Iniciando o Elasticsearch em Docker

Docker Desktop Windows

```
PS E:\projetos\docker-elasticsearch\elastic> wsl -l -v
  NAME                   STATE           VERSION
* docker-desktop-data    Running         2
  docker-desktop         Running         2
  Ubuntu-20.04           Running         2
```

```
PS E:\projetos\docker-elasticsearch\elastic> wsl -d docker-desktop
LAPTOP-V176DRSL:/tmp/docker-desktop-root/mnt/host/e/projetos/docker-elasticsearch/elastic# sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
LAPTOP-V176DRSL:/tmp/docker-desktop-root/mnt/host/e/projetos/docker-elasticsearch/elastic#
```

Docker Wsl2 Linux

```
feliciani@LAPTOP-V176DRSL:~$ sudo sysctl -w vm.max_map_count=262144
[sudo] password for feliciani:
vm.max_map_count = 262144
```

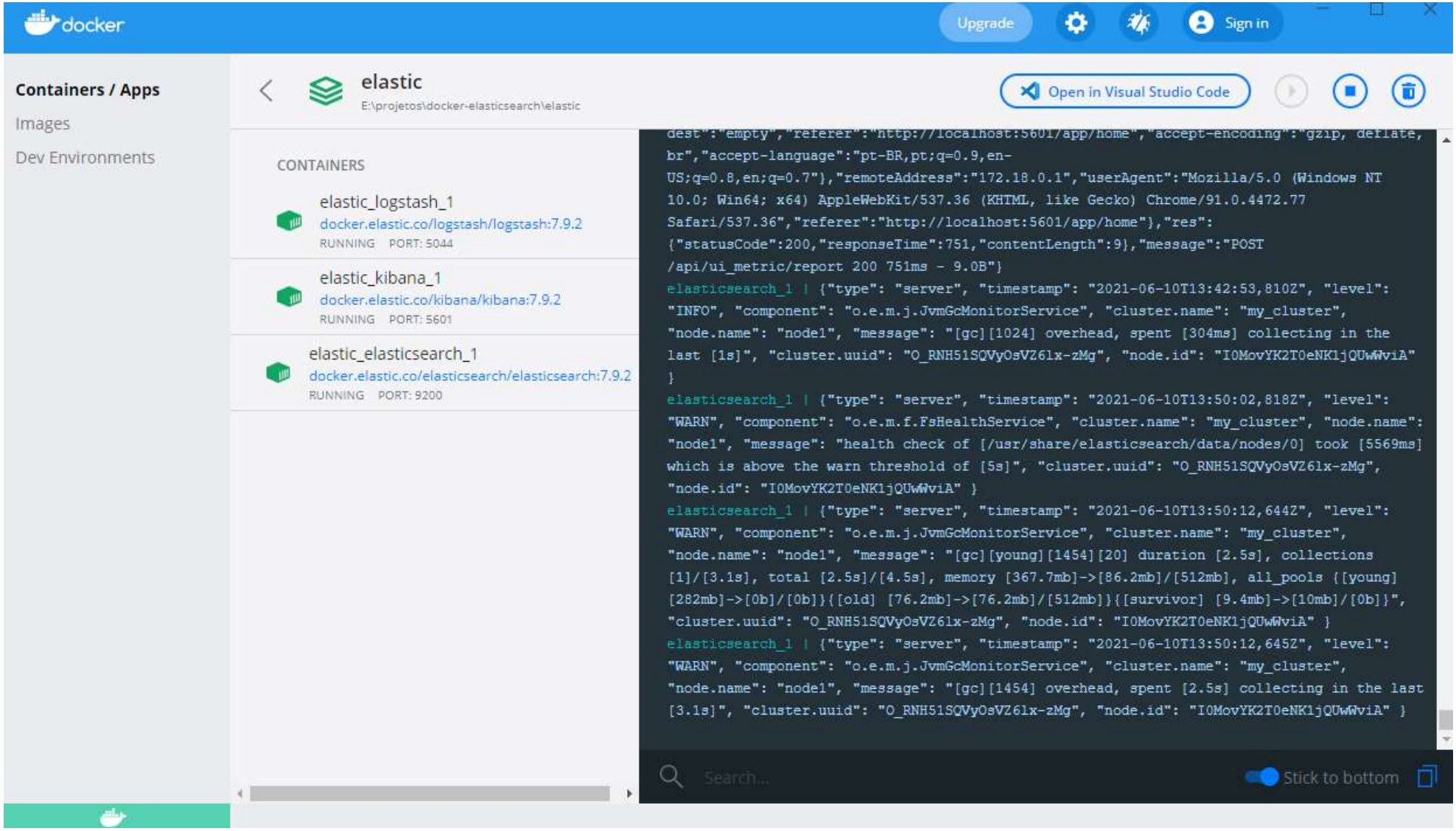
Docker Desktop Windows

```
PS E:\projetos\docker-elasticsearch\elastic> docker-compose up -d
Docker Compose is now in the Docker CLI, try `docker compose up`

Starting elastic_elasticsearch_1 ... done
Starting elastic_kibana_1        ... done
Starting elastic_logstash_1      ... done
```

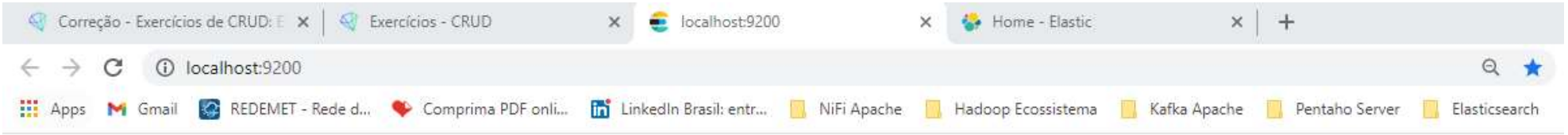
```
PS E:\projetos\docker-elasticsearch\elastic> docker ps
CONTAINER ID   IMAGE                                                  COMMAND                  CREATED        STATUS          PORTS                                            NAMES
d3d012693acc   docker.elastic.co/logstash/logstash:7.9.2              "/usr/local/bin/dock…"   17 hours ago   Up 33 minutes   0.0.0.0:5044->5044/tcp, :::5044->5044/tcp, 0.0.0.0:9600->9600/tcp, :::9600->9600/tcp   elastic_logstash_1
ca700688aa0d   docker.elastic.co/kibana/kibana:7.9.2                  "/usr/local/bin/dumb…"   17 hours ago   Up 33 minutes   0.0.0.0:5601->5601/tcp, :::5601->5601/tcp                                       elastic_kibana_1
37a2fb5958f4   docker.elastic.co/elasticsearch/elasticsearch:7.9.2    "/tini -- /usr/local…"   17 hours ago   Up 34 minutes   0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp                             elastic_elasticsearch_1
```

Docker


docker
Upgrade
Sign in
Containers / Apps
Images
Dev Environments
elastic
E:\projetos\docker-elasticsearch\elastic
Open in Visual Studio Code
CONTAINERS
elastic_logstash_1
docker.elastic.co/logstash/logstash:7.9.2
RUNNING PORT: 5044
elastic_kibana_1
docker.elastic.co/kibana/kibana:7.9.2
RUNNING PORT: 5601
elastic_elasticsearch_1
docker.elastic.co/elasticsearch/elasticsearch:7.9.2
RUNNING PORT: 9200
dest":"empty","referer":"http://localhost:5601/app/home","accept-encoding":"gzip, deflate, br","accept-language":"pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7"},"remoteAddress":"172.18.0.1","userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36","referer":"http://localhost:5601/app/home"},"res":{"statusCode":200,"responseTime":751,"contentLength":9},"message":"POST /api/ui_metric/report 200 751ms - 9.0B"}
elasticsearch_1 | {"type": "server", "timestamp": "2021-06-10T13:42:53,810Z", "level": "INFO", "component": "o.e.m.j.JvmGcMonitorService", "cluster.name": "my_cluster", "node.name": "node1", "message": "[gc][1024] overhead, spent [304ms] collecting in the last [1s]", "cluster.uuid": "O_RNH51SQVyOsVZ6lx-zMg", "node.id": "I0MovYK2T0eNK1jQUwWviA" }
elasticsearch_1 | {"type": "server", "timestamp": "2021-06-10T13:50:02,818Z", "level": "WARN", "component": "o.e.m.f.FsHealthService", "cluster.name": "my_cluster", "node.name": "node1", "message": "health check of [/usr/share/elasticsearch/data/nodes/0] took [5569ms] which is above the warn threshold of [5s]", "cluster.uuid": "O_RNH51SQVyOsVZ6lx-zMg", "node.id": "I0MovYK2T0eNK1jQUwWviA" }
elasticsearch_1 | {"type": "server", "timestamp": "2021-06-10T13:50:12,644Z", "level": "WARN", "component": "o.e.m.j.JvmGcMonitorService", "cluster.name": "my_cluster", "node.name": "node1", "message": "[gc][young][1454][20] duration [2.5s], collections [1]/[3.1s], total [2.5s]/[4.5s], memory [367.7mb]->[86.2mb]/[512mb], all_pools {[young] [282mb]->[0b]/[0b]}{[old] [76.2mb]->[76.2mb]/[512mb]}{[survivor] [9.4mb]->[10mb]/[0b]}", "cluster.uuid": "O_RNH51SQVyOsVZ6lx-zMg", "node.id": "I0MovYK2T0eNK1jQUwWviA" }
elasticsearch_1 | {"type": "server", "timestamp": "2021-06-10T13:50:12,645Z", "level": "WARN", "component": "o.e.m.j.JvmGcMonitorService", "cluster.name": "my_cluster", "node.name": "node1", "message": "[gc][1454] overhead, spent [2.5s] collecting in the last [3.1s]", "cluster.uuid": "O_RNH51SQVyOsVZ6lx-zMg", "node.id": "I0MovYK2T0eNK1jQUwWviA" }
Search...
Stick to bottom

Acessado o Elasticsearch

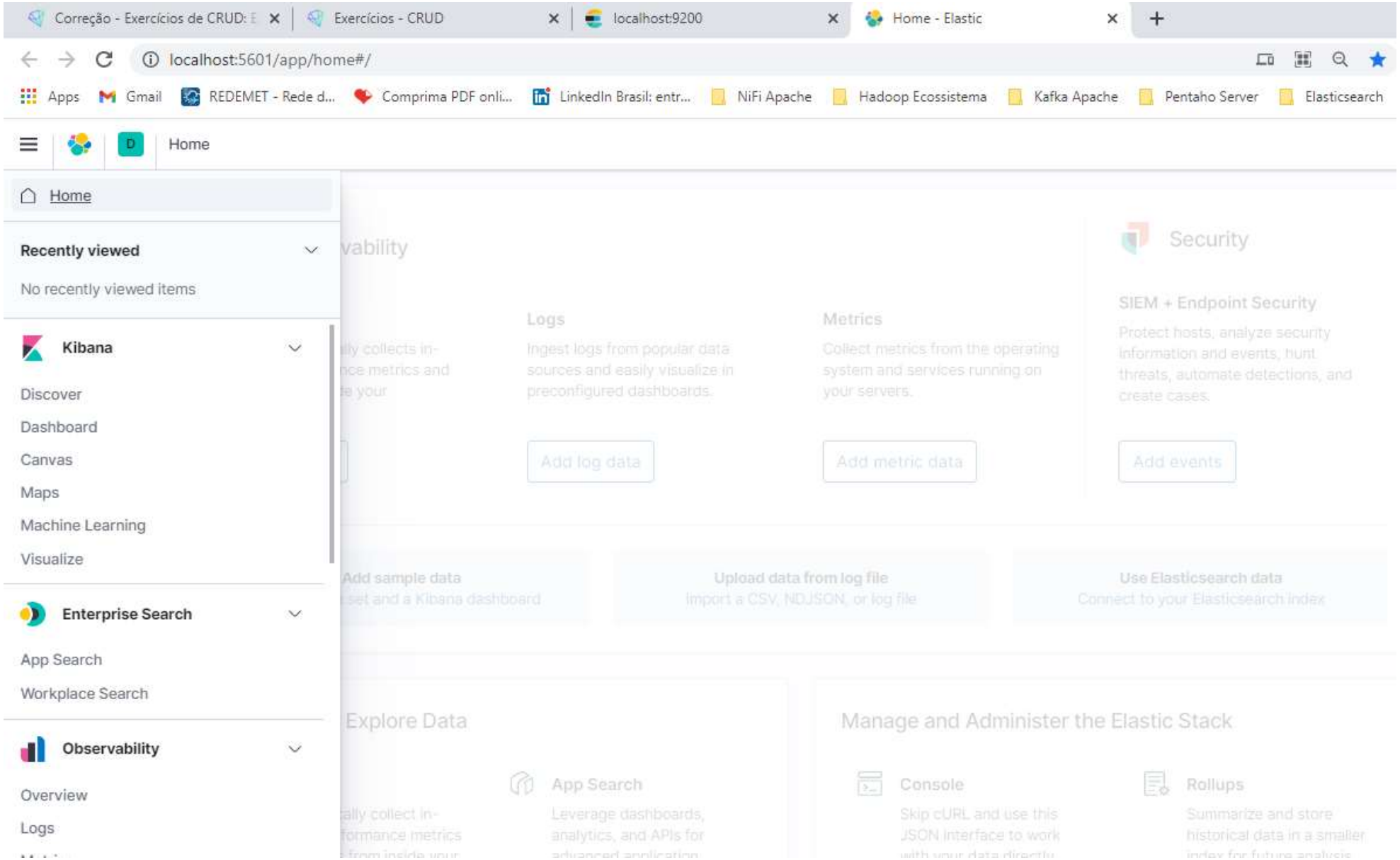
http://localhost:9200




```
{
  "name" : "node1",
  "cluster_name" : "my_cluster",
  "cluster_uuid" : "O_RNH51SQVyOsVZ61x-zMg",
  "version" : {
    "number" : "7.9.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "d34da0ea4a966c4e49417f2da2f244e3e97b4e6e",
    "build_date" : "2020-09-23T00:45:33.626720Z",
    "build_snapshot" : false,
    "lucene_version" : "8.6.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Acessando o KIBANA

http://localhost:5601



Exercitando Logstash

Down nos serviços do ElasricSearch

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ docker-compose down
Stopping elastic_kibana_1        ... done
Stopping elastic_elasticsearch_1 ... done
Removing elastic_logstash_1      ... done
Removing elastic_kibana_1        ... done
Removing elastic_elasticsearch_1 ... done
Removing network elastic_elastic
semantix@NTBSTX7158:~/treinamentos/elastic
```

1. Enviar o arquivo <local>/paris-925.logs para o Logstash, com uso do Filebeat

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ cd filebeat-7.9.2-linux-x86_64/
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ls
LICENSE.txt  data        filebeat.reference.yml  logs                                  modules.d
NOTICE.txt   fields.yml  filebeat.yml            metricbeat-8.0.0-linux-x86_64.tar.gz
README.md    filebeat    kibana                  module
```

Configurar o filebeat.yml

```
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ vi filebeat.yml
```

Entrada dos dados

Saída será logstash

Salvar o arquivo

2. Configurar e executar o logstash com as seguintes configurações

Entrada:
beats {

port => 5044

}

Saída:
elasticsearch {

hosts => [“elasticsearch:9200"]

index => “seu_nome-%{+YYYY.MM.dd}"

}

Configuração do logstash.conf

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ ls
config_vm.sh                  filebeat-7.9.2-linux-x86_64.tar.gz
data                          heartbeat-7.9.2-linux-x86_64
dataset                       heartbeat-7.9.2-linux-x86_64.tar.gz
docker-compose-windows.yml    metricbeat-7.9.2-linux-x86_64
docker-compose.yml            metricbeat-7.9.2-linux-x86_64.tar.gz
elastic-7.5.1                 pipeline
extra_config                  settings
filebeat-7.9.2-linux-x86_64
semantix@NTBSTX7158:~/treinamentos/elastic
$ sudo vi pipeline/logstash.conf
```

```
input {
  beats {
    port => 5044
  }
}

output {
  stdout {
    codec => "json"
  }
  elasticsearch {
    hosts => ["elasticsearch:9200"]
    index => "rodrigo-%{+yyyy.MM.dd}"
  }
}
```

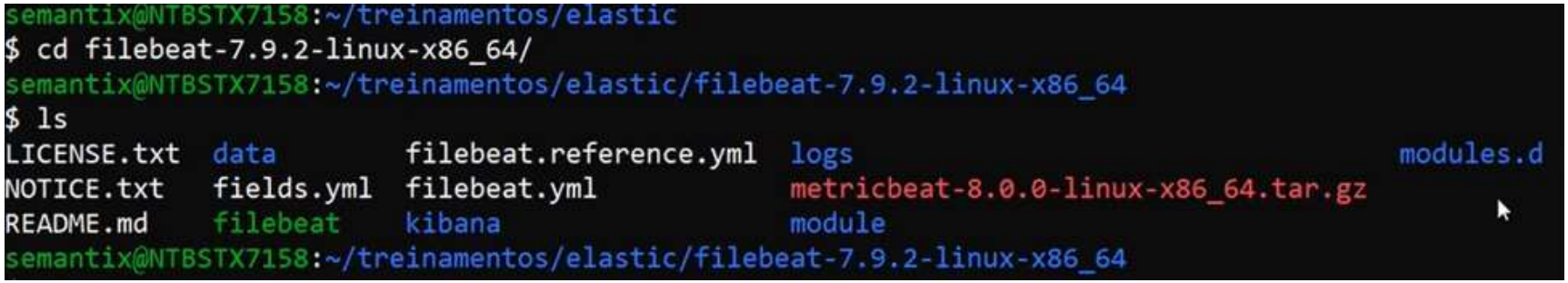
Vai gravar os arquivos no elasticsearch sequencialmente com nome e ano

Recriando os serviços do elasticsearch após as alterações

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ docker-compose up -d
Creating network "elastic_elastic" with driver "bridge"
Creating elastic_elasticsearch_1 ... done
Creating elastic_kibana_1        ... done
Creating elastic_logstash_1      ... done
```

3. Verificar a quantidade de documentos do índice criado pelo Logstash e visualizar seus 10 primeiros documentos

Inicializando o filebeat



Testando a configuração e a saída

Apontando a saída para o logstash porta 5044.

http://localhost:9600

o status deve estar green


```
{"host":"554f7f4e3311","version":"7.9.2","http_address":"0.0.0.0:9600","id":"80ef0758-2c3d-4bfe-8dd7-
9002fcc3ec8b","name":"554f7f4e3311","ephemeral_id":"a7e1f175-5eec-41e1-aefd-
0e6c4d2ea6bf","status":"green","snapshot":false,"pipeline":
{"workers":8,"batch_size":125,"batch_delay":50},"build_date":"2020-09-
23T03:12:32Z","build_sha":"0d3d0617adaa8c0c770469c9c32e18514b5d8f15","build_snapshot":false}
```


A pastas logs e data são úteis quando o serviço cai por algum motivo.

Tendo os dados nessas pastas o serviço saberá onde parou

Removendo as pastas por elas já continham os dados do arquivo paris-925.logs do exercício anterior.

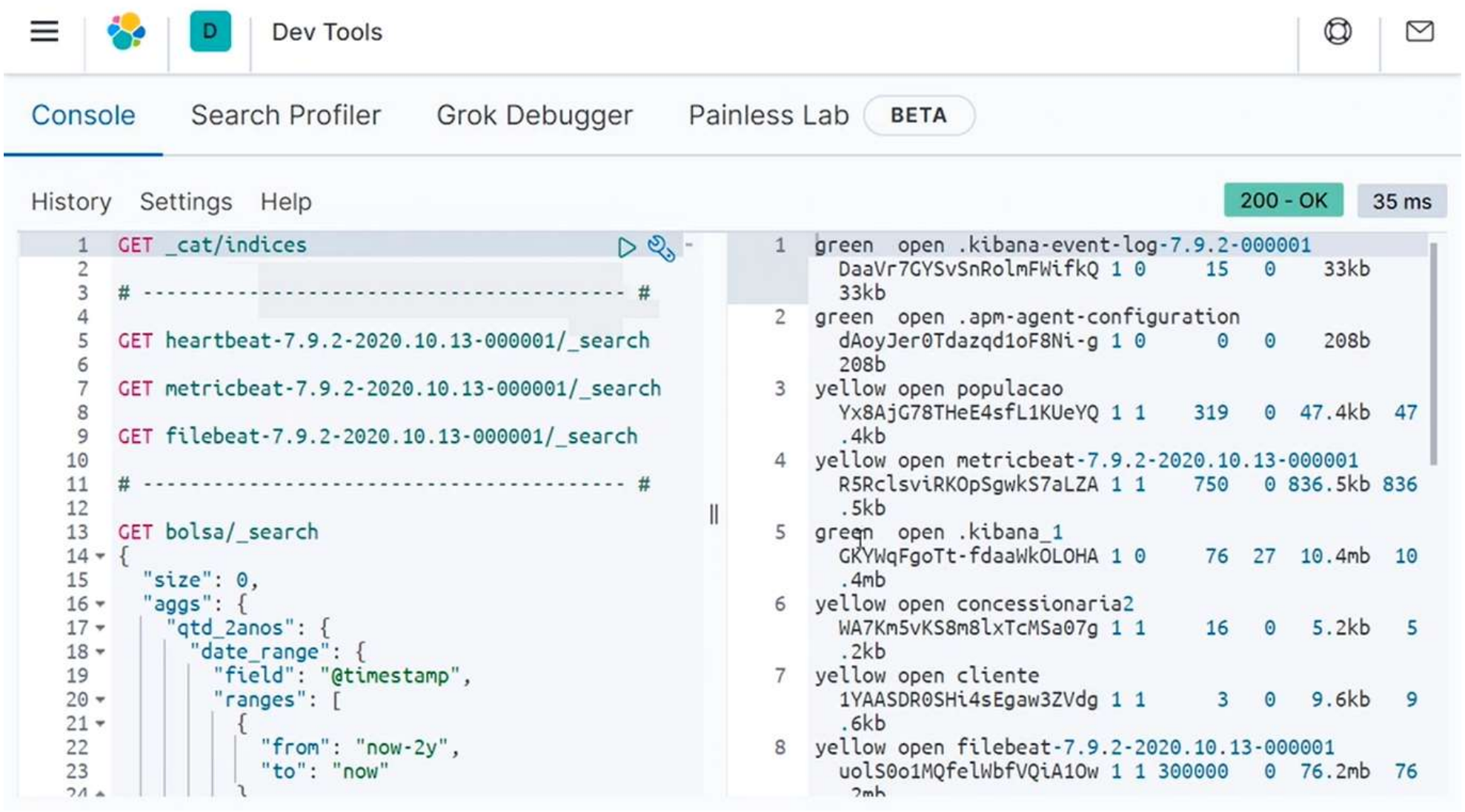
Iniciando o envio do arquivo paris-925.logs

```
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo ./filebeat -e
```

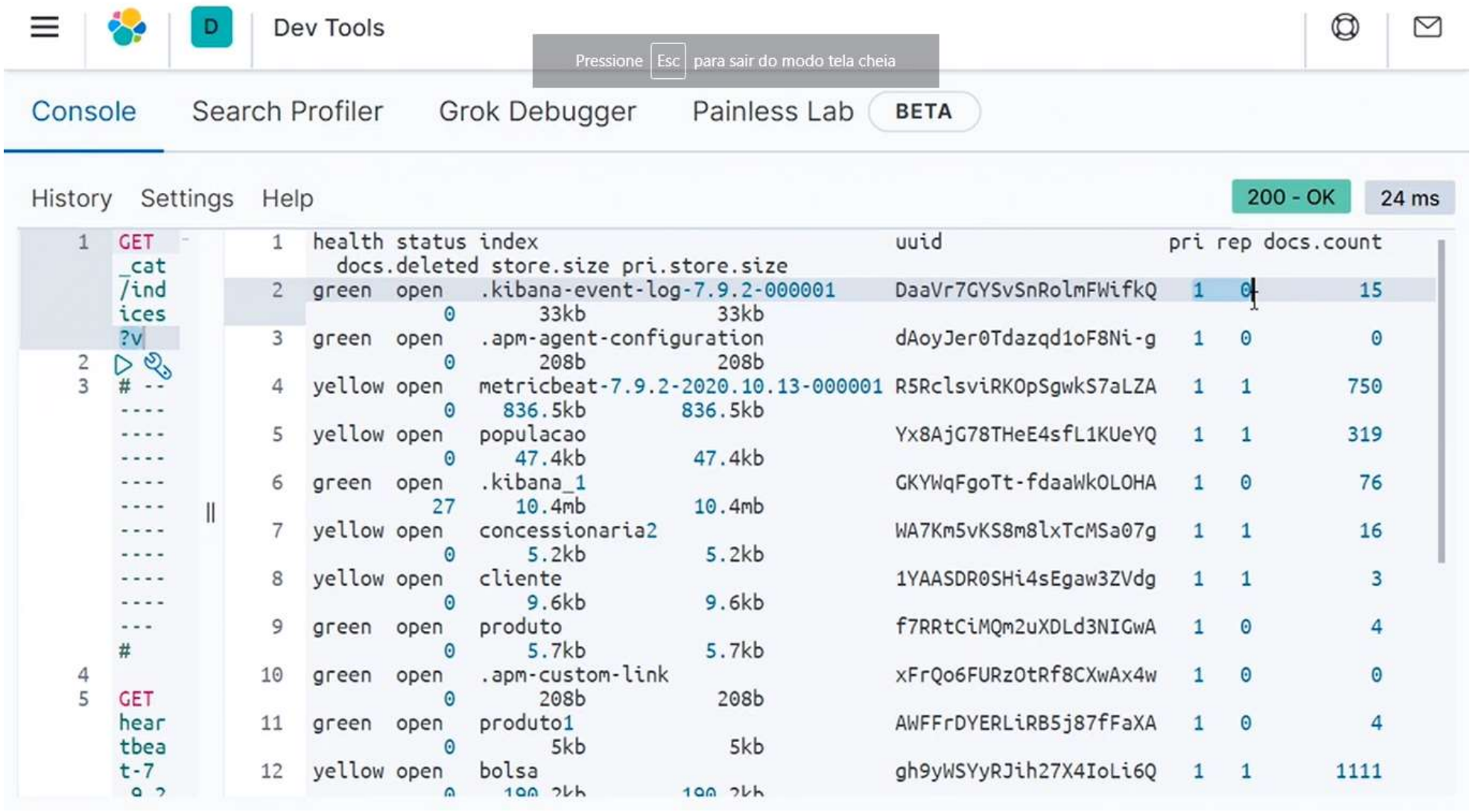
```
2020-10-15T17:40:13.031-0300    INFO    [registrar]     registrar/registrar.go:109      States Loaded from registrar: 0
2020-10-15T17:40:13.031-0300    INFO    [crawler]       beater/crawler.go:71    Loading Inputs: 1
2020-10-15T17:40:13.031-0300    INFO    log/input.go:157        Configured paths: [/home/semantix/treinamentos/elastic/dataset/paris-925.logs]
2020-10-15T17:40:13.031-0300    INFO    [crawler]       beater/crawler.go:141   Starting input (ID: 3976361801678345579)
2020-10-15T17:40:13.032-0300    INFO    [crawler]       beater/crawler.go:108   Loading and starting Inputs completed. Enabled inputs: 1
2020-10-15T17:40:13.032-0300    INFO    cfgfile/reload.go:164   Config reloader started
2020-10-15T17:40:13.032-0300    INFO    log/harvester.go:299    Harvester started for file: /home/semantix/treinamentos/elastic/dataset/paris-925.logs
2020-10-15T17:40:13.032-0300    INFO    cfgfile/reload.go:224   Loading of config files completed.
2020-10-15T17:40:16.009-0300    INFO    [add_cloud_metadata]    add_cloud_metadata/add_cloud_metadata.go:89      add_cloud_metadata: hosting provider type not detected.
2020-10-15T17:40:16.045-0300    INFO    [publisher_pipeline_output]     pipeline/output.go:143  Connecting to backoff(async(tcp://localhost:5044))
2020-10-15T17:40:16.045-0300    INFO    [publisher]     pipeline/retry.go:219   retryer: send unwait signal to consumer
2020-10-15T17:40:16.045-0300    INFO    [publisher]     pipeline/retry.go:223     done
2020-10-15T17:40:16.045-0300    INFO    [publisher_pipeline_output]     pipeline/output.go:151  Connection to backoff(async(tcp://localhost:5044)) established
```

Ficar atento se aparece “open_files”:1.

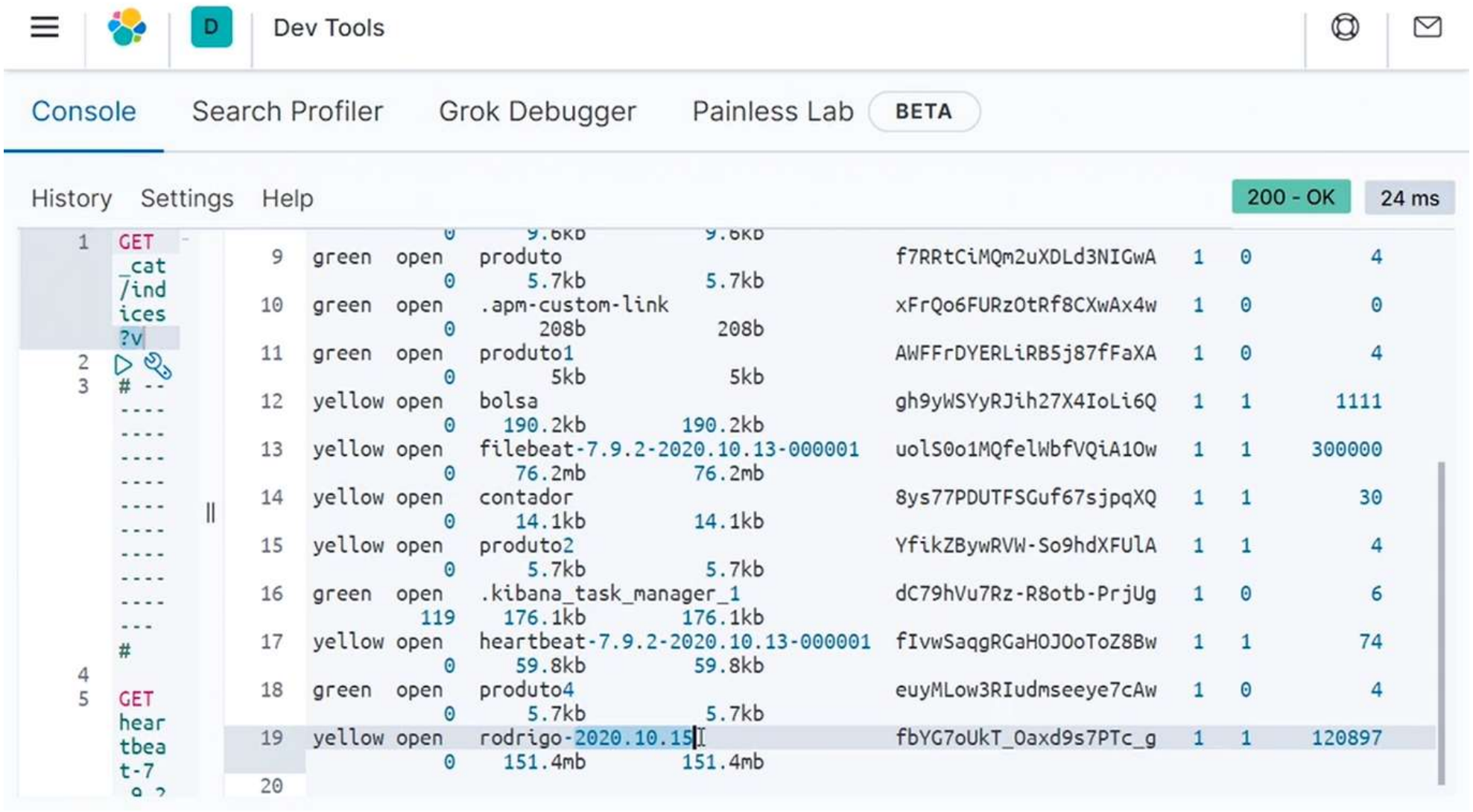
Vendo todos os índices



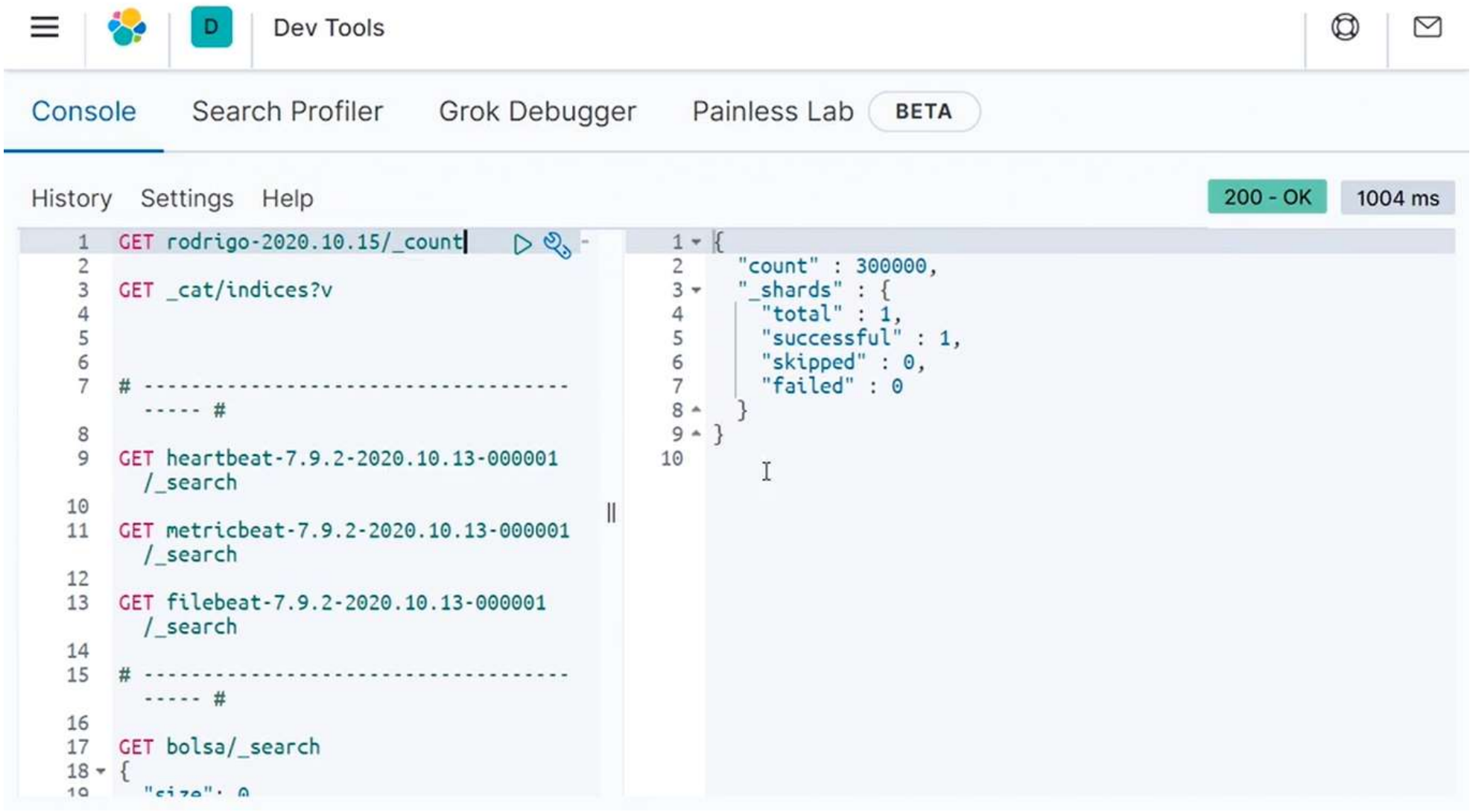
GET _cat/indices?v



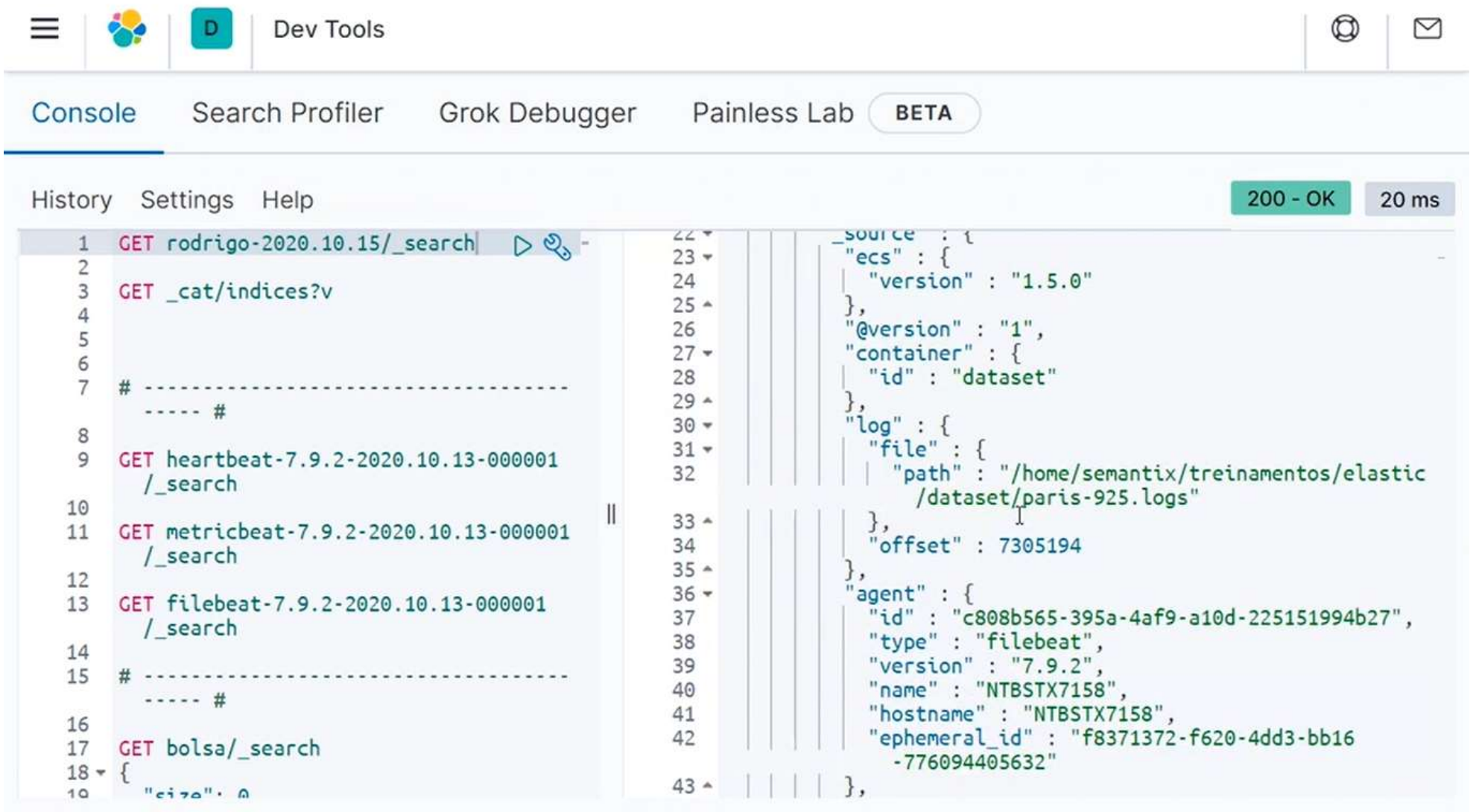
O indice rodrigo tem 120897 documentos

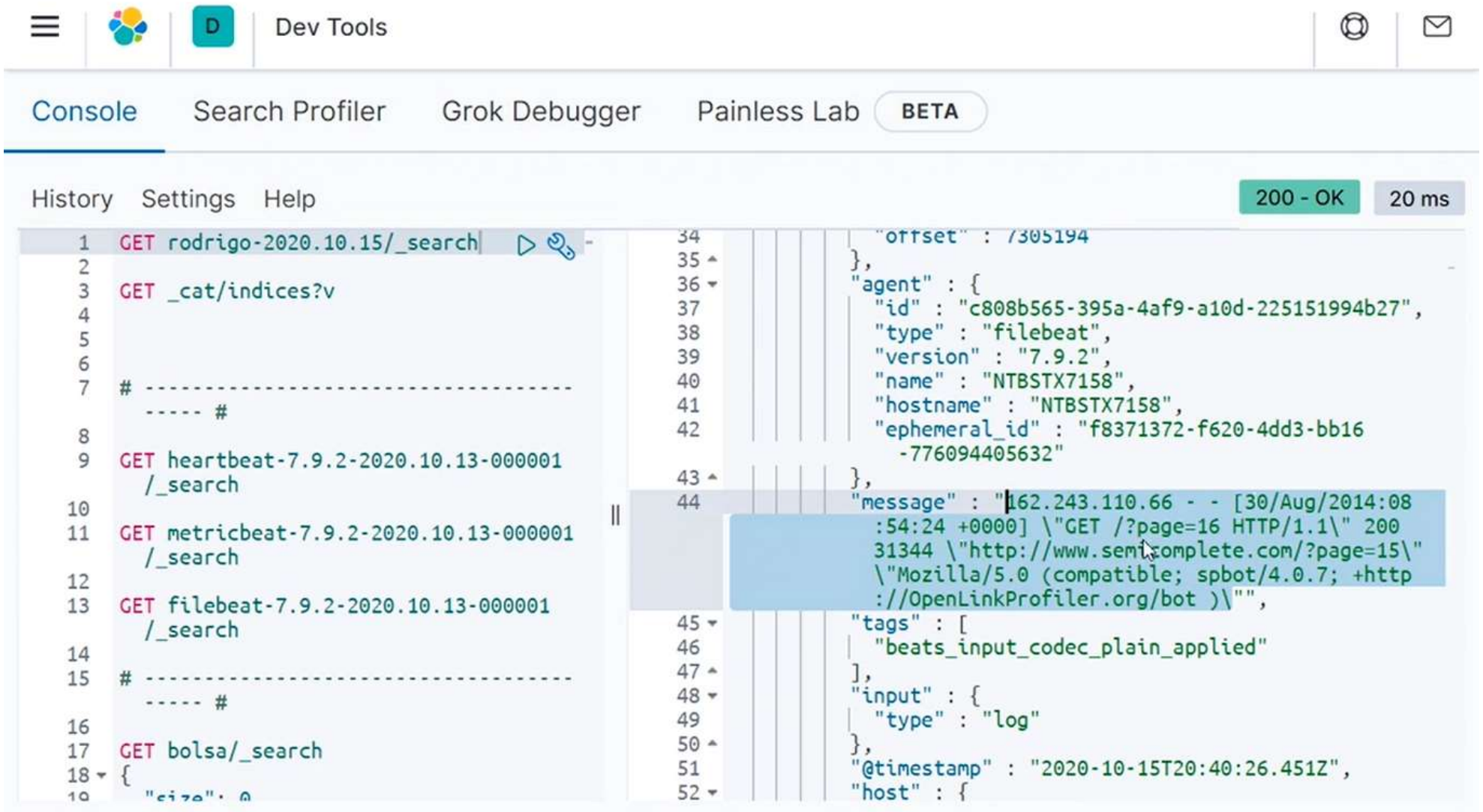


Total de documentos criados



Search mostra os 10 primeiros documentos




D
Dev Tools
Console
Search Profiler
Grok Debugger
Painless Lab
BETA
History
Settings
Help
200 - OK
20 ms
1 GET rodrigo-2020.10.15/_search
3 GET _cat/indices?v
7 # ----------
----- #
9 GET heartbeat-7.9.2-2020.10.13-000001
/_search
11 GET metricbeat-7.9.2-2020.10.13-000001
/_search
13 GET filebeat-7.9.2-2020.10.13-000001
/_search
15 # ----------
----- #
17 GET bolsa/_search
18 {
"size": 0
"offset" : 7305194
},
"agent" : {
"id" : "c808b565-395a-4af9-a10d-225151994b27",
"type" : "filebeat",
"version" : "7.9.2",
"name" : "NTBSTX7158",
"hostname" : "NTBSTX7158",
"ephemeral_id" : "f8371372-f620-4dd3-bb16
-776094405632"
},
"message" : "162.243.110.66 - - [30/Aug/2014:08
:54:24 +0000] \"GET /?page=16 HTTP/1.1\" 200
31344 \"http://www.semicomplete.com/?page=15\"
\"Mozilla/5.0 (compatible; spbot/4.0.7; +http
://OpenLinkProfiler.org/bot)\"",
"tags" : [
"beats_input_codec_plain_applied"
],
"input" : {
"type" : "log"
},
"@timestamp" : "2020-10-15T20:40:26.451Z",
"host" : {