

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

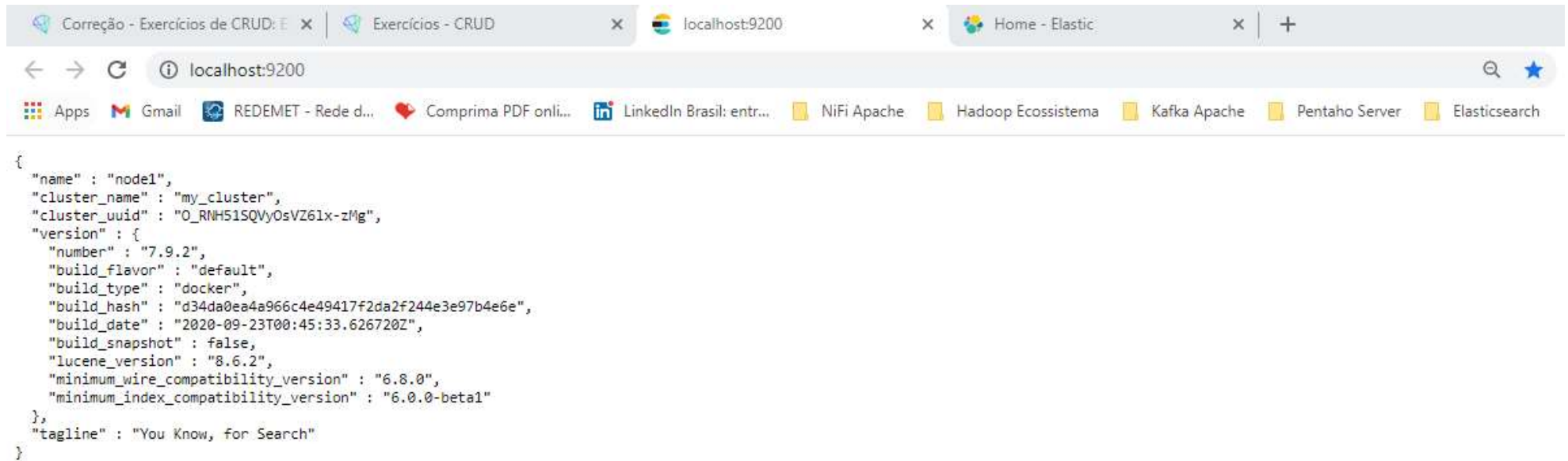
 elastic_elasticsearch_1
docker.elastic.co/elasticsearch/elasticsearch:7.9.2
RUNNING PORT: 9200

```
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>

The screenshot shows a web browser window with the Kibana interface. The browser's address bar displays `localhost:5601/app/home#`. The browser's tab bar shows several open tabs: "Correção - Exercícios de CRUD", "Exercícios - CRUD", "localhost:9200", and "Home - Elastic". The browser's bookmark bar contains links to "Apps", "Gmail", "REDEMET - Rede d...", "Comprima PDF onli...", "LinkedIn Brasil: entr...", "NiFi Apache", "Hadoop Ecosistema", "Kafka Apache", "Pentaho Server", and "Elasticsearch".

The Kibana interface features a left-hand navigation sidebar with the following sections:

- Home** (selected)
- Recently viewed**: No recently viewed items.
- Kibana**: Discover, Dashboard, Canvas, Maps, Machine Learning, Visualize.
- Enterprise Search**: App Search, Workplace Search.
- Observability**: Overview, Logs.

The main content area displays several key sections:

- Logs**: Ingest logs from popular data sources and easily visualize in preconfigured dashboards. Includes an "Add log data" button.
- Metrics**: Collect metrics from the operating system and services running on your servers. Includes an "Add metric data" button.
- Security**: SIEM + Endpoint Security. Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases. Includes an "Add events" button.
- Data Ingestion**: Three buttons for "Add sample data", "Upload data from log file" (Import a CSV, NDJSON, or log file), and "Use Elasticsearch data" (Connect to your Elasticsearch index).
- Explore Data**: Includes "App Search" (Leverage dashboards, analytics, and APIs for advanced application).
- Manage and Administer the Elastic Stack**: Includes "Console" (Skip cURL and use this JSON interface to work with your data directly) and "Rollups" (Summarize and store historical data in a smaller interval for future analysis).

Exercitando Consulta por Intervalo

Acessar o MENU -> Dev Tools

The screenshot shows the Elastic Home interface in a web browser. The browser tabs include 'Correção - Exercícios de Pesquisa', 'Exercícios - Pesquisa e Paginação', 'localhost:9200', and 'Home - Elastic'. The address bar shows 'localhost:5601/app/home#/'. The page features a sidebar menu with 'Home', 'Security', and 'Management' sections. The 'Dev Tools' link under 'Management' is highlighted. The main content area displays various widgets for Logs, Metrics, Security, and Data exploration.

Home

Recently viewed

No recently viewed items.

Security

Overview

Detections

Hosts

Network

Timelines

Cases

Administration

Management

Dev Tools

Ingest Ma Dev Tools

Stack Monitoring

Stack Management

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

Security

SIEM + Endpoint Security

Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases.

Add events

Add sample data

Set up a sample data source and a Kibana dashboard.

Upload data from log file

Import a CSV, NDJSON, or log file.

Use Elasticsearch data

Connect to your Elasticsearch index.

Explore Data

App Search

Leverage dashboards, analytics, and APIs for advanced application search made simple.

Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Rollups

Summarize and store historical data in a smaller index for future analysis.

1. Verificar se existe o índice populacao

The screenshot shows a web browser window with the address bar at `localhost:5601/app/dev_tools#/console`. The browser's tab bar includes several tabs, and the address bar has a search icon, a star, and a list of bookmarks. The DevTools console is open, displaying a list of requests. The first request is a `HEAD` request to `populacao`. The response is a `200 - OK` status with a response time of `325 ms`. A tooltip with the text "Click to send request" is visible over the first request. The console also shows a `GET` request to `produto/_search` with a complex query body. The query body is a JSON object with a `query` field containing a `match` object. The `match` object has a `descricao` field with a `query` of `"windows linux usb"`, an `operator` of `"or"`, and a `minimum_should_match` of `"50%"`. The console also shows a `GET` request to `produto/_search` with a similar query body, but with `minimum_should_match` set to `2`. The Windows taskbar is visible at the bottom of the screen, showing the Start button, search icon, and several application icons. The system tray shows the battery level at `100%` and the time as `14:23`.

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Dev Tools - Elastic x +

localhost:5601/app/dev_tools#/console

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Dev Tools

Console Search Profiler Grok Debugger Painless Lab BETA

History Settings Help

Click to send request

200 - OK 325 ms

```
1 HEAD populacao
2
3
4 #-----#
5
6
7 GET produto/_search
8 {
9   "query": {
10     "match": {
11       "descricao": {
12         "query": "windows linux usb",
13         "operator": "or",
14         "minimum_should_match": "50%"
15       }
16     }
17   }
18 }
19
20
21 GET produto/_search
22 {
23   "query": {
24     "match": {
25       "descricao": {
26         "query": "windows linux usb",
27         "operator": "or",
28         "minimum_should_match": 2
29       }
30     }
31   }
32 }
33
34 GET produto/_search
```

2. Executar as consultas no índice populacao

a) Mostrar os documentos com o atributo "Total Population" menor que 100

Está mostrando na ordem em que os documentos foram indexados

GET populacao/_search

```
{"query":{"range":{"Total Population":{"lt":100}}}}
```

The screenshot shows the Elastic Dev Tools interface in a web browser. The console displays a search query and its results.

Query:

```
1 GET populacao/_search
2 {
3   "query": {
4     "range": {
5       "Total Population": {
6         "lt": 100
7       }
8     }
9   }
10 }
```

Response:

```
1 {
2   "took": 213,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": {
12      "value": 9,
13      "relation": "eq"
14    },
15    "max_score": 1.0,
16    "hits": [
17      {
18        "_index": "populacao",
19        "_type": "_doc",
20        "_id": "Ie5k93kBC_QioruGMv4m",
21        "_score": 1.0,
22        "_source": {
23          "Total Population": 1,
24          "Total Households": 1,
25          "Total Females": 1,
26          "Zip Code": 91371,
27          "Median Age": 73.5,
28          "Total Males": 0,
29          "Average Household Size": 1.0
30        }
31      },
32      {
33        "_index": "populacao",
```

The console also shows other queries and responses, including a HEAD request and a search query for "produto/_search".

b) Mostrar os documentos com o atributo "Median Age" maior que 70

GET populacao/_search

```
{"query":{"range":{"Median Age":{"gt":70}}}}
```

The screenshot shows the Elastic Dev Tools console interface. The left pane displays the search query: `GET populacao/_search` with a range filter on "Median Age" greater than 70. The right pane shows the search results in JSON format. The first result is a document with a "Median Age" of 73.5. The second result is a document with a "Median Age" of 74.0. The console also shows the response status as 200 - OK and the execution time as 1833 ms.

```
1 GET populacao/_search
2 {
3   "query": {
4     "range": {
5       "Median Age": {
6         "gt": 70
7       }
8     }
9   }
10 }
11
12 GET populacao/_search
13 {
14   "query": {
15     "range": {
16       "Total Population": {
17         "lt": 100
18       }
19     }
20   }
21 }
22
23 HEAD populacao
24
25 -----
26
27 GET produto/_search
28 {
29   "query": {
30     "match": {
31       "descricao": {
32         "query": "produto 123456"
33       }
34     }
35   }
36 }
```

```
12   "value": 2,
13   "relation": "eq"
14 },
15   "max_score": 1.0,
16   "hits": [
17     {
18       "_index": "populacao",
19       "_type": "_doc",
20       "_id": "Ie5k93kBC_QioruGMv4m",
21       "_score": 1.0,
22       "_source": {
23         "Total Population": 1,
24         "Total Households": 1,
25         "Total Females": 1,
26         "Zip Code": 91371,
27         "Median Age": 73.5,
28         "Total Males": 0,
29         "Average Household Size": 1.0
30       }
31     },
32     {
33       "_index": "populacao",
34       "_type": "_doc",
35       "_id": "1e5k93kBC_QioruGMv4m",
36       "_score": 1.0,
37       "_source": {
38         "Total Population": 156,
39         "Total Households": 114,
40         "Total Females": 105,
41         "Zip Code": 91046,
42         "Median Age": 74.0,
43         "Total Males": 51,
44         "Average Household Size": 1.37
45       }
46     }
47   ]
48 }
```

200 - OK 1833 ms

100%

14:31

c) Mostrar os documentos 50 (Zip Code: 90056) à 60 (Zip Code: 90067) do índice de populacao

GET populacao/_search

```
{"query":{"range":{"Zip Code":{"gte":90056,"lte":90067}}}}
```

The screenshot shows the Elastic Dev Tools console interface. The left pane displays the search query: `GET populacao/_search` with a range query for Zip Code between 90056 and 90067. The right pane shows the search results, which are two documents. The first document has a Zip Code of 90056 and a score of 1.0. The second document has a Zip Code of 90057 and a score of 1.0. The console also shows a list of tabs at the top, including 'Correção - Exercícios de Consulta', 'Exercícios - Consultas por Intervalo', 'localhost:9200', and 'Dev Tools - Elastic'. The bottom status bar indicates 100% zoom and a time of 14:34.

```
1 GET populacao/_search
2 {
3   "query": {
4     "range": {
5       "Zip Code": {
6         "gte": 90056,
7         "lte": 90067
8       }
9     }
10  }
11 }
12
13 GET populacao/_search
14 {"query":{"range":{"Median Age":{"gt":70}}}}
15
16 GET populacao/_search
17 {
18   "query": {
19     "range": {
20       "Total Population": {
21         "lt": 100
22       }
23     }
24   }
25 }
26
27 HEAD populacao
28
29
30 #-----#
31
32
33 GET produto/_search
```

```
12   "value" : 11,
13   "relation" : "eq"
14 },
15   "max_score" : 1.0,
16   "hits" : [
17     {
18       "_index" : "populacao",
19       "_type" : "doc",
20       "_id" : "Ue5k93kBC_QioruGMv4m",
21       "_score" : 1.0,
22       "_source" : {
23         "Total Population" : 7827,
24         "Total Households" : 3371,
25         "Total Females" : 4391,
26         "Zip Code" : 90056,
27         "Median Age" : 48.4,
28         "Total Males" : 3436,
29         "Average Household Size" : 2.32
30       }
31     },
32     {
33       "_index" : "populacao",
34       "_type" : "doc",
35       "_id" : "Uu5k93kBC_QioruGMv4m",
36       "_score" : 1.0,
37       "_source" : {
38         "Total Population" : 44998,
39         "Total Households" : 15658,
40         "Total Females" : 20698,
41         "Zip Code" : 90057,
42         "Median Age" : 31.2,
43         "Total Males" : 24300,
44         "Average Household Size" : 2.81
45       }
46     }
47   ]
48 }
```

3. Importar através do Kibana o arquivo weekly_MSFT.csv (Guia Arquivos/dataset/weekly_MSFT.csv) com o índice bolsa

Upload data from log file

The screenshot shows the Elastic Home page in a web browser. The browser's address bar displays 'localhost:5601/app/home#/'. The page features a navigation bar at the top with a hamburger menu, the Elastic logo, and a 'Home' link. Below the navigation bar, the main content area is divided into two primary sections: 'Observability' and 'Security'. The 'Observability' section contains three sub-sections: 'APM' (Application Performance Monitoring), 'Logs', and 'Metrics'. Each sub-section has a brief description and an 'Add' button. The 'Logs' sub-section includes a description: 'Ingest logs from popular data sources and easily visualize in preconfigured dashboards.' and an 'Add log data' button. The 'Security' section contains a sub-section 'SIEM + Endpoint Security' with a description: 'Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases.' and an 'Add events' button. Below these sub-sections, there are three main options: 'Add sample data' (Load a data set and a Kibana dashboard), 'Upload data from log file' (Import a CSV, NDJSON, or log file), and 'Use Elasticsearch data' (Connect to your Elasticsearch index). The 'Visualize and Explore Data' section at the bottom left includes 'APM' and 'App Search' sub-sections. The 'Manage and Administer the Elastic Stack' section at the bottom right includes 'Console' and 'Rollups' sub-sections. The browser's taskbar at the bottom shows various application icons and the system clock indicating 14:38.

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Home - Elastic x

localhost:5601/app/home#/

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Home

Observability

APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
[Add APM](#)

Logs
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
[Add log data](#)

Metrics
Collect metrics from the operating system and services running on your servers.
[Add metric data](#)

Security

SIEM + Endpoint Security
Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases.
[Add events](#)

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

APM
Automatically collect in-depth performance metrics and errors from inside your applications.

App Search
Leverage dashboards, analytics, and APIs for advanced application search made simple.

Manage and Administer the Elastic Stack

Console
Skip cURL and use this JSON interface to work with your data directly.

Rollups
Summarize and store historical data in a smaller index for future analysis.

localhost:5601/app/ml#/filedatavisualizer

100% 14:38

Select or drag and drop a file

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Elastic x

localhost:5601/app/ml#/filedatavisualizer

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Machine Learning / Data Visualizer / File

Overview Anomaly Detection Data Frame Analytics **Data Visualizer** Settings

Visualize data from a log file EXPERIMENTAL


The File Data Visualizer helps you understand the fields and metrics in a log file. Upload your file, analyze its data, and then choose whether to import the data into an Elasticsearch index.


The File Data Visualizer supports these file formats:

- Delimited text files, such as CSV and TSV
- Newline-delimited JSON
- Log files with a common format for the timestamp

You can upload files up to 100 MB.

This feature is experimental. Got feedback? Please create an issue in [GitHub](#).





Select or drag and drop a file

Nenhum arquivo selecionado

100% 14:39

Selecionar o arquivo para importar

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Elastic

localhost:5601/app/ml#/filedatavisualizer

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Machine Learning / Data Visualizer / File

Overview Anomaly Detection

Abrir

< > ↑ □ << 05 - Elasticsearch Essential I > Dataset □ Pesquisar Dataset

Organizar Nova pasta

Nome	Data de modificação	Tipo	Tamanho
blogs.csv	07/06/2021 15:48	Arquivo de Valore...	5.200 KB
cars.bulk	07/06/2021 15:48	Arquivo BULK	1 KB
paris-925.logs	07/06/2021 15:49	Arquivo LOGS	66.059 KB
populacaoLA.csv	07/06/2021 15:48	Arquivo de Valore...	12 KB
weekly_MSFT.csv	07/06/2021 15:48	Arquivo de Valore...	59 KB

Nome: weekly_MSFT.csv Todos os arquivos (*.*)

Abrir Cancelar

Select or drag and drop a file

100% 14:40

Apresentação dos dados que serão importados

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Elastic x +

localhost:5601/app/ml#/filedatavisualizer

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Machine Learning / Data Visualizer / File

File contents

First 1,000 lines

```
5 2019-03-29,116.5600,118.7050,115.5215,117.9400,119632716
6 2019-03-22,116.1700,120.8200,116.0500,117.0500,160388610
7 2019-03-15,110.9900,117.2500,110.9800,115.9100,173532134
8 2019-03-08,113.0200,113.2500,108.8000,110.5100,111990712
9 2019-03-01,111.7600,113.2400,110.8800,112.5300,119359497
10 2019-02-22,107.7900,111.2000,106.2900,110.9700,96472580
11 2019-02-15,106.2000,108.3000,104.9650,108.2200,110757176
12 2019-02-08,102.8700,107.2700,102.7700,105.6700,130472196
13 2019-02-01,106.2600,106.4800,102.1700,102.7800,201611213
14 2019-01-25,106.7500,107.8800,104.8600,107.1700,112628578
15 2019-01-18,101.9000,107.9000,101.2600,107.7100,155699162
16 2019-01-11,101.6400,104.8800,100.9800,102.8000,157833149
17 2019-01-04,101.2900,102.5100,97.2000,101.9300,155142140
18 2018-12-28,97.6800,102.4100,93.9600,100.3900,183237806
```

Summary

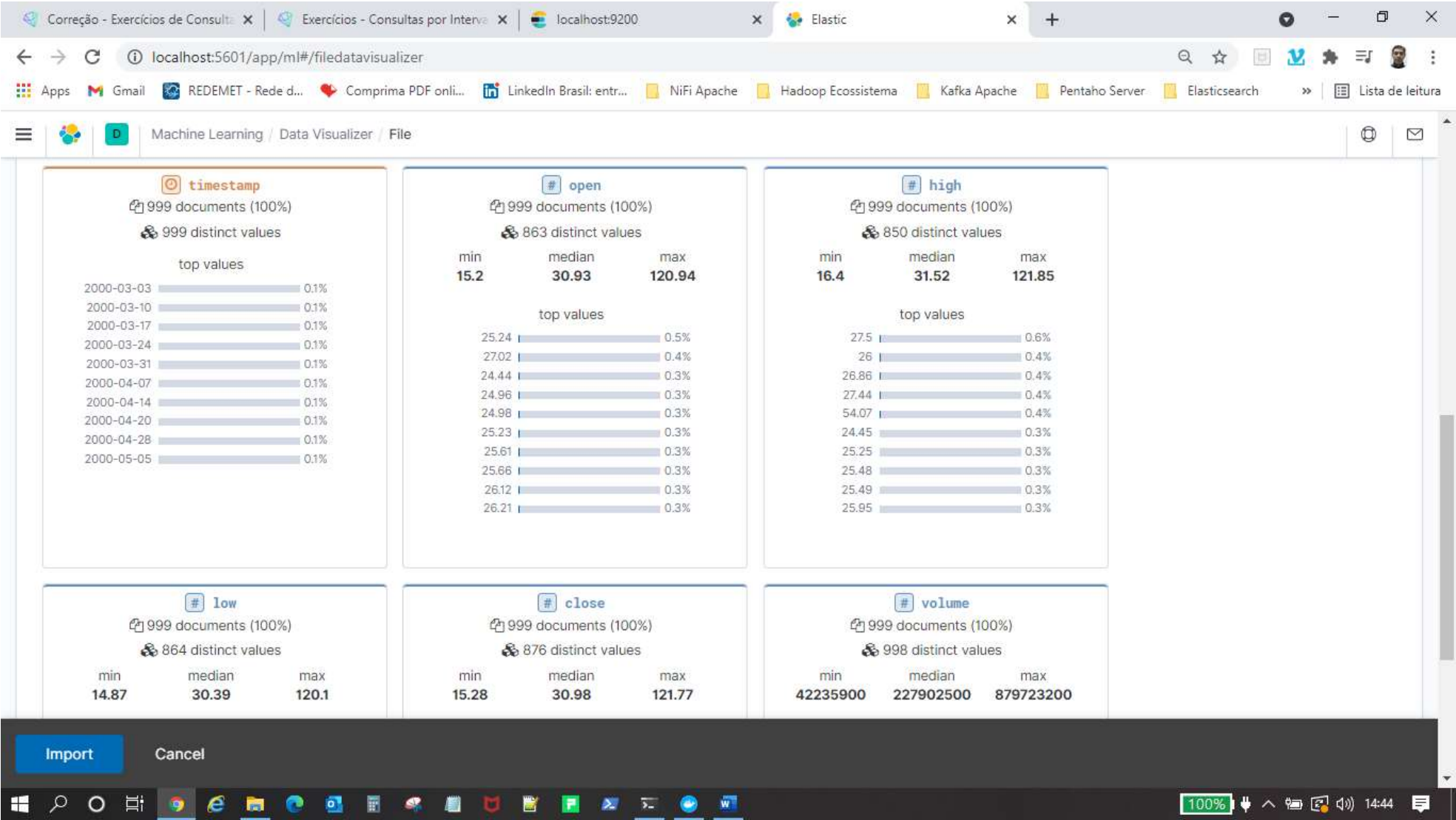
Number of lines analyzed	1000
Format	delimited
Delimiter	,
Has header row	true
Time field	timestamp
Time format	ISO8601

[Override settings](#) [Analysis explanation](#)

Import Cancel

100% 14:43

Algumas estatísticas antes de importar



Importar com o nome bolsa e deixando marcado o Create index pattern para fazer Dashboard no Kibana

Correção - Exercícios de Consulta x Exercícios - Consultas por Intervalo x localhost:9200 x Elastic x

localhost:5601/app/ml#/filedatavisualizer

Apps Gmail REDEMET - Rede d... Comprima PDF onli... LinkedIn Brasil: entr... NiFi Apache Hadoop Ecossistema Kafka Apache Pentaho Server Elasticsearch » Lista de leitura

Machine Learning / Data Visualizer / File

Overview Anomaly Detection Data Frame Analytics **Data Visualizer** Settings

weekly_MSFT.csv

Import data EXPERIMENTAL

Simple Advanced

Index name

bolsa

☒ Create index pattern

Import

Back Cancel

100% 14:47

Dados importados

Correção - Exercícios de Consulta

Exercícios - Consultas por Intervalo

localhost:9200

Elastic

localhost:5601/app/ml#/filedatavisualizer

AppsGmailREDEMET - Rede d...Comprima PDF onli...LinkedIn Brasil: entr...NiFi ApacheHadoop EcossistemaKafka ApachePentaho ServerElasticsearchLista de leitura

Machine Learning / Data Visualizer / File

Index name

bolsa

☒ Create index pattern

Reset

File processed

Index created

Ingest pipeline created

Data uploaded

Index pattern created

✓ Import complete

Index	bolsa
Index pattern	bolsa
Ingest pipeline	bolsa-pipeline
Documents ingested	1111

Back

Cancel

100%

14:49

MENU → Dev Tools

The screenshot shows a web browser window with multiple tabs. The active tab is 'localhost:5601/app/ml#/filedatavisualizer'. The browser's address bar shows the URL. Below the browser window, a sidebar menu is open, displaying the following sections:

- Home
- Recently viewed (No recently viewed items)
- Security
 - Overview
 - Detections
 - Hosts
 - Network
 - Timelines
 - Cases
 - Administration
- Management
 - Dev Tools (highlighted)
 - Ingest Dev Tools
 - Stack Monitoring

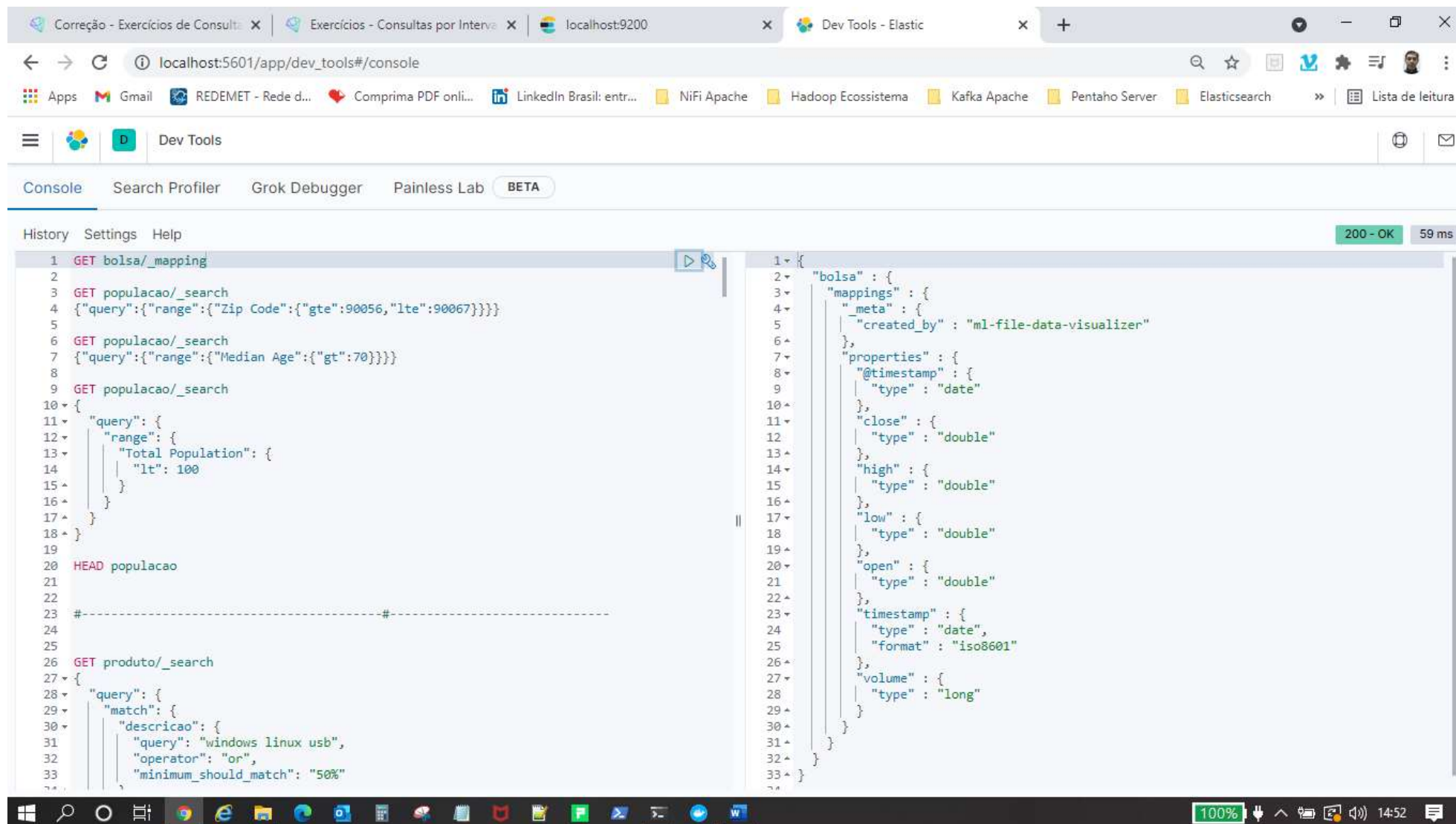
The main content area displays a horizontal pipeline with four steps, each marked with a blue checkmark:

- Index created
- Ingest pipeline created
- Data uploaded
- Index pattern created

At the bottom of the screen, a Windows taskbar is visible, showing the system tray with a 100% battery indicator and the time 14:49.

4. Executar as consultas no índice bolsa

Utilizar o mapping para conhecer os dados



The screenshot shows the Elastic Dev Tools console with the following content:

Console Search Profiler Grok Debugger Painless Lab BETA

History Settings Help

200 - OK 59 ms

```
1 GET bolsa/_mapping
2
3 GET populacao/_search
4 {"query":{"range":{"Zip Code":{"gte":90056,"lte":90067}}}}
5
6 GET populacao/_search
7 {"query":{"range":{"Median Age":{"gt":70}}}}
8
9 GET populacao/_search
10 {
11   "query": {
12     "range": {
13       "Total Population": {
14         "lt": 100
15       }
16     }
17   }
18 }
19
20 HEAD populacao
21
22 -----#
23
24
25 GET produto/_search
26 {
27   "query": {
28     "match": {
29       "descricao": {
30         "query": "windows linux usb",
31         "operator": "or",
32         "minimum_should_match": "50%"
33       }
34     }
35   }
36 }
```

```
1 {
2   "bolsa" : {
3     "mappings" : {
4       "_meta" : {
5         "created_by" : "ml-file-data-visualizer"
6       },
7       "properties" : {
8         "@timestamp" : {
9           "type" : "date"
10        },
11        "close" : {
12          "type" : "double"
13        },
14        "high" : {
15          "type" : "double"
16        },
17        "low" : {
18          "type" : "double"
19        },
20        "open" : {
21          "type" : "double"
22        },
23        "timestamp" : {
24          "type" : "date",
25          "format" : "iso8601"
26        },
27        "volume" : {
28          "type" : "long"
29        }
30      }
31    }
32  }
33 }
```

Windows taskbar at the bottom shows the time as 14:52 and 100% zoom.

O SEARCH mostra que tem 111 documentos

Correção - Exercícios de Consulta | Exercícios - Consultas por Intervalo | localhost:9200 | Dev Tools - Elastic

localhost:5601/app/dev_tools#/console

Apps | Gmail | REDEMET - Rede d... | Comprima PDF onli... | LinkedIn Brasil: entr... | NiFi Apache | Hadoop Ecossistema | Kafka Apache | Pentaho Server | Elasticsearch | Lista de leitura

Dev Tools

Console | Search Profiler | Grok Debugger | Painless Lab | BETA

History | Settings | Help

200 - OK 96 ms

```
1 GET bolsa/_search
2
3 GET bolsa/_mapping
4
5 GET populacao/_search
6 {"query":{"range":{"Zip Code":{"gte":90056,"lte":90067}}}}
7
8 GET populacao/_search
9 {"query":{"range":{"Median Age":{"gt":70}}}}
10
11 GET populacao/_search
12 {
13   "query": {
14     "range": {
15       "Total Population": {
16         "lt": 100
17       }
18     }
19   }
20 }
21
22 HEAD populacao
23
24 #-----#
25
26
27
28 GET produto/_search
29 {
30   "query": {
31     "match": {
32       "descricao": {
33         "query": "windows linux usb",
34         "type": "string"
35       }
36     }
37   }
38 }
```

```
1 {
2   "took" : 57,
3   "timed_out" : false,
4   "_shards" : {
5     "total" : 1,
6     "successful" : 1,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : {
12      "value" : 111,
13      "relation" : "eq"
14    },
15    "max_score" : 1.0,
16    "hits" : [
17      {
18        "_index" : "bolsa",
19        "_type" : "_doc",
20        "_id" : "EWElw_Hk8zUroh1c2ypUT",
21        "_score" : 1.0,
22        "_source" : {
23          "volume" : 48874731,
24          "high" : 121.85,
25          "@timestamp" : "2019-04-17T00:00:00.000-03:00",
26          "low" : 120.1,
27          "close" : 121.77,
28          "open" : 120.94,
29          "timestamp" : "2019-04-17"
30        }
31      },
32      {
33        "_index" : "bolsa",
34        "_type" : "_doc",
35        "_id" : "EWElw_Hk8zUroh1c2ypUT",
36        "_score" : 1.0,
37        "_source" : {
38          "volume" : 48874731,
39          "high" : 121.85,
40          "@timestamp" : "2019-04-17T00:00:00.000-03:00",
41          "low" : 120.1,
42          "close" : 121.77,
43          "open" : 120.94,
44          "timestamp" : "2019-04-17"
45        }
46      }
47    ]
48  }
49 }
```

100% 14:54

a) Visualizar os documentos do dia 2019-01-01 à 2019-03-01. (hits = 9)

GET bolsa/_search

```
{"query":{"range":{"timestamp":{"gte":"2019-01-01","lte":"2019-03-01","format":"yyyy-MM-dd"}}}}
```

The screenshot shows the Elastic Dev Tools console interface. The left pane displays the search query: `GET bolsa/_search` with a range query for the timestamp field from 2019-01-01 to 2019-03-01. The right pane shows the search results, which are two documents. The first document is for the date 2019-03-01 and the second is for 2019-02-22. The status bar at the bottom indicates 200 - OK and 1044 ms execution time.

```
1 GET bolsa/_search
2 {
3   "query": {
4     "range": {
5       "timestamp": {
6         "gte": "2019-01-01",
7         "lte": "2019-03-01",
8         "format": "yyyy-MM-dd"
9       }
10    }
11  }
12 }

13 GET bolsa/_search
14 GET bolsa/_mapping
15 GET populacao/_search
16 {"query":{"range":{"Zip Code":{"gte":90056,"lte":90067}}}}
17
18 GET populacao/_search
19 {"query":{"range":{"Median Age":{"gt":70}}}}
20
21 GET populacao/_search
22 {"query":{"range":{"Total Population":{"lt":100}}}}
23
24 GET populacao/_search
25 {
26   "query": {
27     "range": {
28       "Total Population": {
29         "lt": 100
30       }
31     }
32   }
33 }
```

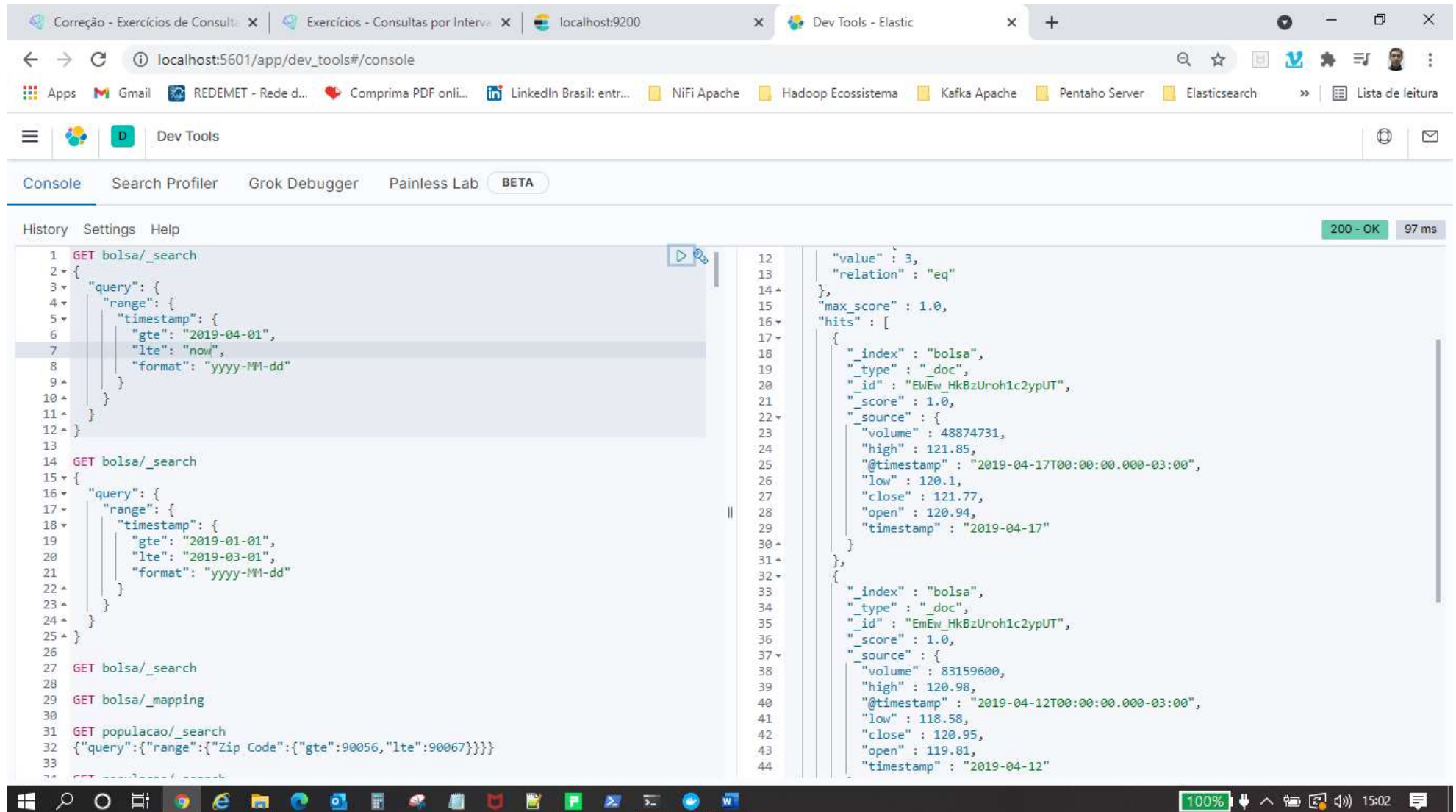
```
12   "value" : 9,
13   "relation" : "eq"
14 },
15   "max_score" : 1.0,
16   "hits" : [
17     {
18       "_index" : "bolsa",
19       "_type" : "doc",
20       "_id" : "GGEW_HkBzUroh1c2ypUT",
21       "_score" : 1.0,
22       "_source" : {
23         "volume" : 119359497,
24         "high" : 113.24,
25         "@timestamp" : "2019-03-01T00:00:00.000-03:00",
26         "low" : 110.88,
27         "close" : 112.53,
28         "open" : 111.76,
29         "timestamp" : "2019-03-01"
30       }
31     },
32     {
33       "_index" : "bolsa",
34       "_type" : "doc",
35       "_id" : "GWEW_HkBzUroh1c2ypUT",
36       "_score" : 1.0,
37       "_source" : {
38         "volume" : 96472580,
39         "high" : 111.2,
40         "@timestamp" : "2019-02-22T00:00:00.000-03:00",
41         "low" : 106.29,
42         "close" : 110.97,
43         "open" : 107.79,
44         "timestamp" : "2019-02-22"
45       }
46     }
47   ]
48 }
```

200 - OK 1044 ms

b) Visualizar os documentos do dia 2019-04-01 até agora. (hits = 3)

GET bolsa/_search

```
{"query":{"range":{"timestamp":{"gte":"2019-04-01","lte":"now","format":"yyyy-MM-dd"}}}}
```



The screenshot shows a web browser window with the Elastic Dev Tools console open. The console displays a GET request to the _search endpoint with a range query for the timestamp field, and the corresponding JSON response showing three hits.

Request:

```
1 GET bolsa/_search
2 {
3   "query": {
4     "range": {
5       "timestamp": {
6         "gte": "2019-04-01",
7         "lte": "now",
8         "format": "yyyy-MM-dd"
9       }
10    }
11  }
12 }
```

Response:

```
12 {
13   "value": 3,
14   "relation": "eq",
15   "max_score": 1.0,
16   "hits": [
17     {
18       "_index": "bolsa",
19       "_type": "doc",
20       "_id": "EWew_HkBzUroh1c2ypUT",
21       "_score": 1.0,
22       "_source": {
23         "volume": 48874731,
24         "high": 121.85,
25         "@timestamp": "2019-04-17T00:00:00.000-03:00",
26         "low": 120.1,
27         "close": 121.77,
28         "open": 120.94,
29         "timestamp": "2019-04-17"
30       }
31     },
32     {
33       "_index": "bolsa",
34       "_type": "doc",
35       "_id": "EmEw_HkBzUroh1c2ypUT",
36       "_score": 1.0,
37       "_source": {
38         "volume": 83159600,
39         "high": 120.98,
40         "@timestamp": "2019-04-12T00:00:00.000-03:00",
41         "low": 118.58,
42         "close": 120.95,
43         "open": 119.81,
44         "timestamp": "2019-04-12"
45       }
46     }
47   ]
48 }
```