Introduction to Elasticsearch

s1270232 Yoshino Tomoaki

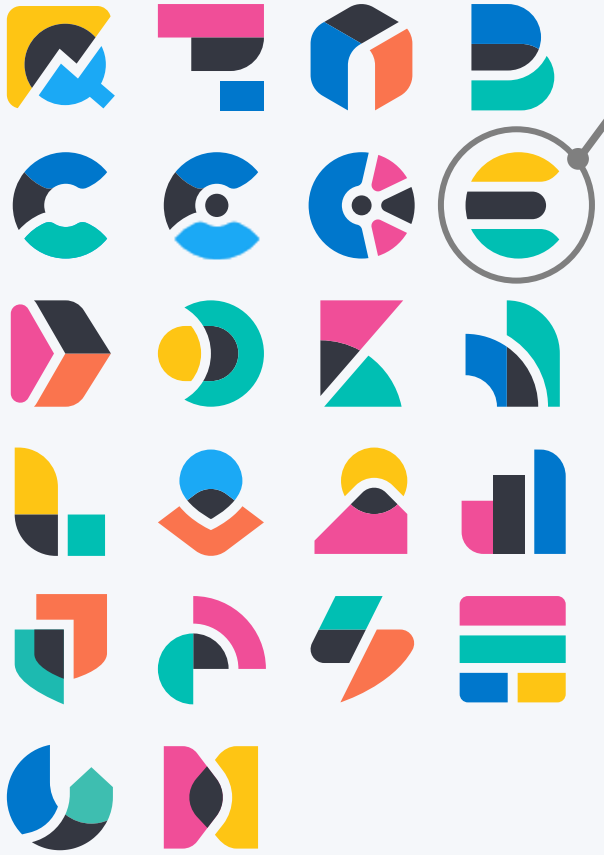
2021.06.23

Agenda

1. What is Elasticsearch
2. Feature of Elasticsearch
3. Others

What is Elasticsearch

elastic



Elasticsearch

elastic

Elasticsearch

- Open Source Distributed

elastic

Elasticsearch

- Open Source Distributed
- NoSQL

elastic

Elasticsearch

- Open Source Distributed
- NoSQL
  - Document oriented

elastic

Elasticsearch

- Open Source Distributed
- NoSQL
  - Document oriented
- **Full-Text Search Engine**

What is Full-Text Search ?

Like Search

- Full Scan

Full-Text Search

- Use Index

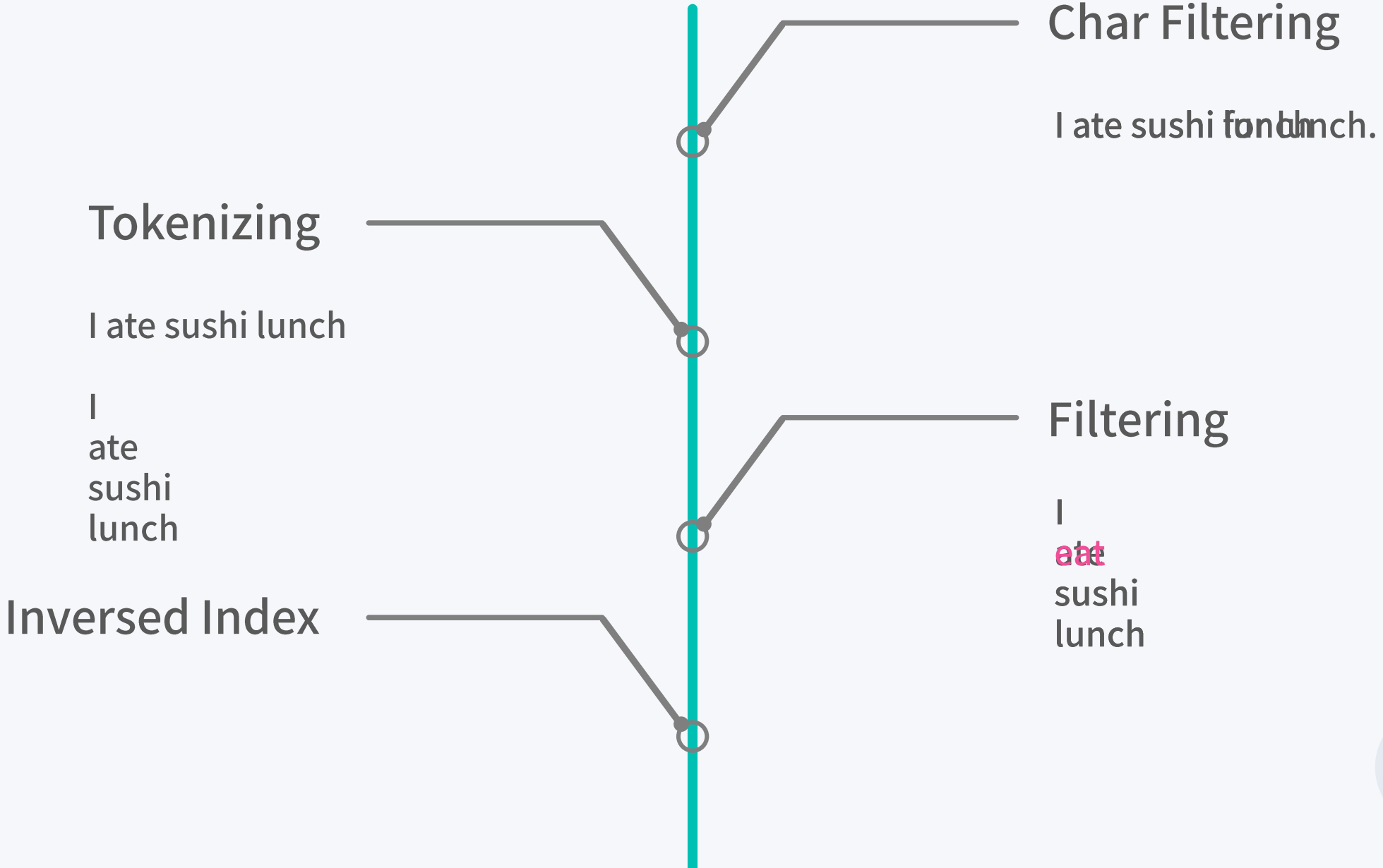
Elasticsearch

Adoption

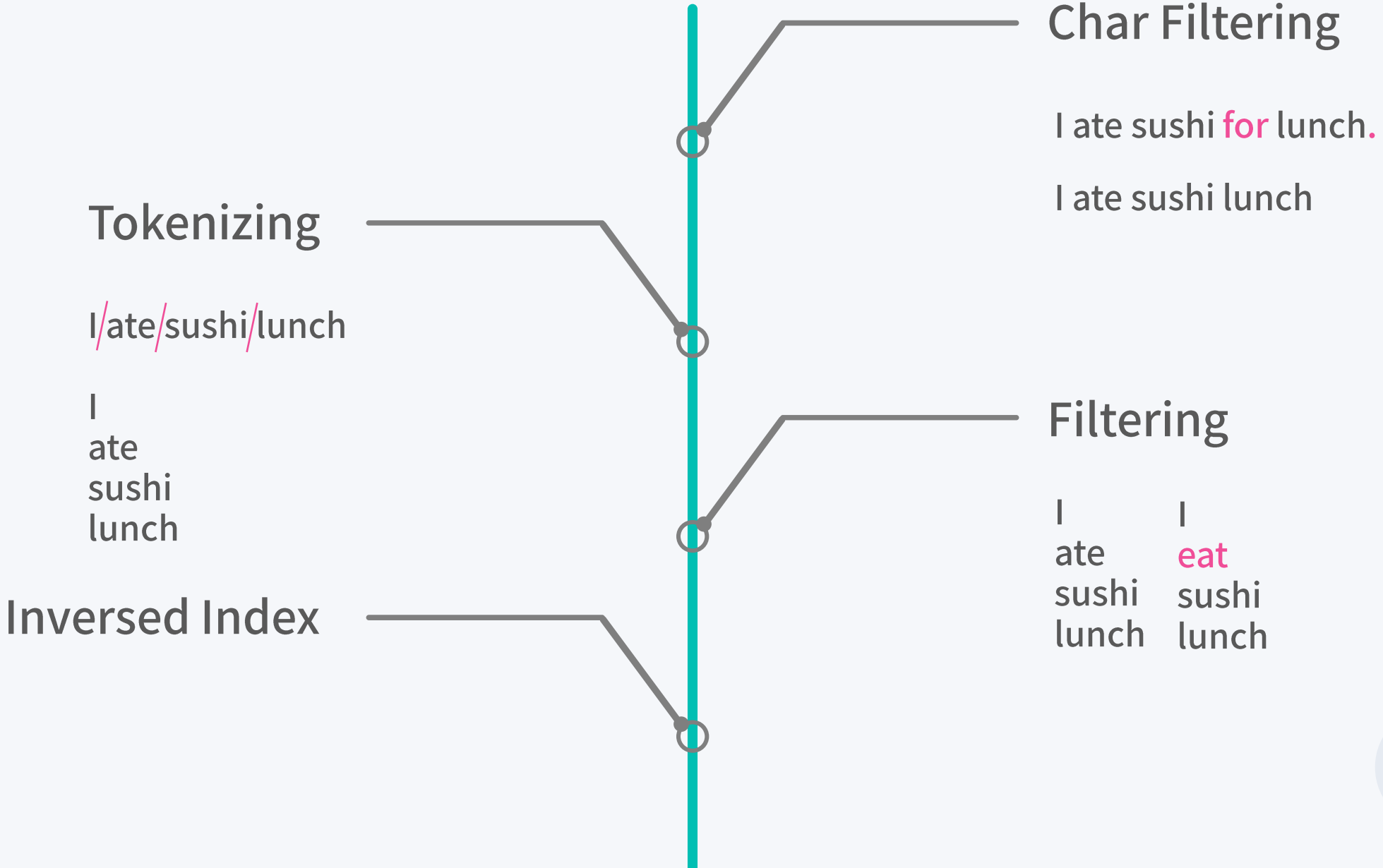
Elasticsearch

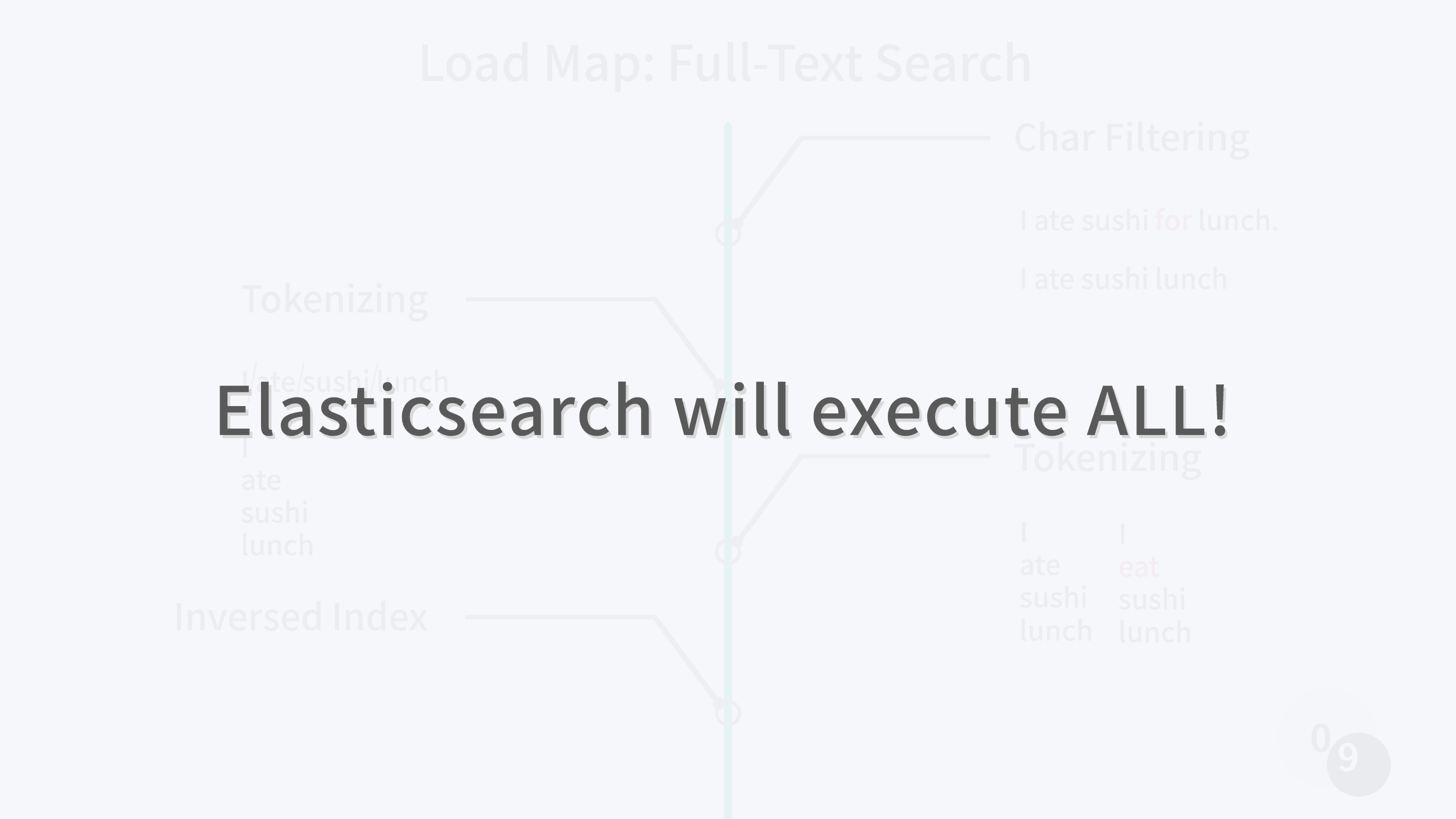
Feature of Elasticsearch

Load Map: Full-Text Search



Load Map: Full-Text Search




Load Map: Full-Text Search
Char Filtering
I ate sushi for lunch.
I ate sushi lunch
Tokenizing
I/ate/sushi/lunch
I
ate
sushi
lunch
Tokenizing
I
ate
sushi
lunch
I
eat
sushi
lunch
Inversed Index
Elasticsearch will execute ALL!
09

Distributed Processing

Faster & Stronger

- Increase Processing Speed
- Fault Tolerance

Environments

Run in Java

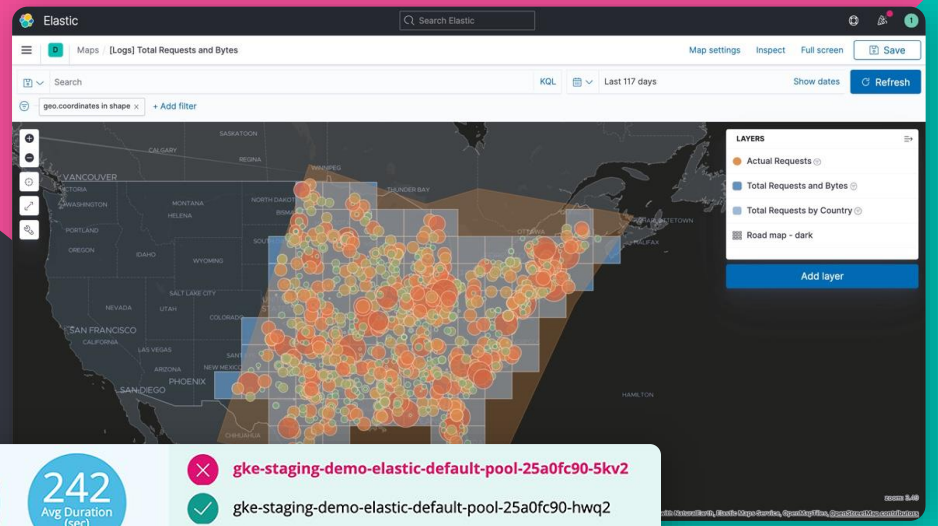
Support many client

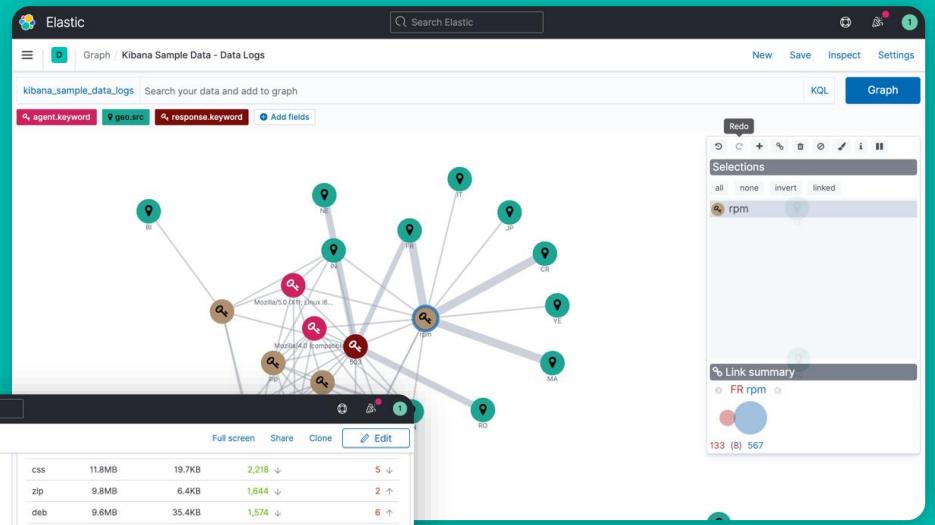
Official

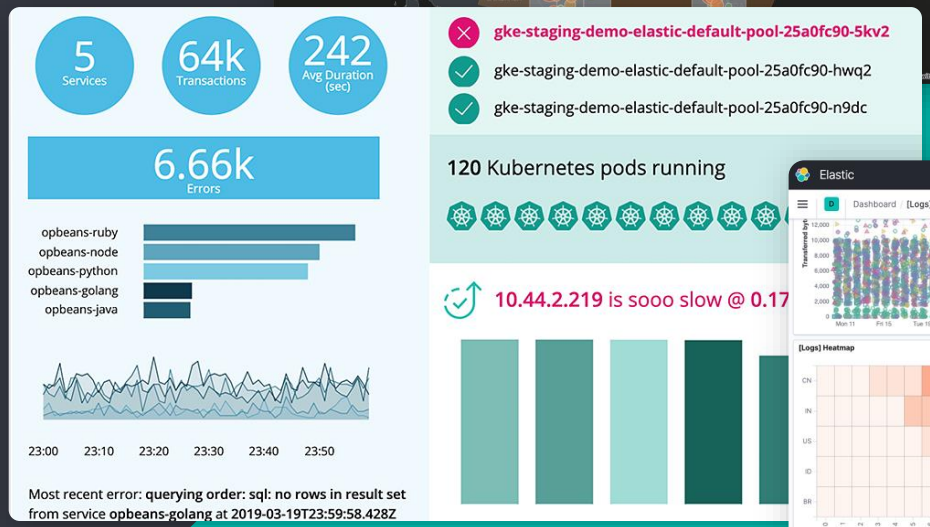
- Java
- JavaScript
- Go
- .NET
- PHP
- Python
- Ruby
- Perl
- eland
- Rust

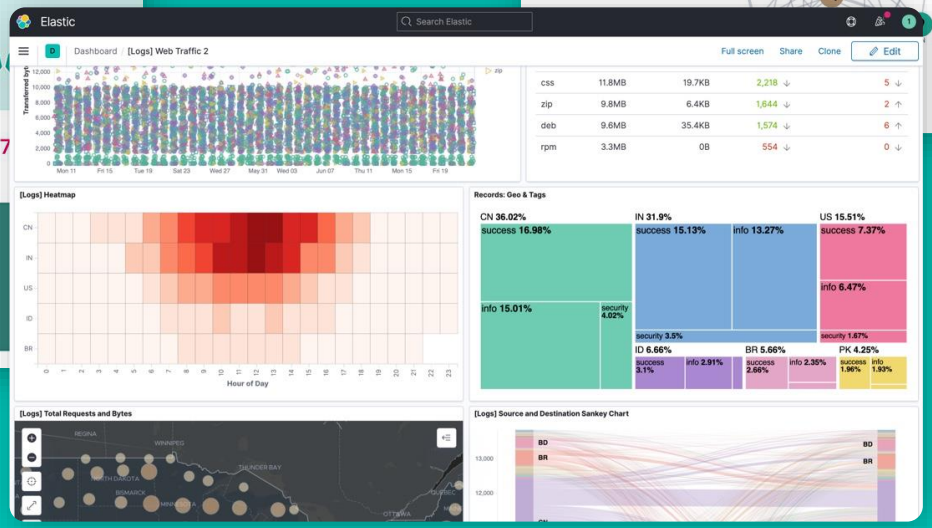
Others

Kibana



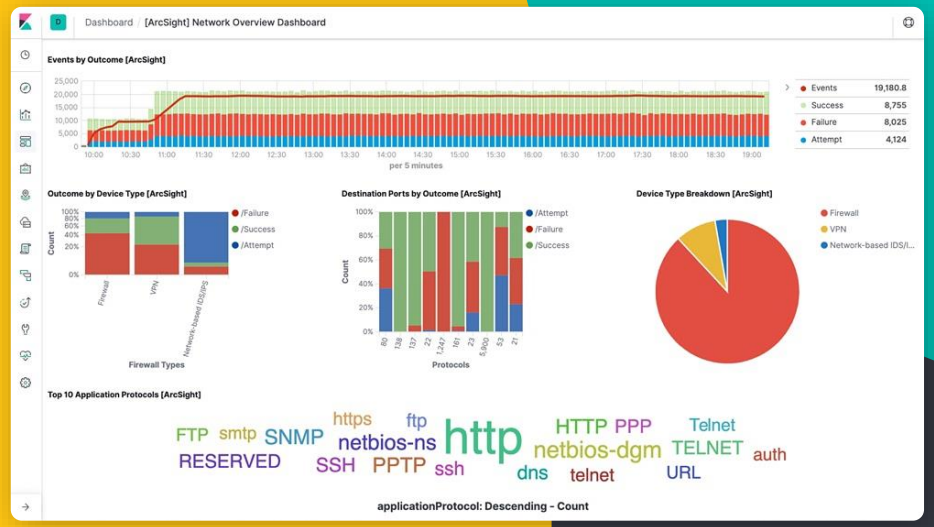


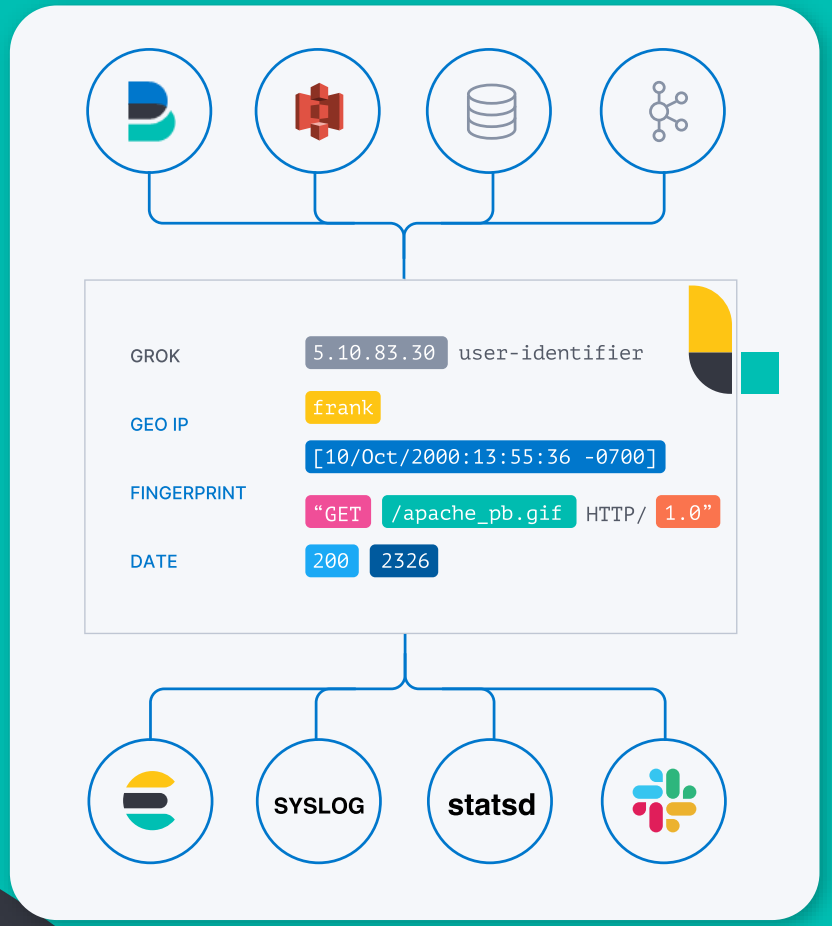




https://www.elastic.co/jp/kibana

Logstash


Dashboard
[ArcSight] Network Overview Dashboard
Events by Outcome [ArcSight]
Outcome by Device Type [ArcSight]
Destination Ports by Outcome [ArcSight]
Device Type Breakdown [ArcSight]
Top 10 Application Protocols [ArcSight]
FTP smtp SNMP https ftp netbios-ns http HTTP PPP Telnet netbios-dgm TELNET auth RESERVED SSH PPTP ssh dns telnet URL
applicationProtocol: Descending - Count


GROK
5.10.83.30
user-identifier
GEO IP
frank
[10/Oct/2000:13:55:36 -0700]
FINGERPRINT
"GET
/apache_pb.gif
HTTP/
1.0"
DATE
200
2326
SYSLOG
statsd

Summary

NoSQL

Document oriented

Schema less

Scalable

Distributed

Search Engine

Full-Text

Very Fast

RESTful

Score

Others

GUI Management

Log Collection

Security

etc.

Elasticsearch

References

- Free and Open Search: The Creators of Elasticsearch, ELK & Kibana | Elastic

  (https://www.elastic.co/)

- Full-text search – Wikipedia

  (https://en.wikipedia.org/wiki/Full-text_search)

Thank you!

s1270232 Yoshino Tomoaki