

Beginner's Crash Course to Elastic Stack

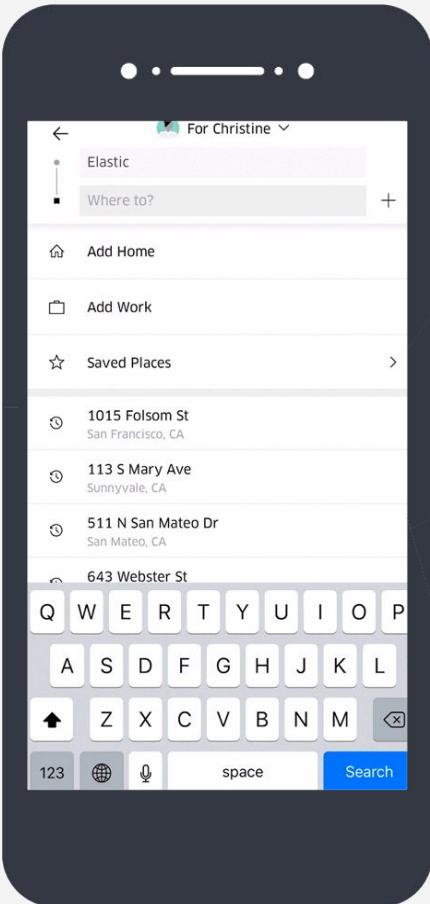
Part 1.1: Intro to Elasticsearch and Kibana

Lisa Jung
Developer Advocate @Elastic

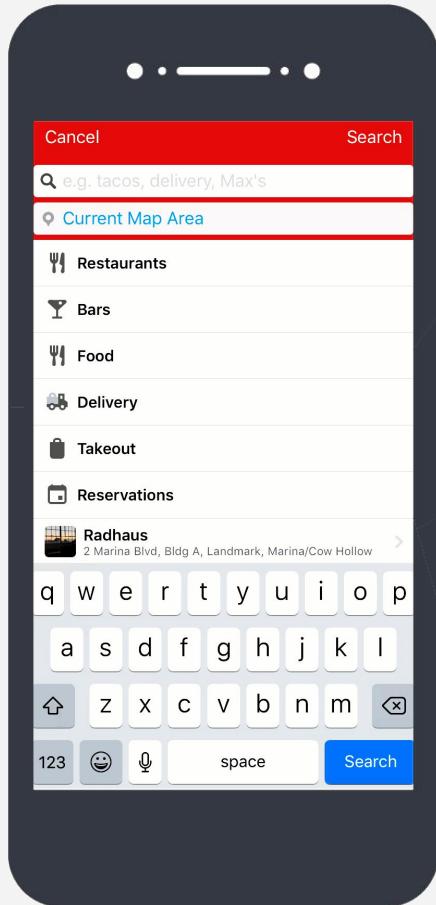


Have you ever used the Elastic Stack before?

- **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

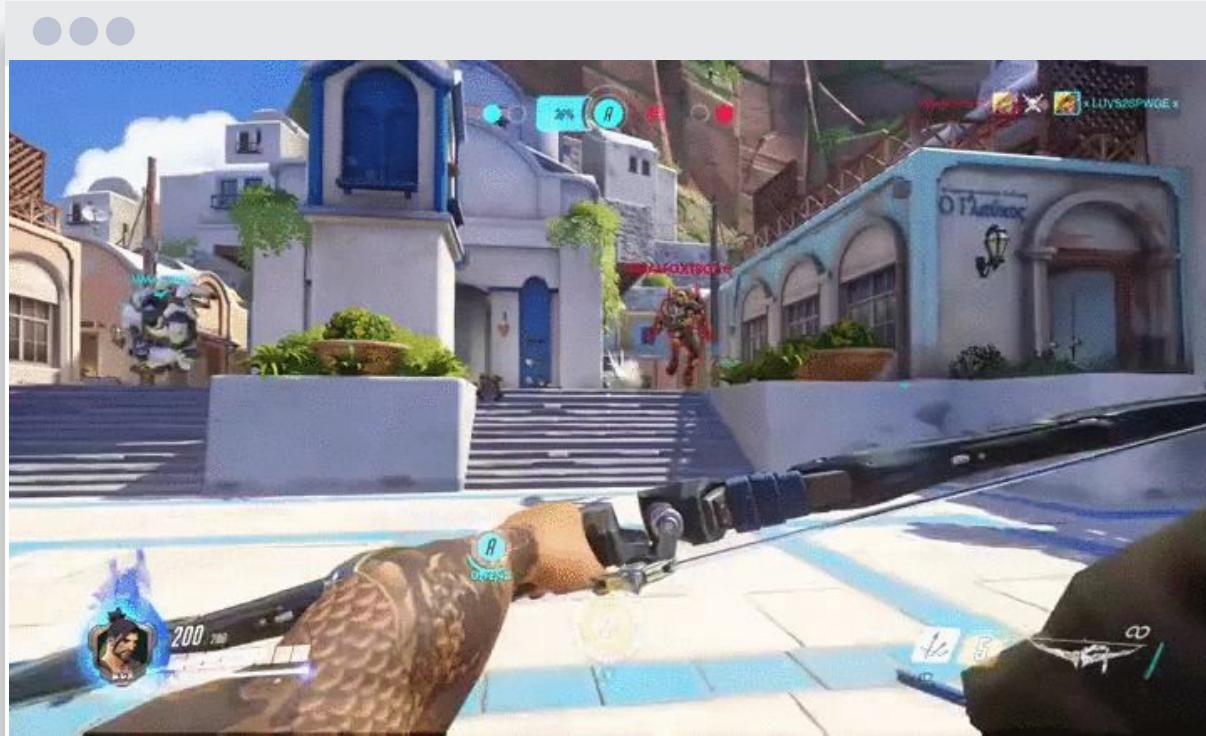
Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



Use Cases

- Logging
- Metrics
- Security Analytics
- Business Analytics

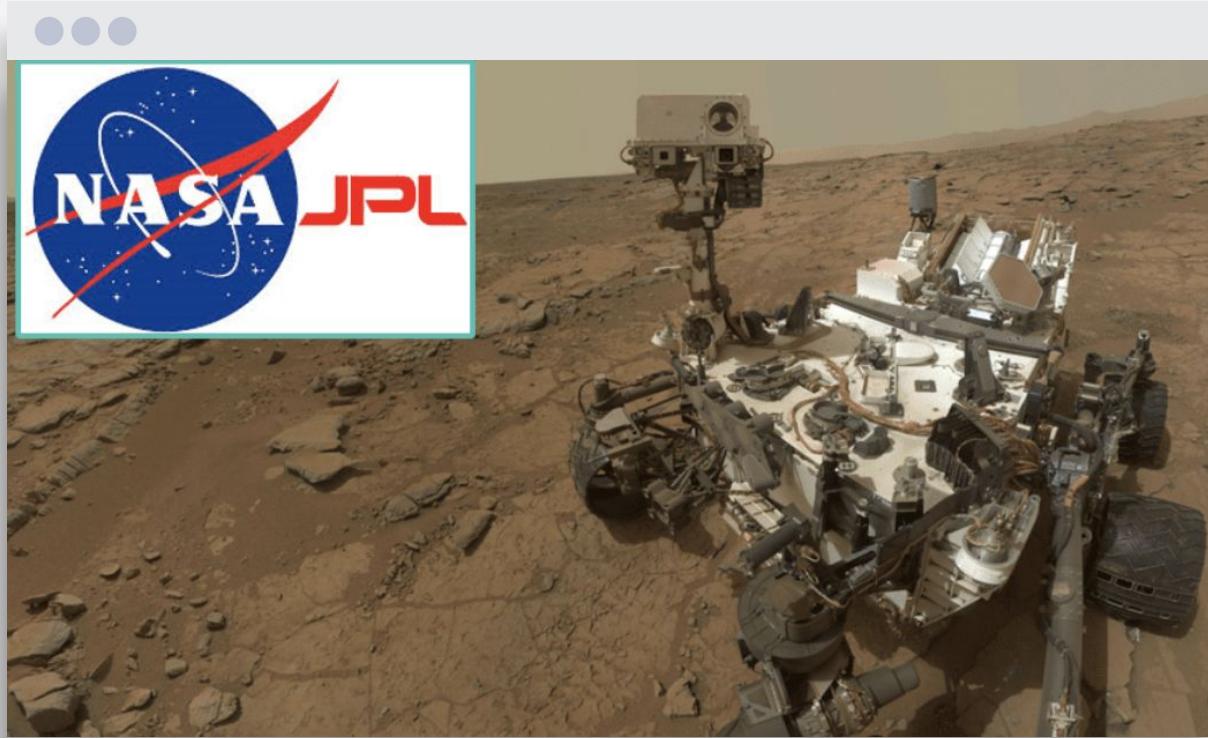
Use Case: Logging



ACTIVISION
BLIZZARD

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

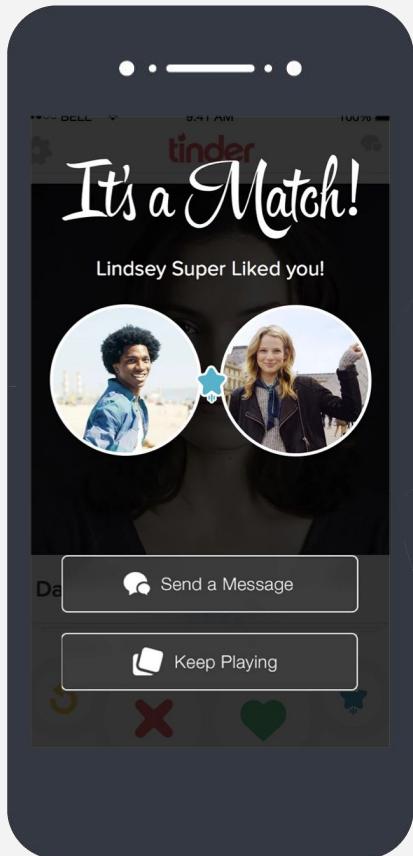
Use Case: Metrics



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 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

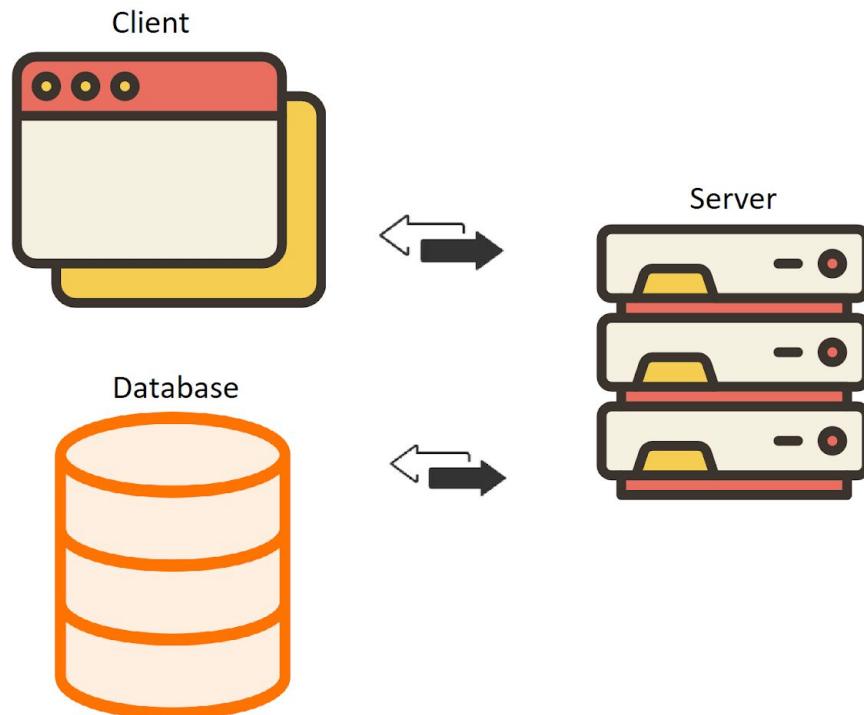
Elasticsearch

Store | Search | Analyze





A screenshot of the Instacart website interface. At the top, there's a navigation bar with icons for search, home, delivery location (Delivery in 94086), account, help, and a cart containing 4 items. The main header features the Safeway logo over a background image of fresh produce like avocados and kale. A search bar is centered, with the word "can" typed into it. Below the search bar is a dropdown menu listing categories under "Canned Goods": Department, Canned Fruit & Applesauce (Aisle), Canned & Jarred Vegetables (Aisle), and Canned Meals & Beans (Aisle). On the left side, there's a "Coupon saving" section with a "Shop Coupons" button. On 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.



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

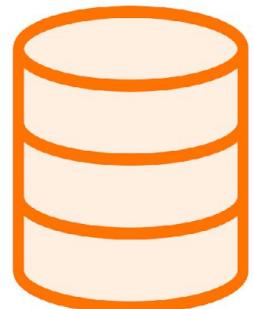
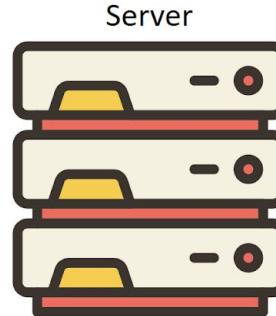
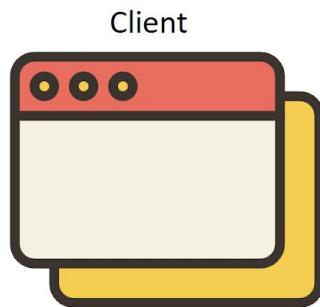
Based on your cart View more

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?



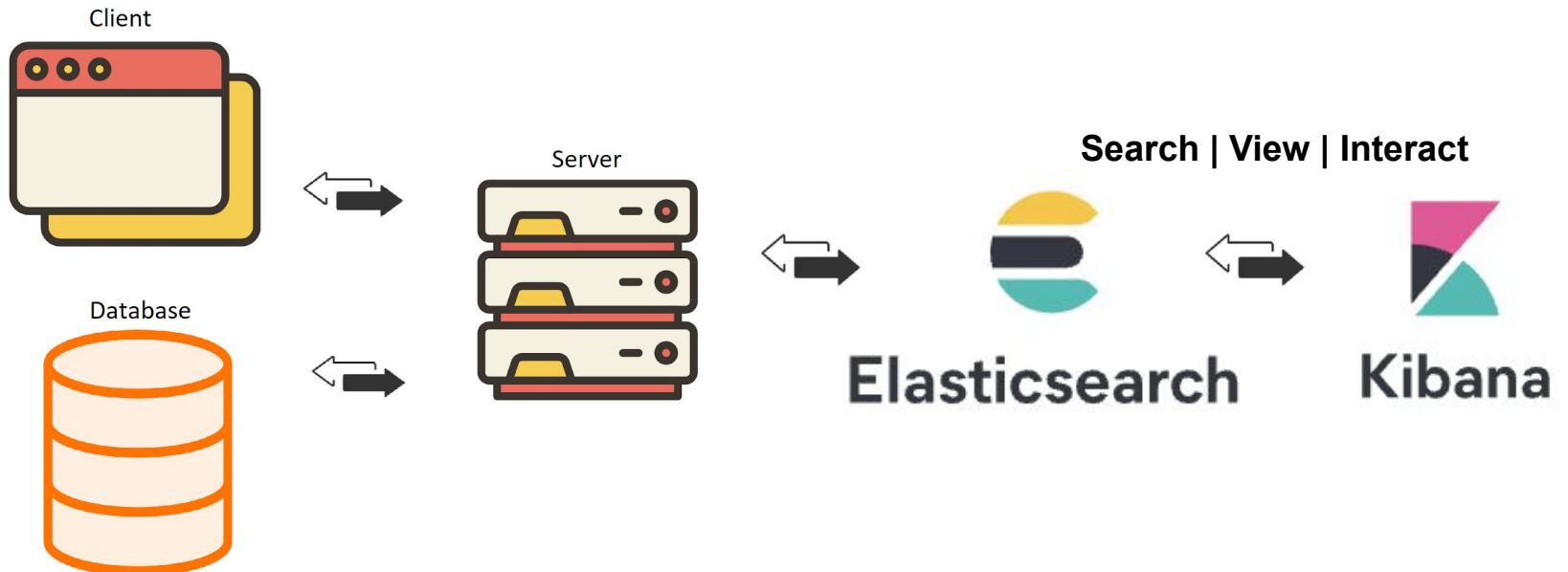


Elasticsearch

Elasticsearch

Store | Search | Analyze

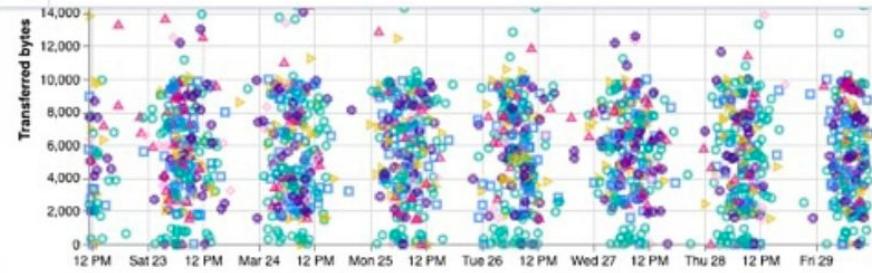






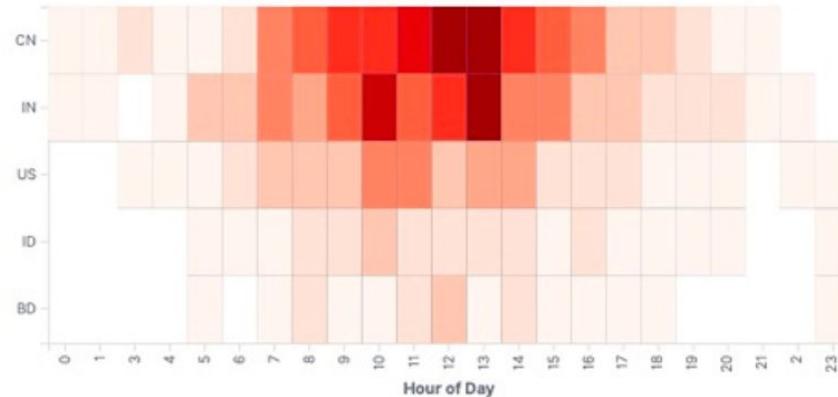
D

- Clock icon
- Gauge icon
- House icon
- Cloud icon
- Bar chart icon
- User icon



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	↓

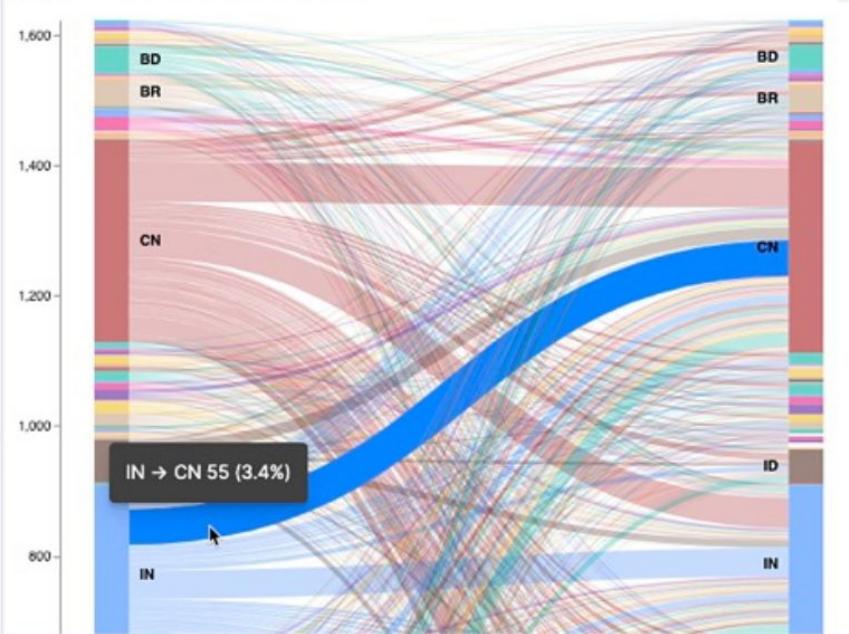
[Logs] Heatmap



[Logs] Unique Visitors by Country



[Vega] Source and Destination Sankey Chart



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

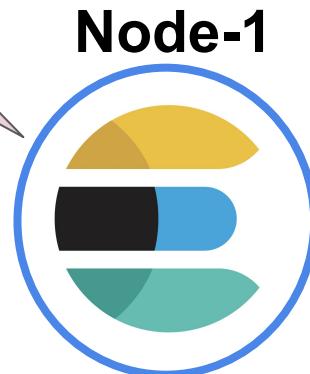
Elasticsearch

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



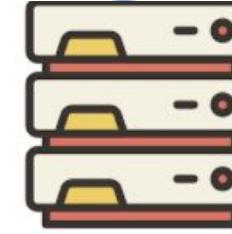
Node-2



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!

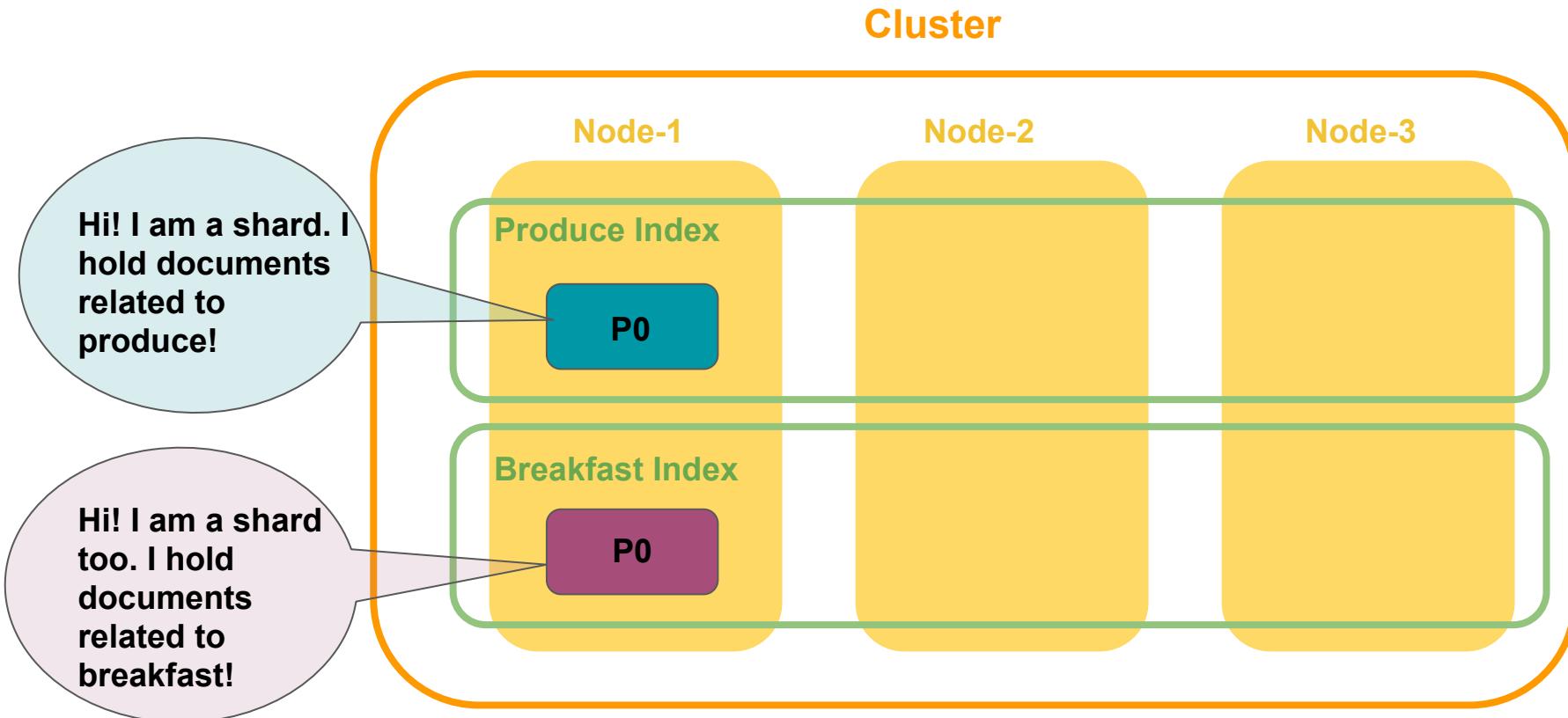
Produce Index

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

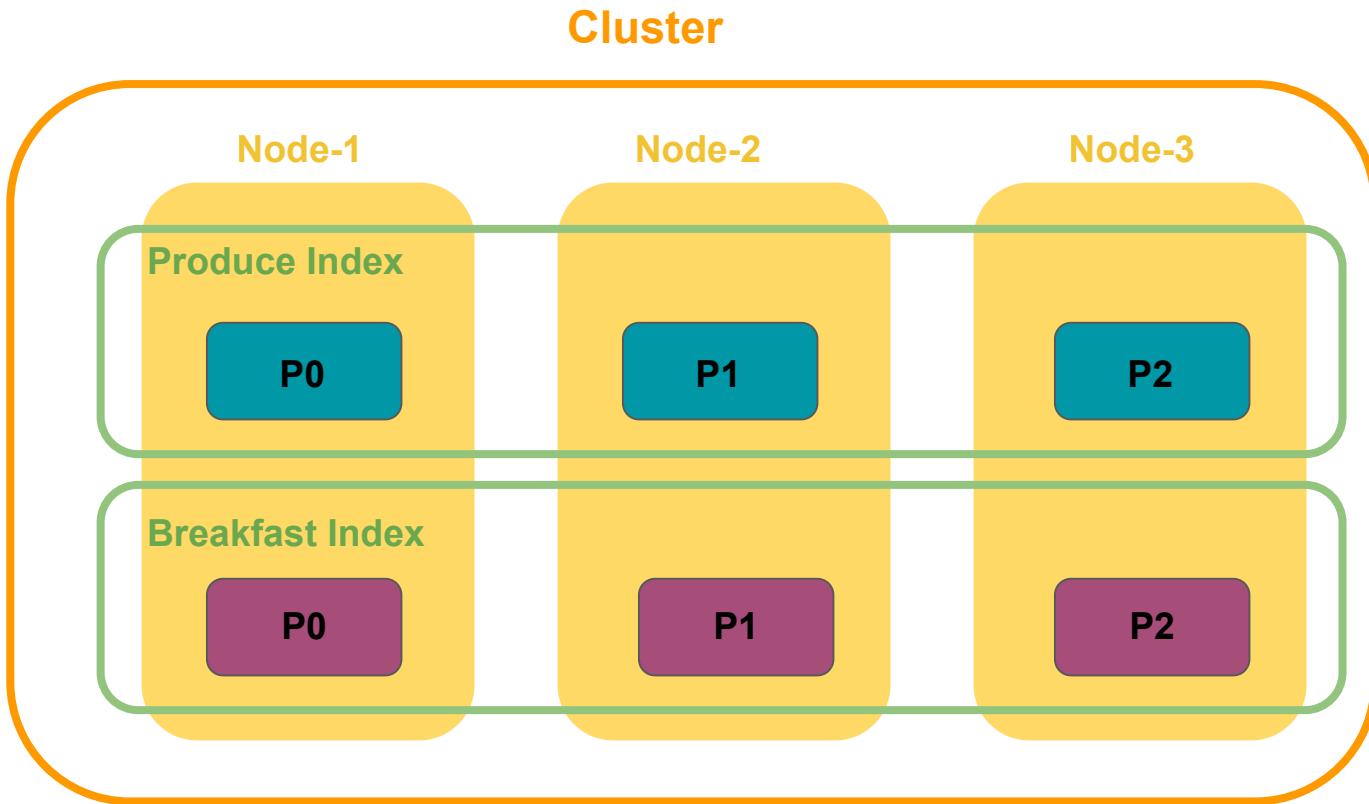
Breakfast Index

```
{  
  "name": "Instant Oatmeal Brown Sugar",  
  "category": "Breakfast",  
  "brand": "Quaker",  
  "price": "$3.59"  
}  
  
{  
  "name": "Pop-Tarts Brown Sugar Cinnamon",  
  "category": "Breakfast",  
  "brand": "Kellogg's",  
  "price": "$2.99"  
}
```

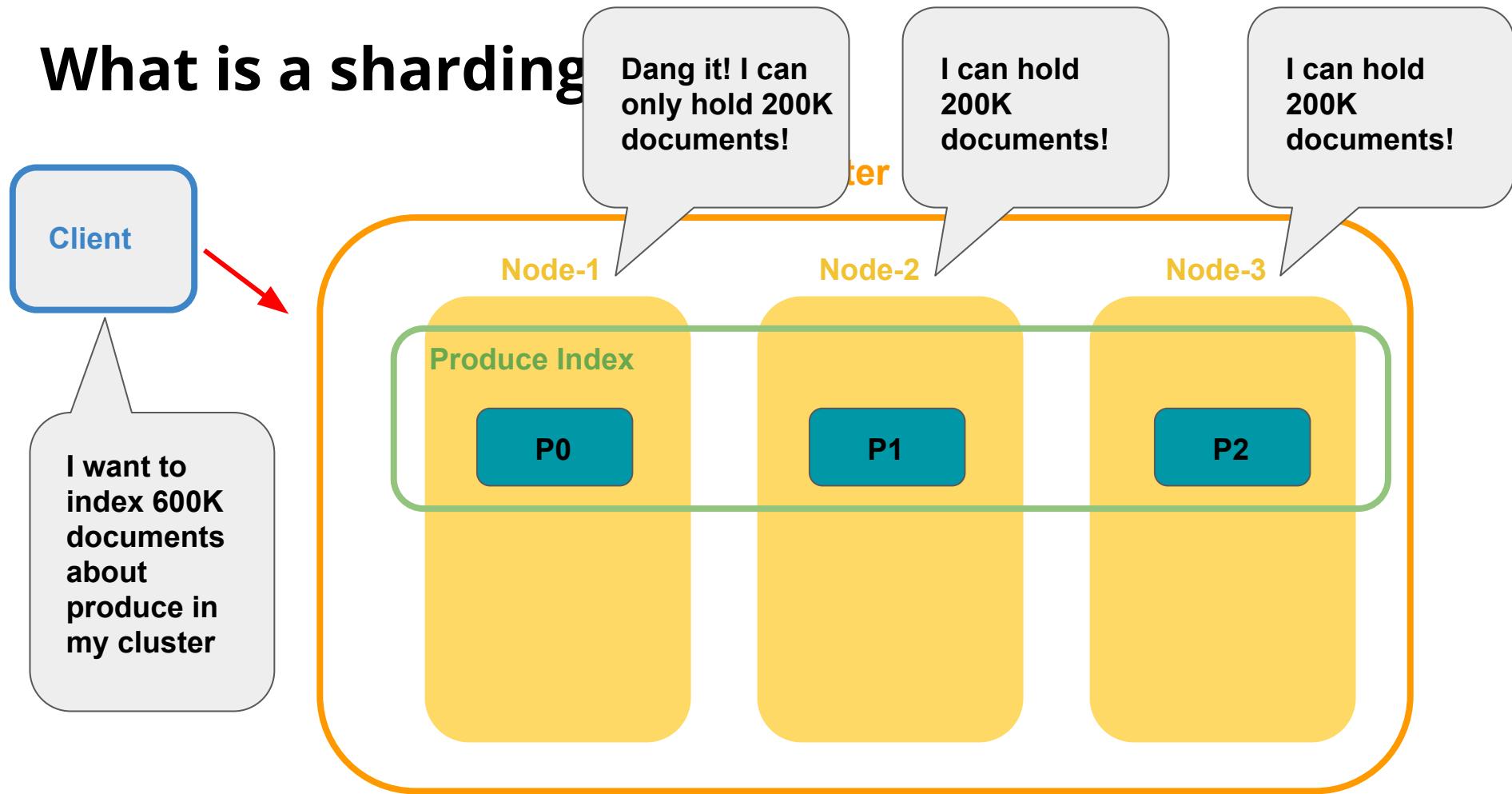
What is a shard?



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

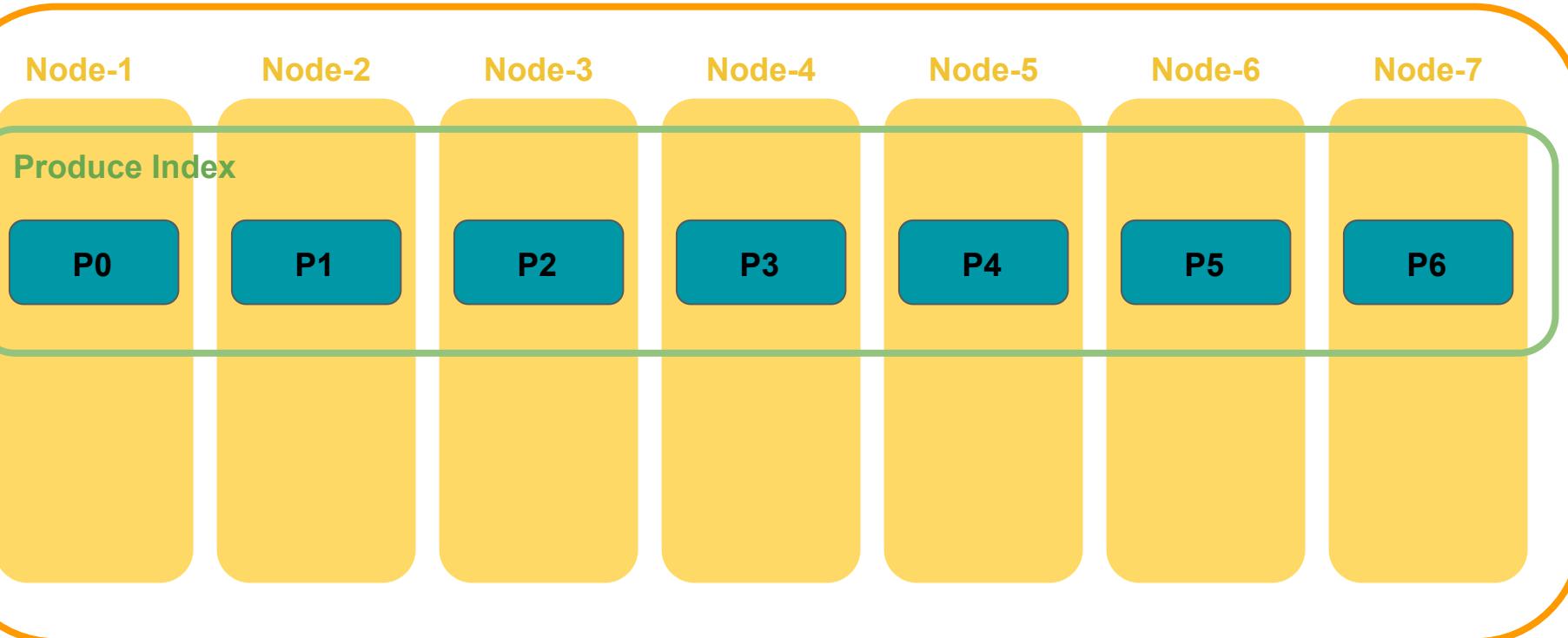
P2

P3

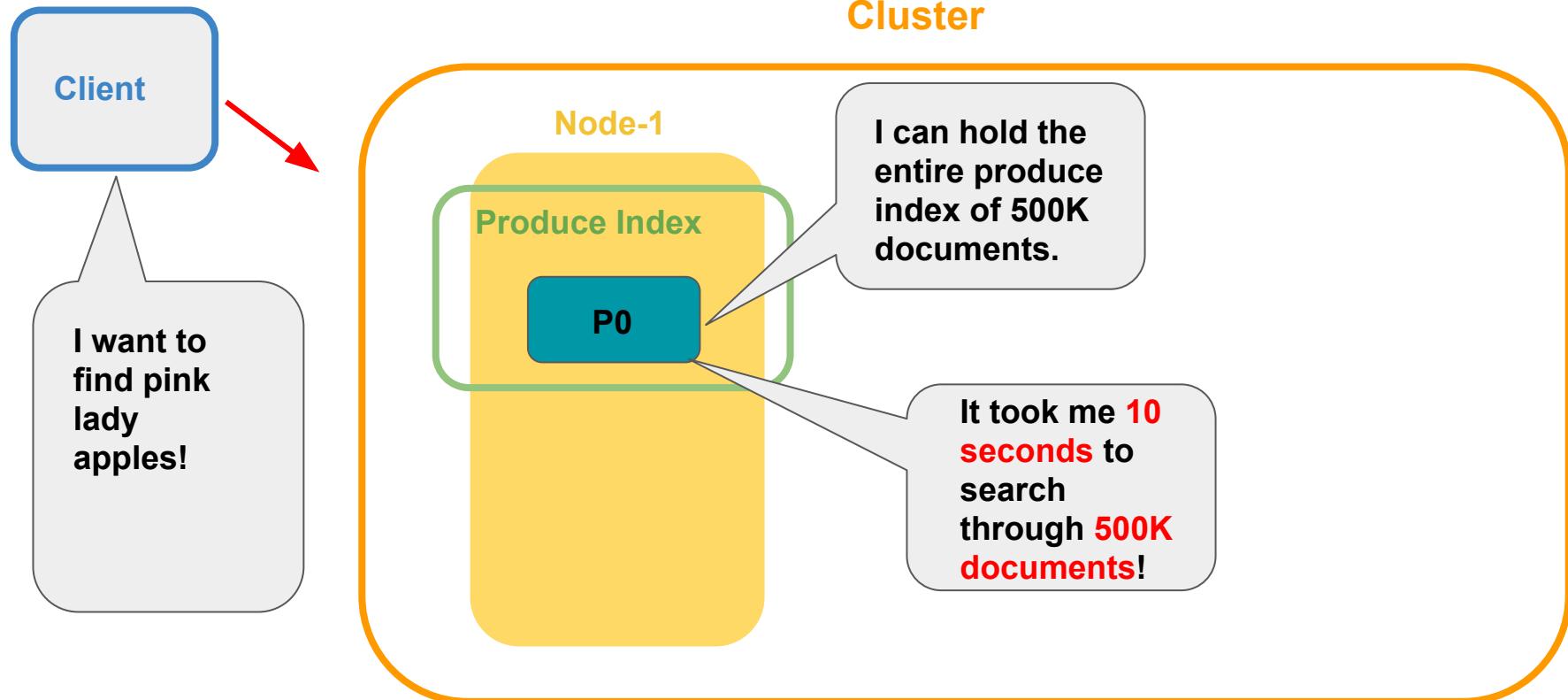
P4

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

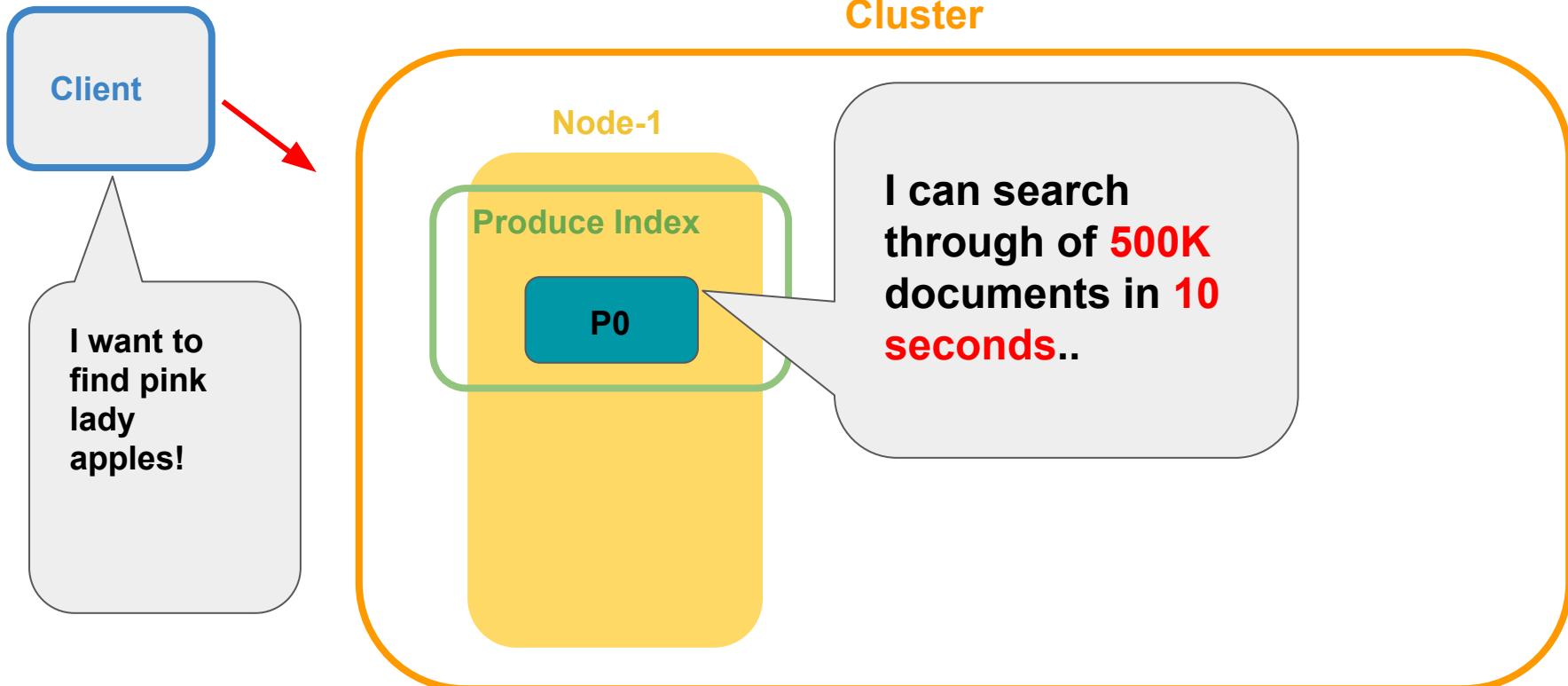
50K

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

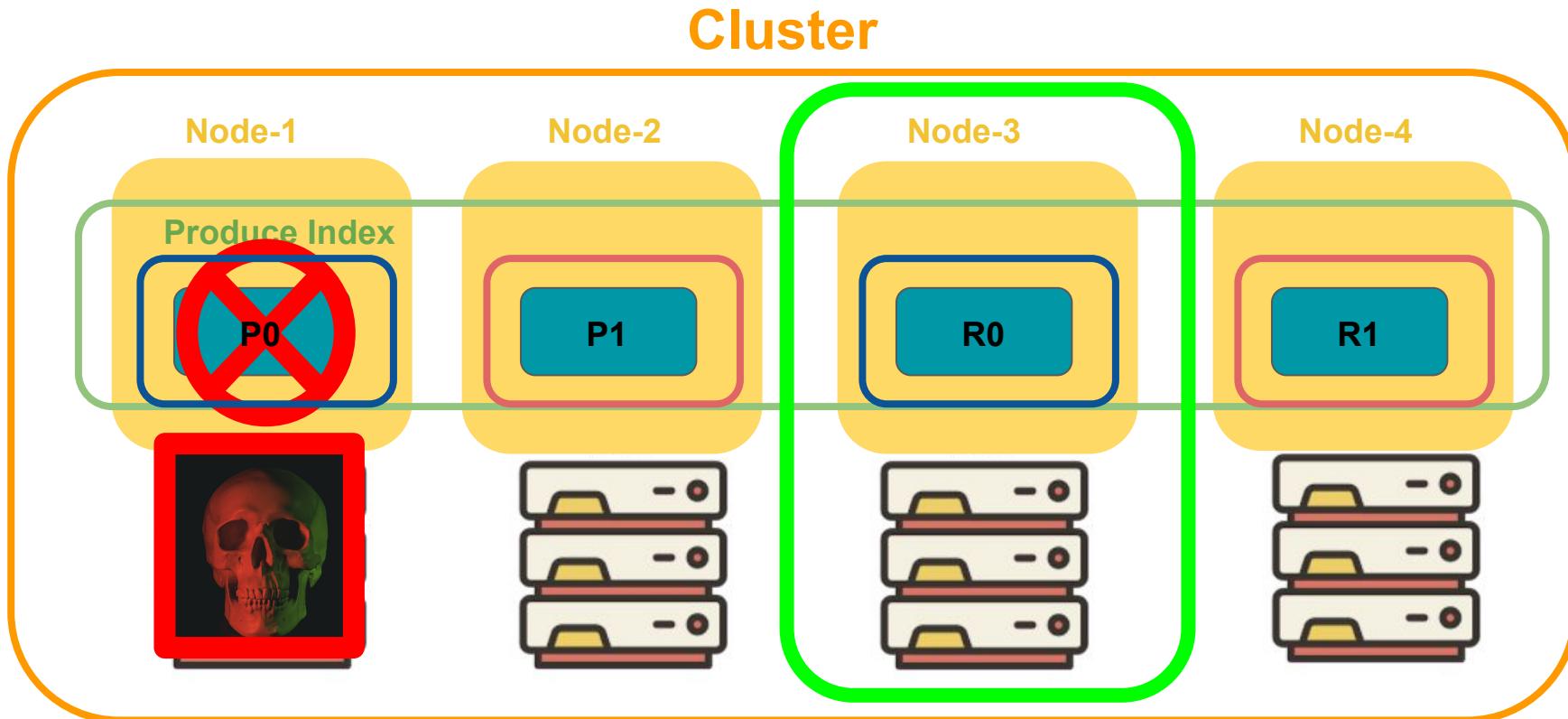
50K



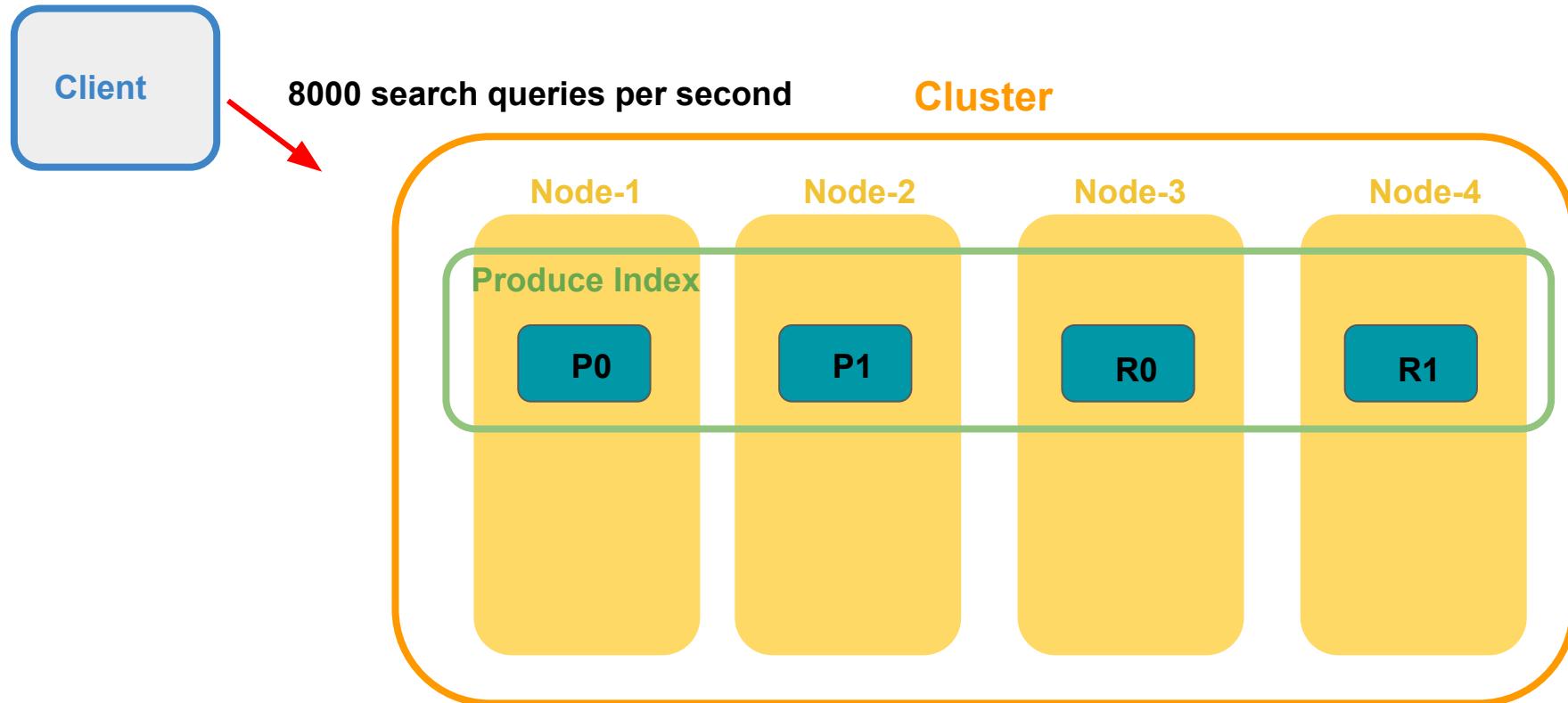
#SPONGEBOBMOVIE



What are replica shards?



Replica shards can improve the performance of your search



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



Click on the link to the workshop repo.

<https://ela.st/orionhacks-elastic>

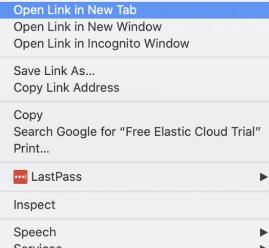
Scroll down to the Resources section & open Free Elastic Cloud Trial link in a new tab.

OrionHacks Workshop: Intro to Elasticsearch and Kibana

This repo contains all resources shared during the Intro to Elasticsearch and Kibana workshop at OrionHacks(1/16/2021).

Resources

[Free Elastic Cloud Trial](#)



[Presentation](#)

[Blog Beginner's guide](#)

[Elastic Austin User Group](#)
all future events!

Getting information about cluster and nodes

Syntax:

```
GET _API/parameter
```

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

ELASTICSEARCH SERVICE

Deploy Elasticsearch and Kibana in 3 minutes or less

As part of a special arrangement, attendees get access to a longer trial period (30 vs. 14 days) of the Elasticsearch Service on Elastic Cloud.

- 30-day free trial. No credit card required.
- Get the latest versions, powerful features such as machine learning and alerting, and optimized deployment templates for your logging use case.
- Requires use of corporate email address.

Enter your email Start Free Trial

By submitting you agree to the Elastic Cloud Standard Terms of Service and to receive occasional emails from elastic. Your personal data will be processed in accordance with elastic's privacy statement.

Summary

First cluster Edit

Data

grp.data.HighIO.1 A Kibana Instance

Fault tolerance

1 zone 2 zones 3 zones

RAM per Node 1GB 2GB 4GB 8GB 16GB 32GB 64GB

Architecture

Zone 1

grp-data-1@HighIO grp-data-2@HighIO

Zone 2

grp-data-3@HighIO grp-data-4@HighIO

Instances 1 RAM per Zone 1 GB

Summary 1 RAM 1 instance 1 zone 1024 RAM

User settings overrides

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



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

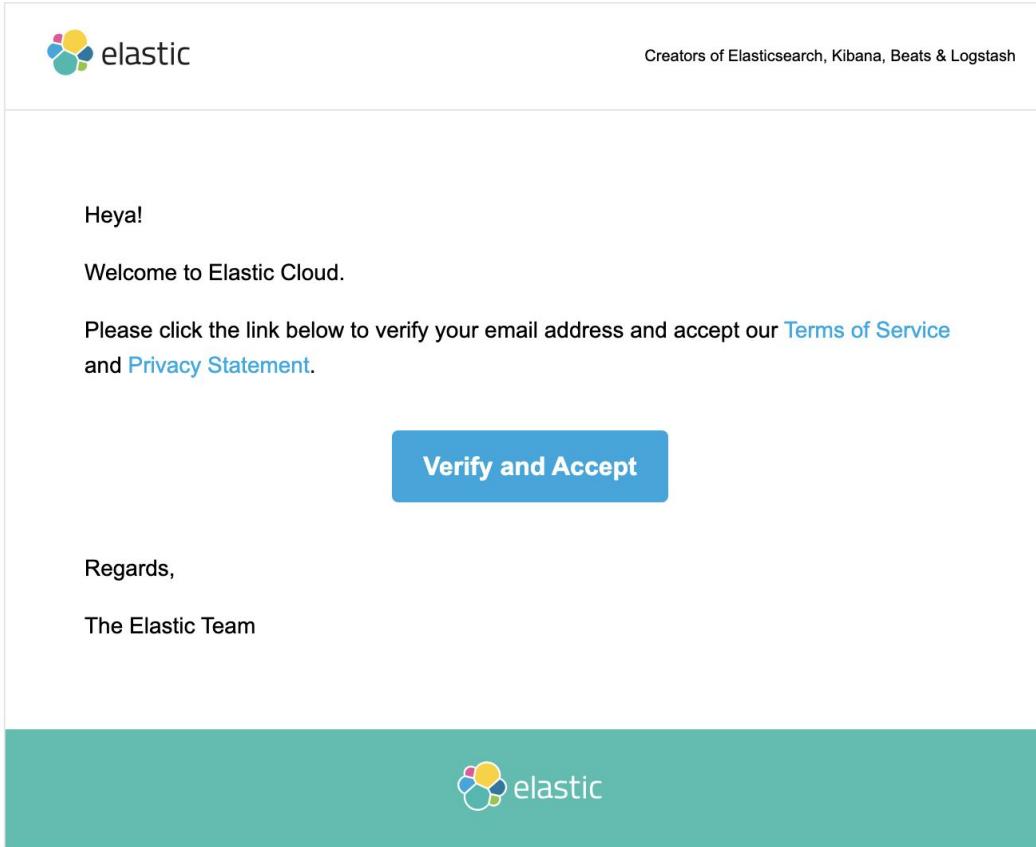
Go to the email account you signed up with and verify your email.



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 Elastic Cloud. The header features 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 prominent blue button labeled "Verify and Accept" is centered below this text. The footer contains the text "Regards," and "The Elastic Team". The entire email is set against a white background with a teal footer bar containing the Elastic logo.

Heya!

Welcome to Elastic Cloud.

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

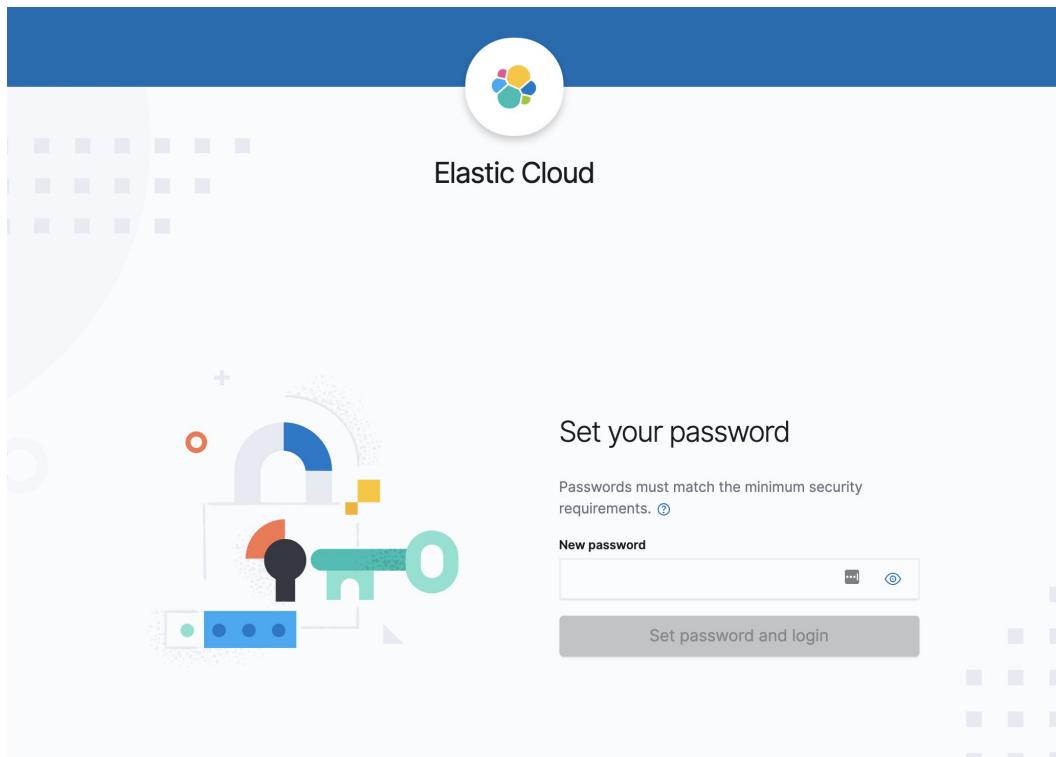
Verify and Accept

Regards,

The Elastic Team



Enter your password.



Click on start your free trial.

The screenshot shows the Elastic Cloud interface. At the top, there's a navigation bar with the Elastic logo and a search bar. Below it, a "Cloud" section header is visible. The main content area features a "Elasticsearch Service" card with a circular icon, a decorative graphic of interconnected nodes, and the text "Get started with Elasticsearch Service". It encourages users to create their first deployment on AWS, GCP, or Azure and adds additional products like Kibana, machine learning, or APM. A prominent blue button labeled "Start your free trial" is highlighted with a red box. Below this, a "Platform features" section lists several benefits with checkmarks. To the right, there are two more cards: one for "News" (listing recent releases) and one for "Training" (offering a certification exam). At the bottom, links lead to the "Elastic Learning Portal" and the "Explore the training catalog".

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.

Elastic

Cloud / Deployments / Create

[Deployments](#)
[Create deployment](#)

[Extensions](#)
[API keys](#)
[Traffic filters](#)
[Help](#)

Welcome to your 30 day free trial of Elasticsearch Service

What do you want to do with your data?
Put your data to work for you with a pre-configured solution. [Learn more](#)

Elastic Stack
Deploy Elasticsearch and Kibana. Search, analyze, and visualize data from any source, in any format.

Elastic Enterprise Search
Easily implement powerful search experiences for your website, app, or workplace with refined APIs and tools.

Elastic Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Elastic Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Select Select Select Select

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

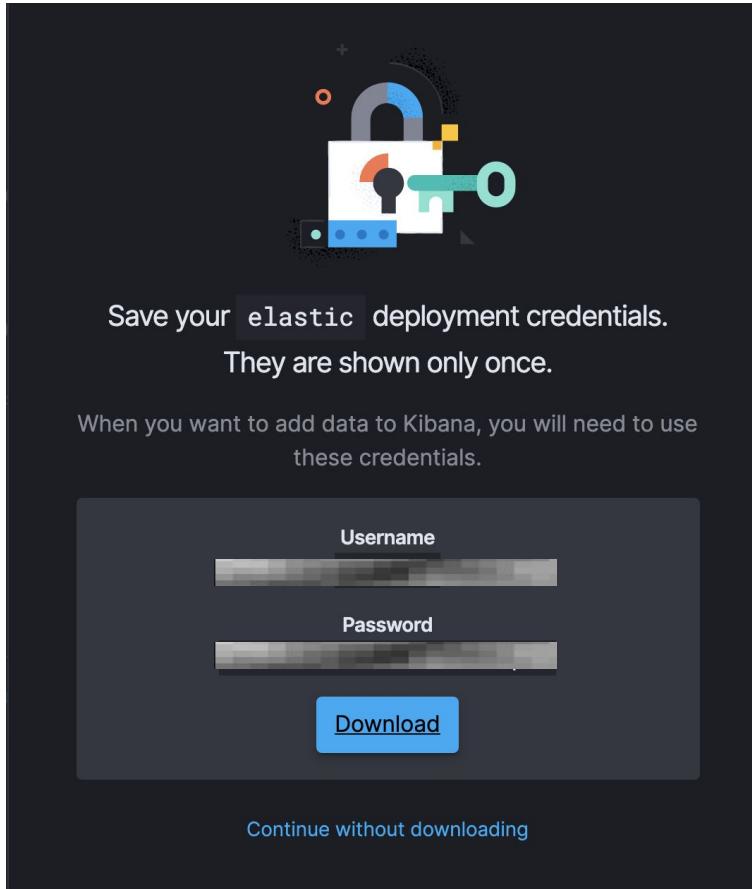
Name your deployment

You can always change this later.

OrionHacks-Elastic

 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

OrionHacks-Elastic

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](#)

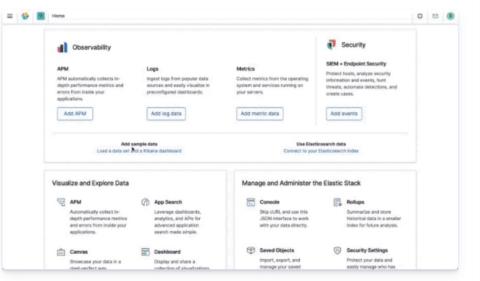
Deployment name: OrionHacks-Elastic [Edit](#)
Deployment ID: 316be9b

Deployment version: v7.10.1

Deployment status: ● Healthy

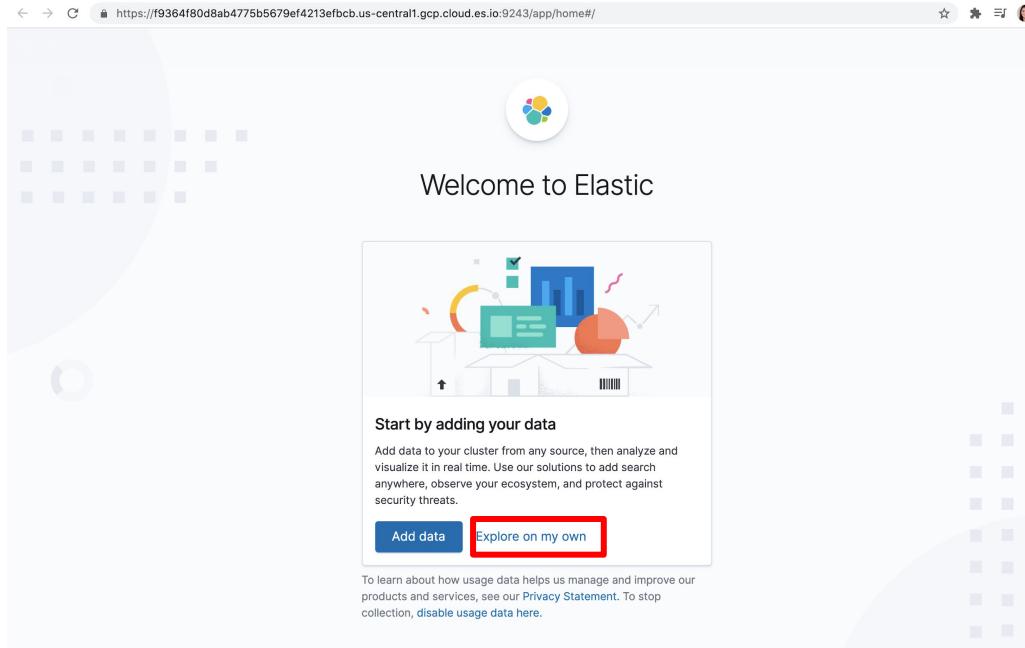
[Open Kibana](#) [Manage](#)

us-central1 (Iowa)

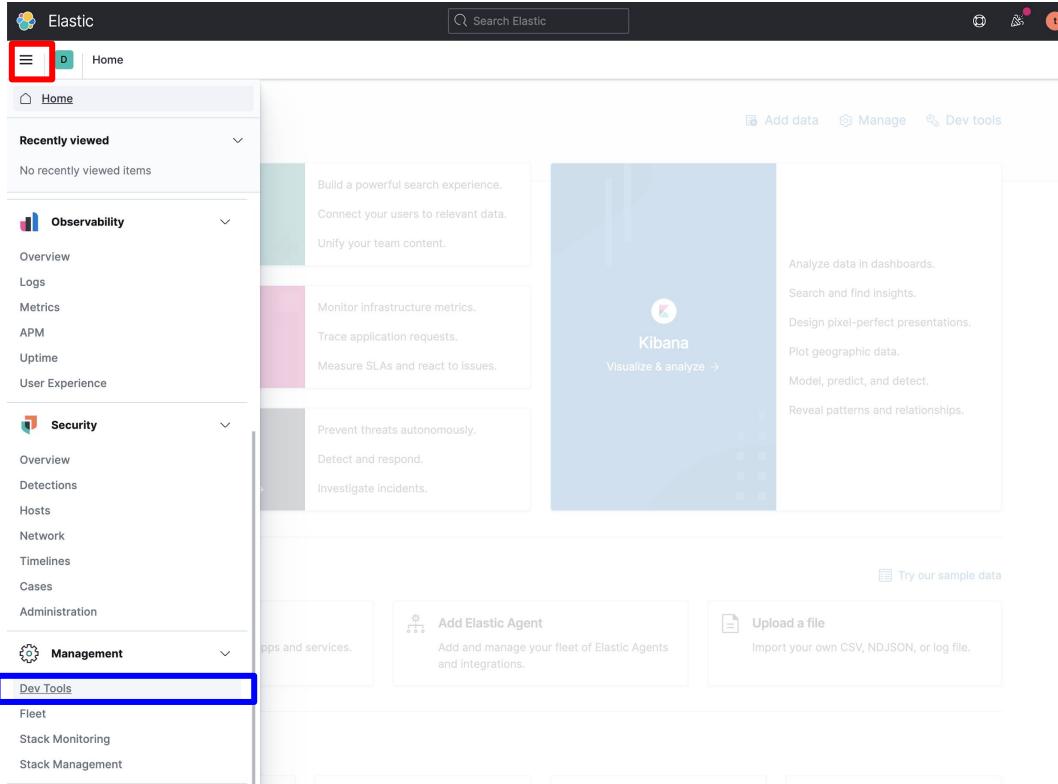


The screenshot shows the Elastic Cloud interface for a deployment named "OrionHacks-Elastic". On the left, there's a sidebar with navigation links for Elasticsearch, Kibana, APM, Enterprise Search, Logs and metrics, Activity, Security, and Performance. Below that is a section for "Extensions" with "API keys" and "Traffic filters". The main content area displays the deployment details: "Deployment name: OrionHacks-Elastic", "Deployment ID: 316be9b", and "Deployment version: v7.10.1". It also shows the deployment status as "Healthy". A large blue button labeled "Open Kibana" is highlighted with a red box. Below it, there's a note about saving credentials and a link to reset the password. To the right, there's a preview of the Kibana interface with various sections like Observability, Security, Visualize and Explore Data, and Manage and Administer the Elastic Stack. At the top right of the main content area, there's a location indicator for "us-central1 (Iowa)".

Click on Explore on my own option.



Click on menu icon, and open Dev Tools.



Click on Explore on my own option.

The screenshot shows the Elasticsearch Dev Tools interface. On the left, the 'Console' tab is selected, displaying a search request:

```
GET _search
{
  "query": {
    "match_all": {}
  }
}
```

A blue box highlights this request. On the right, a modal window titled 'Welcome to Console' provides an introduction to the UI:

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:

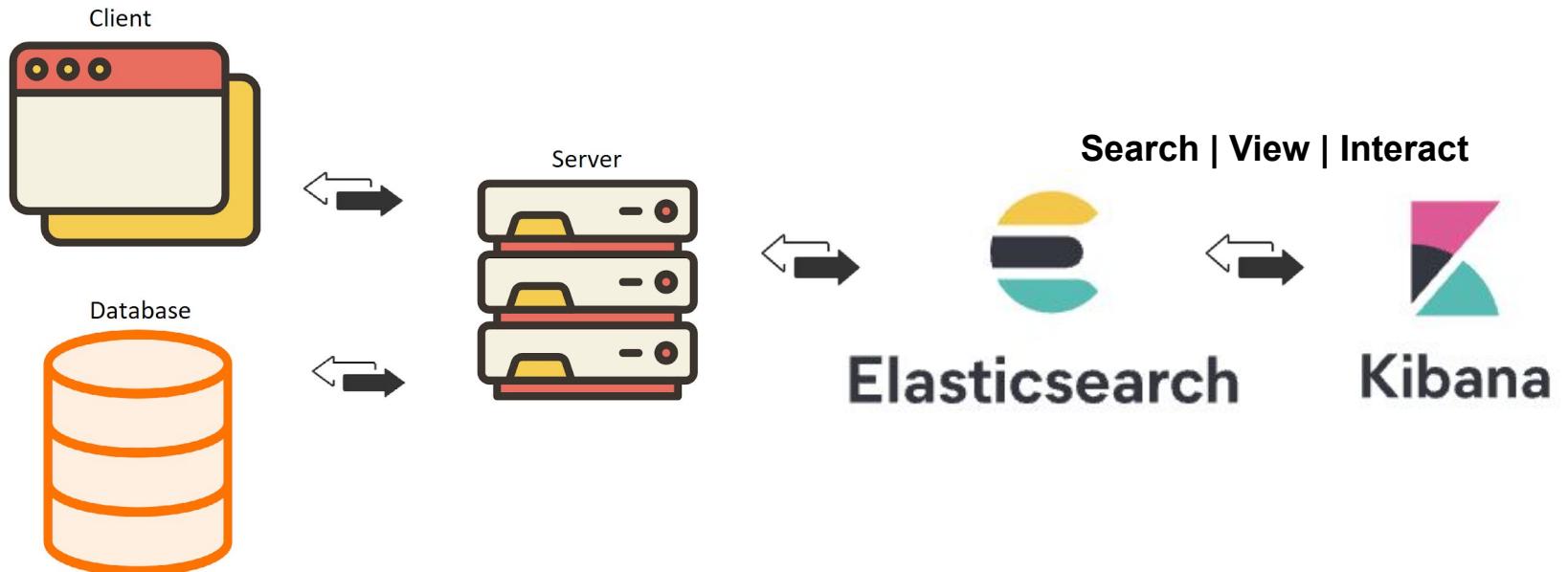
```
1 # index a doc
2 PUT index/_doc/1
3 {
4   "body": "here"
5 }
6
7 # and get it ...
8 GET index/_doc/1
```

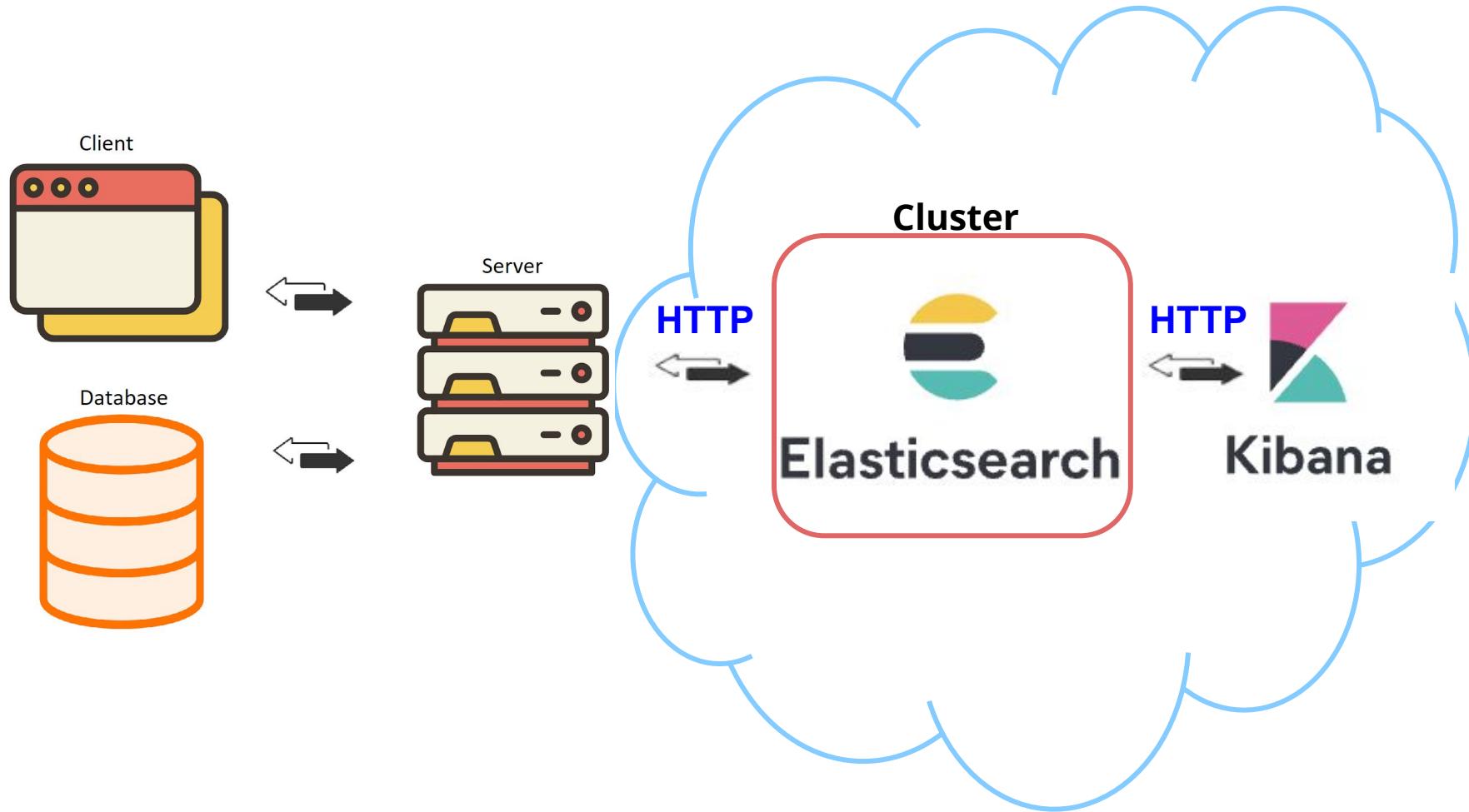
While typing a request, Console will make suggestions which you can then accept by hitting Enter/Tab. These suggestions are made based on the request structure as well as your indices and types.

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 the Elastic Austin User Group for updates on future workshops!

Meetup

Start a new group
50% OFF

Exp



Part of **Elastic - 142 groups**

Elastic Austin User Group

Austin, TX

589 members · Public group

Organized by Elastic Meetup Team and 1 other

Share: [f](#) [t](#) [in](#)

About Events Members Photos Discussions More

Manage group

Create event



Lisa Jung

Developer Advocate @Elastic

E-mail: lisa.jung@elastic.co

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

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

Twitter: @LisaHJung

