DIGITALHOUSE

Implementação do stack ELK

Certified Tech Developer
The Ultimate Degree

1) Criação do arquivo de configuração de Logstash

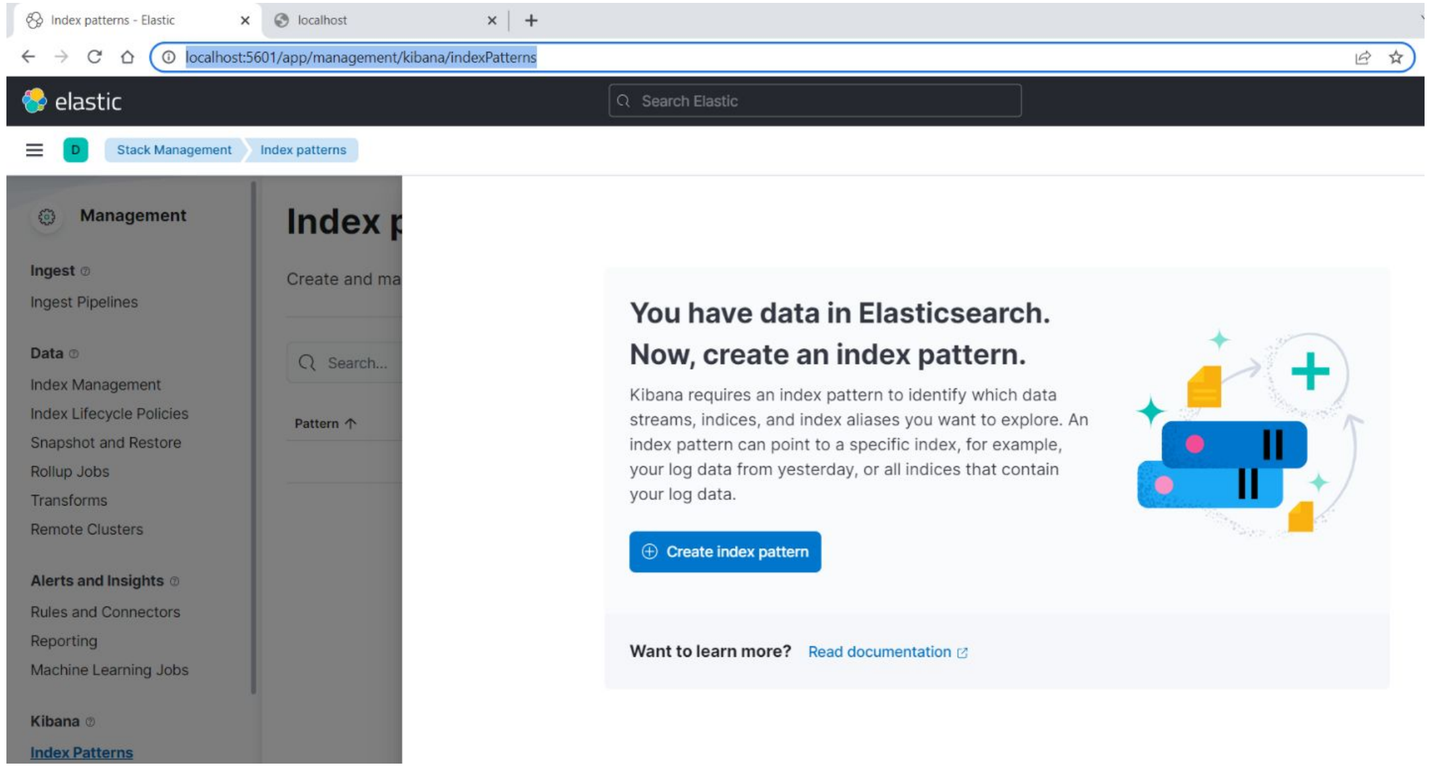
Vamos gerar um arquivo de configuração **dh-spring-elk-conf.conf** dentro da pasta conf de Logstash com as configurações de input, filter e output.

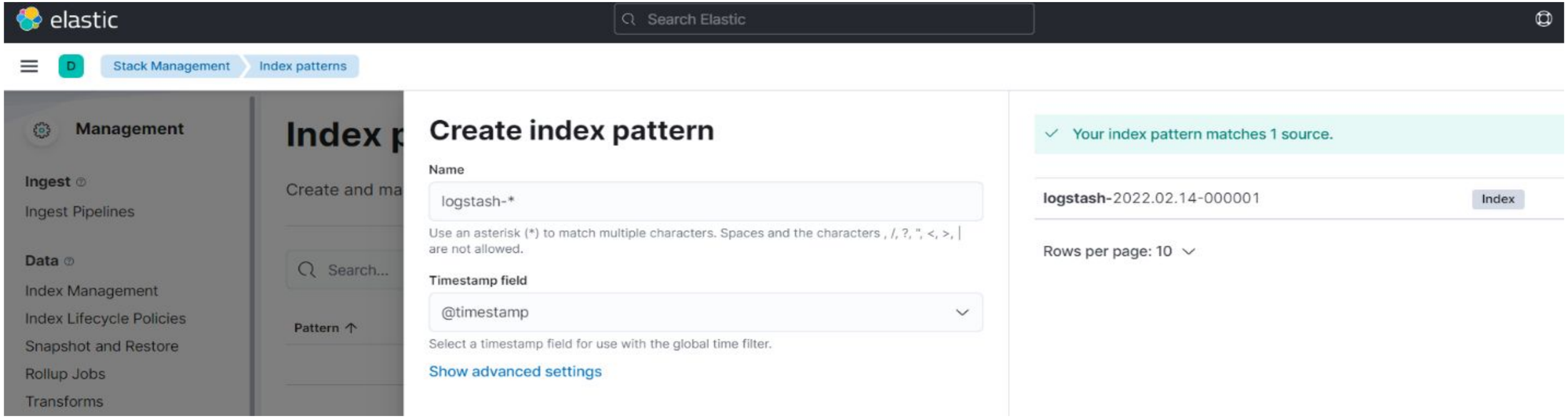
Este arquivo será utilizado para a inicialização do Logstash.: **logstash -f ../config/dh-spring-elk-conf.conf**

2) Criação de índice em Kibana

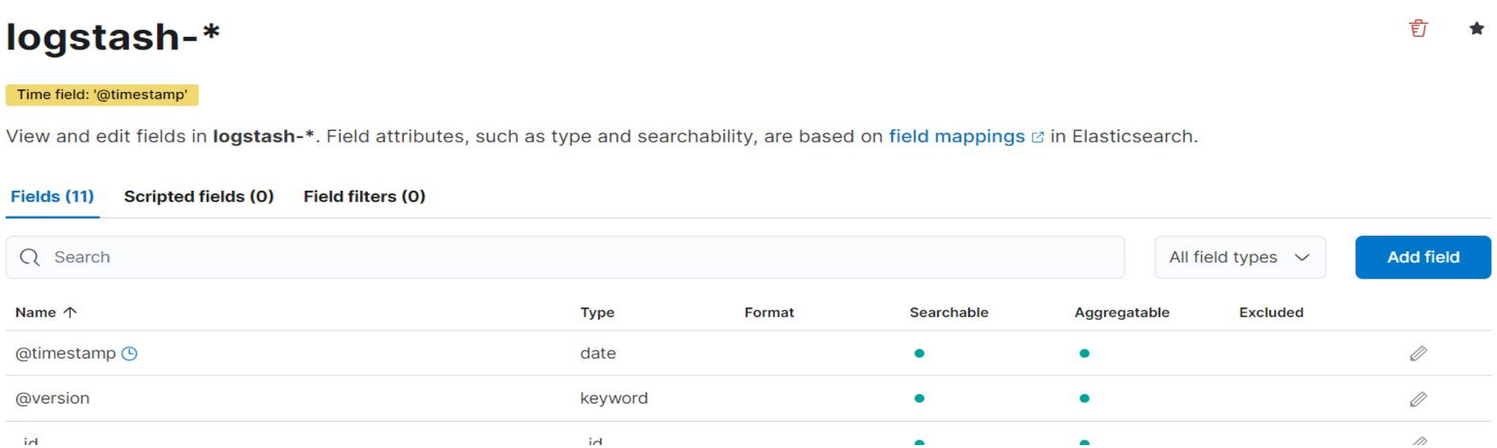
Vamos gerar o **índice** em Kibana com base no padrão de login que Logstash tem ao pegar a informação do nosso log de aplicação e colocá-lo no Elastic. Se inicia com **logstash-***.

Introduzimos a seguinte URL http://localhost:5601/app/management/kibana/indexPatterns e selecionamos a opção de criação de índice.





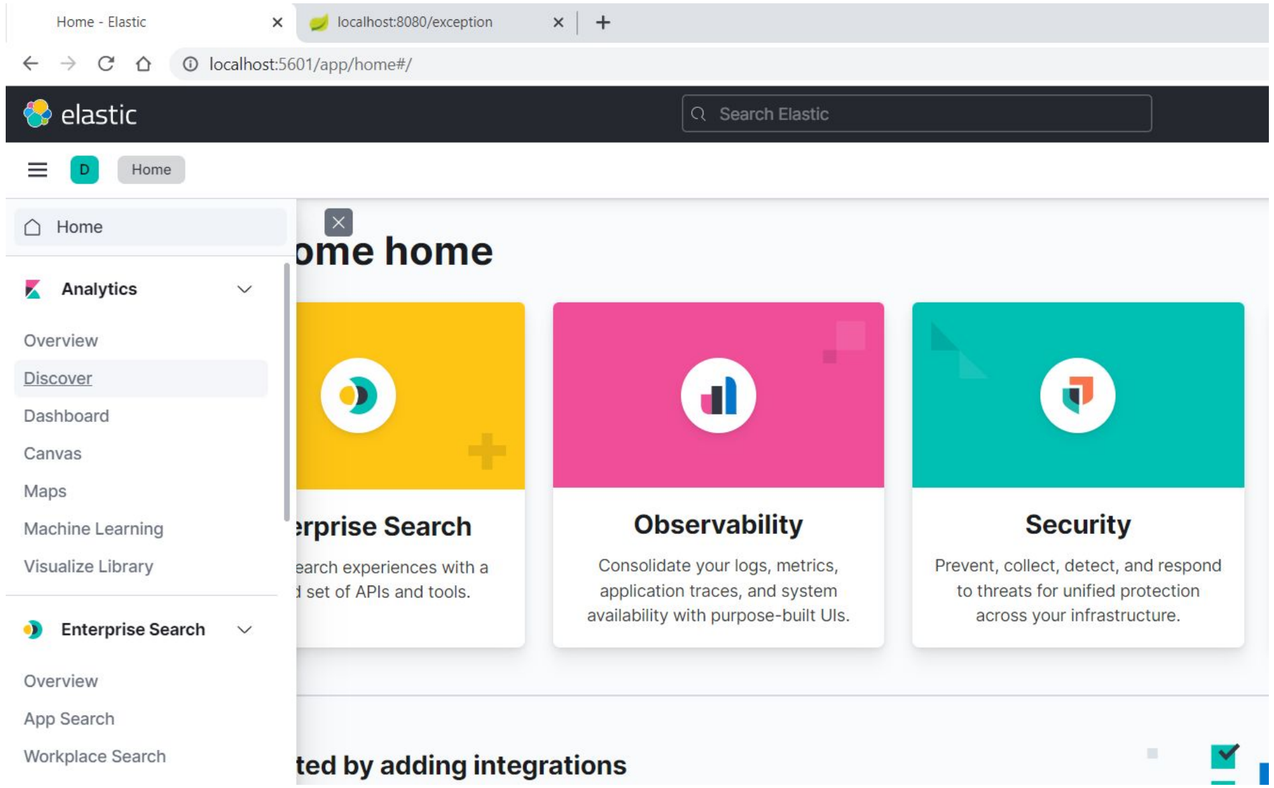
Após confirmar a criação, veremos a tela de êxito com os *fields* indexados do nosso índice.

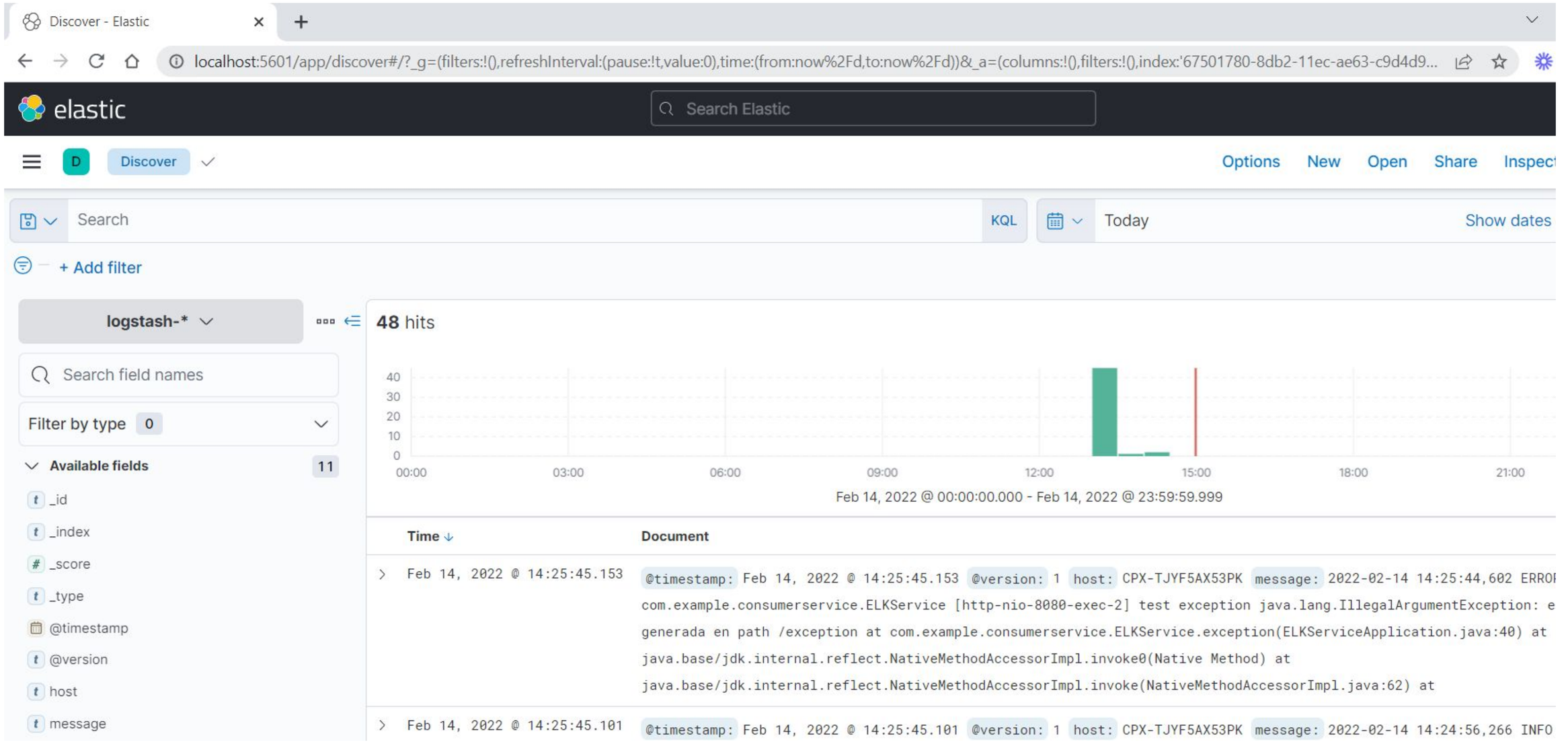


3) Visualização de logs centralizados

Neste terceiro passo, realizamos interações com a nossa aplicação que gera os logs no nosso arquivo analisado pelo Logstash, a fim de alimentar a nossa base de dados em Elasticsearch.

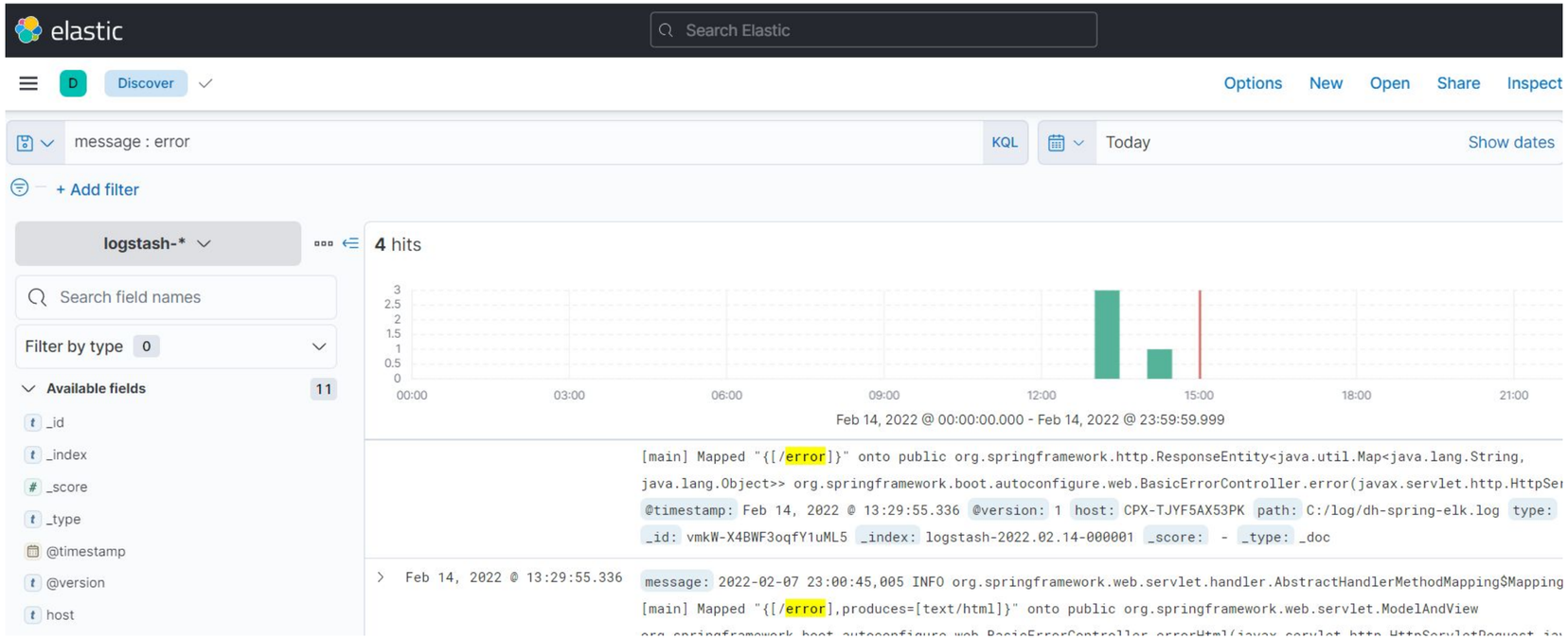
Ao finalizar, podemos ver as entradas em Kibana nos direcionando à opção **Analytics** e selecionando **Discover**.




Discover - Elastic
localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now%2Fd,to:now%2Fd))&_a=(columns:!(),filters:!(),index:'67501780-8db2-11ec-ae63-c9d4d9...
elastic
Search Elastic
D
Discover
Options
New
Open
Share
Inspect
Search
KQL
Today
Show dates
+ Add filter
logstash-*
Search field names
Filter by type 0
Available fields 11
_id
_index
_score
_type
@timestamp
@version
host
message
48 hits
40
30
20
10
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Feb 14, 2022 @ 00:00:00.000 - Feb 14, 2022 @ 23:59:59.999
Time
Document
Feb 14, 2022 @ 14:25:45.153
@timestamp: Feb 14, 2022 @ 14:25:45.153 @version: 1 host: CPX-TJYF5AX53PK message: 2022-02-14 14:25:44,602 ERROR
com.example.consumerservice.ELKService [http-nio-8080-exec-2] test exception java.lang.IllegalArgumentException: e
generada en path /exception at com.example.consumerservice.ELKService.exception(ELKServiceApplication.java:40) at
java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at
java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at
Feb 14, 2022 @ 14:25:45.101
@timestamp: Feb 14, 2022 @ 14:25:45.101 @version: 1 host: CPX-TJYF5AX53PK message: 2022-02-14 14:24:56,266 INFO

4) Consultas por queries KQL

Finalmente, Kibana nos permite realizar consultas nos dados indexados em Elasticsearch usando a sintaxe do framework KQL. Podemos, por exemplo, consultar todos os erros onde mensagem que está logada é do tipo erro:



DIGITALHOUSE

Muito obrigado!