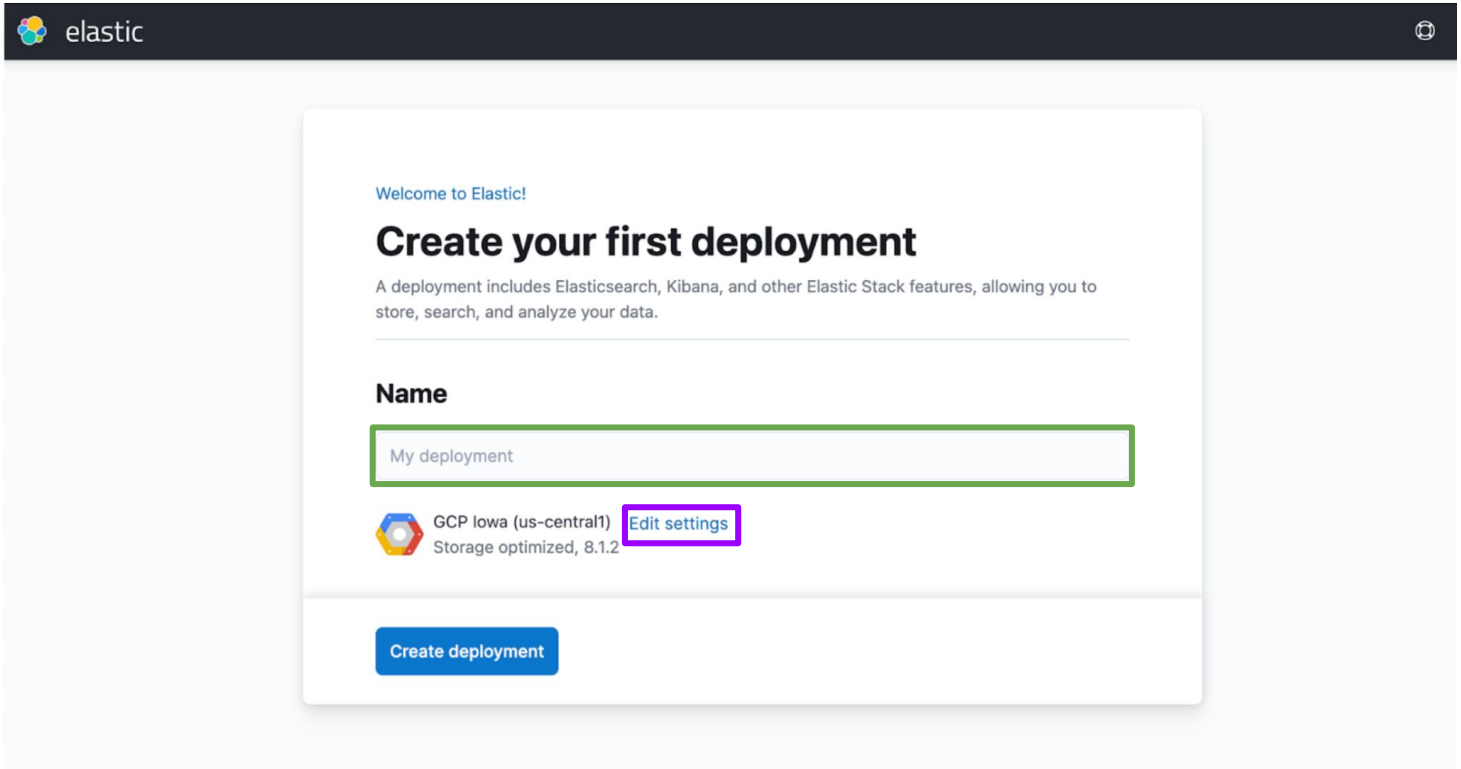


Trial comes with the following

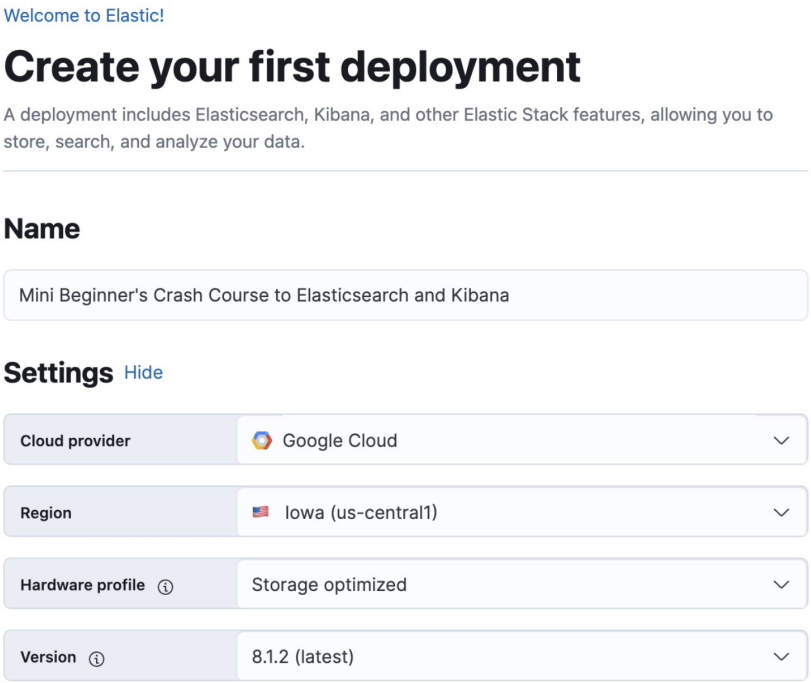
- 8 GB memory
- 240 GB storage
- High availability across two zones
- One-click upgrade to the latest versions of Kibana and Elasticsearch
- Advanced security features like authentication and role-based access control
- Alerting capabilities to trigger notifications
- Monitoring to optimize your cluster health
- Protect your cluster with Encryption at REST



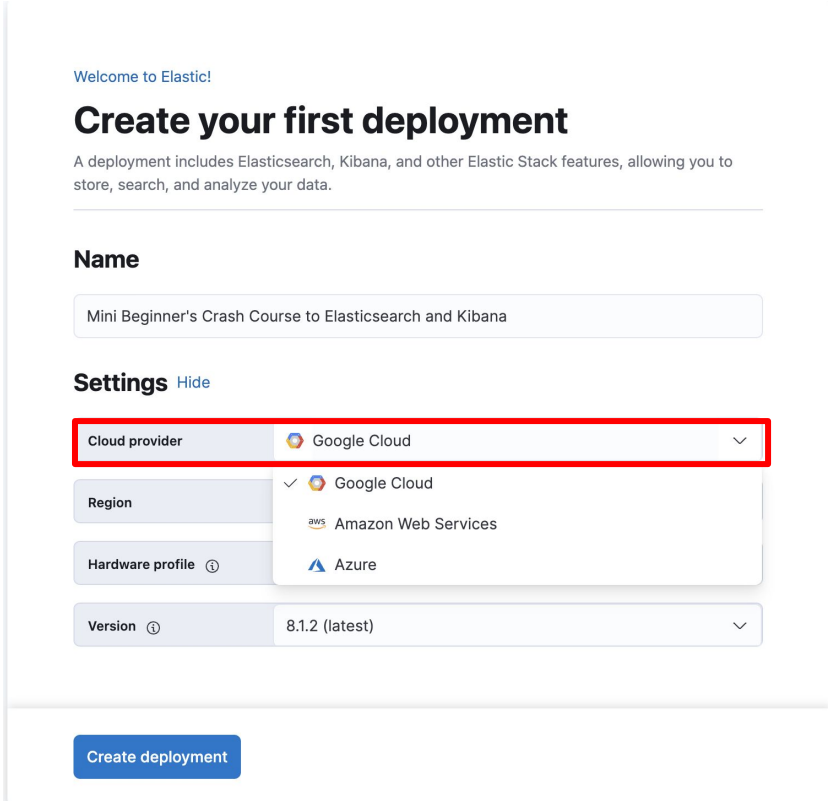
Name your deployment and click on *Edit settings* option



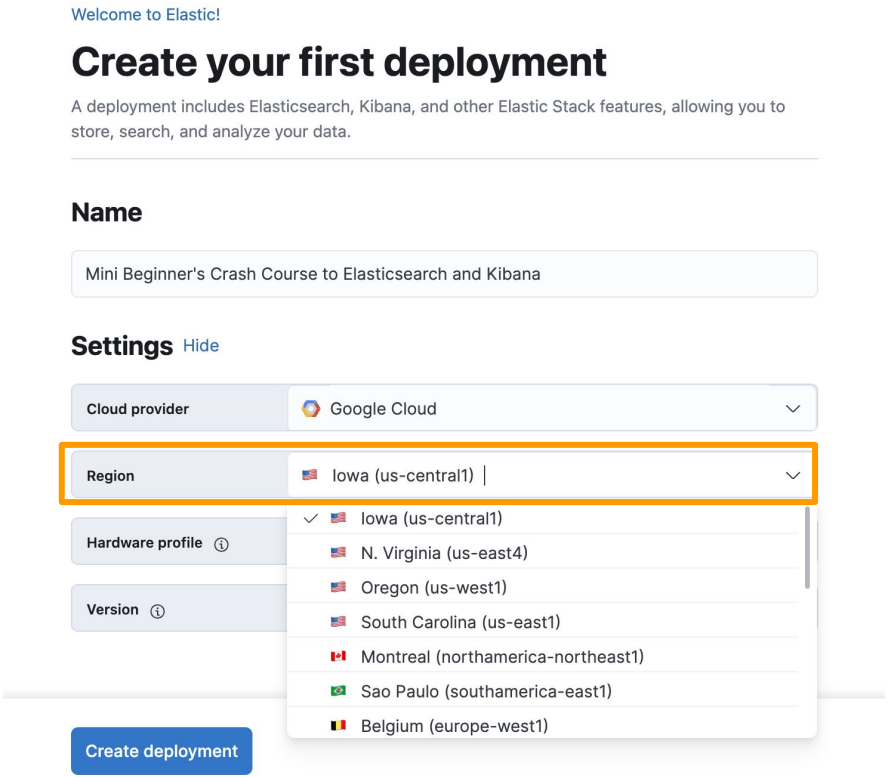
Configure your deployment settings



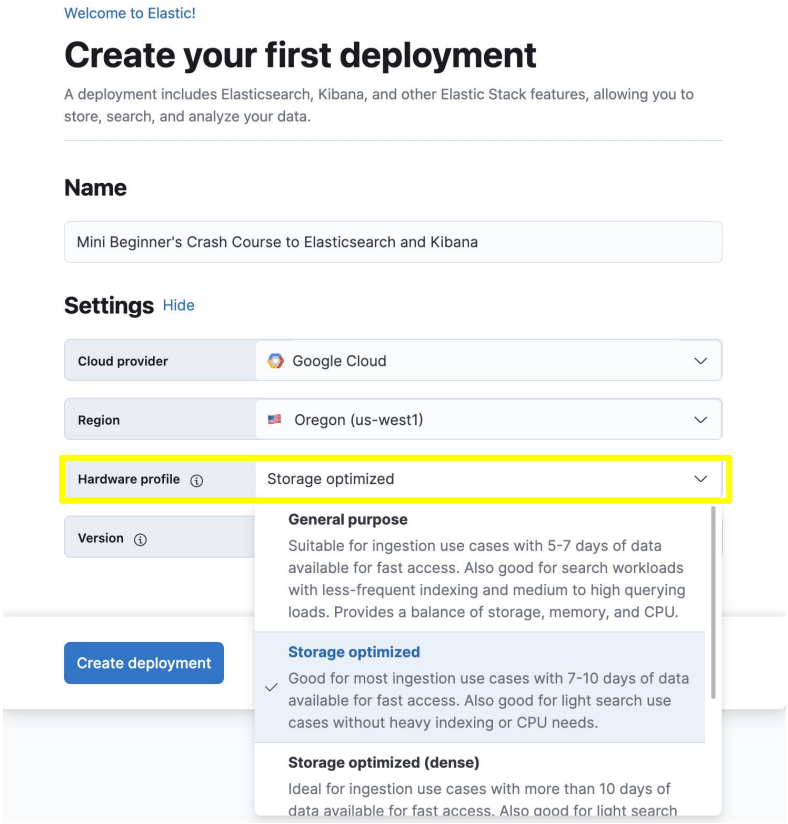
Choose the cloud provider of your choice



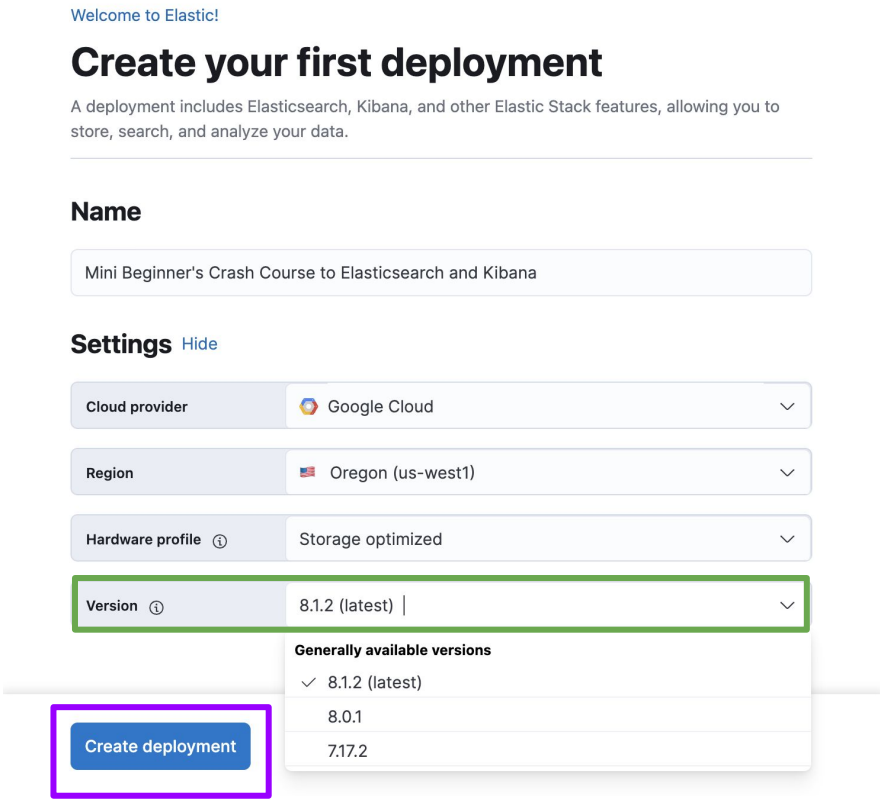
Select the region closest to you



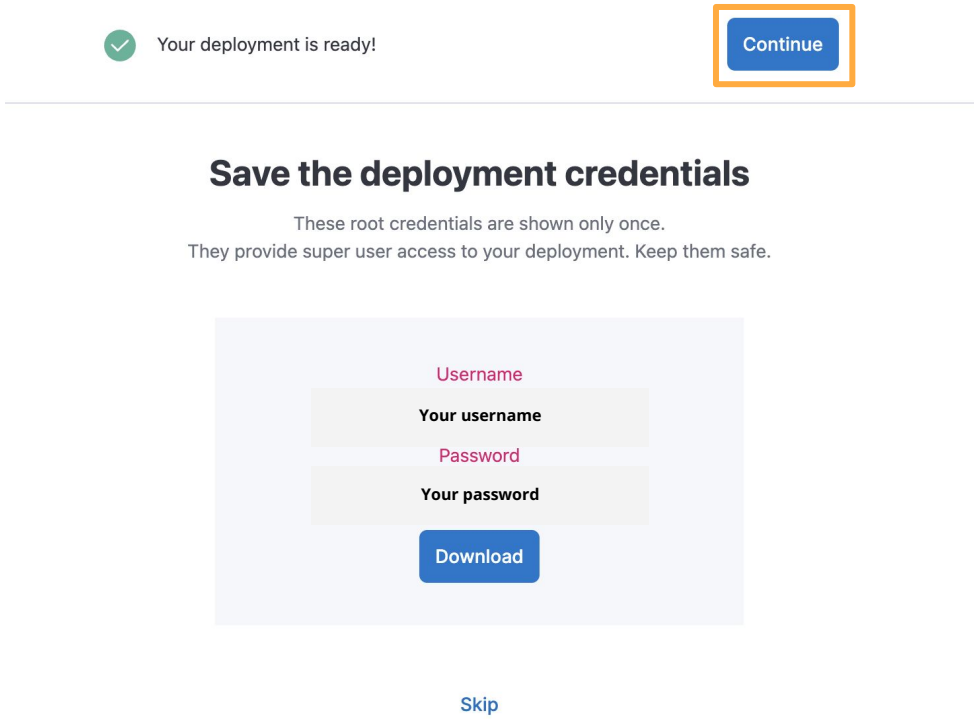
Select your hardware profile



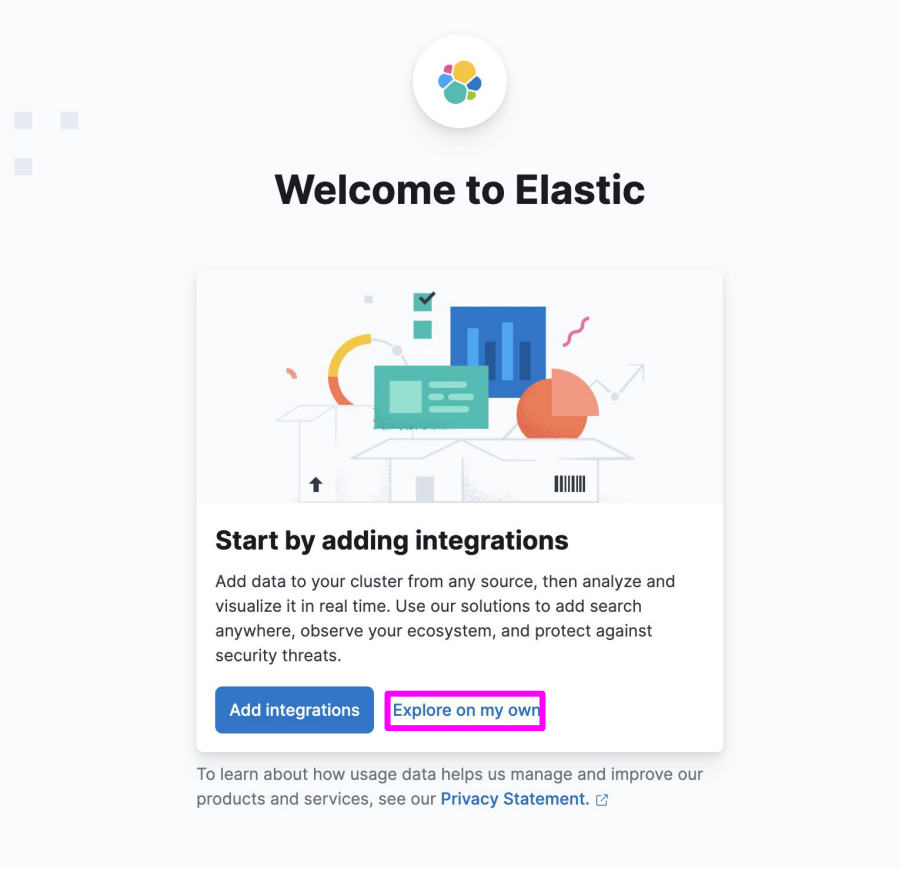
Select the latest version of the Elastic Stack



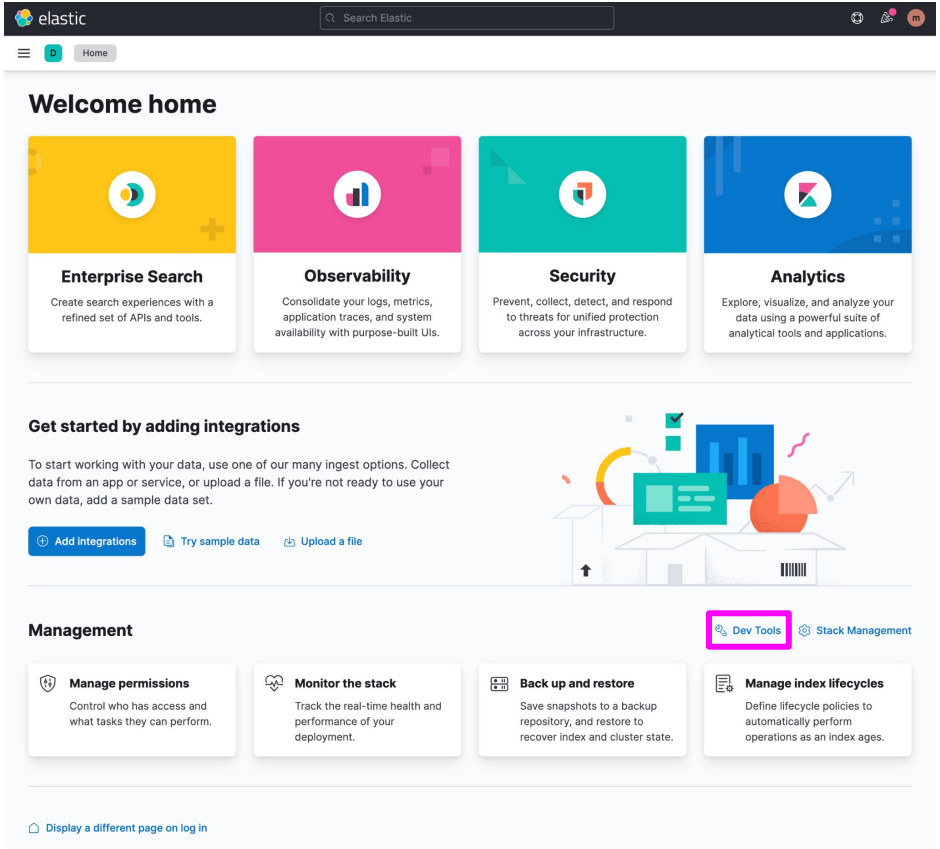
Save your deployment credentials



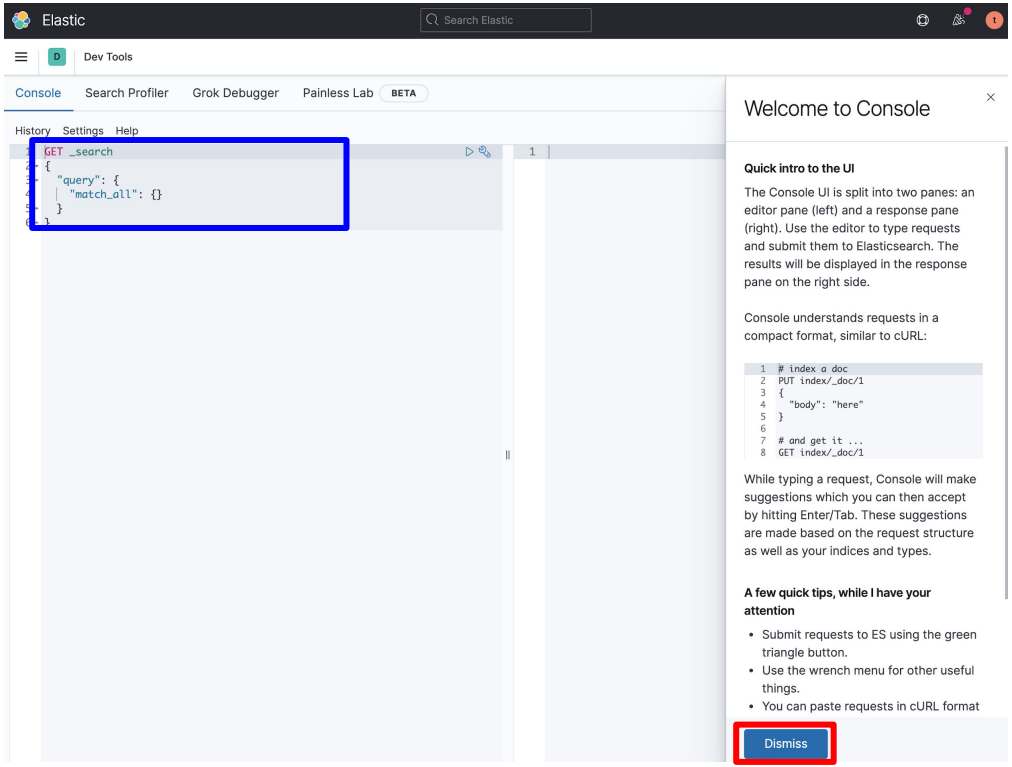
Click on *Explore on my own* option

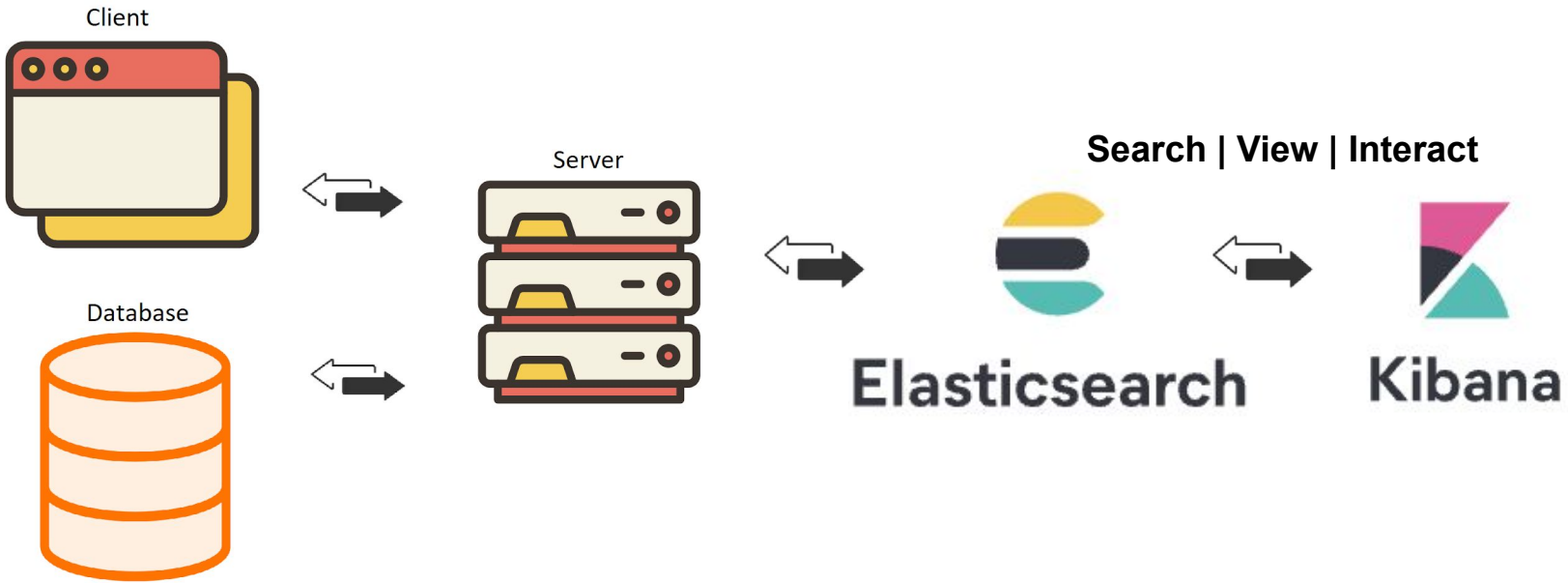


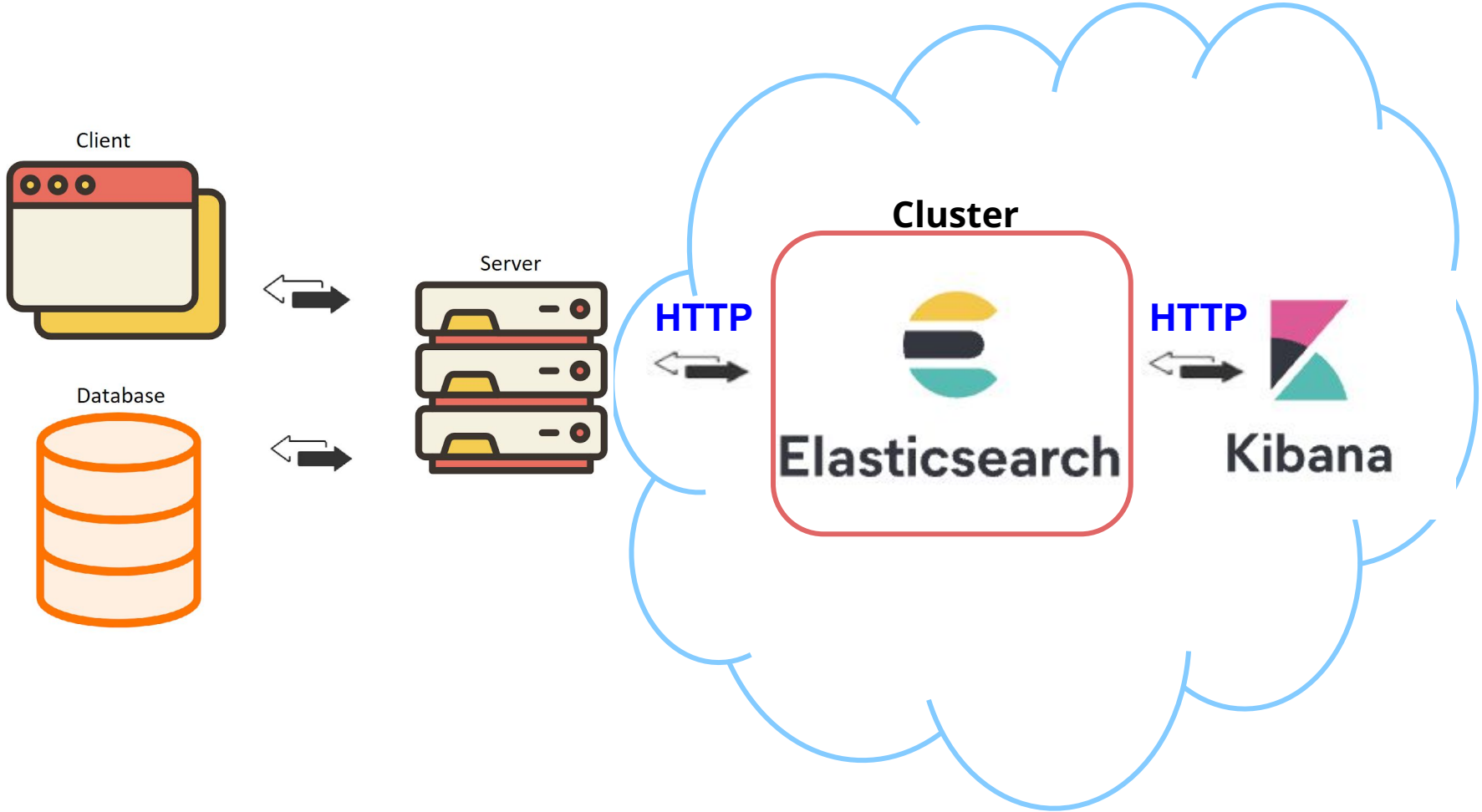
Click on *Dev Tools* option



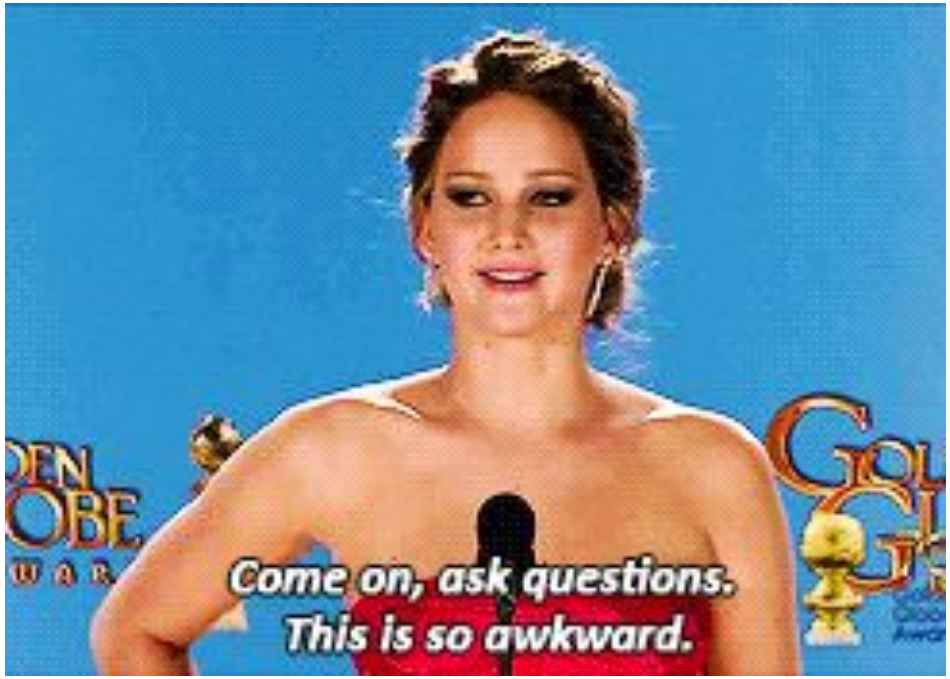
Click on dismiss and delete the default query




Client
Database
Server
Search | View | Interact
Elasticsearch
Kibana


Client
Database
Server
HTTP
Cluster
Elasticsearch
HTTP
Kibana

Questions?



Want to continue learning about Elasticsearch & Kibana?

- **Beginner's Crash Course to Elastic Stack**
  - https://ela.st/beginners-crash-course
- **Mini Beginner's Crash Course to Elasticsearch & Kibana**
  - https://ela.st/mini-beginners-crash-course


Lisa Jung

Developer Advocate @ Elastic

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

Blog: https://dev.to/lisahjung

Twitter: @LisaHJung