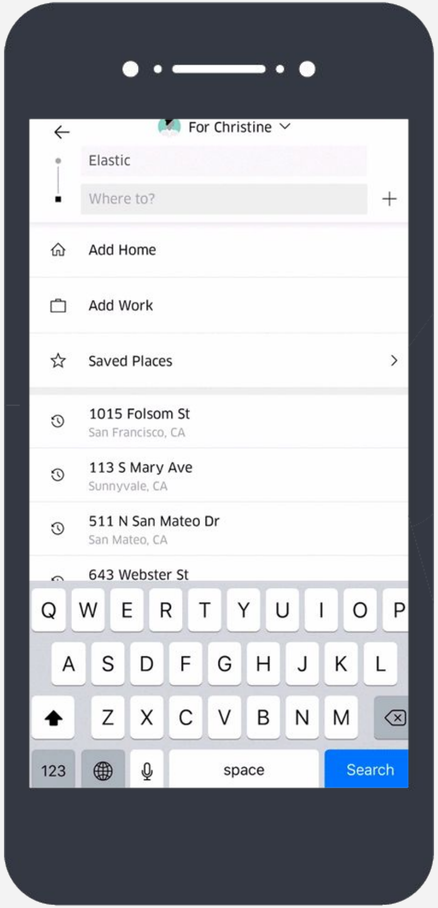
elastic

Beginner’s Crash Course to the Elastic Stack

Part 1.1: Intro to Elasticsearch & Kibana

Lisa Jung
Developer Advocate @Elastic

Searching for **Rides**



For Christine

Elastic

Where to?

Add Home

Add Work

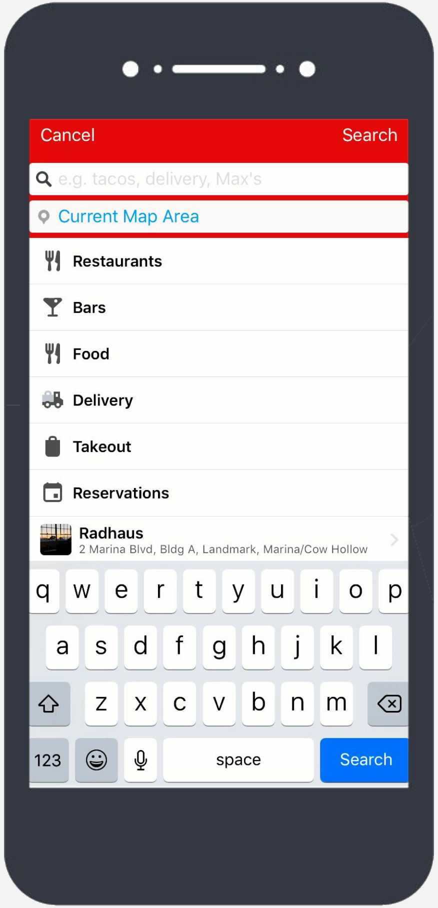
Saved Places

1015 Folsom St
San Francisco, CA

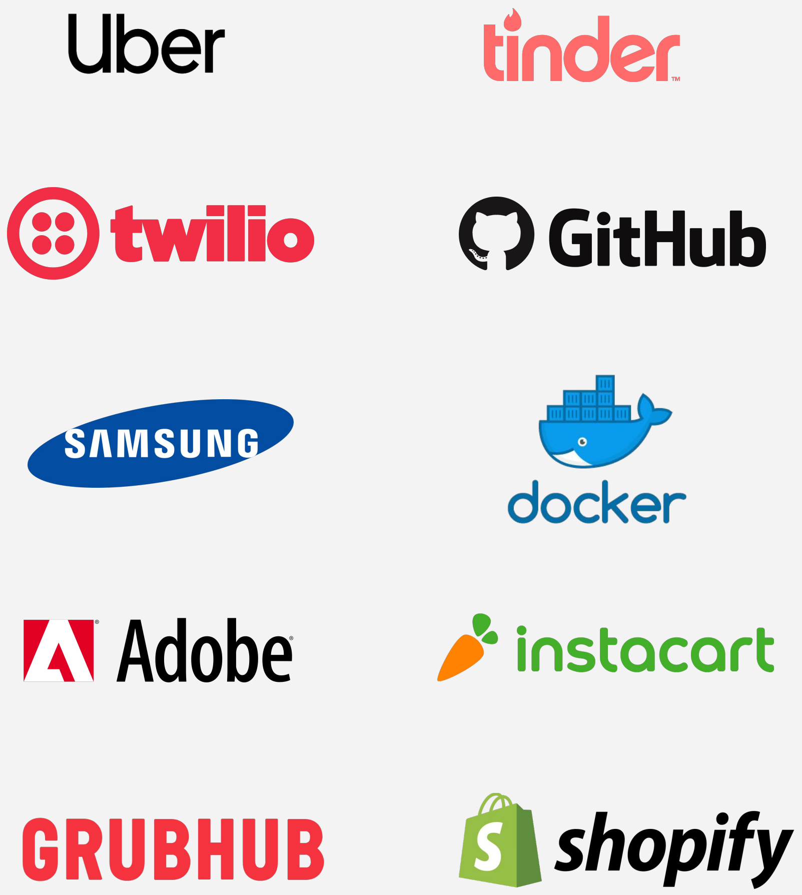
113 S Mary Ave
Sunnyvale, CA

511 N San Mateo Dr
San Mateo, CA

643 Webster St



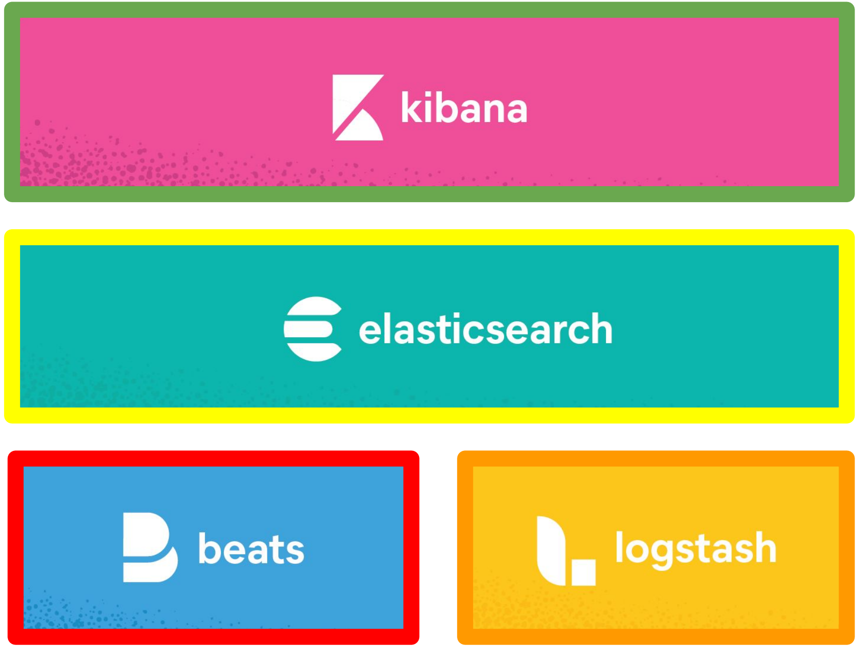
Searching for Restaurants



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.



kibana

elasticsearch

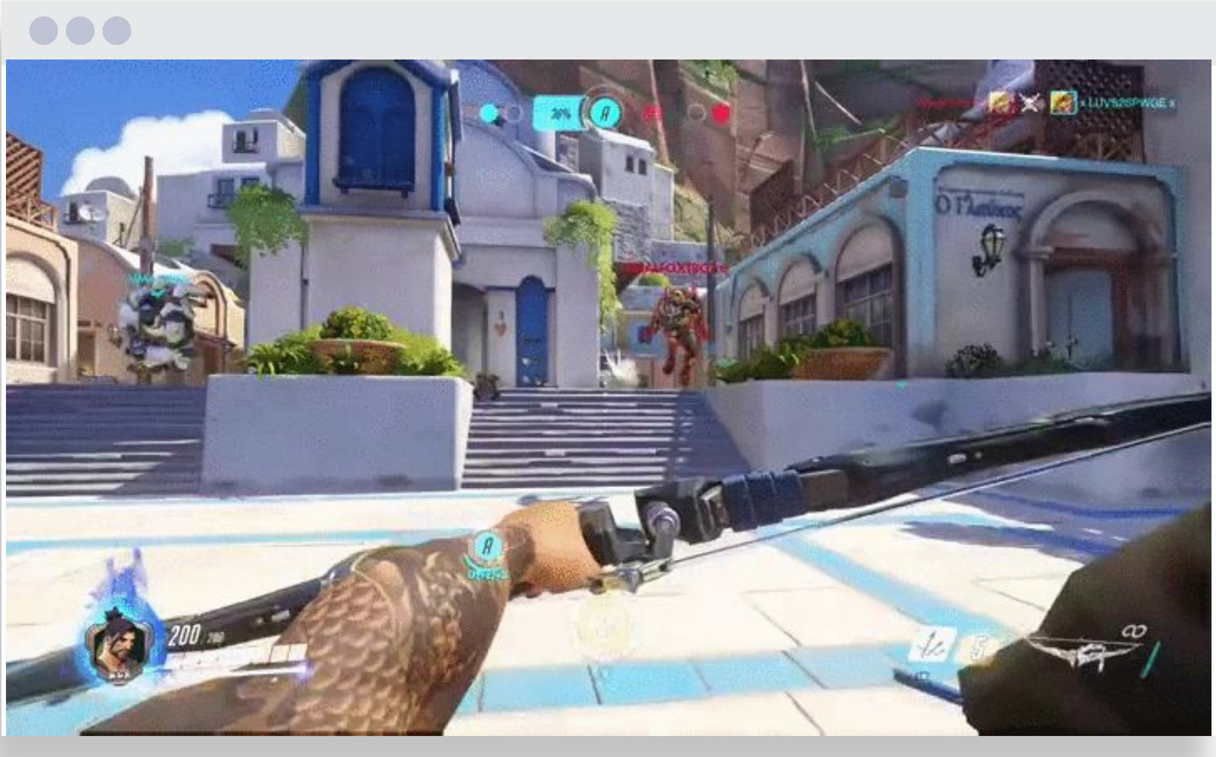
beats

logstash

Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

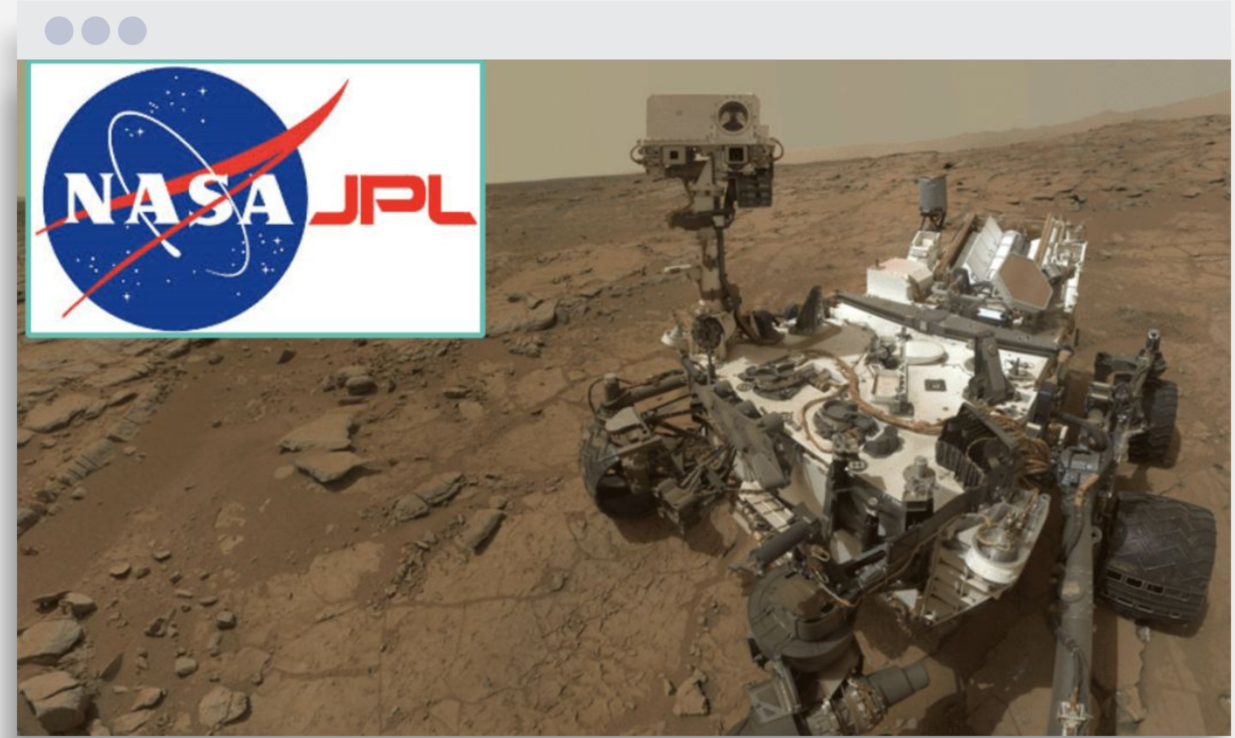
Use Case: Logging



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

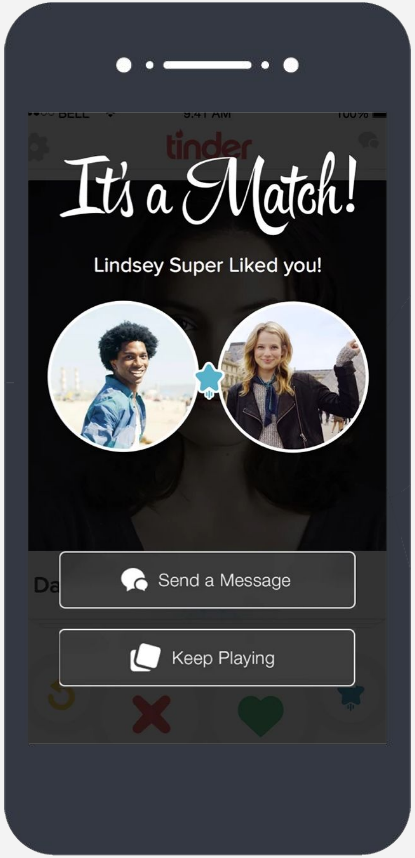
ACTIVISION
BLIZZARD

Use Case: Metrics



Use Case: Security Analytics

Use Case: Business Analytics



It's a Match!

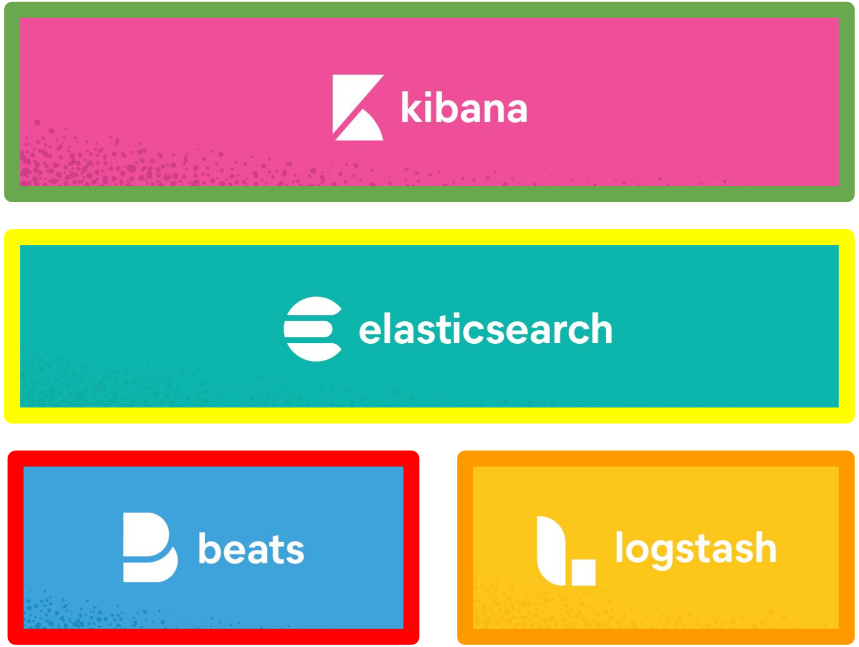
Lindsey Super Liked you!

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.



kibana

elasticsearch

beats

logstash

elastic

Beginner's Crash Course to Elastic Stack

Part 1.1: Intro to Elasticsearch and Kibana

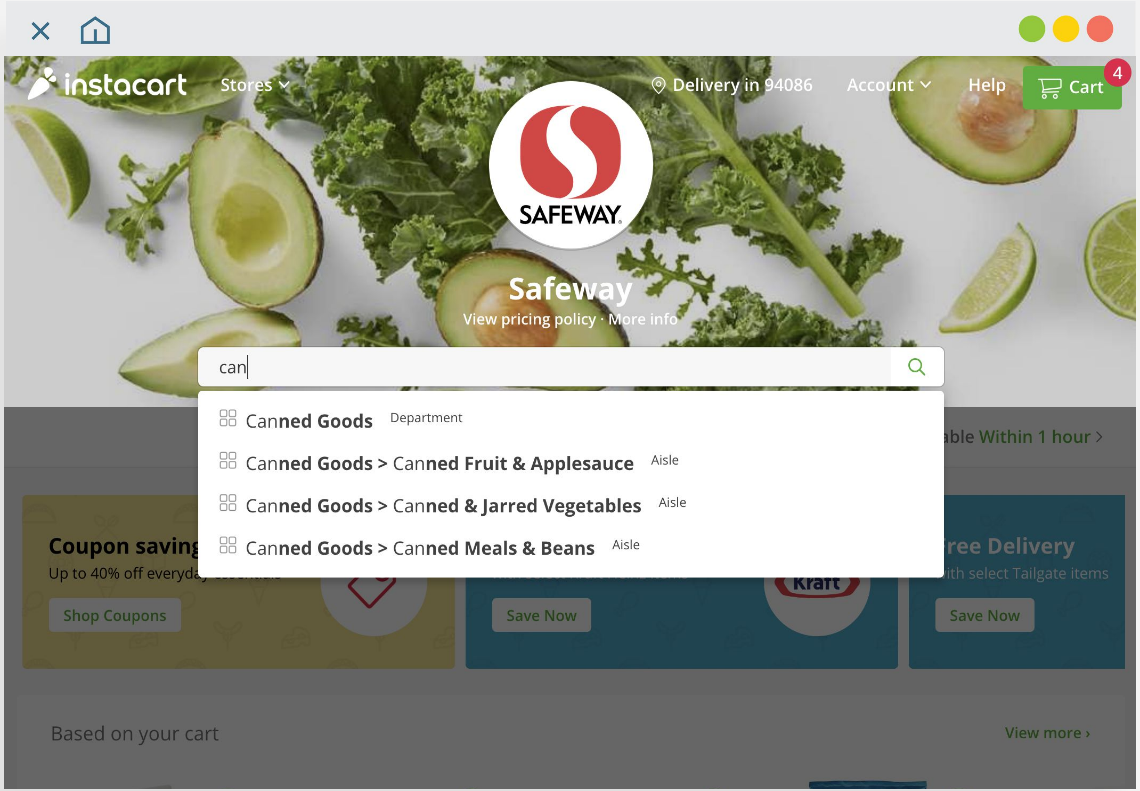
By the end of this workshop, you will be able to:

- 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

Elasticsearch

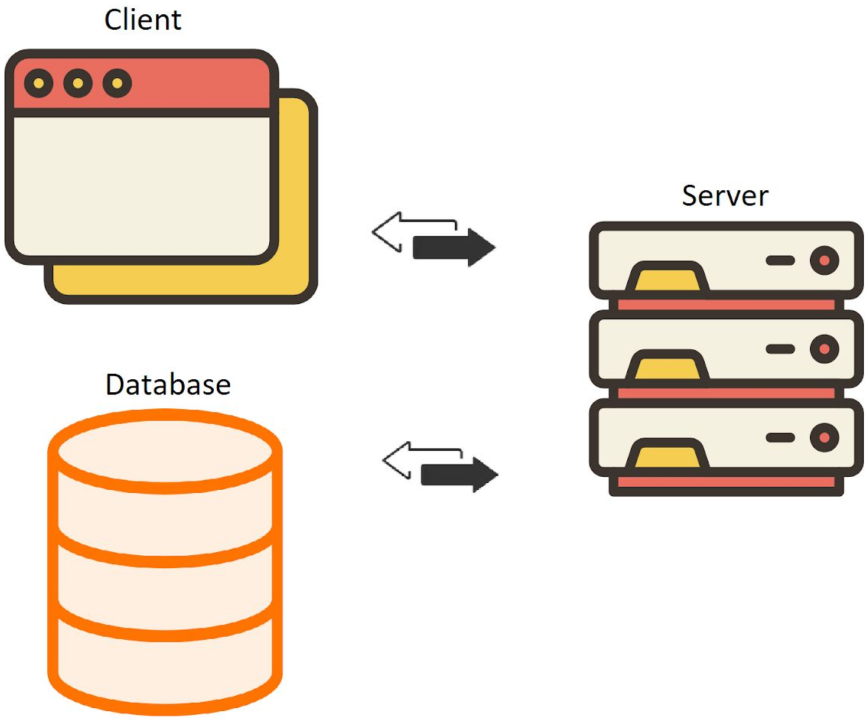
Store | Search | Analyze

instacart



can

Canned Goods	Department
Canned Goods > Canned Fruit & Applesauce	Aisle
Canned Goods > Canned & Jarred Vegetables	Aisle
Canned Goods > Canned Meals & Beans	Aisle



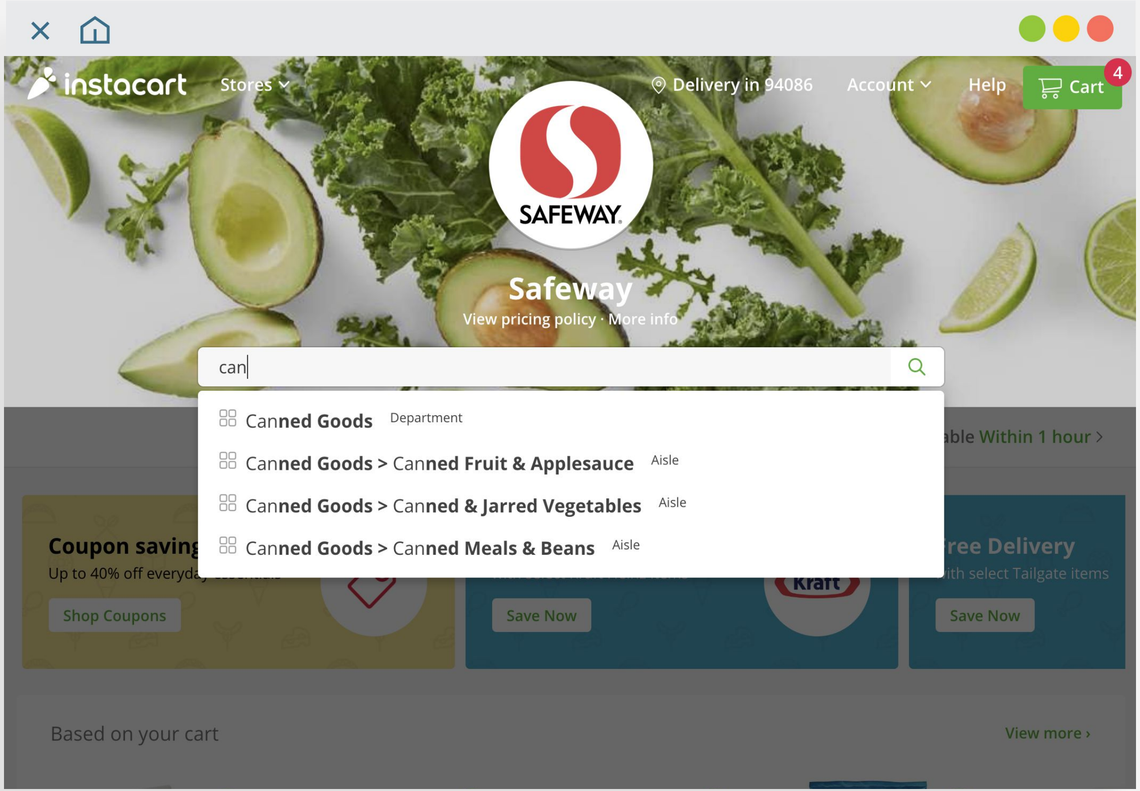
Client

Server

Database

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

instacart



can

Canned Goods Department

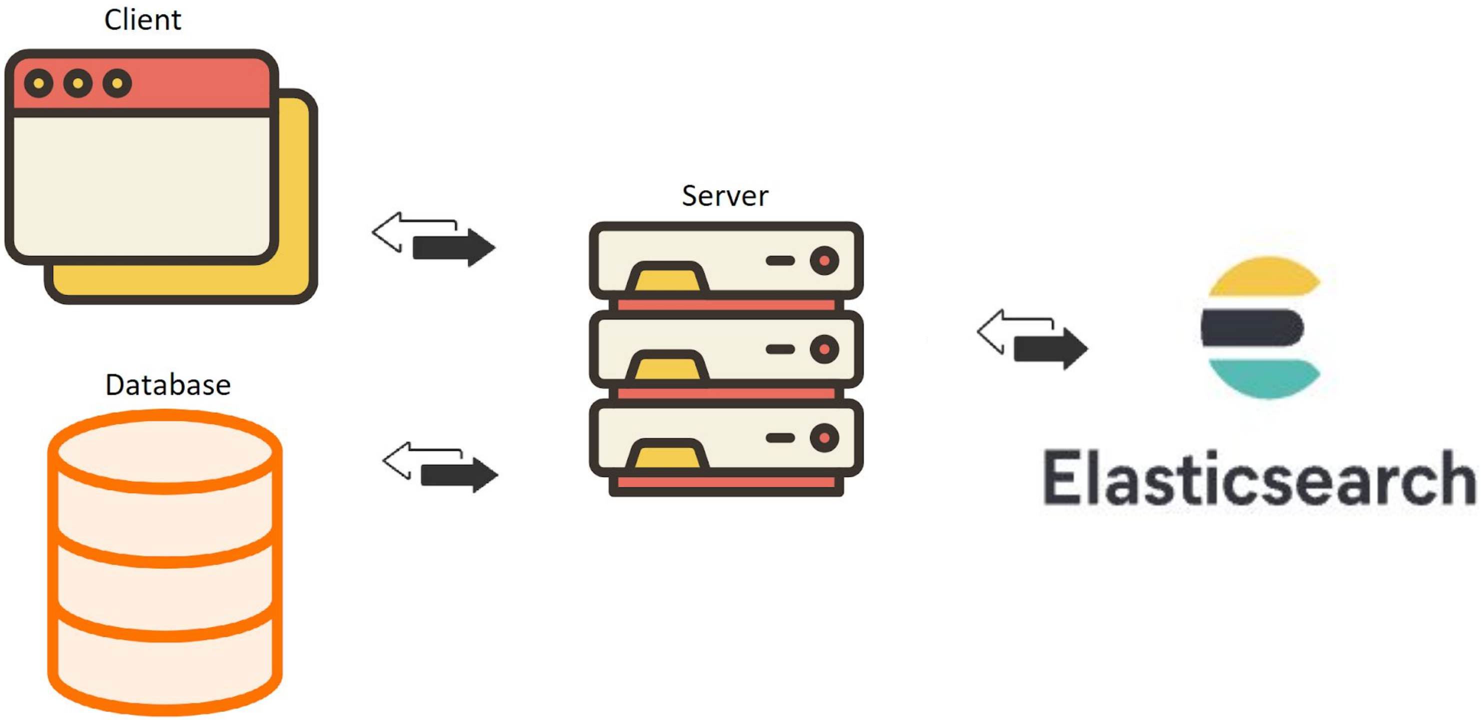
Canned Goods > Canned Fruit & Applesauce Aisle

Canned Goods > Canned & Jarred Vegetables Aisle

Canned Goods > Canned Meals & Beans Aisle

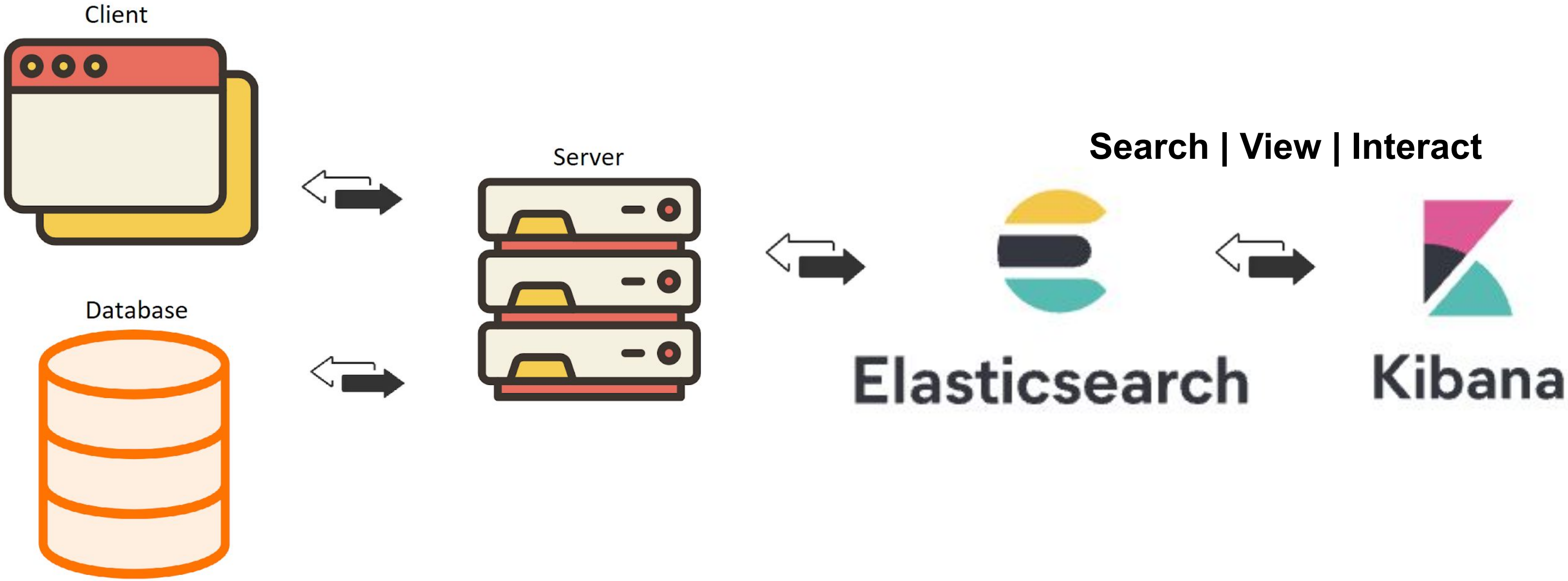
Find me a list of peanut butter brands. I want highest rated brands at the top.

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

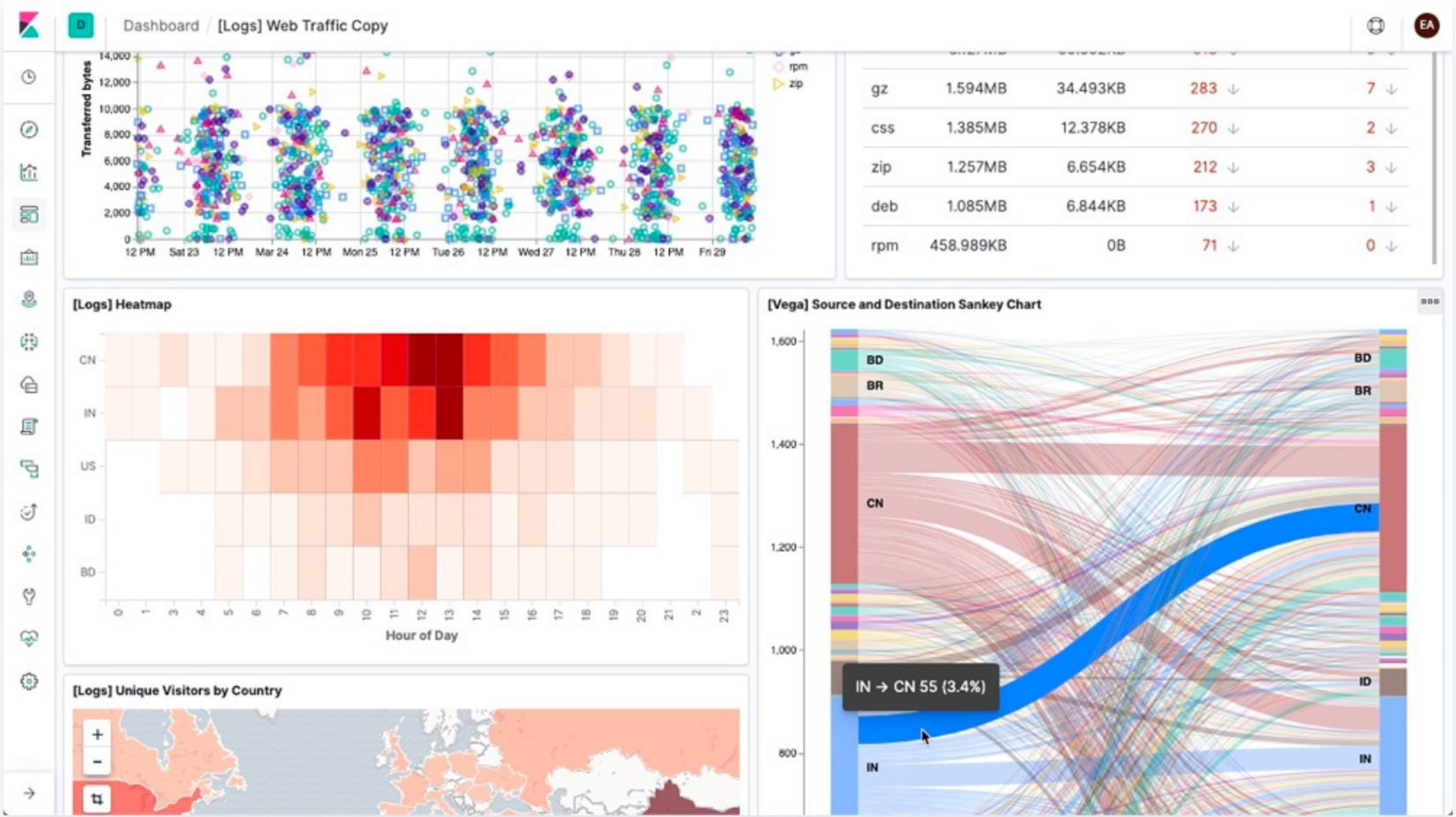

Client
Server
Database
Elasticsearch

Elasticsearch

Store | Search | Analyze



Search | View | Interact



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

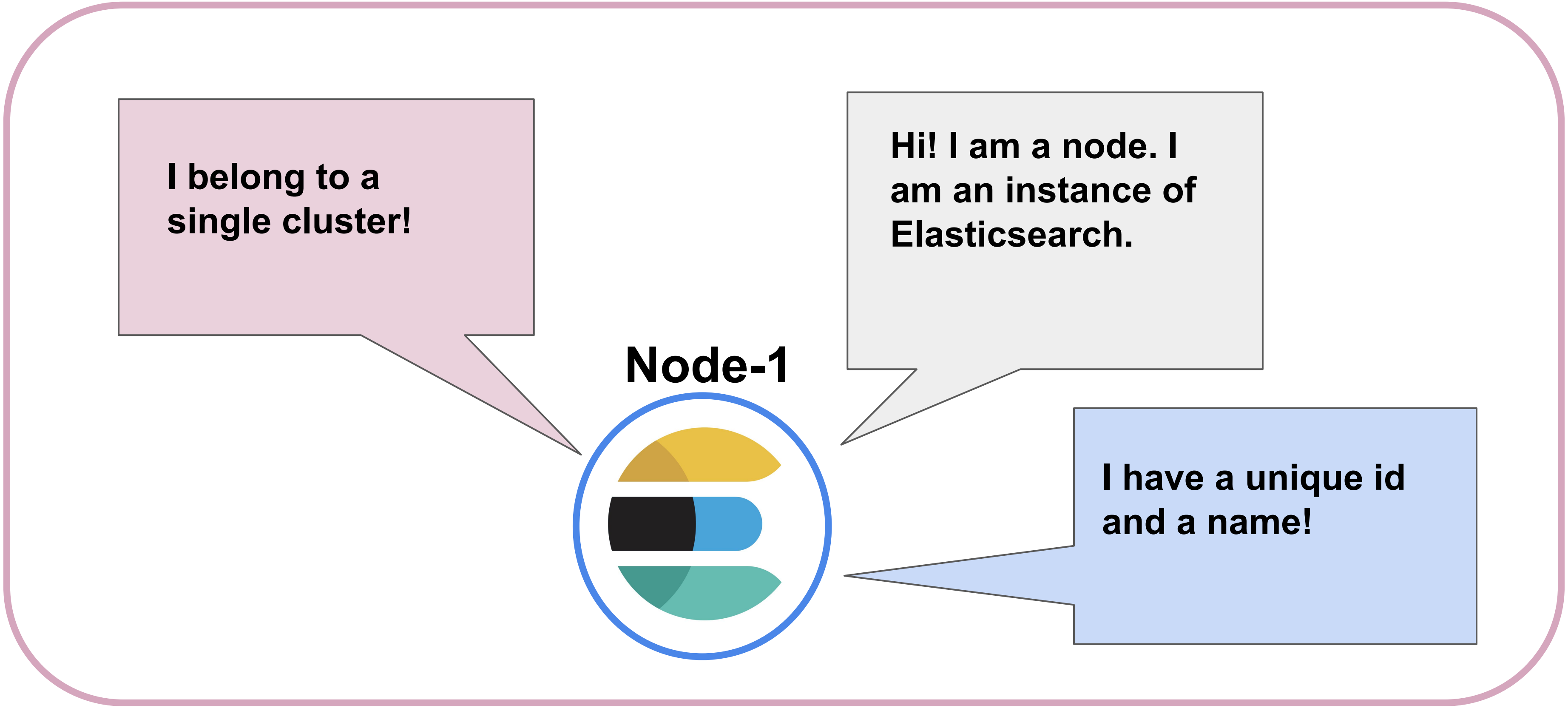
By the end of this workshop, you will be able to:

- 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



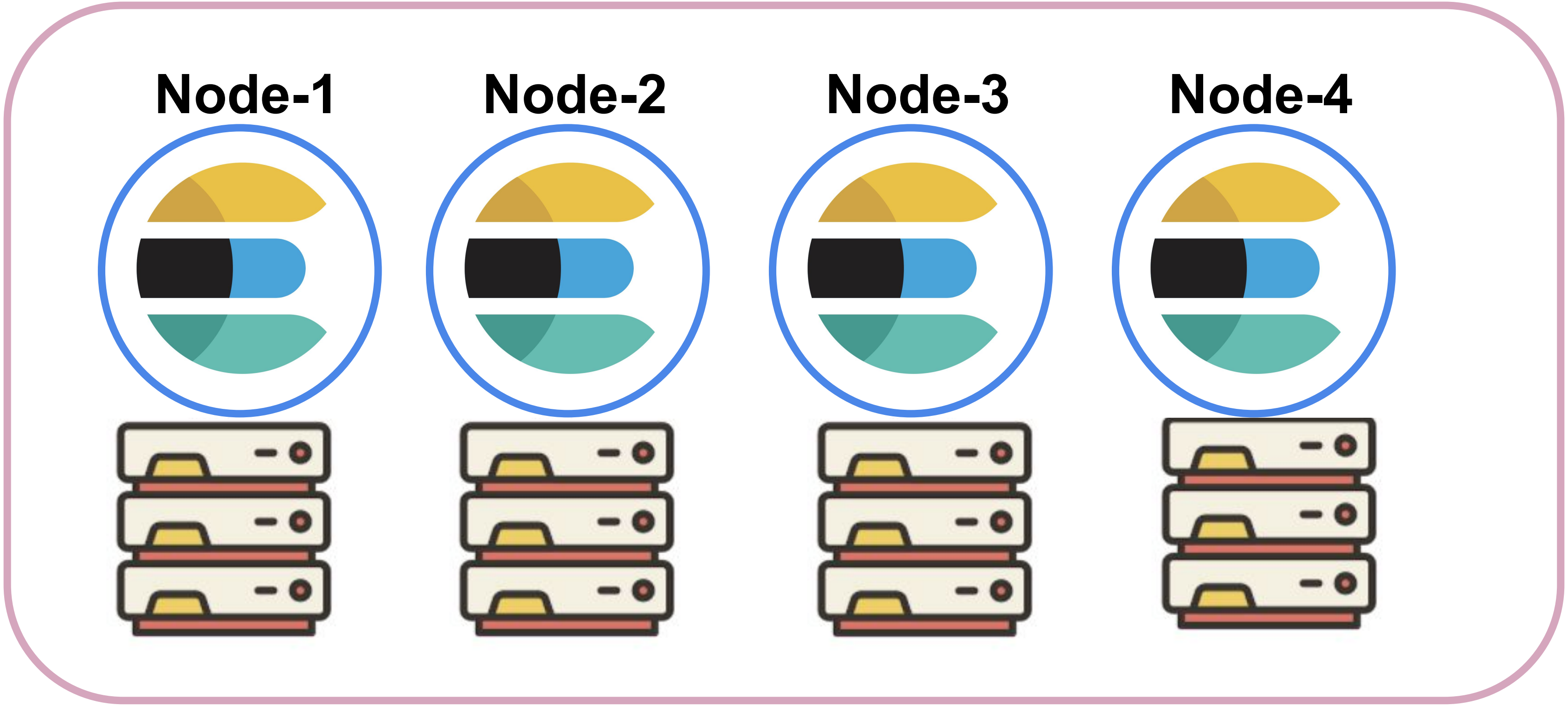
I belong to a single cluster!

Hi! I am a node. I am an instance of Elasticsearch.

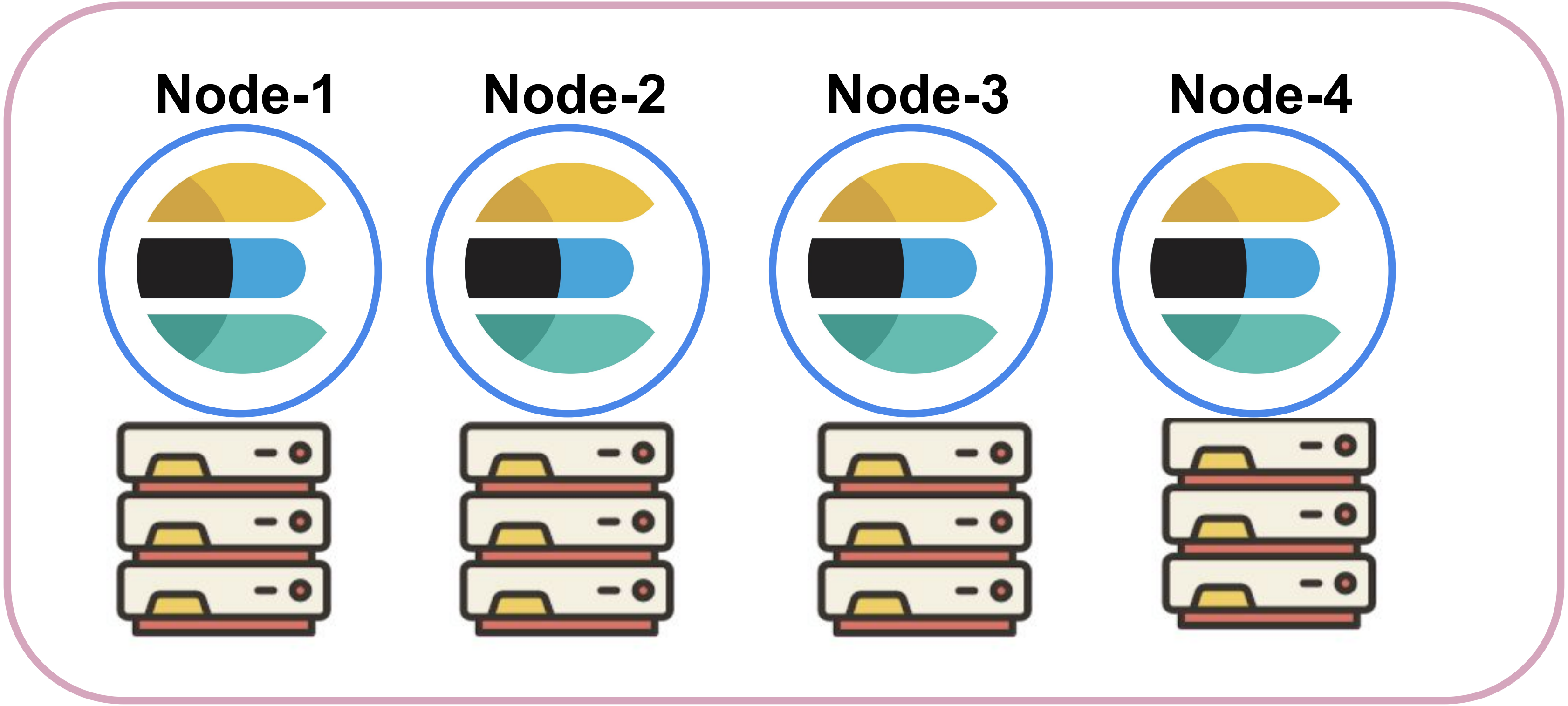
Node-1

I have a unique id and a name!

Cluster



Cluster



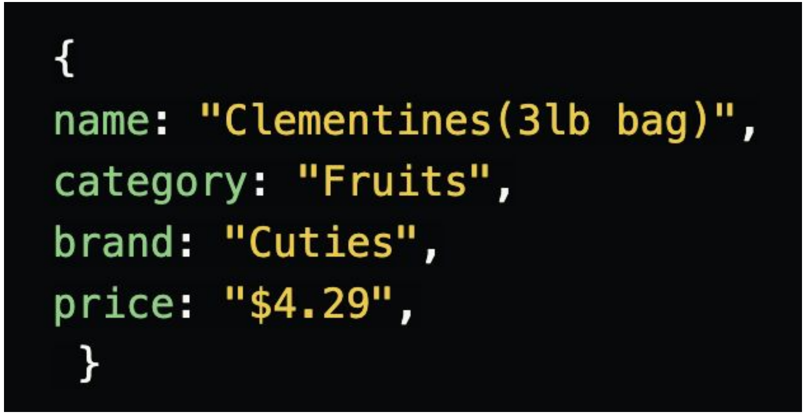
Node-1

Node-2

Node-3

Node-4

Data is stored as documents!

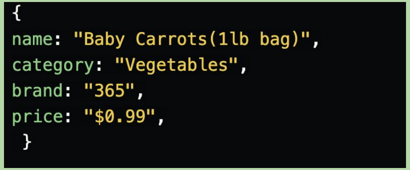


```
{
name: "Clementines(3lb bag)",
category: "Fruits",
brand: "Cuties",
price: "$4.29",
 }
```

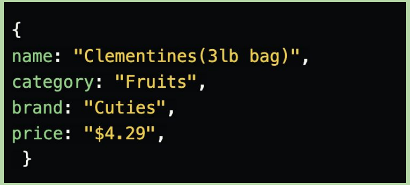
I am a document, a JSON object that is stored in Elasticsearch under a unique ID!

Document grouped into an index!

Produce Index

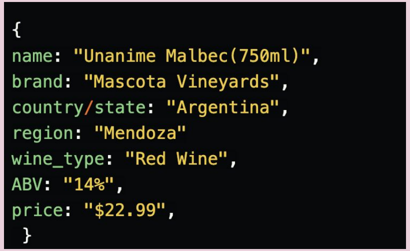


```
{
name: "Baby Carrots(1lb bag)",
category: "Vegetables",
brand: "365",
price: "$0.99",
 }
```

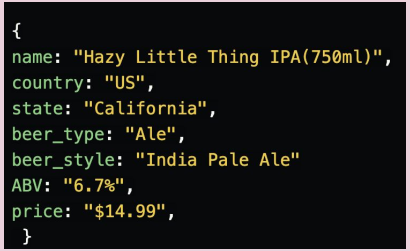


```
{
name: "Clementines(3lb bag)",
category: "Fruits",
brand: "Cuties",
price: "$4.29",
 }
```

Wine & Beer Index

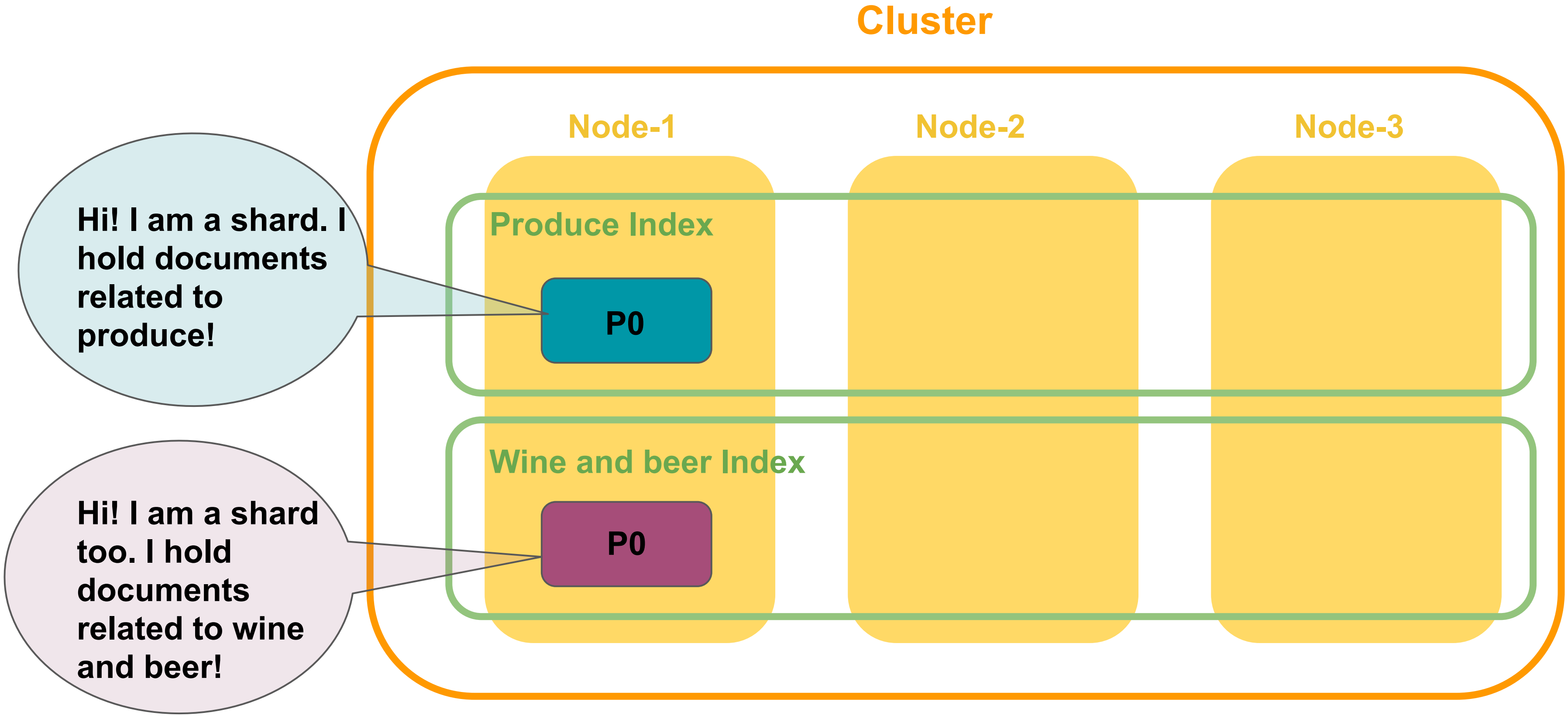


```
{
name: "Unanime Malbec(750ml)",
brand: "Mascota Vineyards",
country/state: "Argentina",
region: "Mendoza"
wine_type: "Red Wine",
ABV: "14%",
price: "$22.99",
 }
```



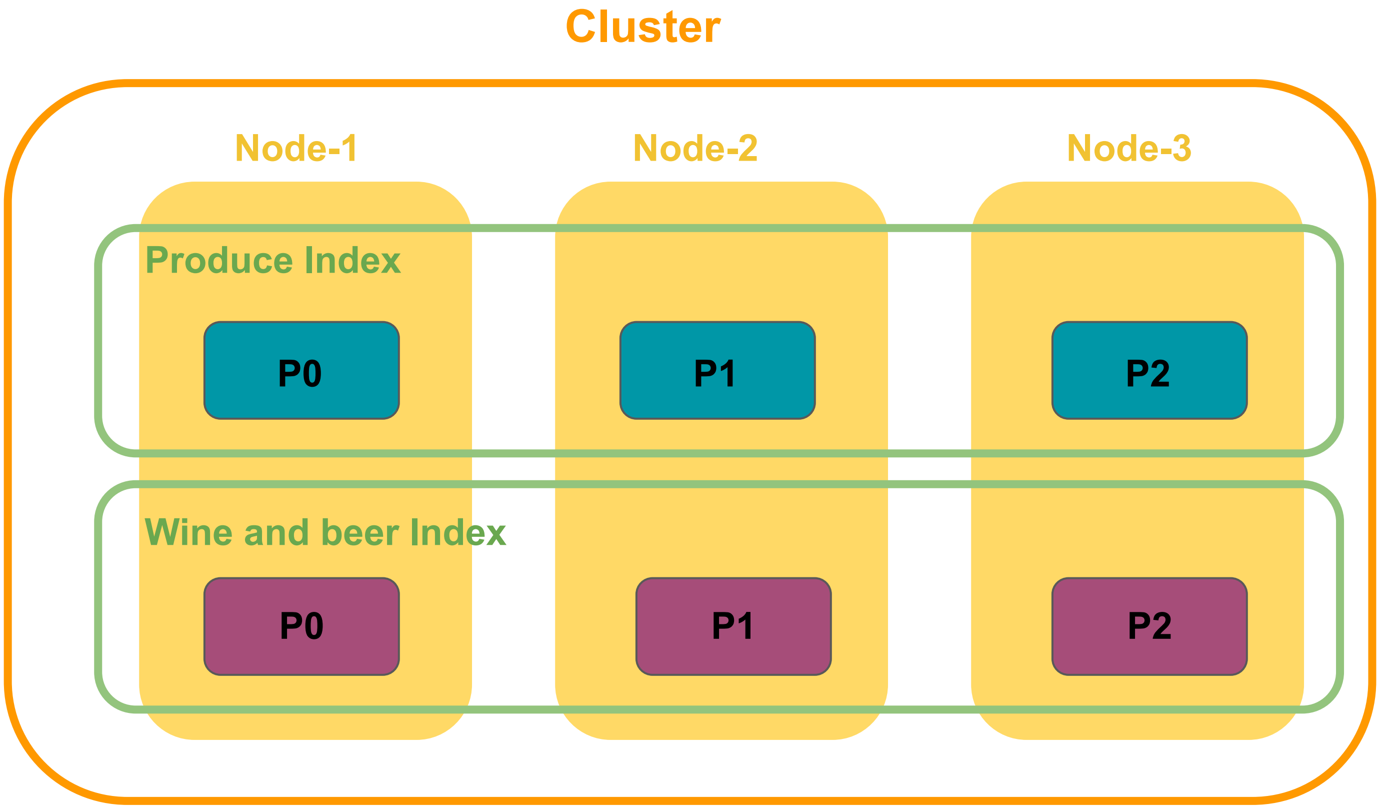
```
{
name: "Hazy Little Thing IPA(750ml)",
country: "US",
state: "California",
beer_type: "Ale",
beer_style: "India Pale Ale"
ABV: "6.7%",
price: "$14.99",
 }
```

What is a shard?

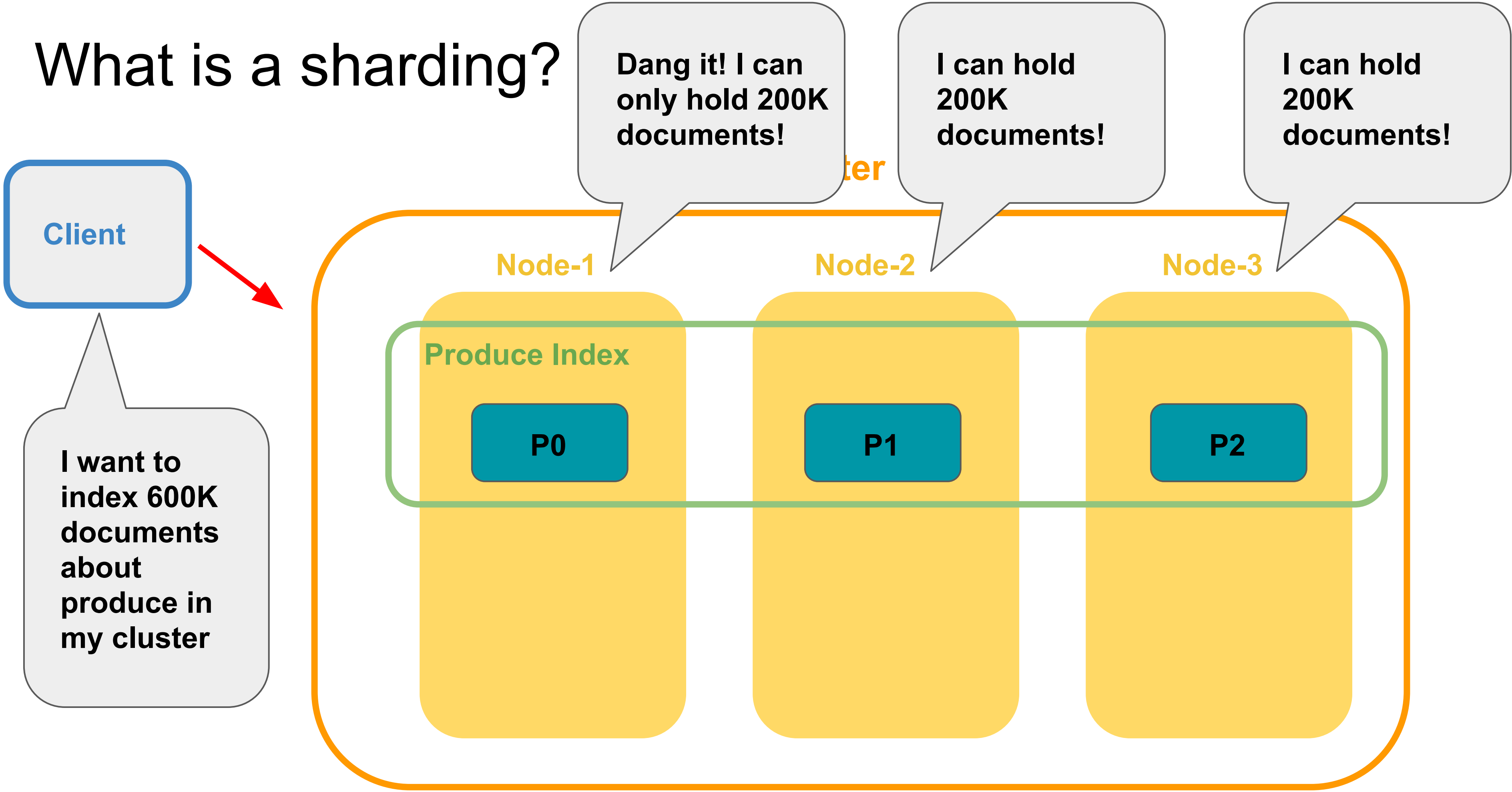


Cluster
Node-1
Node-2
Node-3
Produce Index
P0
Wine and beer Index
P0
Hi! I am a shard. I hold documents related to produce!
Hi! I am a shard too. I hold documents related to wine and beer!

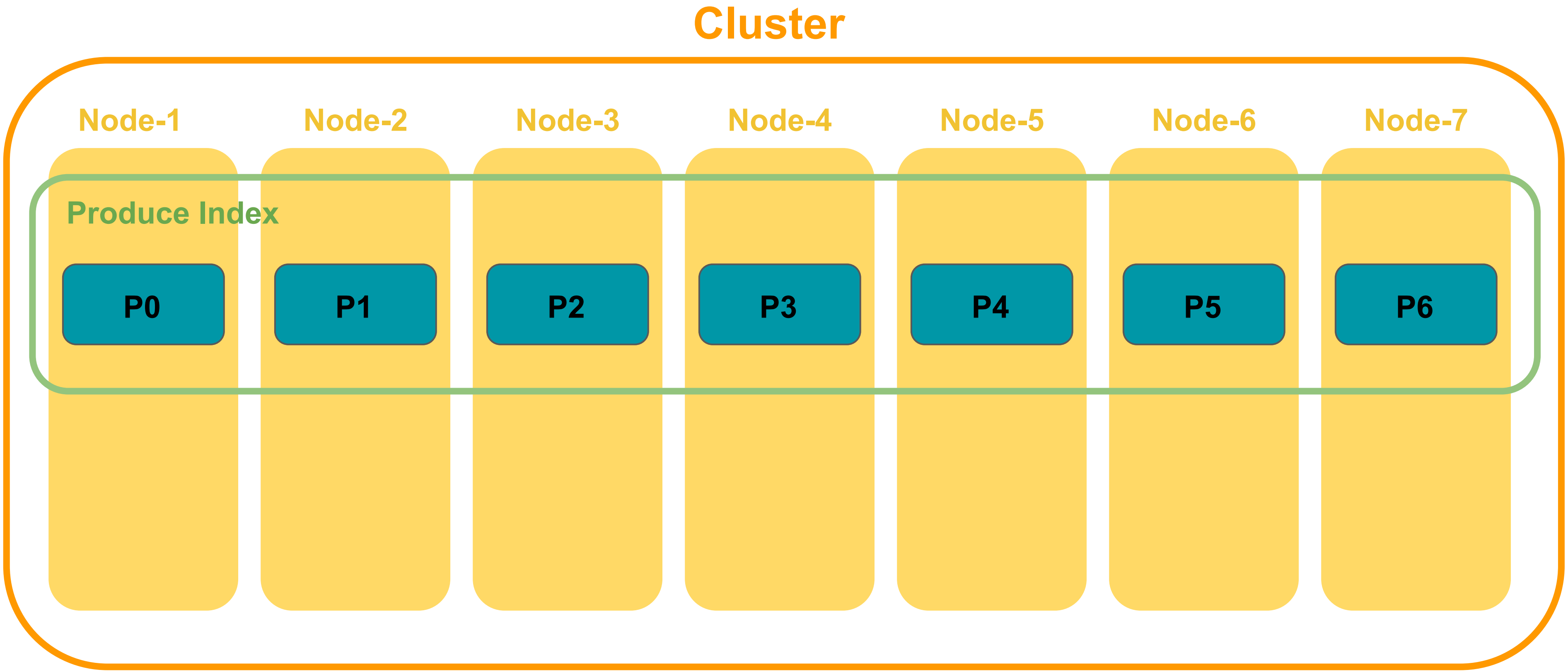
What is a sharding?



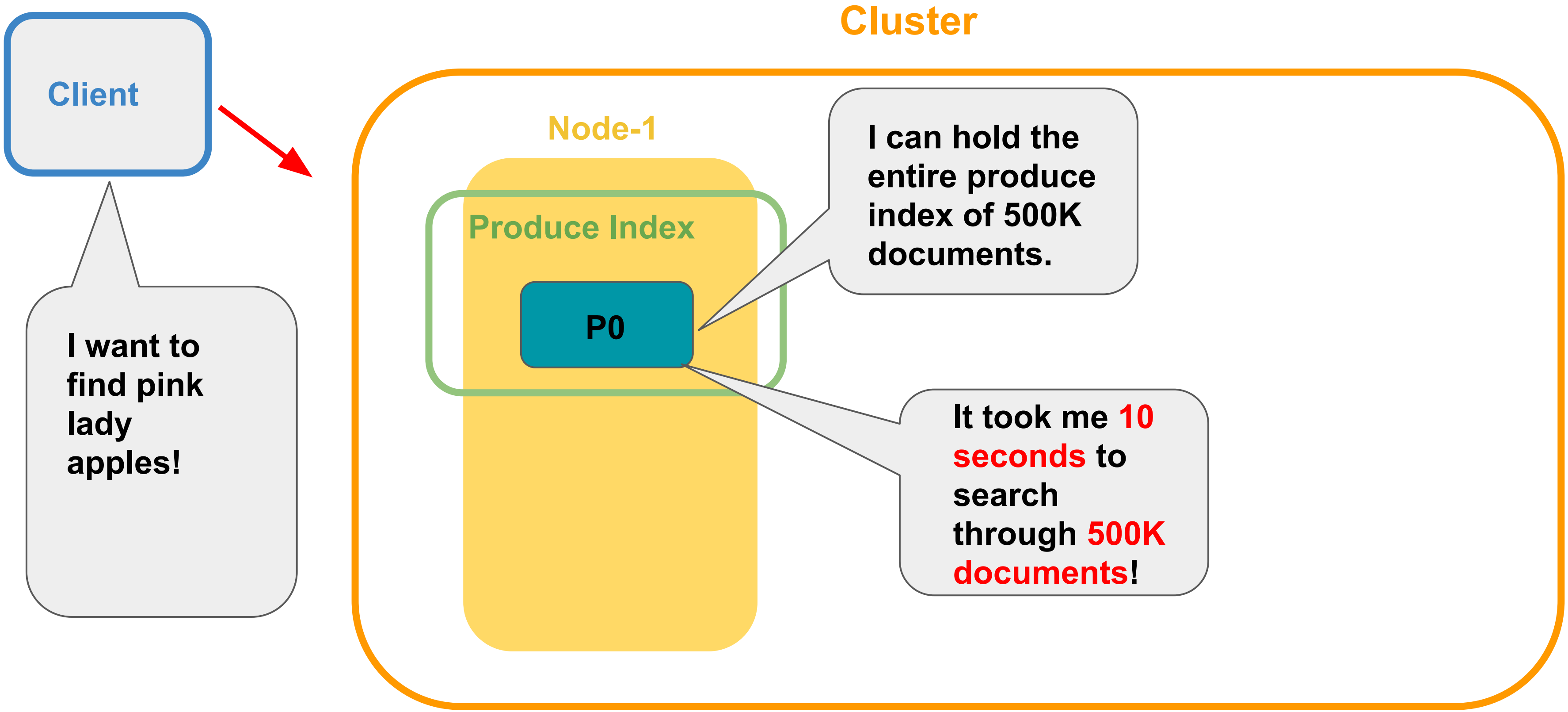
What is a sharding?


Dang it! I can only hold 200K documents!
I can hold 200K documents!
I can hold 200K documents!
ter
Client
Node-1
Node-2
Node-3
Produce Index
P0
P1
P2
I want to index 600K documents about produce in my cluster

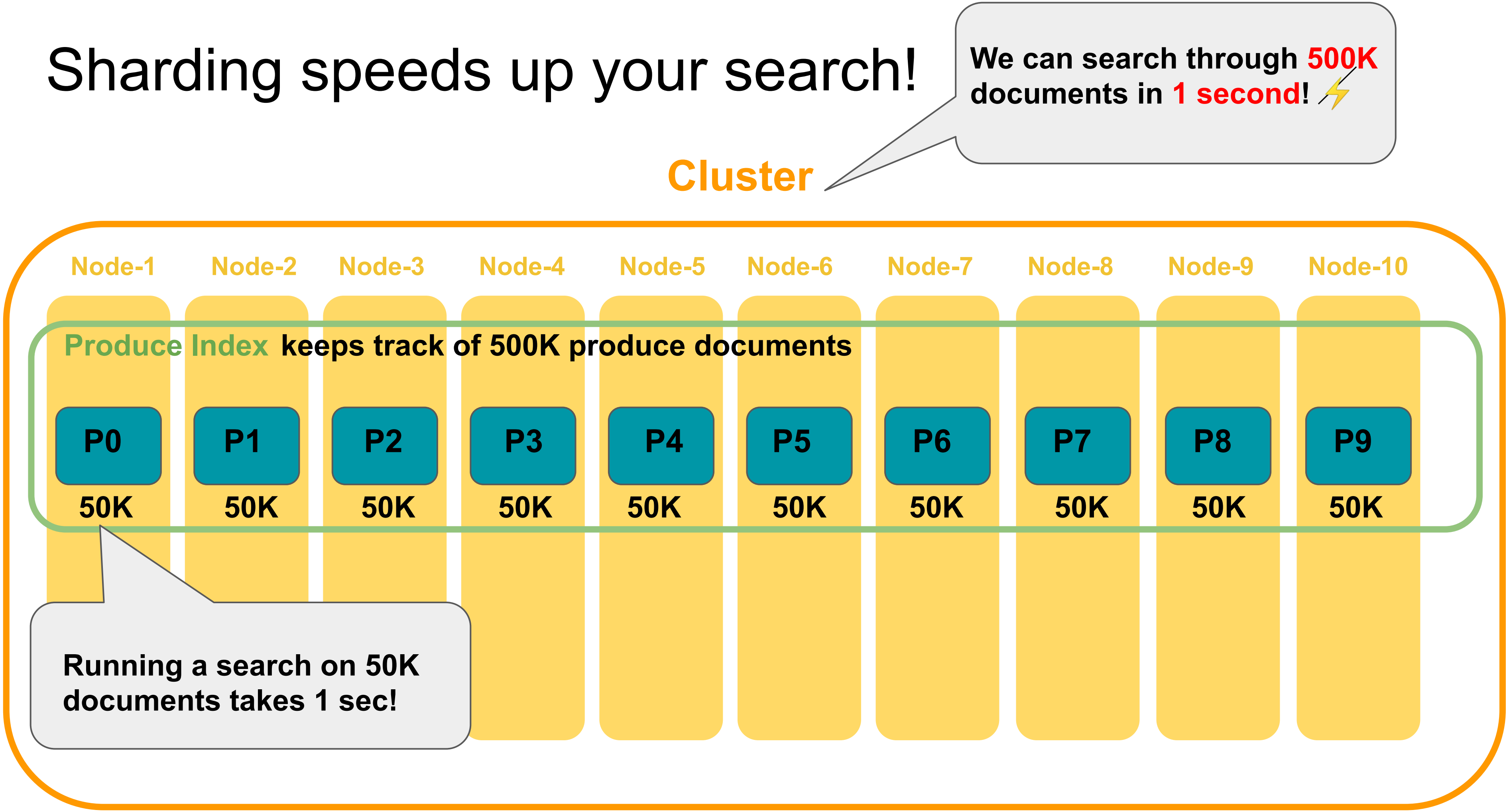
What is a sharding?



What is a sharding?


Client
I want to find pink lady apples!
Cluster
Node-1
Produce Index
P0
I can hold the entire produce index of 500K documents.
It took me 10 seconds to search through 500K documents!

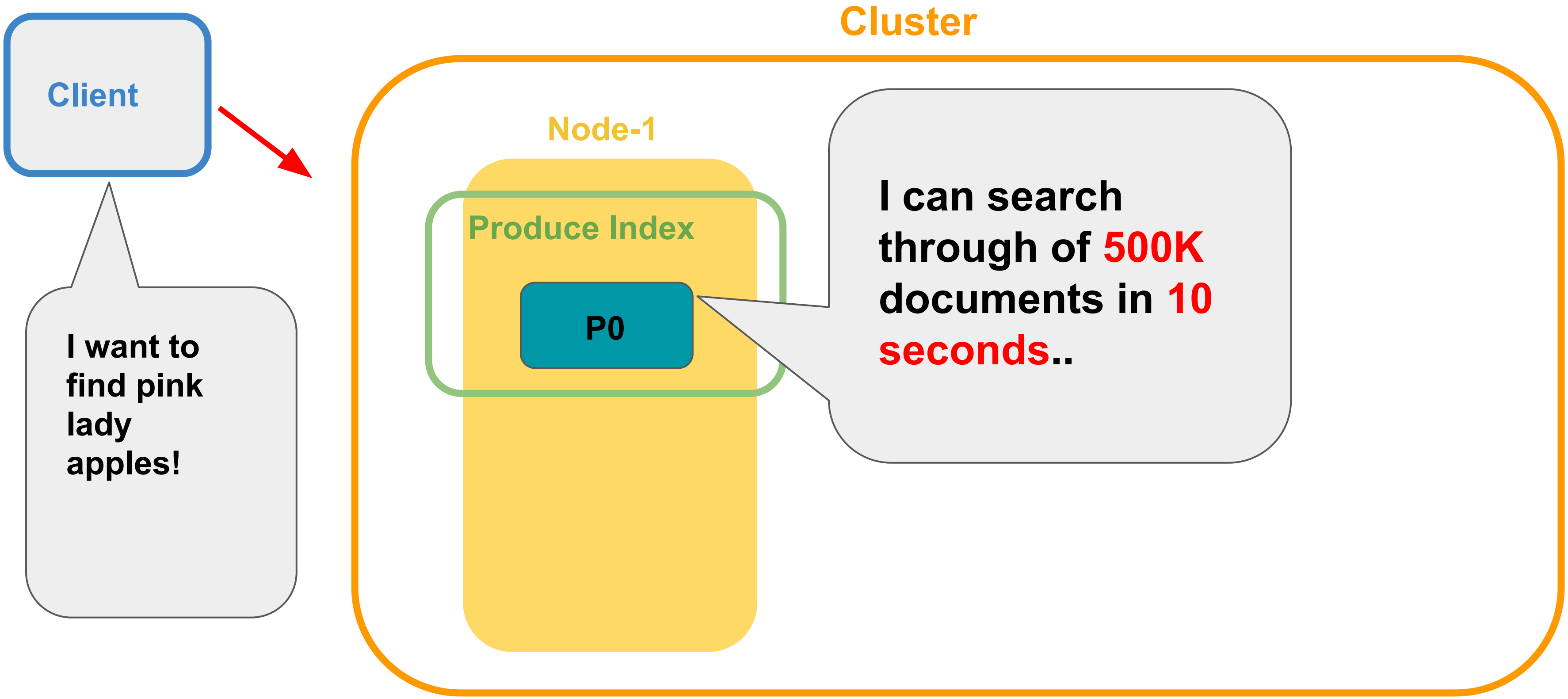
Sharding speeds up your search!



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

Running a search on 50K documents takes 1 sec!

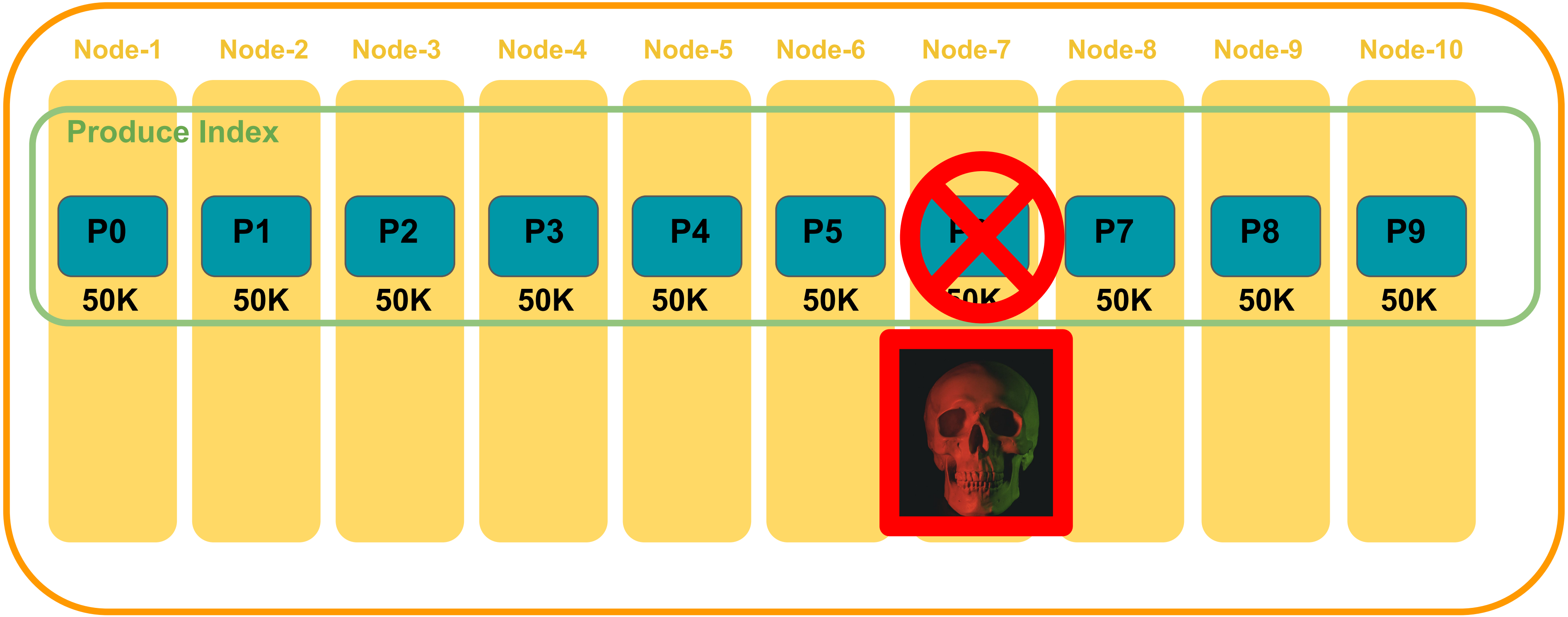
What is a sharding?


Client
I want to find pink lady apples!
Cluster
Node-1
Produce Index
P0
I can search through of 500K documents in 10 seconds..

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 50K

P1 50K

P2 50K

P3 50K

P4 50K

P5 50K

P 0K

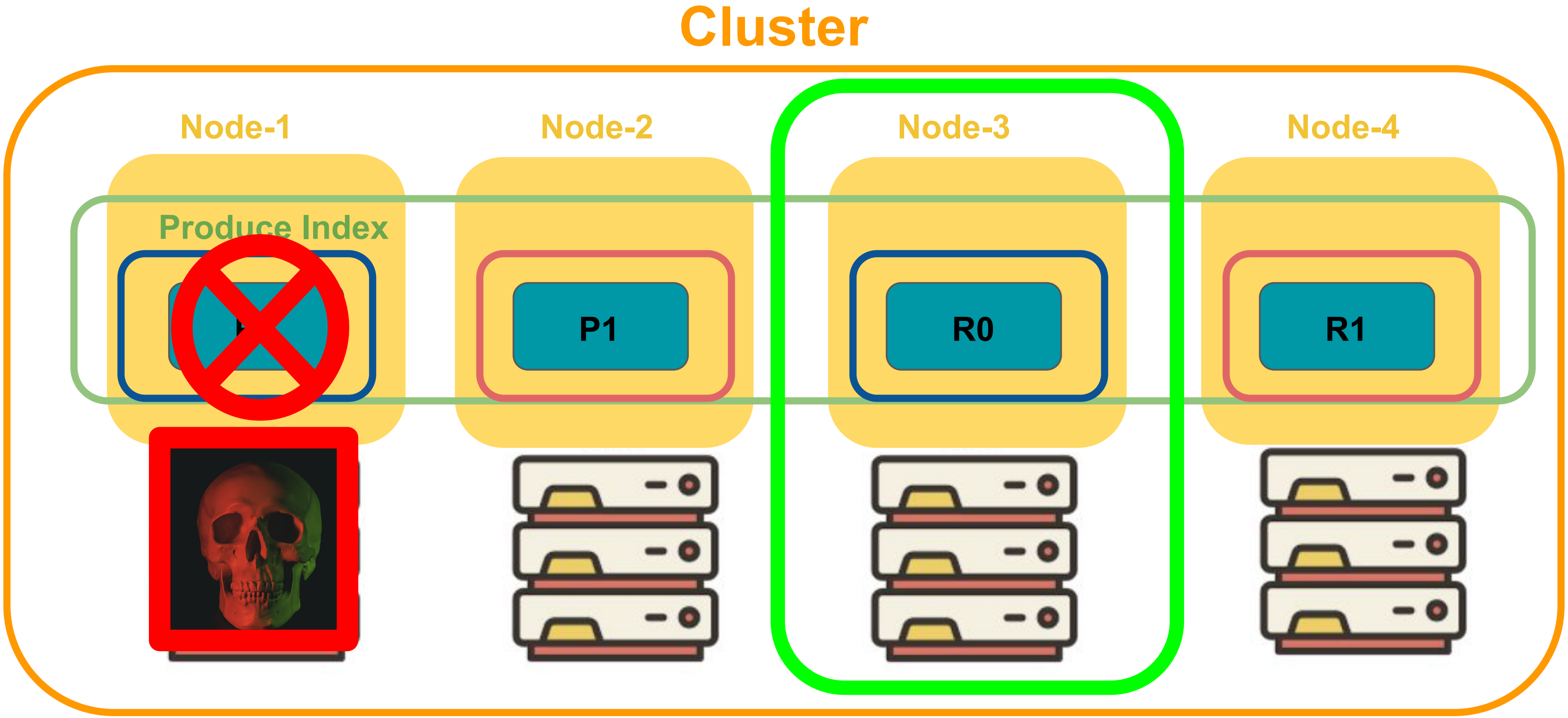
P7 50K

P8 50K

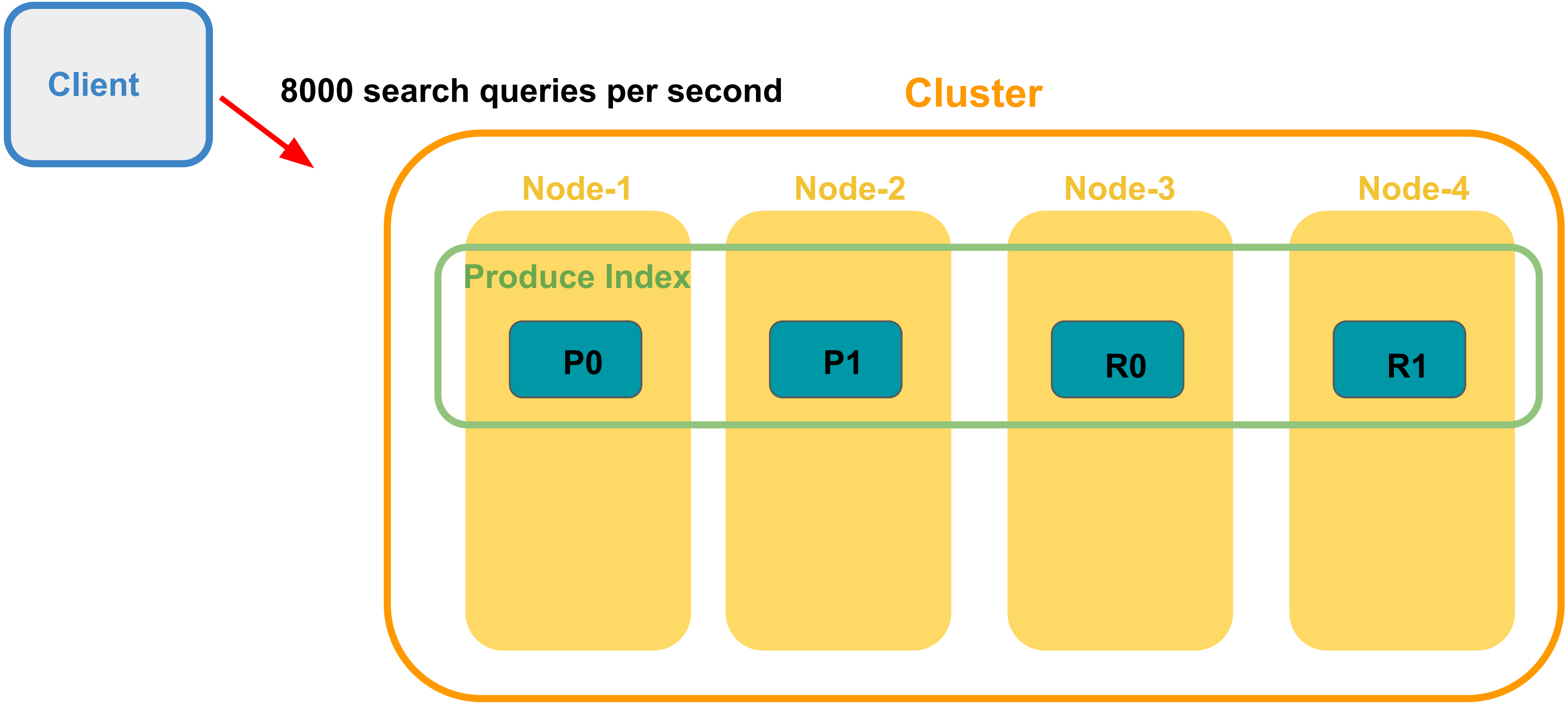
P9 50K

#SPONGEBOBMOVIE

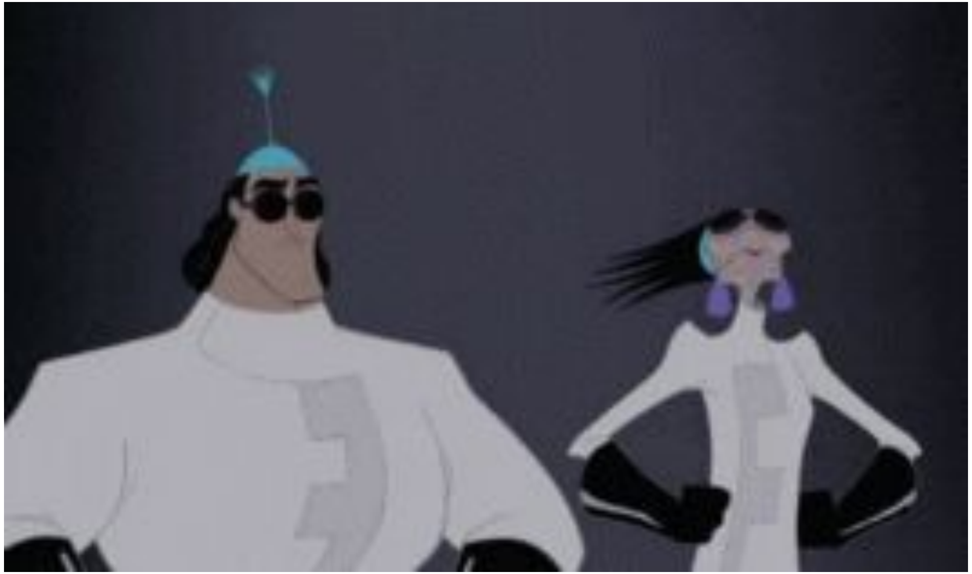
What are replica shards?



Replica shards can improve the performance of your search



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



Questions?

Lisa Jung

Developer Advocate @Elastic

E-mail: lisa.jung@elastic.co

Blog: https://dev.to/lisahjung

Twitter: @LisaHJung

SCAN ME