**Steps to setup ELK for centralizing the logs**

For MacOS local setup

1. Download Elasticsearch, Kibana and Logstash from website of elastic and unzip it on the desired folder.

For Elasticsearch https://www.elastic.co/downloads/elasticsearch

For Kibana https://www.elastic.co/downloads/kibana

For Logstash https://www.elastic.co/downloads/logstash

1. To solve the gatekeeper issue run this command to quarantine the jdk.app of Elasticsearch

**sudo xattr -r -d com.apple.quarantine /path/to/elasticsearch/jdk.app**

**Gatekeeper issue**: Gatekeeper is a security feature of the macOS operating system by Apple. It enforces code signing and

verifies downloaded applications before allowing them to run, thereby reducing the likelihood of inadvertently executing malware.

1. Run Elasticsearch from terminal go to the Elasticsearch directory and run the command

**./bin/elasticsearch**

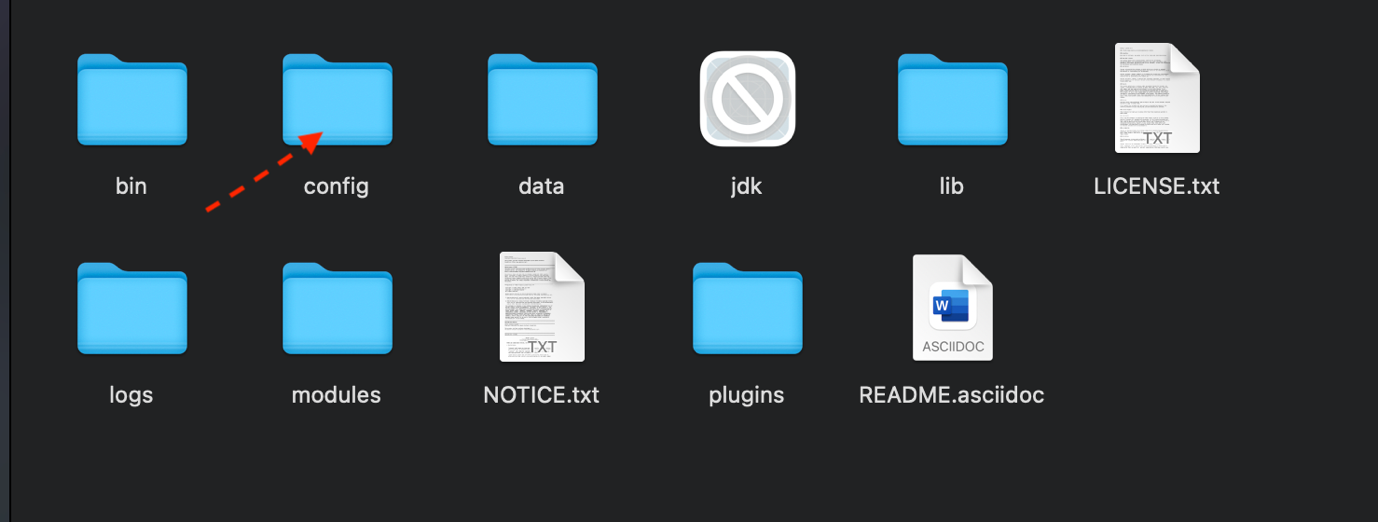
1. Now the Elasticsearch self-configured its SSL certificate and given the basic credentials for login. Copy those credentials and save it for further uses.

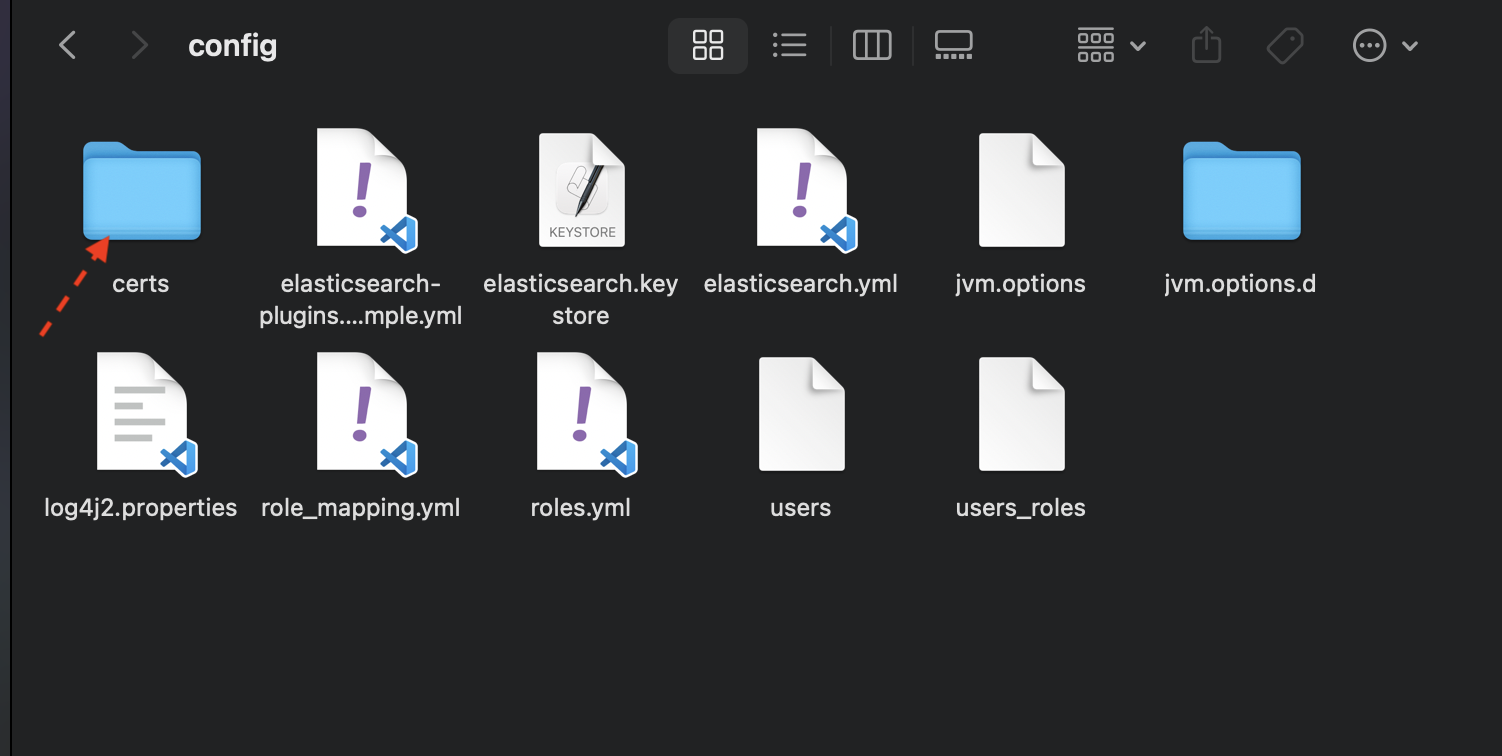
Elastic Search default username is ‘elastic’

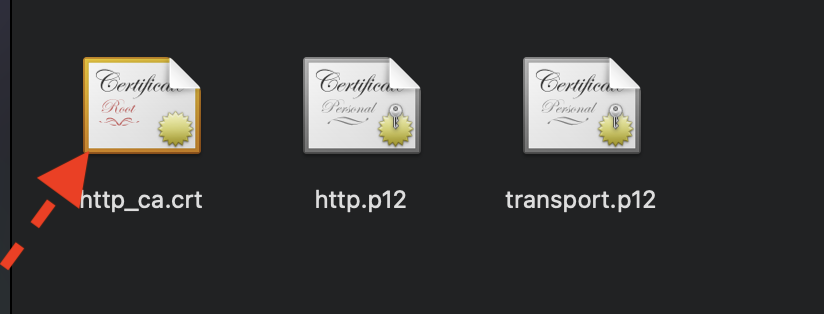
1. Now add the Elasticsearch certificate for the system trust store using this command

**sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <path\_to\_certificate>.crt**

Usually, we can get the Elasticsearch certificates from path of elastic search <version info>/config/certs/http\_ca.cert



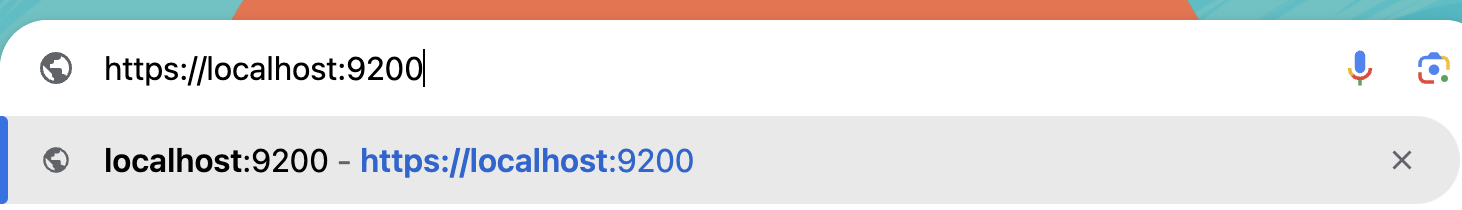


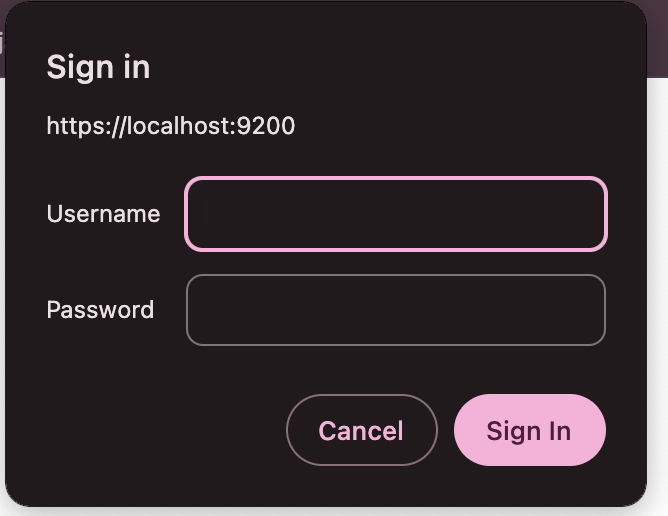


1. Now again run elasticsearch from terminal go to the elasticsearch directory and run the command

**./bin/elasticsearch**

1. We can check that from typing the URL on web browser   <https://locahost:9200> and use the credentials.



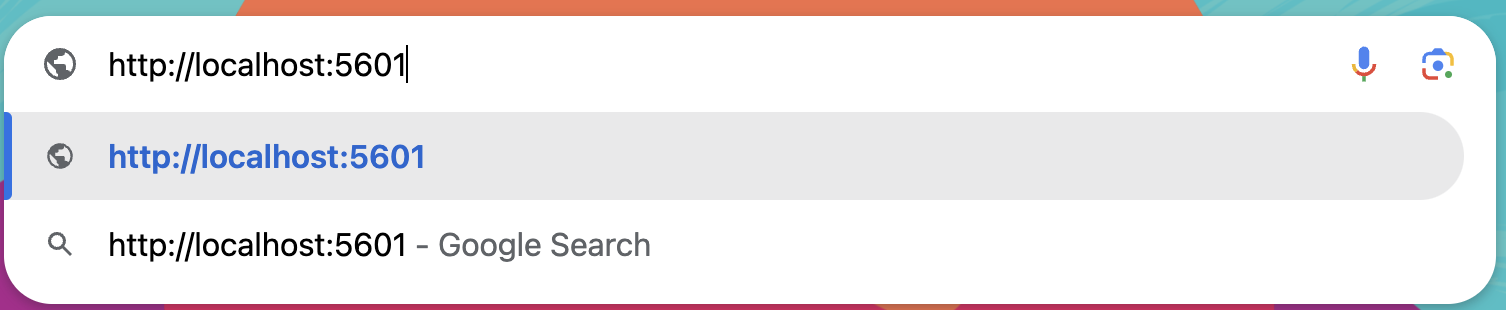


1. Now run the Kibana from terminal go to the Kibana directory and run command

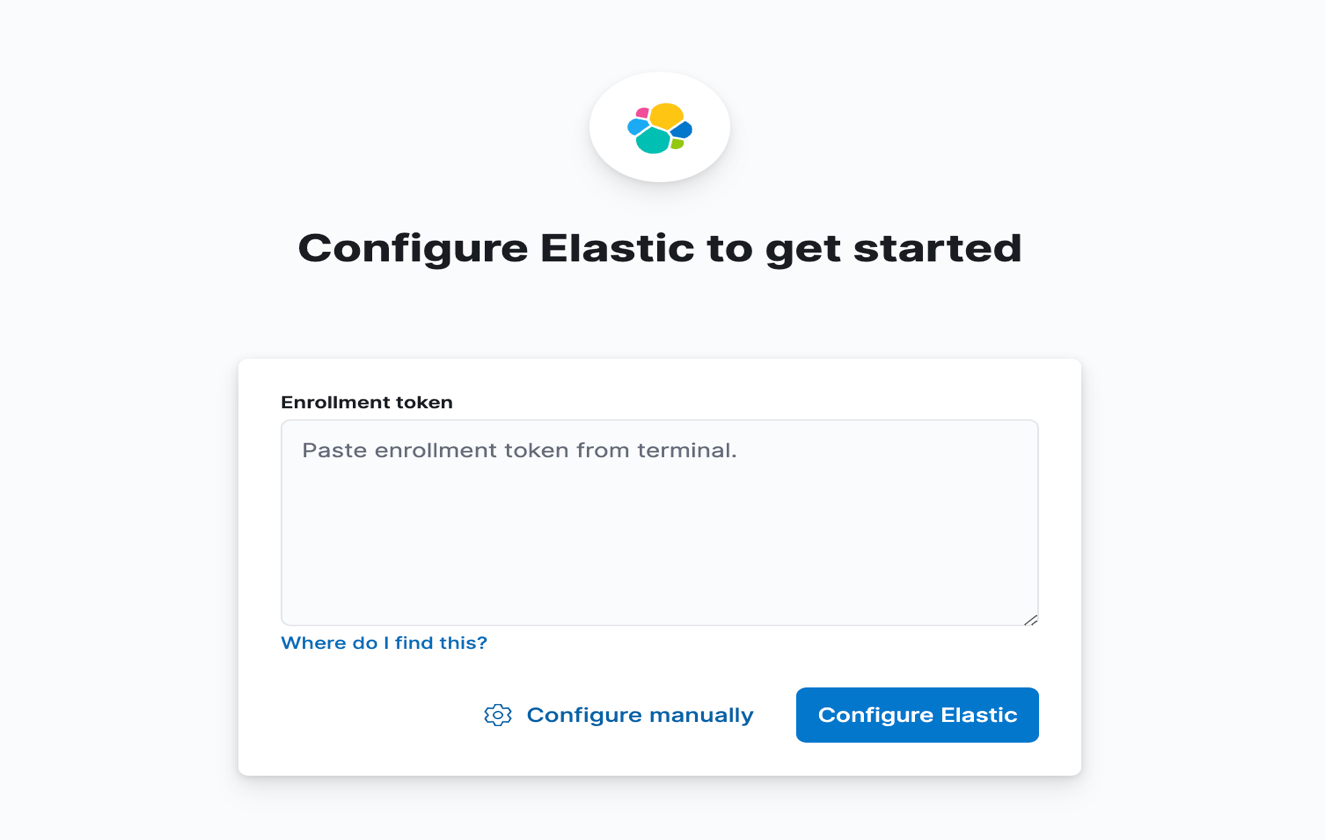
**./bin/kibana**

1. We can check that from typing the URL on web browser it also gives us the top for login

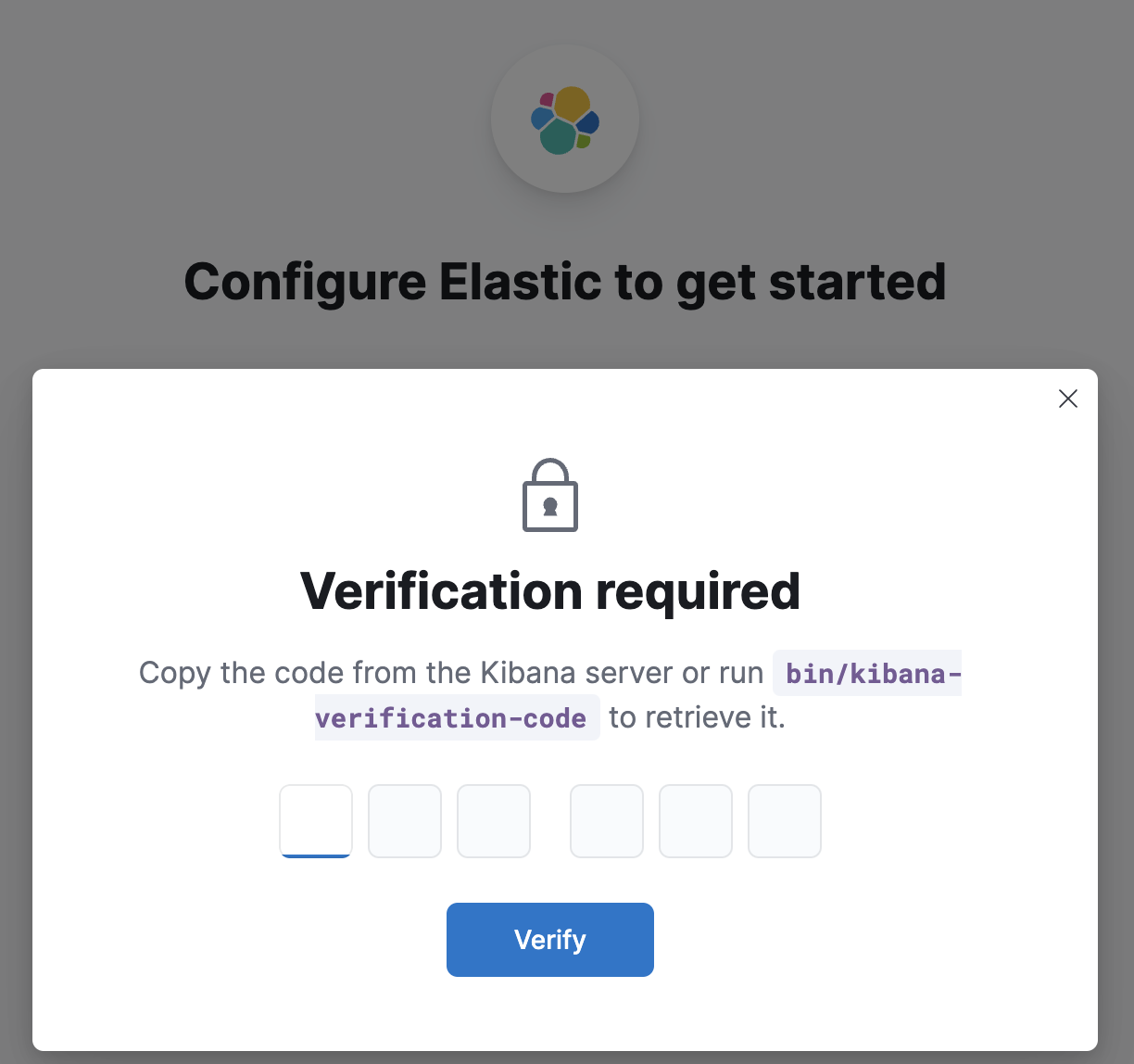
[**http://localhost:5601**](http://localhost:5601)

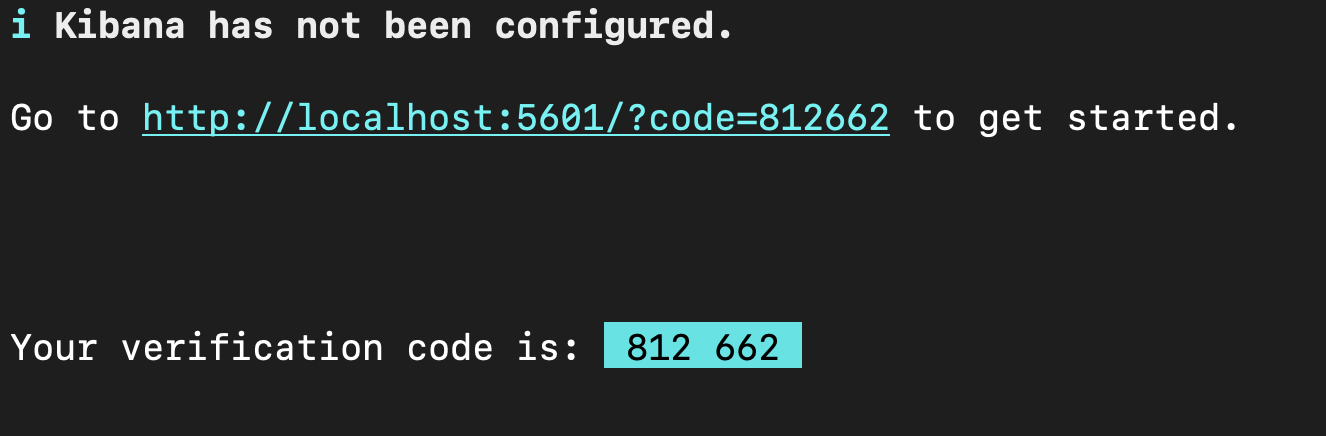


1. kibana is asking for elasticsearch token we can get if when we run elasticsearch first time use that token then use credentials for login into kibana.

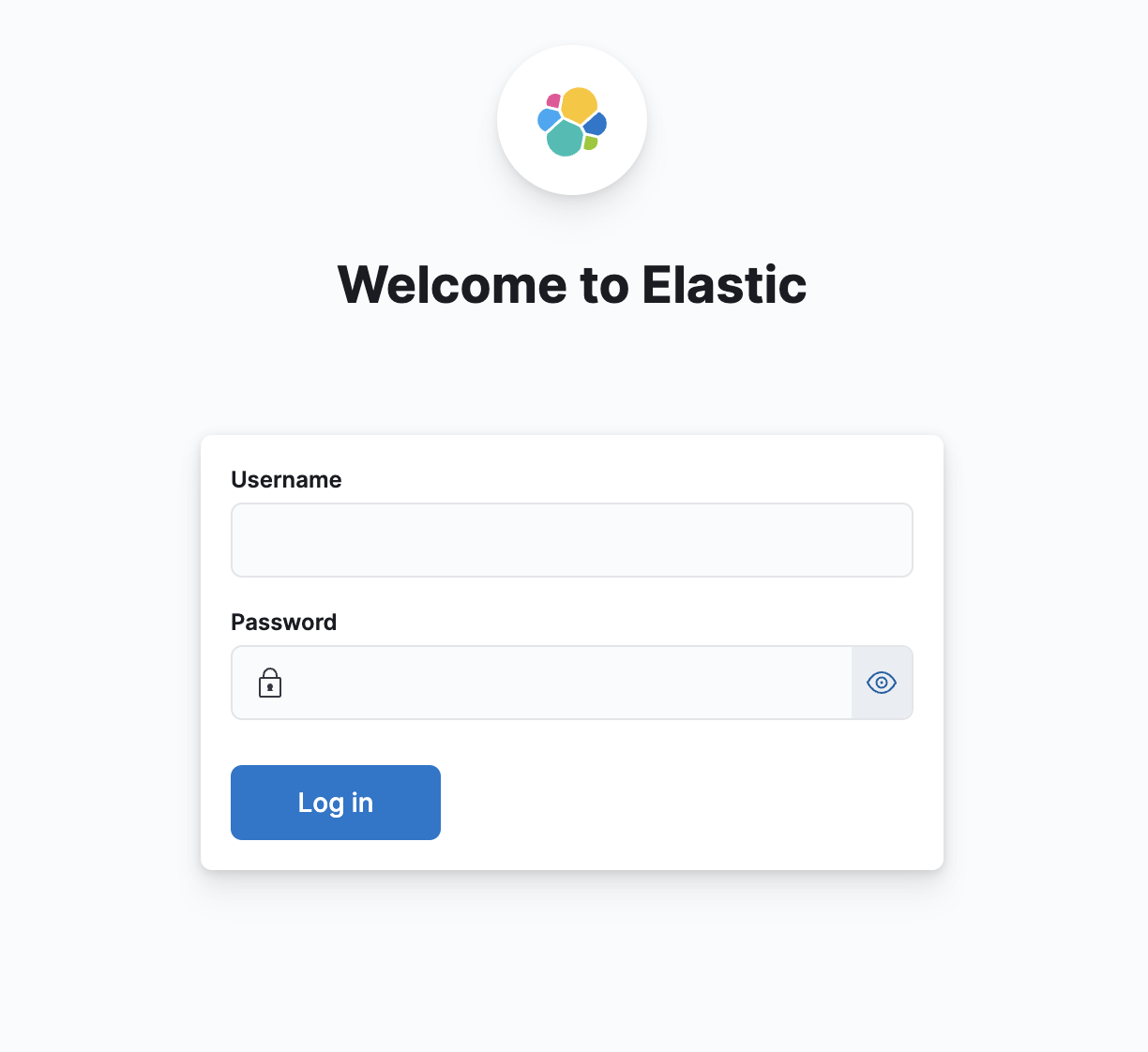


Give the token to kibana and then it will ask for OPT which we can get in terminal from where we run our kibana.

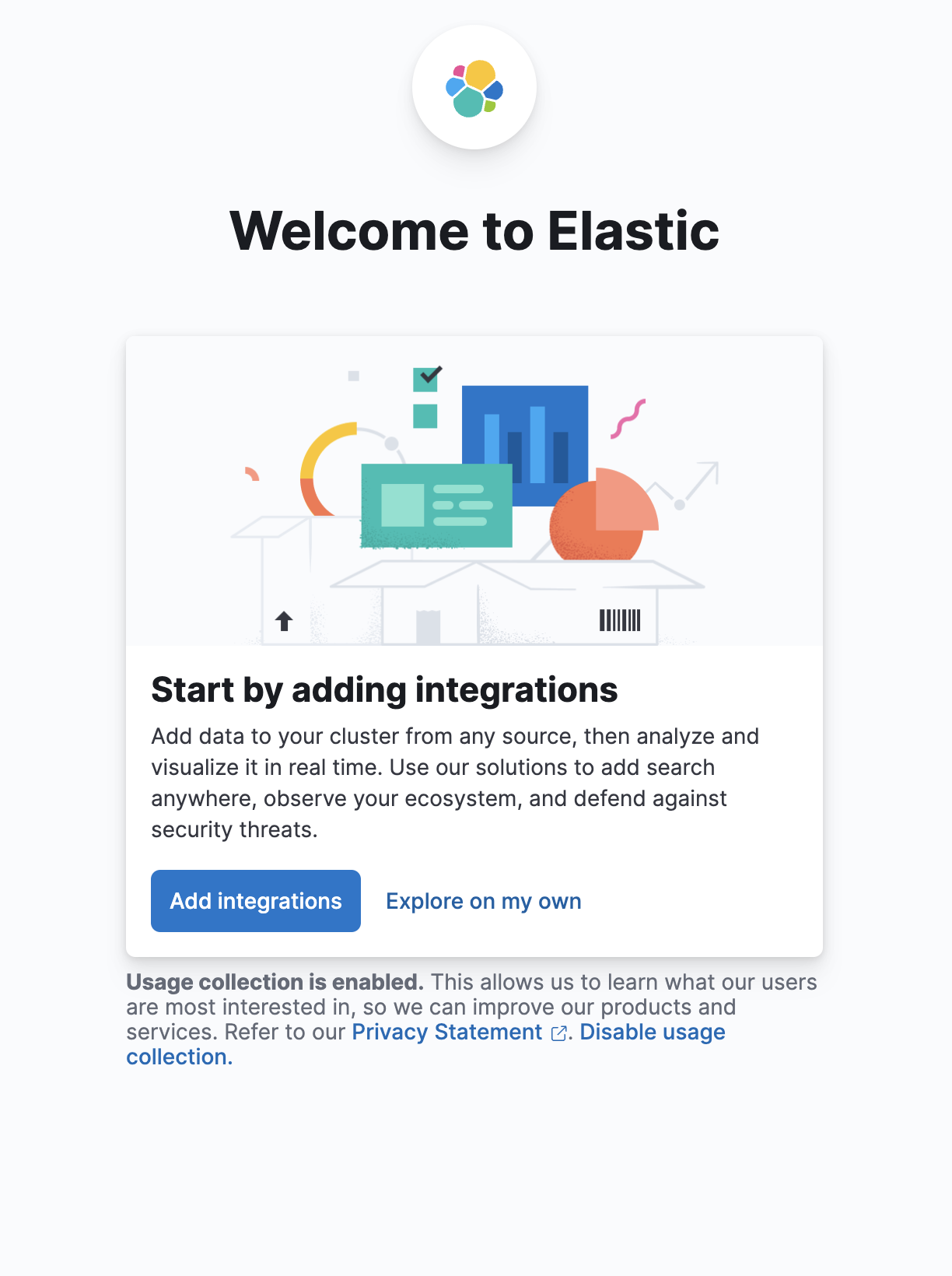


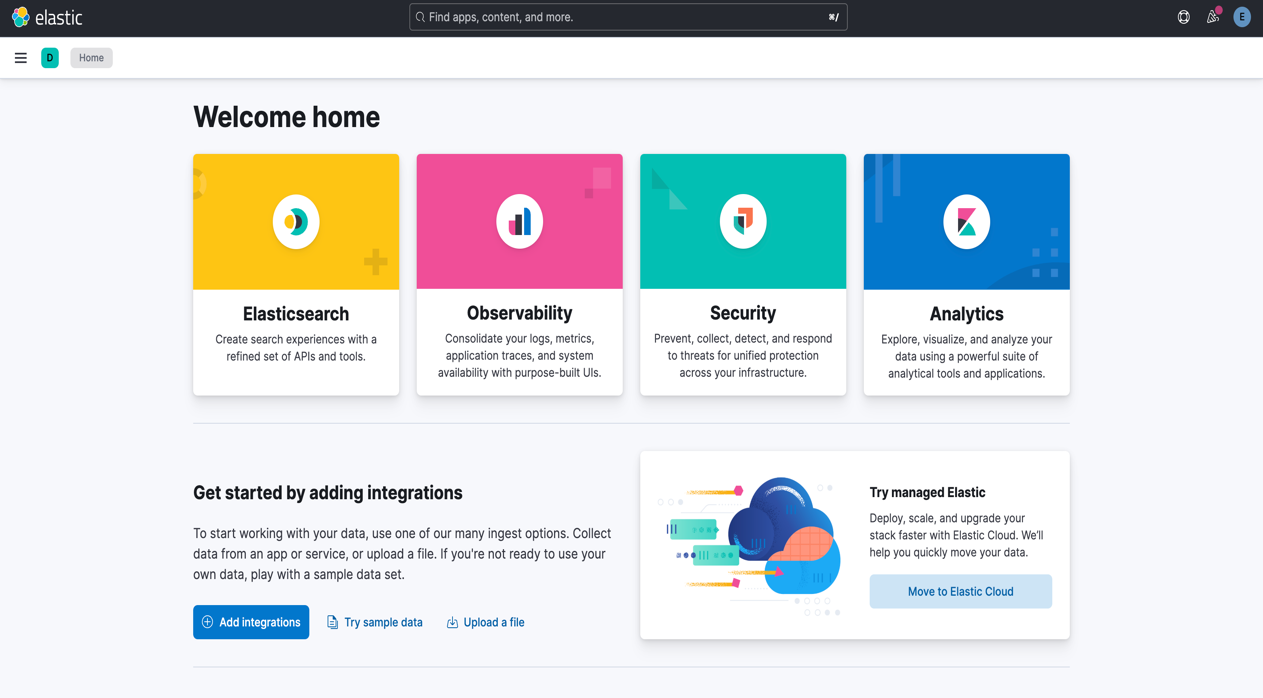


After OTP verification it will ask you for the credentials



Give the credentials and it will land you to next page where it will ask about integration.





1. After that we need create the logstash filter to send the logs to elasticsearch. For that went to the confing folder of the logstash and create a logstash.conf file and write the filter in this file.

In that filter give the path of your log file, username, password and certificate path of elasticsearch.

You can also mention about the index name on that filter.

Basic logstash filter look like that.

input {

file {

path => "Path/to/your/log/file" # Update with the actual path to your log file

start\_position => "beginning" # Start reading the file from the beginning

sincedb\_path => "/dev/null" # Prevent Logstash from remembering the last read position

}

}

filter {

grok {

match => {

"message" => "%{TIMESTAMP\_ISO8601:timestamp} - %{LOGLEVEL:log\_level} - %{GREEDYDATA:log\_message}"

}

}

date {

match => ["timestamp", "yyyy-MM-dd HH:mm:ss,SSS"]

target => "@timestamp"

}

}

output {

elasticsearch {

hosts => ["https://localhost:9200"] # Elasticsearch host (update if necessary)

index => "index/name" # Name of the index in Elasticsearch

ssl => true

cacert => "elasticsearch/certificate/path"

user => "elastic"

password => "password of elasticsearch"

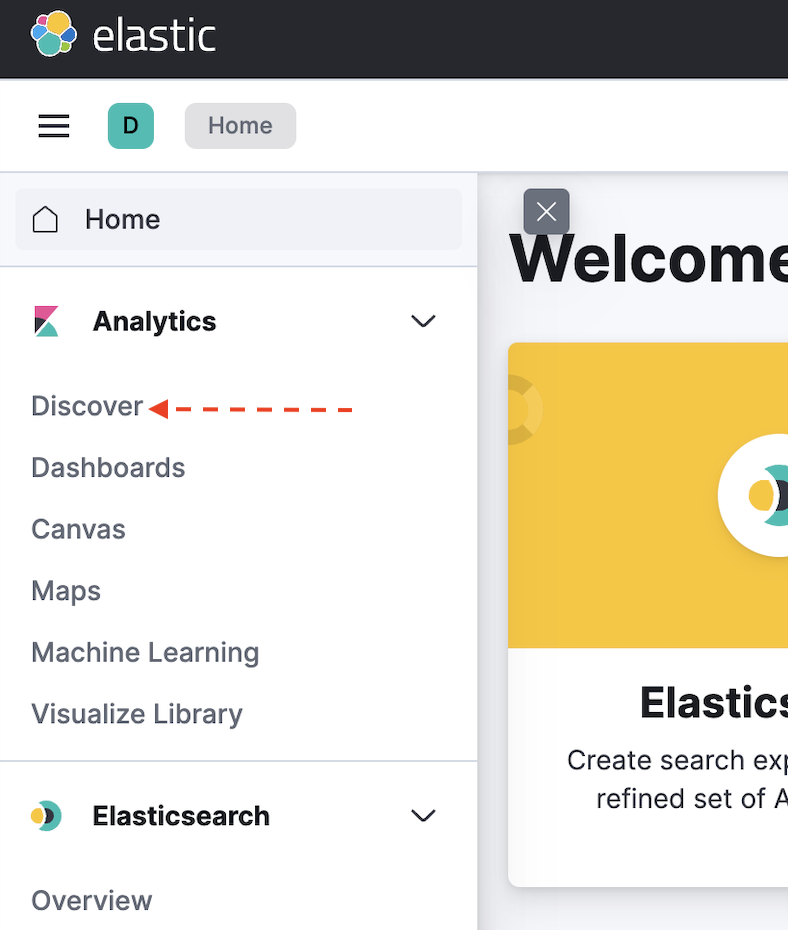
}

}

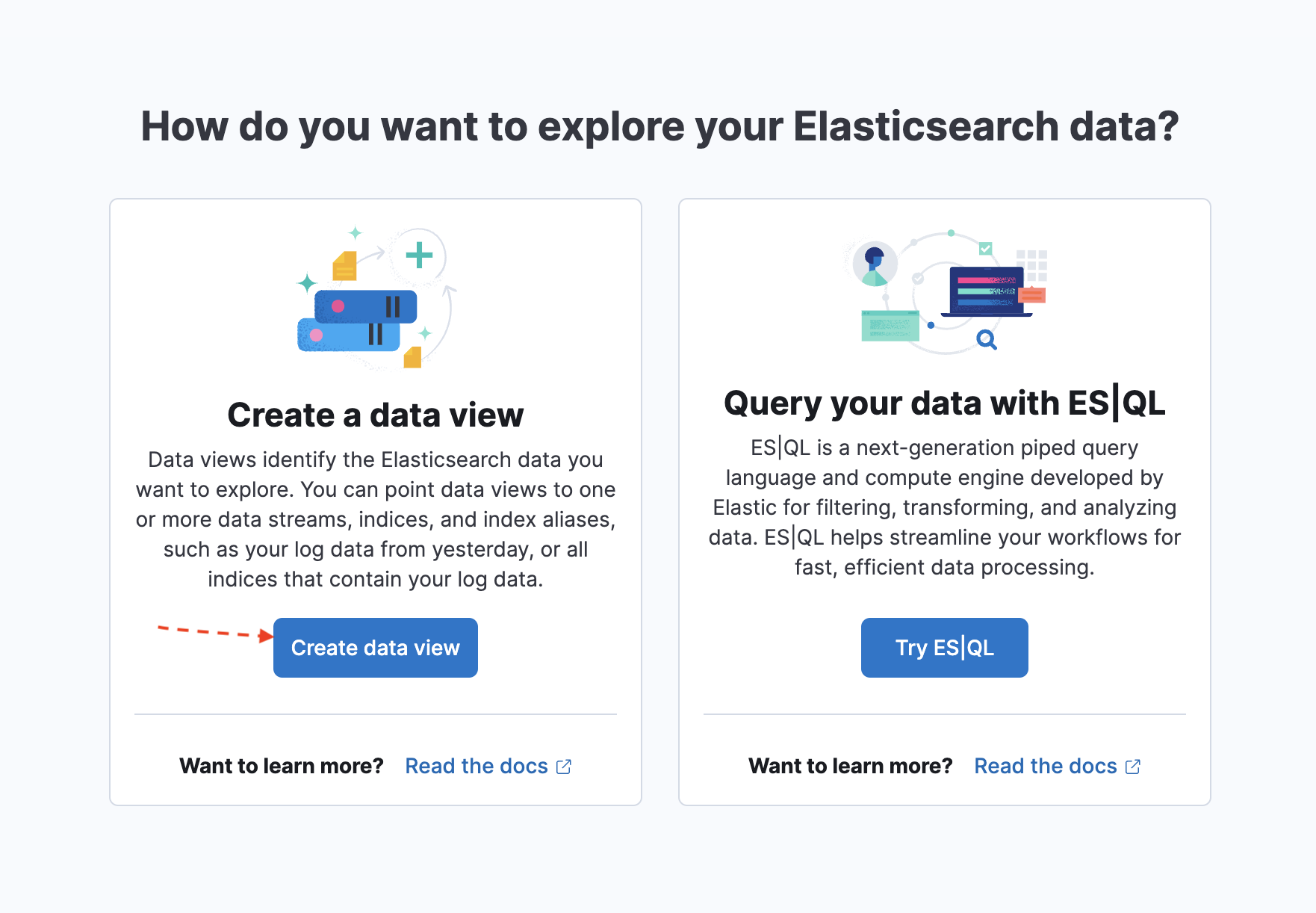
1. After that we run the logstash pipeline using this command from logstash directory to run the logstash pipeline.

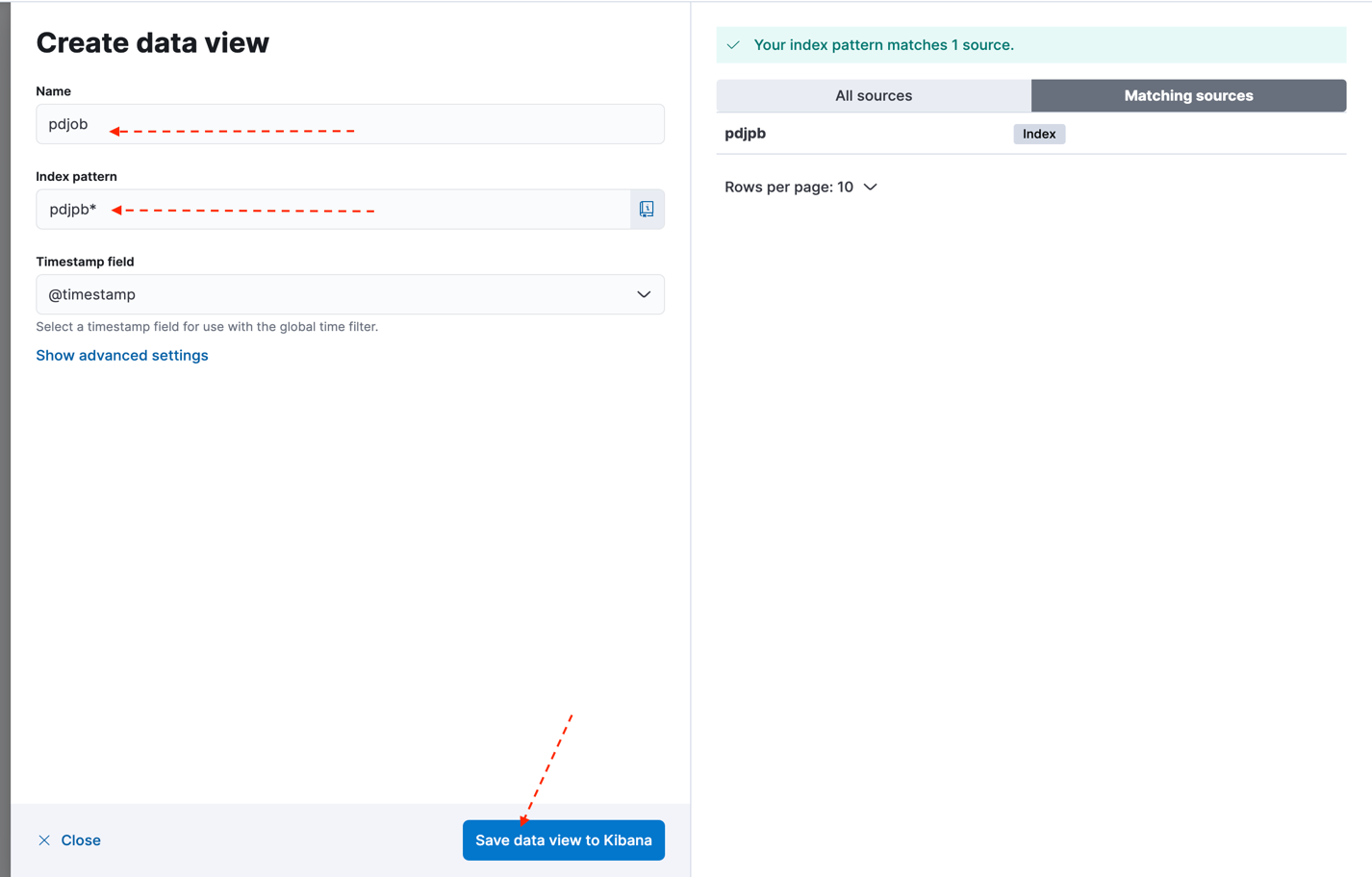
**./bin/logstash -f config/logstash.conf**

1. After that went to Kibana click on three lines on top left corner then open the discover tab.



1. Now create the data view to see the logs.



1. Now give name to the data view and then match the index pattern for which index pattern you want to create view. Now click to save data view to kibana on the bottam.  
   
2. Now final outcomes look like that.

