

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

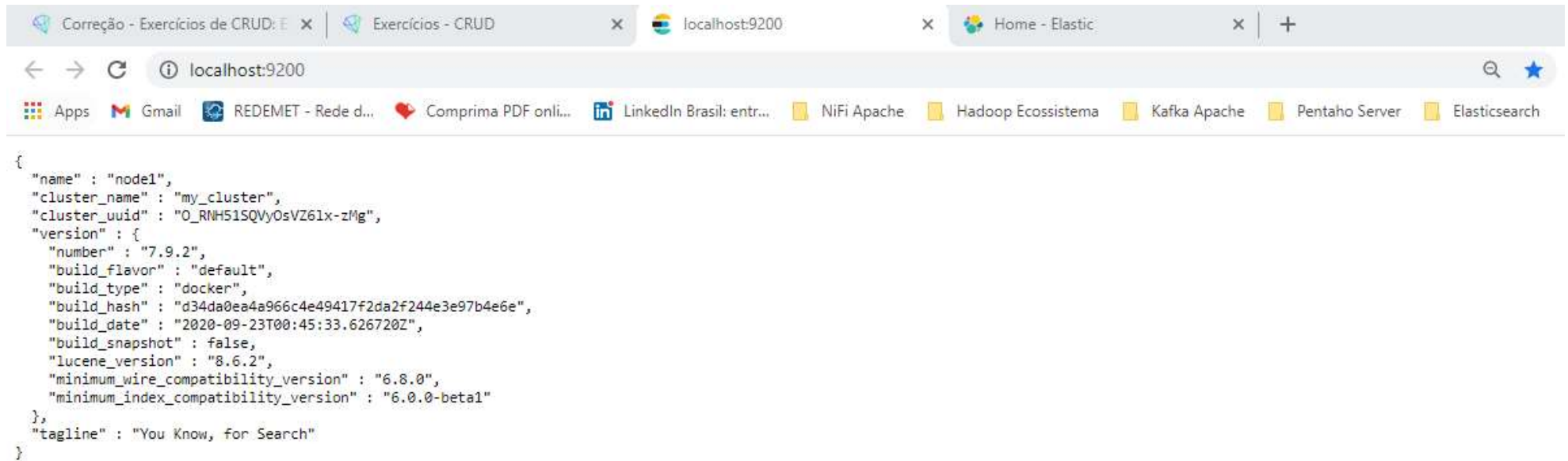
 elastic_elasticsearch_1
docker.elastic.co/elasticsearch/elasticsearch:7.9.2
RUNNING PORT: 9200

```
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 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 Ecosystema', 'Kafka Apache', 'Pentaho Server', and 'Elasticsearch'. The Kibana interface features a left-hand navigation menu with a 'Home' button at the top. Below it, the 'Recently viewed' section shows 'No recently viewed items'. The main menu categories are 'Kibana', 'Enterprise Search', and 'Observability'. The 'Kibana' category is expanded, showing sub-items: 'Discover', 'Dashboard', 'Canvas', 'Maps', 'Machine Learning', and 'Visualize'. The 'Enterprise Search' category shows 'App Search' and 'Workplace Search'. The 'Observability' category shows '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 contains three large buttons: 'Add sample data' (with the subtext 'Import a CSV, NDJSON, or log file'), 'Upload data from log file' (with the subtext 'Import a CSV, NDJSON, or log file'), and 'Use Elasticsearch data' (with the subtext 'Connect to your Elasticsearch index'). The bottom section is titled 'Explore Data' and 'Manage and Administer the Elastic Stack'. Under 'Explore Data', there is a sub-section 'App Search' with the description 'Leverage dashboards, analytics, and APIs for advanced application'. Under 'Manage and Administer the Elastic Stack', there are two sub-sections: 'Console' (with the description 'Skip cURL and use this JSON interface to work with your data directly') and 'Rollups' (with the description 'Summarize and store historical data in a smaller interval for future analysis').

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 Ecosystema 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

Import a CSV, NDJSON, or log file

Upload data from log file

Import a CSV, NDJSON, or log file

Use Elasticsearch data

Connect to your Elasticsearch index

Explore Data

Manage and Administer the Elastic Stack

App Search

Leverage dashboards, analytics, and APIs for advanced application

Console

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

Rollups

Summarize and store historical data in a smaller interval for future analysis

Exercitando Ordem de Busca de Documentos

Acessar o MENU -> Dev Tools

Correção - Exercícios de Pesquisa x Exercícios - Pesquisa e Paginação x localhost:9200 Home - Elastic x +

localhost:5601/app/home#/

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

Home

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

localhost:5601/app/dev_tools

Availability

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 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.

97%

17:29

Realizar todas as buscas a seguir no índice produto

Verificando se existe o INDEX produto

The screenshot shows a web browser window with the address bar at `localhost:5601/app/dev_tools#/console`. The browser tabs include "Correção - Exercícios Ordem de...", "Exercícios - Ordem de Busca", "localhost:9200", and "Dev Tools - Elastic". The browser's bookmark bar shows various links like "Apps", "Gmail", "REDEMET - Rede d...", "Comprima PDF onli...", "LinkedIn Brasil: entr...", "NiFi Apache", "Hadoop Ecossistema", "Kafka Apache", "Pentaho Server", "Elasticsearch", and "Lista de leitura".

The DevTools console is open, showing the "Console" tab. A tooltip above the console says "Click to send request". The console history shows a request to `HEAD produto` which returned a `200 - OK` status in `122 ms`. Below this, a `GET produto/_search` request is shown with a complex JSON query body:

```
1 HEAD produto
2
3
4 #-----#
5
6
7 GET produto/_search
8 {
9   "query": {
10     "bool": {
11       "should": [
12         {
13           "match": {
14             "nome": "memória"
15           }
16         },
17         {
18           "match": {
19             "descricao": "usb"
20           }
21         }
22       ],
23       "must_not": [
24         {
25           "match": {
26             "descricao": "linux"
27           }
28         }
29       ]
30     }
31   }
32 }
33
```

The response for the `GET produto/_search` request is shown on the right side of the console, displaying `1 200 - OK`.

1. Buscar os documentos que contenham as palavras “Windows” e “Linux” no atributo descrição

GET produto/_search

```
{"query":{"match":{"descricao":{"query":"windows e linux","operator":"and"}}}}
```

The screenshot shows a web browser window with the DevTools console open. The console displays a REST client request and its response.

Request:

```
1 GET produto/_search
2 {
3   "query": {
4     "match": {
5       "descricao": {
6         "query": "windows e linux",
7         "operator": "and"
8       }
9     }
10  }
11 }
```

Response:

```
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" : 1,
13      "relation" : "eq"
14    },
15    "max_score" : 2.748536,
16    "hits" : [
17      {
18        "_index" : "produto",
19        "_type" : "_doc",
20        "_id" : "1",
21        "_score" : 2.748536,
22        "_source" : {
23          "nome" : "mouse",
24          "qtd" : 50,
25          "descricao" : "com fio USB, compatível com Windows, Mac e Linux"
26        }
27      }
28    ]
29  }
30 }
```

The response status is 200 - OK and the execution time is 2240 ms.

2. Buscar os documentos que contenham as palavras “Windows”, “Linux” ou “USB” no atributo descrição

GET produto/_search

```
{"query":{"match":{"descricao":"windows linux usb"}}
```

The screenshot shows the Elastic DevTools console interface. The left pane displays the REST client history with three requests. The first request is highlighted, showing a GET request to `produto/_search` with a match query for "windows linux usb". A tooltip "Click to send request" points to the send button. The right pane shows the JSON response, which indicates 3 hits. The first hit is for a document with id "1", named "mouse", with a quantity of 50 and a description "com fio USB, compativel com Windows, Mac e Linux". The second hit is for a document with id "2", named "hd", with a quantity of 20 and a description "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8, Windows 7". The status bar at the top right of the console shows "200 - OK" and "86 ms".

```
1 GET produto/_search
2 {
3   "query": {
4     "match": {
5       "descricao": "windows linux usb"
6     }
7   }
8 }
9
10 GET produto/_search
11 {
12   "query": {
13     "match": {
14       "descricao": {
15         "query": "windows e linux",
16         "operator": "and"
17       }
18     }
19   }
20 }
21
22 HEAD produto
23
24 #-----#
25
26
27
28 GET produto/_search
29 {
30   "query": {
31     "bool": {
32       "should": [
33         {
34           "match": {
35             "descricao": "windows linux usb"
36           }
37         }
38       ]
39     }
40   }
41 }
```

```
8   "failed": 0
9 },
10 "hits": {
11   "total": {
12     "value": 3,
13     "relation": "eq"
14   },
15   "max_score": 2.110161,
16   "hits": [
17     {
18       "_index": "produto",
19       "_type": "_doc",
20       "_id": "1",
21       "_score": 2.110161,
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": 1.455858,
33       "_source": {
34         "nome": "hd",
35         "qtd": 20,
36         "descricao": "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8, Windows 7"
37       }
38     },
39     {
40       "_index": "produto"
```


TAMBÉM PODERIA SER DESSA FORMA, UTILIZANDO O OPERADOR `or`

GET produto/_search

```
{"query":{"match":{"descricao":{"query":"windows linux usb","operator":"or"}}}}
```

Correção - Exercícios Ordem de Busca | Exercícios - Ordem de Busca | 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 Ecosistema | Kafka Apache | Pentaho Server | Elasticsearch | Lista de leitura

Dev Tools

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

History | Settings | Help

200 - OK 113 ms

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

```
15   "max_score" : 2.110161,
16   "hits" : [
17     {
18       "_index" : "produto",
19       "_type" : "_doc",
20       "_id" : "1",
21       "_score" : 2.110161,
22       "_source" : {
23         "nome" : "mouse",
24         "qtd" : 50,
25         "descricao" : "com fio USB, compatível com Windows, Mac e Linux"
26       }
27     },
28     {
29       "_index" : "produto",
30       "_type" : "_doc",
31       "_id" : "2",
32       "_score" : 1.455858,
33       "_source" : {
34         "nome" : "hd",
35         "qtd" : 20,
36         "descricao" : "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8, Windows 7"
37       }
38     },
39     {
40       "_index" : "produto",
41       "_type" : "_doc",
42       "_id" : "6",
43       "_score" : 0.801211,
44       "_source" : {
45         "nome" : "teclado",
46         "qtd" : 100,
47         "descricao" : "USB",

```

3. Buscar os documentos que contenham pelo menos 2 palavras da seguinte lista de palavras: “Windows”; “Linux” e “USB” no atributo descrição

GET produto/_search

```
{ "query": { "match": { "descricao": { "query": "windows linux usb", "operator": "or", "minimum_should_match": 2 } } } }
```

The screenshot shows a web browser window with the Elastic Dev Tools console open. The console displays a series of GET requests to the `produto/_search` endpoint. The first request is a match query for "windows linux usb" with an operator of "or" and a minimum_should_match of 2. The response shows 2 hits. The second request is a match query for "windows linux usb" with an operator of "or". The response shows 2 hits. The third request is a match query for "windows linux usb". The response shows 2 hits.

Console Output:

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

Response (Hit 1):

```
8   "failed" : 0
9 },
10 "hits" : {
11   "total" : {
12     "value" : 2,
13     "relation" : "eq"
14   },
15   "max_score" : 2.110161,
16   "hits" : [
17     {
18       "_index" : "produto",
19       "_type" : "_doc",
20       "_id" : "1",
21       "_score" : 2.110161,
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" : 1.455858,
33       "_source" : {
34         "nome" : "hd",
35         "qtd" : 20,
36         "descricao" : "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8, Windows 7"
37       }
38     }
39   ]
40 }
```

4. Buscar os documentos que contenham pelo menos 50 % da seguinte lista de palavras: “Windows”; “Linux” e “USB” no atributo descrição

GET produto/_search

```
{ "query": { "match": { "descricao": { "query": "windows linux usb", "operator": "or", "minimum_should_match": "50%" } } } }
```

The screenshot shows a web browser window with the Elastic Dev Tools console open. The console displays a search request and its response. The request is a GET request to the endpoint `produto/_search` with the following JSON body:

```
{ "query": { "match": { "descricao": { "query": "windows linux usb", "operator": "or", "minimum_should_match": "50%" } } } }
```

The response is a 200 OK status with a response time of 47 ms. The response body is a JSON object containing the following information:

```
{ "failed": 0, "hits": { "total": { "value": 3, "relation": "eq" }, "max_score": 2.110161, "hits": [ { "_index": "produto", "_type": "doc", "_id": "1", "_score": 2.110161, "_source": { "nome": "mouse", "qtd": 50, "descricao": "com fio USB, compativel com Windows, Mac e Linux" }, "_type": "doc", "_id": "2", "_score": 1.455858, "_source": { "nome": "hd", "qtd": 20, "descricao": "Interface USB 2.0, 500GB, Sistema: Windows 10, Windows 8, Windows 7" }, "_index": "produto" } ] } }
```