



# Introduction to Elasticsearch and Kibana

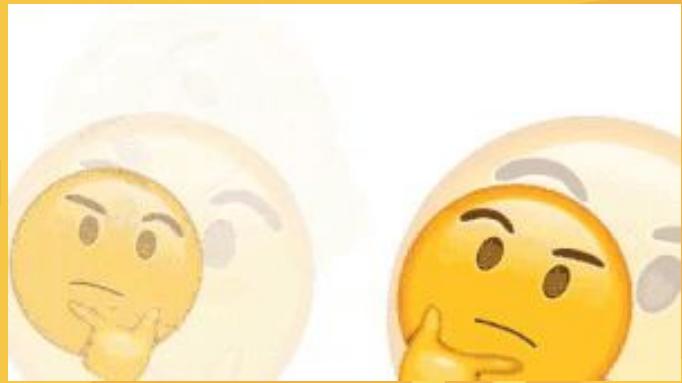
Lisa Jung  
Developer Advocate @ Elastic

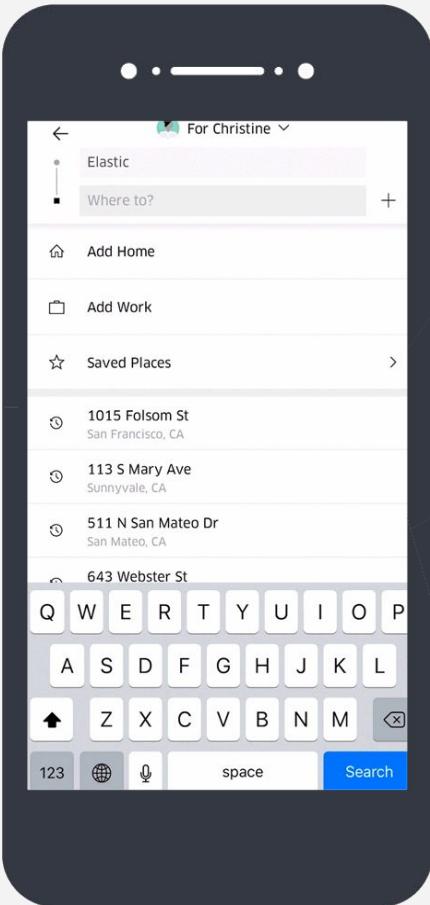


# Have you ever used the Elastic Stack before?

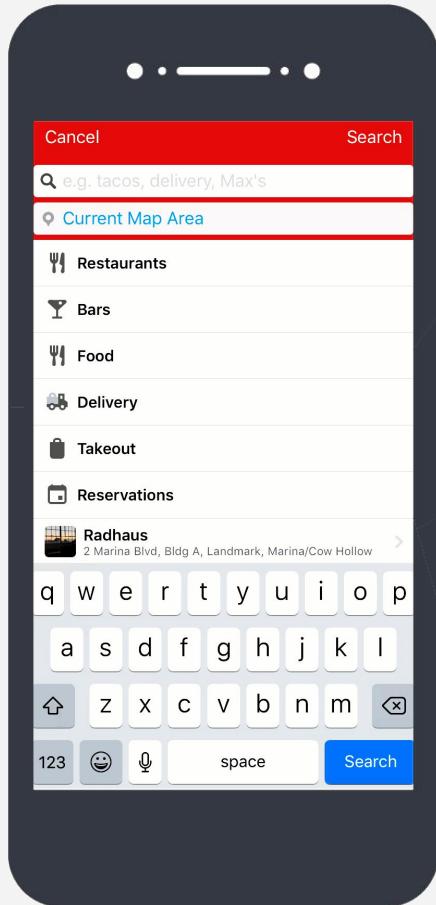
Type **yes** in the chat if you have used it

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





# Searching for Rides



# Searching for Restaurants

Uber

tinder

 twilio

 GitHub





 Adobe

 instacart

GRUBHUB

 shopify

Searching for  
Rides

# The Elastic Stack

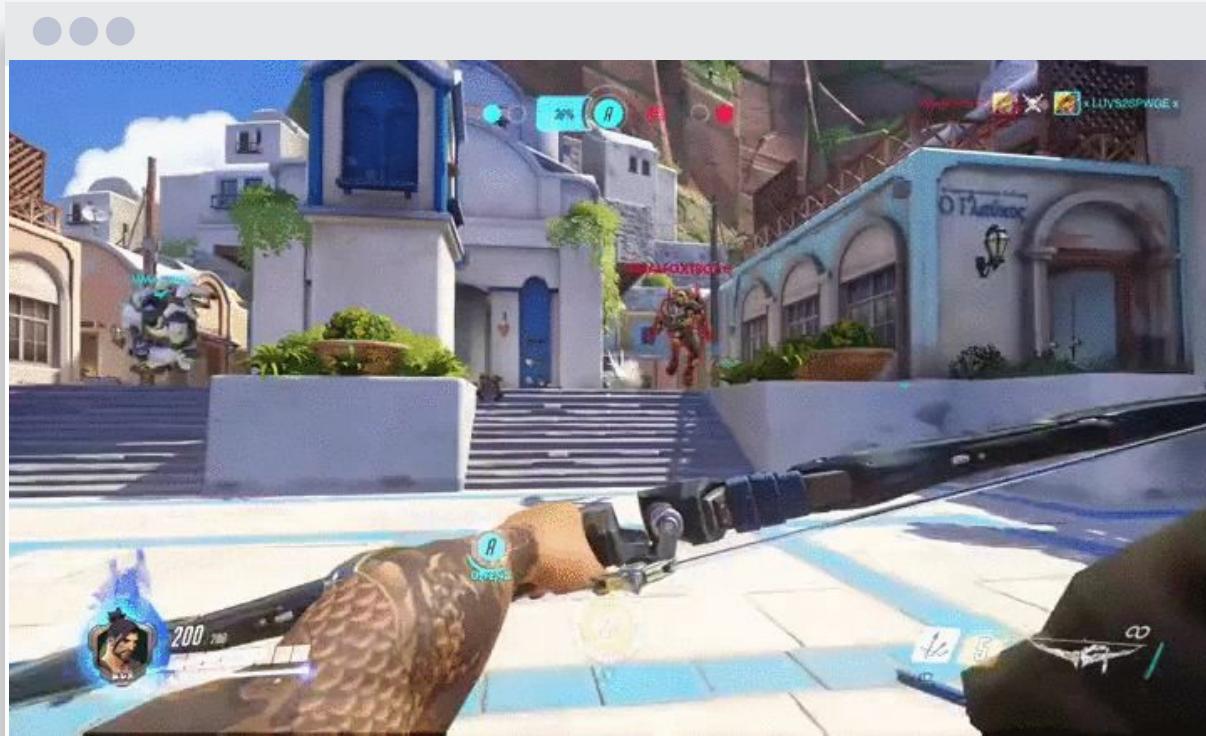
Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



# Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

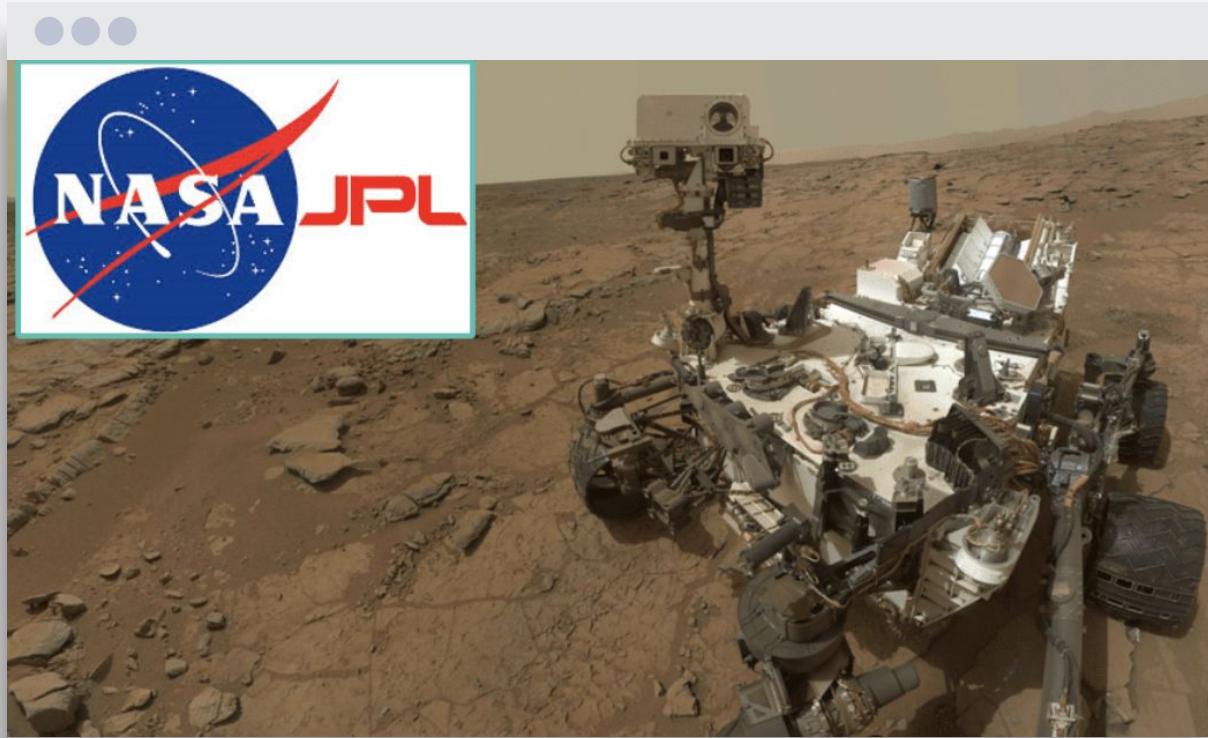
# Use Case: Logging



[https://www.reddit.com/r/gaming/comments/4lhm69/overwatch\\_blocked\\_pharahs\\_rocket\\_with\\_hanzos\\_arrow/](https://www.reddit.com/r/gaming/comments/4lhm69/overwatch_blocked_pharahs_rocket_with_hanzos_arrow/)

ACTIVISION  
BLIZZARD

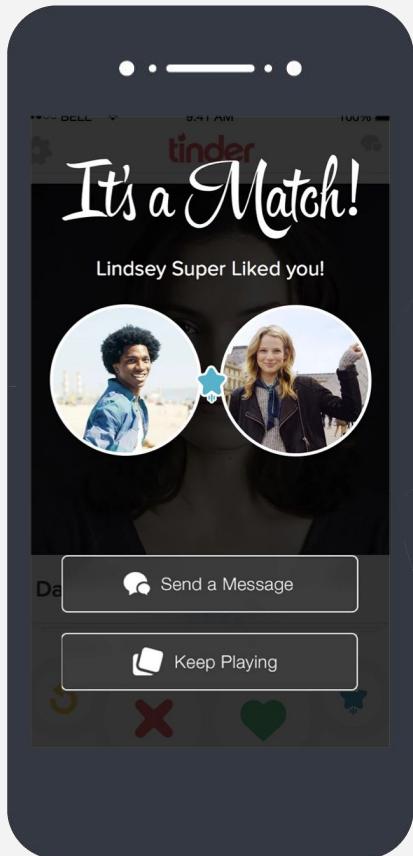
# Use Case: Metrics



# 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.





# Introduction to Elasticsearch and Kibana

Lisa Jung  
Developer Advocate @ Elastic



# **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 a "Stores" button are visible. To the right are links for "Delivery in 94086", "Account", "Help", and a green "Cart" button with a red notification badge showing the number 4. The background features a collage of fresh produce like avocados and kale. A large white search bar contains the text "can". Below it, a dropdown menu lists search results:

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

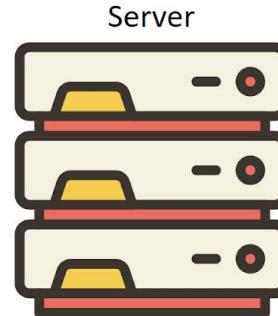
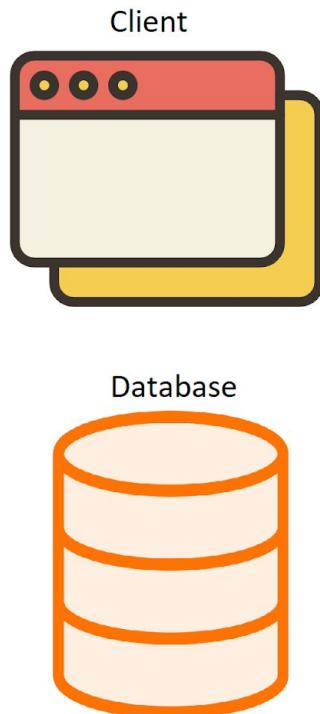
On the left side of the screen, there's a "Coupon saving" section with a "Shop Coupons" button. On the right, there are promotional banners for "Kraft" and "Free Delivery". At the bottom, a message says "Based on your cart" with a "View more" link.

**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

# Kibana

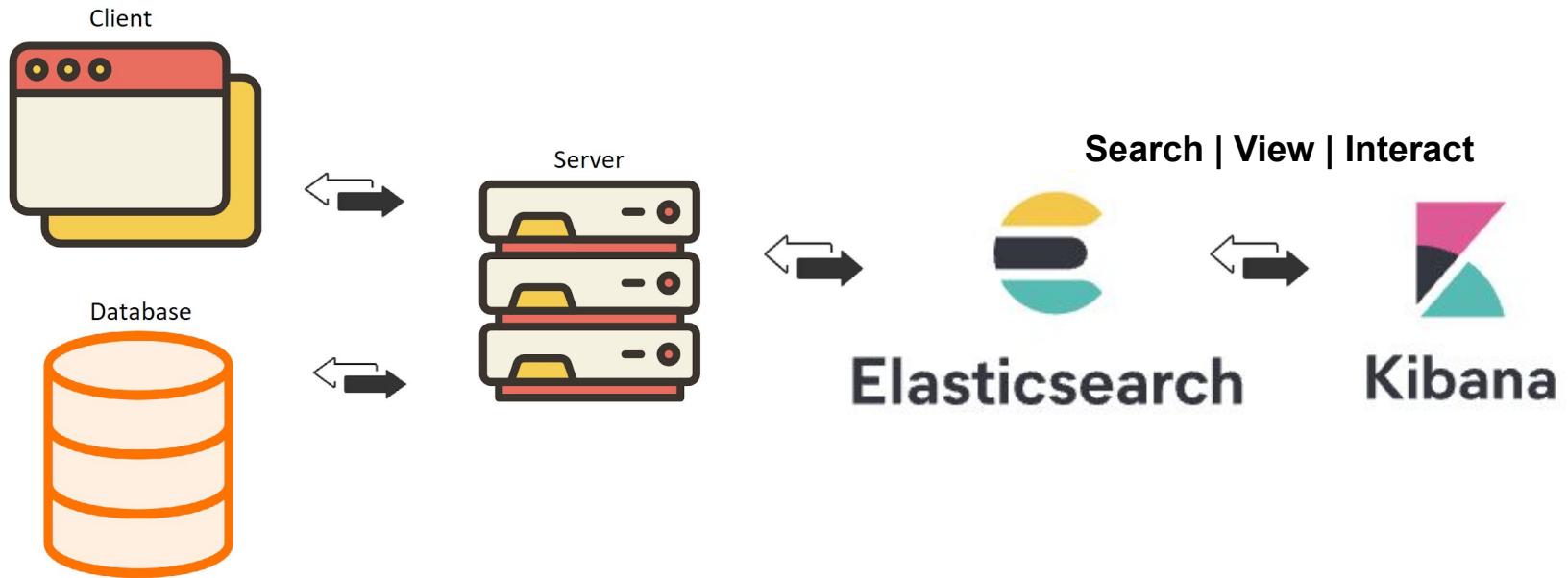
Visualize | Manage

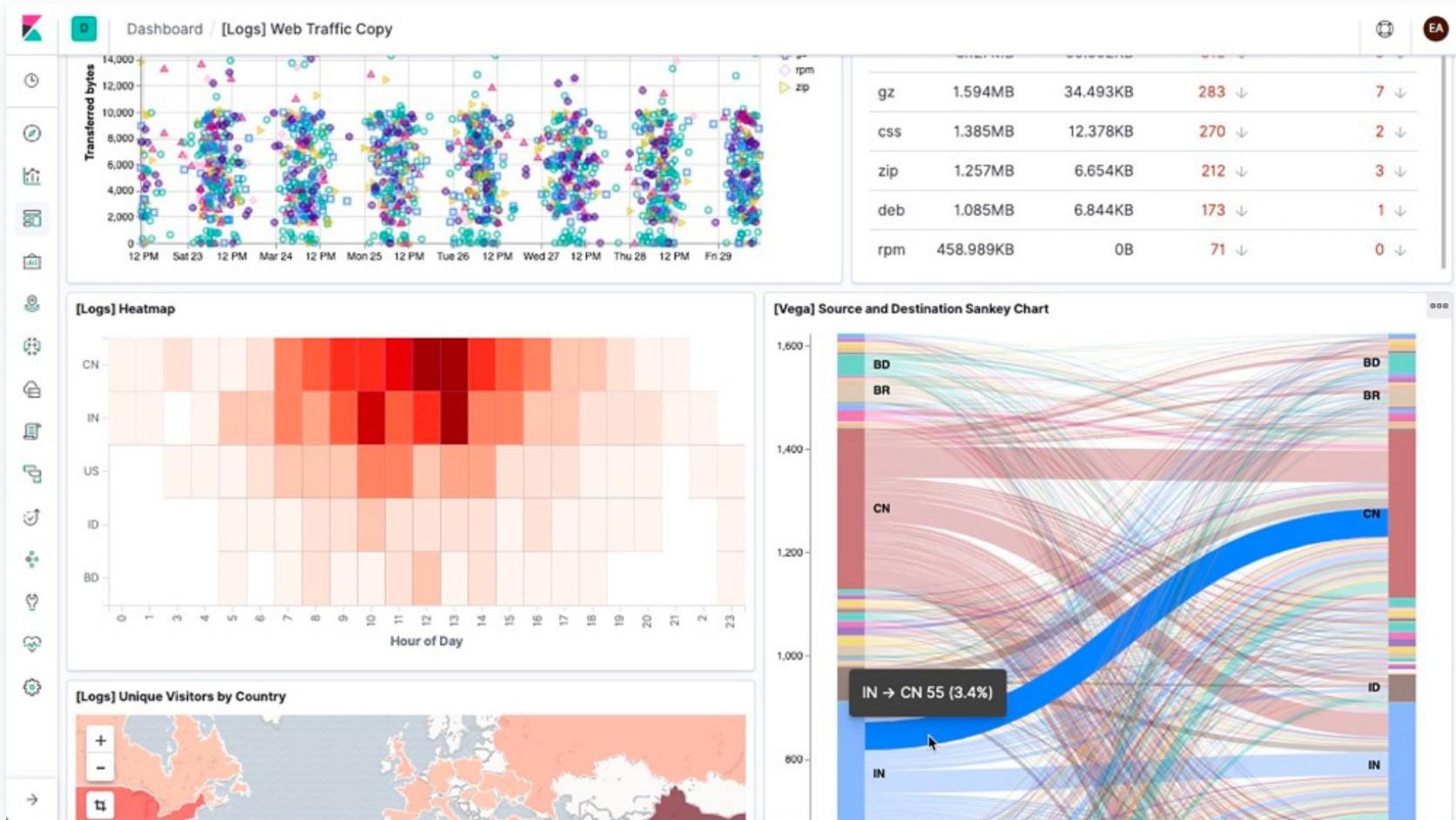
# Elasticsearch

Store | Search | Analyze



**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

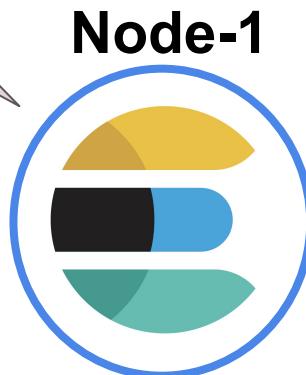
# Elasticsearch

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!

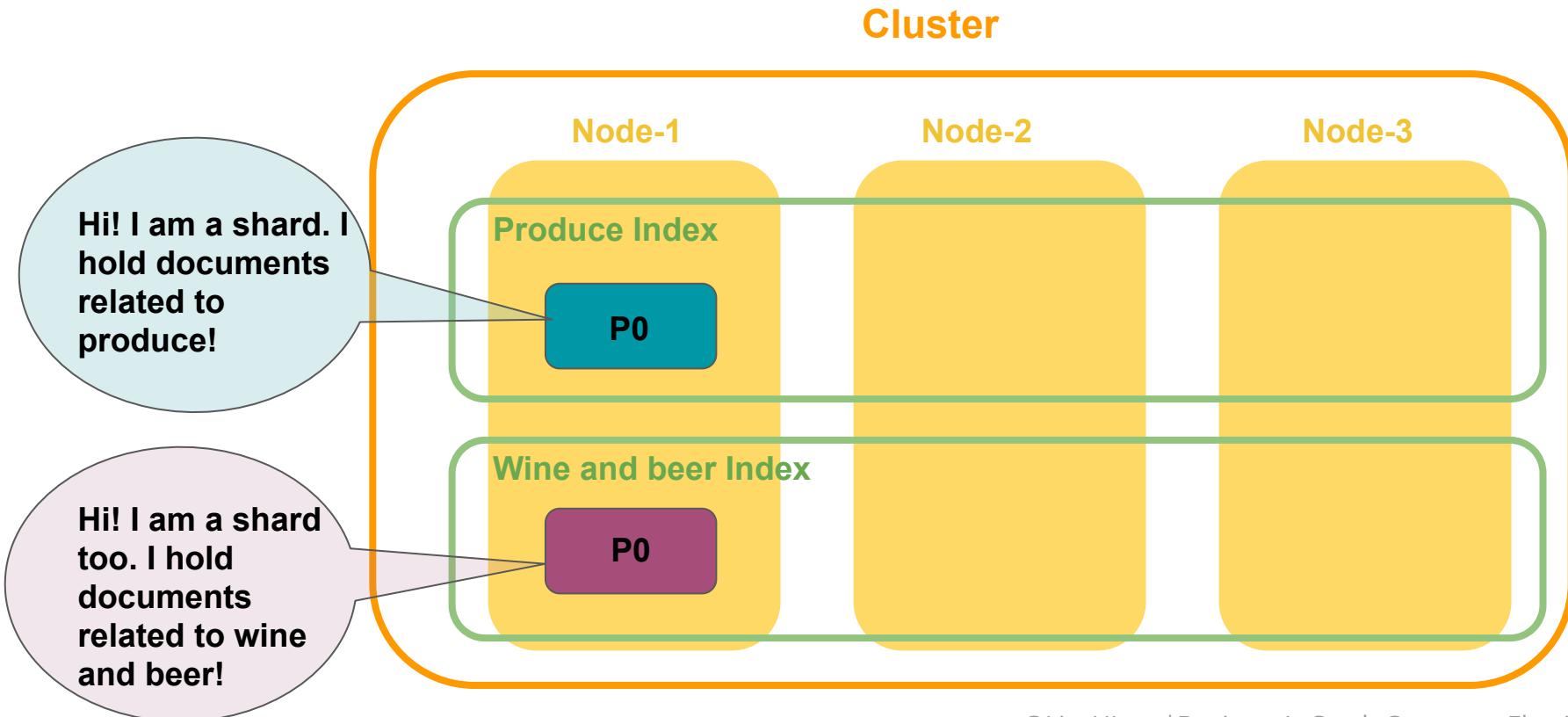
## Produce Index

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

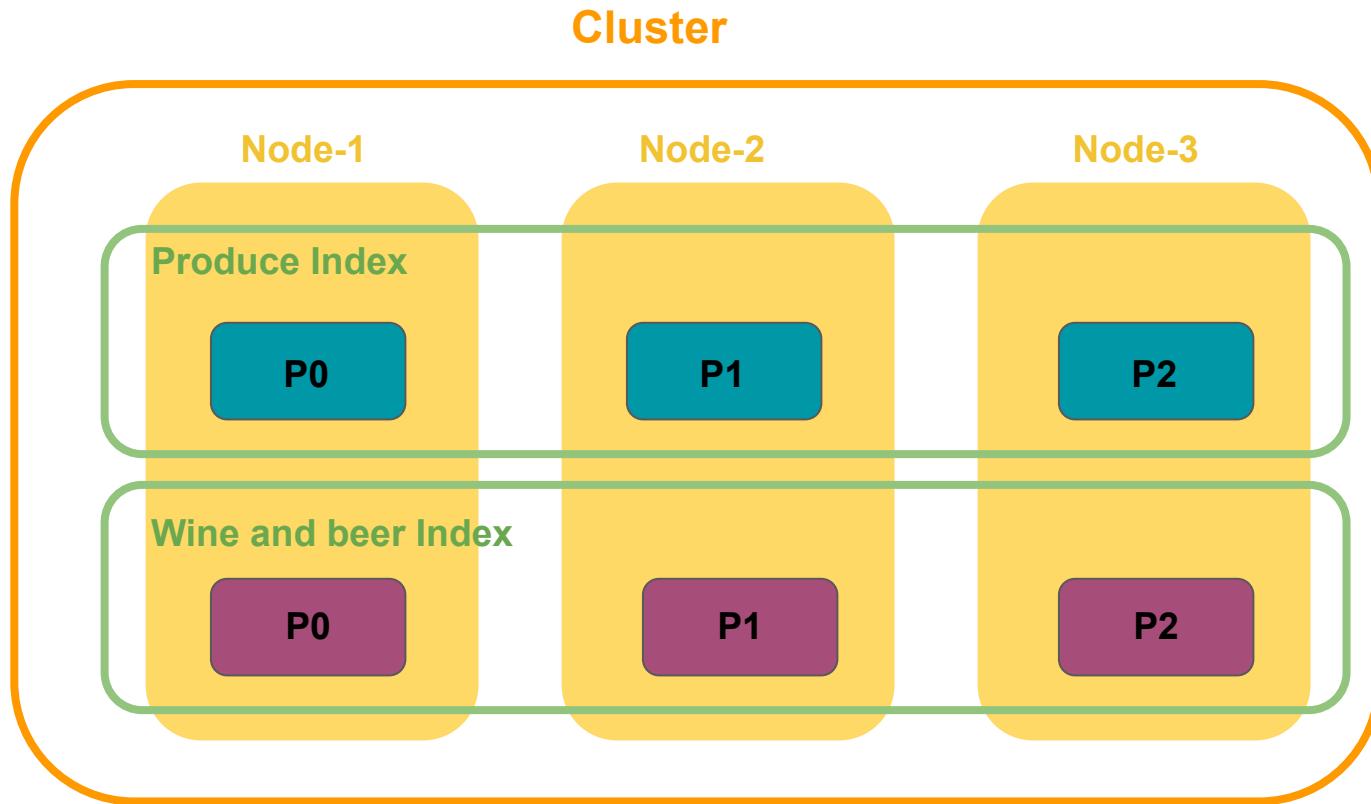
## Wine & Beer Index

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

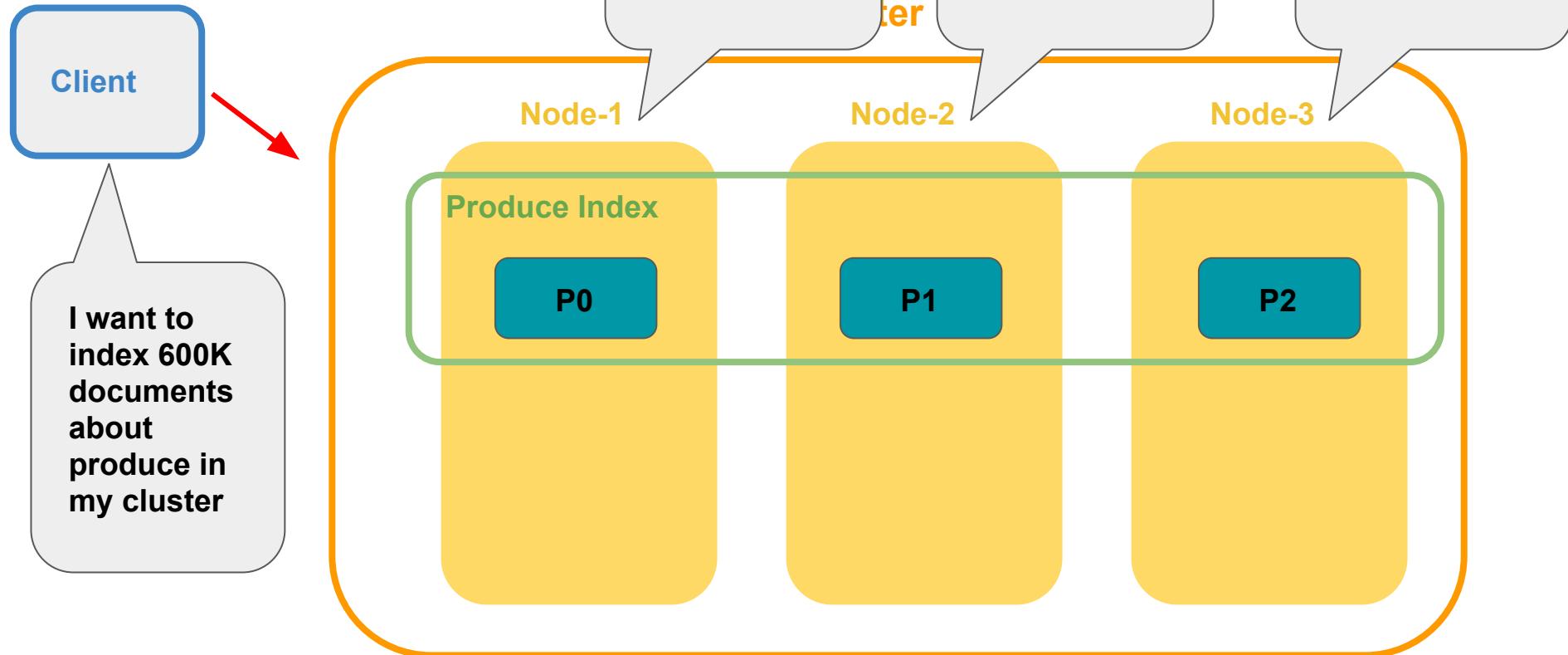
# What is a shard?



# What is sharding?



# What is sharding?



# What is sharding?

Cluster

Node-1

Node-2

Node-3

Node-4

Node-5

Node-6

Node-7

Produce Index

P0

P1

P2

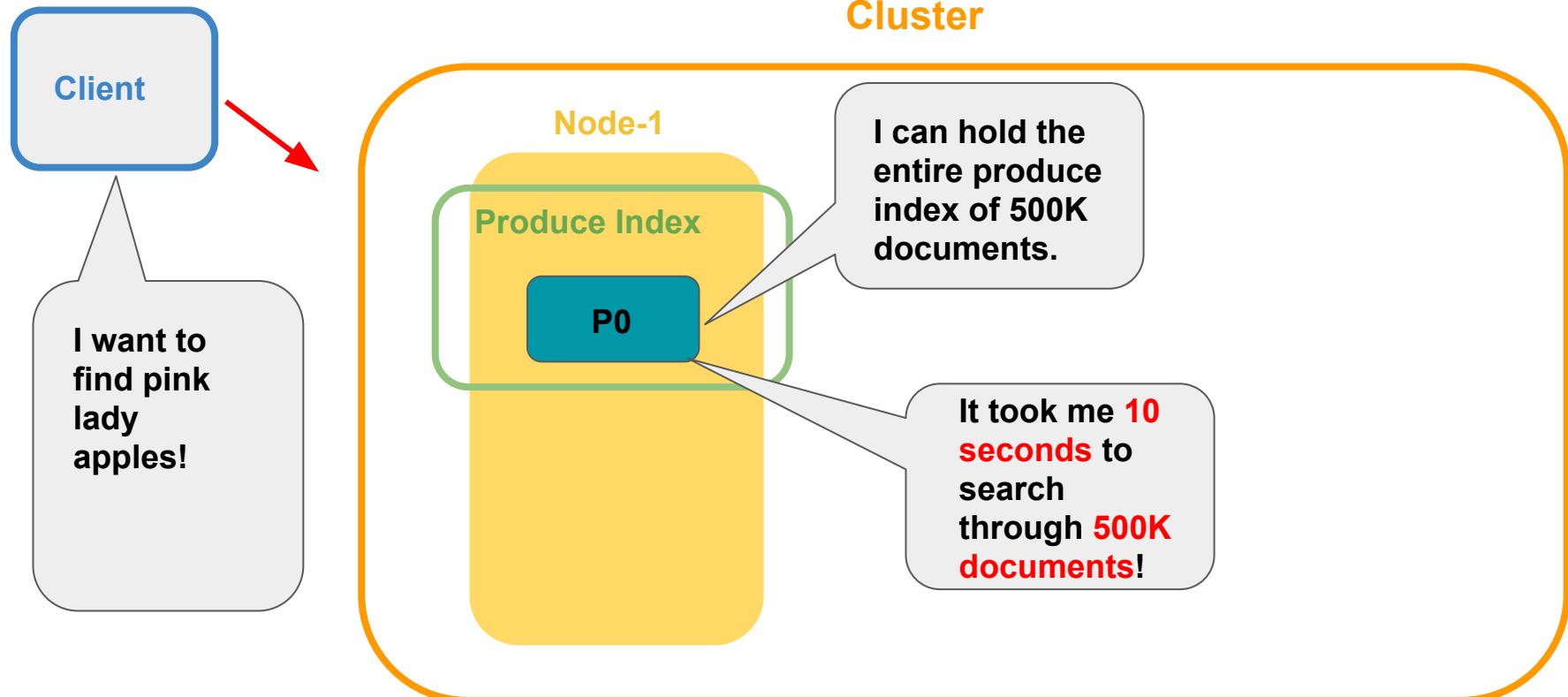
P3

P4

P5

P6

# What is sharding?



# 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

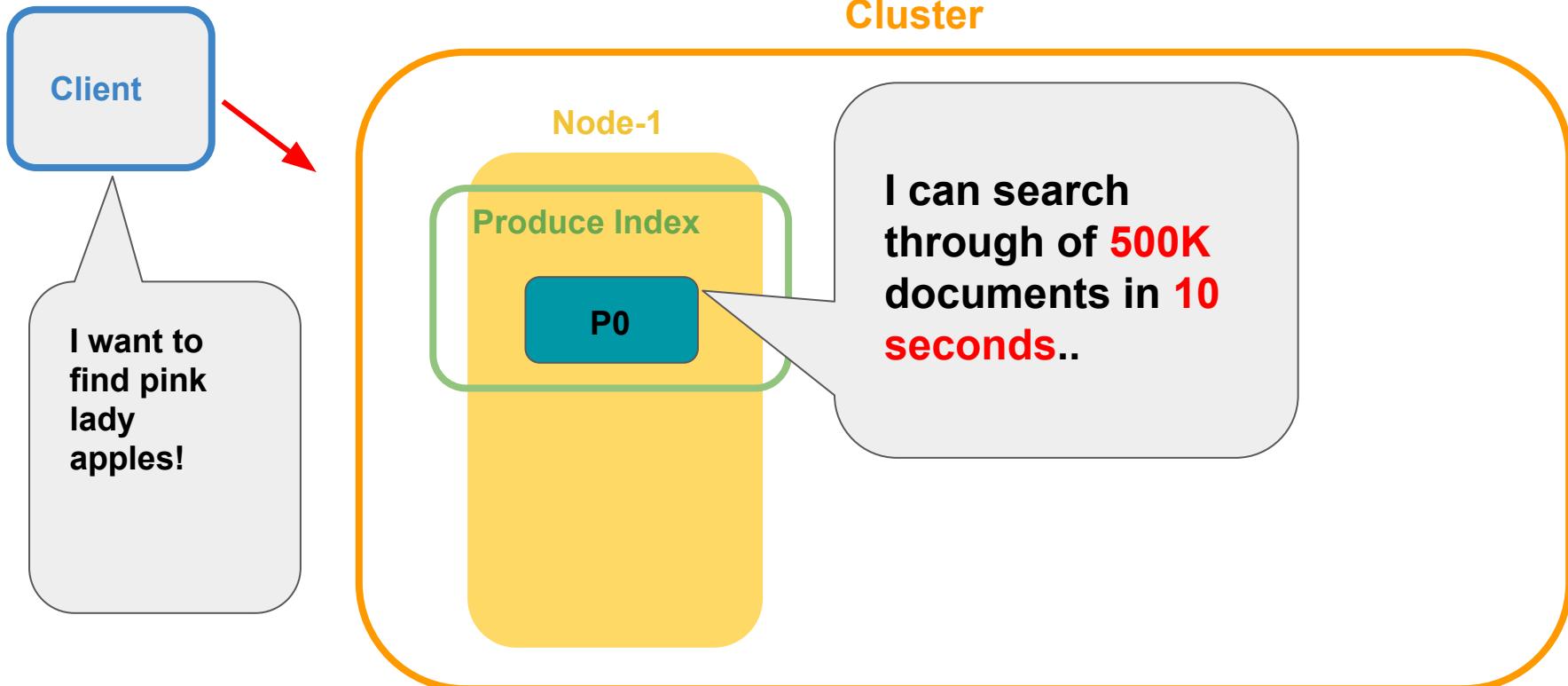
50K

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

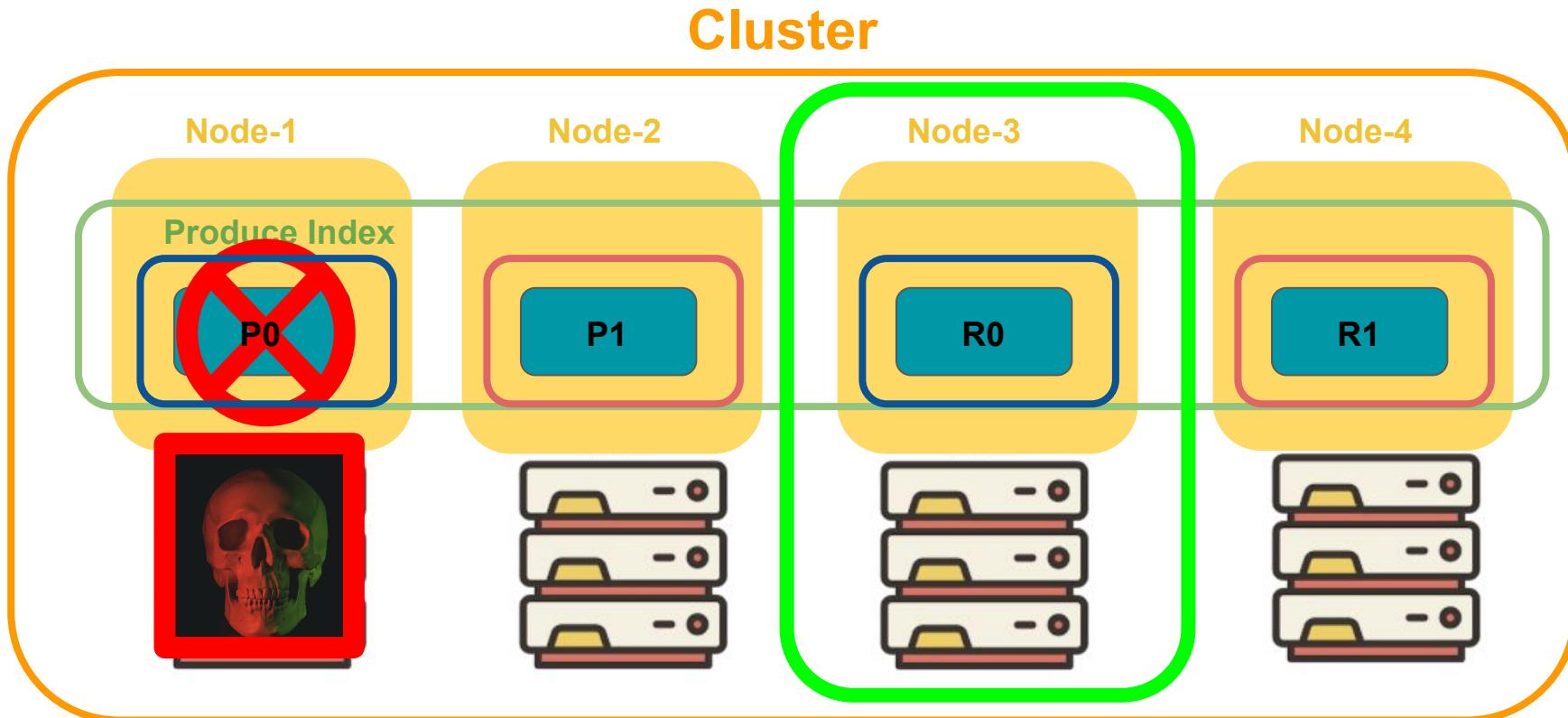


#SPONGEBOBMOVIE

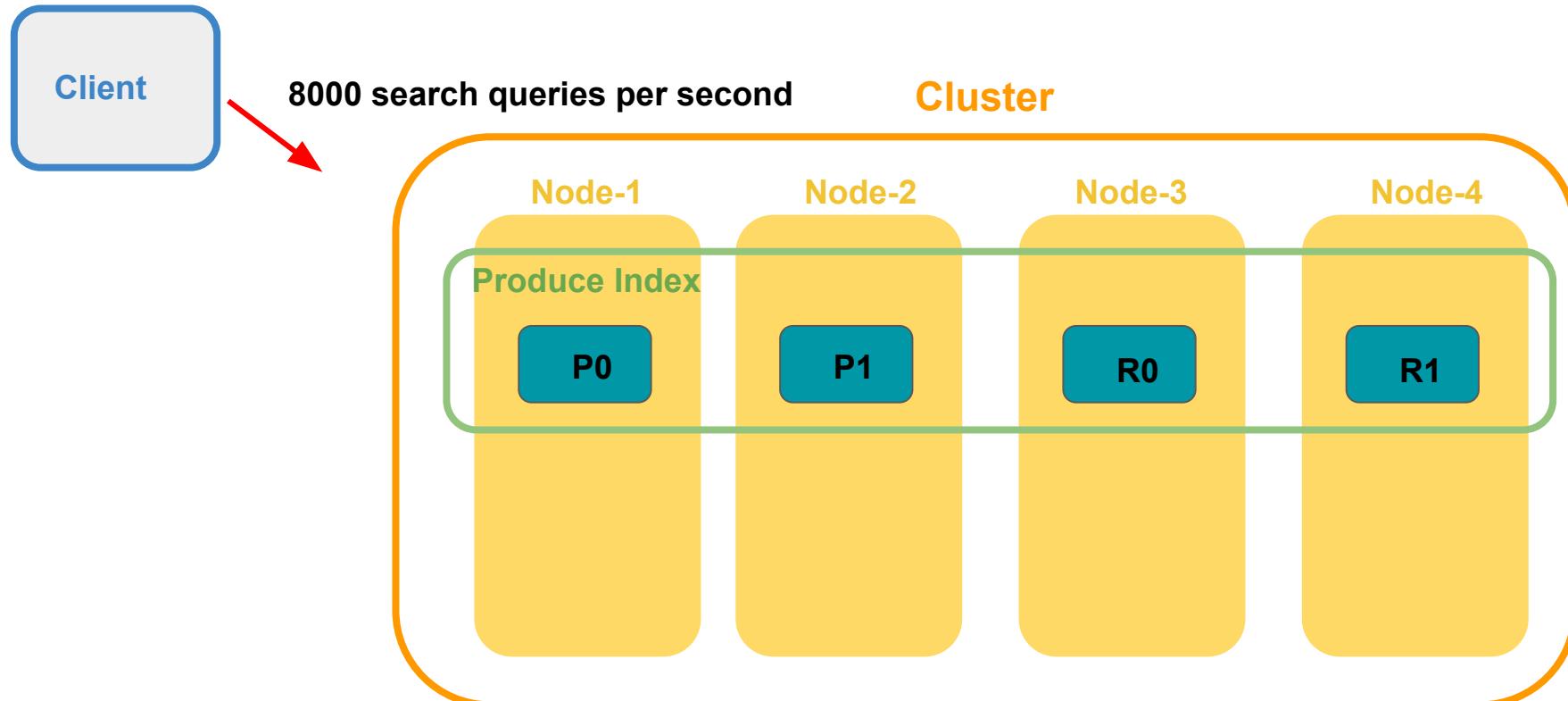


Lionsgate

# 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



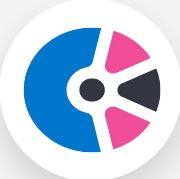
## Elastic Cloud

Deploy instantly on AWS,  
Azure or Google Cloud



## Elastic Cloud Enterprise

Centrally manage multiple  
deployments on your infra



## Elastic Cloud on Kubernetes

<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

The screenshot shows the Elasticsearch Service dashboard. At the top left is the 'ELASTICSEARCH SERVICE' logo. Below it, a section titled 'Deploy Elasticsearch and Kibana in 3 minutes or less' includes a note about a longer trial period (30 vs. 14 days). A 'Try it free' button is highlighted with a red box. The main area displays deployment configurations for 'Data' and 'Kibana' instances across two zones, with a summary of cluster metrics like version (v7.0.1), total memory (24.08 GB), and storage (125.78 TB).

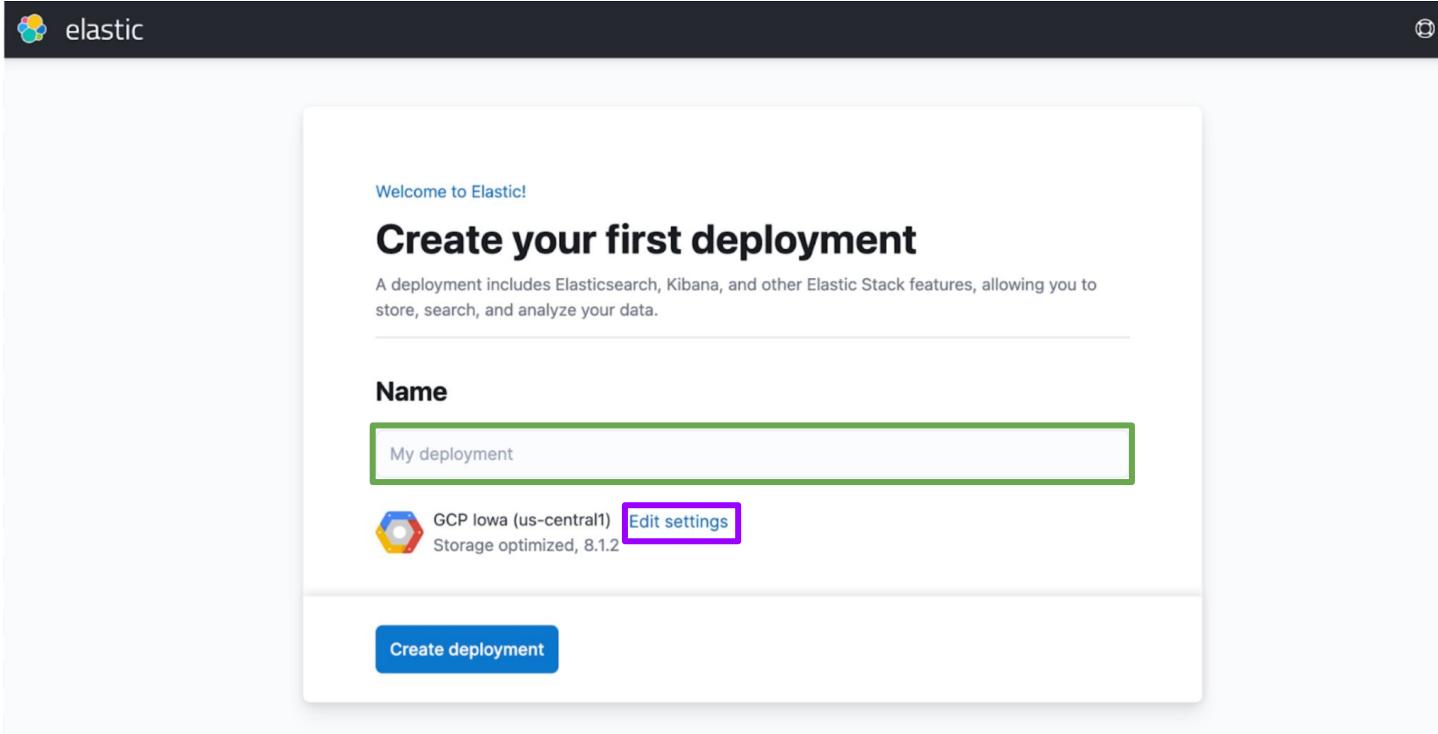
## Trial comes with the following

- 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

The screenshot shows the 'Start your free Elastic Cloud trial' page. It features the 'elastic' logo at the top right. Below it, a heading says 'Start your free Elastic Cloud trial' with a note 'No credit card required'. There are fields for 'Email' and 'Password', both with placeholder icons. A large 'Start free trial' button is highlighted with a purple border. Below the button, there's a link 'Or sign up with' followed by 'Google' and 'Microsoft' social login buttons.

# Name your deployment and click on *Edit settings* option



The screenshot shows the 'Create your first deployment' page in the Elastic interface. At the top, there's a dark header bar with the Elastic logo and a gear icon. Below it is a white card with the following content:

- Welcome to Elastic!
- Create your first deployment**
- A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.
- Name**: A text input field containing "My deployment".
- Cloud provider and region**: Shows "GCP Iowa (us-central1)" with a "Storage optimized, 8.1.2" badge. The "Edit settings" link next to the provider name is highlighted with a purple rectangle.
- Create deployment** button at the bottom.

# Configure your deployment settings

Welcome to Elastic!

## Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

### Name

Mini Beginner's Crash Course to Elasticsearch and Kibana

### Settings [Hide](#)

Cloud provider

Google Cloud

Region

Iowa (us-central1)

Hardware profile  ⓘ

Storage optimized

Version  ⓘ

8.1.2 (latest)

# Choose the cloud provider of your choice

Welcome to Elastic!

## Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

### Name

Mini Beginner's Crash Course to Elasticsearch and Kibana

### Settings Hide

Cloud provider

Google Cloud

Region

✓ Google Cloud

Hardware profile ①

aws Amazon Web Services

▲ Azure

Version ①

8.1.2 (latest)

Create deployment

# Select the region closest to you

Welcome to Elastic!

## Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

### Name

Mini Beginner's Crash Course to Elasticsearch and Kibana

### Settings Hide

Cloud provider  Google Cloud ▾

Region  Iowa (us-central1) | ▾

- ✓  Iowa (us-central1)
-  N. Virginia (us-east4)
-  Oregon (us-west1)
-  South Carolina (us-east1)
-  Montreal (northamerica-northeast1)
-  Sao Paulo (southamerica-east1)
-  Belgium (europe-west1)

Hardware profile  ⓘ

Version  ⓘ

**Create deployment**

# Select your hardware profile

Welcome to Elastic!

## Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

### Name

Mini Beginner's Crash Course to Elasticsearch and Kibana

### Settings Hide

Cloud provider

Google Cloud

Region

Oregon (us-west1)

Hardware profile  ⓘ

Storage optimized

Version  ⓘ

#### General purpose

Suitable for ingestion use cases with 5-7 days of data available for fast access. Also good for search workloads with less-frequent indexing and medium to high querying loads. Provides a balance of storage, memory, and CPU.

Create deployment

#### Storage optimized

Good for most ingestion use cases with 7-10 days of data available for fast access. Also good for light search use cases without heavy indexing or CPU needs.

#### Storage optimized (dense)

Ideal for ingestion use cases with more than 10 days of data available for fast access. Also good for light search

# Select the latest version of the Elastic Stack

Welcome to Elastic!

## Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

### Name

Mini Beginner's Crash Course to Elasticsearch and Kibana

### Settings Hide

Cloud provider

Google Cloud

Region

Oregon (us-west1)

Hardware profile ⓘ

Storage optimized

Version ⓘ

8.1.2 (latest) |

#### Generally available versions

✓ 8.1.2 (latest)

8.0.1

7.17.2

Create deployment

# Save your deployment credentials

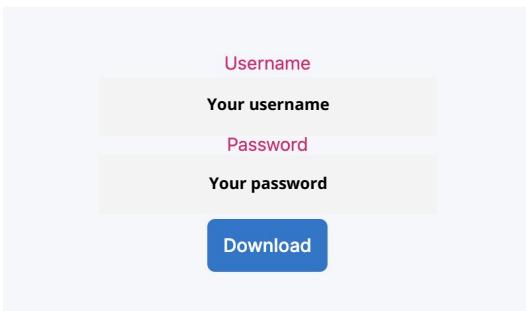
 Your deployment is ready!

Continue

## Save the deployment credentials

These root credentials are shown only once.

They provide super user access to your deployment. Keep them safe.



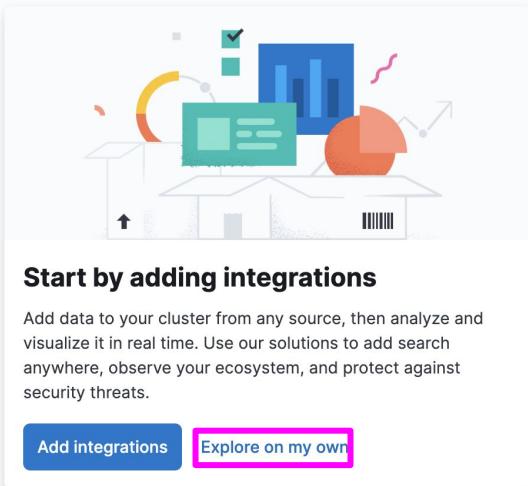
Username  
Your username

Password  
Your password

Download

Skip

# Click on *Explore on my own* option



The screenshot shows the 'Welcome to Elastic' interface. At the top is a circular logo with three colored dots (blue, green, yellow). Below it is the text 'Welcome to Elastic'. A central graphic features a house with various data visualization elements like charts and arrows above it. Below the graphic, the text 'Start by adding integrations' is followed by a descriptive paragraph about adding data from sources and using solutions for search, visualization, and security. At the bottom, there are two buttons: 'Add integrations' (blue) and 'Explore on my own' (pink, with a pink border).

To learn about how usage data helps us manage and improve our products and services, see our [Privacy Statement](#).

# Click on *Dev Tools* option

The screenshot shows the Elastic Stack Home page. At the top, there's a navigation bar with the elastic logo, a search bar, and user icons. Below it is a section titled "Welcome home" featuring four colored tiles: yellow (Enterprise Search), pink (Observability), teal (Security), and blue (Analytics). Each tile has an icon and a brief description. Underneath this is a section titled "Get started by adding integrations" with instructions and three buttons: "Add integrations", "Try sample data", and "Upload a file". To the right of these buttons is a decorative graphic of data visualization elements like charts and graphs. Below this is a "Management" section with five items: "Manage permissions", "Monitor the stack", "Back up and restore", "Manage index lifecycles", and "Dev Tools". The "Dev Tools" button is highlighted with a pink box. At the bottom left is a link to "Display a different page on log in".

# Click on dismiss and delete the default query

The screenshot shows the Elastic Dev Tools interface. On the left is the editor pane containing a code editor with a blue border around the first line of code. The code is:GET \_search
{
 "query": {
 "match\_all": {}
}On the right is the response pane titled "Welcome to Console". It contains a "Quick intro to the UI" section with text and a code example, and a "A few quick tips, while I have your attention" section with a bulleted list. A red box highlights the "Dismiss" button at the bottom of the intro section.

Welcome to Console

Quick intro to the UI

The Console UI is split into two panes: an editor pane (left) and a response pane (right). Use the editor to type requests and submit them to Elasticsearch. The results will be displayed in the response pane on the right side.

Console understands requests in a compact format, similar to cURL:

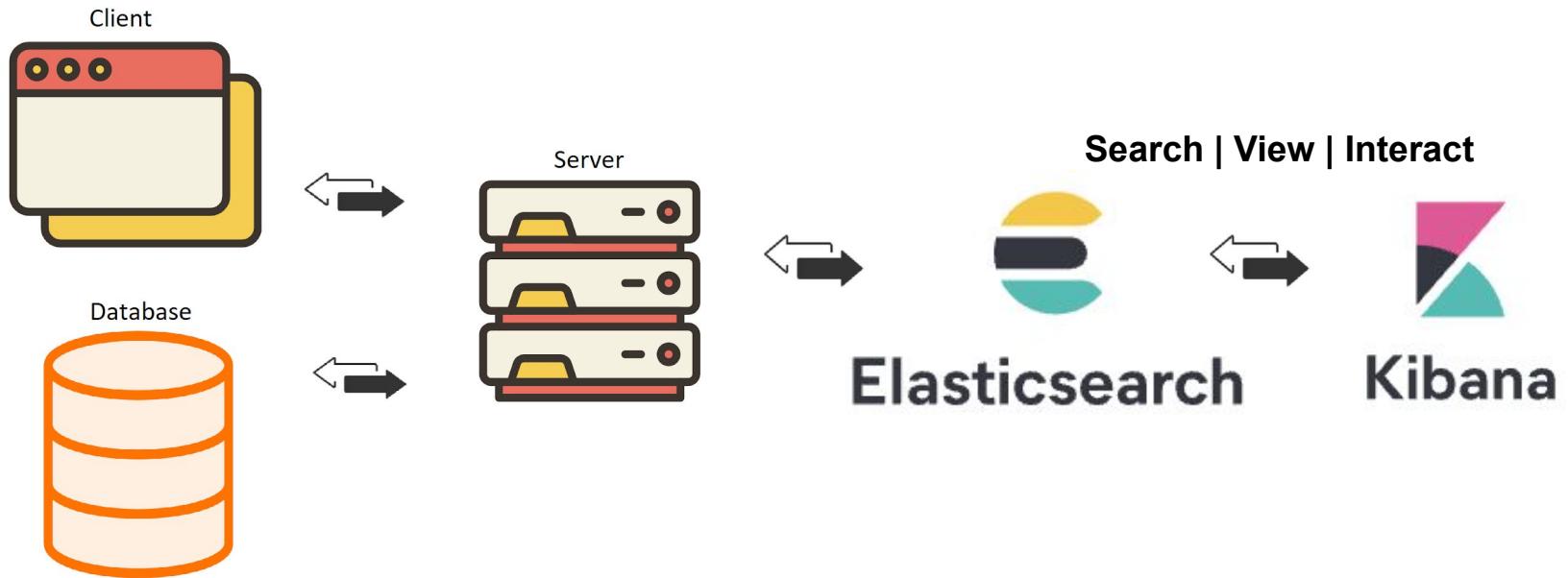
```
1 # index a doc
2 PUT index/_doc/1
3 {
4   "body": "here"
5 }
6
7 # and get it ...
8 GET index/_doc/1
```

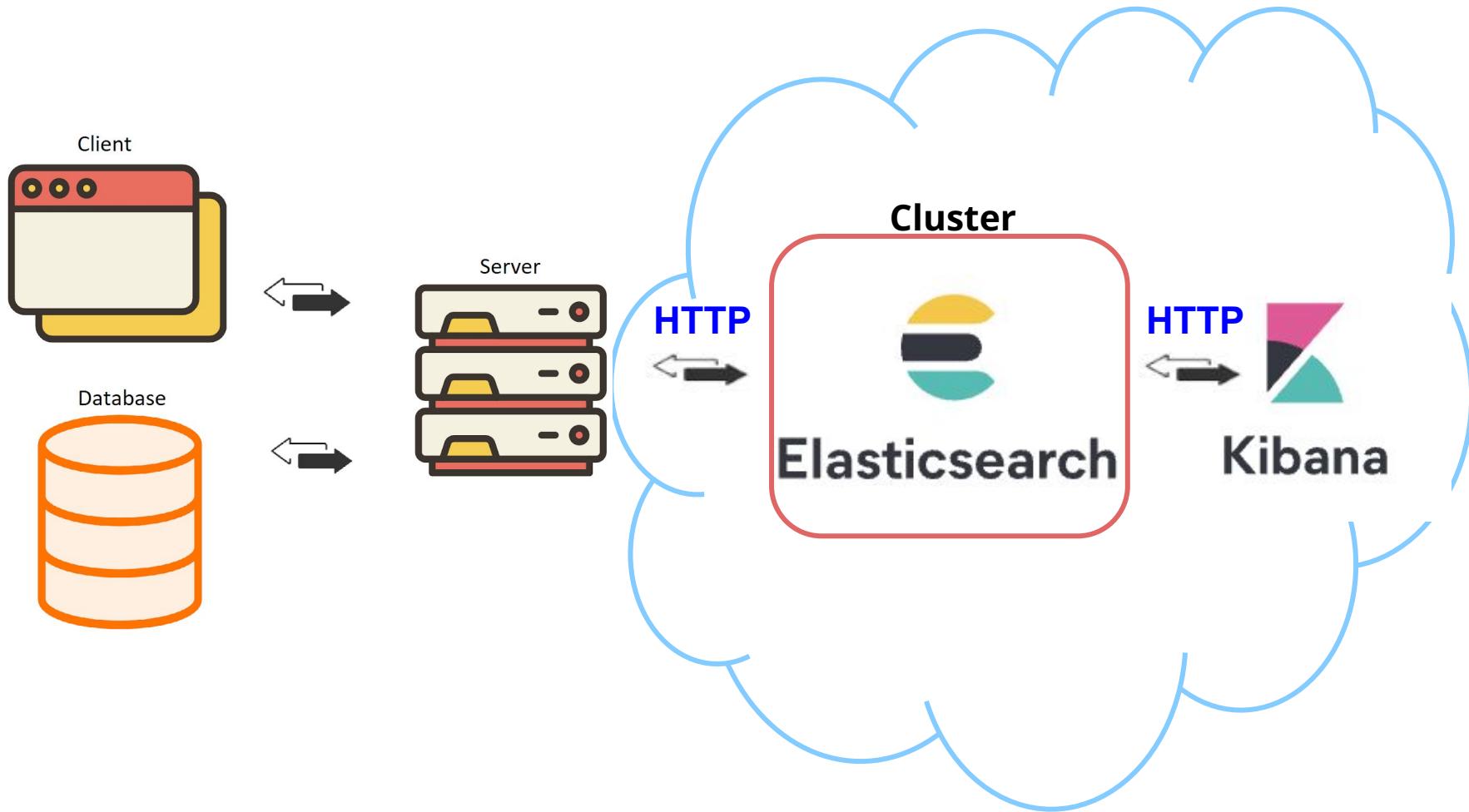
While typing a request, Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure as well as your indices and types.

A few quick tips, while I have your attention

- Submit requests to ES using the green triangle button.
- Use the wrench menu for other useful things.
- You can paste requests in cURL format

**Dismiss**



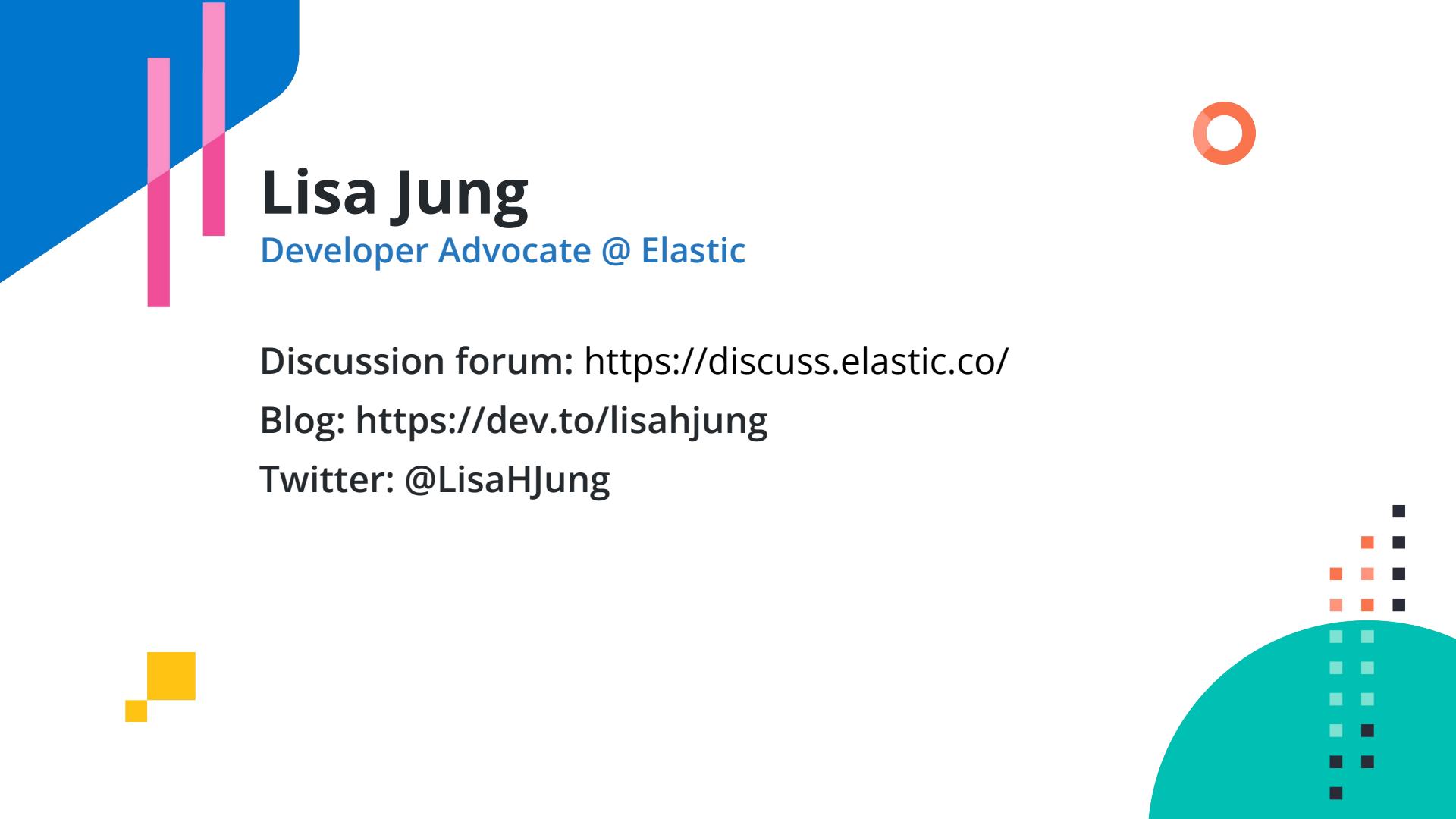


# Questions?



# 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

