



# 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-04Fl2hA9vvASBkYPe~QZmw](https://join.slack.com/t/elasticstack/shared_invite/zt-an1h0etg-04Fl2hA9vvASBkYPe~QZmw)



# Vancouver Meetup: Beginner's Crash Course to the Elastic Stack Series

Part 1: Intro to Elasticsearch and Kibana

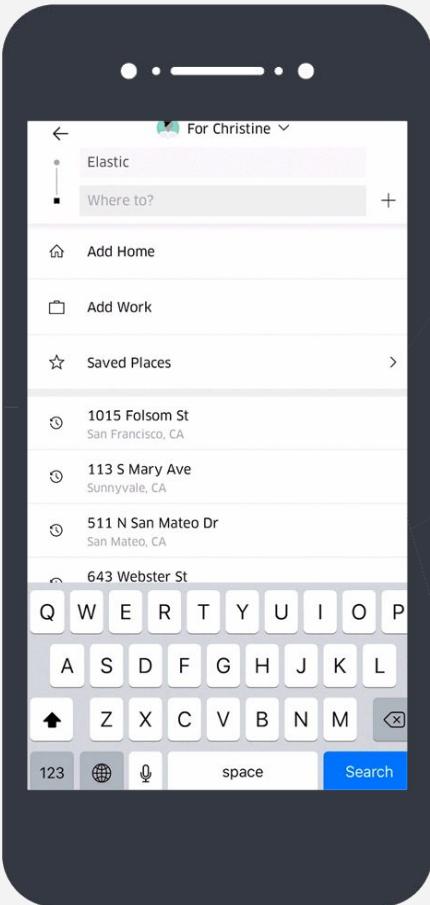
---

Lisa Jung  
Developer Advocate @Elastic

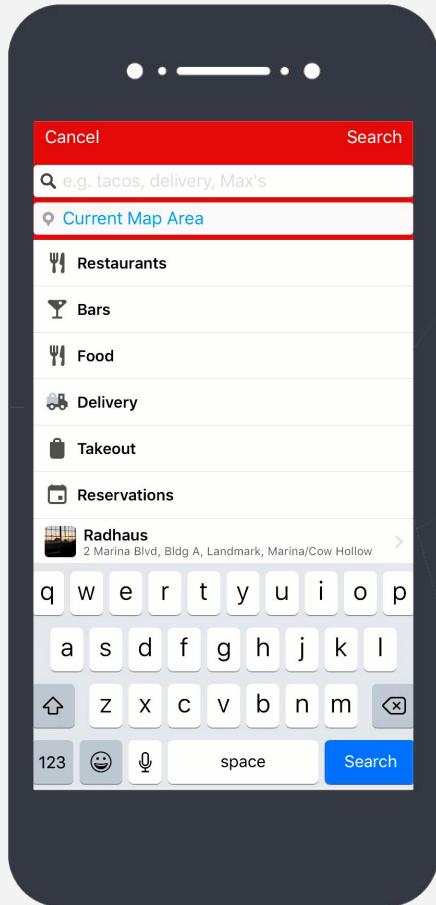


# Have you ever used the Elastic Stack before?

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



# Searching for Rides



# Searching for Restaurants

Uber

tinder

 twilio

 GitHub





 Adobe

 instacart

GRUBHUB

 shopify

Searching for  
Rides

## The Elastic Stack

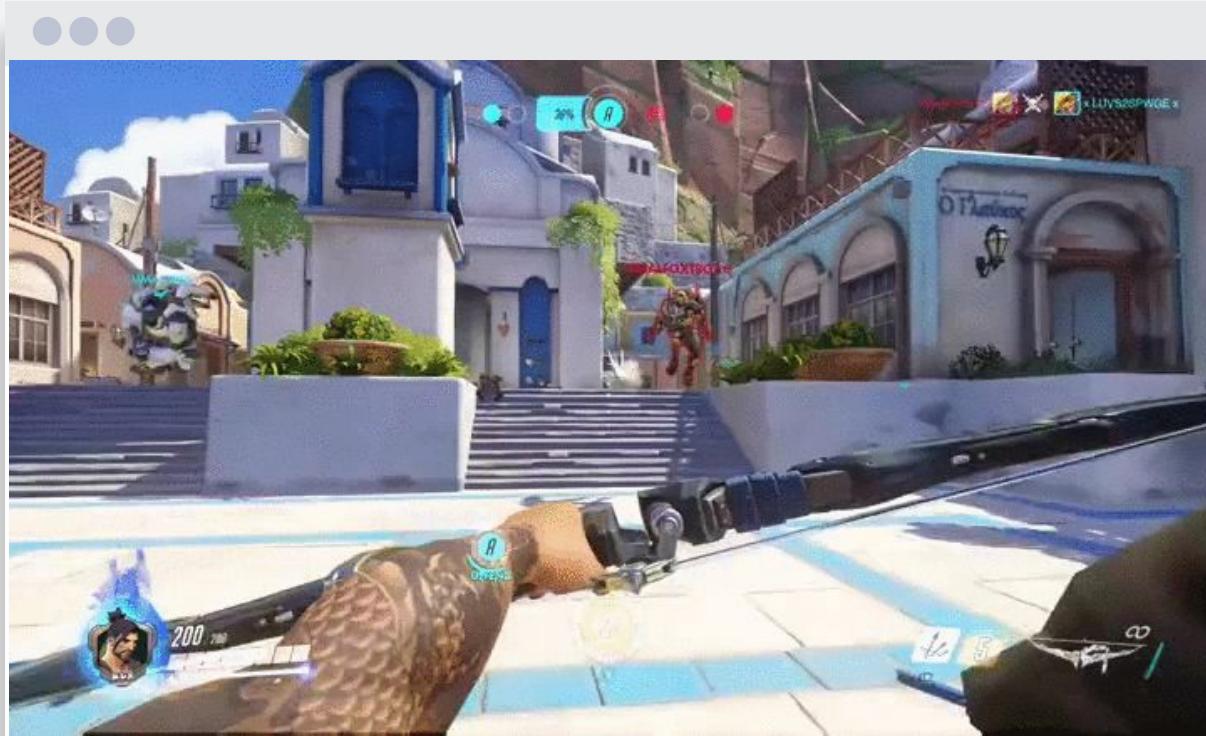
Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



# Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

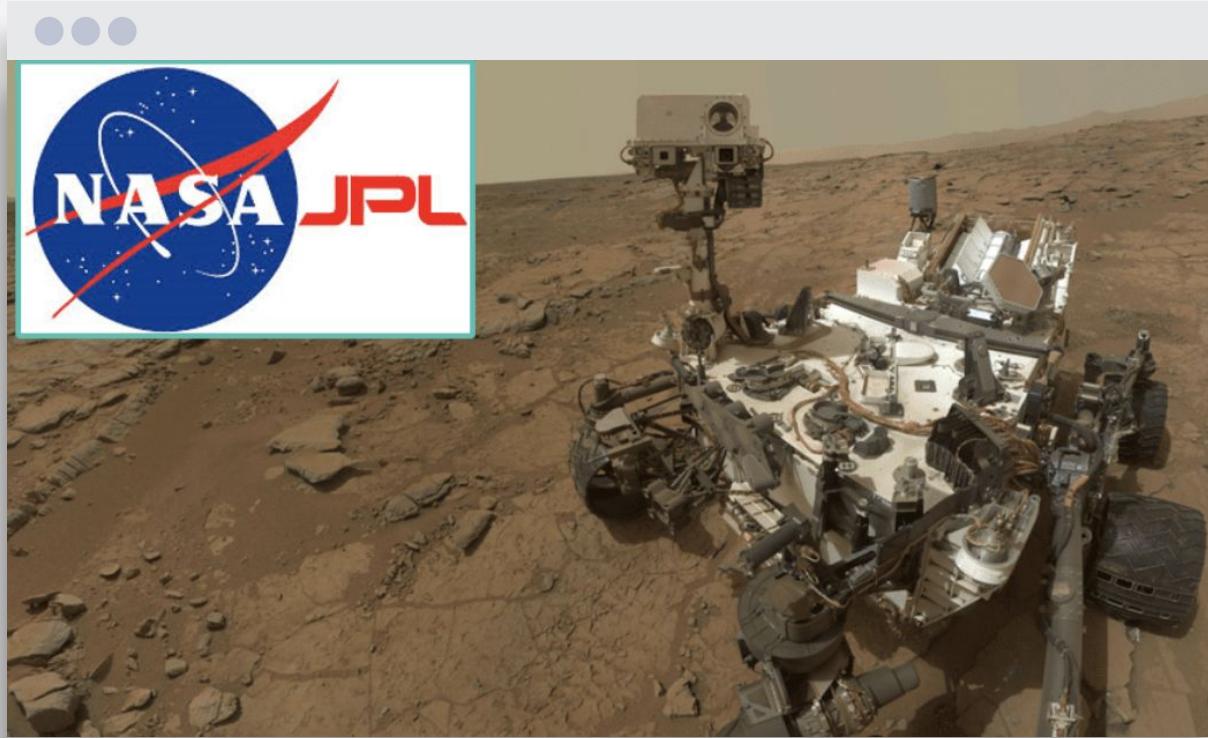
# Use Case: Logging



ACTIVISION  
BLIZZARD

[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/)

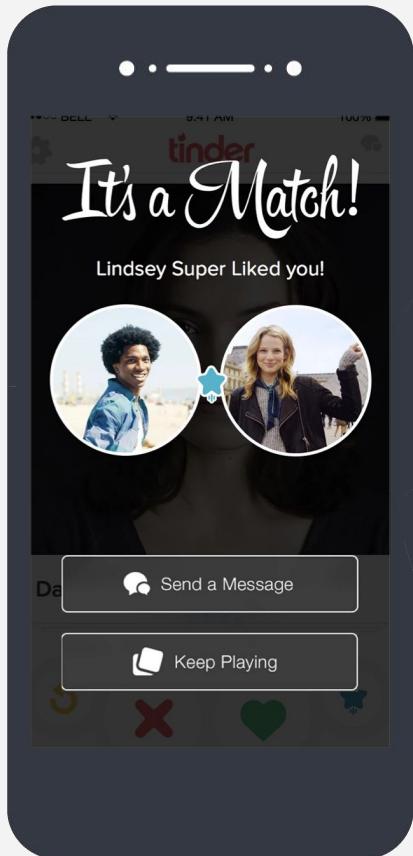
# Use Case: Metrics



# 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.





# **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.

A screenshot of the Instacart mobile website. At the top, the Instacart logo is visible along with a "Stores" button, a location indicator ("Delivery in 94086"), an "Account" button, a "Help" link, and a "Cart" button with a red badge showing the number 4. The background features a collage of fresh produce like avocados and kale. A search bar contains the partial text "can". 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

Below the search bar, there's a "Coupon saving" section with a "Shop Coupons" button, a "Save Now" button next to a Kraft logo, and another "Save Now" button. At the bottom, it says "Based on your cart" and "View more".

can

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

Coupon saving  
Up to 40% off everyday

Shop Coupons Save Now Kraft Save Now

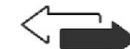
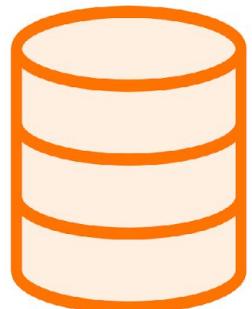
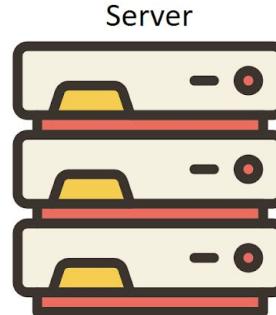
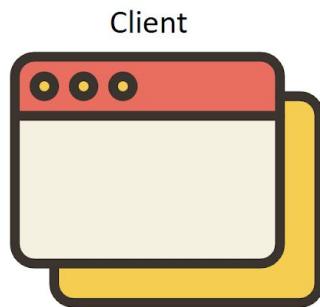
Based on your cart View more

**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 Srircalah? Srirracha?**



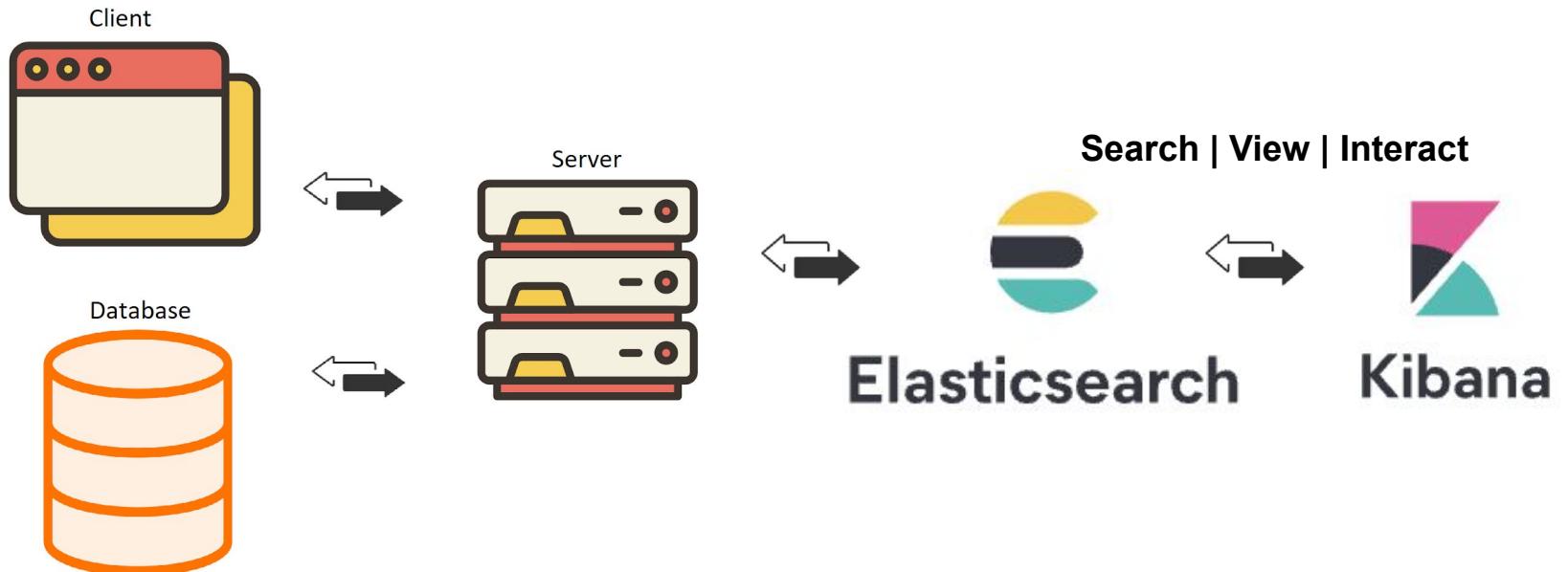


Elasticsearch

# Elasticsearch

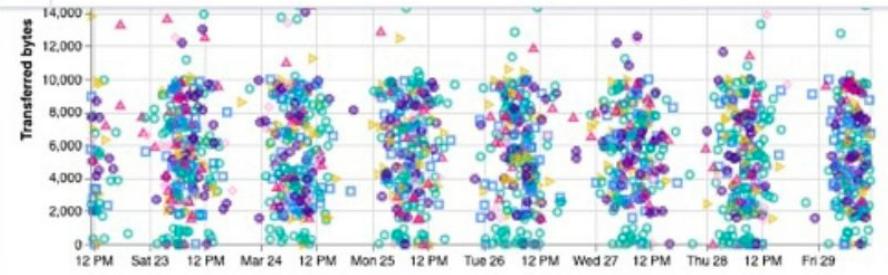
Store | Search | Analyze





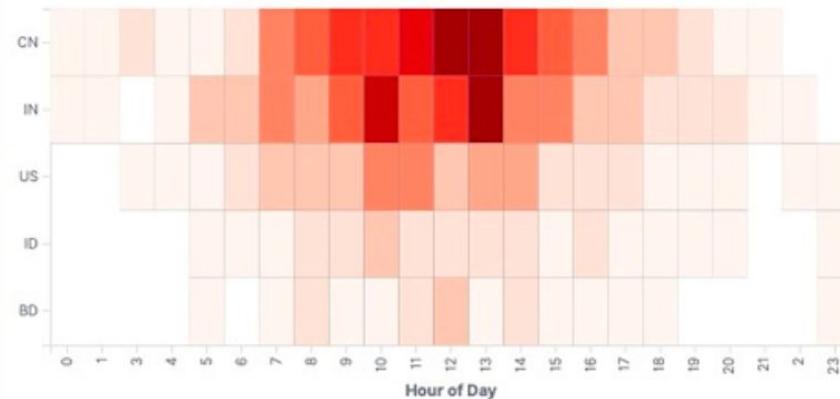


- [Logs](#)
- [Metrics](#)
- [Discover](#)
- [Visualize](#)
- [Dashboard](#)
- [Geospatial](#)
- [A/B Test](#)
- [Alerting](#)
- [Cloud](#)
- [Settings](#)
- [Logout](#)

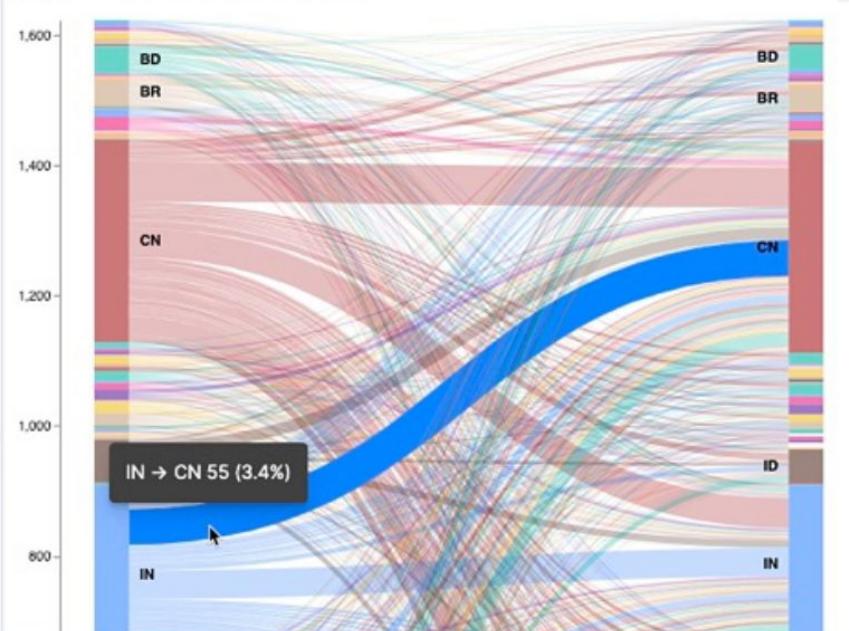


gz	1.594MB	34.493KB	283	↓	7	↓
css	1.385MB	12.378KB	270	↓	2	↓
zip	1.257MB	6.654KB	212	↓	3	↓
deb	1.085MB	6.844KB	173	↓	1	↓
rpm	458.989KB	0B	71	↓	0	↓

## [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

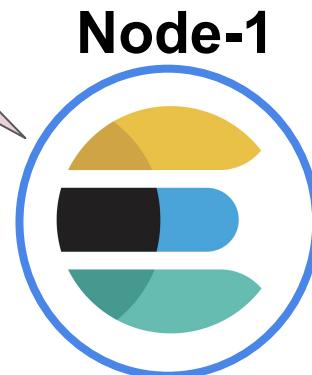
# Elasticsearch

Store | Search | Analyze



# Cluster

I belong to a single cluster!



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

I have a unique id and a name!

# Cluster

**Node-1**



**Node-2**



**Node-3**



**Node-4**





# 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!

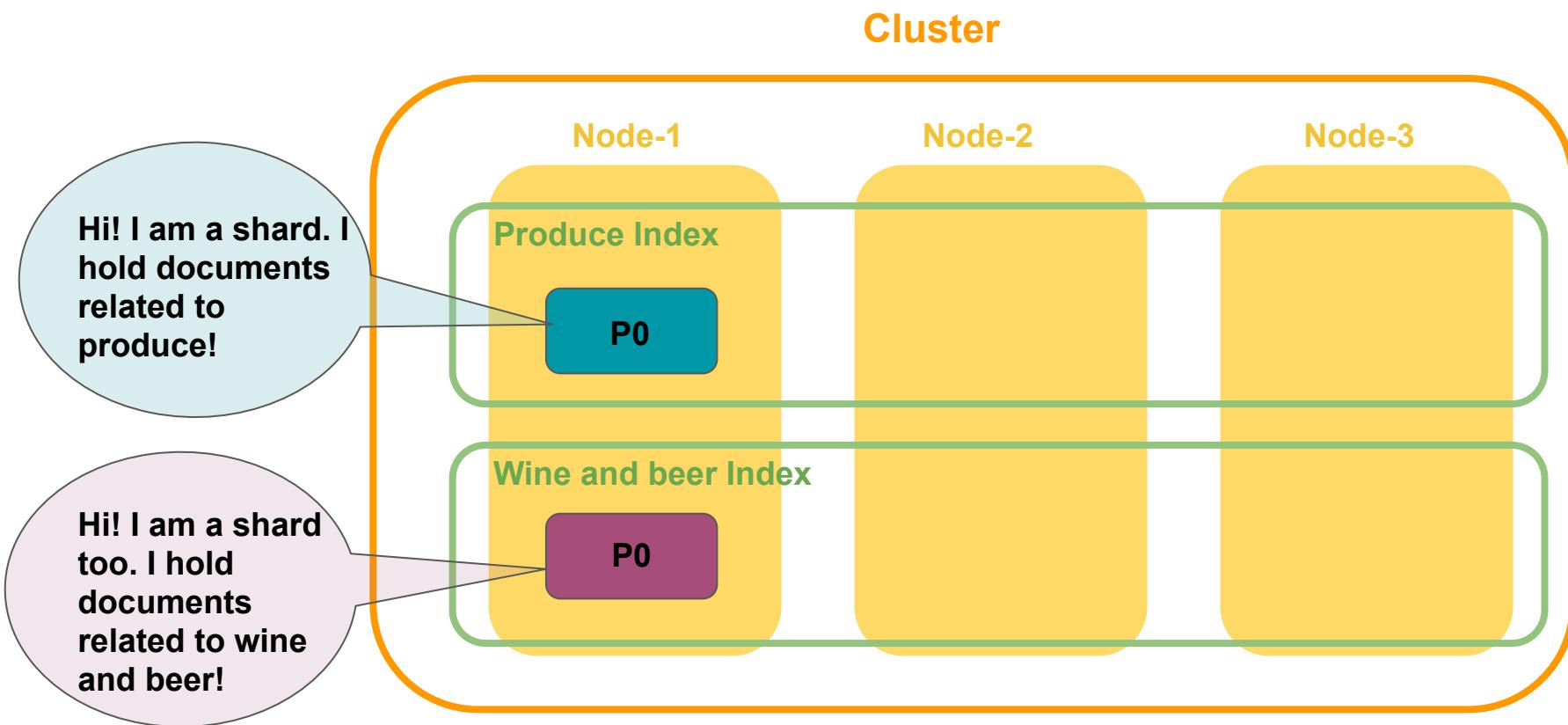
## Produce Index

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

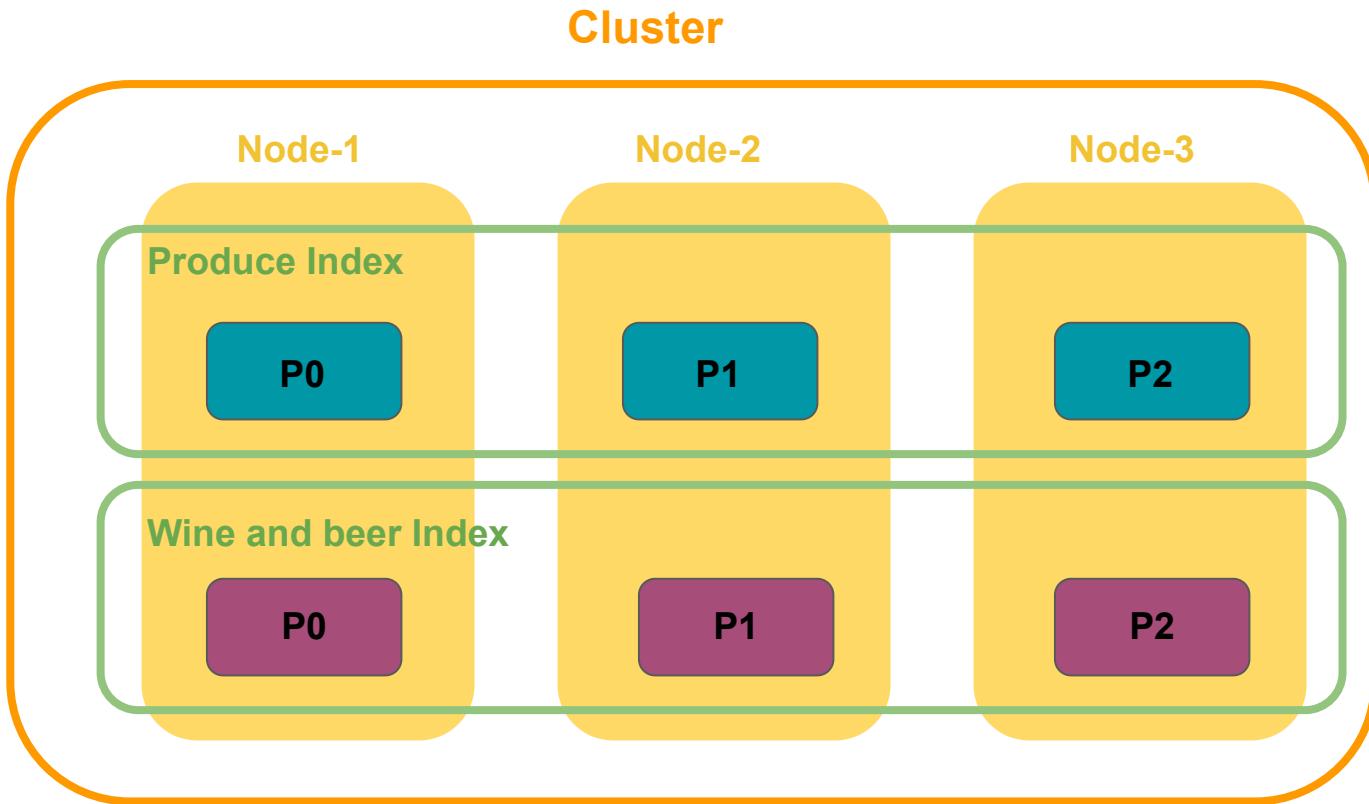
## Wine & Beer Index

```
{  
  "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"  
}
```

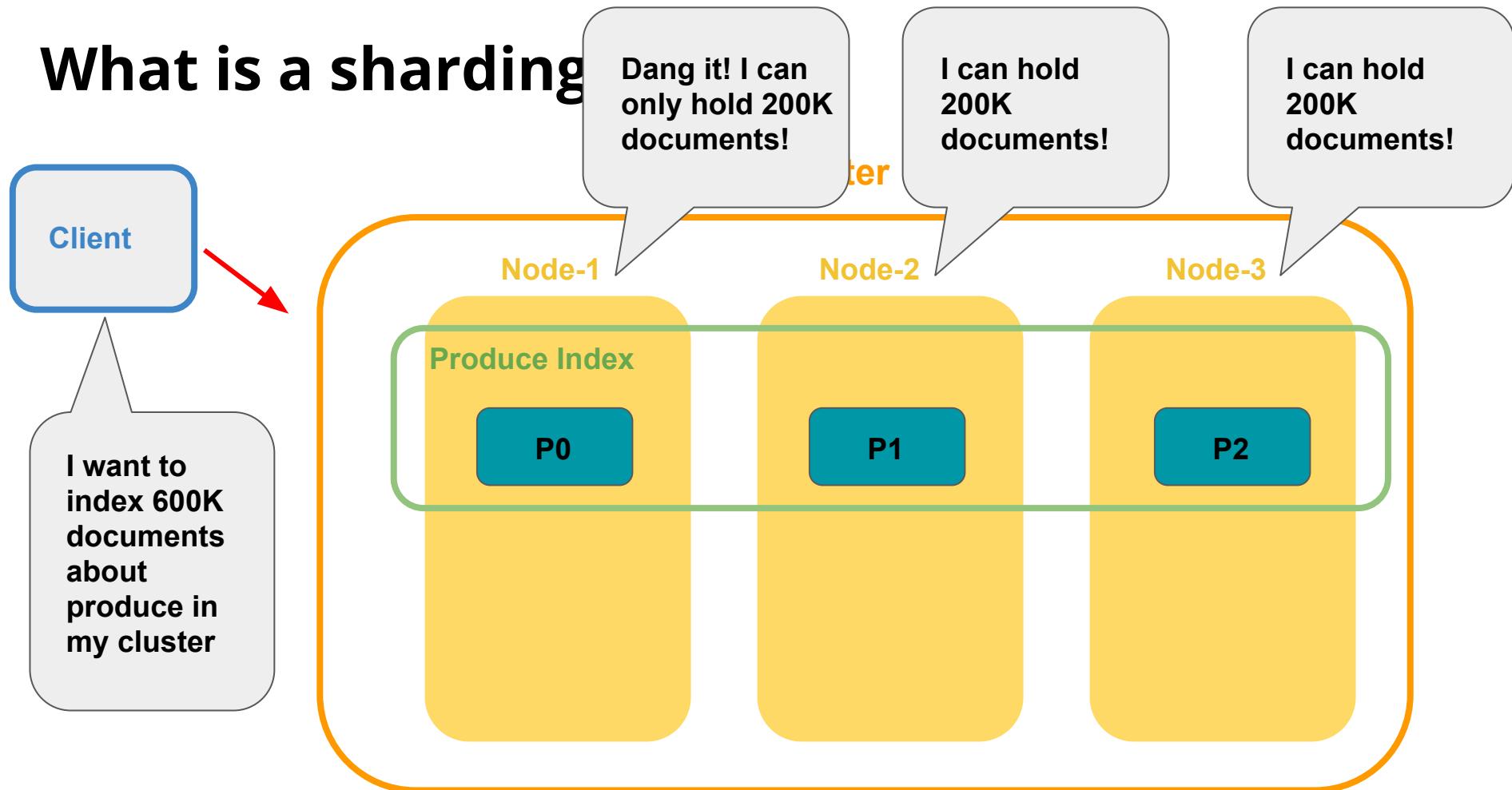
# What is a shard?



# What is a sharding?



# What is a sharding



# What is a sharding?

Cluster

Node-1

Node-2

Node-3

Node-4

Node-5

Node-6

Node-7

Produce Index

P0

P1

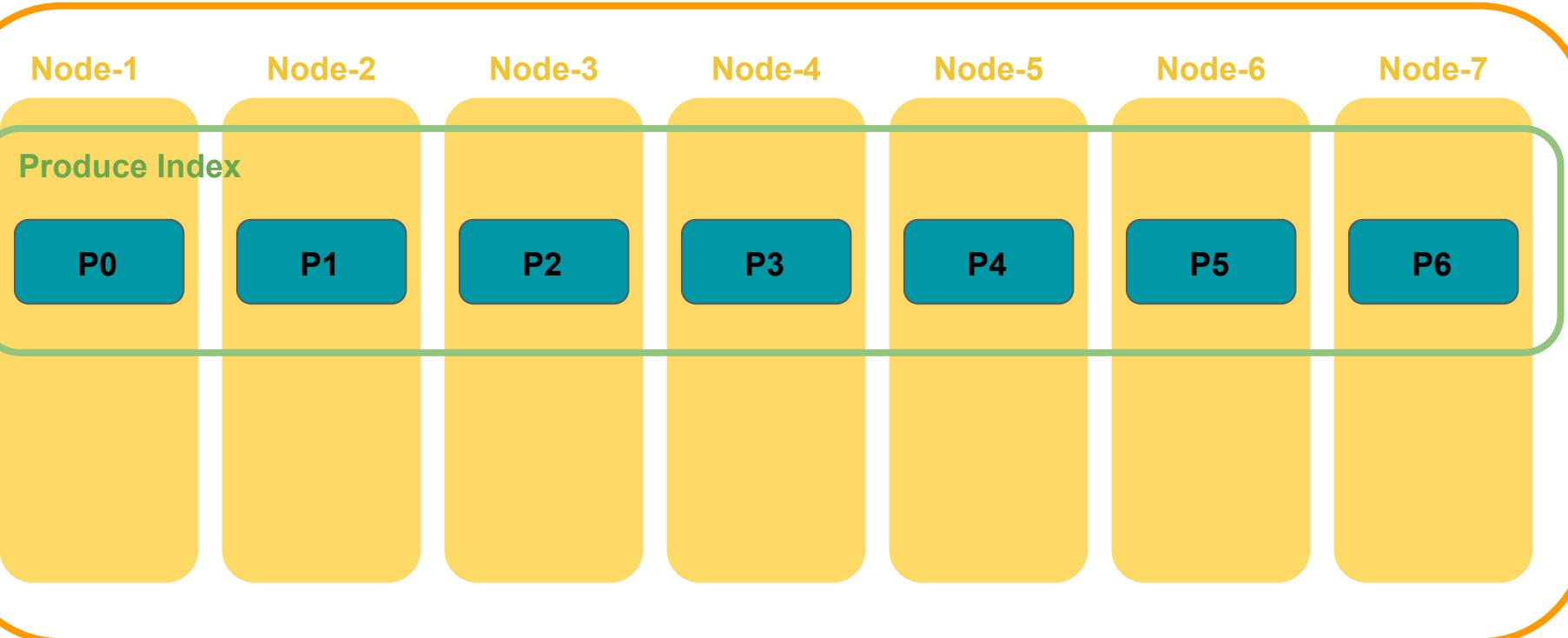
P2

P3

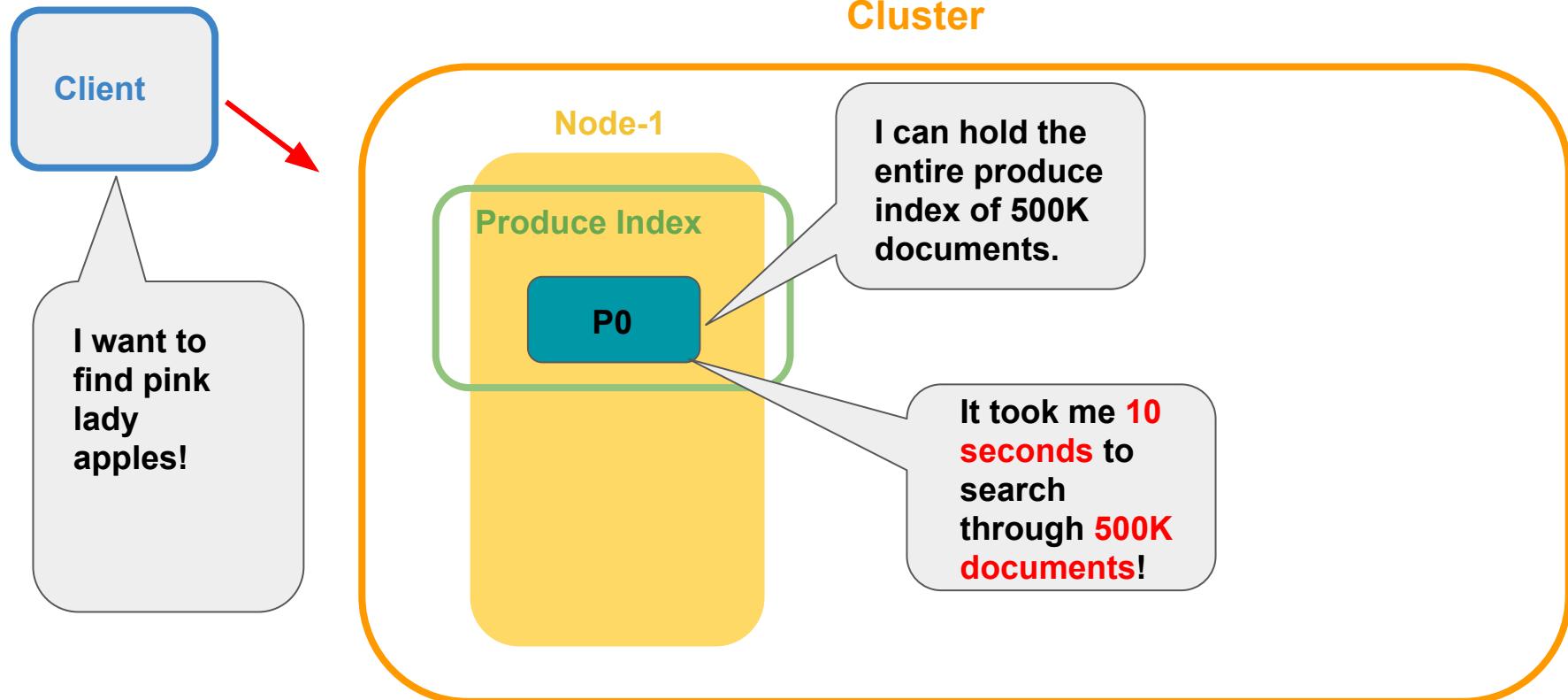
P4

P5

P6



# What is 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 keeps track of 500K produce documents

P0

50K

P1

50K

P2

50K

P3

50K

P4

50K

P5

50K

P6

50K

P7

50K

P8

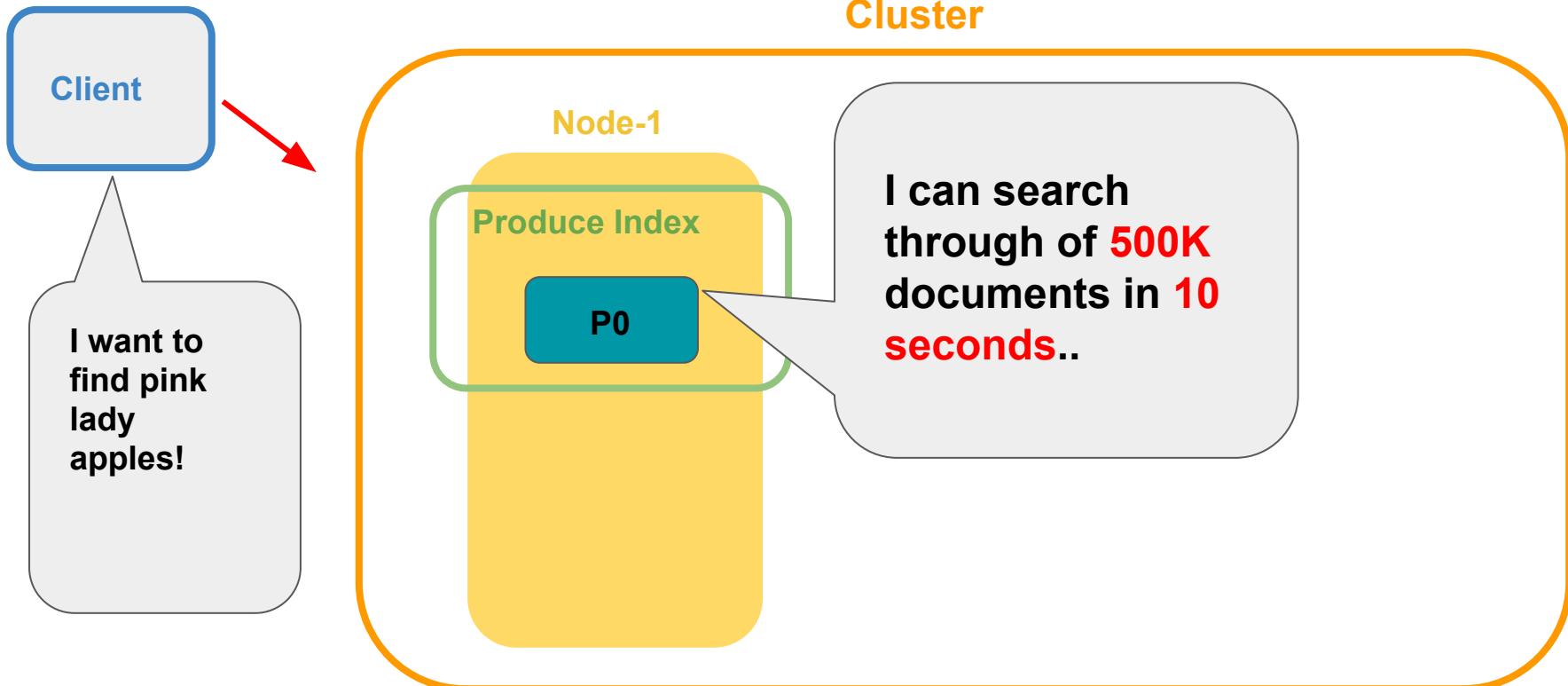
50K

P9

50K

Running a search on 50K documents takes 1 sec!

# What is 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

50K

P1

50K

P2

50K

P3

50K

P4

50K

P5

50K

P6

50K

P7

50K

P8

50K

P9

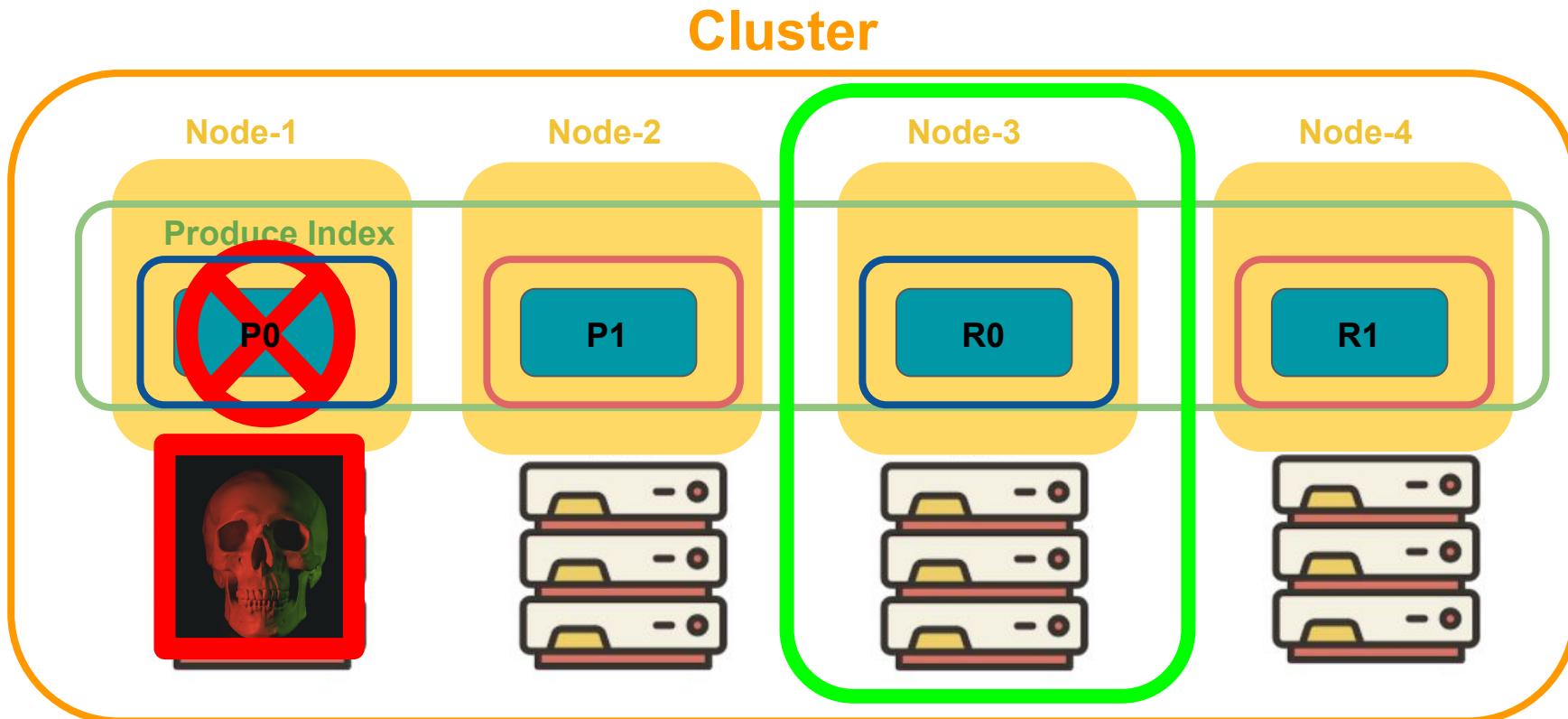
50K



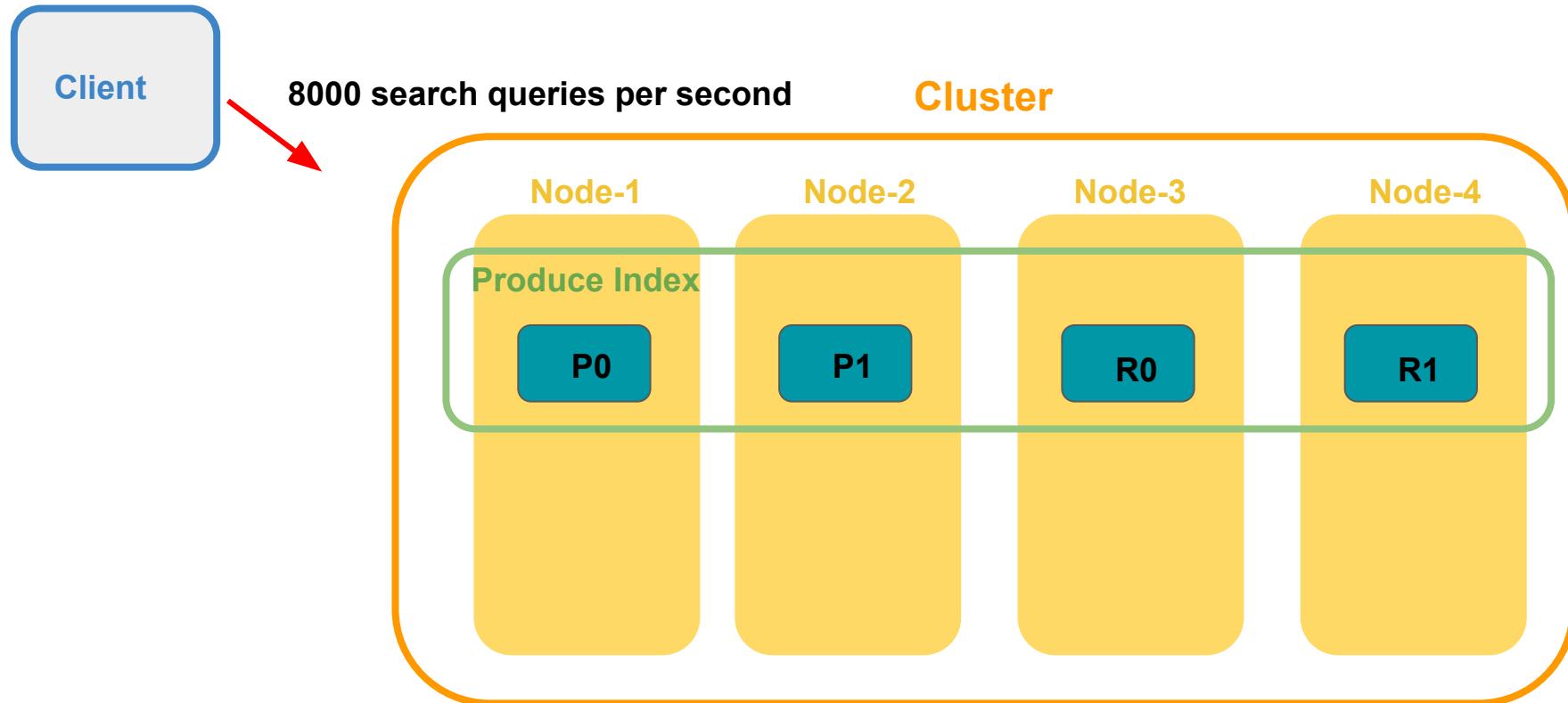
#SPONGEBOBMOVIE



# What are replica shards?



# Replica shards can improve the performance of your search



# 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

- [Free Elastic Cloud Trial](#)
  - Open Link in New Tab
  - Open Link in New Window
  - Open Link in Incognito Window
  - Save Link As...
  - Copy Link Address
  - Copy
  - Search Google for "Free Elastic Cloud Trial"
  - Print...
  - LastPass
  - Inspect
  - Speech
  - Services
- [Instructions for download](#)
- [Presentation](#)
- [Data set from Kaggle](#)

Elastic Austin User Group Want to attend live workshops? Join the Elastic Austin User Group to keep up to date on all



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

The screenshot shows two main sections. On the left, a blue header reads "ELASTICSEARCH SERVICE" with a logo. Below it, a section titled "Deploy Elasticsearch and Kibana in 3 minutes or less" contains text about a 30-day free trial and a "Start Free Trial" button. A red box highlights the "Enter your email" input field and the "Start Free Trial" button. On the right, a "First cluster" configuration interface shows "Edit Data" for "grp.data.HighIO.1" (A Kibana Instance). It includes tabs for Deployments, Logs, Snapshots, API Console, Kibana, APM, Metrics, Security, Performance, and Custom plugins. The "Fault tolerance" section shows 1 zone selected. RAM per Node is set to 8 GB. The "Architecture" section shows two zones: Zone 1 with 1 instance and Zone 2 with 1 instance, both using 1 GB RAM per zone. A "Summary" table provides cluster statistics.

## 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

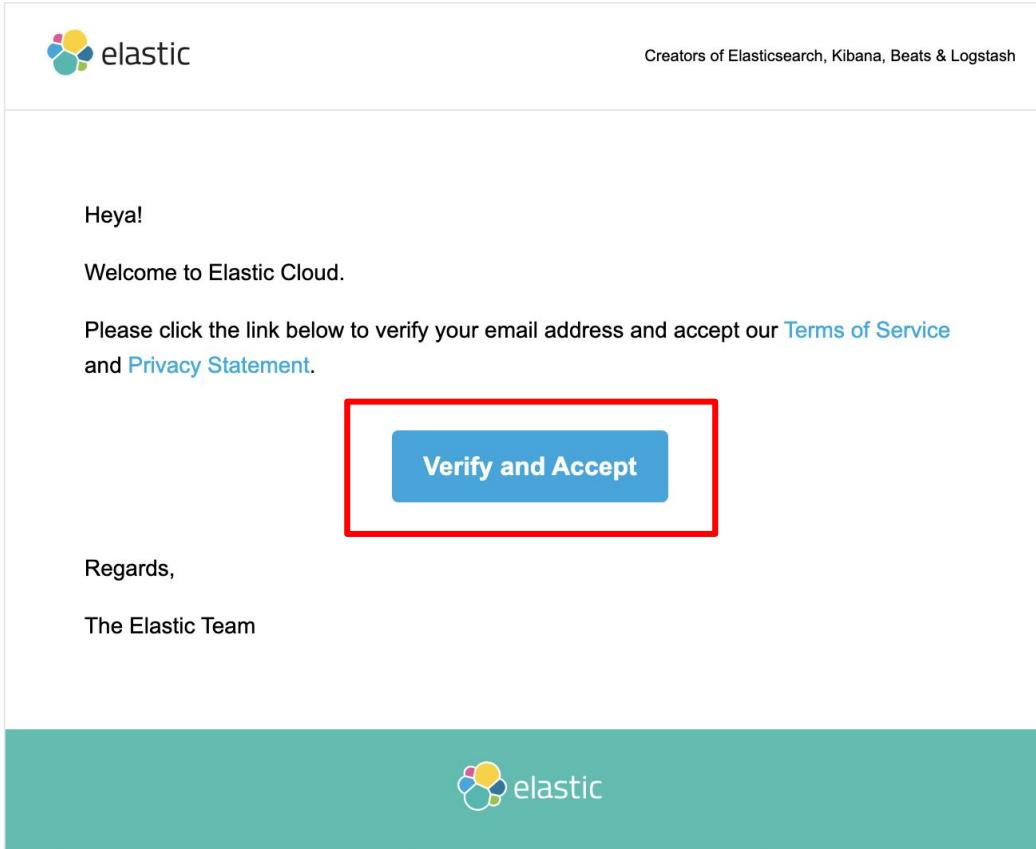
# Go to the email account you signed up with and verify your email.



Please Verify Your Email

Splendid! Head to your inbox! You should see an email verifying your account and quick-start information.

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



The image shows a screenshot of an email from the company 'elastic'. The email header includes the 'elastic' logo and the text 'Creators of Elasticsearch, Kibana, Beats & Logstash'. The body of the email starts with 'Heya!', followed by 'Welcome to Elastic Cloud.' and a message asking the recipient to click a link to verify their email address and accept the 'Terms of Service' and 'Privacy Statement'. A blue button labeled 'Verify and Accept' is centered below the message, and it is highlighted with a red rectangular box. The email concludes with 'Regards,' and 'The Elastic Team'. The footer of the email features the 'elastic' logo again.

Heya!

Welcome to Elastic Cloud.

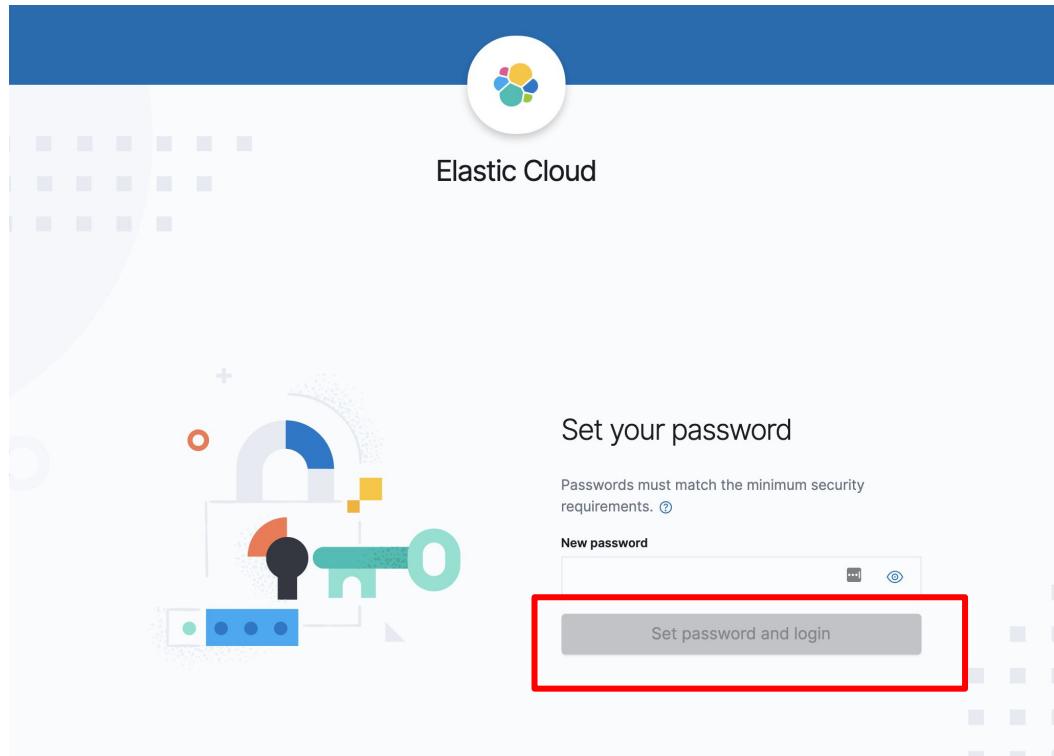
Please click the link below to verify your email address and accept our [Terms of Service](#) and [Privacy Statement](#).

**Verify and Accept**

Regards,

The Elastic Team

# Enter your password.



# Click on start your free trial.

The screenshot shows the Elastic Cloud interface for the Elasticsearch Service. At the top left is the Elastic logo. Below it, a navigation bar includes 'Cloud' and other service icons. The main content area features a large 'Elasticsearch Service' section with a circular icon and a cluster diagram. Below this is a heading 'Get started with Elasticsearch Service'. A paragraph describes creating a deployment on the cloud platform of choice, mentioning Kibana, machine learning, or APM. A prominent blue button labeled 'Start your free trial' is centered, with a red rectangular box highlighting it. To the right, there's a 'News' sidebar with recent announcements and a 'Training' sidebar with a 'Get certified!' section and a link to the Elastic Learning Portal.

Elastic

Cloud

Elasticsearch Service

Get started with Elasticsearch Service

Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.

Start your free trial

Platform features

- ✓ Cloud hosting on AWS, GCP or Azure
- ✓ Logs, metrics, and APM in one place
- ✓ Includes machine learning, security, and more
- ✓ One-click upgrades with no downtime
- ✓ Same-day new version releases
- ✓ Monitored 24/7

News

Elastic Cloud Terraform provider now available in beta

DECEMBER 17, 2020 New!

Elastic Stack 7.10.1 released

DECEMBER 9, 2020 New!

Elastic Cloud is now available on Amazon Web Services in Asia Pacific (Hong Kong)

DECEMBER 8, 2020 New!

Training

Get certified!

Challenge yourself and your Elasticsearch expertise by taking the performance-based certification exam.

Elastic Learning Portal

Explore the training catalog

# Select the Elastic Stack.

The screenshot shows the Elasticsearch Service interface for creating a deployment. The left sidebar includes links for Deployments, Create deployment, Extensions, API keys, Traffic filters, and Help. The main content area features a welcome message for a 30-day free trial and a section asking what you want to do with your data. Four service options are listed:

- Elastic Stack**: Deploy Elasticsearch and Kibana. Search, analyze, and visualize data from any source, in any format. **Select** button highlighted with a red box.
- Elastic Enterprise Search**: Easily implement powerful search experiences for your website, app, or workplace with refined APIs and tools. **Select** button.
- Elastic Observability**: Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs. **Select** button.
- Elastic Security**: Prevent, collect, detect, and respond to threats for unified protection across your infrastructure. **Select** button.

# Configure your settings.

**Select hardware profile**

**I/O Optimized** Recommended

Use for all-purpose workloads, including time-series data like logs and metrics. [See details](#)

**Compute Optimized**

Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage. [See details](#)

**Memory Optimized**

Perform memory-intensive operations efficiently, including workloads with frequent aggregations. [See details](#)

**Hot-Warm Architecture**

Useful for time-series analytics that benefit from automatic index curation. [See details](#)

**Cross Cluster Search** Not available in trial

Search data across one or more associated remote deployments. [See details](#)

---

**Deployment settings**

Choose the cloud provider, region, and Elastic Stack version.

**Cloud provider**

Pick a cloud and let us handle the rest. No additional accounts required.

 Google Cloud     Azure     Amazon Web Services

Collapse ▾

**Region**

Select the location of your deployment.

 West US 2 (Washington)

**Version**

Choose the Elastic Stack version.

7.10.1

# Name your deployment then create deployment.

## Region

Select the location of your deployment.

 West US 2 (Washington)

## Version

Choose the Elastic Stack version.

7.10.1

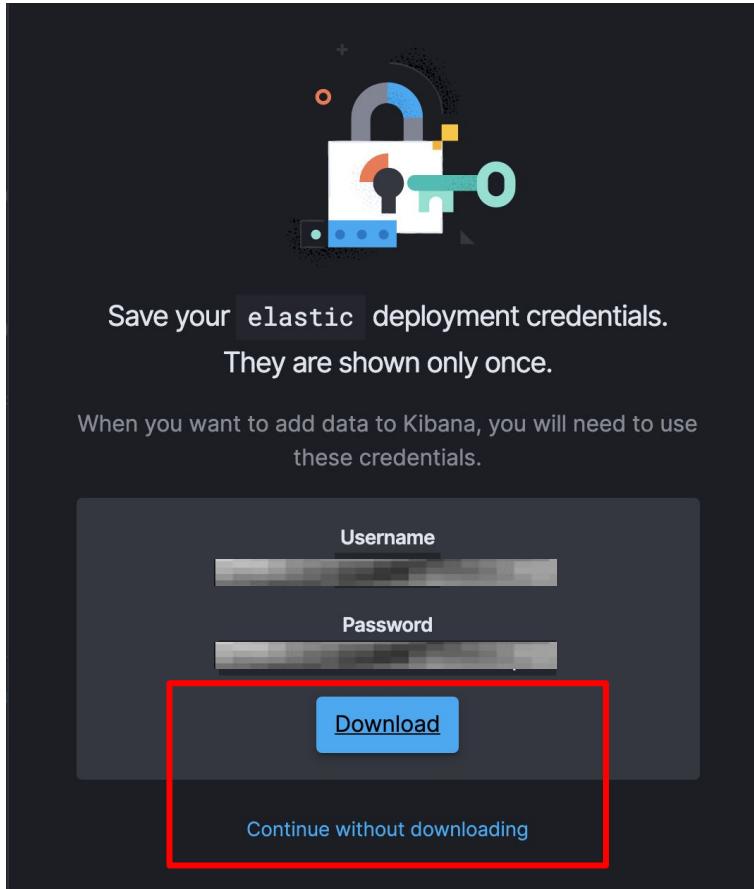
### Name your deployment

You can always change this later.

Beginner's Crash Course

 Create deployment

# Save your deployment credentials.



# 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.

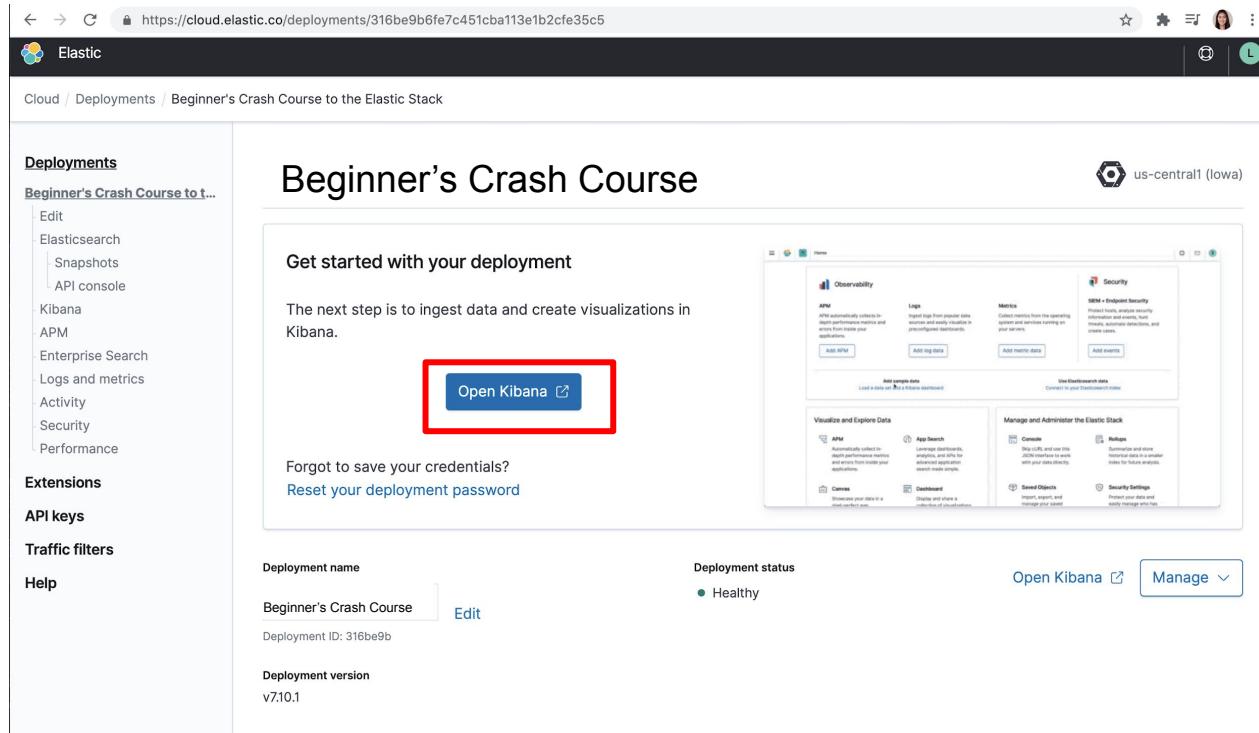
**Open Kibana**

Forgot to save your credentials?  
[Reset your deployment password](#)

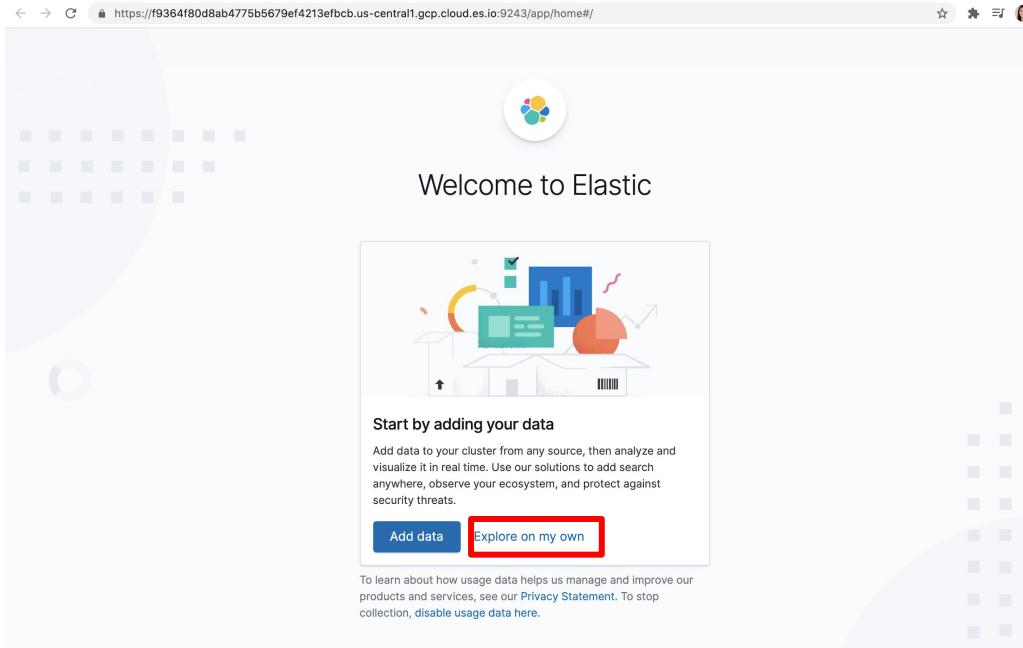
**Deployment name**  
Beginner's Crash Course [Edit](#)  
Deployment ID: 316be9b6fe7c451cba113e1b2cfe35c5

**Deployment status**  
● Healthy

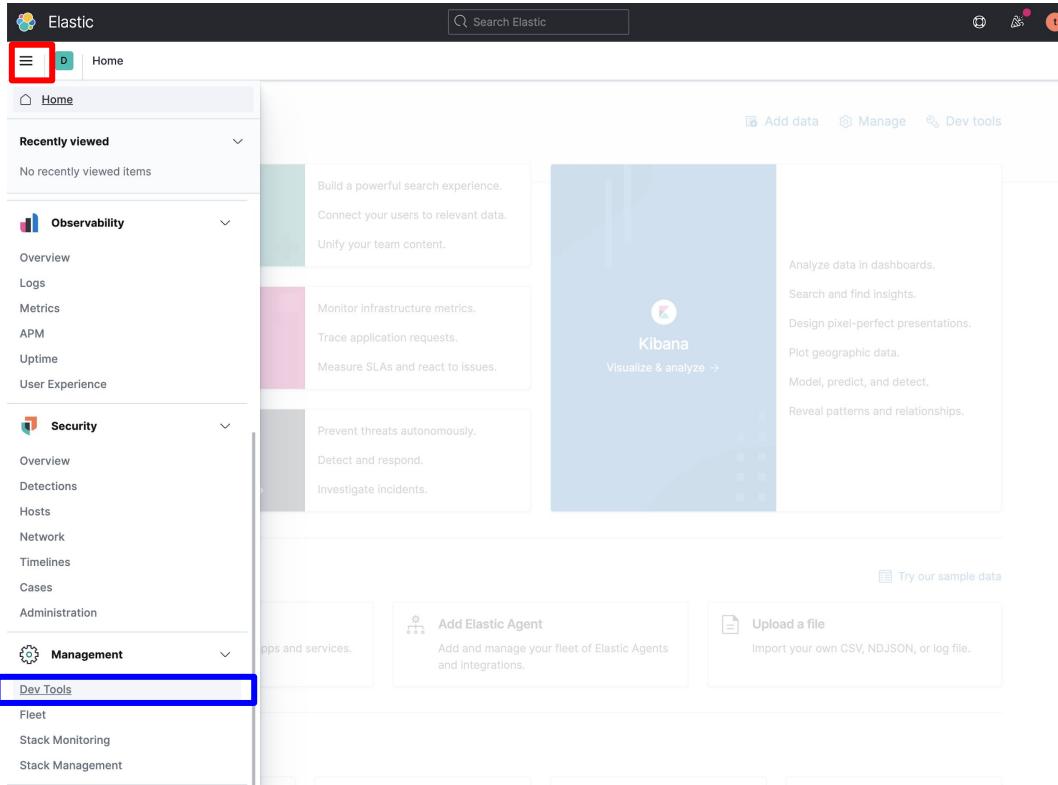
**Open Kibana** [Manage](#)



# Click on Explore on my own option.



# Click on menu icon, and open Dev Tools.



# Click on dismiss and delete the default query.

The screenshot shows the Elasticsearch Dev Tools interface. On the left, there's a navigation bar with 'Console' selected, along with 'Search Profiler', 'Grok Debugger', and 'Painless Lab'. Below the navigation is a toolbar with 'History', 'Settings', and 'Help'. A search bar at the top right contains the placeholder 'Search Elastic'. The main area is split into two panes: an editor pane on the left and a response pane on the right. In the editor pane, a 'GET \_search' request is typed, starting with '{ "query": { "match\_all": {} } }'. This entire line is highlighted with a blue rectangular box. To the right of the editor is a 'Welcome to Console' modal window. The modal has a close button 'x' at the top right. Inside, there's a 'Quick intro to the UI' section with text explaining the split-pane layout and cURL support, followed by a code example. At the bottom of the modal is a 'Dismiss' button, which is also highlighted with a red rectangular box.

Dev Tools

Console Search Profiler Grok Debugger Painless Lab BETA

History Settings Help

GET \_search

```
{ "query": { "match_all": {} } }
```

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:

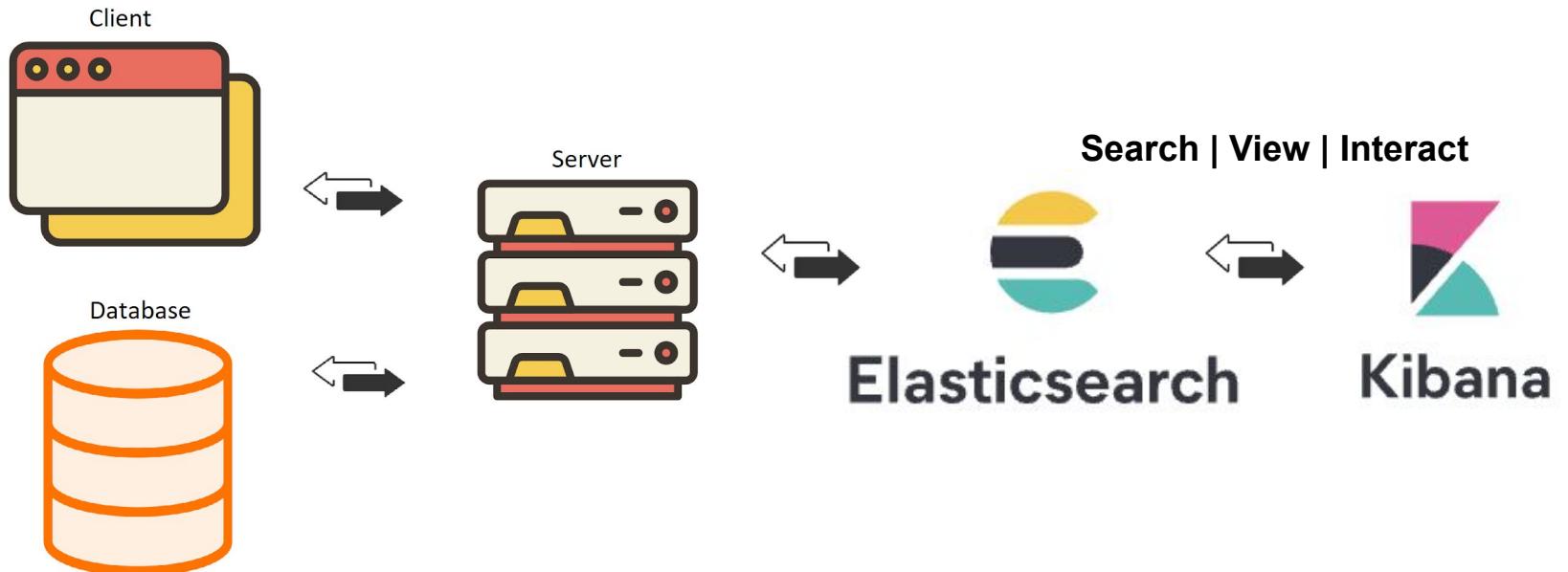
```
1 # index a doc
2 PUT index/_doc/1
3 {
4   "body": "here"
5 }
6
7 # and get it ...
8 GET index/_doc/1
```

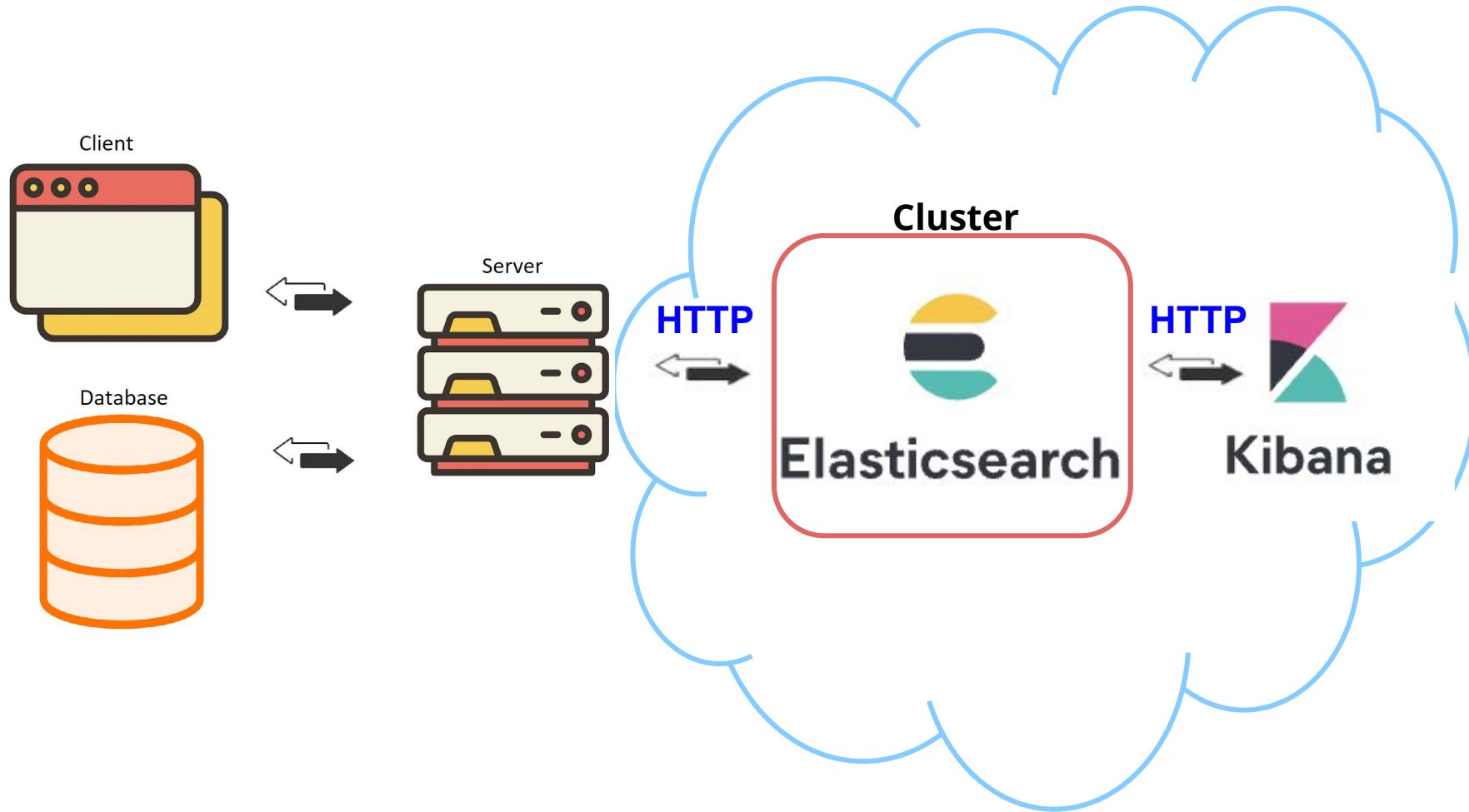
While typing a request, Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure as well as your indices and types.

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?



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



A teal-colored event banner for a beginner's course. At the top left is a white plus sign icon. To its right, the text "Beginner's Course - Part 2/2" is displayed in large white font. Below this, the title "Understanding the relevance of your search with Elasticsearch & Kibana" is written in a large, bold, white sans-serif font. In the bottom left corner, the word "Vancouver" is written in white. Below it, the date and time "Thu, Feb 4, 4:00 PM (PST)" are shown in white. At the bottom left, there is a blue button with the white text "Get Tickets". To the left of the button are five social media sharing icons: Facebook, Twitter, LinkedIn, Pinterest, and Email. The bottom right corner features a small graphic of three teal bars of increasing height.

+Beginner's Course - Part 2/2

Understanding the relevance of your search with Elasticsearch & Kibana

Vancouver

Thu, Feb 4, 4:00 PM (PST)

f t in p e

Get Tickets



# Lisa Jung

Developer Advocate @Elastic

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

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

Twitter: @LisaHJung