

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
d3d012693acc	docker.elastic.co/logstash/logstash:7.9.2	NAMES			
:::5044->5044/tcp,		"/usr/local/bin/dock...	17 hours ago	Up 33 minutes	0.0.0.0:5044->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


 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

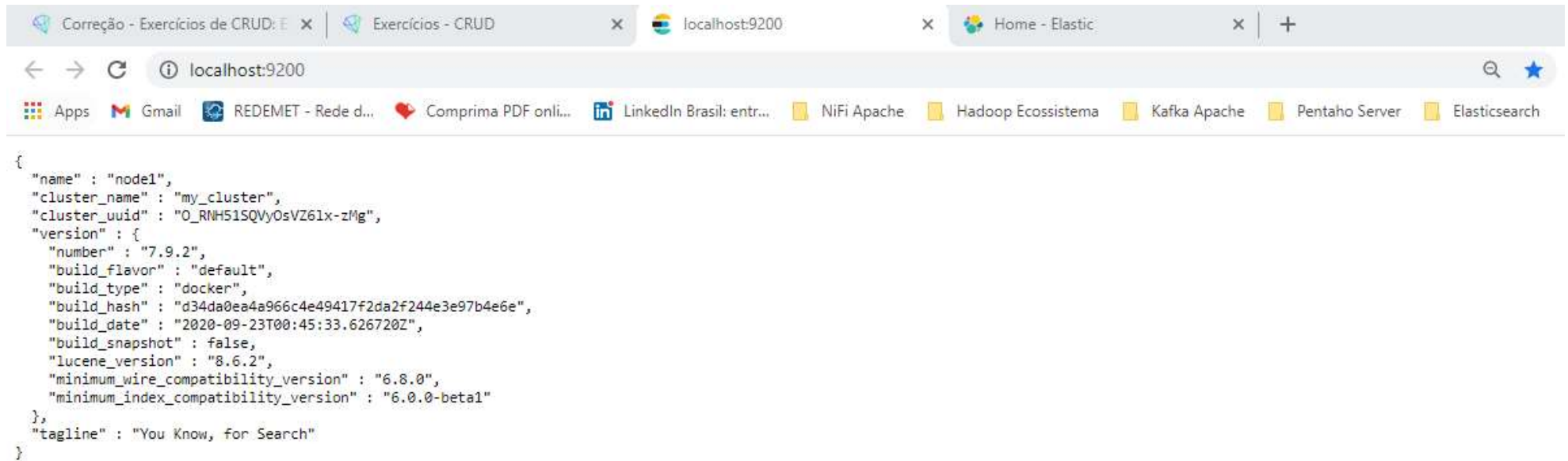
 **elastic_elasticsearch_1**
docker.elastic.co/elasticsearch/elasticsearch:7.9.2
RUNNING PORT: 9200

```
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 includes several 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 menu with the following sections: 'Home' (with a home icon), 'Recently viewed' (showing 'No recently viewed items'), 'Kibana' (with a dropdown arrow), 'Enterprise Search' (with a dropdown arrow), and 'Observability' (with a dropdown arrow). The 'Kibana' section includes links to 'Discover', 'Dashboard', 'Canvas', 'Maps', 'Machine Learning', and 'Visualize'. The 'Enterprise Search' section includes links to 'App Search' and 'Workplace Search'. The 'Observability' section includes links to 'Overview' and 'Logs'. The main content area of the Kibana home page is divided into several sections. The top section is titled 'Security' and includes a sub-section 'SIEM + Endpoint Security' with the description 'Protect hosts, analyze security information and events, hunt threats, automate detections, and create cases.' Below this, there are three buttons: 'Add log data', 'Add metric data', and 'Add events'. The middle section is titled 'Explore Data' and includes a sub-section 'App Search' with the description 'Leverage dashboards, analytics, and APIs for advanced application'. Below this, there are three buttons: 'Add sample data', 'Upload data from log file', and 'Use Elasticsearch data'. The bottom section is titled 'Manage and Administer the Elastic Stack' and includes a sub-section 'Console' with the description 'Skip cURL and use this JSON interface to work with your data directly.' Below this, there are three buttons: 'Add sample data', 'Upload data from log file', and 'Use Elasticsearch data'.

Correção - Exercícios de CRUD: E x | Exercícios - CRUD 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 Ecosistema Kafka Apache Pentaho Server Elasticsearch

Home

Home

Recently viewed

No recently viewed items

Kibana

Discover

Dashboard

Canvas

Maps

Machine Learning

Visualize

Enterprise Search

App Search

Workplace Search

Observability

Overview

Logs

Security

SIEM + Endpoint Security

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

Add log data

Add metric data

Add events

Add sample data

Upload data from log file

Use Elasticsearch data

Explore Data

Manage and Administer the Elastic Stack

App Search

Console

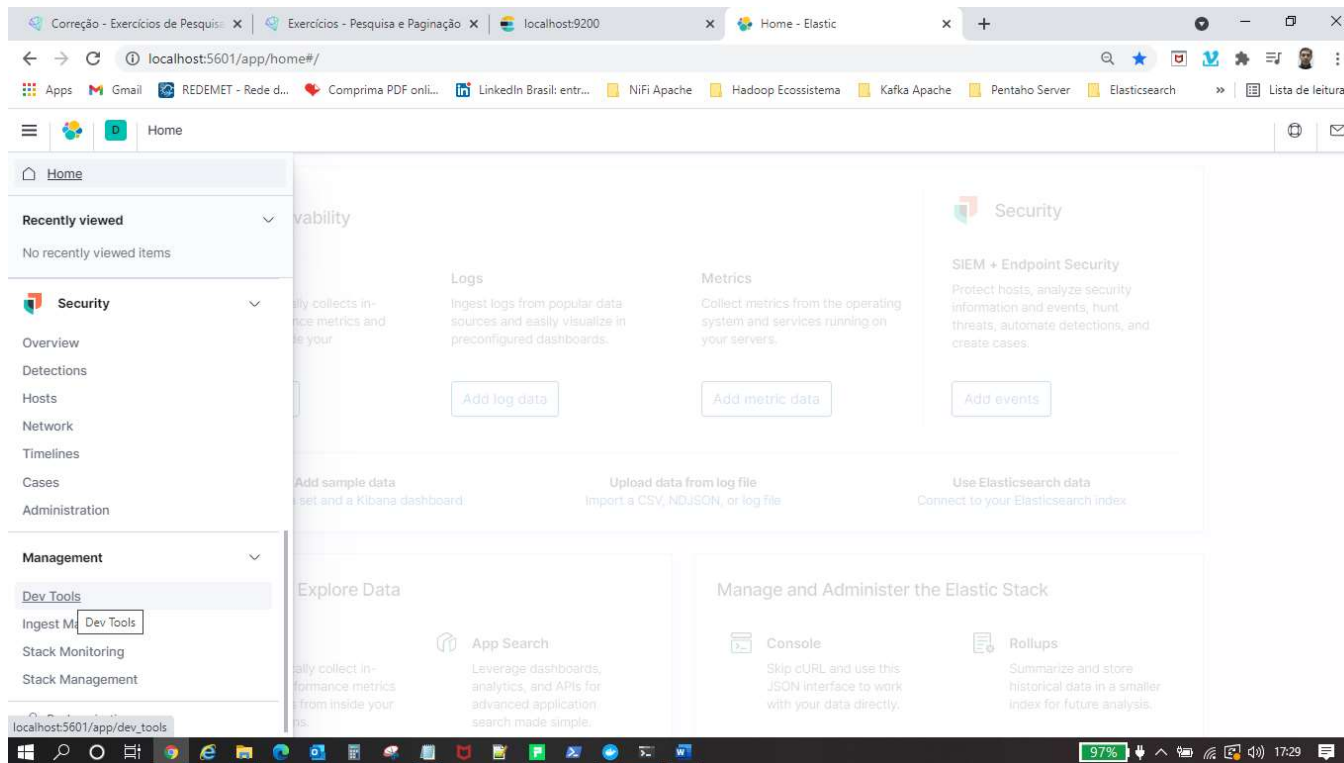
Rollups

Exercitando Pesquisa e Paginação

1. Pesquisar no índice produto os documentos com os seguintes atributos:

- a) Nome = mouse
- b) Quantidade = 30
- c) Descrição = USB
- d) Nome = hd e descrição = windows
- e) Nome = memória e descrição = DDR4

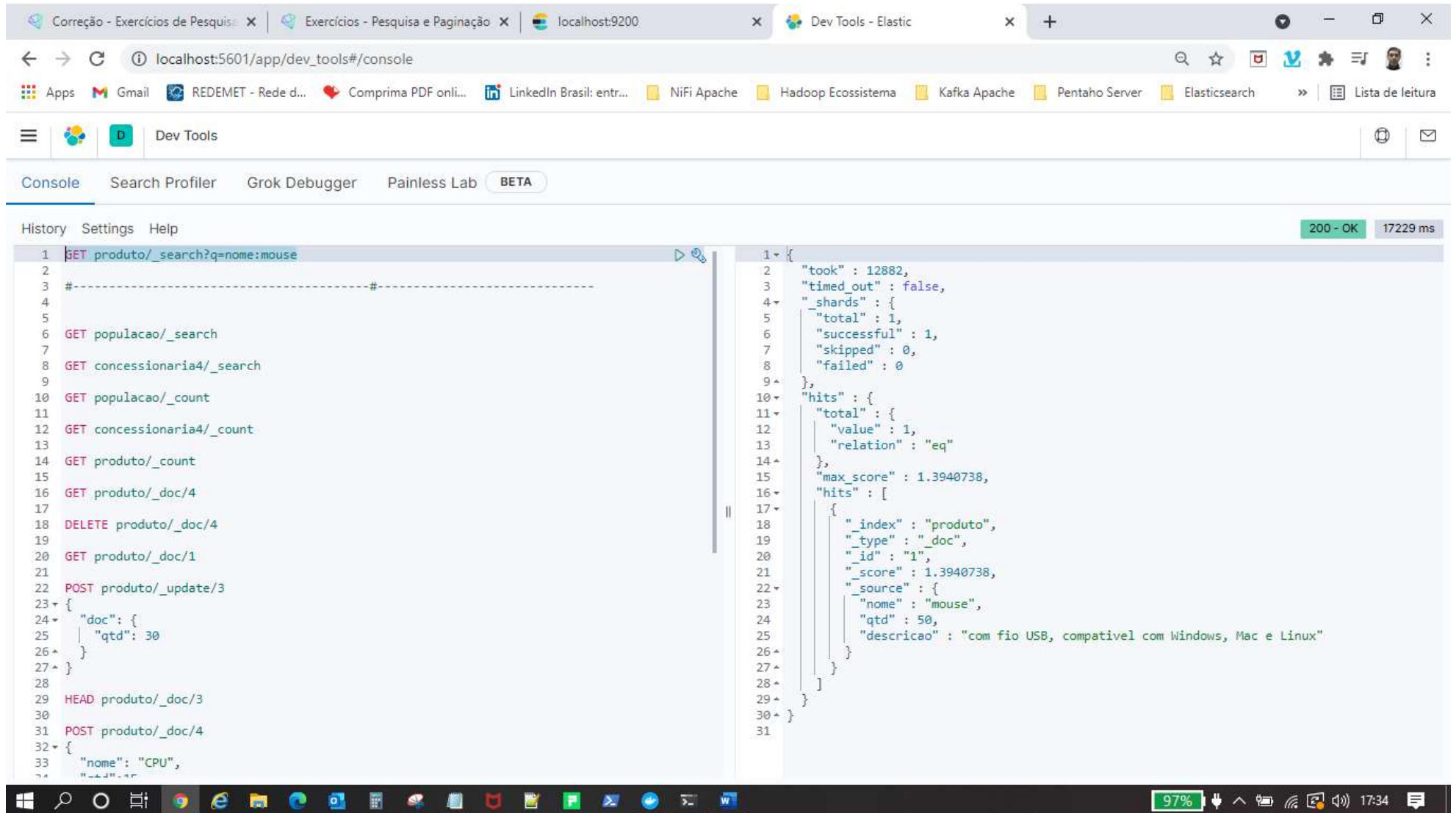
Acessar o MENU -> Dev Tools



a) Pesquisar Nome = mouse

GET produto/_search?q=nome:mouse

Encontrou 1 valor



b) Pesquisar Quantidade = 30

GET produto/_search?q=qtd:30

Encontrou 1 valor

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 DevTools interface is open. The 'Console' tab is active, displaying a REST client history on the left and a JSON response on the right.

REST Client History (Left Panel):

```
1 GET produto/_search?q=qtd:30
2
3 GET produto/_search?q=nome:mouse
4
5 #-----#
6
7 GET populacao/_search
8
9 GET concessionaria4/_search
10
11 GET populacao/_count
12
13 GET concessionaria4/_count
14
15 GET produto/_count
16
17 GET produto/_doc/4
18
19 DELETE produto/_doc/4
20
21 GET produto/_doc/1
22
23 POST produto/_update/3
24 {
25   "doc": {
26     "qtd": 30
27   }
28 }
29
30
31 HEAD produto/_doc/3
32
33 POST produto/_doc/4
```

JSON Response (Right Panel):

```
{
  "took": 226,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 1.0,
    "hits": [
      {
        "_index": "produto",
        "_type": "_doc",
        "_id": "3",
        "_score": 1.0,
        "_source": {
          "nome": "mem\u00f3ria ram",
          "qtd": 30,
          "descricao": "8GB, DDR4"
        }
      }
    ]
  }
}
```

The status bar at the bottom of the DevTools console shows `200 - OK` and `322 ms`. The Windows taskbar at the very bottom shows the system clock at 17:44 and a battery level of 97%.

c) Pesquisar Descrição = USB

GET produto/_search?q=descricao:usb

Encontrou 2 valores

The screenshot shows a web browser window with the address bar at `localhost:5601/app/dev_tools#/console`. The DevTools console is open, displaying a REST client interface. A request is being executed: `GET produto/_search?q=descricao:usb`. The response is a JSON object indicating a successful search with 2 hits.

Request:

```
1 GET produto/_search?q=descricao:usb
2
3 GET produto/_search?q=qtd:30
4
5 GET produto/_search?q=nome:mouse
6
7 #-----#
8
9
10 GET populacao/_search
11
12 GET concessionaria4/_search
13
14 GET populacao/_count
15
16 GET concessionaria4/_count
17
18 GET produto/_count
19
20 GET produto/_doc/4
21
22 DELETE produto/_doc/4
23
24 GET produto/_doc/1
25
26 POST produto/_update/3
27 {
28   "doc": {
29     "qtd": 30
30   }
31 }
32
33 HEAD produto/_doc/3
```

Response:

```
1 {
2   "took" : 58,
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" : 2,
13      "relation" : "eq"
14    },
15    "max_score" : 0.5754429,
16    "hits" : [
17      {
18        "_index" : "produto",
19        "_type" : "_doc",
20        "_id" : "1",
21        "_score" : 0.5754429,
22        "_source" : {
23          "nome" : "mouse",
24          "qtd" : 50,
25          "descricao" : "com fio USB, compativel com Windows, Mac e Linux"
26        }
27      },
28      {
29        "_index" : "produto",
30        "_type" : "_doc",
31        "_id" : "2",
32        "_score" : 0.5169233,
33        "_source" : {
34          "nome" : "mouse",
35          "qtd" : 50,
36          "descricao" : "com fio USB, compativel com Windows, Mac e Linux"
37        }
38      }
39    ]
40  }
41 }
```

The console also shows a status bar at the bottom right indicating `200 - OK` and `81 ms`.

d) Pesquisar Nome = hd e descrição = windows

GET produto/_search?q=nome:hd&q=descricao:windows

Encontrou 2 valores

Correção - Exercícios de Pesquisa

Exercícios - Pesquisa e Paginação

localhost:9200

Dev Tools - Elastic

localhost:5601/app/dev_tools#/console

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

Dev Tools

ConsoleSearch ProfilerGrok DebuggerPainless LabBETA

HistorySettingsHelp

1 GET produto/_search?q=nome:hd&q=descricao:windows

2

3 GET produto/_search?q=descricao:usb

4

5 GET produto/_search?q=qtd:30

6

7 GET produto/_search?q=nome:mouse

8

9 #-----#

10

11

12 GET populacao/_search

13

14 GET concessionaria4/_search

15

16 GET populacao/_count

17

18 GET concessionaria4/_count

19

20 GET produto/_count

21

22 GET produto/_doc/4

23

24 DELETE produto/_doc/4

25

26 GET produto/_doc/1

27

28 POST produto/_update/3

29 {

30 "doc": {

31 "qtd": 30

32 }

33 }

1 {

2 "took" : 1,

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" : 2,

13 "relation" : "eq"

14 },

15 "max_score" : 0.92419624,

16 "hits" : [

17 {

18 "_index" : "produto",

19 "_type" : "_doc",

20 "_id" : "2",

21 "_score" : 0.92419624,

22 "_source" : {

23 "nome" : "hd",

24 "qtd" : 20,

25 "descricao" : "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8,

26 Windows 7"

27 }

28 },

29 {

30 "_index" : "produto",

31 "_type" : "_doc",

32 "_id" : "1",

33 "_score" : 0.5754429,

97%

17:50

e) Pesquisar Nome = memória e descrição = DDR4

GET produto/_search?q=nome:memória&q=descricao:DDR4

Encontrou 1 valor.

Se eu colocasse GB não encontraria nada, teria que ser 8GB.

The screenshot shows a web browser window with the DevTools console open. The console displays a history of REST client requests and the response for the first request.

History:

- 1 GET produto/_search?q=nome:memória&q=descricao:DDR4
- 2 GET produto/_search?q=nome:hd&q=descricao:windows
- 3 GET produto/_search?q=descricao:usb
- 4 GET produto/_search?q=qtd:30
- 5 GET produto/_search?q=nome:mouse
- 6 #-----#
- 7 GET populacao/_search
- 8 GET concessionaria4/_search
- 9 GET populacao/_count
- 10 GET concessionaria4/_count
- 11 GET produto/_count
- 12 GET produto/_doc/4
- 13 DELETE produto/_doc/4
- 14 GET produto/_doc/1
- 15 POST produto/_update/3
- 16 {
- 17 "doc": {
- 18 "qtd": 30
- 19 }
- 20 }

Response (200 - OK, 1163 ms):

```
{
  "took": 2,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.9530773,
    "hits": [
      {
        "_index": "produto",
        "_type": "_doc",
        "_id": "3",
        "_score": 0.9530773,
        "_source": {
          "nome": "memória ram",
          "qtd": 30,
          "descricao": "8GB, DDR4"
        }
      }
    ]
  }
}
```

2. Pesquisar todos os índices, limitando a pesquisa em 5 documentos em cada página e visualizar a 4 página (Documentos entre 16 á 20)

- Paginação

GET _all/_search?&size=5&from=15

The screenshot shows a web browser window with the URL `localhost:5601/app/dev_tools#/console`. The browser's address bar and tabs are visible at the top. Below the browser window, the Elastic Dev Tools console is open, displaying a REST client request and its response.

Request:

```
1 GET _all/_search?&size=5&from=15
2
3 GET produto/_search?q=nome:memória&q=descricao:DDR4
4
5 GET produto/_search?q=nome:hd&q=descricao:windows
6
7 GET produto/_search?q=descricao:usb
8
9 GET produto/_search?q=qtd:30
10
11 GET produto/_search?q=nome:mouse
12
13 #-----#
14
15
16 GET populacao/_search
17
18 GET concessionaria4/_search
19
20 GET populacao/_count
21
22 GET concessionaria4/_count
23
24 GET produto/_count
25
26 GET produto/_doc/4
27
28 DELETE produto/_doc/4
29
30 GET produto/_doc/1
31
32 POST produto/_update/3
33 {
34   "..."
35 }
```

Response:

```
1 {
2   "took" : 781,
3   "timed_out" : false,
4   "_shards" : {
5     "total" : 10,
6     "successful" : 10,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : {
12      "value" : 394,
13      "relation" : "eq"
14    },
15    "max_score" : 1.0,
16    "hits" : [
17      {
18        "_index" : ".kibana_1",
19        "_type" : "_doc",
20        "_id" : "ui-metric:console:GET_get",
21        "_score" : 1.0,
22        "_source" : {
23          "ui-metric" : {
24            "count" : 3
25          },
26          "type" : "ui-metric",
27          "updated_at" : "2021-06-10T17:53:13.836Z"
28        }
29      },
30      {
31        "_index" : ".kibana_1",
32        "_type" : "_doc",
33        "_id" : "ui-metric:console:HEAD_exists",
34        "..." : "..."
35      }
36    ]
37  }
38 }
```

The console shows a status bar at the top right indicating a `200 - OK` response with a duration of `814 ms`. A tooltip "Click to send request" is visible over the send button in the REST client interface.