



Beginner's Crash Course to Elastic Stack Series

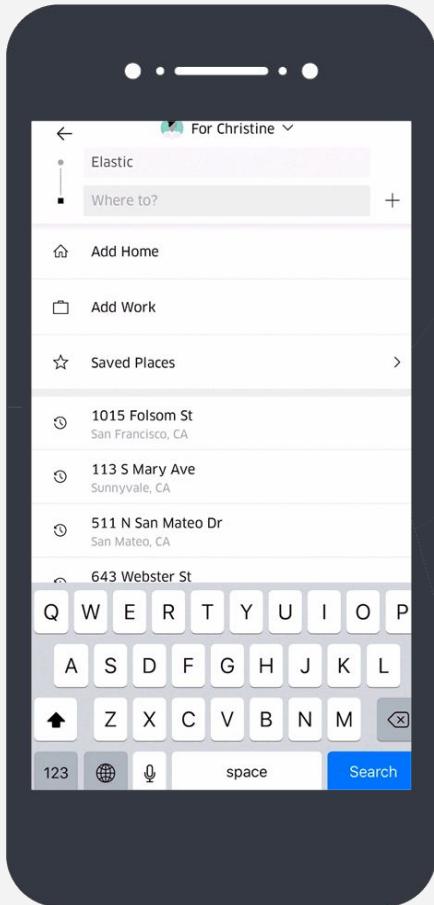
Part 1: Intro to Elasticsearch and Kibana

Lisa Jung
Developer Advocate @Elastic

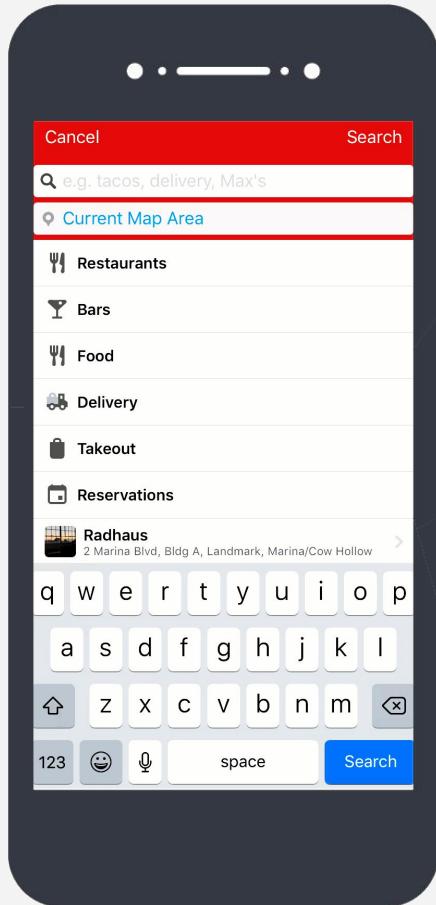


Have you ever used the Elastic Stack before?

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



Searching for Rides



Searching for Restaurants

Uber

tinder

 twilio

 GitHub





 Adobe

 instacart

GRUBHUB

 shopify

Searching for
Rides

The Elastic Stack

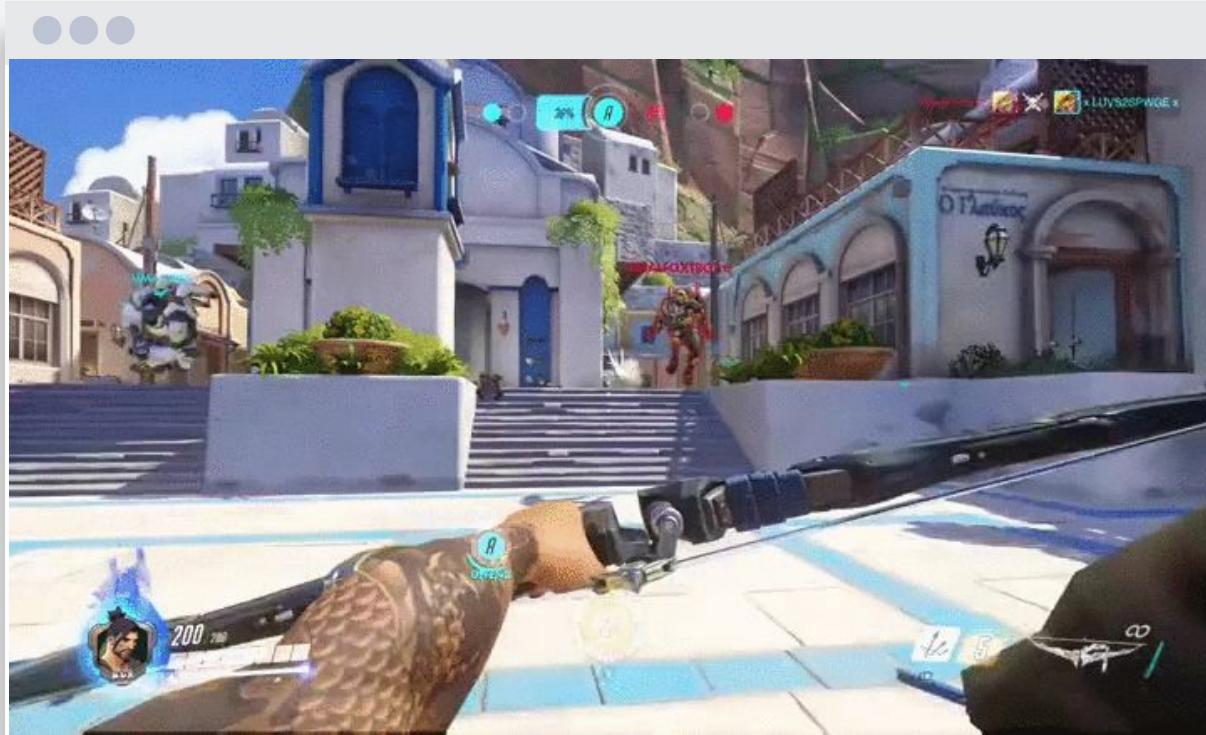
Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

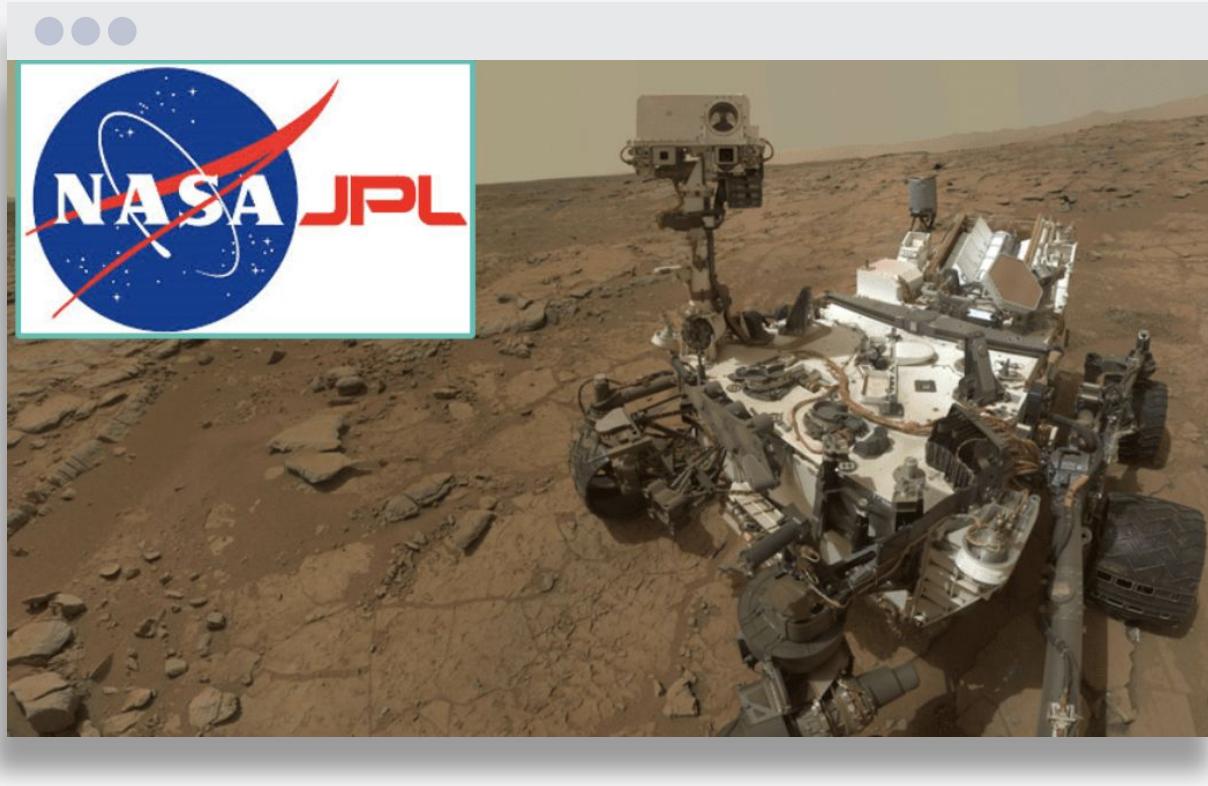
Use Case: Logging



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

ACTIVISION
BLIZZARD

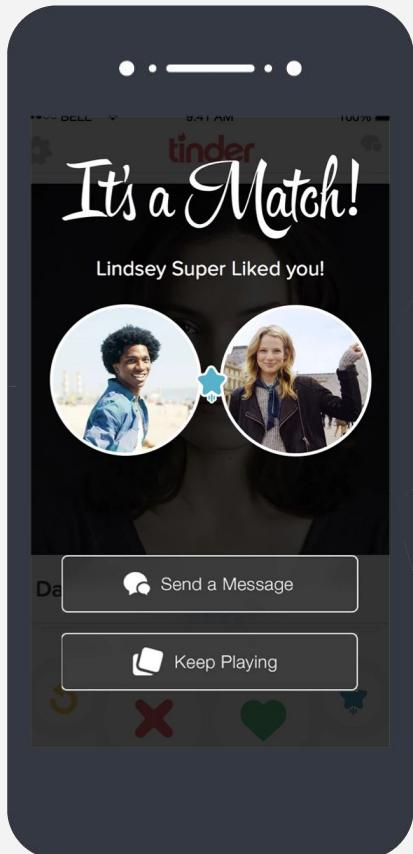
Use Case: Metrics



Use Case: Security Analytics



Use Case: Business Analytics



The Elastic Stack

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





Elastic Bootcamp for Students

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, Delete) operations with Elasticsearch and Kibana

Elasticsearch

Store | Search | Analyze



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



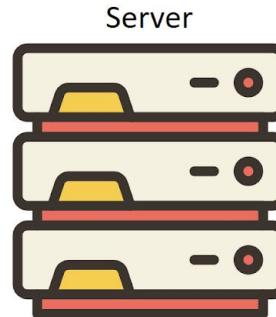
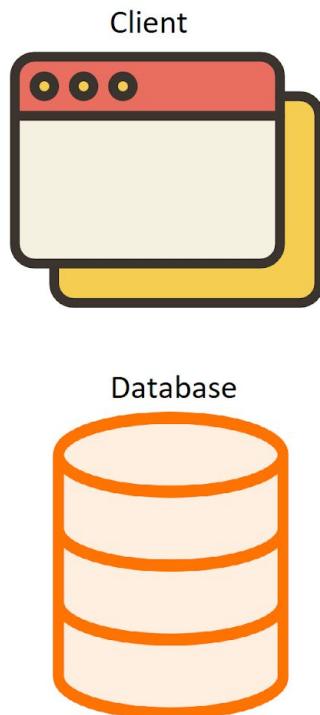
A screenshot of the Instacart mobile website. At the top, the Instacart logo and navigation links like "Stores" and "Account" are visible. A green header bar shows "Delivery in 94086". On the right, there are three colored dots (green, yellow, red) and a "Cart" button with a "4" notification. The main content area features a background image of fresh produce like avocados and kale. A white search bar has "can" typed into it, and a dropdown menu lists search results: "Canned Goods Department", "Canned Goods > Canned Fruit & Applesauce Aisle", "Canned Goods > Canned & Jarred Vegetables Aisle", and "Canned Goods > Canned Meals & Beans Aisle". Below the search bar, a "Coupon saving" section offers up to 40% off everyday items, with buttons for "Shop Coupons" and "Save Now". To the right, there are promotional banners for "Free Delivery" with select Tailgate items and "Save Now" buttons for Kraft products. At the bottom, a message says "Based on your cart" with a "View more" link.

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 Srircalah? Srirracha?



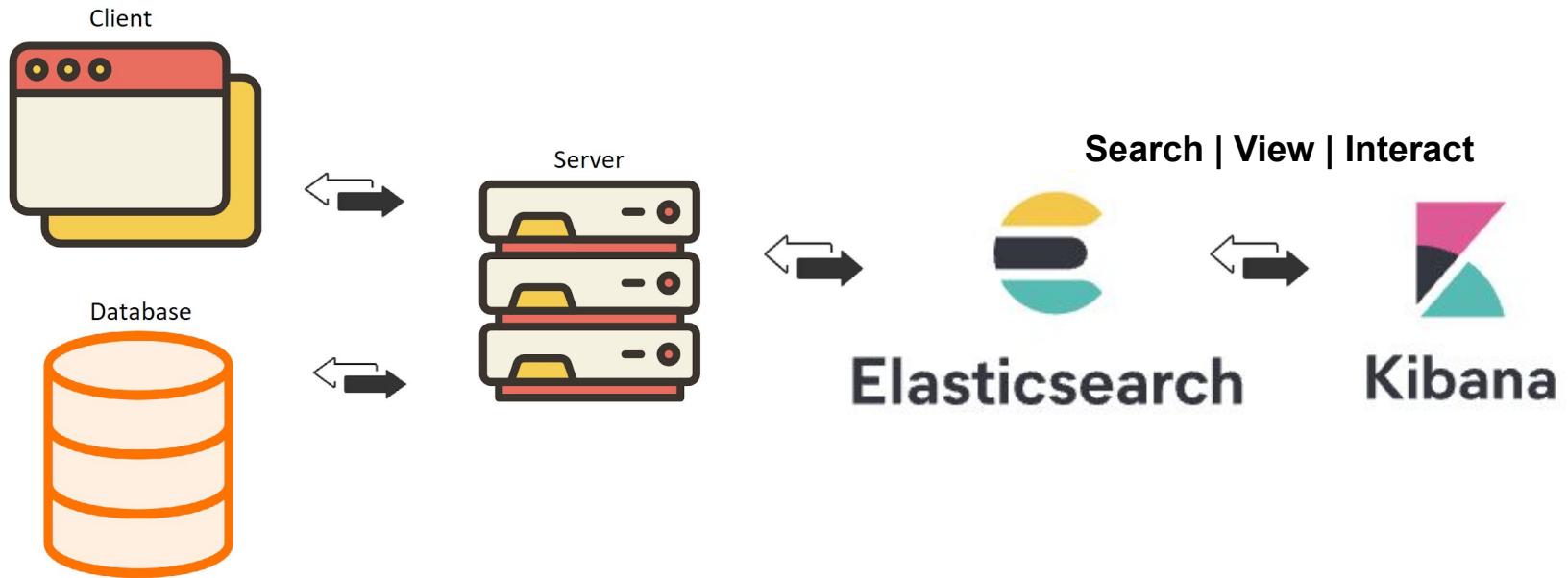


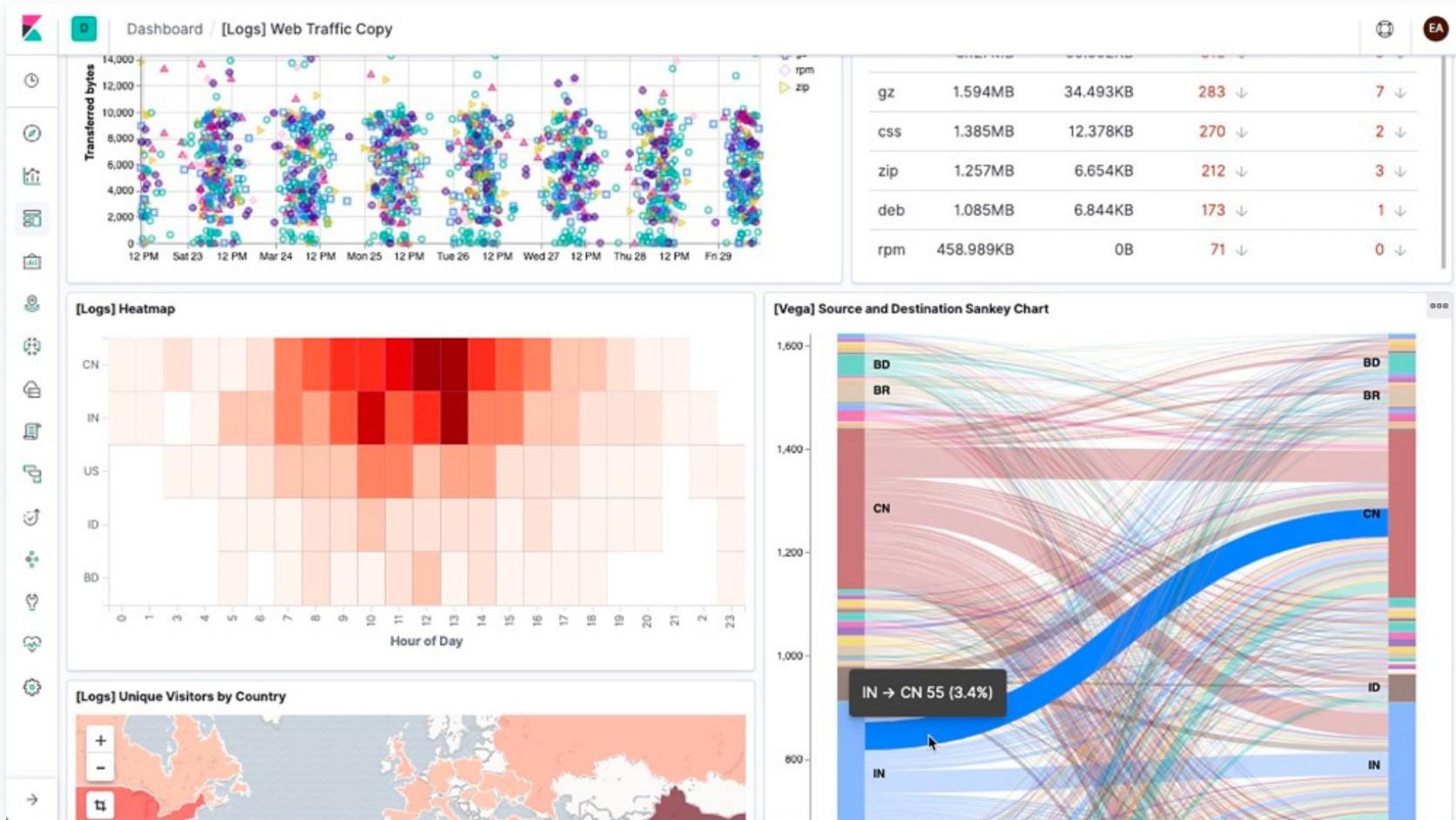
Elasticsearch

Elasticsearch

Store | Search | Analyze







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

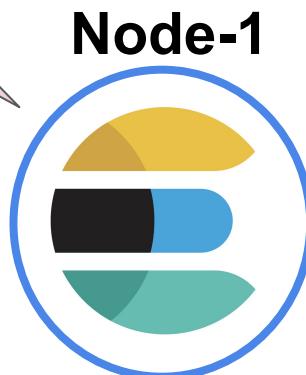
Elasticsearch

Store | Search | Analyze



Cluster

I belong to a single cluster!



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

I have a unique id and a name!

Cluster

Node-1



Node-2



Node-3



Node-4





@LisaHJung | Beginner's Crash Course to Elastic Stack

Cluster

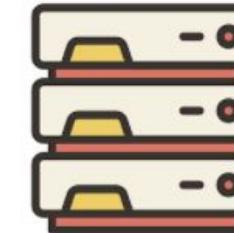
Node-1



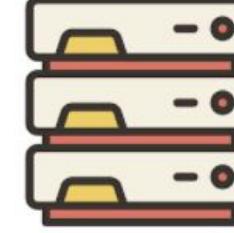
Node-2



Node-3



Node-4



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!

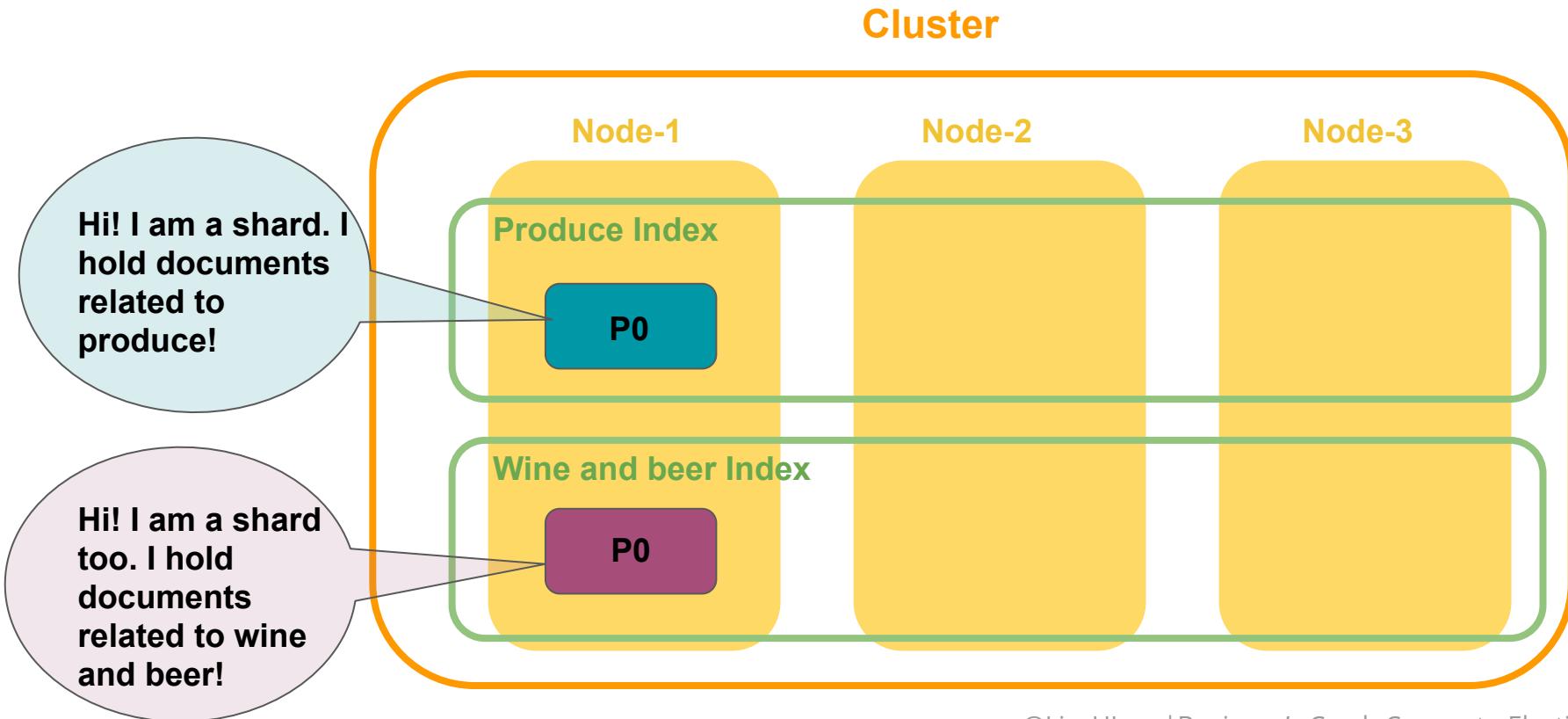
Produce Index

```
{  
  "name": "Baby Carrots(1lb bag)",  
  "category": "Vegetables",  
  "brand": "365",  
  "price": "$0.99"  
}  
  
{  
  "name": "Clementines(3lb bag)",  
  "category": "Fruits",  
  "brand": "Cuties",  
  "price": "$4.29"  
}
```

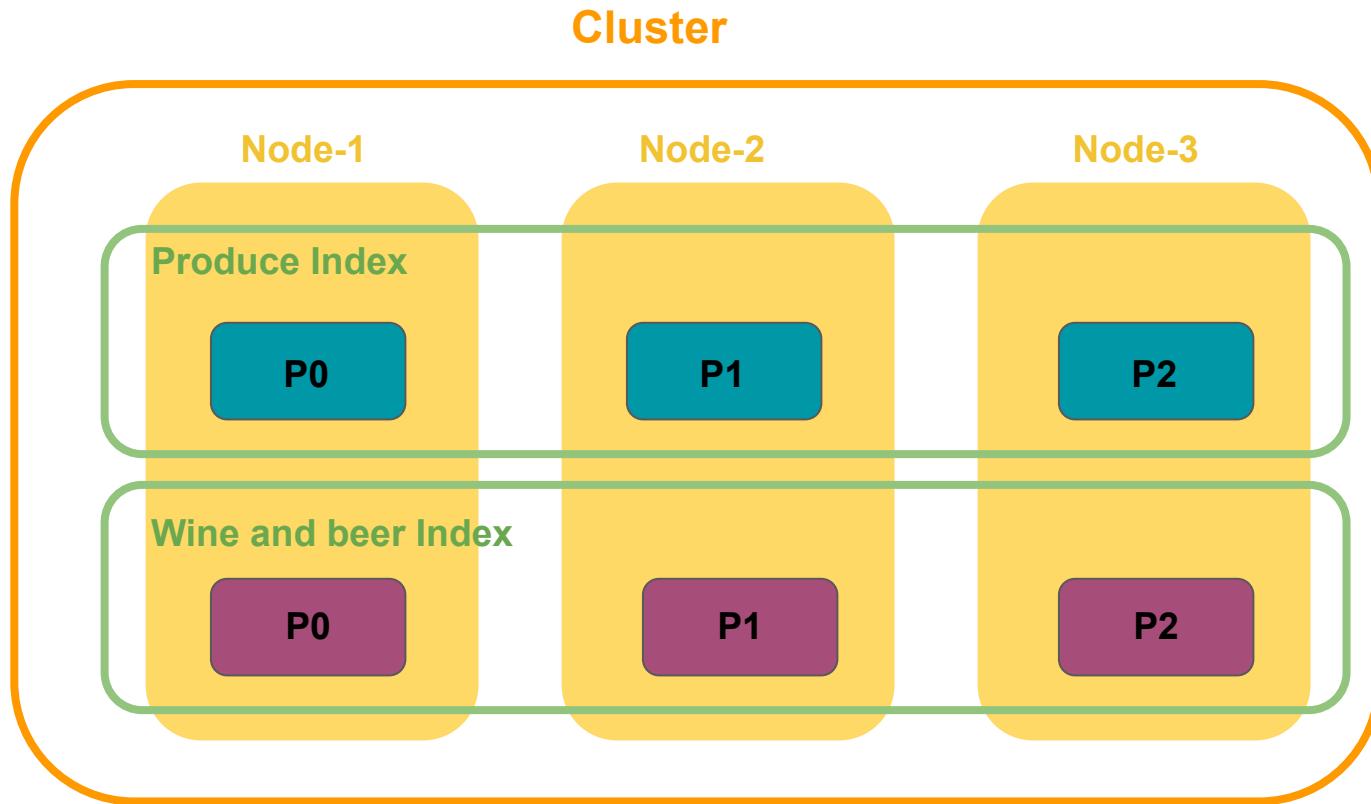
Wine & Beer Index

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

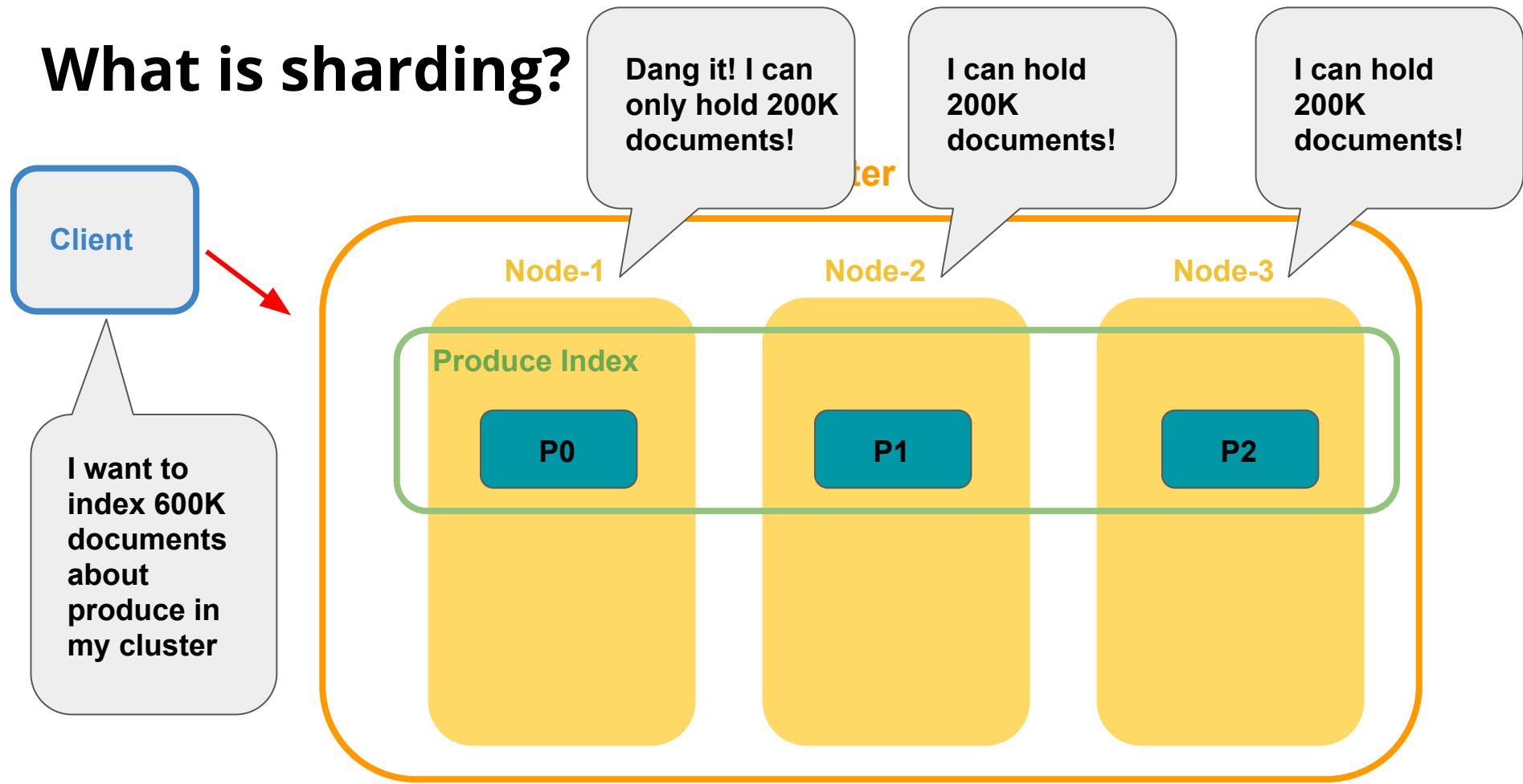
What is a shard?



What is sharding?



What is sharding?



What is sharding?

Cluster

Node-1

Node-2

Node-3

Node-4

Node-5

Node-6

Node-7

Produce Index

P0

P1

P2

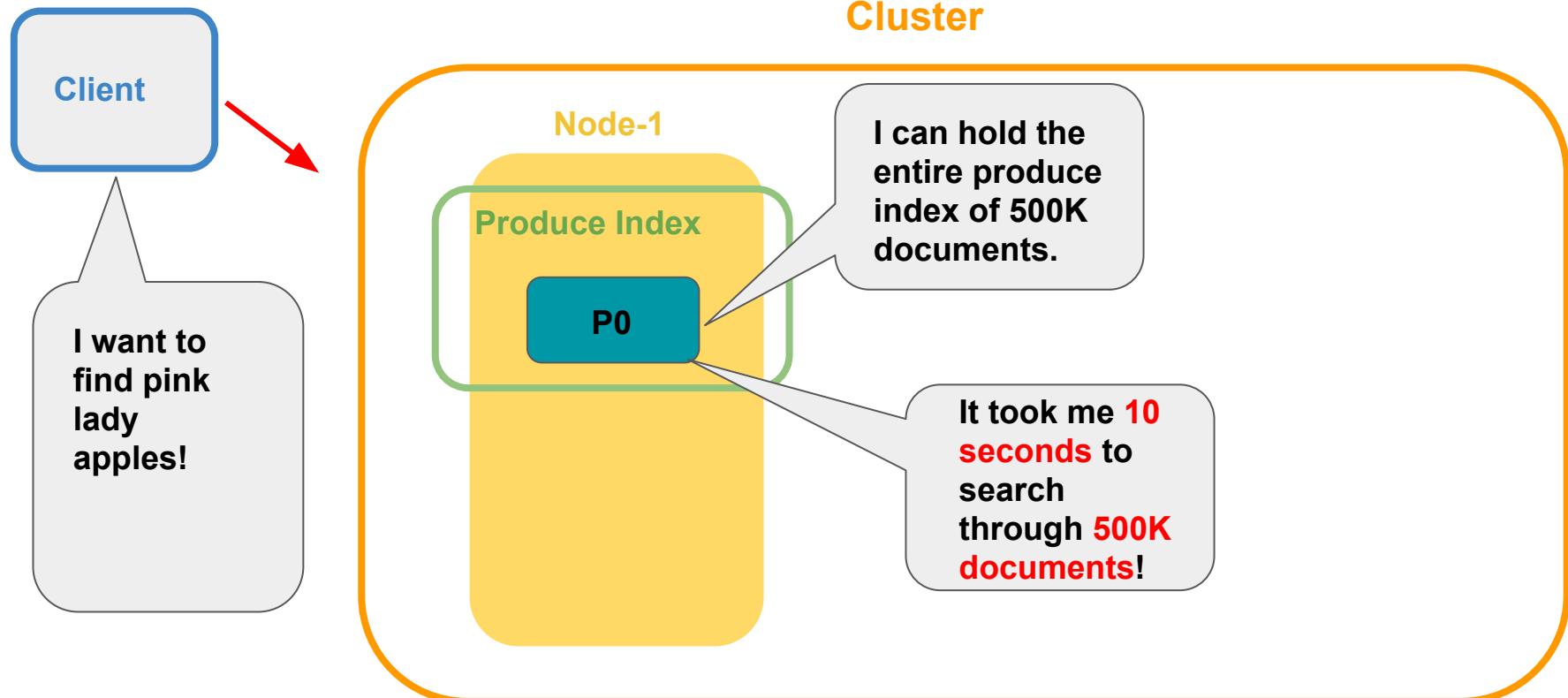
P3

P4

P5

P6

What is sharding?



I want to find pink lady apples!

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 keeps track of 500K produce documents

P0

50K

P1

50K

P2

50K

P3

50K

P4

50K

P5

50K

P6

50K

P7

50K

P8

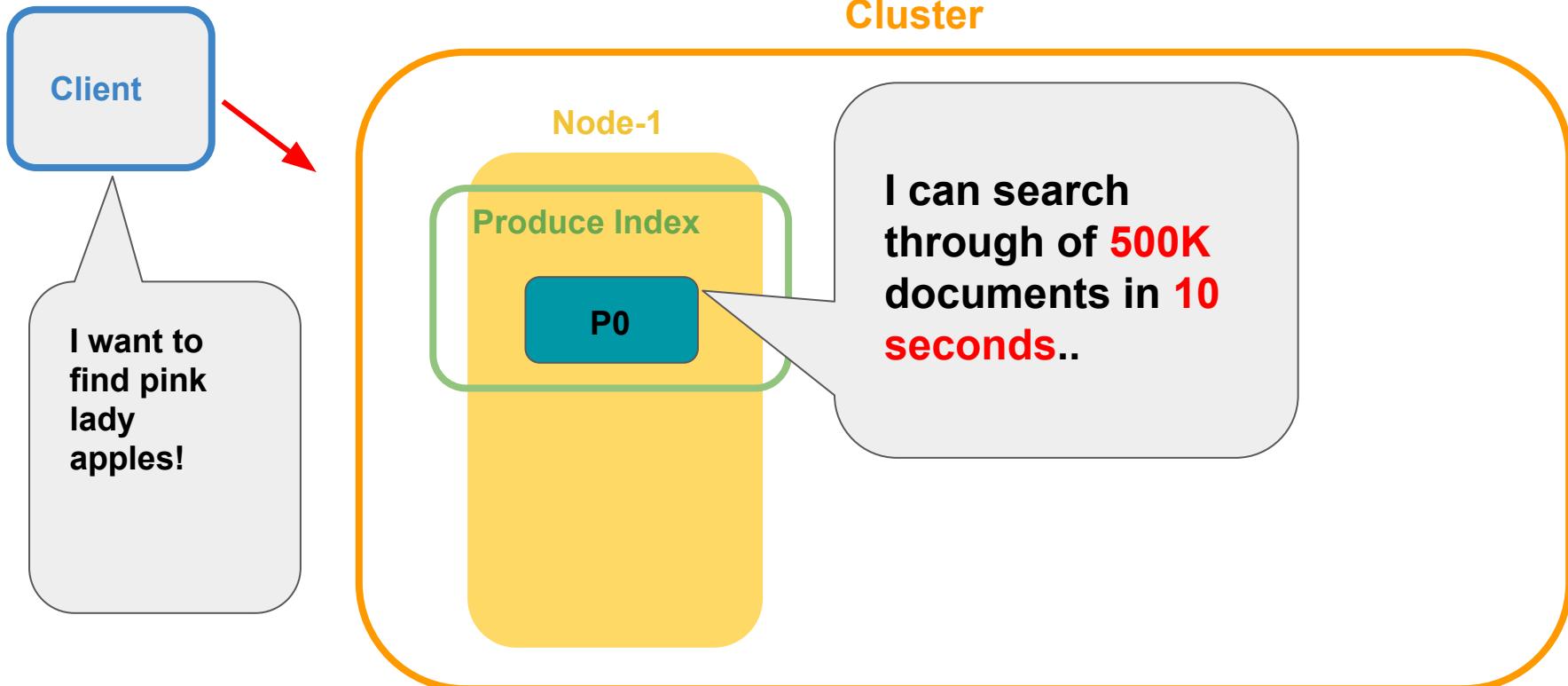
50K

P9

50K

Running a search on 50K documents takes 1 sec!

What is sharding?



I want to find pink lady apples!

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

P6

50K

P7

50K

P8

50K

P9

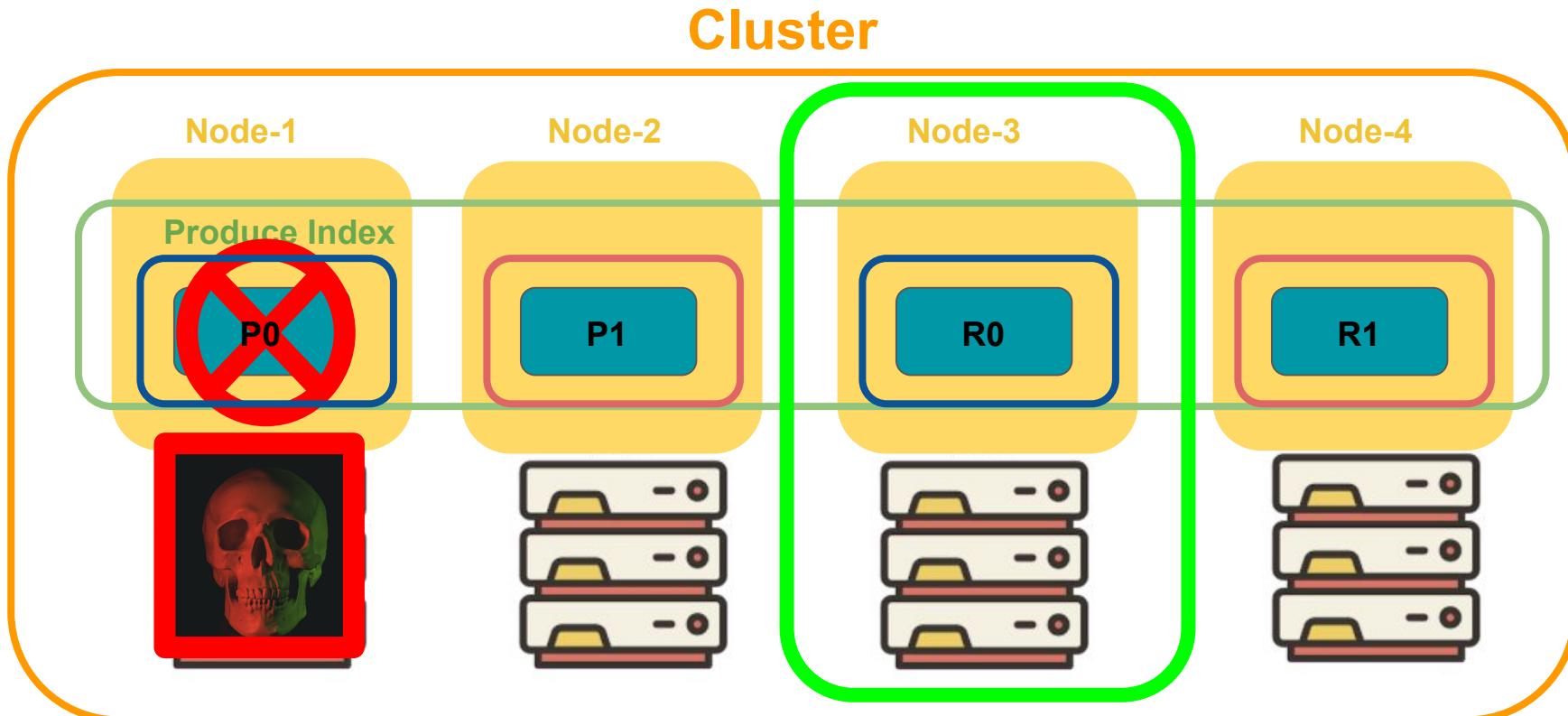
50K



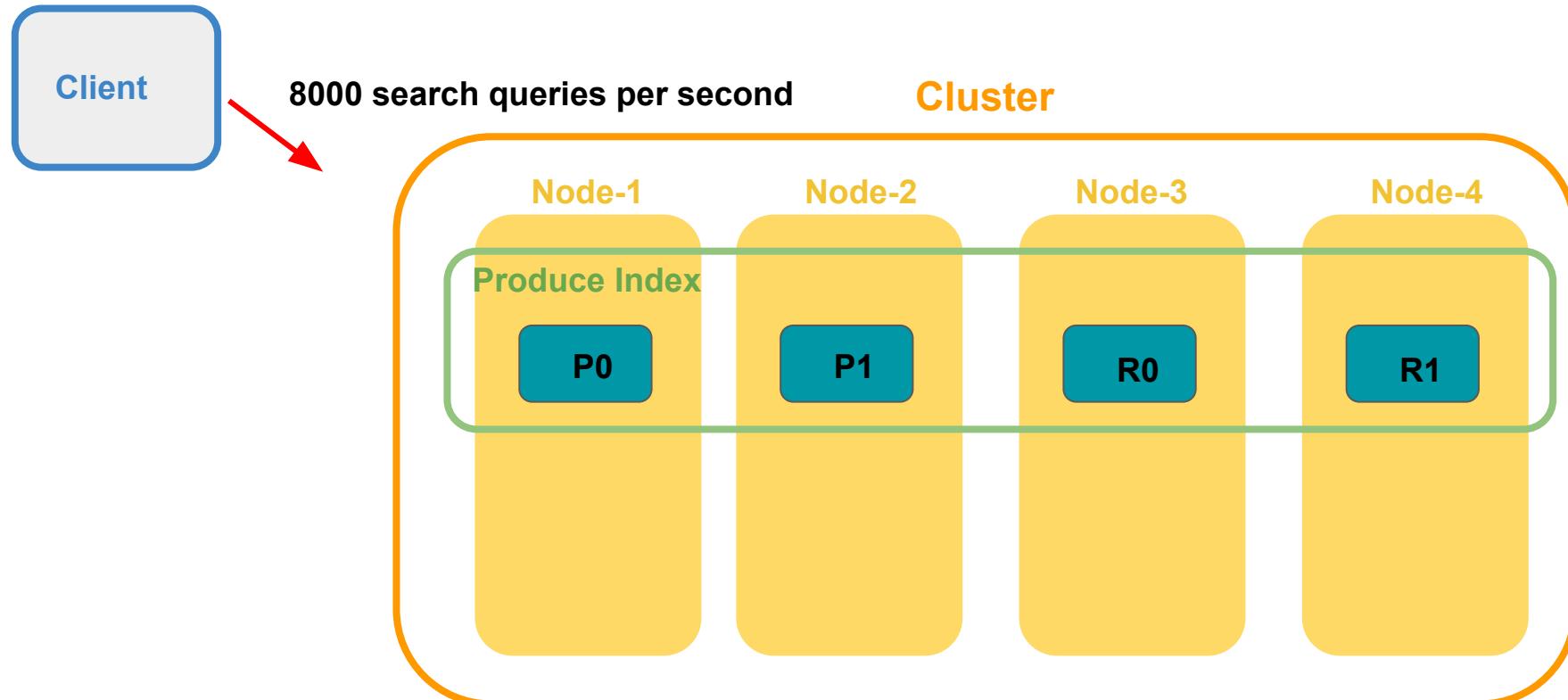
#SPONGEBOBMOVIE



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

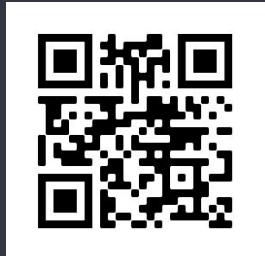
Discussion forum: <https://discuss.elastic.co/>

Blog: <https://dev.to/lisahjung>

Twitter: @LisaHJung

Connect with the Elastic Community

 **Elastic
meetups**



[https://ela.st/
amervirtual](https://ela.st/amervirtual)



**Elastic Community
Slack Workspace**



<https://ela.st/slack>



**YouTube
Channel**



[https://ela.st/
community-
youtube](https://ela.st/community-youtube)

Elastic Contributor Program



Join the [Elastic Contributor Program](#), which recognizes the hard work of our awesome contributors!

Start contributing code, presentations, tutorials, and more today to earn yourself a spot on the leaderboard and the chance to win free training, Elastic swag, bragging rights, and more.



elastic.co/community/contributor

Raymond asked:

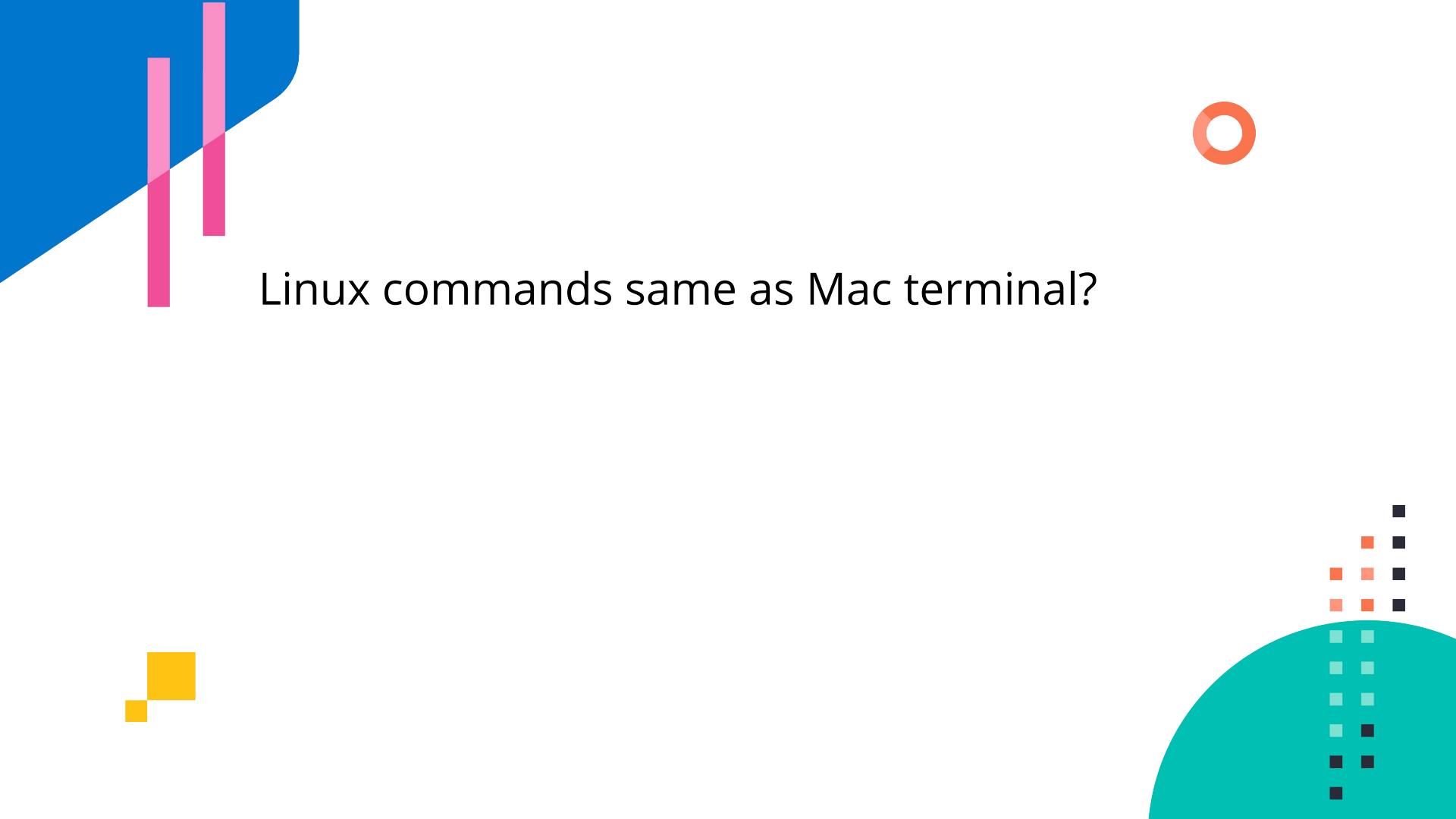
For people who come from a RDBMS background like SQL Server, how does this Elastic database compare to it?

Raymond asked:

Is Node like tables and Clusters like servers
in SQL Server?

Igor asked:

Do the nodes use cache to find the data that is being searched?



Linux commands same as Mac terminal?

Linford asked:

What is the best way to perform sharding
with one node?

Raymond asked:

What are some disadvantages with using Elastic?

Partha asked:

At which point does using Elasticsearch give value vs searching through a SQL db (empirically in size of db). Note that there is overhead in maintaining yet another microservice.

Christopher asked:

Do you have experience and /or can you recommend using REDIS with an established ELK Stack???

<https://discuss.elastic.co/>

Raymond asked:

What's with the errors and warnings?

```
[license.  
log [22:07:18.575] [info][plugins][watcher] Your basic license does not support watcher. Please upgrade your license.  
log [22:07:18.577] [info][kibana-monitoring][monitoring][monitoring][plugins] Starting monitoring stats collection  
log [22:07:18.971] [error][data][elasticsearch] [version_conflict_engine_exception]: [task:Actions-actions_telemetry]  
document already exists (current version [22])  
log [22:07:18.973] [error][data][elasticsearch] [version_conflict_engine_exception]: [task:Lens-lens_telemetry]: vers  
already exists (current version [22])  
log [22:07:18.981] [error][data][elasticsearch] [version_conflict_engine_exception]: [task:Alerting-alerting_telemet  
document already exists (current version [22])  
log [22:07:18.983] [error][data][elasticsearch] [version_conflict_engine_exception]: [task:endpoint:user-artifact-pa  
conflict, document already exists (current version [14155])  
log [22:07:19.021] [error][data][elasticsearch] [version_conflict_engine_exception]: [task:apm-telemetry-task]: vers  
already exists (current version [34])  
log [22:07:19.190] [info][listening] Server running at http://localhost:5601  
log [22:07:20.137] [info][server][Kibana][http] http server running at http://localhost:5601
```

Partha asked:

Does Elasticsearch have support to secure :9200 and :5601? Authentication/ tokens etc

1. <https://www.elastic.co/guide/en/elasticsearch/reference/7.10/secure-cluster.html>
2. <https://www.elastic.co/guide/en/elasticsearch/reference/7.10/encrypting-communications.html>
3. <https://www.elastic.co/guide/en/elasticsearch/reference/7.10/setting-up-authentication.html>