

# Setup ELK System

## Install Elasticsearch

1. Download the file from <https://www.elastic.co/downloads/elasticsearch>

## Download Elasticsearch

### 1 Download and unzip Elasticsearch

Choose platform:

macOS aarch64 |

macOS aarch64

sha asc

2. Extract the tar, navigate to \${location}/elasticsearch-8.12.2/bin
3. Run ./elasticsearch

```
srikanthjosyula@Srikanths-Air bin % ./elasticsearch
warning: ignoring JAVA_HOME=/Users/srikanthjosyula/Documents/softwares/jdk-11.0.16; using bundled JDK
CompileCommand: exclude org/apache/lucene/util/MSBRadixSorter.computeCommonPrefixLengthAndBuildHistogram bool exclude = true
CompileCommand: exclude org/apache/lucene/util/RadixSelector.computeCommonPrefixLengthAndBuildHistogram bool exclude = true
Mar 03, 2024 10:39:24 AM sun.util.locale.provider.LocaleProviderAdapter <clinit>
WARNING: COMPAT locale provider will be removed in a future release
[2024-03-03T10:39:26,084][INFO ][o.a.l.i.v.PanamaVectorizationProvider] [Srikanths-Air.hitronhub.home] Java vector incubator API enabled
[2024-03-03T10:39:26,486][INFO ][o.e.n.Node ] [Srikanths-Air.hitronhub.home] version[8.12.2], pid[2921], build[tar/48a287a]
S[Mac OS X/13.2.1/aarch64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/21.0.2/21.0.2+13-58]
[2024-03-03T10:39:26,487][INFO ][o.e.n.Node ] [Srikanths-Air.hitronhub.home] JVM home [/Users/srikanthjosyula/Documents/so
DK [true]
[2024-03-03T10:39:26,487][INFO ][o.e.n.Node ] [Srikanths-Air.hitronhub.home] JVM arguments [-Des.networkaddress.cache.ttl=
er.allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow
io.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true
org.elasticsearch.preallocate, -XX:+UseG1GC, -Djava.io.tmpdir=/var/folders/yg/lf9fvt1n7fzbb6r15b_x09_c0000gn/T/elasticsearch-16263241929
clude,org.apache.lucene.util.MSBRadixSorter::computeCommonPrefixLengthAndBuildHistogram, -XX:CompileCommand=exclude,org.apache.lucene.ut
eapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_err_pid%p.log, -Xlog:gc*,gc+age=tra
lesize=64m, -Xms8192m, -Xmx8192m, -XX:MaxDirectMemorySize=4294967296, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1ReservePercent=25, -D
```

4. Try loading localhost:9200, and if any issues are seen, try Disabling X-Pack security allows  
Elasticsearch to start successfully. Re run elasticsearch by below command  
**./elasticsearch -E xpack.security.enabled=false**
5. As of ES 8, SSL/TLS is ON by default for HTTP clients. The WARN message says http client did not trust this server's certificate which means that you need to tell your browser to trust the server certificate. it is self-signed by default, so that's probably the reason. Or you can simply disable SSL in your elasticsearch.yml configuration, that would also work
6. Once loaded you should see as below when localhost:9200 is called

```
{
  "name" : "Srikanths-Air.hitronhub.home",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "rdJ4Xs3xQV-T8QgbkPS-0A",
  "version" : {
    "number" : "8.12.2",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "48a287ab9497e852de30327444b0809e55d46466",
    "build_date" : "2024-02-19T10:04:32.774273190Z",
    "build_snapshot" : false,
    "lucene_version" : "9.9.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

## Install Logstash

1. Download the file from <https://www.elastic.co/downloads/logstash>

### Download Logstash

#### 1 Download and unzip Logstash

Choose platform:

macOS aarch64

📄 macOS aarch64

📄 [sha](#) 📄 [asc](#)

2. In the same page we can see that its mentioned to logstash.conf

#### 2 Configure Logstash

Prepare a logstash.conf [config file](#).

#### 3 Run Logstash

Run `bin/logstash -f logstash.conf`

3. We need to create logstash.conf, where we can mention about the location where our file is present for the Elasticsearch to know where to pick from

```
srikanthjosityula@Srikanths-Air bin % cat logstash.conf
input {
  file {
    path => "/Users/srikanthjosityula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot-elk.log"
    start_position => "beginning"
  }
}

output{
  stdout {
    codec => json
  }
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "springboot-elk"
  }
}
```

## Install Kibana

1. Download the file from <https://www.elastic.co/downloads/kibana>

## Download Kibana

## 1 Download and unzip Kibana

Choose platform:

macOS aarch64 | 

📄 macOS aarch64

[↓ sha](#)
[↓ asc](#)

 [asc](#)

2. Extract the tar file,

```

srikanthjoshiyula@Srikanths-Air ~ % cd ~/Documents/software/kibana-8.12.2
srikanthjoshiyula@Srikanths-Air kibana-8.12.2 % ls
LICENSE.txt  README.txt  config      logs        node_modules packages     src
NOTICE.txt   bin         data        node        package.json plugins      x-pack
srikanthjoshiyula@Srikanths-Air kibana-8.12.2 %

```

- Before we start Kibana, we need to make sure its connecting to elasticsearch, so navigate to `{Home Location}/kibana-8.12.2/config`

```
srikanthjosyula@Srikanths-Air config % ls
kibana.yml      node.options
srikanthjosyula@Srikanths-Air config %
```

4. Open the .yml file, and enable the elasticsearch host. As we need to let Kibana to talk to elastic search to capture logs/data

```
## ENABLED by SRIKANTH
elasticsearch.hosts: ["http://localhost:9200"]
```


- Now, navigate to bin folder of Kibana `${HOME_LOC}/kibana-8.12.2/bin`
- Start the `kibana.sh`

```


$krakenjobstatus-elastic@kraken-kibana bin % kibana
Kibana is currently running on legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.12/production.html#openssl-legacy-provider
{"_level": "info", "@timestamp": "2024-03-03T19:49:38.768Z", "log.logger": "elastic-apm-node", "ecs.version": "8.10.0", "agent.version": "4.2.0", "env":{"pid":"3832","profile":"","mode/bin/node","os":{"derwin 2
...
    "captureBody":{"source":"start","value":false,"commonName":"capture_body"},"captureHeaders":{"source":"start","value":false,"env":{"cid":"3832","profile":"","mode/bin/node","os":{"derwin 2
...
    "captureStackTraces":{"source":"start","value":true,"environment":{"source":"start","value":"production"},"globalLabels":{"source":"start","value":["git ver", "fsbd489cf5f9c676ca4f86ca9ae358632"]},"sourceValue":
...
    "transactionSampleRate":{"source":"start","value":128,"commonName":"service_interval"},"source":"start","value":128,"sourceValue":128},"serveU
...
    "captureSpanStackTraces":{"source":"start","sourceValue":false,"secretToken":{"source":"start","value":"[REDACTED]","commonName":"secret_token"},"serviceName":{"source":"start","value":"kibana","comm
...
    "nname":"service_version"},"serviceVersion":{"source":"start","value":"8.12.2","commonName":"service_version"},"activationMethod":{"require","message":"Elastic APM Node.js Agent v4.2.0")
...
2024-03-03T19:49:38.772-0400[INFO][node] Kibana is starting
2024-03-03T19:49:35.275-0400[INFO][node] Kibana process configured with roles: [background_tasks, ui]
2024-03-03T19:49:38.841-0400[INFO][plugins-service] Plugin "cloudChat" is disabled.
2024-03-03T19:49:38.841-0400[INFO][plugins-service] Plugin "cloudExperiments" is disabled.
2024-03-03T19:49:41.064-0400[INFO][plugins-service] Plugin "cloudFullStory" is disabled.
2024-03-03T19:49:41.431-0400[INFO][plugins-service] Plugin "profilingDataAccess" is disabled.
```

7. We can see the Kibana started on port 5601


```
[2024-03-03T11:02:49.205-04:00][INFO] ][plugins.fleet] Task Fleet-Usage-Sender-1.1.4 scheduled with interval 1h
[2024-03-03T11:02:49.206-04:00][INFO] ][plugins.fleet.fleet:check-deleted-files-task:1.0.1] Started with interval of [1d] and timeout
[2024-03-03T11:02:49.206-04:00][INFO] ][plugins.fleet] Task Fleet-Metrics-Task:1.0.0 scheduled with interval 1h
[2024-03-03T11:02:49.212-04:00][INFO] ][plugins.monitoring.monitoring] config sourced from: production cluster
[2024-03-03T11:02:49.242-04:00][INFO] ][plugins.observability] Installing SLO shared resources
[2024-03-03T11:02:49.243-04:00][INFO] ][plugins.observability] Installing SLO component template [.slo-observability.sli-mappings]
[2024-03-03T11:02:49.243-04:00][INFO] ][plugins.observability] Installing SLO component template [.slo-observability.sli-settings]
[2024-03-03T11:02:49.244-04:00][INFO] ][plugins.observability] Installing SLO component template [.slo-observability.summary-mappings]
[2024-03-03T11:02:49.244-04:00][INFO] ][plugins.observability] Installing SLO component template [.slo-observability.summary-settings]
[2024-03-03T11:02:49.248-04:00][INFO] ][plugins.alerting] Installing ILM policy .alerts-ilm-policy
[2024-03-03T11:02:49.249-04:00][INFO] ][plugins.alerting] Installing component template .alerts-framework-mappings
[2024-03-03T11:02:49.250-04:00][INFO] ][plugins.alerting] Installing component template .alerts-legacy-alert-mappings
[2024-03-03T11:02:49.264-04:00][INFO] ][plugins.alerting] Installing component template .alerts-ecs-mappings
[2024-03-03T11:02:49.268-04:00][INFO] ][plugins.ruleRegistry] Installing component template .alerts-technical-mappings
[2024-03-03T11:02:50.110-04:00][INFO] ][http.server.Kibana] http server running at http://localhost:5601
[2024-03-03T11:02:50.160-04:00][INFO] ][plugins.fleet] Task Fleet-Usage-Logger-Task scheduled with interval 15m
[2024-03-03T11:02:50.177-04:00][INFO] ][plugins.telemetry] Telemetry collection is enabled. For more information on telemetry settings
gs-kbn.html.
[2024-03-03T11:02:50.196-04:00][INFO] ][plugins.monitoring.monitoring.kibana-monitoring] Starting monitoring stats collection
[2024-03-03T11:02:50.203-04:00][ERROR][plugins.observabilityAIAssistant] Failed to resolve ELSER model definition: Error: Platinum, E
```

 elastic

Find apps, content, and more.


 Home

## Welcome home




### Observability

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



### Security

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





### Analytics


Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.


### Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

 Add integrations

 Try sample data

 Upload a file



### Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

Move to Elastic Cloud

# View Logs Kibana

## Step1 : Check the Indexes for the logs in Elasticsearch

1. Open [http://localhost:9200/\\_cat](http://localhost:9200/_cat), we will get all the categories

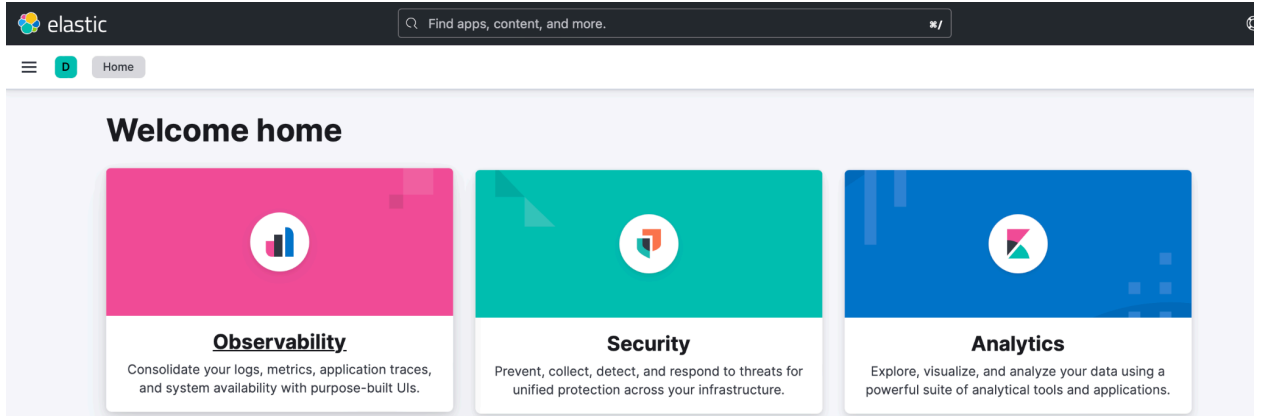
```
=^.^=  
/_cat/allocation  
/_cat/shards  
/_cat/shards/{index}  
/_cat/master  
/_cat/nodes  
/_cat/tasks  
/_cat/indices  
/_cat/indices/{index}  
/_cat/segments  
/_cat/segments/{index}  
/_cat/count  
/_cat/count/{index}  
/_cat/recovery  
/_cat/recovery/{index}  
/_cat/health  
/_cat/pending_tasks  
/_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/component_templates/_cat/ml/anomaly_detectors  
/_cat/ml/anomaly_detectors/{job_id}  
/_cat/ml/datafeeds  
/_cat/ml/datafeeds/{datafeed_id}  
/_cat/ml/trained_models  
/_cat/ml/trained_models/{model_id}  
/_cat/ml/data_frame/analytics  
/_cat/ml/data_frame/analytics/{id}  
/_cat/transforms  
/_cat/transforms/{transform_id}
```

2. Navigate to Indexes [http://localhost:9200/\\_cat/indices](http://localhost:9200/_cat/indices)
3. We can see our indexes . These are the indexes internally created by ELK, we can view this content in kibana

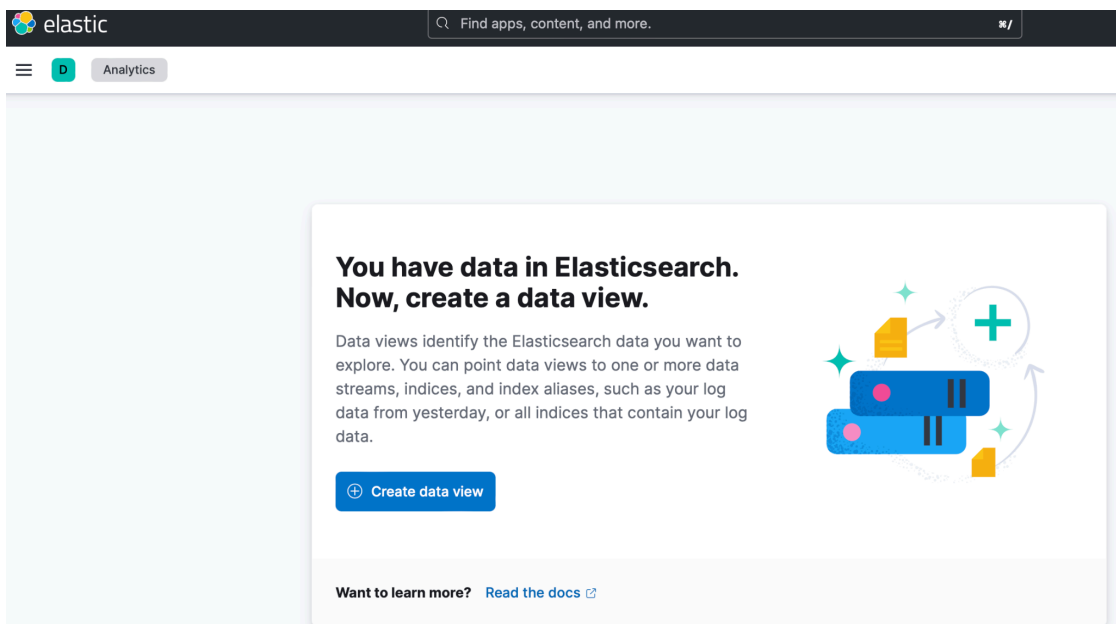
```
yellow open springboot-elk oIX7r4oqT3CBZ0HjZlXcaQ 1 1 35 0 109.6kb 109.6kb 109.6kb  
yellow open .ds-logs-generic-default-2024.03.03-000001 cnJd5v7oQt-p_A7sC3DlcQ 1 1 35 0 132.4kb 132.4kb 132.4kb
```

## Step2 : Check Logs on Kibana

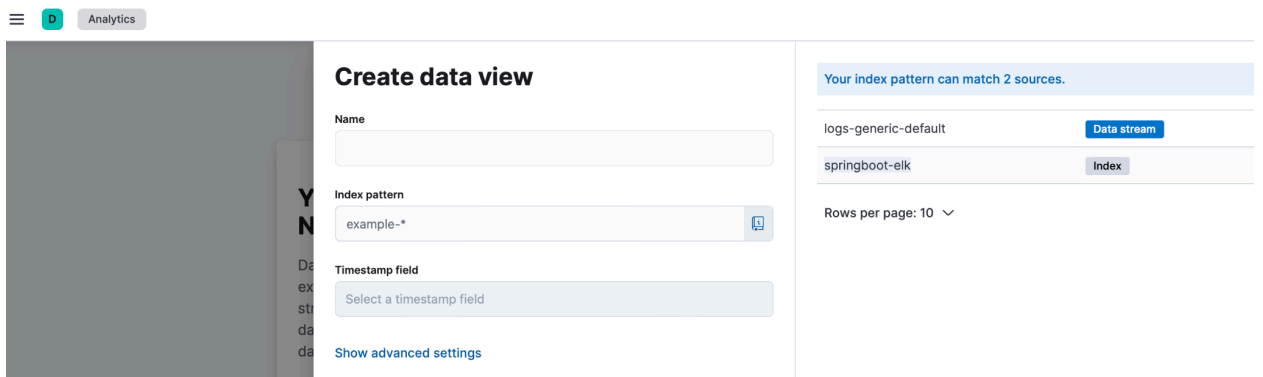
1. Open Kibana which is running on <http://localhost:5601/app/home#/>
2. Navigate to Analytics



3. Click on create data view



4. We can see our index patterns there



5. Provide your index pattern and save the view

## Create data view

**Name**

**Index pattern**

**Timestamp field**

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

✓ Your index pattern matches 1 source.

All sources **Matched**

springboot-elk **Index**

Rows per page: 10

- Once we click on discover, we can see the hits and logs, where we can see our logs and other details in json format

The screenshot shows the Elastic Discover interface. The top bar includes the Elastic logo, a search bar, and navigation links like 'Discover', 'Visualize', 'Dashboard', 'Settings', 'Alerts', 'Inspect', and 'Save'. The main area is divided into several sections:

- Left Sidebar:** Contains 'Available fields' (e.g., @timestamp, @version, event.original, host.name, log.file.path, message) and 'Empty fields'.
- Top Bar:** Shows the search field 'Sample Springbook ELK Logging' and a search bar with the placeholder 'Filter your data using KQL syntax'.
- Search Results:** Displays 95 hits. A table shows the first three hits, each with a timestamp, version, event.original, host.name, log.file.path, and message.
- Field Statistics:** A chart showing the distribution of the selected fields.
- Expanded Document:** A detailed view of a single document, showing its \_id, \_index, \_score, and all fields (event.original, host.name, log.file.path, message).

The 'Expanded document' section shows the following details:

- \_id:** 57WuCY480buhYhQe5vJ
- \_index:** springboot-elk
- \_score:** -
- @timestamp:** Mar 4, 2024 @ 09:36:49.476
- @version:** 1
- event.original:** 2024-03-03 16:23:46.906 INFO 5734 --- [http-nio-8090-exec-10] c.sample.elk.controller.UserController : Requesting to fetch user by id: 1
- host.name:** Srikanths-Air.hitronhub.home
- log.file.path:** /Users/srikanthjoshi/Projects/springboot-elk-stack-example/logs/springboot-elk.log
- message:** 2024-03-03 16:23:46.906 INFO 5734 --- [http-nio-8090-exec-10] c.sample.elk.controller.UserController : Requesting to fetch user by id: 1