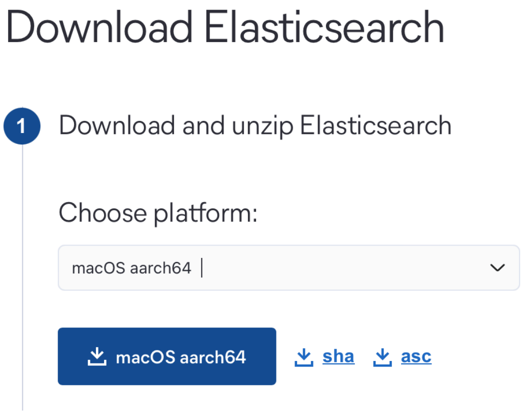
Setup ELK System

Install Elasticsearch

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



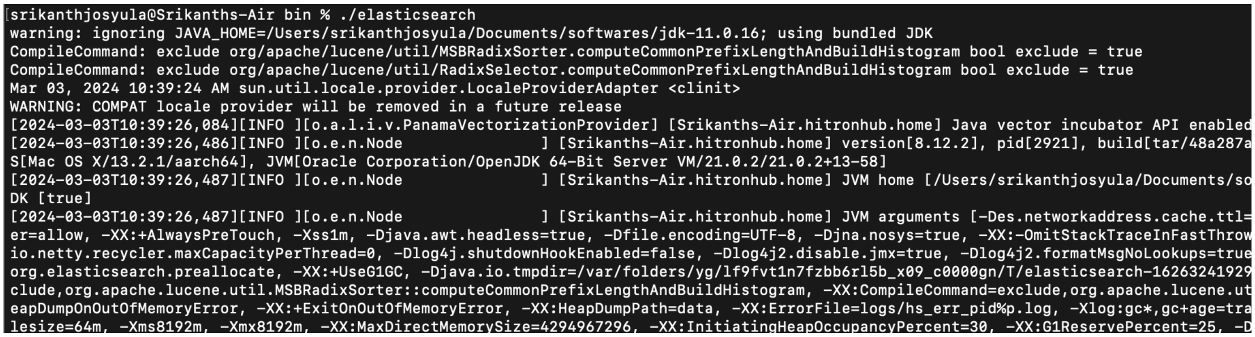
Download Elasticsearch

1 Download and unzip Elasticsearch

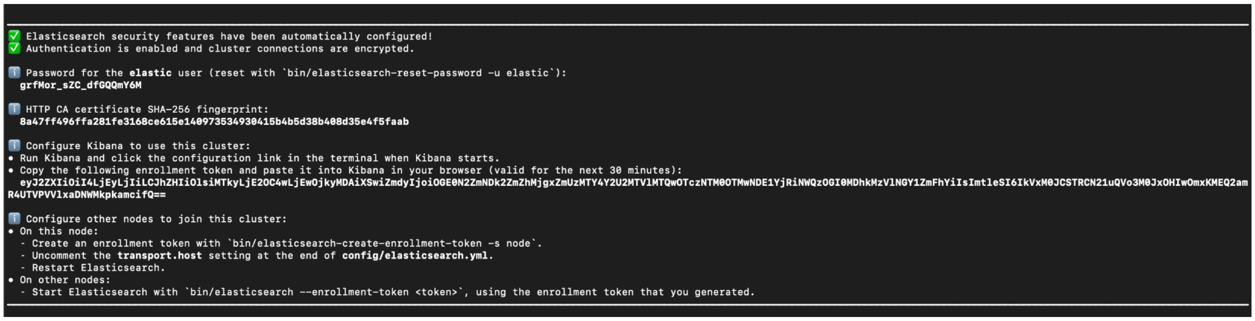
Choose platform:

macOS aarch64

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/lf9fvt1n7fzbb6rl5b_x09_c0000gn/T/elasticsearch-1626324192
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
```



```
✅ Elasticsearch security features have been automatically configured!
✅ Authentication is enabled and cluster connections are encrypted.

ℹ️ Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):
  grfMor_sZC_dfGQQmY6M

ℹ️ HTTP CA certificate SHA-256 fingerprint:
  8a47ff496ffa281fe3168ce615e140973534930415b4b5d38b408d35e4f5faab

ℹ️ Configure Kibana to use this cluster:
• Run Kibana and click the configuration link in the terminal when Kibana starts.
• Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):
  eyJ2ZXIiOiI4LjEyLjIiLCJhZHIiOlsiMTkyLjE2OC4wLjEwOjkyMDAiXSwiZmdyIjoiOGE0N2ZmNDk2ZmZhMjgxZmUzMTY4Y2U2MTVlMTQwOTczNTM0OTMwNDE1YjRiNWQzOGI0MDhkMzVlNGY1ZmFhYiIsImtleSI6IkVxM0JCSTRCN21uQVo3M0JxOHIwOmxKMEQ2am
R4UTVPVVlxaDNWMkpkamcifQ==

ℹ️ Configure other nodes to join this cluster:
• On this node:
  - Create an enrollment token with `bin/elasticsearch-create-enrollment-token -s node`.
  - Uncomment the transport.host setting at the end of config/elasticsearch.yml.
  - Restart Elasticsearch.
• On other nodes:
  - Start Elasticsearch with `bin/elasticsearch --enrollment-token <token>`, using the enrollment token that you generated.
```

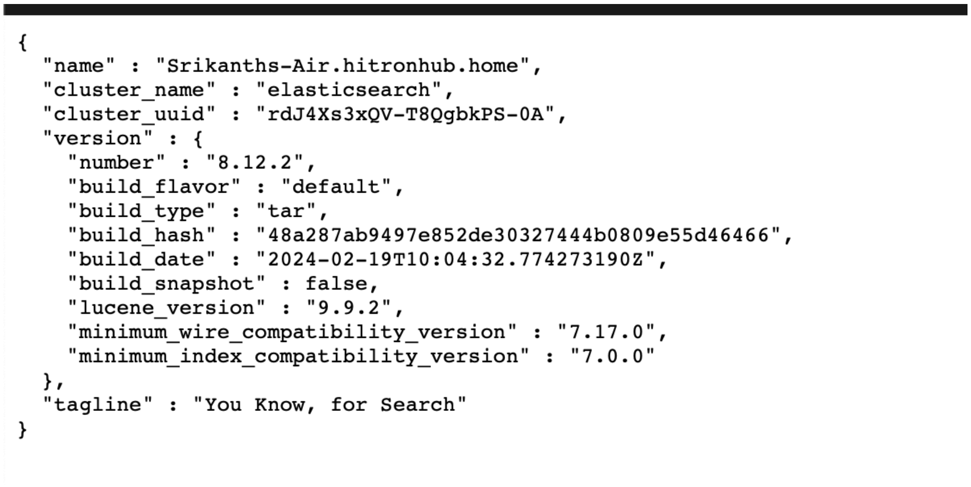
4. Try loading localhost:9200, and if any issues are seen, try Disabling X-Pack security allowed Elasticsearch to start successfully. Re run elasticsearch by below command

   ./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

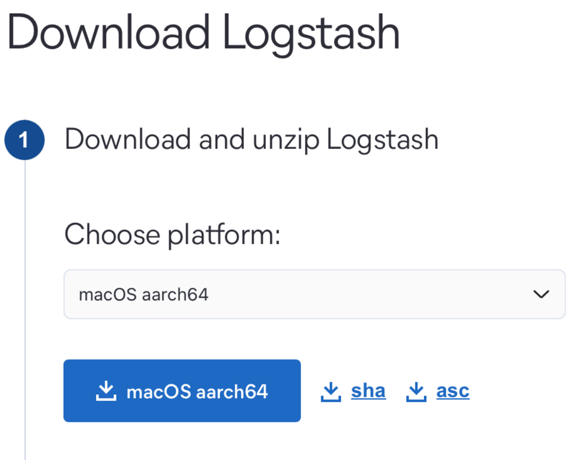
6. Once loaded you should see as below when localhost:9200 is called



```
{
  "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



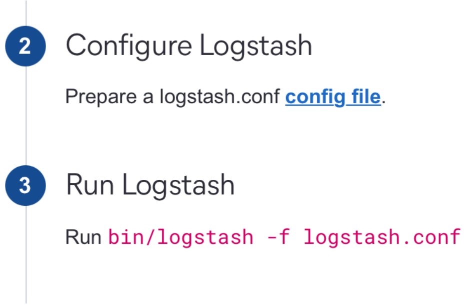
Download Logstash

1 Download and unzip Logstash

Choose platform:

macOS aarch64

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



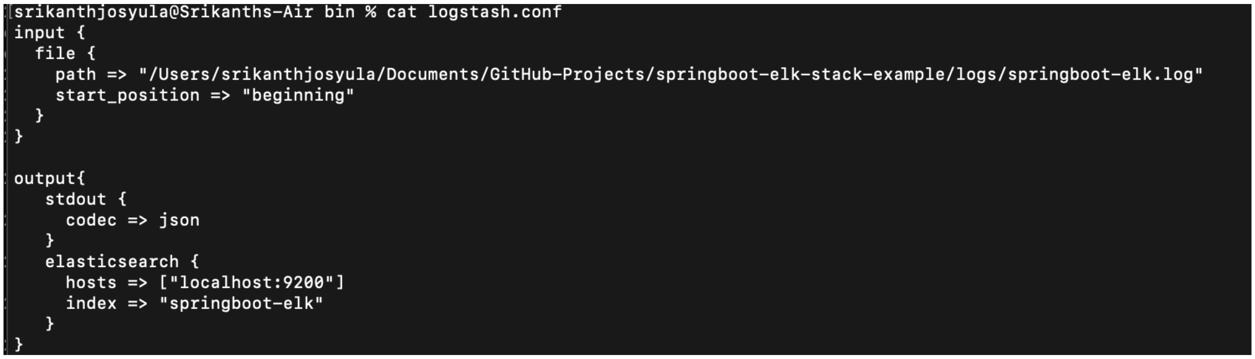
2 Configure Logstash

Prepare a logstash.conf config file.

3 Run Logstash

Run `bin/logstash -f logstash.conf`

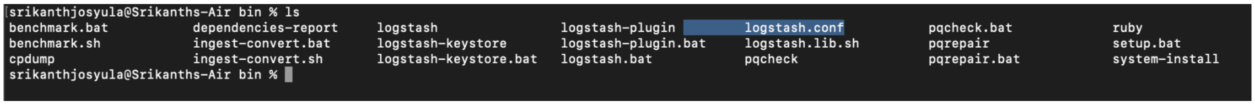
3. We need to create logstash.conf, where we can mention about the location where our file is present for the Elasticsearch to know where to pick from



```
srikanthjosyula@Srikanths-Air bin % cat logstash.conf
input {
  file {
    path => "/Users/srikanthjosyula/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"
   }
}
```

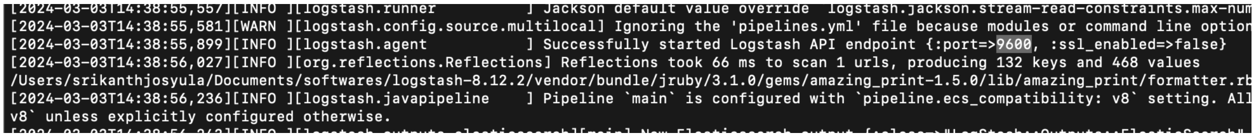
4. In input we give from where the file needs to be picked from and output is where our elasticsearch is hosted



```
srikanthjosyula@Srikanths-Air bin % ls
benchmark.bat          dependencies-report    logstash               logstash-plugin        logstash.conf          pqcheck.bat            ruby
benchmark.sh           ingest-convert.bat     logstash-keystore      logstash-plugin.bat    logstash.lib.sh        pqrepair               setup.bat
cpdump                 ingest-convert.sh      logstash-keystore.bat  logstash.bat           pqcheck                pqrepair.bat           system-install
srikanthjosyula@Srikanths-Air bin %
```

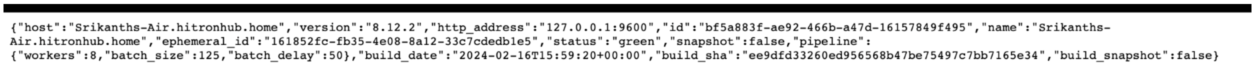
5. We need to run the logstash now. To start it we need to run the command

./logstash -f /Users/srikanthjosyula/Documents/softwares/logstash-8.12.2/bin/logstash.conf

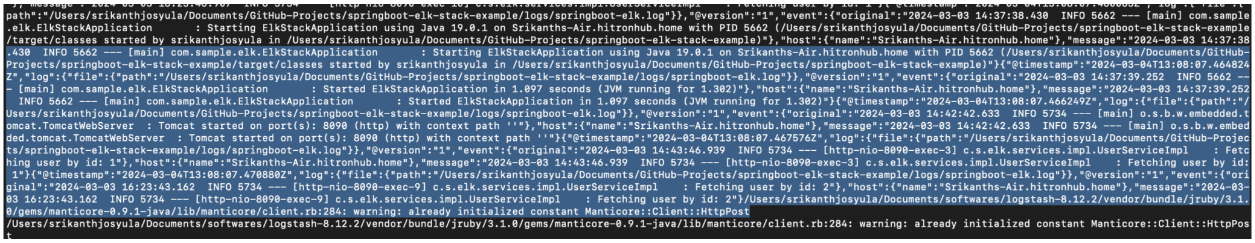


```
[2024-03-03T14:38:55,557][INFO ][logstash.runner          ] Jackson default value override `logstash.jackson.stream-read-constraints.max-num
[2024-03-03T14:38:55,581][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line option
[2024-03-03T14:38:55,899][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
[2024-03-03T14:38:56,027][INFO ][org.reflections.Reflections] Reflections took 66 ms to scan 1 urls, producing 132 keys and 468 values
/Users/srikanthjosyula/Documents/softwares/logstash-8.12.2/vendor/bundle/jruby/3.1.0/gems/amazing_print-1.5.0/lib/amazing_print/formatter.rb
[2024-03-03T14:38:56,236][INFO ][logstash.javapipeline    ] Pipeline `main` is configured with `pipeline.ecs_compatibility: v8` setting. All
v8` unless explicitly configured otherwise.
```

6. Logstash is started on port 9600 http://localhost:9600/



```
{"host":"Srikanths-Air.hitronhub.home","version":"8.12.2","http_address":"127.0.0.1:9600","id":"bf5a883f-ae92-466b-a47d-16157849f495","name":"Srikanths-
Air.hitronhub.home","ephemeral_id":"161852fc-fb35-4e08-8a12-33c7cdedb1e5","status":"green","snapshot":false,"pipeline":
{"workers":8,"batch_size":125,"batch_delay":50},"build_date":"2024-02-16T15:59:20+00:00","build_sha":"ee9dfd33260ed956568b47be75497c7bb7165e34","build_snapshot":false}
```

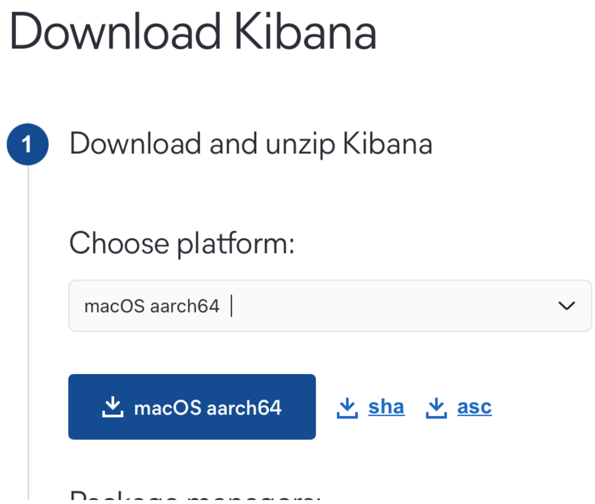


```
path":"/Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot-elk.log"}},"@version":"1","event":{"original":"2024-03-03 14:37:38.430  INFO 5662 --- [main] com.sample
.elk.ElkStackApplication       : Starting ElkStackApplication using Java 19.0.1 on Srikanths-Air.hitronhub.home with PID 5662 (/Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example
/target/classes started by srikanthjosyula in /Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example)"},"host":{"name":"Srikanths-Air.hitronhub.home"},"message":"2024-03-03 14:37:38
.430  INFO 5662 --- [main] com.sample.elk.ElkStackApplication       : Starting ElkStackApplication using Java 19.0.1 on Srikanths-Air.hitronhub.home with PID 5662 (/Users/srikanthjosyula/Documents/GitHub-
Projects/springboot-elk-stack-example/target/classes started by srikanthjosyula in /Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example)"}{"@timestamp":"2024-03-04T13:08:07.464824
Z","log":{"file":{"path":"/Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot-elk.log"}},"@version":"1","event":{"original":"2024-03-03 14:37:39.252  INFO 5662 --
- [main] com.sample.elk.ElkStackApplication       : Started ElkStackApplication in 1.097 seconds (JVM running for 1.302)"},"host":{"name":"Srikanths-Air.hitronhub.home"},"message":"2024-03-03 14:37:39.252
  INFO 5662 --- [main] com.sample.elk.ElkStackApplication       : Started ElkStackApplication in 1.097 seconds (JVM running for 1.302)"}{"@timestamp":"2024-03-04T13:08:07.466249Z","log":{"file":{"path":"/
Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot-elk.log"}},"@version":"1","event":{"original":"2024-03-03 14:42:42.633  INFO 5734 --- [main] o.s.b.w.embedded.t
omcat.TomcatWebServer  : Tomcat started on port(s): 8090 (http) with context path ''"},"host":{"name":"Srikanths-Air.hitronhub.home"},"message":"2024-03-03 14:42:42.633  INFO 5734 --- [main] o.s.b.w.embed
ded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8090 (http) with context path ''"}{"@timestamp":"2024-03-04T13:08:07.467576Z","log":{"file":{"path":"/Users/srikanthjosyula/Documents/GitHub-Projec
ts/springboot-elk-stack-example/logs/springboot-elk.log"}},"@version":"1","event":{"original":"2024-03-03 14:43:46.939  INFO 5734 --- [http-nio-8090-exec-3] c.s.elk.services.impl.UserServiceImpl    : Fetc
hing user by id: 1"},"host":{"name":"Srikanths-Air.hitronhub.home"},"message":"2024-03-03 14:43:46.939  INFO 5734 --- [http-nio-8090-exec-3] c.s.elk.services.impl.UserServiceImpl    : Fetching user by id:
 1"}{"@timestamp":"2024-03-04T13:08:07.470880Z","log":{"file":{"path":"/Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot-elk.log"}},"@version":"1","event":{"ori
ginal":"2024-03-03 16:23:43.162  INFO 5734 --- [http-nio-8090-exec-9] c.s.elk.services.impl.UserServiceImpl    : Fetching user by id: 2"},"host":{"name":"Srikanths-Air.hitronhub.home"},"message":"2024-03-
03 16:23:43.162  INFO 5734 --- [http-nio-8090-exec-9] c.s.elk.services.impl.UserServiceImpl    : Fetching user by id: 2"}/Users/srikanthjosyula/Documents/softwares/logstash-8.12.2/vendor/bundle/jruby/3.1.
0/gems/manticore-0.9.1-java/lib/manticore/client.rb:284: warning: already initialized constant Manticore::Client::HttpPost
/Users/srikanthjosyula/Documents/softwares/logstash-8.12.2/vendor/bundle/jruby/3.1.0/gems/manticore-0.9.1-java/lib/manticore/client.rb:284: warning: already initialized constant Manticore::Client::HttpPos
t
```

7. Logs will be see on console with logstash

Install Kibana

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

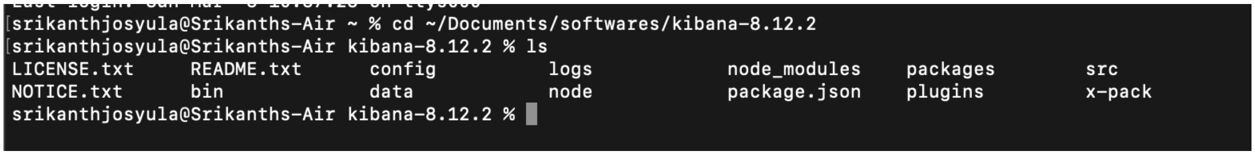


Download Kibana

1 Download and unzip Kibana

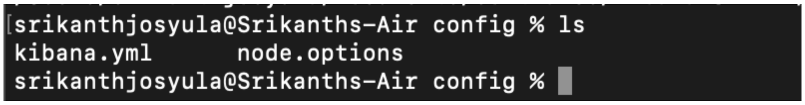
Choose platform:

2. Extract the tar file,



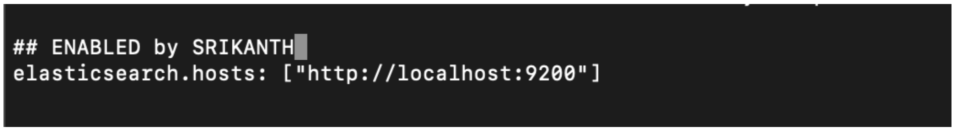
```
[srikanthjosyula@Srikanths-Air ~ % cd ~/Documents/softwares/kibana-8.12.2
[srikanthjosyula@Srikanths-Air kibana-8.12.2 % ls
LICENSE.txt      README.txt       config           logs             node_modules     packages         src
NOTICE.txt       bin              data             node           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

3. Before we start Kibana, we need to make sure its connecting to elasticsearch, so navigate to ${Home_Location}/kibana-8.12.2/config



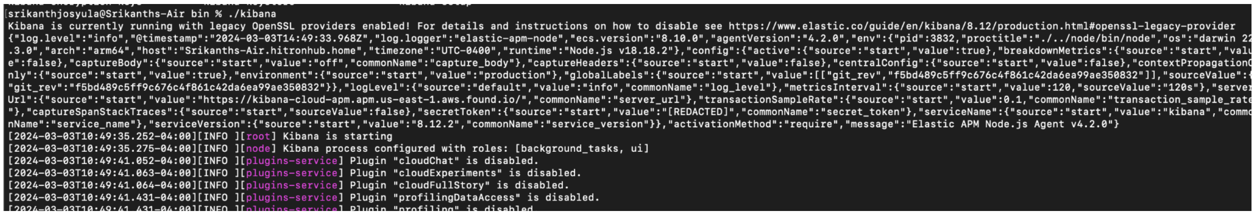
```
[srikanthjosyula@Srikanths-Air config % ls
kibana.yml       node.options
srikanthjosyula@Srikanths-Air config % 
```

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



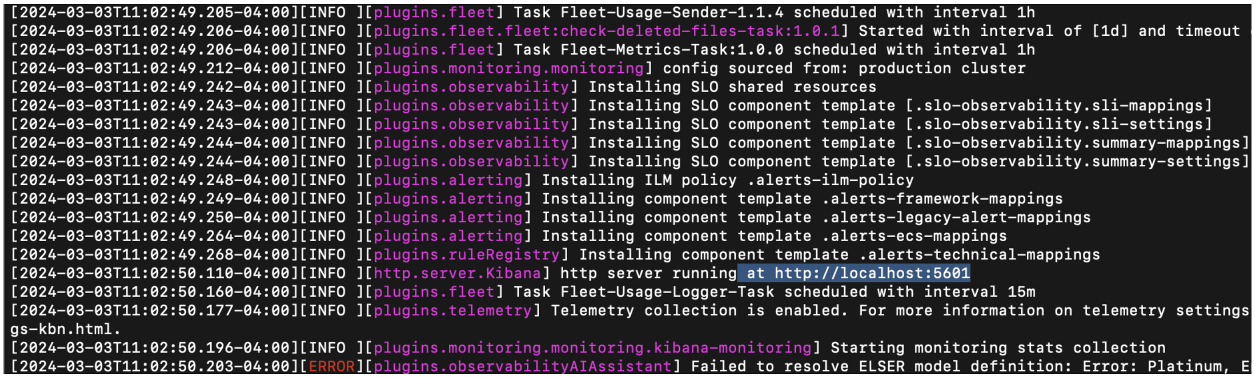
```
## ENABLED by SRIKANTH
elasticsearch.hosts: ["http://localhost:9200"]
```

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

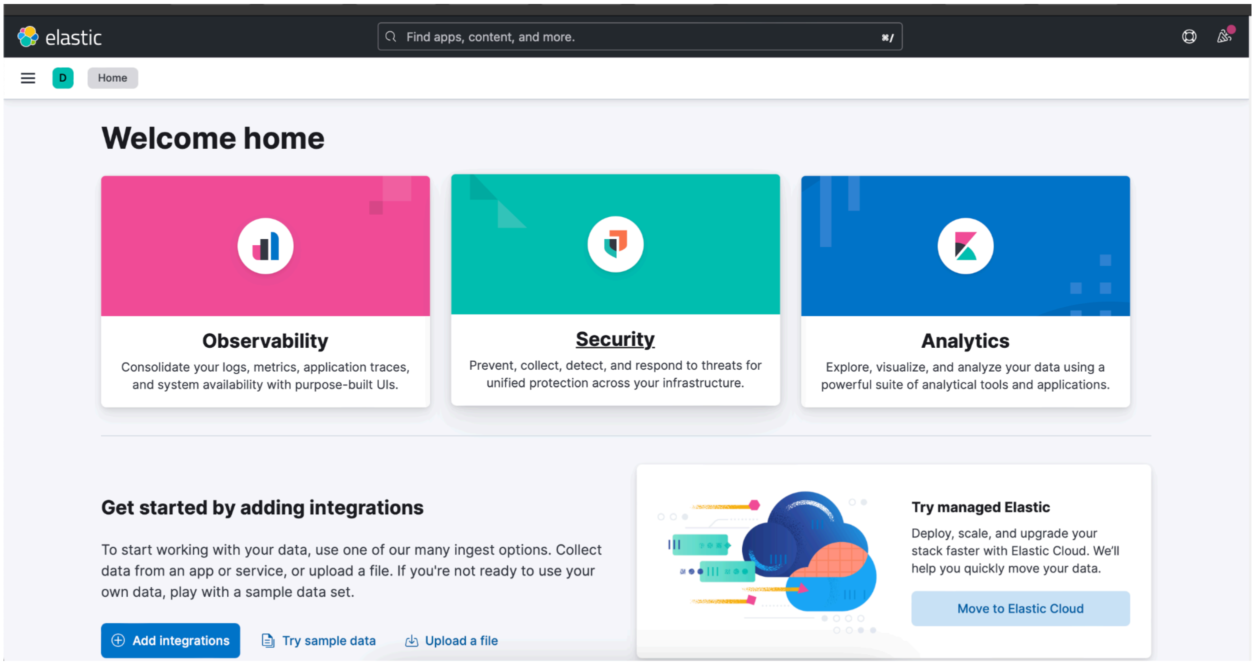


```
[srikanthjosyula@Srikanths-Air bin % ./kibana
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.12/production.html#openssl-legacy-provider
{"log.level":"info","@timestamp":"2024-03-03T14:49:33.968Z","log.logger":"elastic-apm-node","ecs.version":"8.10.0","agentVersion":"4.2.0","env":{"pid":3832,"proctitle":"./../node/bin/node","os":"darwin 22
.3.0","arch":"arm64","host":"Srikanths-Air.hitronhub.home","timezone":"UTC-0400","runtime":"Node.js v18.18.2"},"config":{"active":{"source":"start","value":true},"breakdownMetrics":{"source":"start","valu
e":false},"captureBody":{"source":"start","value":"off","commonName":"capture_body"},"captureHeaders":{"source":"start","value":false},"centralConfig":{"source":"start","value":false},"contextPropagationO
nly":{"source":"start","value":true},"environment":{"source":"start","value":"production"},"globalLabels":{"source":"start","value":[["git_rev","f5bd489c5ff9c676c4f861c42da6ea99ae350832"]],"sourceValue":{
"git_rev":"f5bd489c5ff9c676c4f861c42da6ea99ae350832"}},"logLevel":{"source":"default","value":"info","commonName":"log_level"},"metricsInterval":{"source":"start","value":120,"sourceValue":"120s"},"server
Url":{"source":"start","value":"https://kibana-cloud-apm.apm.us-east-1.aws.found.io/","commonName":"server_url"},"transactionSampleRate":{"source":"start","value":0.1,"commonName":"transaction_sample_rate
"},"captureSpanStackTraces":{"source":"start","sourceValue":false},"secretToken":{"source":"start","value":"[REDACTED]","commonName":"secret_token"},"serviceName":{"source":"start","value":"kibana","commo
nName":"service_name"},"serviceVersion":{"source":"start","value":"8.12.2","commonName":"service_version"}},"activationMethod":"require","message":"Elastic APM Node.js Agent v4.2.0"}
[2024-03-03T10:49:35.252-04:00][INFO ][root] Kibana is starting
[2024-03-03T10:49:35.275-04:00][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
[2024-03-03T10:49:41.052-04:00][INFO ][plugins-service] Plugin "cloudChat" is disabled.
[2024-03-03T10:49:41.063-04:00][INFO ][plugins-service] Plugin "cloudExperiments" is disabled.
[2024-03-03T10:49:41.064-04:00][INFO ][plugins-service] Plugin "cloudFullStory" is disabled.
[2024-03-03T10:49:41.431-04:00][INFO ][plugins-service] Plugin "profilingDataAccess" is disabled.
[2024-03-03T10:49:41.431-04:00][INFO ][plugins-service] Plugin "profiling" 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
```



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.

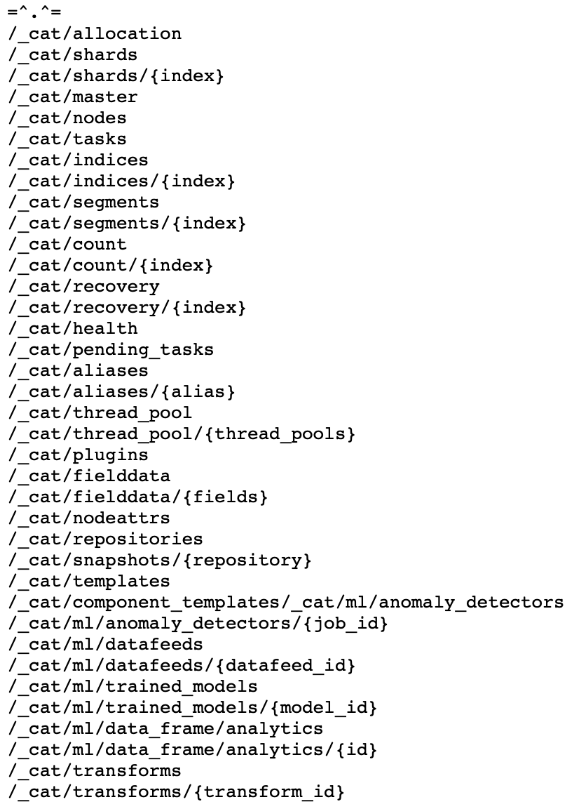
Try managed Elastic

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

View Logs Kibana

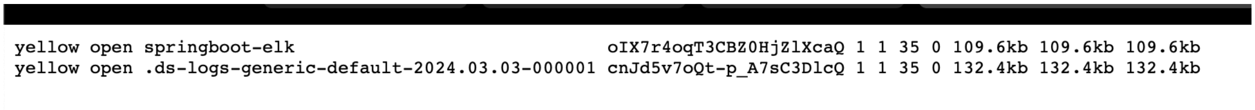
Step1 : Check the Indexes for the logs in Elasticsearch

1. Open 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}
```

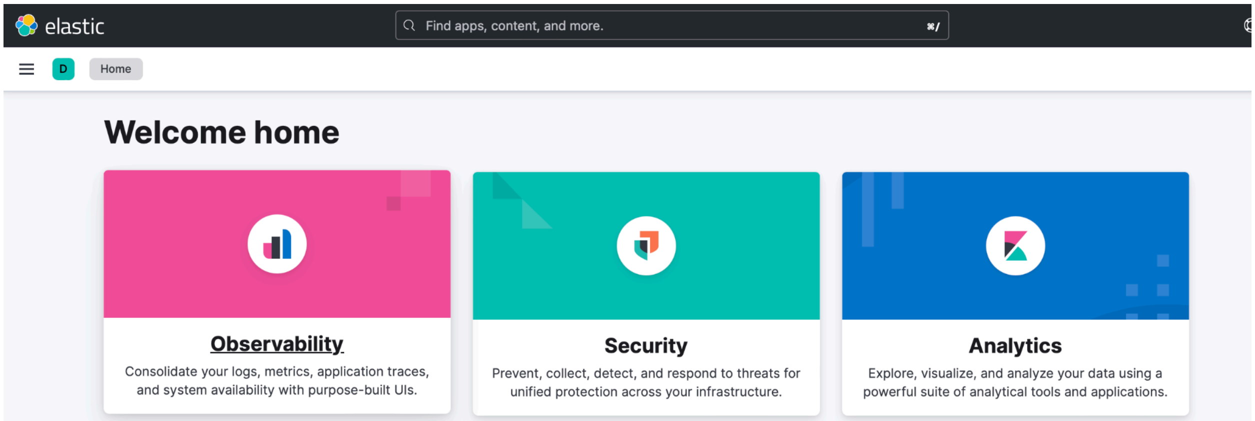
2. Navigate to Indexes http://localhost:9200/_cat/indices
3. We can see our indexes . These are the indexes internally created by ELK, we can view this content in kibana



```
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



Welcome home

Observability

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

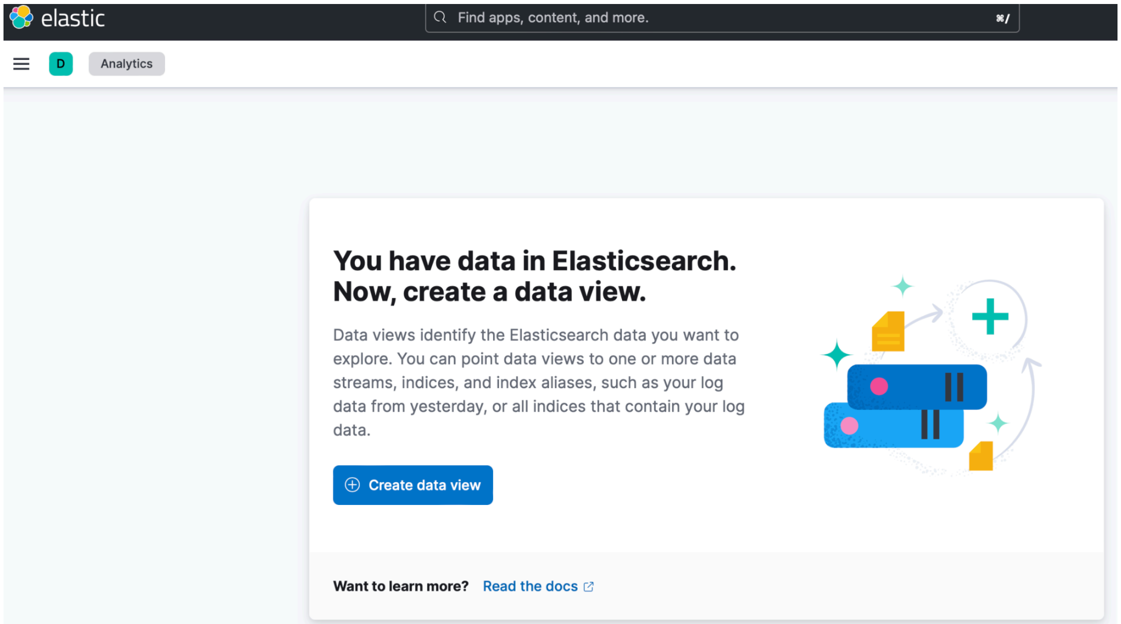
Security

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.

3. Click on create data view

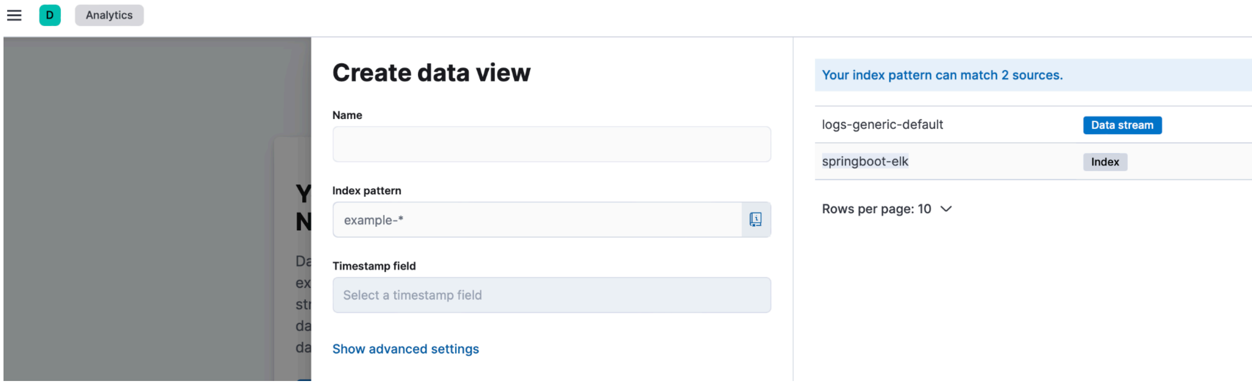


You have data in Elasticsearch. Now, create a data view.

Data views identify the Elasticsearch data you want to explore. You can point data views to one or more data streams, indices, and index aliases, such as your log data from yesterday, or all indices that contain your log data.

Want to learn more? Read the docs

4. We can see our index patterns there



Create data view

Name

Index pattern

example-*

Timestamp field

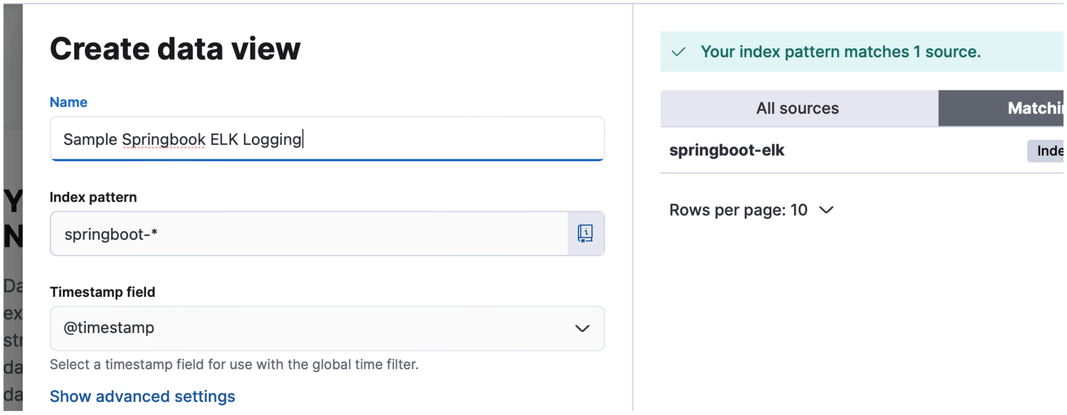
Select a timestamp field

Your index pattern can match 2 sources.

logs-generic-default	Data stream
springboot-elk	Index

Rows per page: 10

5. Provide your index pattern and save the view



Create data view

Name: Sample Springbook ELK Logging

Index pattern: springboot-*

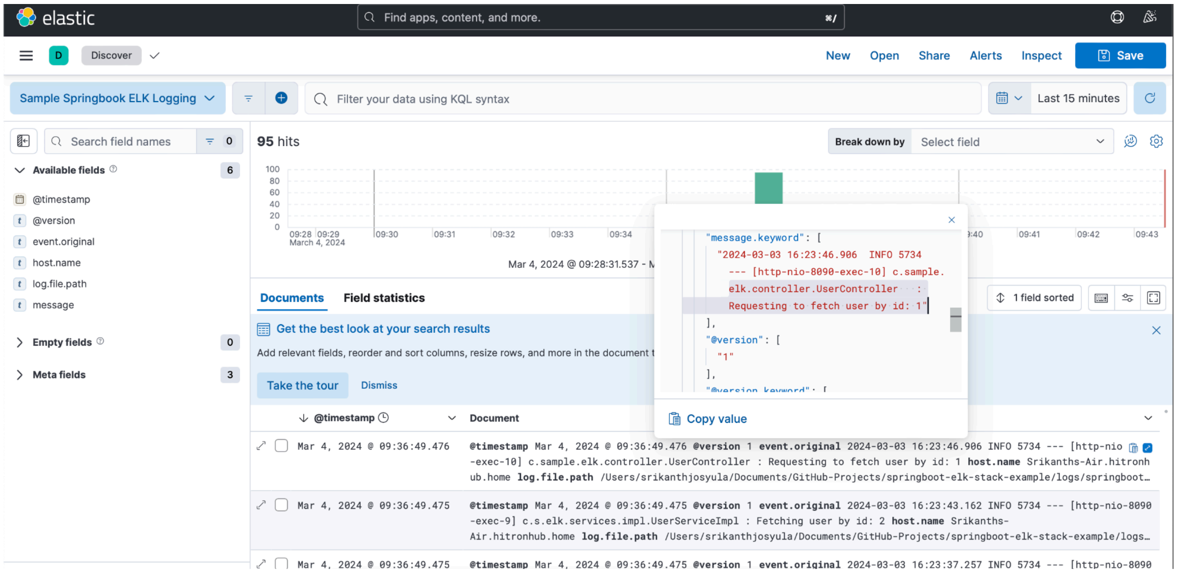
Timestamp field: @timestamp

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

✓ Your index pattern matches 1 source.

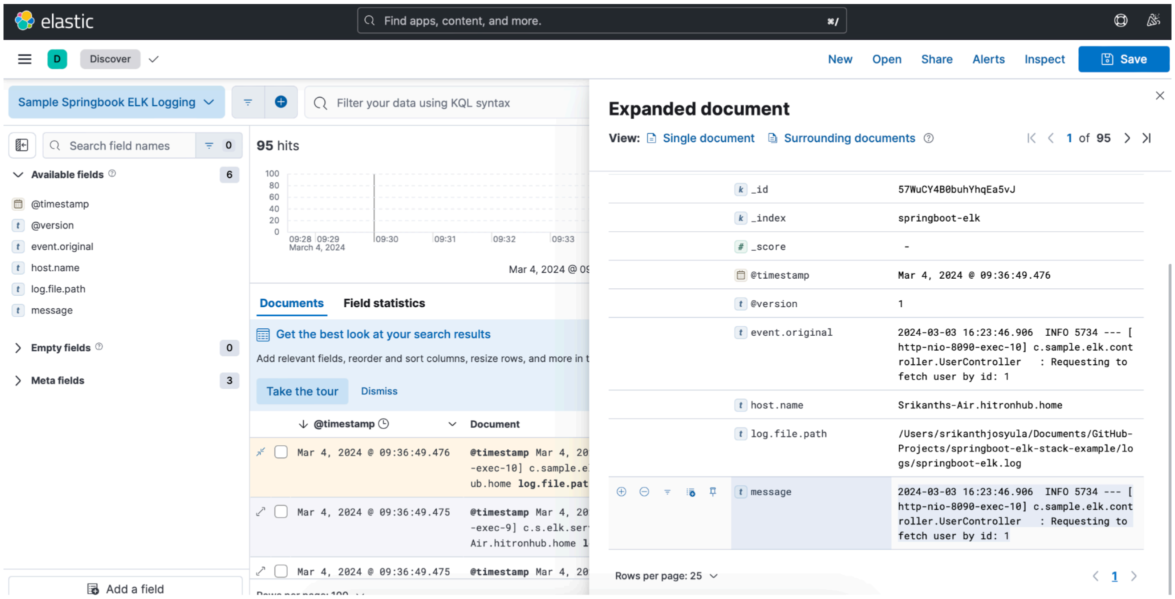
All sources	Matchi
springboot-elk	Inde

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



```
"message.keyword": [
  "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"
],
"@version": [
  "1"
],
"@version.keyword": [
```

```
Mar 4, 2024 @ 09:36:49.476   @timestamp Mar 4, 2024 @ 09:36:49.476 @version 1 event.original 2024-03-03 16:23:46.906 INFO 5734 --- [http-nio
                             -exec-10] c.sample.elk.controller.UserController : Requesting to fetch user by id: 1 host.name Srikanths-Air.hitronh
                             ub.home log.file.path /Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs/springboot…
Mar 4, 2024 @ 09:36:49.475   @timestamp Mar 4, 2024 @ 09:36:49.475 @version 1 event.original 2024-03-03 16:23:43.162 INFO 5734 --- [http-nio-8090
                             -exec-9] c.s.elk.services.impl.UserServiceImpl : Fetching user by id: 2 host.name Srikanths-
                             Air.hitronhub.home log.file.path /Users/srikanthjosyula/Documents/GitHub-Projects/springboot-elk-stack-example/logs…
Mar 4, 2024 @ 09:36:49.475   @timestamp Mar 4, 2024 @ 09:36:49.475 @version 1 event.original 2024-03-03 16:23:37.257 INFO 5734 --- [http-nio-8090
```



Expanded document

View: Single document | Surrounding documents — 1 of 95

_id	57WuCY4B0buhYhqEa5vJ
_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/srikanthjosyula/Documents/GitHub-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

```
Mar 4, 2024 @ 09:36:49.476   @timestamp Mar 4, 20
                             -exec-10] c.sample.e
                             ub.home log.file.pat
Mar 4, 2024 @ 09:36:49.475   @timestamp Mar 4, 20
                             -exec-9] c.s.elk.ser
                             Air.hitronhub.home l
Mar 4, 2024 @ 09:36:49.475   @timestamp Mar 4, 20
```