ELK

Your Name:- Lokesh Rajendra Khadse
Eidiko Systems Integrators
EmpID:- 1177

What is ELK?

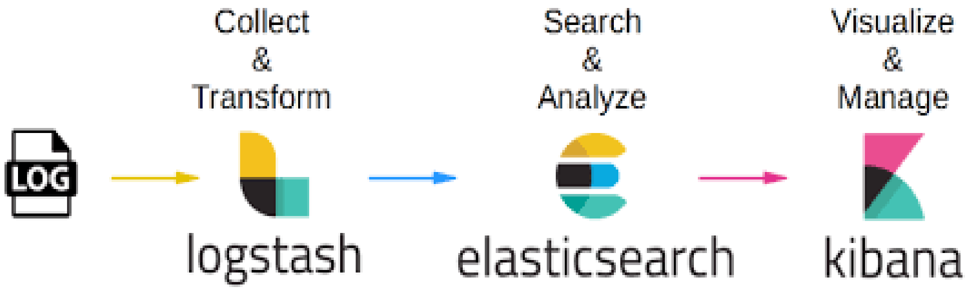
1. ELK is an acronym that stands for Elasticsearch, Logstash, and Kibana.

Elasticsearch: Search and analytics engine that helps you quickly find and analyze large amounts of data. It stores data in a way that makes it easy to search .

Logstash: Data collection and processing tool. Transforms data from various sources before sending it to Elasticsearch for indexing.

Kibana: Visualization dashboard for Elasticsearch data.

Diagram

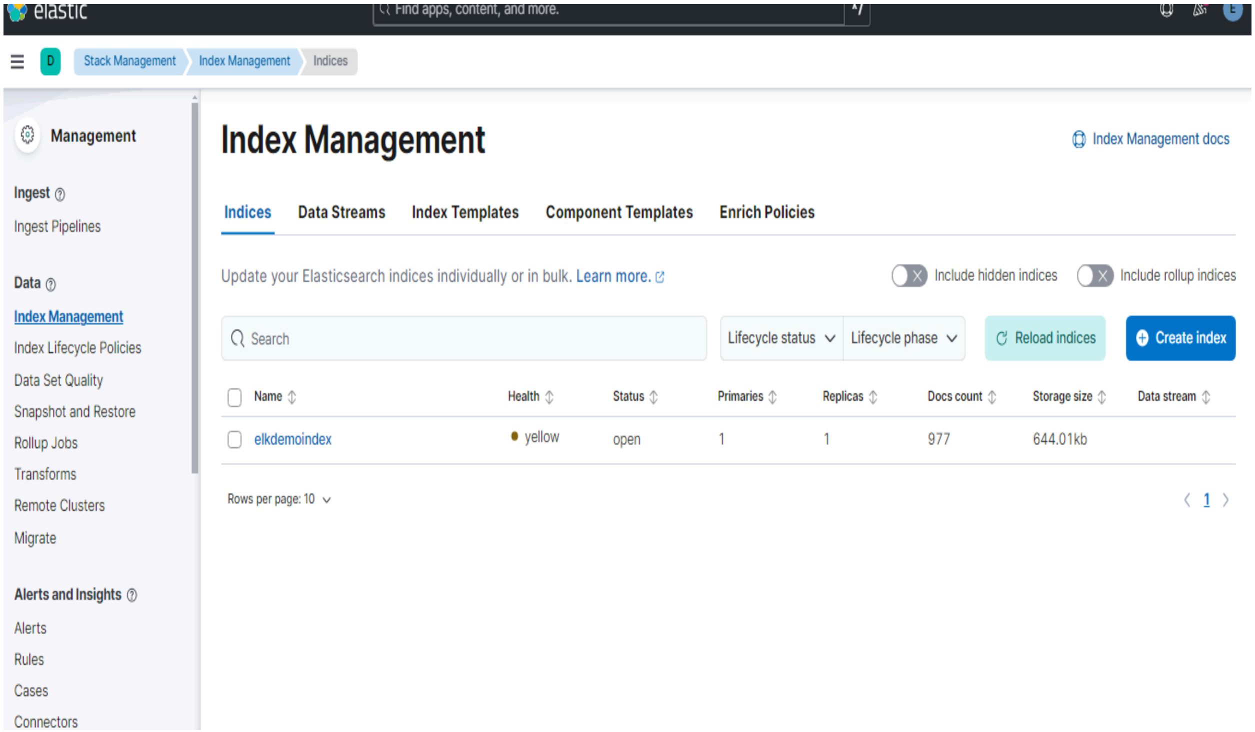


logback-spring.xml

```
<configuration>

   <appender name="COMMON_FILE"
class="ch.qos.logback.core.rolling.RollingFileAppender">

       <file>C:/Users/Sreenivas
Bandaru/Desktop/MICROSERVICES/Logs/project.log</file>

       <encoder>

           <pattern>%d{yyyy-MM-dd HH:mm:ss} %-5level [%thread] %logger{36} -
%msg%n</pattern>

       </encoder>

       <rollingPolicy
class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">

           <fileNamePattern>C:/Users/Sreenivas
Bandaru/Desktop/MICROSERVICES/Logs/spring-%d{yyyy-MM-dd}.%i.log</fileNamePatter
n>

           <maxFileSize>10MB</maxFileSize>

           <maxHistory>30</maxHistory>

       </rollingPolicy>

   </appender>



   <root level="INFO">

       <appender-ref ref="COMMON_FILE" />

   </root>

</configuration>
```

Steps

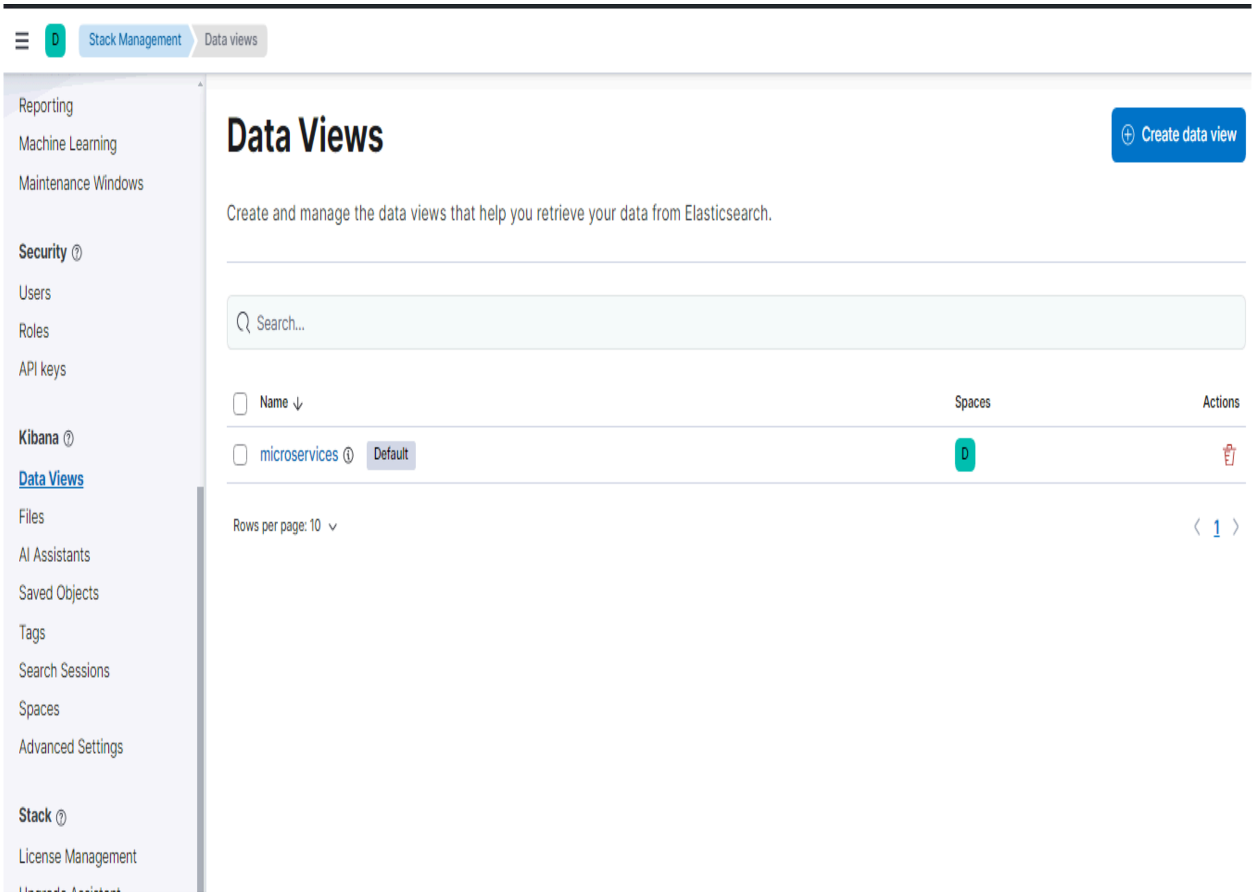
1. Download ElasticSearch , Logstash and kibana and extract it.
2. Run ElasticSearch , and kibana
3. Then after, go to the ElasticSearch\bin folder and open the batch file of ElasticSearch.
4. ElasticSearch generates password and token.
5. Then after, go to the Kibana/bin folder and open the batch file of Kibana.
6. Kibana give us port number where we have to go there and login on this port with the help of ElasticSearch credentials.
7. After that we have to update the Logstash file and save it.
8. Open cmd and run this command :- `logstash.bat -f ./config/logstash-sample.conf`
9. If this process is properly worked or connected then data will be shown on your logstash cmd in json format.
10. Then go to kibana in kibana, go to stack management and create Dataview and save it. (match your index name properly)
11. Now you are able to see your logs with the help of all this process.



Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
elkdemoindex	● yellow	open	1	1	977	644.01kb	



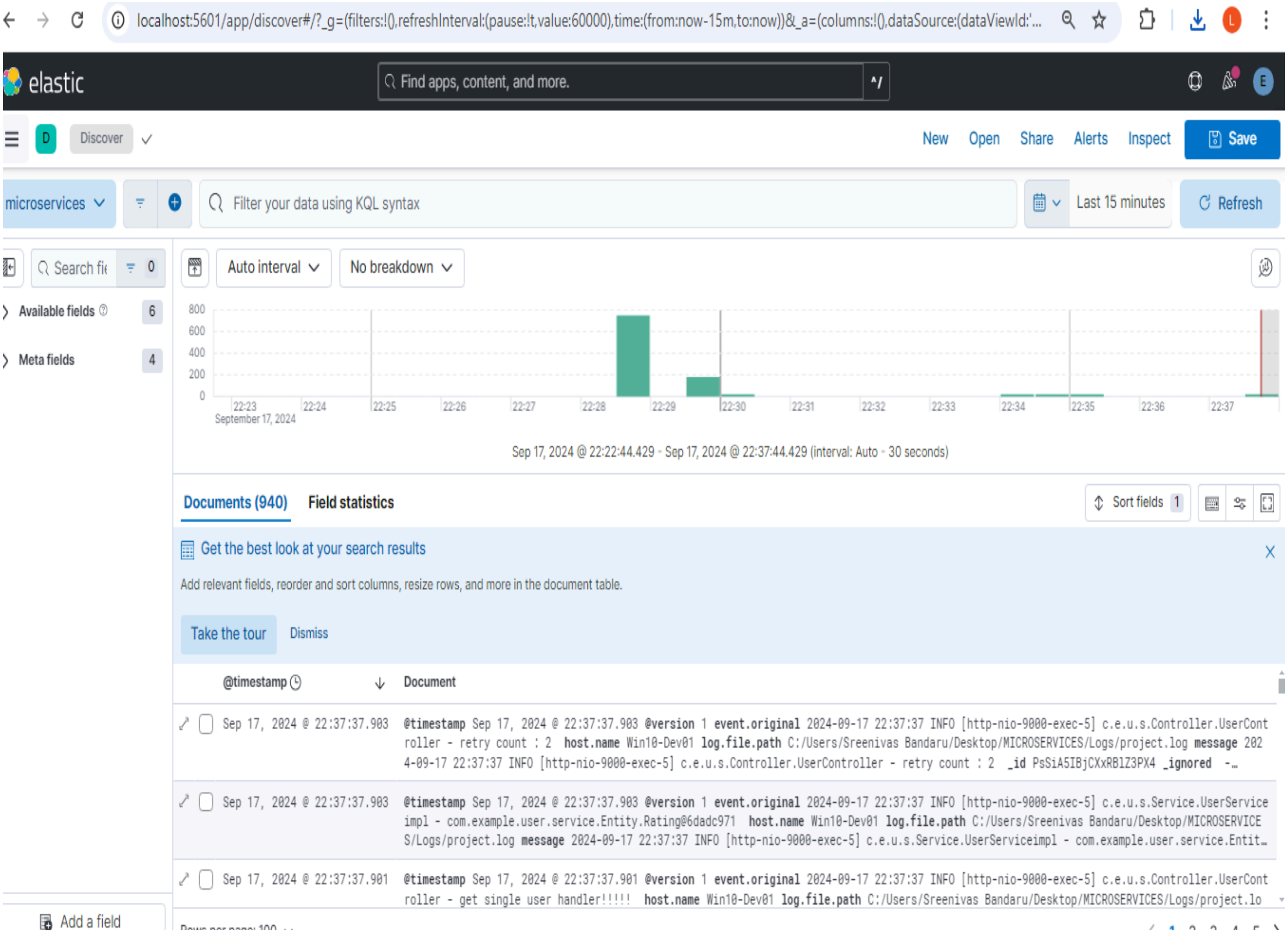
Data Views

Create and manage the data views that help you retrieve your data from Elasticsearch.

□	Name ↓	Spaces	Actions
□	microservices ⓘ Default	D	🗑

Rows per page: 10 ⌄

〈 1 〉



localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-15m,to:now))&_a=(columns:!(),dataSource:(dataViewId:'...

Sep 17, 2024 @ 22:22:44.429 - Sep 17, 2024 @ 22:37:44.429 (interval: Auto - 30 seconds)

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

```
@timestamp                   Document
Sep 17, 2024 @ 22:37:37.903  @timestamp Sep 17, 2024 @ 22:37:37.903 @version 1 event.original 2024-09-17 22:37:37 INFO [http-nio-9000-exec-5] c.e.u.s.Controller.UserCont
                             roller - retry count : 2  host.name Win10-Dev01 log.file.path C:/Users/Sreenivas Bandaru/Desktop/MICROSERVICES/Logs/project.log message 202
                             4-09-17 22:37:37 INFO [http-nio-9000-exec-5] c.e.u.s.Controller.UserController - retry count : 2  _id PsSiA5IBjCXxRBlZ3PX4 _ignored  -…
Sep 17, 2024 @ 22:37:37.903  @timestamp Sep 17, 2024 @ 22:37:37.903 @version 1 event.original 2024-09-17 22:37:37 INFO [http-nio-9000-exec-5] c.e.u.s.Service.UserService
                             impl - com.example.user.service.Entity.Rating@6dadc971  host.name Win10-Dev01 log.file.path C:/Users/Sreenivas Bandaru/Desktop/MICROSERVICE
                             S/Logs/project.log message 2024-09-17 22:37:37 INFO [http-nio-9000-exec-5] c.e.u.s.Service.UserServiceimpl - com.example.user.service.Entit…
Sep 17, 2024 @ 22:37:37.901  @timestamp Sep 17, 2024 @ 22:37:37.901 @version 1 event.original 2024-09-17 22:37:37 INFO [http-nio-9000-exec-5] c.e.u.s.Controller.UserCont
                             roller - get single user handler!!!!!  host.name Win10-Dev01 log.file.path C:/Users/Sreenivas Bandaru/Desktop/MICROSERVICES/Logs/project.lo
```