- **Mr. Vijay Kumar**
- Software Architect
- **14+** Years of Experience

Email: **vijumca@gmail.com**

Agenda

01 Need For Log Analysis

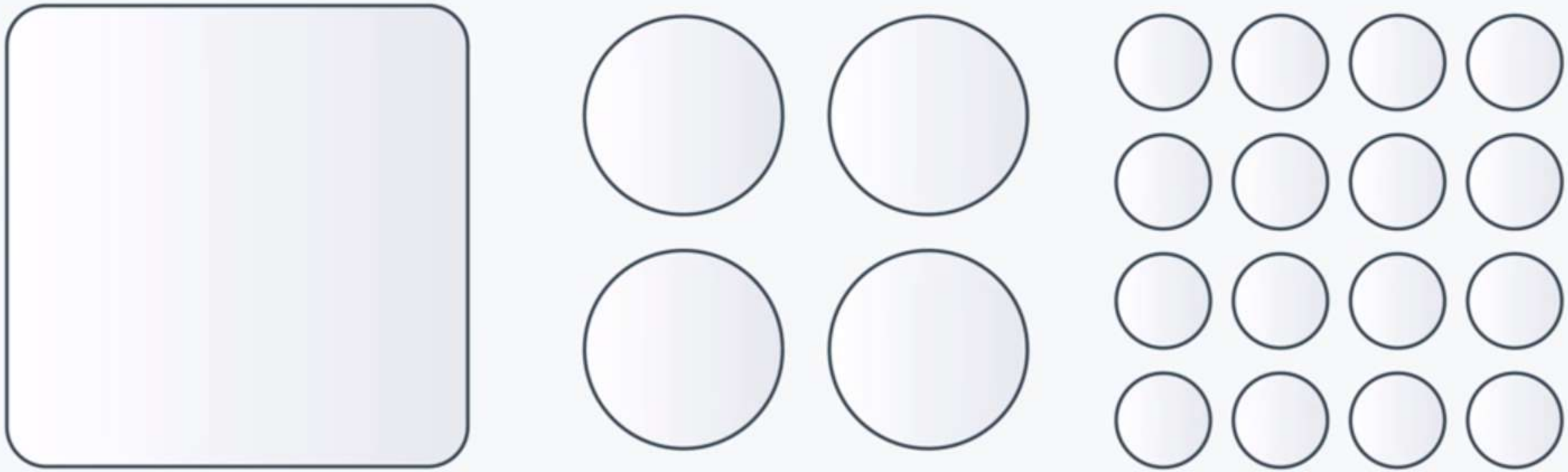
02 Problems With Log Analysis

03 What Is ELK Stack?

04 Features Of ELK Stack

05 Companies Using ELK Stack

Monolithic vs. SOA vs. Microservices



Monolithic

Single Unit

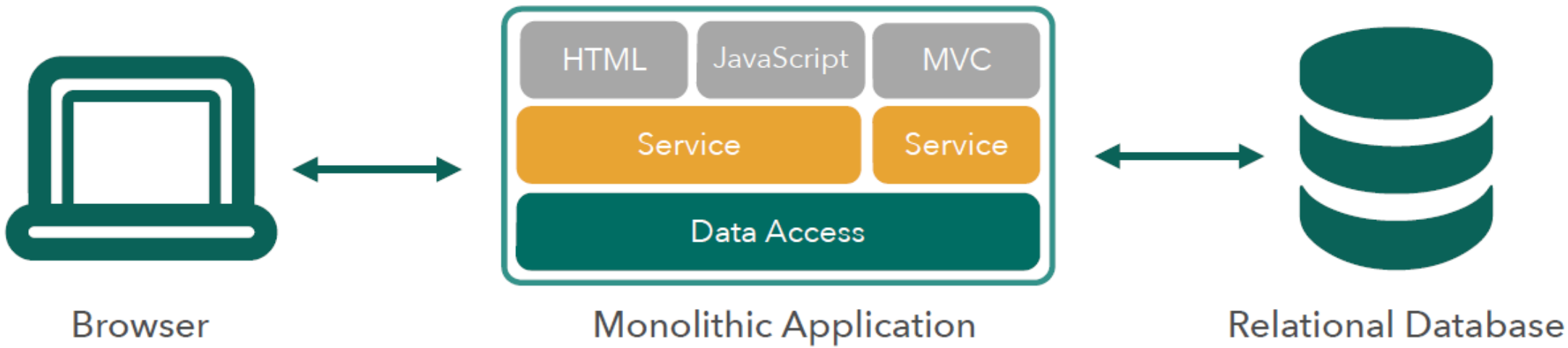
SOA

Coarse-grained

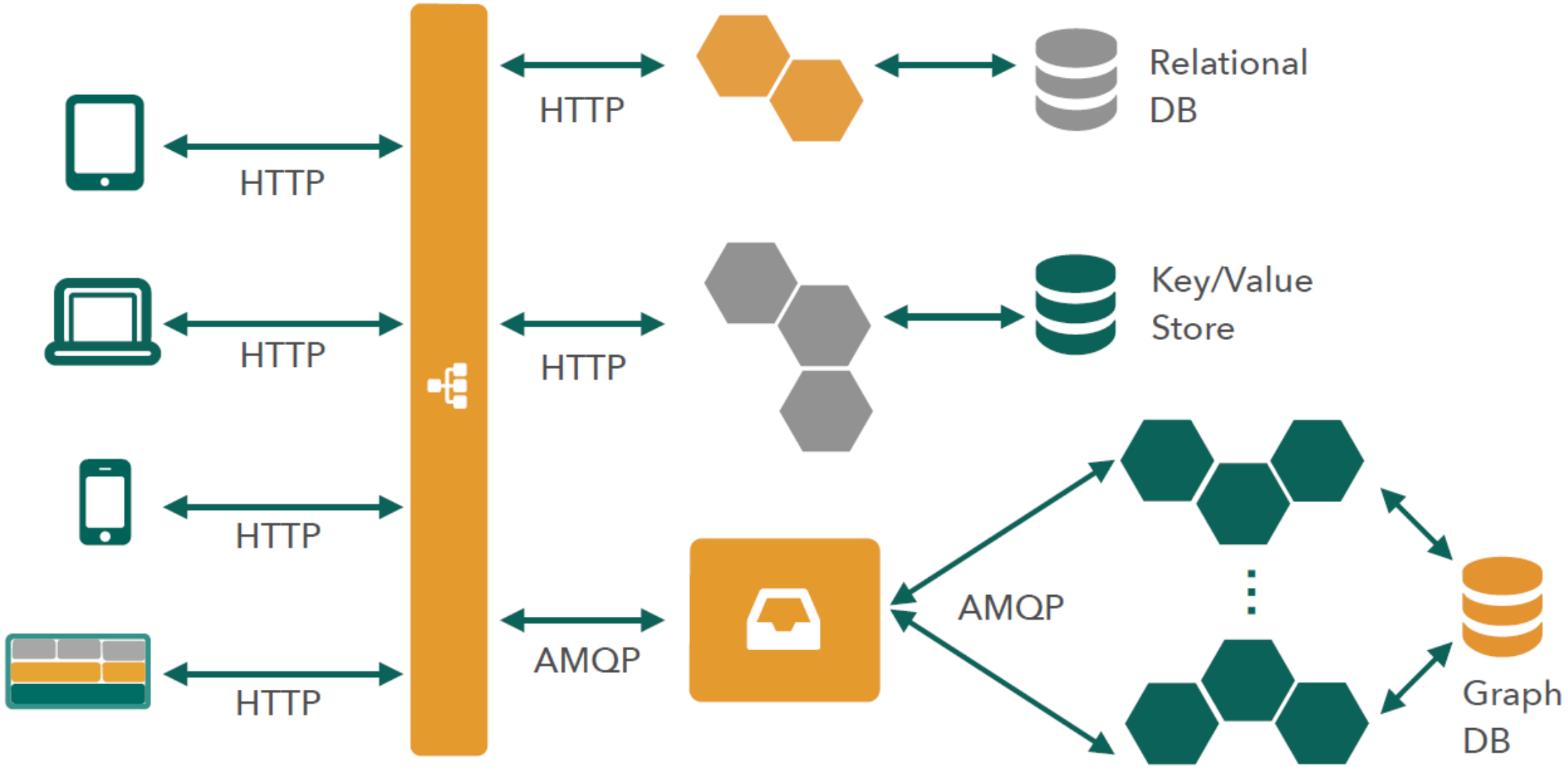
Microservices

Fine-grained

Monolithic Architecture



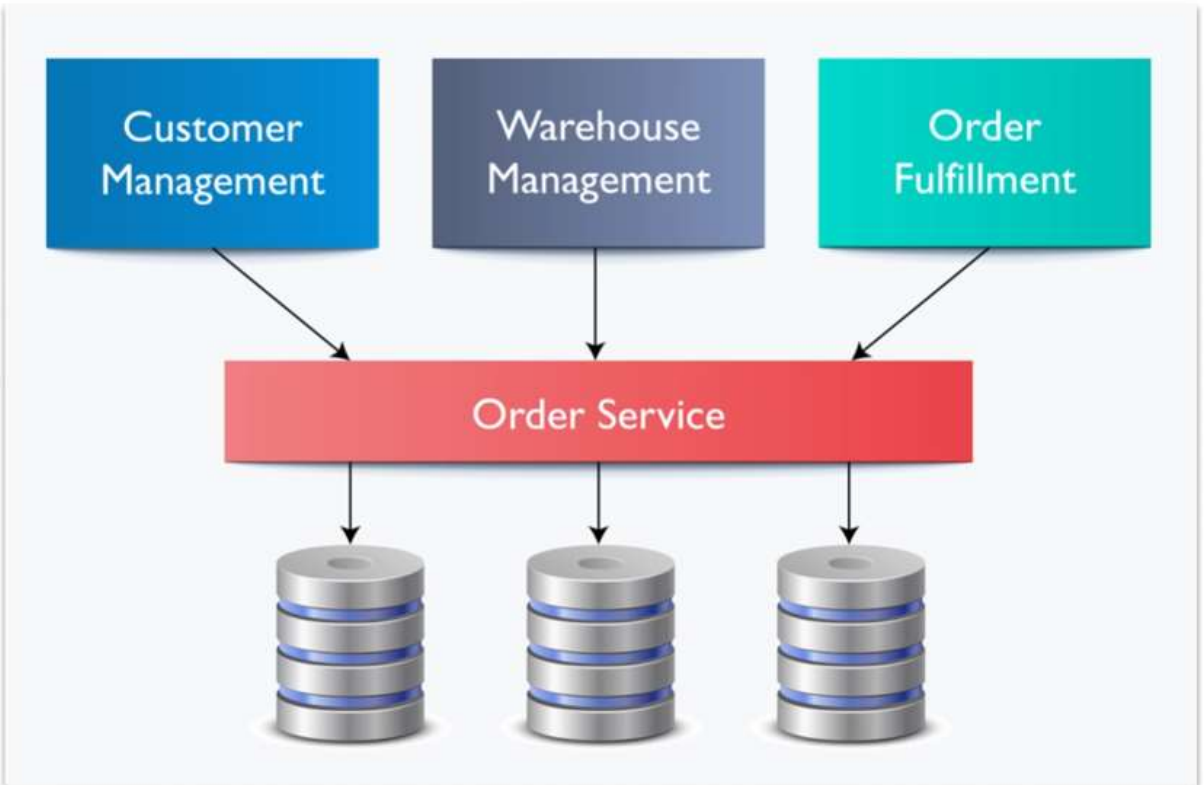
Microservice Architecture



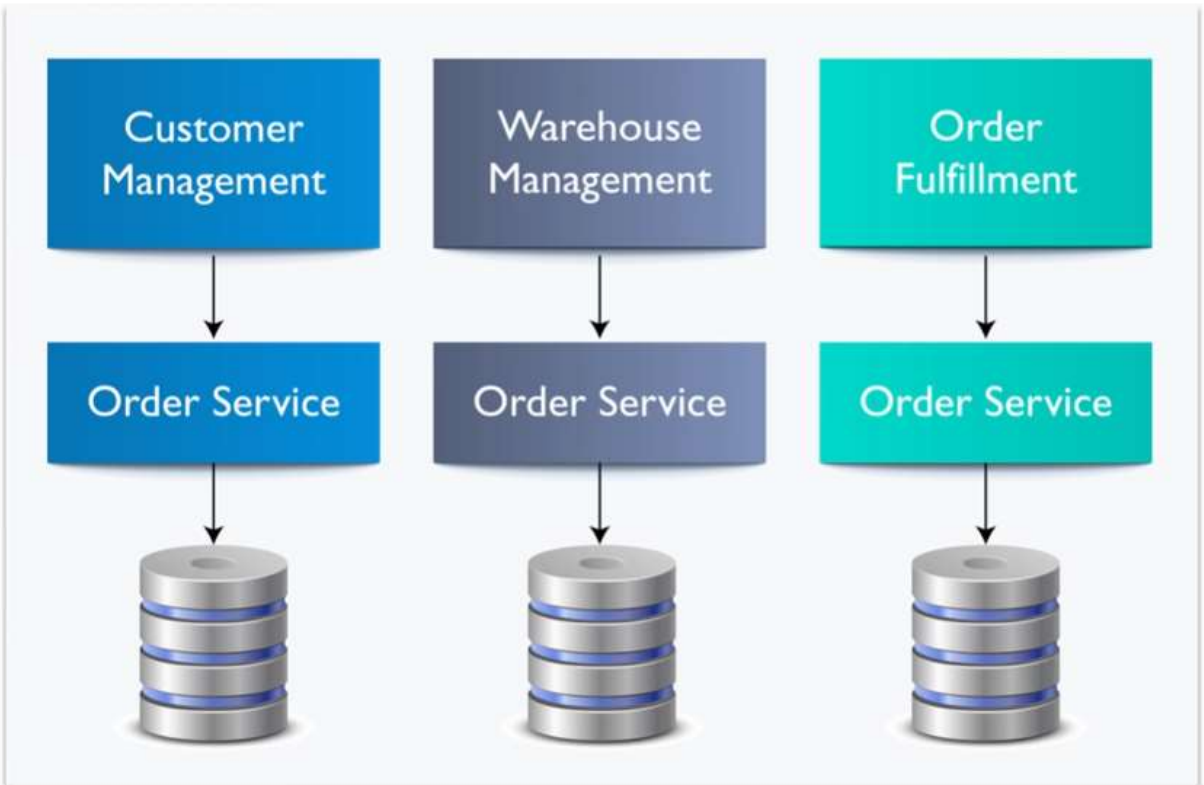
Microservice Architectures

- Simple / Challenging
- Modularity Based on Component Services
- Change Cycles Decoupled / Enable Frequent Deploys
- Efficient Scaling
- Individual Components Less Intimidating to New Developers
- Enables Scaling of Development
- Eliminates Long-Term Commitment to Technical Stack

Component Sharing



SOA



Microservices

SOA Vs Microservice

Centralized Governance

SOA is like an orchestra where each artist is performing with his/her instrument while the music director guides them all.

De-Centralized Governance

With Microservices each dancer is independent and know what they need to do. If they miss some steps they know how to get back on the sequence.

Stack

Microservice
Centralize
Logging

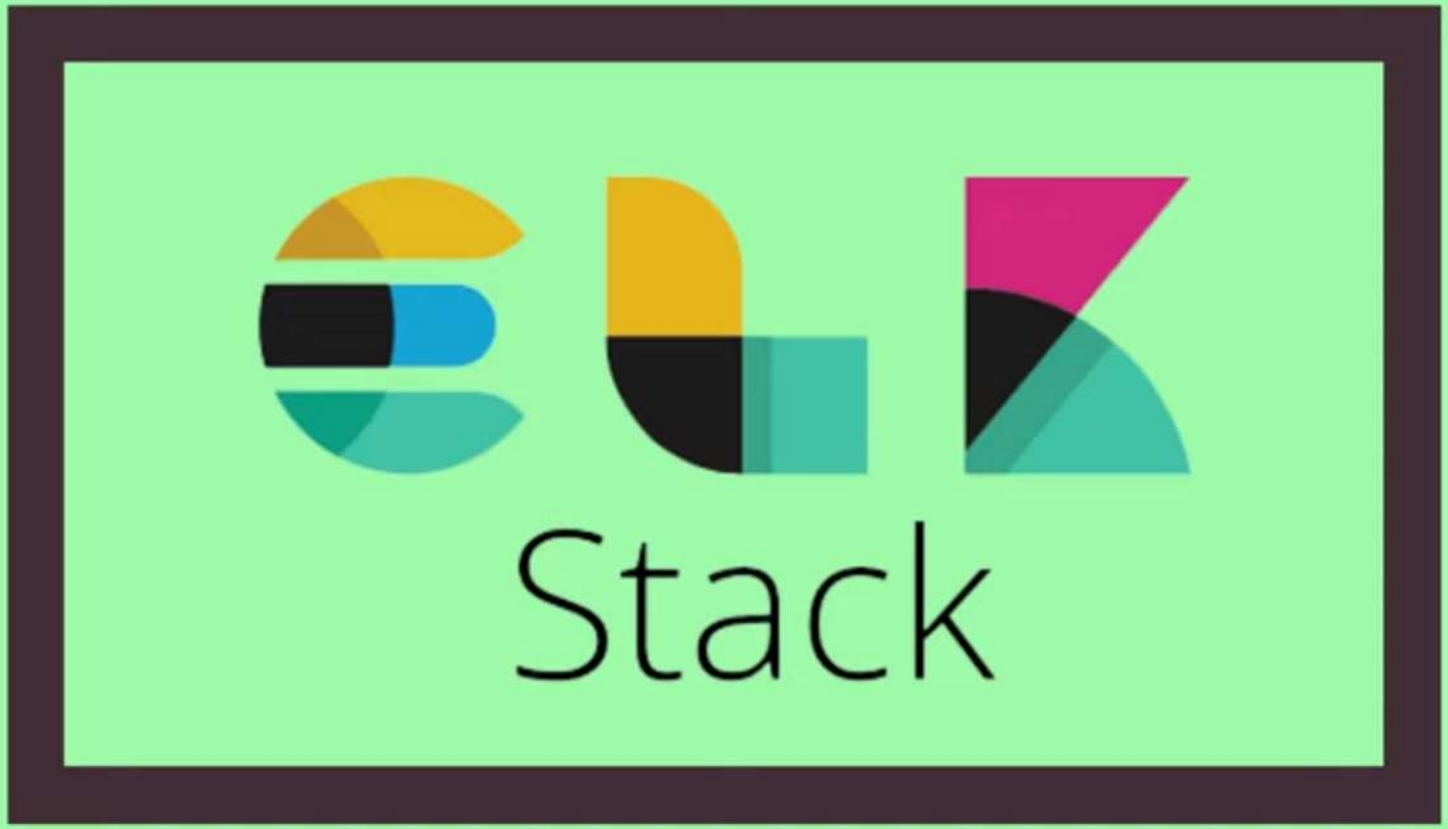
What is ELK ?

elastic

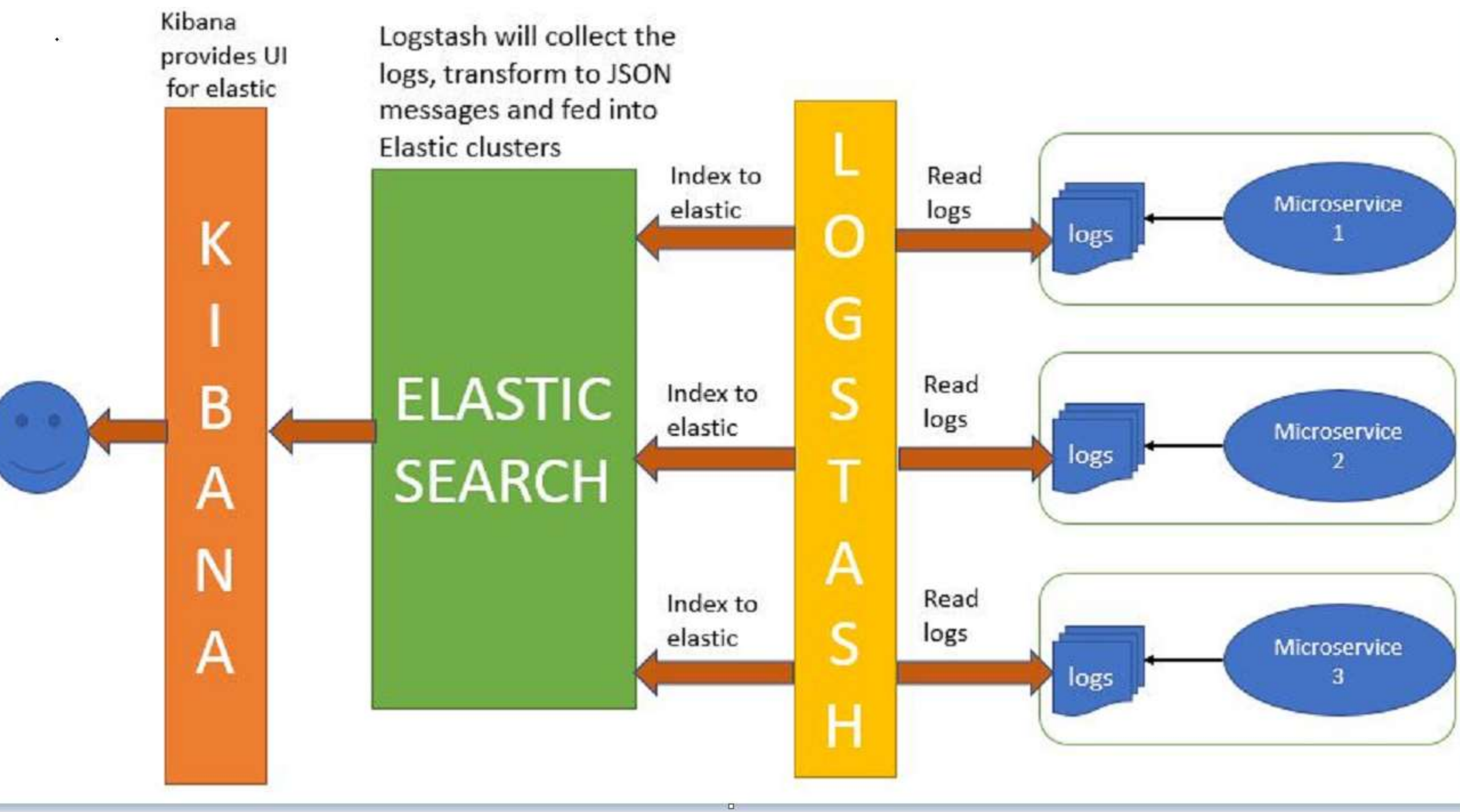
+

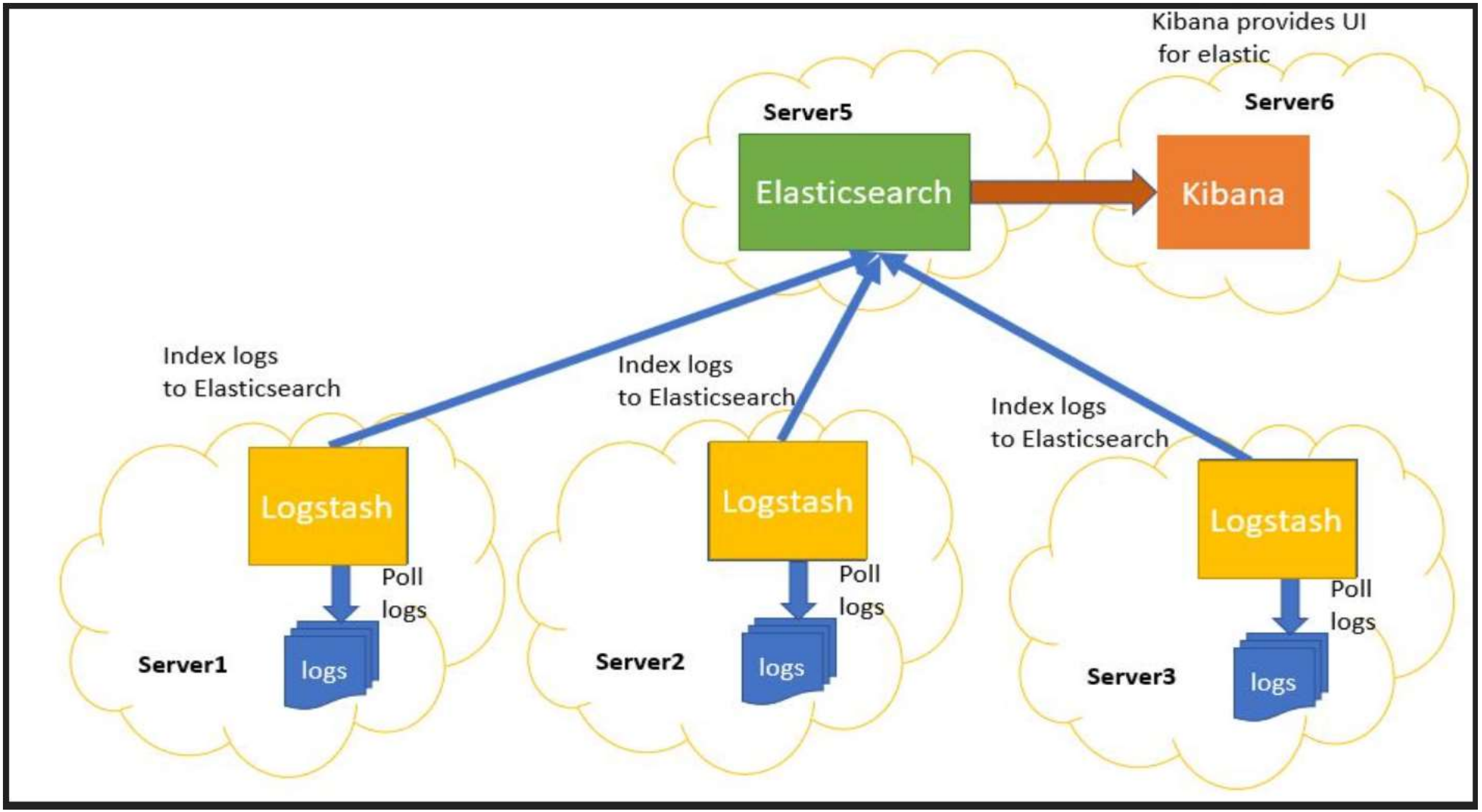
logstash

kibana

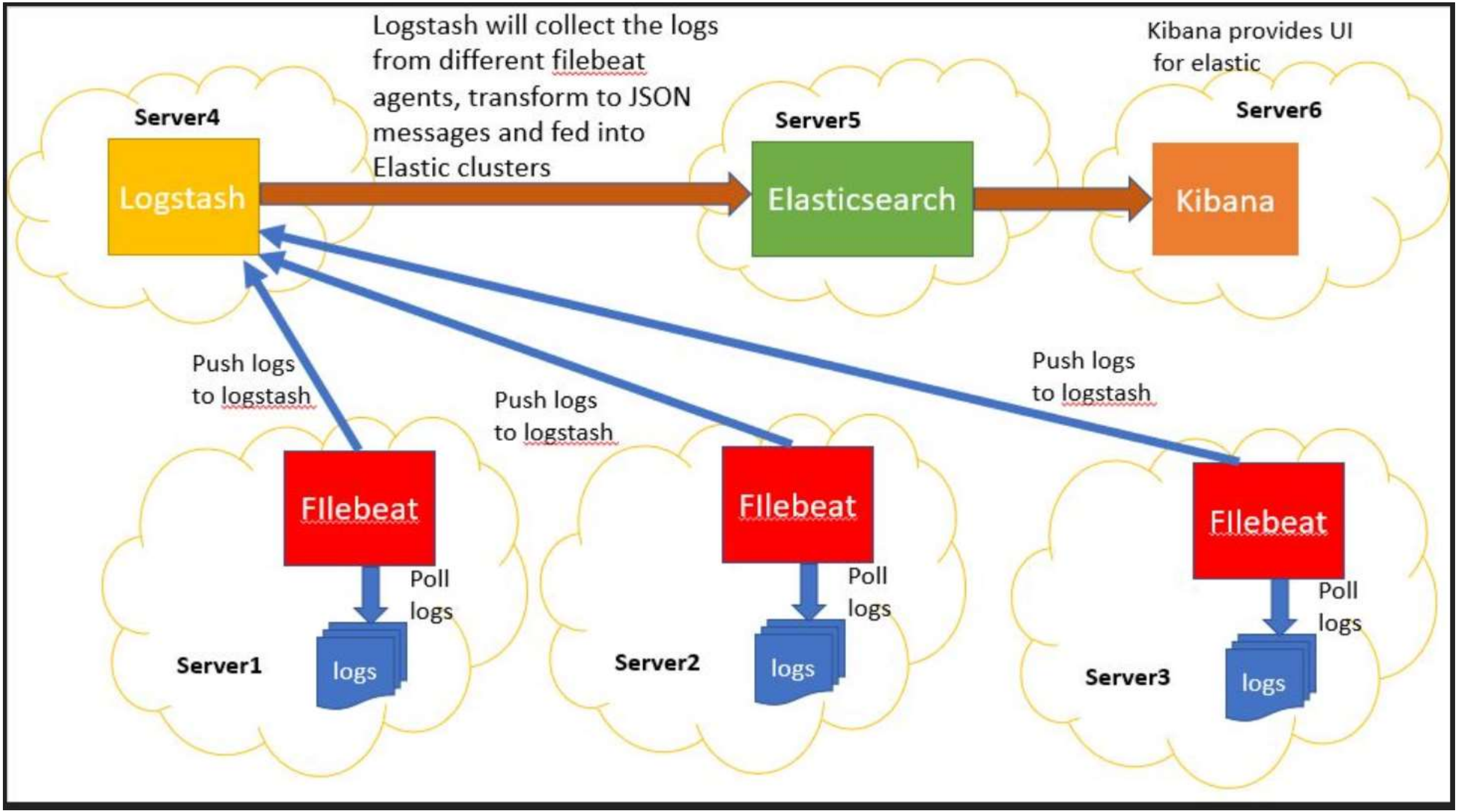


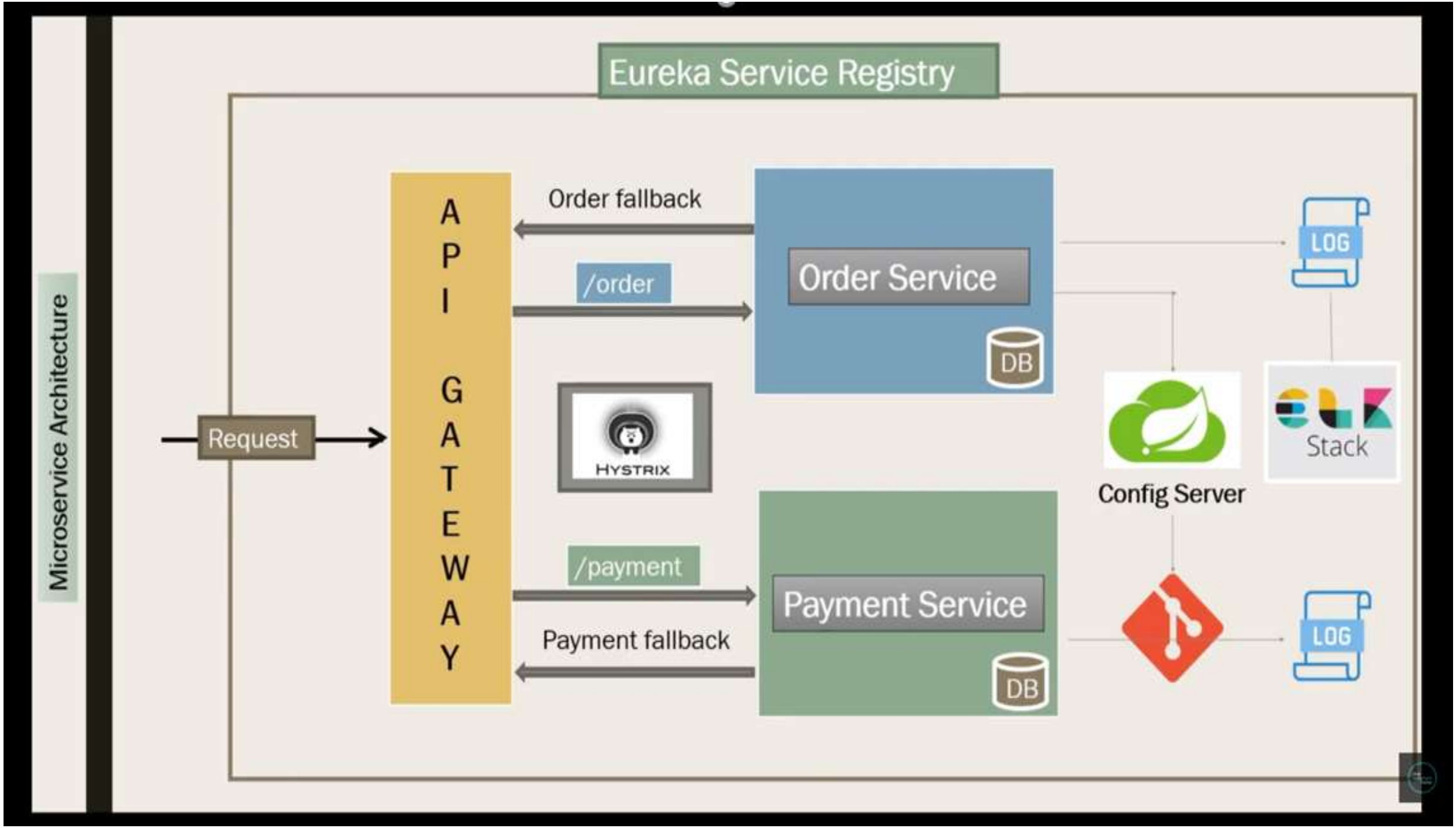
Microservice - Centralize Logging


Kibana provides UI for elastic
Logstash will collect the logs, transform to JSON messages and fed into Elastic clusters
KIBANA
ELASTIC SEARCH
LOGSTASH
Index to elastic
Index to elastic
Index to elastic
Read logs
Read logs
Read logs
logs
logs
logs
Microservice 1
Microservice 2
Microservice 3


Kibana provides UI
for elastic
Server5
Server6
Elasticsearch
Kibana
Index logs
to Elasticsearch
Index logs
to Elasticsearch
Index logs
to Elasticsearch
Logstash
Logstash
Logstash
Poll
logs
Poll
logs
Poll
logs
Server1
Server2
Server3
logs
logs
logs


LOG
LOG
LOG
Collect &
Transform
Search &
Analyze
Visualize
& Manage


Logstash will collect the logs from different filebeat agents, transform to JSON messages and fed into Elastic clusters
Kibana provides UI for elastic
Server4
Logstash
Server5
Elasticsearch
Server6
Kibana
Push logs to logstash
Push logs to logstash
Push logs to logstash
FIlebeat
Poll logs
logs
Server1
FIlebeat
Poll logs
logs
Server2
FIlebeat
Poll logs
logs
Server3


Microservice Architecture
Eureka Service Registry
Request
API GATEWAY
Order fallback
/order
HYSTRIX
/payment
Payment fallback
Order Service
DB
Payment Service
DB
LOG
Stack
Config Server
LOG

Overview of the Elastic Stack


Search & Analyze
Collect & Transform
Visualize & Manage
What is ELK Stack?

Need For Log Analysis

Let's understand why do we need Log Analysis?

What Is Log Analysis?

Log Analysis Is The Process Of Analyzing The Computer/ Machine Generated Data

Need For Log Analysis

Issue Debugging

Predictive Analysis

Security Analysis

Performance Analysis

Internet of Things & Debugging

Problems With Log Analysis

1. Non-consistent log format
2. Non-consistent time format
3. Decentralized logs
4. Expert knowledge requirement

Problems With Log Analysis

1. Non-consistent log format
2. Non-consistent time format
3. Decentralized logs
4. Expert knowledge requirement

Tomcat Logs

```
ffMay 24, 2015 3:56:26 PM org.apache.catalina.startup.HostConfig  deployWAR
INFO: Deployment of web application archive \soft\apache-tomcat-7.0.62\webapps\sample.war
has finished in 253 ms
```

Apache Access Logs

```
127.0.0.1 - - [24/May/2015:15:54:59 +0530] "GET /favicon.ico HTTP/1.1" 200 21630
```

IIS Logs

```
2012-05-02 17:42:15 172.24.255.255 - 172.20.255.255 80 GET /images/favicon.ico - 200
Mozilla/4.0+(compatible;MSIE+5.5;+Windows+2000+Server)
```

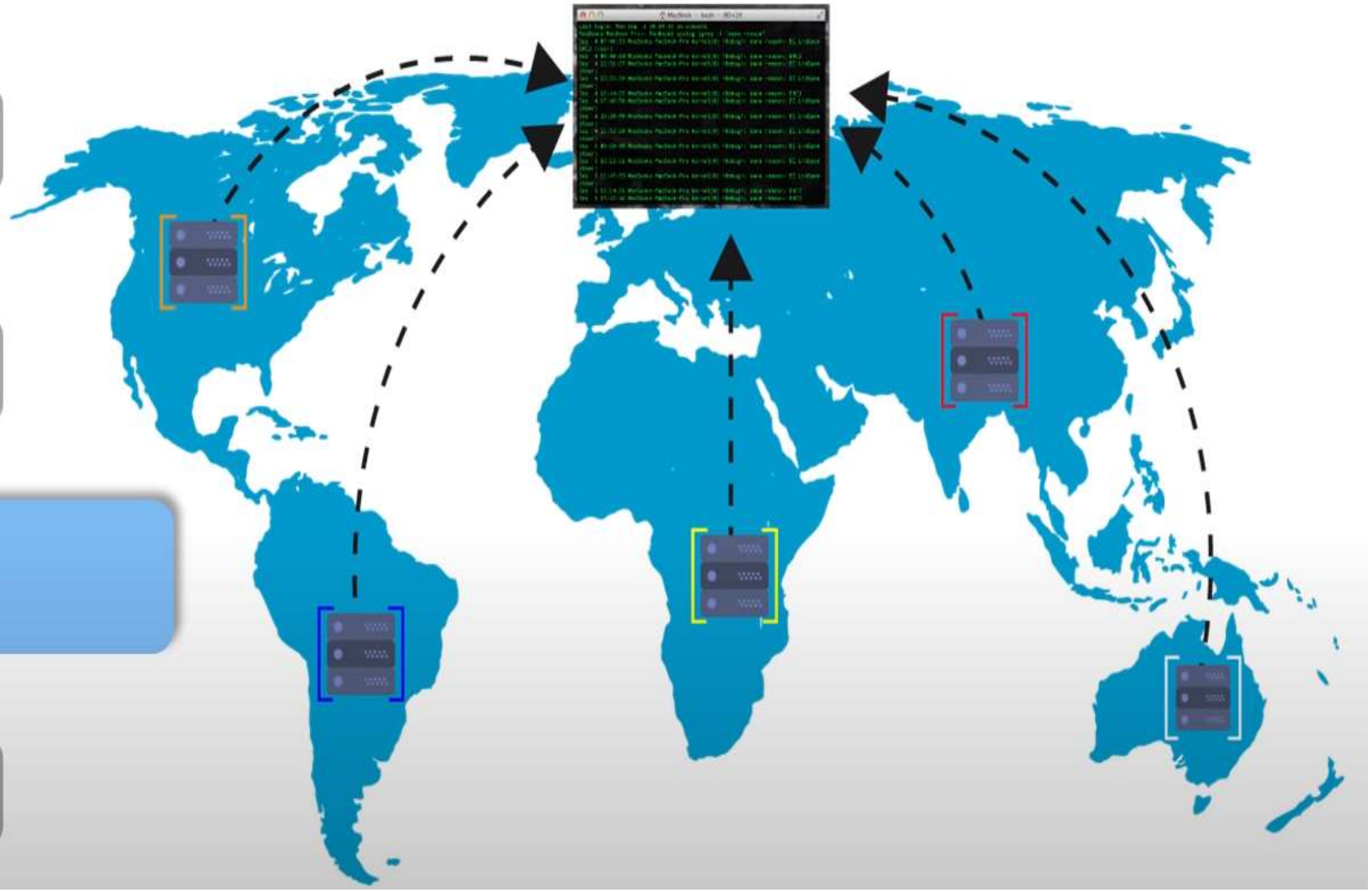
Problems With Log Analysis

1. Non-consistent log format
2. Non-consistent time format
3. Decentralized logs
4. Expert knowledge requirement

- 142920788
- Oct 12 23:21:45
- [5/May/2015:08:09:10 +0000]
- Tue 01-01-2009 6:00
- 2015-05-30 T 05:45 UTC
- Sat Jul 23 02:16:57 2014
- 07:38, 11 December 2012 (UTC)

Problems With Log Analysis

1. Non-consistent log format
2. Non-consistent time format
3. Decentralized Logs
4. Expert knowledge requirement



Problems With Log Analysis

1. Non-consistent log format
2. Non-consistent time format
3. Decentralized logs
4. **Expert Knowledge Requirement**

- Everyone do not have access to the logs
- General people might not have technical expertise to understand the information
- This can slow down the analysis process

Log Management Tools

splunk>

logentries™

graylog

sumologic

LOGGLY

ELK vs. Splunk

Elk	Splunk
Elk is open source tool	Splunk is a commercial tool.
Elk stack does not offer Solaris Portability because of Kibana.	Splunk offers Solaris Portability.
Processing speed is strictly limited.	Offers accurate and speedy processes.
ELK is a technology stack created with the combination Elastic Search-Logstash-Kibana.	Splunk is a proprietary tool. It provides both on-premise and cloud solutions.
In ELK Searching, Analysis & Visualization will be only possible after the ELK stack is setup.	Splunk is a complete data management package at your disposal.
ELK tool does not support integration with other tools.	Splunk is a useful tool for setting up integrations with other tools.

Case Studies

NetFlix

Netflix heavily relies on ELK stack. The company using ELK stack to monitor and analyze customer service operation's security log. It allows them to index, store, and search documents from more than fifteen clusters which comprise almost 800 nodes.

LinkedIn

The famous social media marketing site LinkedIn uses ELK stack to monitor performance and security. The IT team integrated ELK with Kafka to support their load in real time. Their ELK operation includes more than 100 clusters across six different data centers.

Tripwire:

Tripwire is a worldwide Security Information Event Management system. The company uses ELK to support information packet log analysis.

Medium:

Medium is a famous blog-publishing platform. They use ELK stack to debug their production issues. The company also uses ELK to detect DynamoDB hotpots. Moreover, using this stack, the company can support 25 million unique readers as well as thousands of published posts each week.

Advantages and Disadvantages of ELK stack

Advantages

- ELK works best when logs from various Apps of an enterprise converge into a single ELK instance

- It provides amazing insights for this single instance and also eliminates the need to log into hundred different log data sources
- Rapid on-premise installation
- Easy to deploy Scales vertically and horizontally
- Elastic offers a host of language clients which includes Ruby. Python. PHP, Perl, .NET, Java, and JavaScript, and more
- Availability of libraries for different programming and scripting languages

Disadvantages

- Different components In the stack can become difficult to handle when you move on to complex setup
- There’s nothing like trial and error. Thus, the more you do, the more you learn along the way

What Is ELK Stack?

ELK Stack is a combination of **three** open source tools which forms a **log management tool/ platform**, that helps in deep ***searching***, ***analyzing*** and ***visualizing*** the log generated from different machines

What is it ?

- Elasticsearch is a search engine based on the Lucene library.
- It provides a distributed full-text search engine with an HTTP web interface
- It is schema-free JSON documents.
- Elasticsearch is developed in Java and is released as open source under the terms of the Apache License

What Is ELK Stack: ElasticSearch

elasticsearch

Features

- ✓ search engine/ search server
- ✓ NoSQL database i.e. can't use SQL for queries.
- ✓ Based on Apache Lucene and provides RESTful API
- ✓ Provides horizontal scalability, reliability and multenant capability for real time search
- ✓ Uses indexes to search which makes it faster

Why we need it?

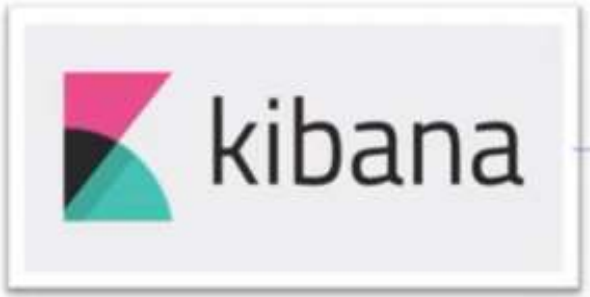
- Elasticsearch is able to achieve fast search responses because, instead of searching the text directly, it searches an index.

- For Example

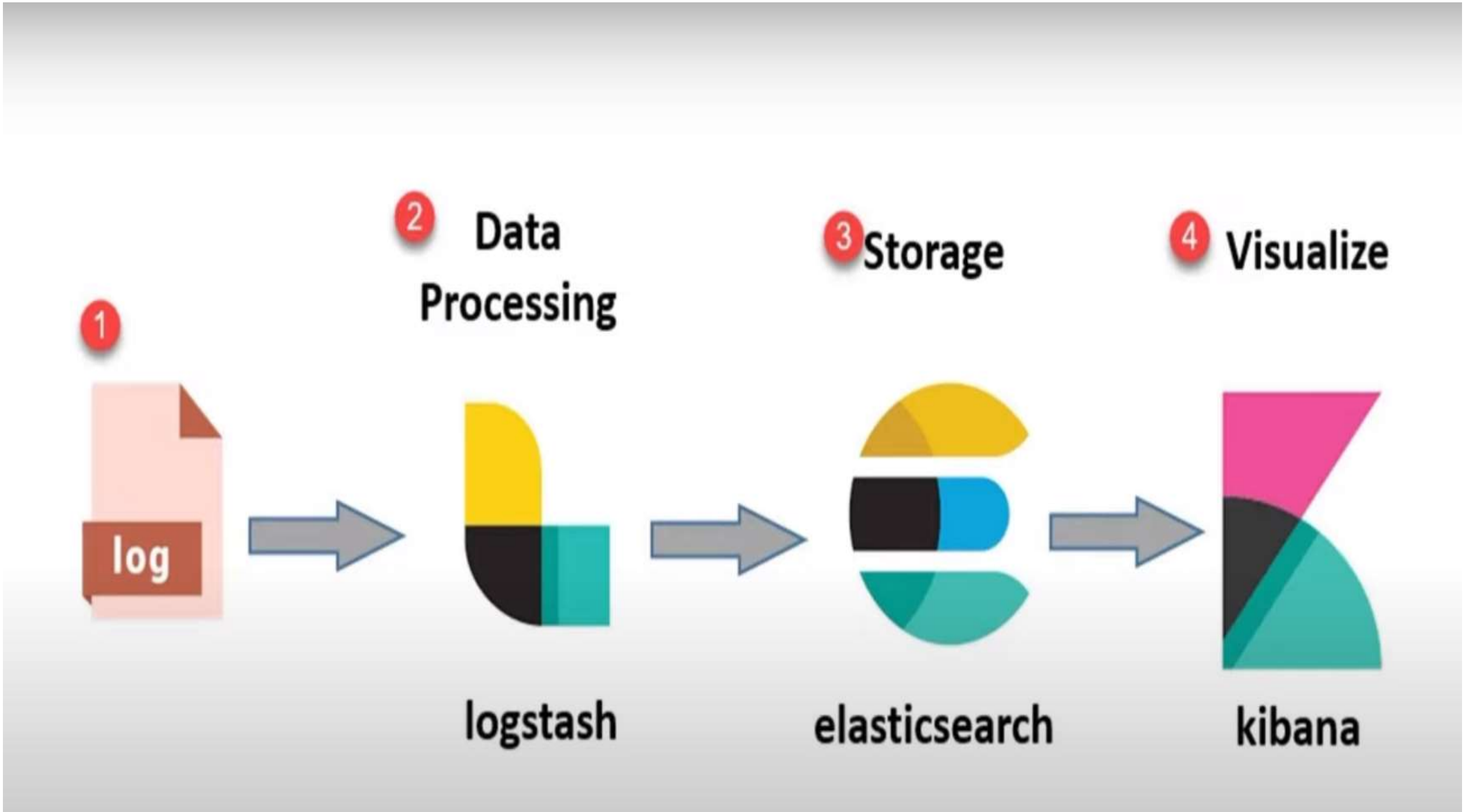

kibana
LOG
logstash
elasticsearch

Elasticsearch is a NoSQL database that is based on the Lucene search engine which will helps us to store inputs/logs

Logstash is a log pipeline tool that accepts inputs/logs from various sources, & exports the data to various targets



Kibana is a visualization UI layer , which will helps developer to monitor application logs


1
log
2
Data
Processing
logstash
3
Storage
elasticsearch
4
Visualize
kibana

What Is Elasticsearch?

- Real time distributed and analytics engine
- Open Source developed in Java
- Elasticsearch is based on the Lucene engine on top of which we have a rest interface.
- Supports full-text search i.e completely document based instead of tables and schemas
- Used for Single Page Application Projects

Why Elasticsearch?

Query

- Lets you perform and combine many types of searches like structured, unstructured, geo, metric etc.
- You can ask a query "anyway you want"

Analyze

- Lets you understand billions of log lines easily
- Provides aggregations which help you zoom out to explore trends and patterns in your data

Advantages Of Elasticsearch

Scalability

Really Fast

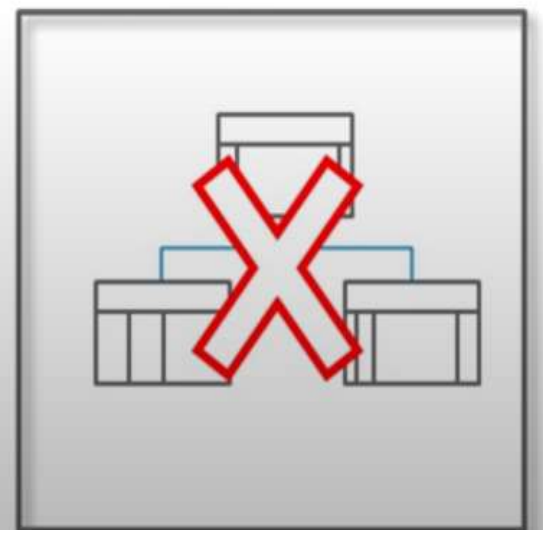
Multilingual

Advantages Of Elasticsearch

Document Oriented

Autocompletion & Instant Search

Schema Free



What Is ELK Stack: ElasticSearch

Companies Using ElasticSearch

guardian

GitHub

StumbleUpon

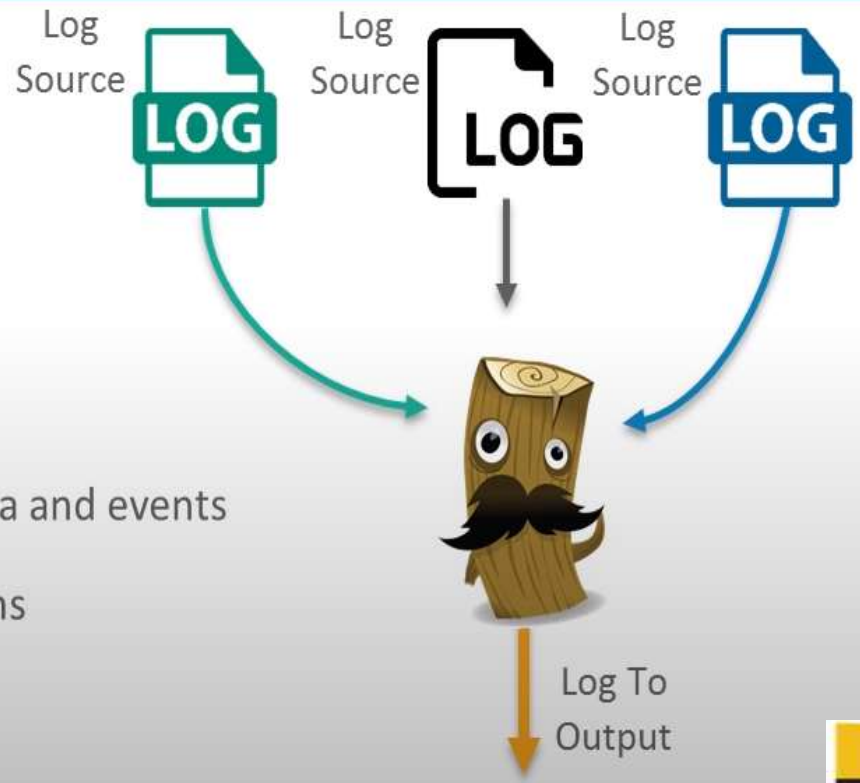
WIKIPEDIA
The Free Encyclopedia

SOUNDCLOUD

What Is ELK Stack: LogStash

Features

- ✓ Data pipeline tool
- ✓ Centralizes the data processing
- ✓ Collects, parses and analyzes large variety of structured/ unstructured data and events
- ✓ Provides plugins to connect to various types of input sources and platforms



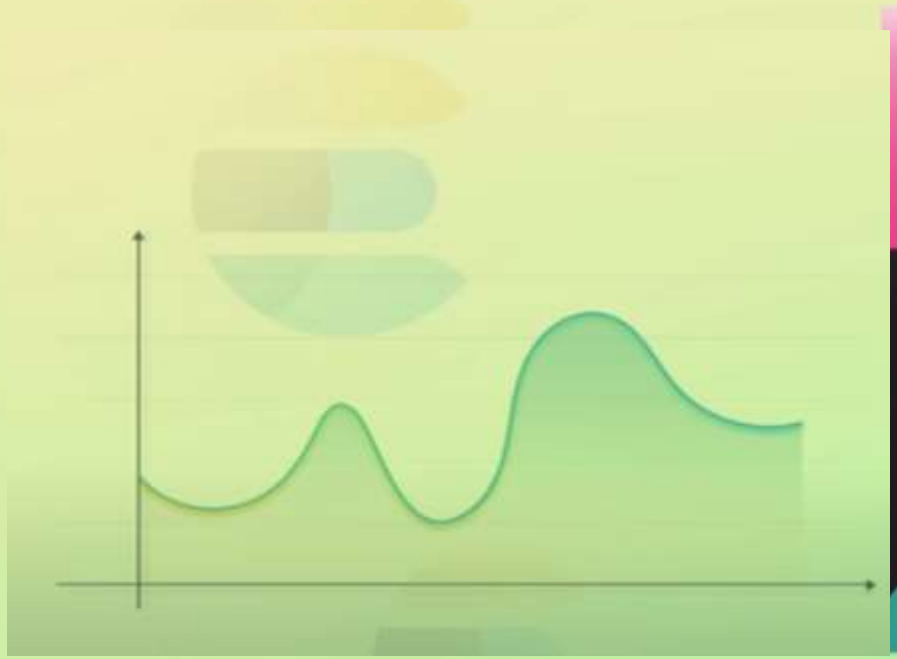
What Is ELK Stack: Kibana

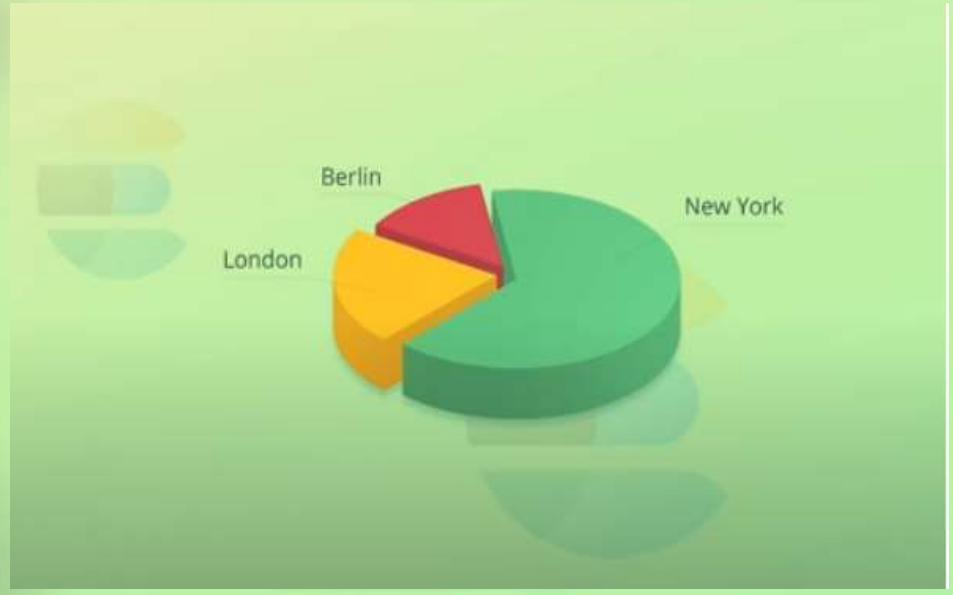
kibana

Features

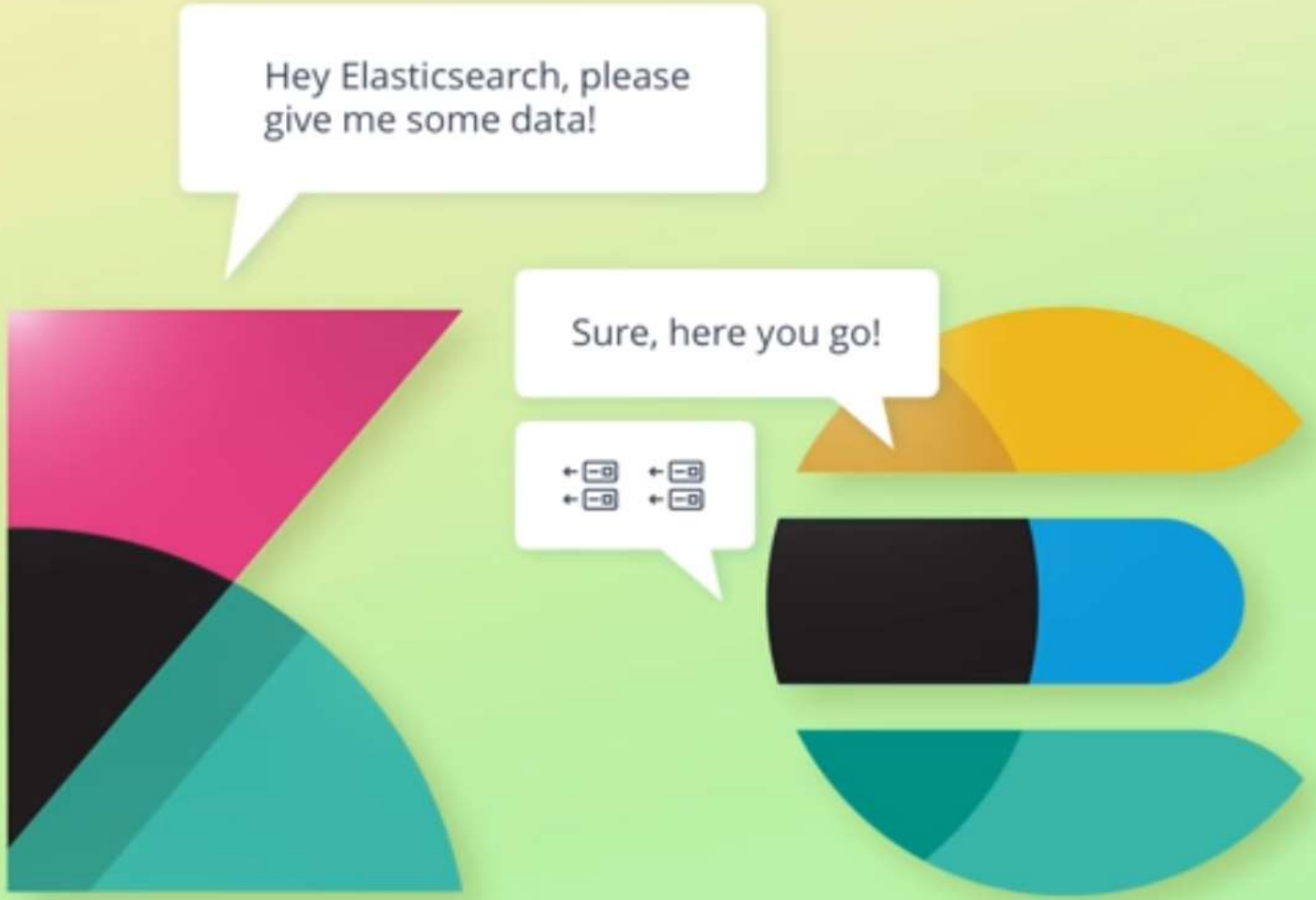
- ✓ Visualization tool
- ✓ provides real-time analysis, summarization, charting, and debugging capabilities.
- ✓ Provides instinctive and user friendly interface
- ✓ Allows sharing of snapshots of the logs searched through.
- ✓ Permits saving the dashboard and managing multiple dashboards

Kibana

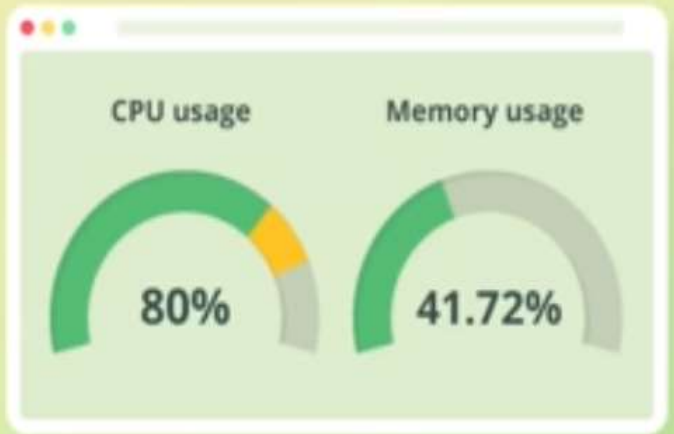




An analytics & visualization platform


Hey Elasticsearch, please give me some data!
Sure, here you go!

Dashboards



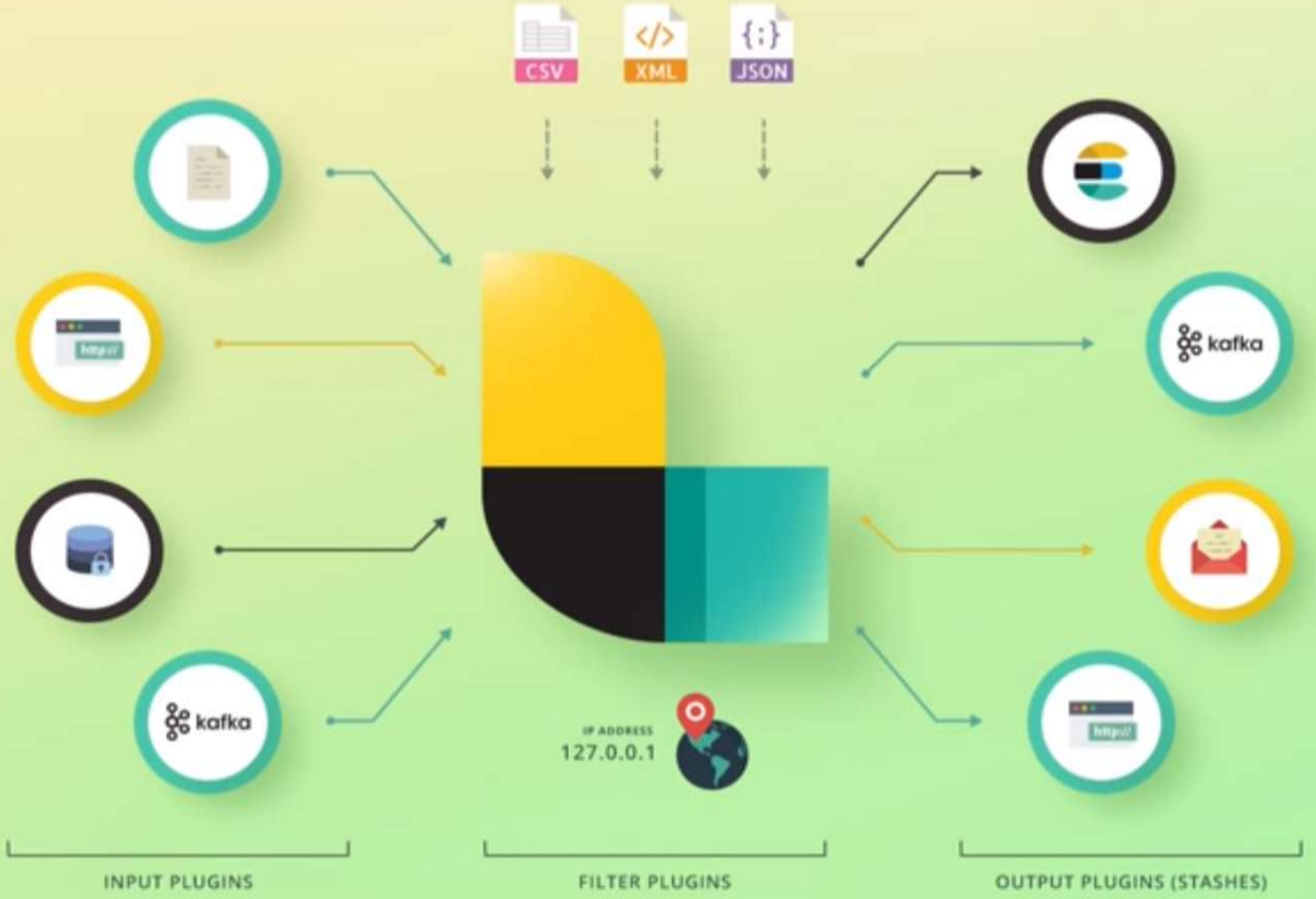
System administration

Developers

Management

Logstash

A data processing pipeline


CSV
XML
JSON
kafka
kafka
IP ADDRESS
127.0.0.1
INPUT PLUGINS
FILTER PLUGINS
OUTPUT PLUGINS (STASHES)

Example pipeline configuration

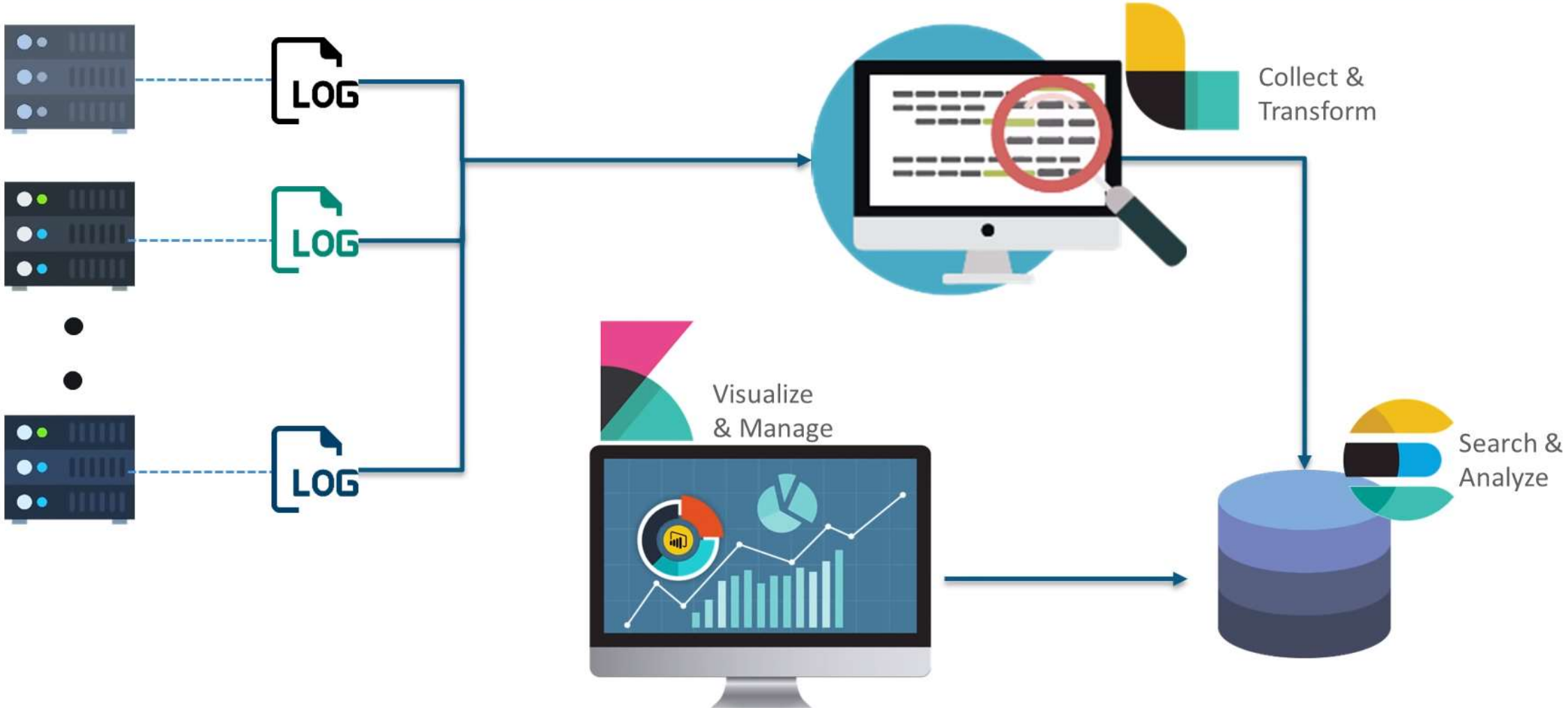
```
input {
    file {
        path => "/path/to/apache_access.log"
    }
}

filter {
    if [request] in ["/robots.txt", "/favicon.ico"] {
        drop { }
    }
}

output {
    file {
        path => "%{type}_%{+yyyy_MM_dd}.log"
    }
}
```


```
184.252.108.229 - joe [20/Sep/2017:13:22:22 +0200] "GET /products/view/123" 200 12798
```

184.252.108.229	-	joe	[20/Sep/2017:13:22:22 +0200]	GET	/products/view/123	200	12798

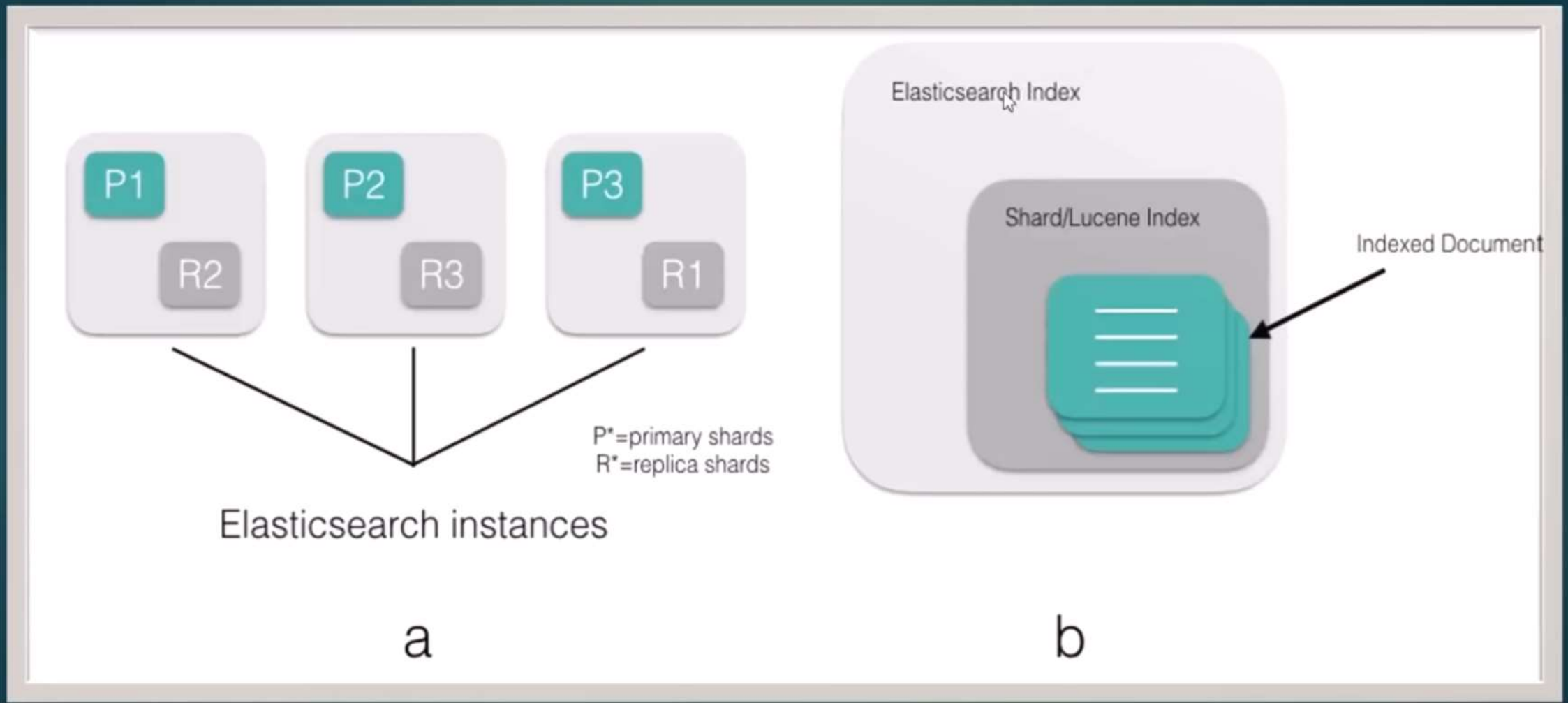
```
{
   "ip_address": "184.252.108.229",
   "user": "joe",
   "http_verb": "GET",
   "request_path": "/products/view/123",
   "http_status": 200,
   ...
}
```

How ELK Stack Works?

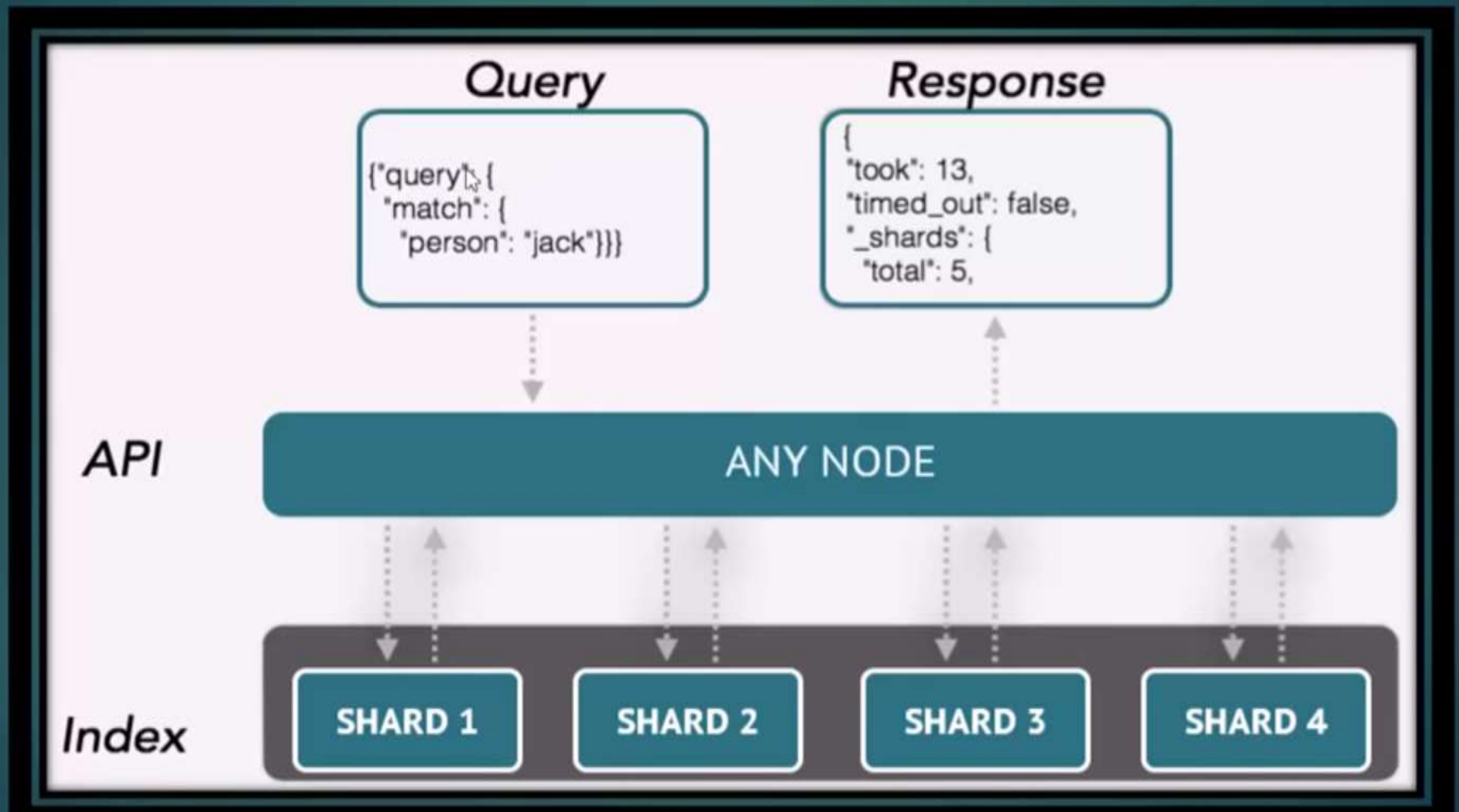


Spring boot - ELK

How Elasticsearch represents data ?



Flow Architecture



Basic Concepts

Near Real Time

Elasticsearch is a near real time search platform that is there is a slight from the time you index a document until the time it becomes searchable

Cluster

A cluster is a collection of one or more nodes that together holds the entire data. It provides federated indexing and search capabilities across all nodes and is identified by a unique name (by default it is '***elasticsearch***')

Node

A node is a single server which is a part of cluster, stores data and participates in the cluster's indexing and search capabilities

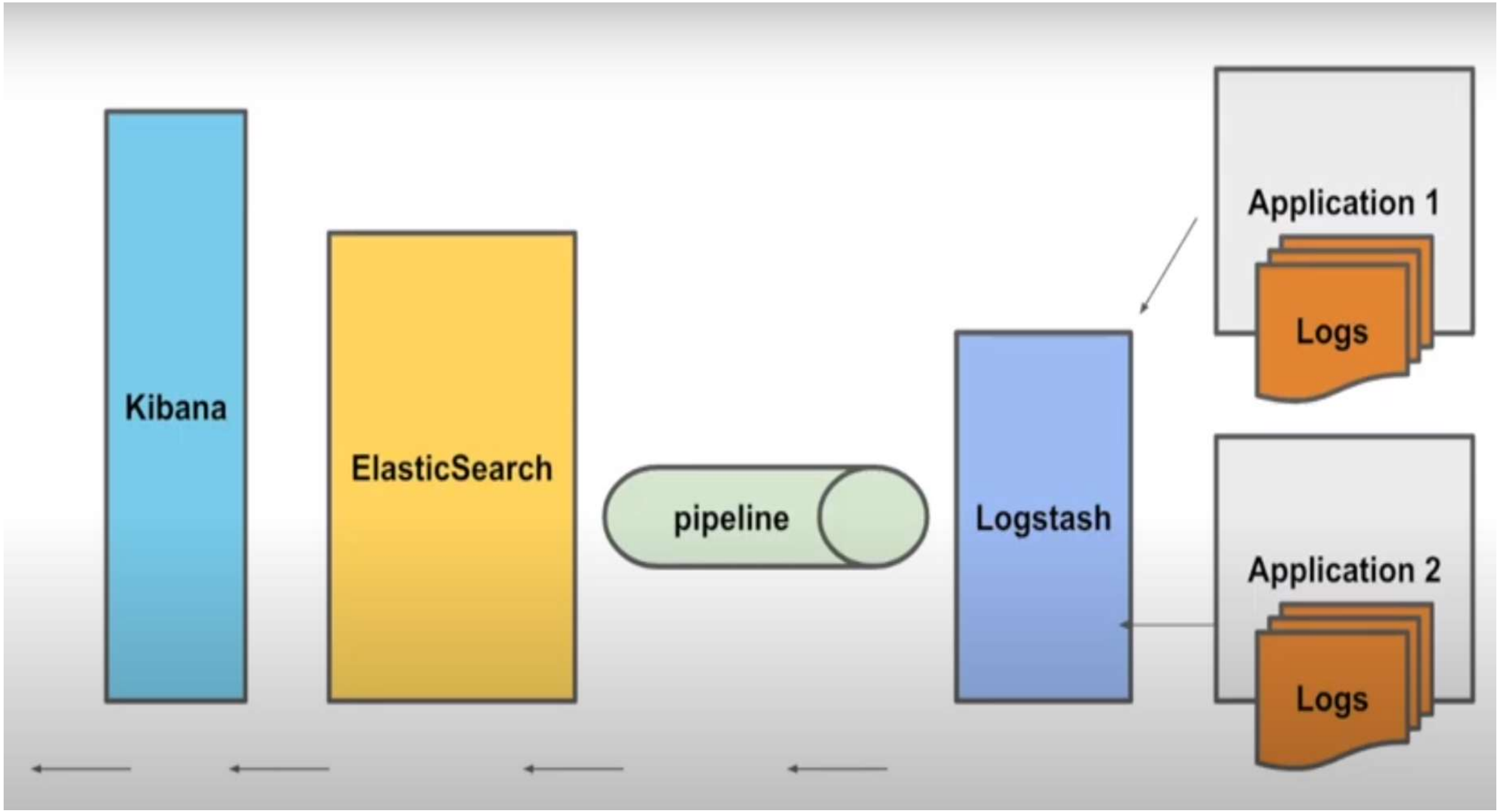
Basic Concepts

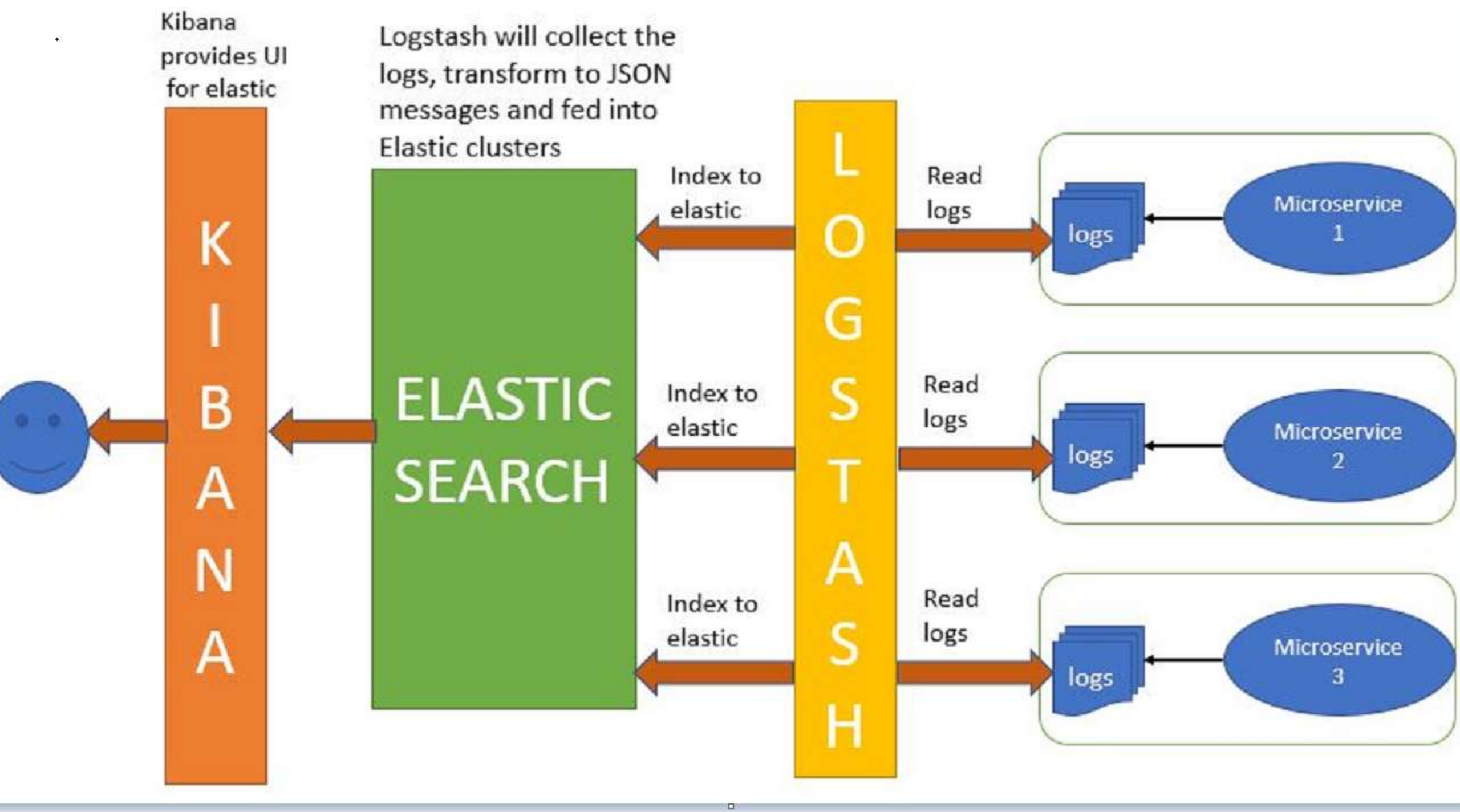
Index

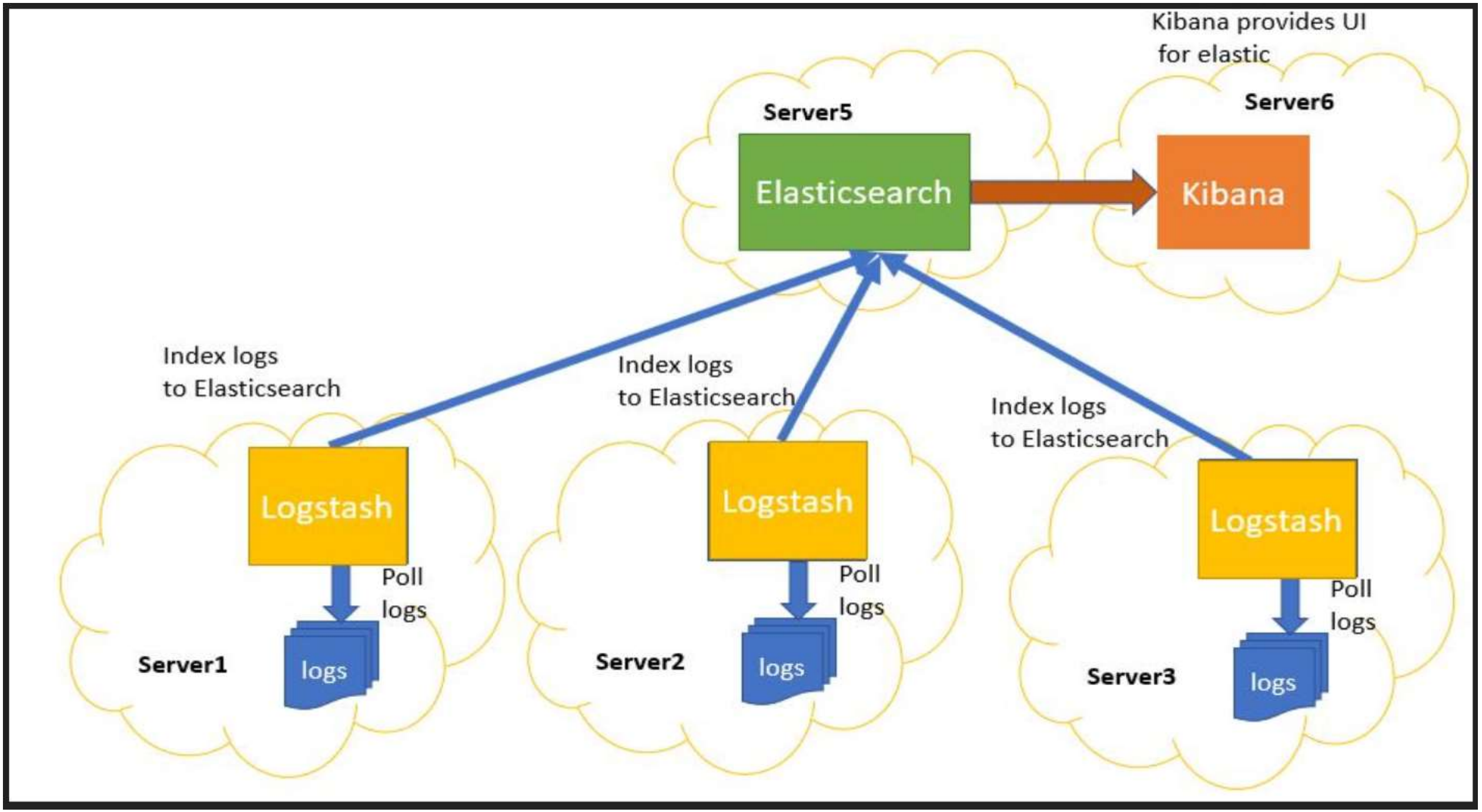
An index is a collection of documents with similar characteristics and is identified by a name. This name is used to refer to the index while performing indexing, search, update, and delete operations against the documents in it.

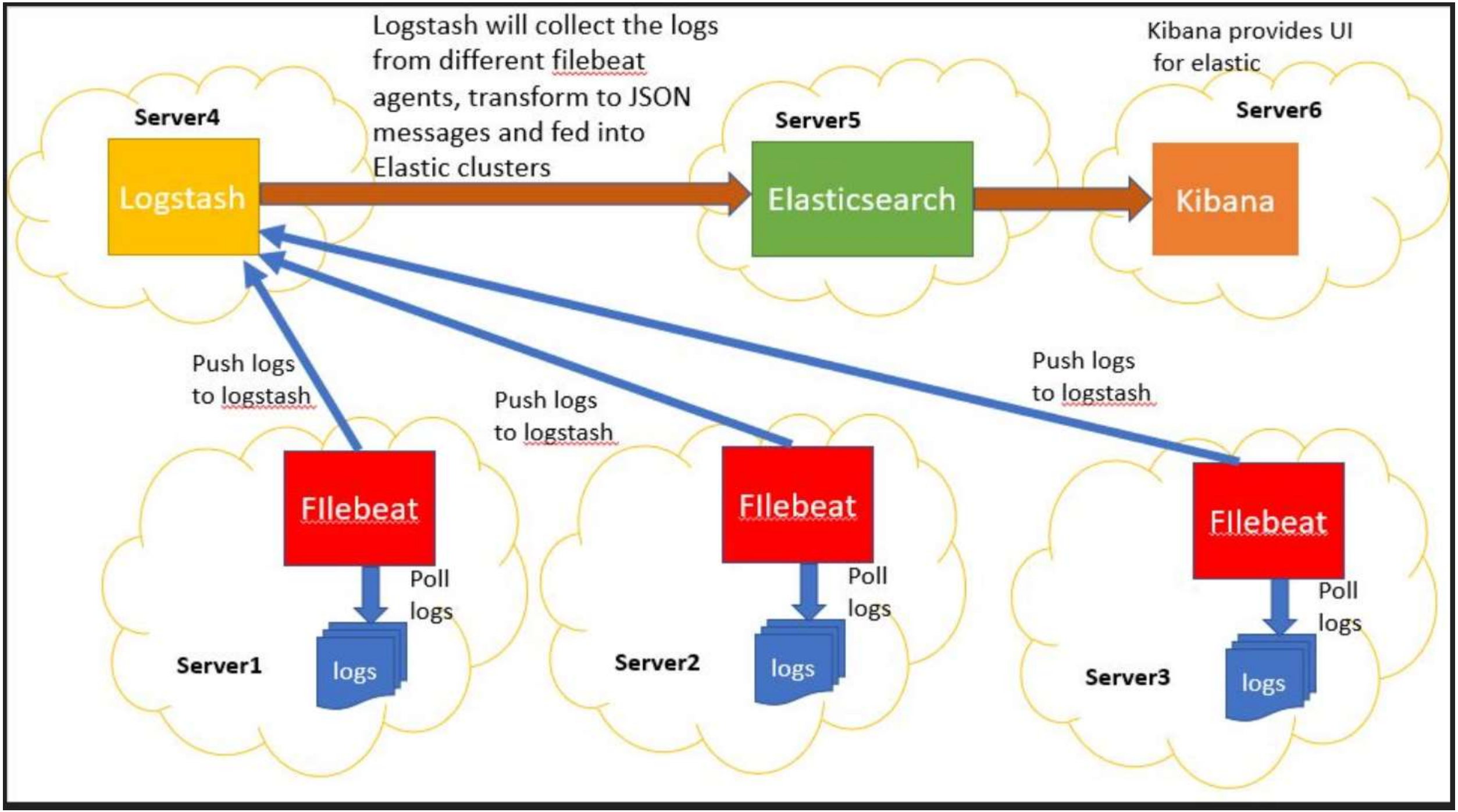
Type

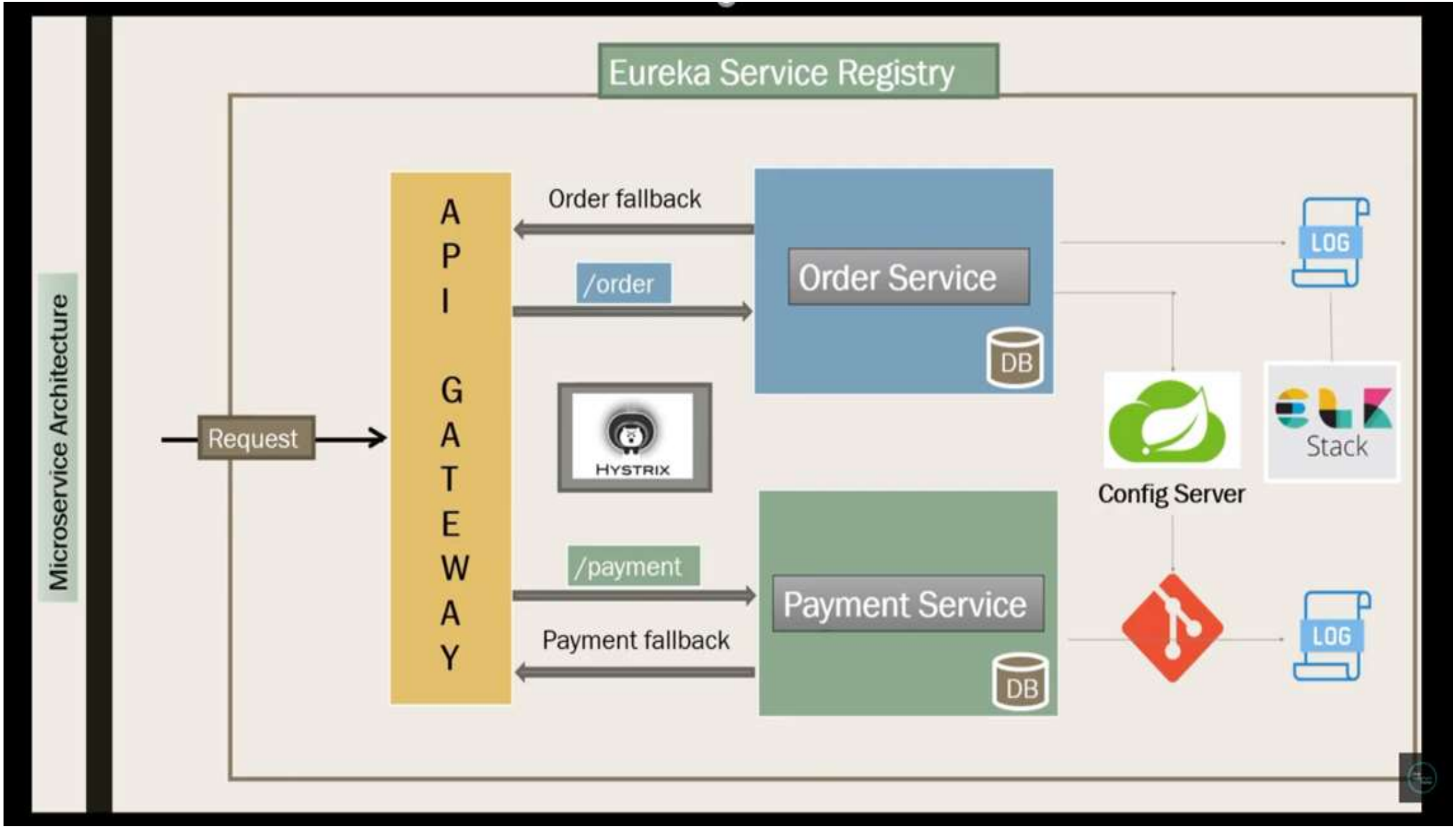
A type is a logical category/ partition of an index whose semantics is completely. It is defined for documents that have a set of common fields. You can define more than one type in your index


Kibana
ElasticSearch
pipeline
Logstash
Application 1
Logs
Application 2
Logs


Kibana provides UI for elastic
Logstash will collect the logs, transform to JSON messages and fed into Elastic clusters
KIBANA
ELASTIC SEARCH
LOGSTASH
Index to elastic
Index to elastic
Index to elastic
Read logs
Read logs
Read logs
logs
logs
logs
Microservice 1
Microservice 2
Microservice 3


Kibana provides UI
for elastic
Server5
Server6
Elasticsearch
Kibana
Index logs
to Elasticsearch
Index logs
to Elasticsearch
Index logs
to Elasticsearch
Logstash
Logstash
Logstash
Poll
logs
Poll
logs
Poll
logs
Server1
Server2
Server3
logs
logs
logs


Logstash will collect the logs from different filebeat agents, transform to JSON messages and fed into Elastic clusters
Kibana provides UI for elastic
Server4
Logstash
Server5
Elasticsearch
Server6
Kibana
Push logs to logstash
Push logs to logstash
Push logs to logstash
FIlebeat
Poll logs
logs
Server1
FIlebeat
Poll logs
logs
Server2
FIlebeat
Poll logs
logs
Server3


Microservice Architecture
Eureka Service Registry
Request
API GATEWAY
Order fallback
/order
HYSTRIX
/payment
Payment fallback
Order Service
DB
Payment Service
DB
LOG
Stack
Config Server
LOG

ElasticSearch

- https://www.elastic.co/downloads/elasticsearch

Logstash

- https://www.elastic.co/downloads/logstash

Kibana

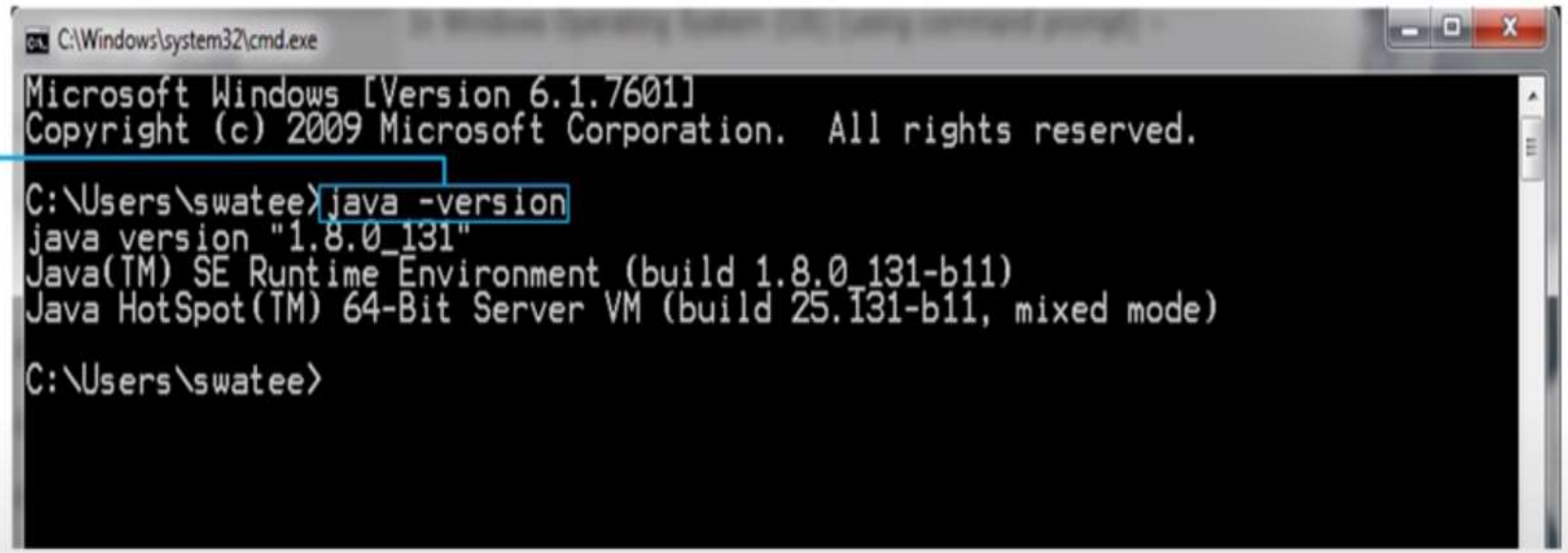
- https://www.elastic.co/downloads/kibana

Installation

Install the latest Java version.

OR

If you already have Java Installed then check for its version using **java -version** command in cmd

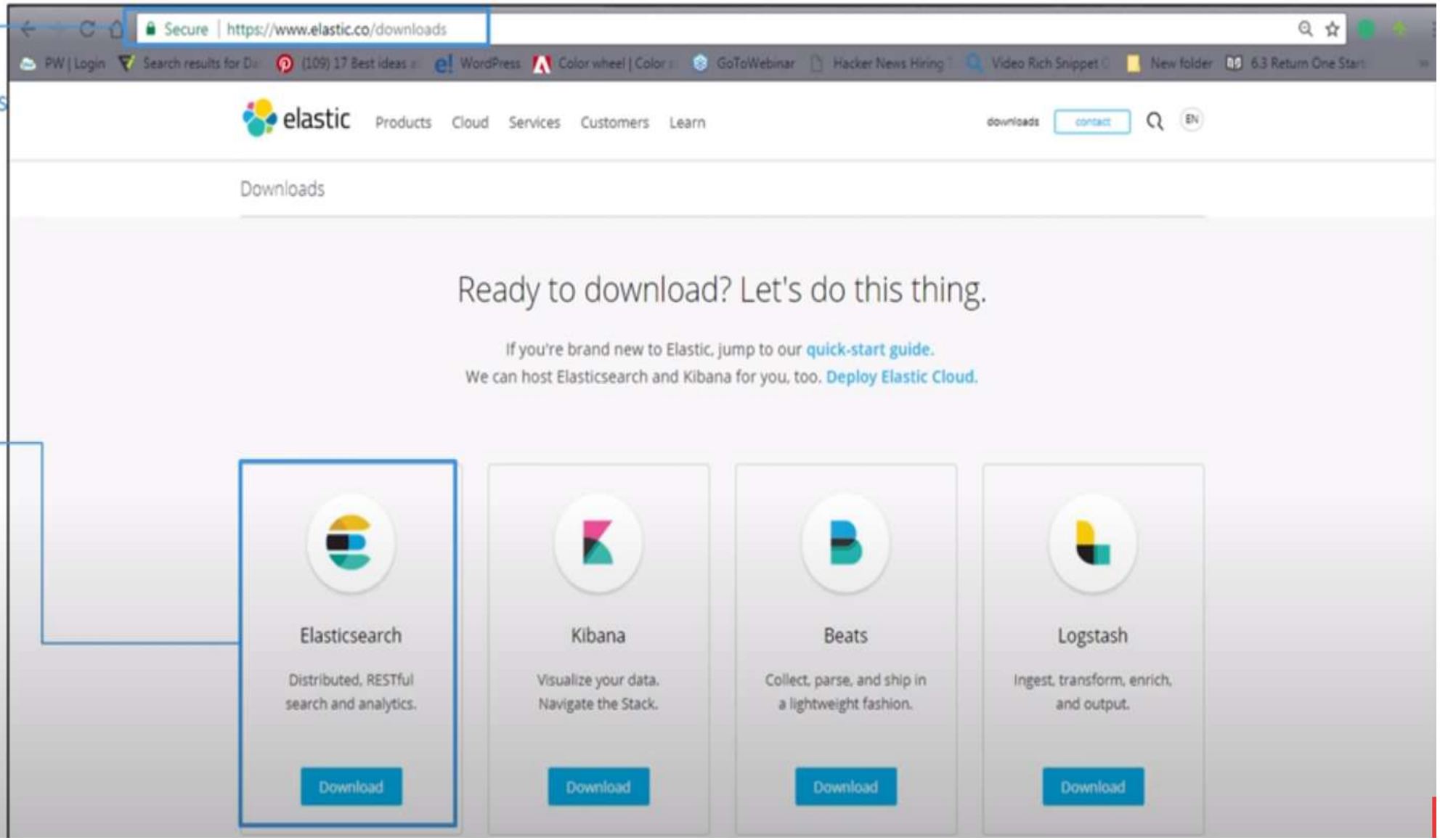


NOTE: Java version must be 7 or more

Installation

2

Go to
https://www.elastic.co/downloads



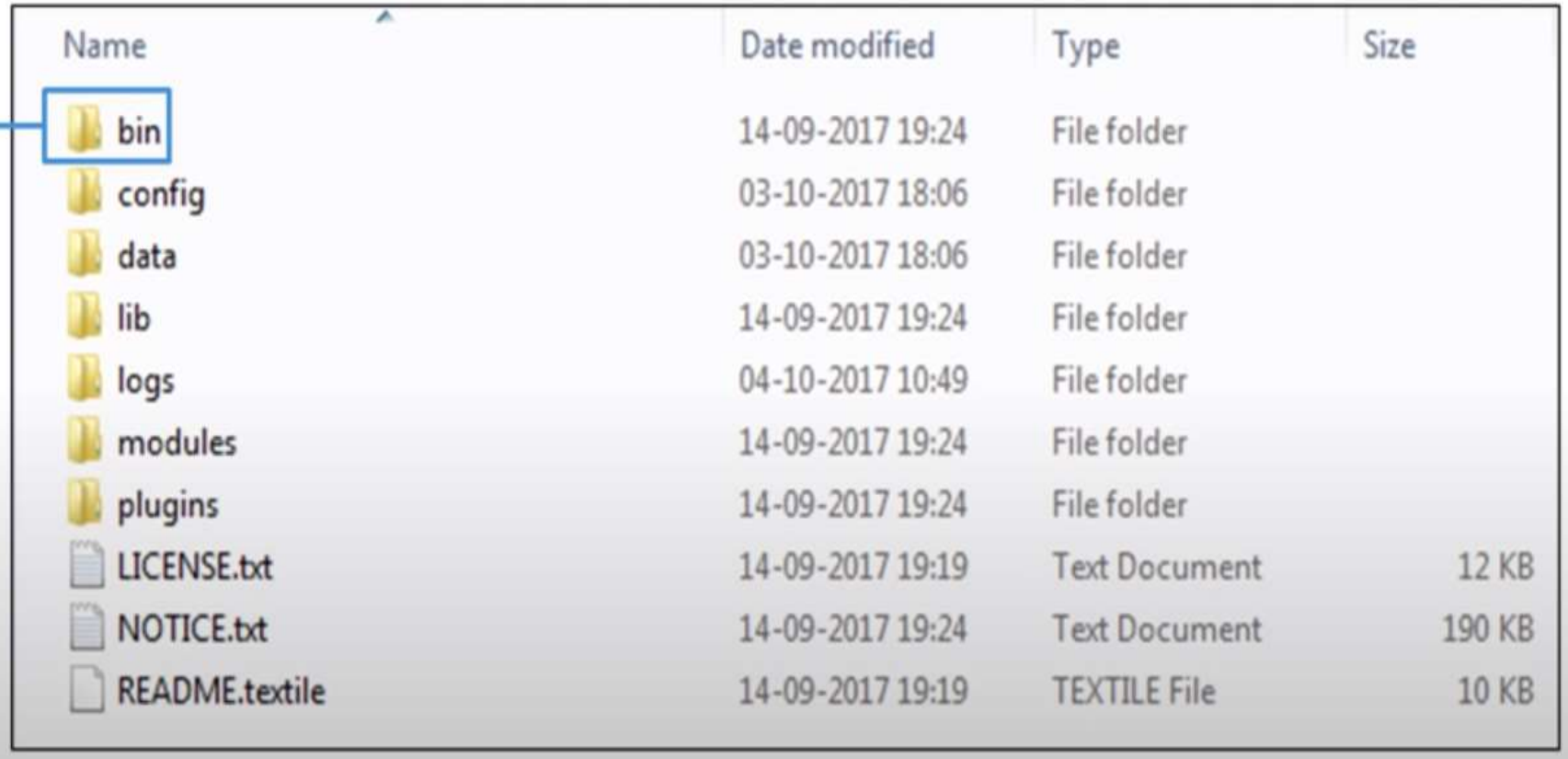
3

Click on Download
to get the zip file

Installation

4 Unzip the file

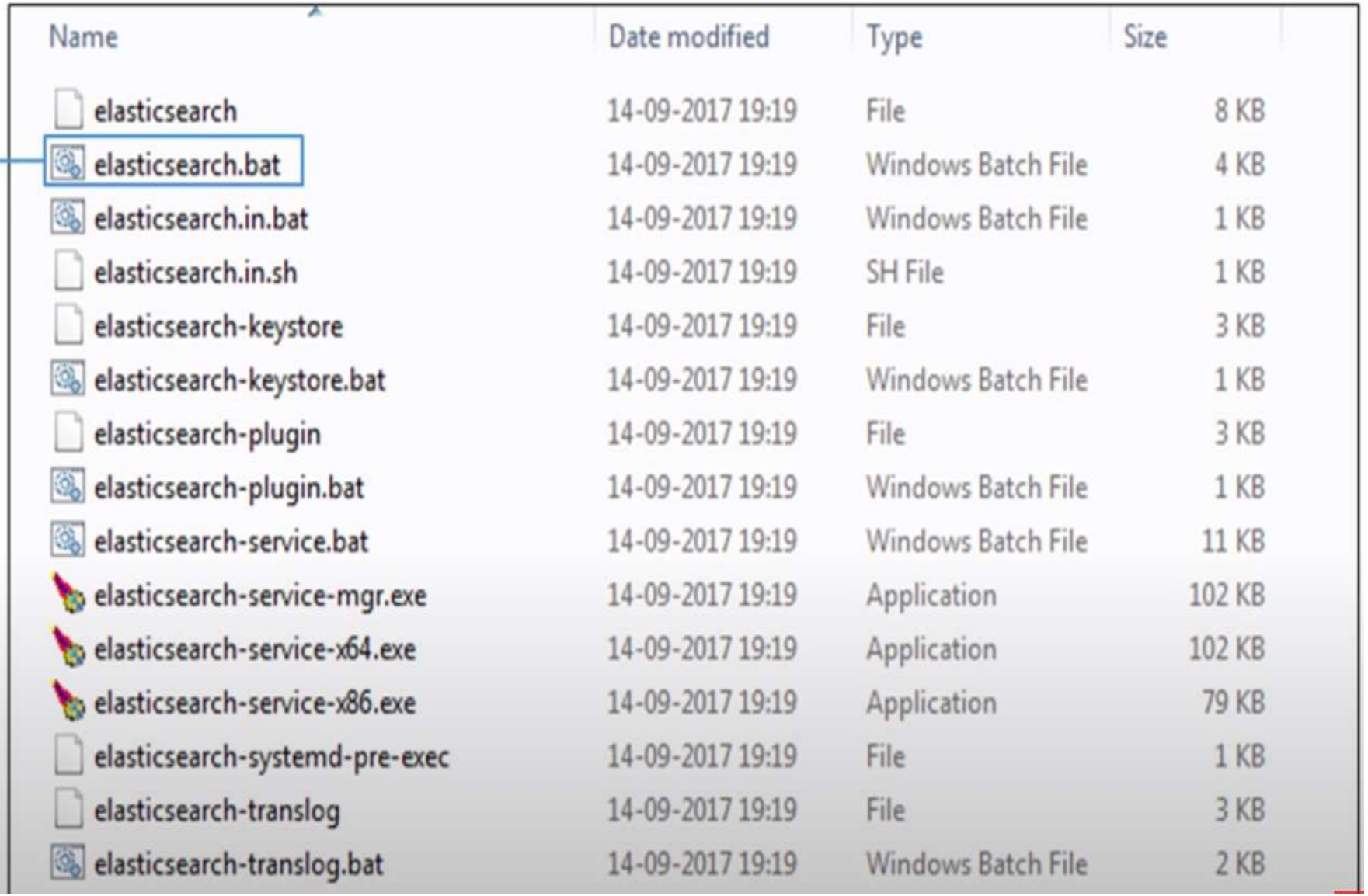
5 Go to **bin** folder



Installation

6

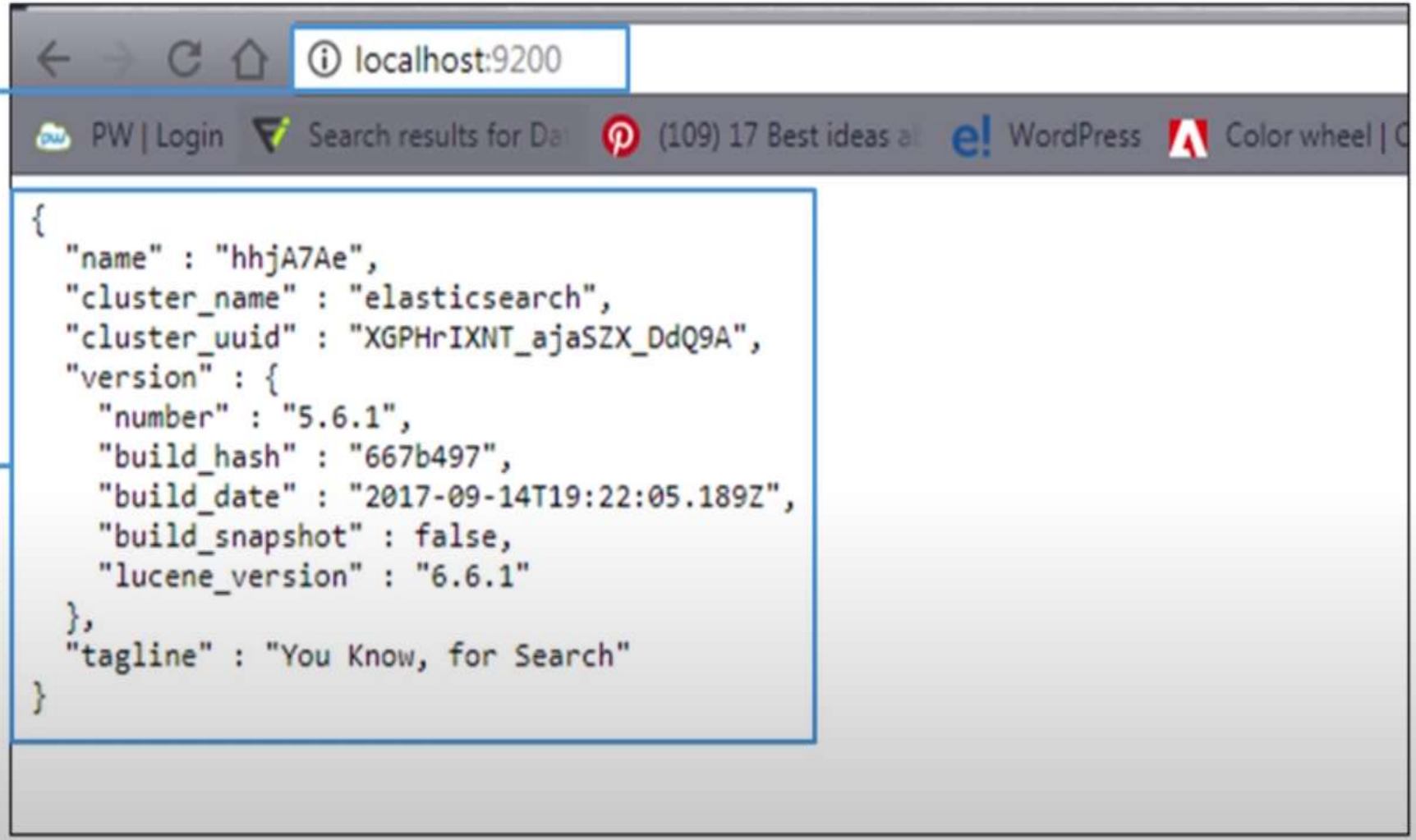
Double click on `elasticsearch.bat` file



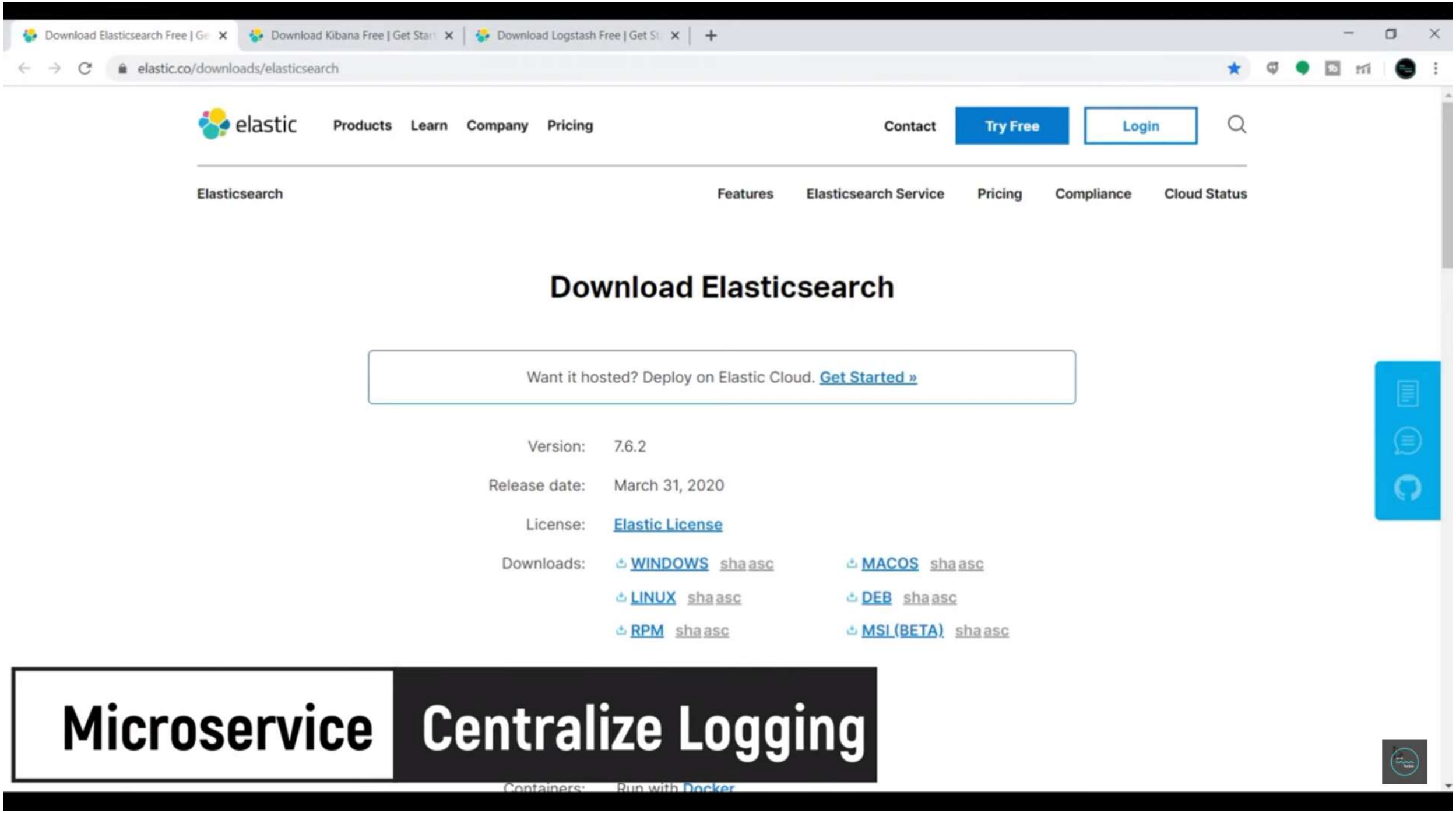
Name	Date modified	Type	Size
elasticsearch	14-09-2017 19:19	File	8 KB
elasticsearch.bat	14-09-2017 19:19	Windows Batch File	4 KB
elasticsearch.in.bat	14-09-2017 19:19	Windows Batch File	1 KB
elasticsearch.in.sh	14-09-2017 19:19	SH File	1 KB
elasticsearch-keystore	14-09-2017 19:19	File	3 KB
elasticsearch-keystore.bat	14-09-2017 19:19	Windows Batch File	1 KB
elasticsearch-plugin	14-09-2017 19:19	File	3 KB
elasticsearch-plugin.bat	14-09-2017 19:19	Windows Batch File	1 KB
elasticsearch-service.bat	14-09-2017 19:19	Windows Batch File	11 KB
elasticsearch-service-mgr.exe	14-09-2017 19:19	Application	102 KB
elasticsearch-service-x64.exe	14-09-2017 19:19	Application	102 KB
elasticsearch-service-x86.exe	14-09-2017 19:19	Application	79 KB
elasticsearch-systemd-pre-exec	14-09-2017 19:19	File	1 KB
elasticsearch-translog	14-09-2017 19:19	File	3 KB
elasticsearch-translog.bat	14-09-2017 19:19	Windows Batch File	2 KB

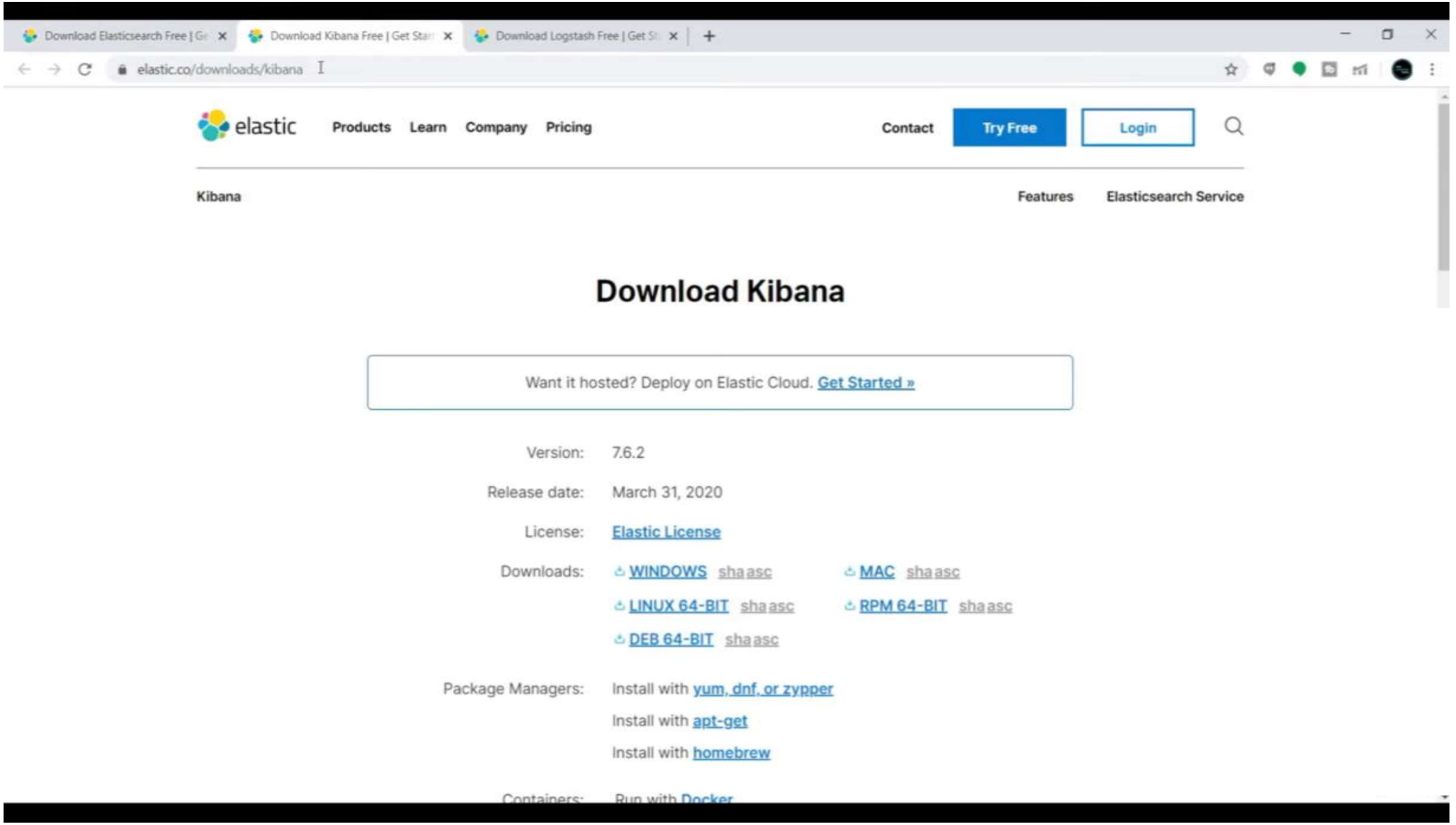
Installation

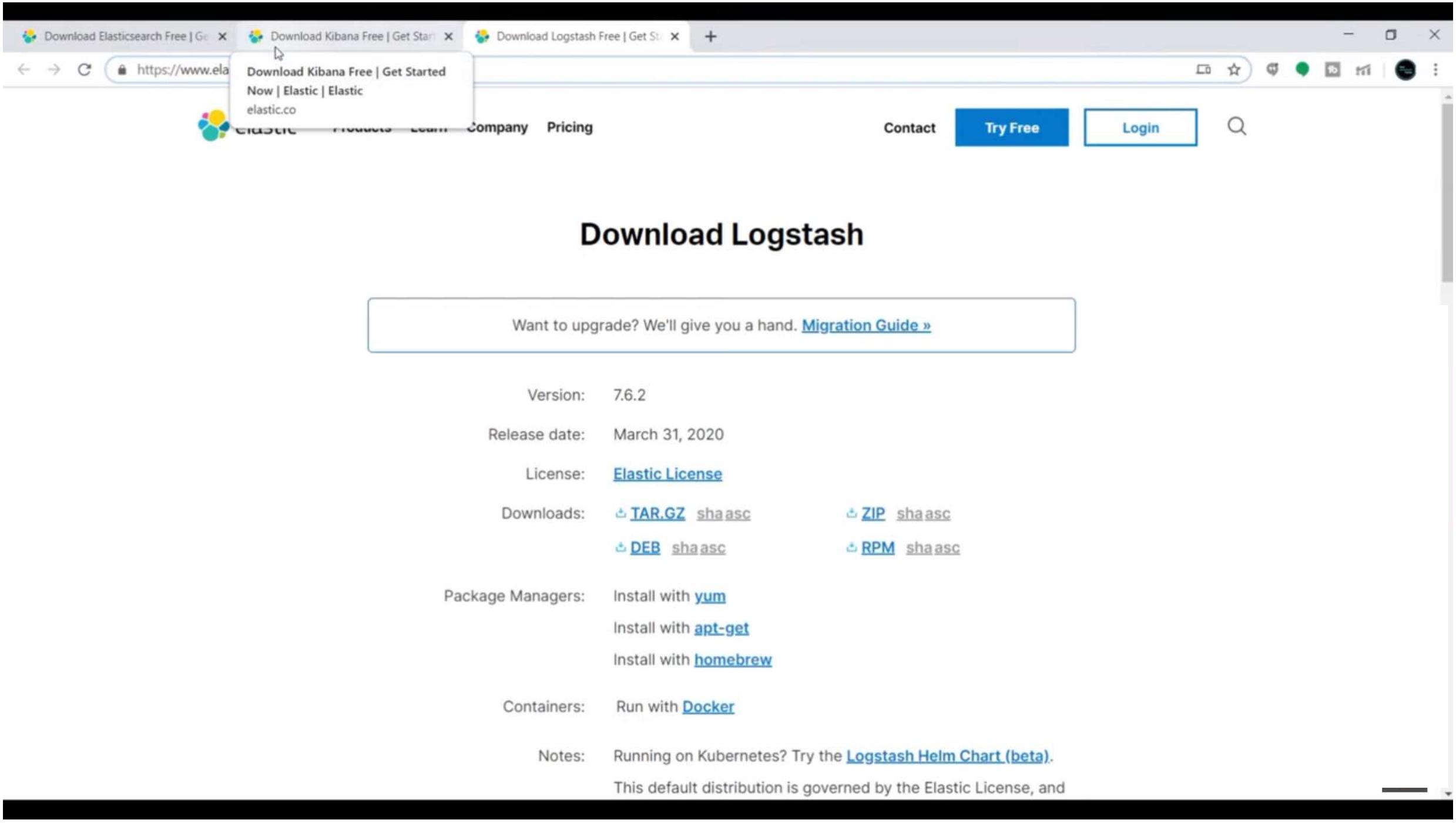
8 Open a browser and type **localhost:9200**



9 If you can see this message on the browser that means your Elasticsearch is up and running


Download Elasticsearch Free | Ge
Download Kibana Free | Get Star
Download Logstash Free | Get St
elastic.co/downloads/elasticsearch
elastic
Products
Learn
Company
Pricing
Contact
Try Free
Login
Elasticsearch
Features
Elasticsearch Service
Pricing
Compliance
Cloud Status
Download Elasticsearch
Want it hosted? Deploy on Elastic Cloud. Get Started »
Version: 7.6.2
Release date: March 31, 2020
License: Elastic License
Downloads:
WINDOWS sha asc
MACOS sha asc
LINUX sha asc
DEB sha asc
RPM sha asc
MSI (BETA) sha asc
Containers: Run with Docker
Microservice
Centralize Logging


Download Elasticsearch Free | Ge
Download Kibana Free | Get Star
Download Logstash Free | Get St
elastic.co/downloads/kibana
elastic
Products
Learn
Company
Pricing
Contact
Try Free
Login
Kibana
Features
Elasticsearch Service
Download Kibana
Want it hosted? Deploy on Elastic Cloud. Get Started »
Version: 7.6.2
Release date: March 31, 2020
License: Elastic License
Downloads: WINDOWS sha asc
MAC sha asc
LINUX 64-BIT sha asc
RPM 64-BIT sha asc
DEB 64-BIT sha asc
Package Managers: Install with yum, dnf, or zypper
Install with apt-get
Install with homebrew
Containers: Run with Docker

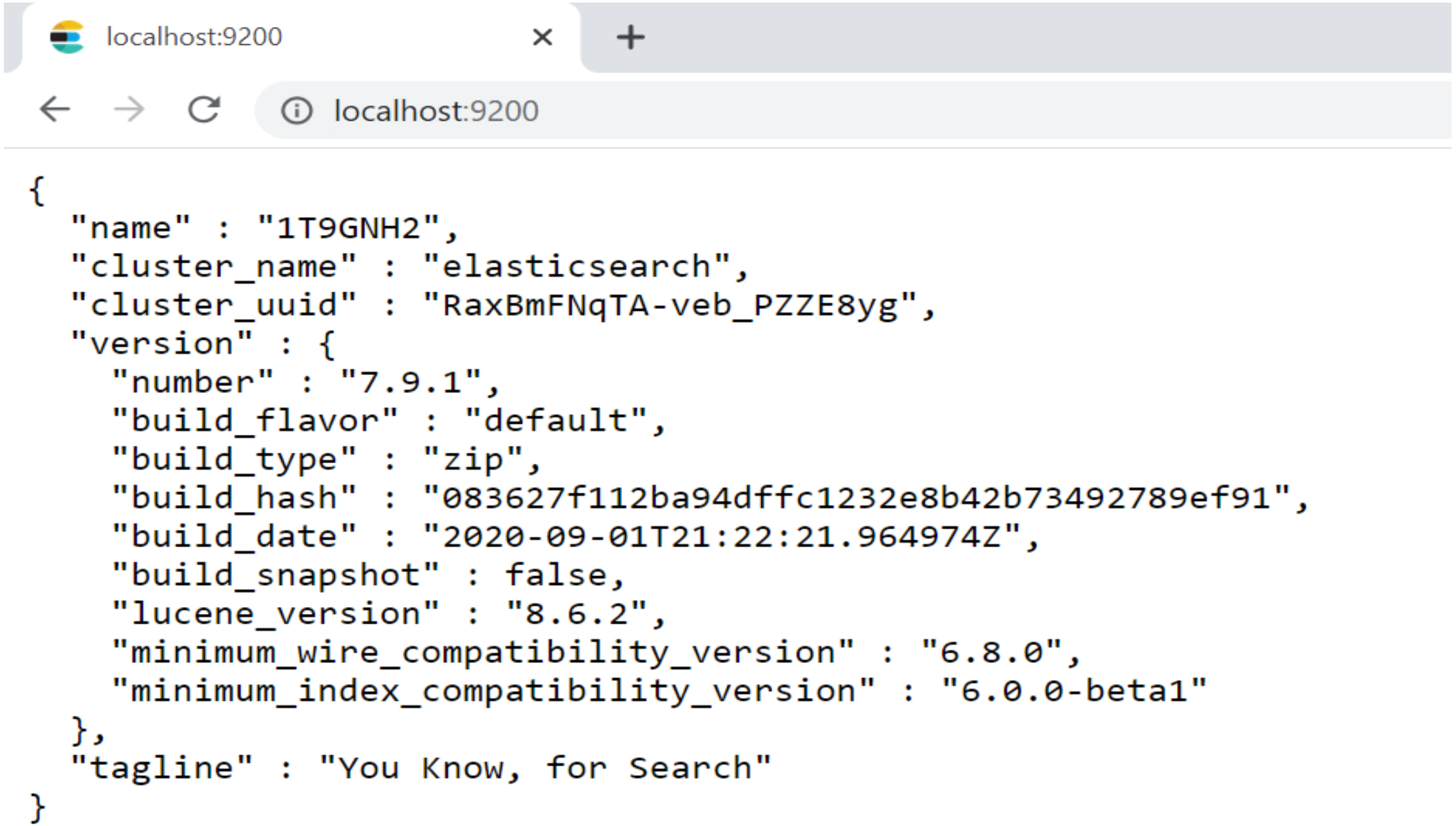

Download Elasticsearch Free | Ge
Download Kibana Free | Get Start
Download Logstash Free | Get St
Download Kibana Free | Get Started Now | Elastic | Elastic
elastic.co
https://www.ela
Company
Pricing
Contact
Try Free
Login
Download Logstash
Want to upgrade? We'll give you a hand. Migration Guide »
Version: 7.6.2
Release date: March 31, 2020
License: Elastic License
Downloads: TAR.GZ sha asc ZIP sha asc
DEB sha asc RPM sha asc
Package Managers: Install with yum
Install with apt-get
Install with homebrew
Containers: Run with Docker
Notes: Running on Kubernetes? Try the Logstash Helm Chart (beta).
This default distribution is governed by the Elastic License, and

Elastic Search Configuration

Select C:\Windows\System32\cmd.exe - elasticsearch

```
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Training\springboot\kibana\elasticsearch-7.9.1-windows-x86_64\elasticsearch-7.9.1\bin>elasticsearch
future versions of Elasticsearch will require Java 11; your Java version from [C:\Program Files\Java\jdk1.8.0_181\jre] d
oes not meet this requirement
future versions of Elasticsearch will require Java 11; your Java version from [C:\Program Files\Java\jdk1.8.0_181\jre] d
oes not meet this requirement
Warning: with JDK 8 on Windows, Elasticsearch may be unable to derive correct
  ergonomic settings due to a JDK issue (JDK-8074459). Please use a newer
  version of Java.
Warning: MaxDirectMemorySize may have been miscalculated due to JDK-8074459.
  Please use a newer version of Java or set MaxDirectMemorySize explicitly.
[2020-09-21T12:27:35,879][INFO ][o.e.n.Node               ] [1T9GNH2] version[7.9.1], pid[828], build[default/zip/083627
f112ba94dffc1232e8b42b73492789ef91/2020-09-01T21:22:21.964974Z], OS[Windows 10/10.0/amd64], JVM[Oracle Corporation/Java
HotSpot(TM) 64-Bit Server VM/1.8.0_181/25.181-b13]
[2020-09-21T12:27:35,883][INFO ][o.e.n.Node               ] [1T9GNH2] JVM home [C:\Program Files\Java\jdk1.8.0_181\jre]
[2020-09-21T12:27:35,905][INFO ][o.e.n.Node               ] [1T9GNH2] JVM arguments [-Des.networkaddress.cache.ttl=60, -
Des.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8,
-Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.n
etty.recycler.maxCapacityPerThread=0, -Dio.netty.allocator.numDirectArenas=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j
2.disable.jmx=true, -Djava.locale.providers=SPI,JRE, -Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancy
Fraction=75, -XX:+UseCMSInitiatingOccupancyOnly, -Djava.io.tmpdir=C:\Users\vg672483\AppData\Local\Temp\elasticsearch, -X
X:+HeapDumpOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_err_pid%p.log, -XX:+PrintGCDetails, -XX:+Pri
ntGCDateStamps, -XX:+PrintTenuringDistribution, -XX:+PrintGCApplicationStoppedTime, -Xloggc:logs/gc.log, -XX:+UseGCLogFi
leRotation, -XX:NumberOfGCLogFiles=32, -XX:GCLogFileSize=64m, -XX:MaxDirectMemorySize=536870912, -Delasticsearch, -Des.p
ath.home=C:\Training\springboot\kibana\elasticsearch-7.9.1-windows-x86_64\elasticsearch-7.9.1, -Des.path.conf=C:\Trainin
g\springboot\kibana\elasticsearch-7.9.1-windows-x86_64\elasticsearch-7.9.1\config, -Des.distribution.flavor=default, -De
dresses {127.0.0.1:9200}, {[::1]:9200}
[2020-09-21T12:28:10,648][INFO ][o.e.n.Node               ] [1T9GNH2] started
```

Elastic Search Configuration



Kibana Configuration

change.log | kibana.yml

```
# Specifies the address to which the Kibana server will bind. IP addresses and host names are
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
#server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# The maximum payload size in bytes for incoming server requests.
#server.maxPayloadBytes: 1048576

# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
#elasticsearch.preserveHost: true
```

Kibana Execution

```
C:\Training\springboot\kibana\kibana-7.9.1-windows-x86_64\bin>kibana.bat
  log   [07:40:36.050] [warning][plugins-discovery] Expect plugin "id" in camelCase, but found: beats_management
  log   [07:40:36.095] [warning][plugins-discovery] Expect plugin "id" in camelCase, but found: triggers_actions_ui
  log   [07:41:05.976] [info][plugins-service] Plugin "visTypeXy" is disabled.
ted saved objects attributes after restart, please set xpack.encryptedSavedObjects.encryptionKey in kibana.yml
  log   [07:42:57.833] [warning][ingestManager][plugins] Fleet APIs are disabled due to the Encrypted Saved Objects plugin using an ephemeral encryption key. Please set xpa
ck.encryptedSavedObjects.encryptionKey in kibana.yml.
  log   [07:42:57.955] [warning][actions][actions][plugins] APIs are disabled due to the Encrypted Saved Objects plugin using an ephemeral encryption key. Please set xpack.
encryptedSavedObjects.encryptionKey in kibana.yml.
  log   [07:42:57.990] [warning][alerting][alerts][plugins][plugins] APIs are disabled due to the Encrypted Saved Objects plugin using an ephemeral encryption key. Please s
et xpack.encryptedSavedObjects.encryptionKey in kibana.yml.
  log   [07:42:58.183] [info][monitoring][monitoring][plugins] config sourced from: production cluster
  log   [07:42:58.638] [info][savedobjects-service] Waiting until all Elasticsearch nodes are compatible with Kibana before starting saved objects migrations...
  log   [07:42:58.639] [info][savedobjects-service] Starting saved objects migrations
  log   [07:42:58.703] [info][savedobjects-service] Creating index .kibana_task_manager_1.
  log   [07:42:59.384] [info][savedobjects-service] Pointing alias .kibana_task_manager to .kibana_task_manager_1.
  log   [07:42:59.525] [info][savedobjects-service] Finished in 823ms.
  log   [07:42:59.572] [info][plugins-system] Starting [92] plugins: [taskManager,licensing,observability,globalSearch,globalSearchProviders,code,usageCollection,ossTelemet
ry,kibanaUsageCollection,telemetryCollectionManager,telemetry,telemetryCollectionXpack,newsfeed,mapsLegacy,kibanaLegacy,translations,legacyExport,timelion,share,esUiShared,
charts,bfetch,expressions,data,home,cloud,console,consoleExtensions,apmOss,searchprofiler,painlessLab,grokdebugger,management,upgradeAssistant,licenseManagement,watcher,ind
exPatternManagement,advancedSettings,fileUpload,dataEnhanced,savedObjects,visualizations,visTypeVislib,visTypeVega,visTypeTimeseries,visTypeTimelion,features,security,snaps
hotRestore,reporting,enterpriseSearch,encryptedSavedObjects,ingestManager,indexManagement,rollup,remoteClusters,crossClusterReplication,indexLifecycleManagement,beats_manag
ement,transform,ingestPipelines,maps,graph,canvas,visTypeTagcloud,visTypeTable,visTypeMetric,visTypeMarkdown,visualize,tileMap,regionMap,inputControlVis,discover,discoverEn
hanced,dashboard,lens,dashboardMode,savedObjectsManagement,spaces,lists,eventLog,actions,case,alerts,alertingBuiltins,ml,securitySolution,infra,monitoring,logstash,apm,upti
me]
  log   [07:42:59.576] [info][plugins][taskManager][taskManager] TaskManager is identified by the Kibana UUID: d4bb979b-4b3d-467c-b678-de76f3e79b30
  log   [07:42:59.649] [info][plugins][watcher] Your basic license does not support watcher. Please upgrade your license.
  log   [07:42:59.651] [info][crossClusterReplication][plugins] Your basic license does not support crossClusterReplication. Please upgrade your license.
  log   [07:42:59.668] [info][kibana-monitoring][monitoring][monitoring][plugins] Starting monitoring stats collection
  log   [07:43:07.260] [info][status][plugin:kibana@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.279] [info][status][plugin:elasticsearch@7.9.1] Status changed from uninitialized to yellow - Waiting for Elasticsearch
  log   [07:43:07.281] [info][status][plugin:elasticsearch@7.9.1] Status changed from yellow to green - Ready
  log   [07:43:07.288] [info][status][plugin:xpack_main@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.313] [info][status][plugin:monitoring@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.320] [info][status][plugin:spaces@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.325] [info][status][plugin:security@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.332] [info][status][plugin:beats_management@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.449] [info][status][plugin:apm_oss@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.473] [info][status][plugin:console_legacy@7.9.1] Status changed from uninitialized to green - Ready
  log   [07:43:07.499] [info][listening] Server running at http://localhost:5601
  log   [07:43:08.996] [info][server][Kibana][http] http server running at http://localhost:5601
```

localhost:5601/app/home#/

Welcome to Elastic

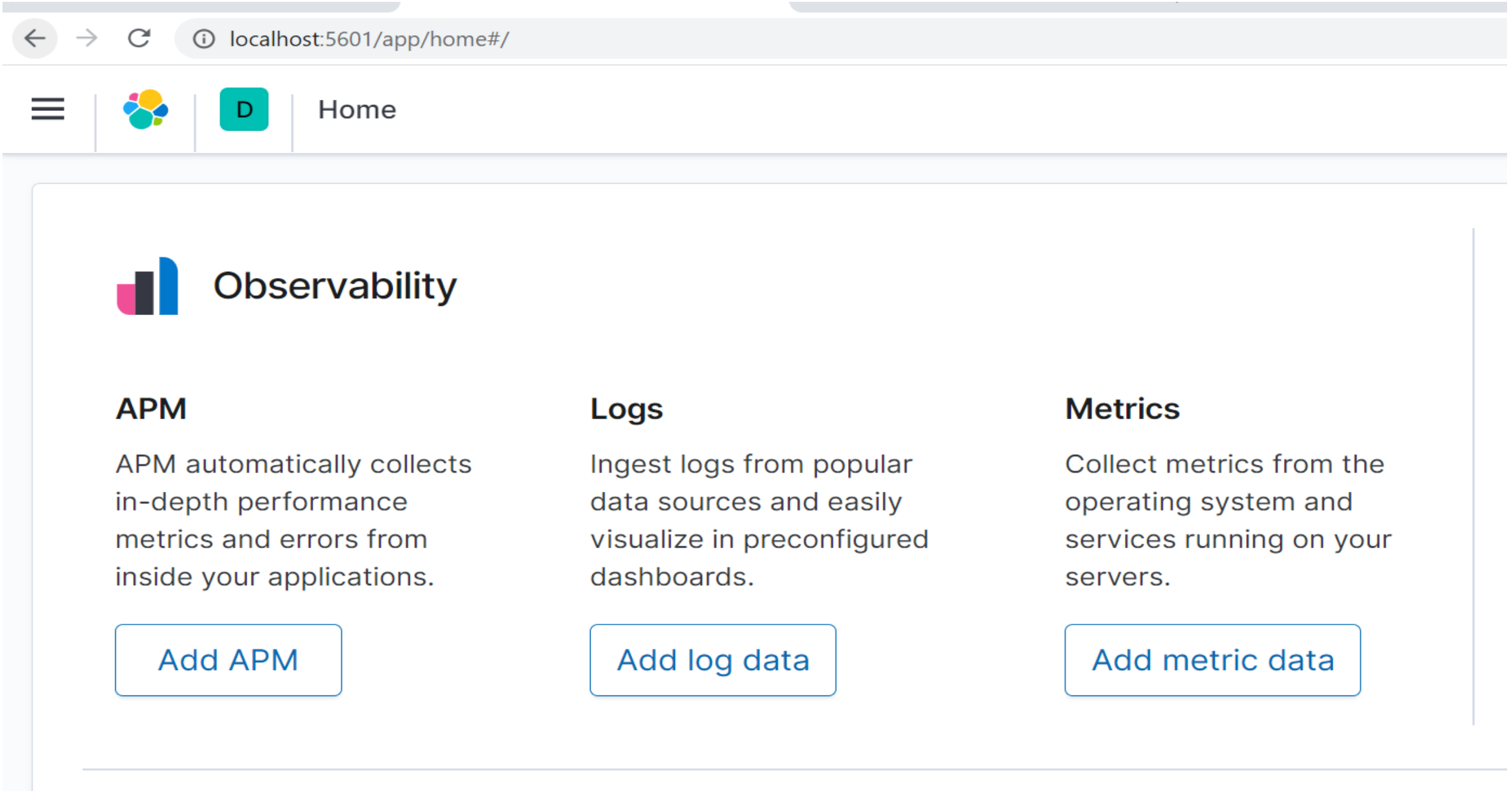
Let's get started

We noticed that you don't have any data in your cluster. You can try our sample data and dashboards or jump in with your own data.

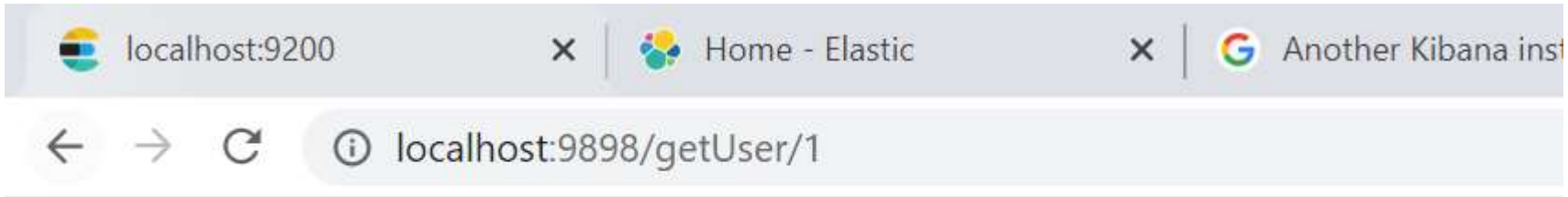
Try our sample data

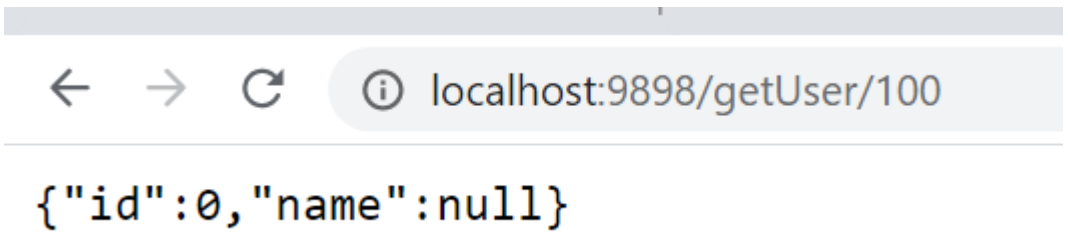
Explore on my own

Spring Boot Application



Spring Boot Application





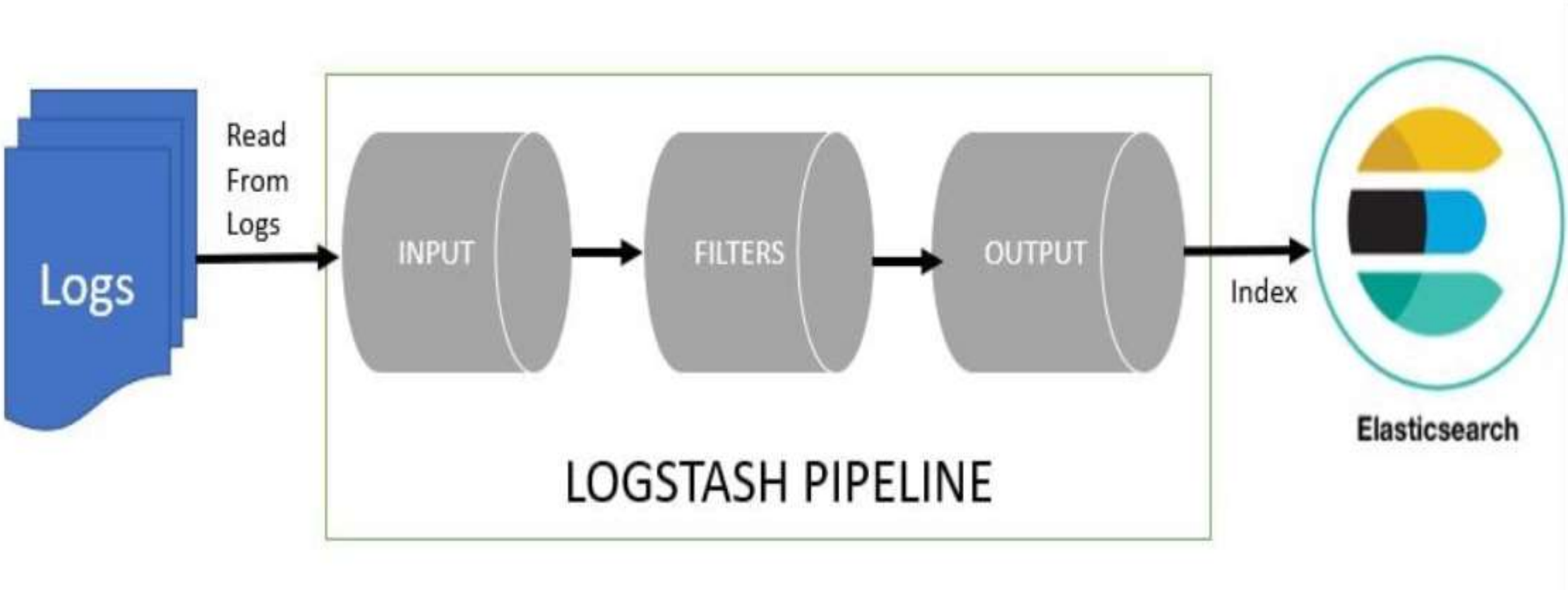
Spring Boot Exception - Application

```
        at org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:373)
2020-09-21 13:41:57.037 ERROR 19212 --- [nio-9898-exec-6] c.j.elk.ElkStackExampleApplication       : User Not Found with ID : 100
        at org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
        at org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:868)
        at org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1594)
        at org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
        at java.lang.Thread.run(Thread.java:748)
```

```
o.s.web.servlet.DispatcherServlet        : Completed initialization in 7 ms
2020-09-21 13:41:23.135  INFO 19212 --- [http-nio-9898-exec-3]
c.j.elk.ElkStackExampleApplication       : user found : com.javatechie.elk.User@7530c28d
2020-09-21 13:41:27.371 ERROR 19212 --- [http-nio-9898-exec-4]
c.j.elk.ElkStackExampleApplication       : User Not Found with ID : 100
2020-09-21 13:41:37.734  INFO 19212 --- [http-nio-9898-exec-5]
c.j.elk.ElkStackExampleApplication       : user found : com.javatechie.elk.User@70bc282f
2020-09-21 13:41:57.037 ERROR 19212 --- [http-nio-9898-exec-6]
c.j.elk.ElkStackExampleApplication       : User Not Found with ID : 100
```

```
logging.file=C:/elk/spring-boot-elk.log
```

Next we will configure the logstash pipeline-



LogStash Configuration

```
input {
  file {
    type => "java"
    path => "C:/elk/spring-boot-elk.log"
    codec => multiline {
      pattern => "^%{YEAR}-%{MONTHNUM}-%{MONTHDAY} %{TIME}.*"
      negate => "true"
      what => "previous"
    }
  }
}

filter {
  #If log line contains tab character followed by 'at' then we will tag that entry as sta
  if [message] =~ "\tat" {
    grok {
      match => ["message", "^(\tat)"]
      add_tag => ["stacktrace"]
    }
  }

}
```

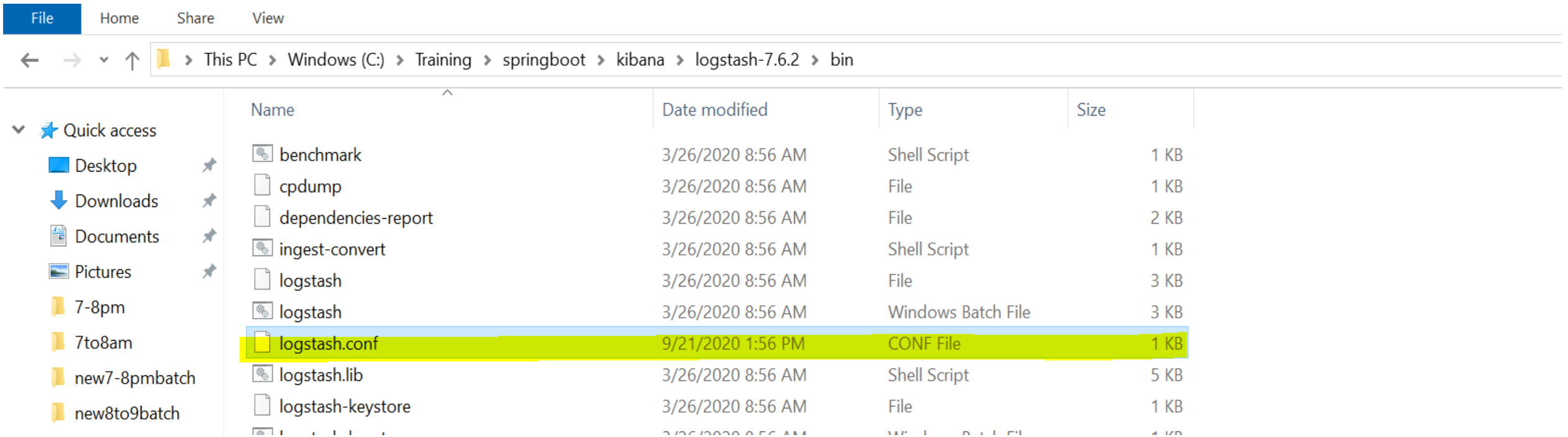
LogStash Configuration

```
output {

  stdout {
    codec => rubydebug
  }

  # Sending properly parsed log events to elasticsearch
  elasticsearch {
    hosts => ["localhost:9200"]
  }
}
```

Start logstash using the command prompt as follows-

```
logstash -f logstash.conf
```

Kibana Installation Path



Spring boot - ELK

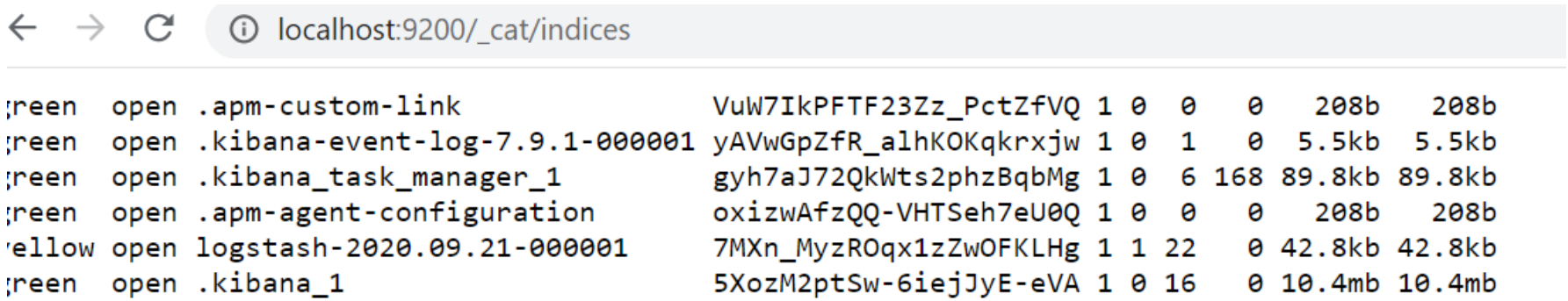
sh configuration for creating a simple

C:\Windows\System32\cmd.exe - logstash -f logstash.conf

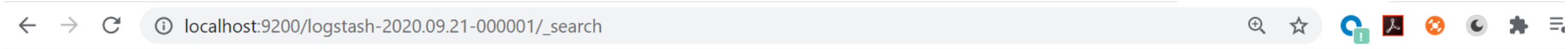
```
    "@timestamp" => 2020-09-21T08:31:06.924Z,
          "path" => "C:/Training/springboot/kibana/log/elk-stack.log",
       "message" => "2020-09-21 13:41:23.135  INFO 19212 --- [http-nio-9898-exec-3] c.j.elk.ElkStackExampleApplication
     : user found : com.javatechie.elk.User@7530c28d\r"
}
{
      "@version" => "1",
          "host" => "1T9GNH2",
    "@timestamp" => 2020-09-21T08:31:06.925Z,
          "path" => "C:/Training/springboot/kibana/log/elk-stack.log",
       "message" => "2020-09-21 13:41:27.371 ERROR 19212 --- [http-nio-9898-exec-4] c.j.elk.ElkStackExampleApplication
     : User Not Found with ID : 100\r"
}
{
      "@version" => "1",
          "host" => "1T9GNH2",
    "@timestamp" => 2020-09-21T08:31:06.925Z,
          "path" => "C:/Training/springboot/kibana/log/elk-stack.log",
       "message" => "2020-09-21 13:41:37.734  INFO 19212 --- [http-nio-9898-exec-5] c.j.elk.ElkStackExampleApplication
     : user found : com.javatechie.elk.User@70bc282f\r"
}
{
      "@version" => "1",
          "host" => "1T9GNH2",
    "@timestamp" => 2020-09-21T08:31:06.925Z,
          "path" => "C:/Training/springboot/kibana/log/elk-stack.log",
       "message" => "2020-09-21 13:41:57.037 ERROR 19212 --- [http-nio-9898-exec-6] c.j.elk.ElkStackExampleApplication
     : User Not Found with ID : 100\r"
}
```

Spring boot - ELK


```
=^.^=
/_cat/allocation
/_cat/shards
/_cat/shards/{index}
/_cat/master
/_cat/nodes
/_cat/tasks
/_cat/indices
/_cat/indices/{index}
/_cat/segments
/_cat/segments/{index}
/_cat/count
/_cat/count/{index}
/_cat/recovery
/_cat/recovery/{index}
/_cat/health
/_cat/pending_tasks
/_cat/aliases
/_cat/aliases/{alias}
/_cat/thread_pool
/_cat/thread_pool/{thread_pools}
/_cat/plugins
/_cat/fielddata
/_cat/fielddata/{fields}
/_cat/nodeattrs
/_cat/repositories
/_cat/snapshots/{repository}
/_cat/templates
/_cat/ml/anomaly_detectors
/_cat/ml/anomaly_detectors/{job_id}
/_cat/ml/trained_models
/_cat/ml/trained_models/{model_id}
/_cat/ml/datafeeds
/_cat/ml/datafeeds/{datafeed_id}
/_cat/ml/data_frame/analytics
/_cat/ml/data_frame/analytics/{id}
```

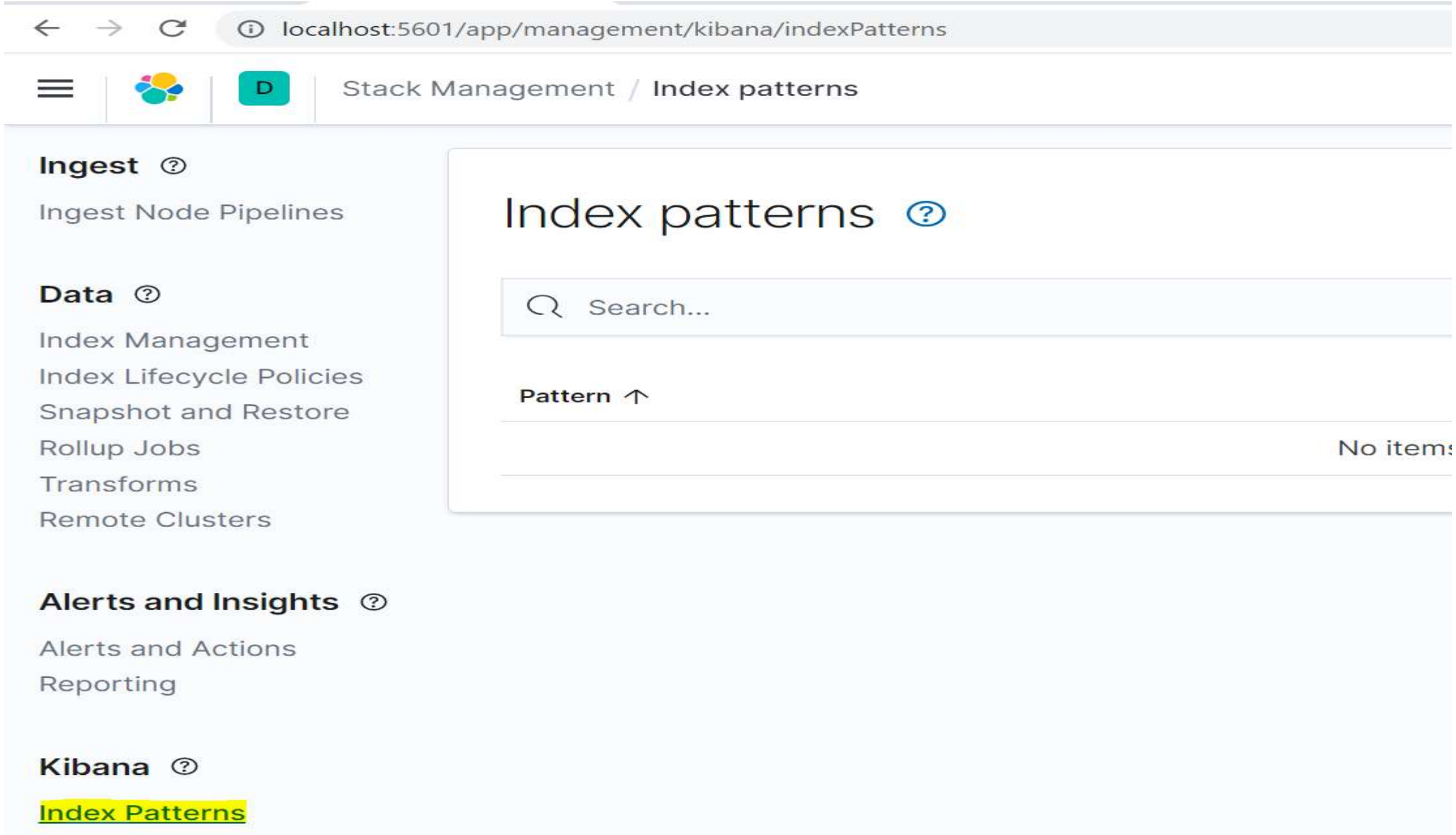


Spring boot - ELK

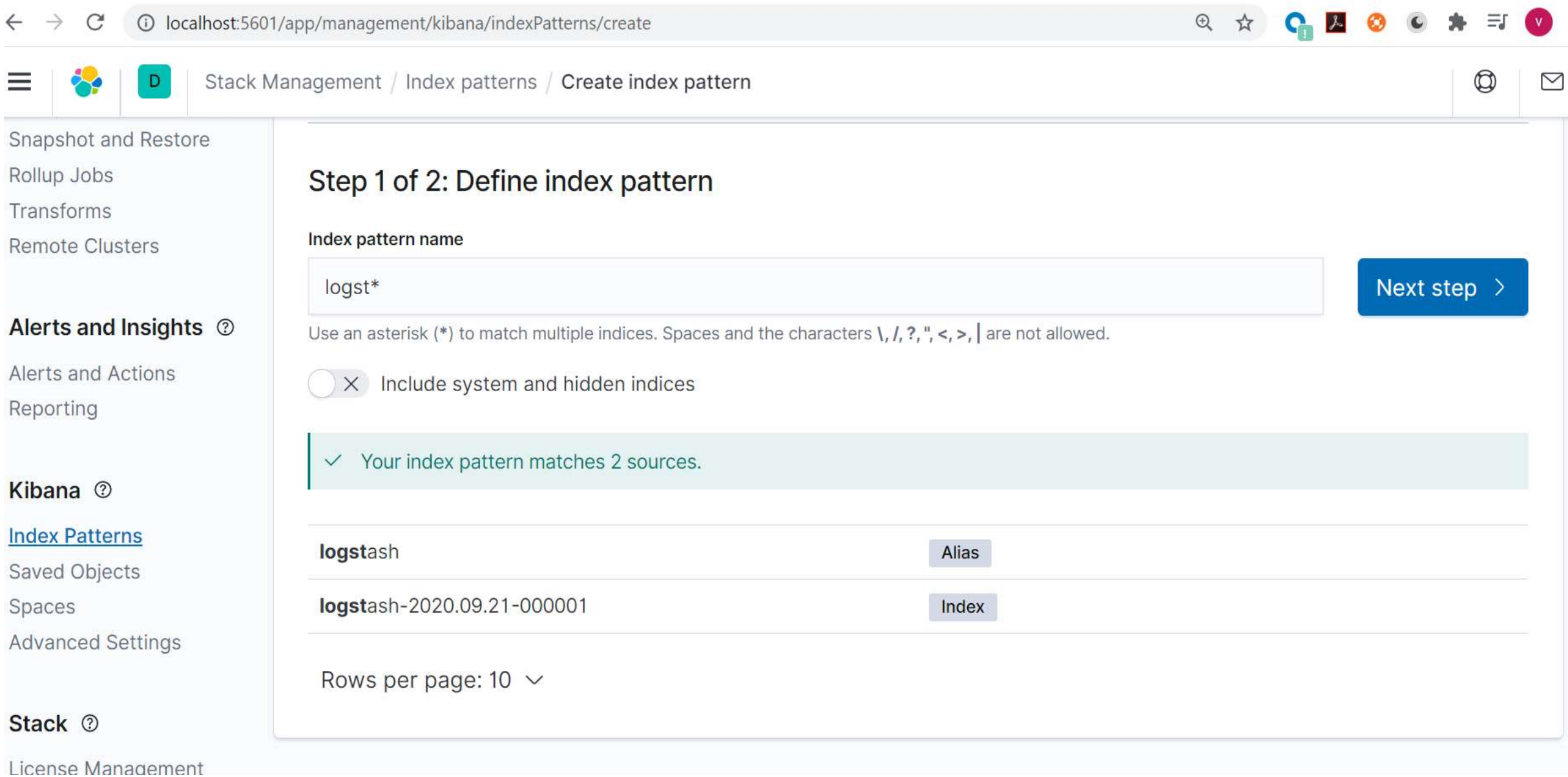



```
{"took":3,"timed_out":false,"_shards":{"total":1,"successful":1,"skipped":0,"failed":0},"hits":{"total":{"value":22,"relation":"eq"},"max_score":1.0,"h
[{"_index":"logstash-2020.09.21-000001","_type":"_doc","_id":"OgPJr3QBJamL3rnCvRXH","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp
09-21T08:31:06.921Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:49.817  INFO 19212 --- [main]
o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 9898 (http)\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"OwPJr3QBJamL3rnCvRXH","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.922Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:50.049  INFO 19212 --- [main]
o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 1733 ms\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"PAPJr3QBJamL3rnCvRXH","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.924Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:41:18.240  INFO 19212 --- [http-nio-9898-exec-1] o.
[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'dispatcherServlet'\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"PQPJr3QBJamL3rnCvRXS","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.921Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:49.829  INFO 19212 --- [main]
o.apache.catalina.core.StandardService   : Starting service [Tomcat]\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"PgPJr3QBJamL3rnCvRXS","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.922Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:50.421  INFO 19212 --- [main]
o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"PwPJr3QBJamL3rnCvRXS","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.924Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:41:18.241  INFO 19212 --- [http-nio-9898-exec-1]
o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"NgPJr3QBJamL3rnCvRWQ","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.846Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:48.215  INFO 19212 --- [main]
c.j.elk.ElkStackExampleApplication       : Starting ElkStackExampleApplication on 1T9GNH2 with PID 19212 (C:\\Training\\springboot\\kibana\\elk-stack-l
example-master\\target\\classes started by vg672483 in C:\\Training\\springboot\\kibana\\elk-stack-logging-example-master)\r"}},{"_index":"logstash-202
000001","_type":"_doc","_id":"NwPJr3QBJamL3rnCvRWQ","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.919Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:48.221  INFO 19212 --- [main]
c.j.elk.ElkStackExampleApplication       : No active profile set, falling back to default profiles: default\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"OAPJr3QBJamL3rnCvRWQ","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.922Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:50.049  INFO 19212 --- [main] o.a.c.c.C.[Tomcat]
[localhost].[/]       : Initializing Spring embedded WebApplicationContext\r"}},{"_index":"logstash-2020.09.21-
000001","_type":"_doc","_id":"OQPJr3QBJamL3rnCvRWQ","_score":1.0,"_source":{"@version":"1","host":"1T9GNH2","@timestamp":"2020-09-
21T08:31:06.923Z","path":"C:/Training/springboot/kibana/log/elk-stack.log","message":"2020-09-21 13:23:50.701  INFO 19212 --- [main]
c.j.elk.ElkStackExampleApplication       : Started ElkStackExampleApplication in 3.166 seconds (JVM running for 5.23)\r"}}]}}
```

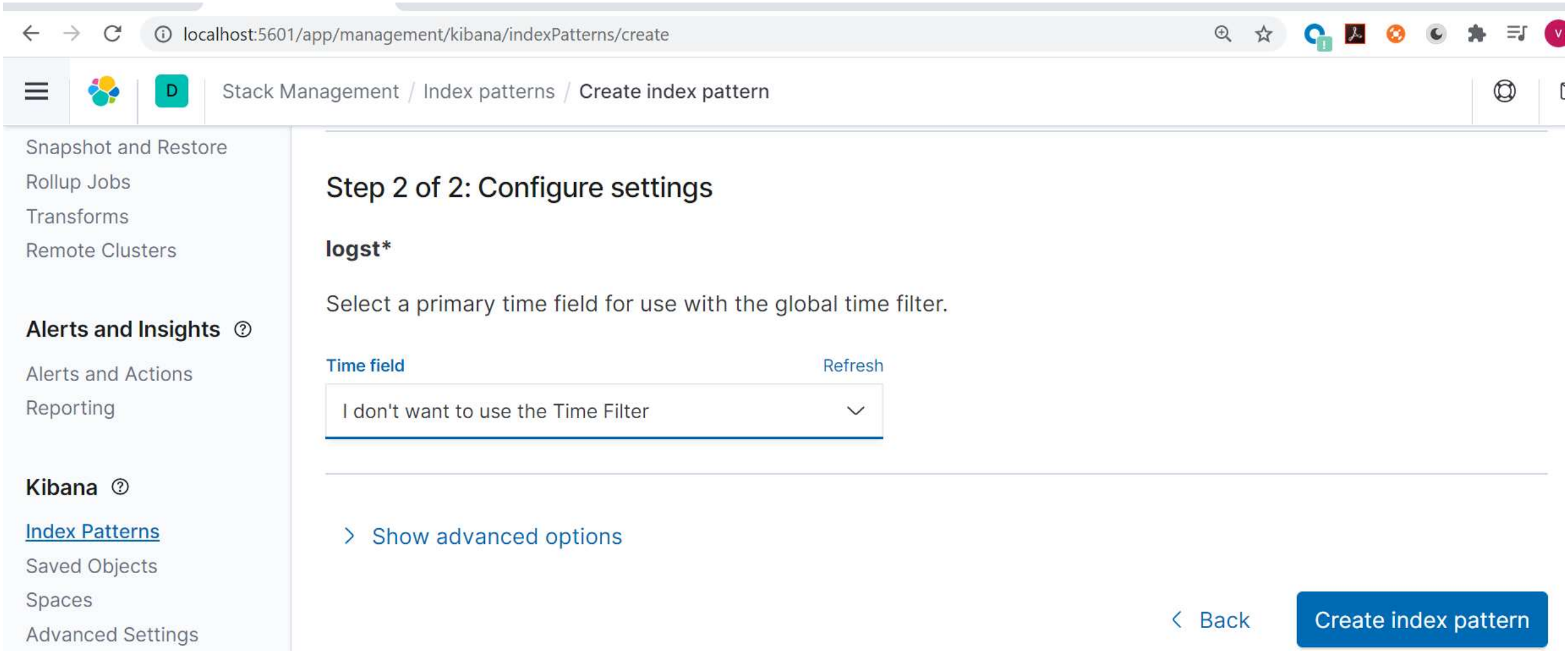
Spring boot - ELK



Spring boot - ELK



Spring boot - ELK



Spring boot - ELK

Spring boot - ELK

> @version: 1 host: 1T9GNH2 @timestamp: Sep 21, 2020 @ 14:01:06.925 path: C:/Training/springboot/kibana/log/elk-stack.log message: 2020-09-21 13:41:27.371 ERROR 19212 --- [http-nio-9898-exec-4] c.j.elk.ElkStackExampleApplication : User Not Found with ID : 100 _id: RAPJr3QBJamL3rnCvRX_ _type: _doc _index: logstash-2020.09.21-000001 _score: 0

> @version: 1 host: 1T9GNH2 @timestamp: Sep 21, 2020 @ 14:01:06.924 path: C:/Training/springboot/kibana/log/elk-stack.log message: 2020-09-21 13:41:23.135 INFO 19212 --- [http-nio-9898-exec-3] c.j.elk.ElkStackExampleApplication : user found : com.javatechie.elk.User@7530c28d _id: QwPJr3QBJamL3rnCvRX_ _type: _doc _index: logstash-2020.09.21-000001 _score: 0

Spring boot - ELK