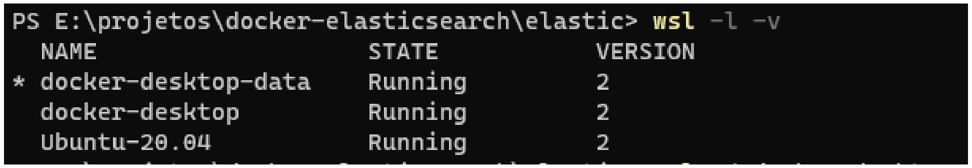
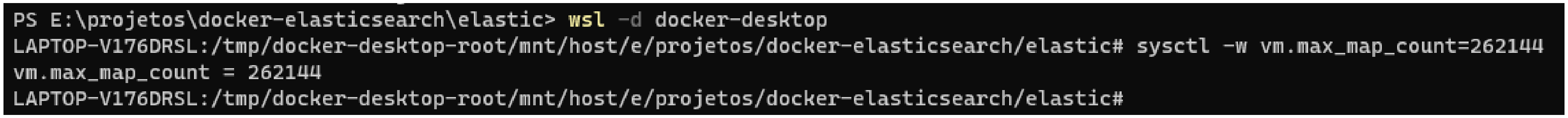
Iniciando o Elasticsearch em Docker

Docker Desktop Windows

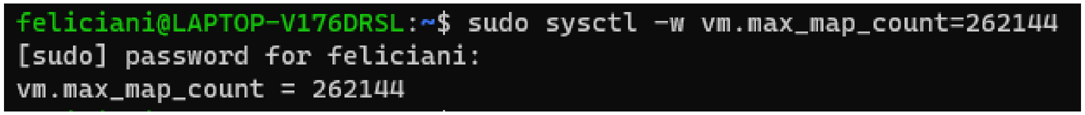


```
PS E:\projetos\docker-elasticsearch\elastic> wsl -l -v
  NAME                   STATE           VERSION
* docker-desktop-data    Running         2
  docker-desktop         Running         2
  Ubuntu-20.04           Running         2
```



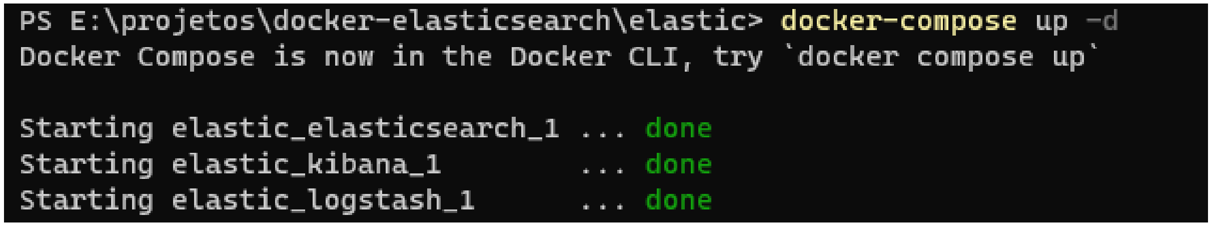
```
PS E:\projetos\docker-elasticsearch\elastic> wsl -d docker-desktop
LAPTOP-V176DRSL:/tmp/docker-desktop-root/mnt/host/e/projetos/docker-elasticsearch/elastic# sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
LAPTOP-V176DRSL:/tmp/docker-desktop-root/mnt/host/e/projetos/docker-elasticsearch/elastic#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

Docker Wsl2 Linux

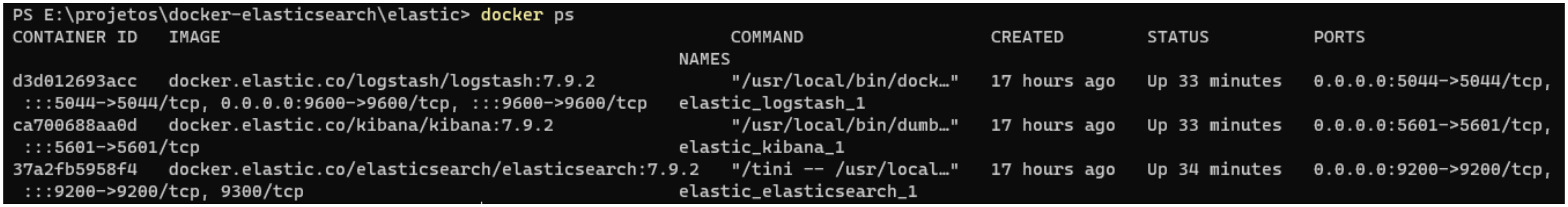


```
feliciani@LAPTOP-V176DRSL:~$ sudo sysctl -w vm.max_map_count=262144
[sudo] password for feliciani:
vm.max_map_count = 262144
```

Docker Desktop Windows

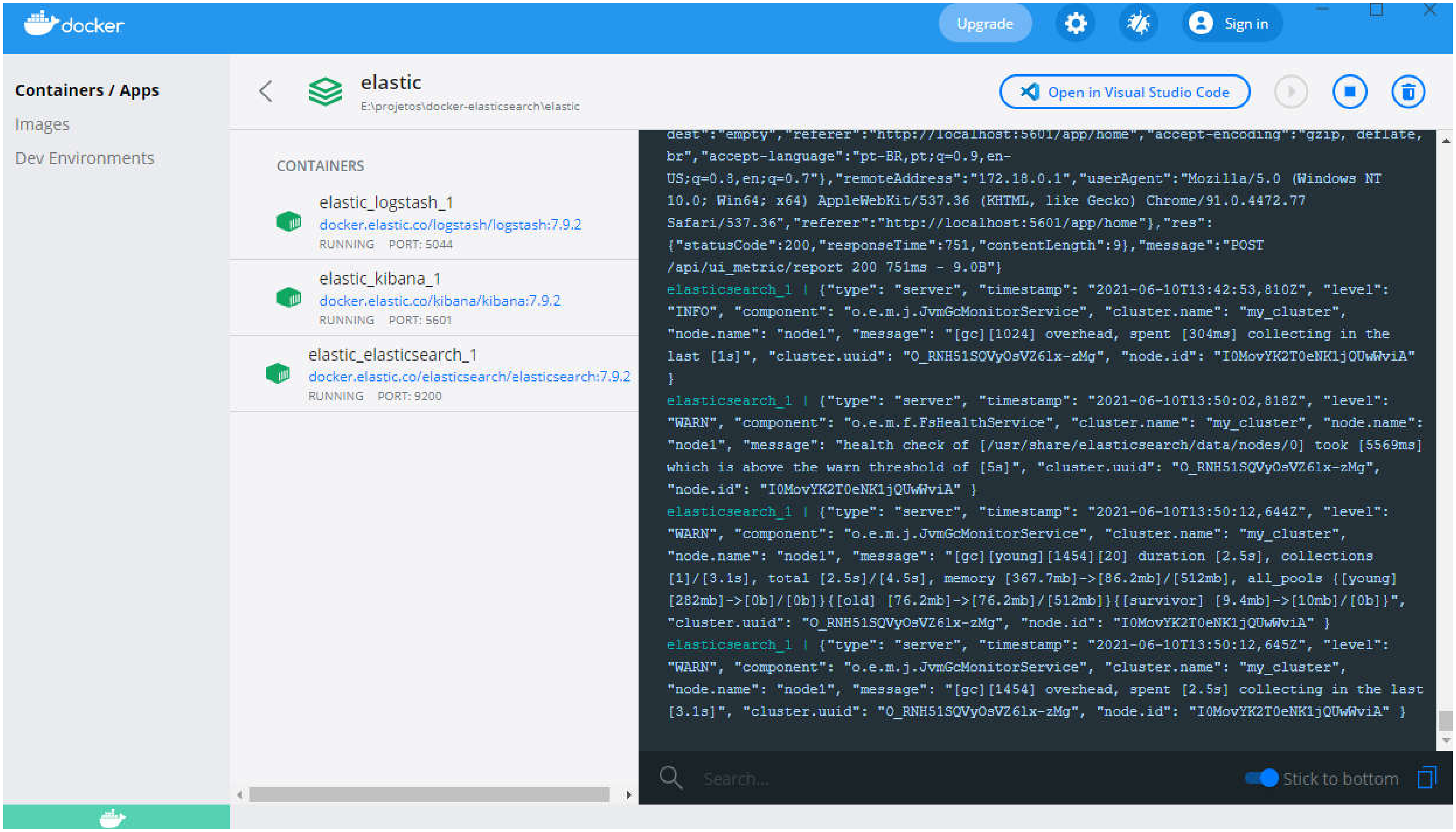


```
PS E:\projetos\docker-elasticsearch\elastic> docker-compose up -d
Docker Compose is now in the Docker CLI, try `docker compose up`

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



elastic
E:\projetos\docker-elasticsearch\elastic

CONTAINERS

elastic_logstash_1
docker.elastic.co/logstash/logstash:7.9.2
RUNNING PORT: 5044

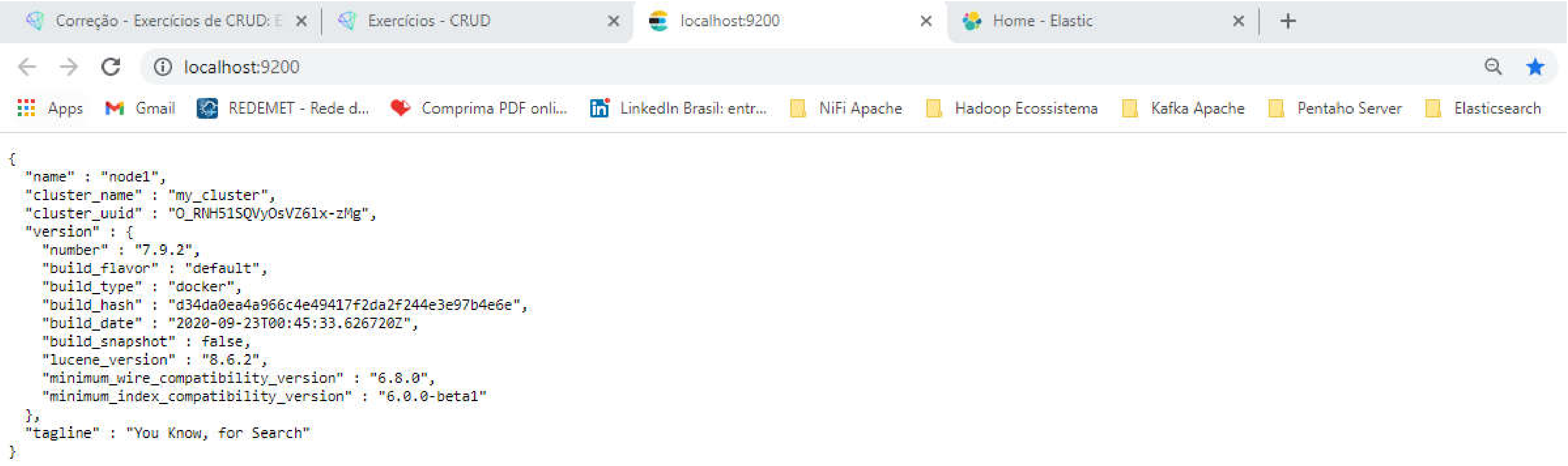
elastic_kibana_1
docker.elastic.co/kibana/kibana:7.9.2
RUNNING PORT: 5601

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_RNH51SQVyOsVZ61x-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_RNH51SQVyOsVZ61x-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_RNH51SQVyOsVZ61x-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_RNH51SQVyOsVZ61x-zMg", "node.id": "I0MovYK2T0eNK1jQUwWviA" }
```

Acessado o Elasticsearch

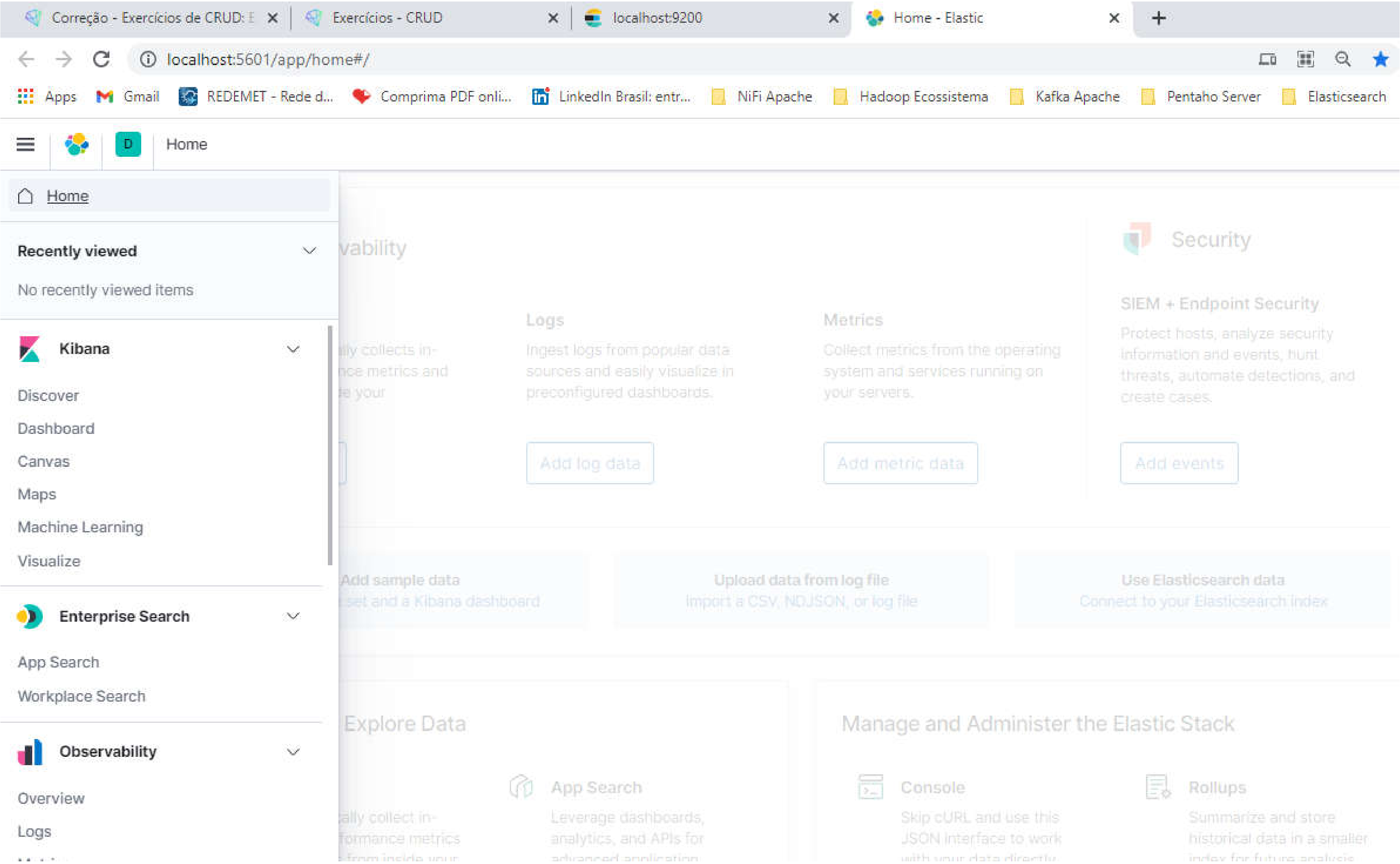
http://localhost:9200



```
{
  "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



Correção - Exercícios de CRUD: E ✕ | Exercícios - CRUD ✕ | localhost:9200 ✕ | Home - Elastic ✕ | +

localhost:5601/app/home#/

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

D Home

Home

Recently viewed

No recently viewed items

Kibana

- Discover
- Dashboard
- Canvas
- Maps
- Machine Learning
- Visualize

Enterprise Search

- App Search
- Workplace Search

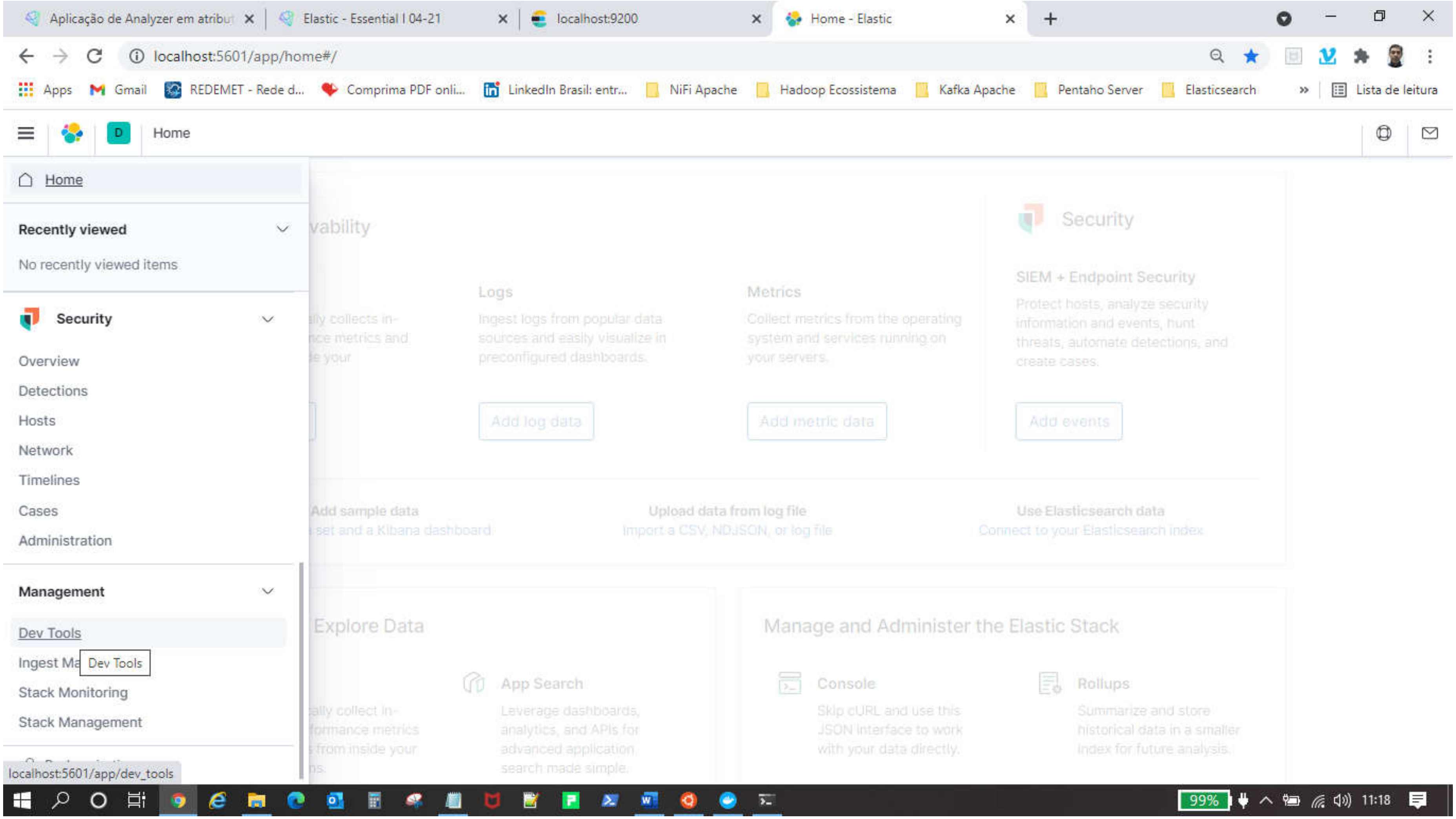
Observability

- Overview
- Logs

vability
ally collects in-
nce metrics and
e your
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 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
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

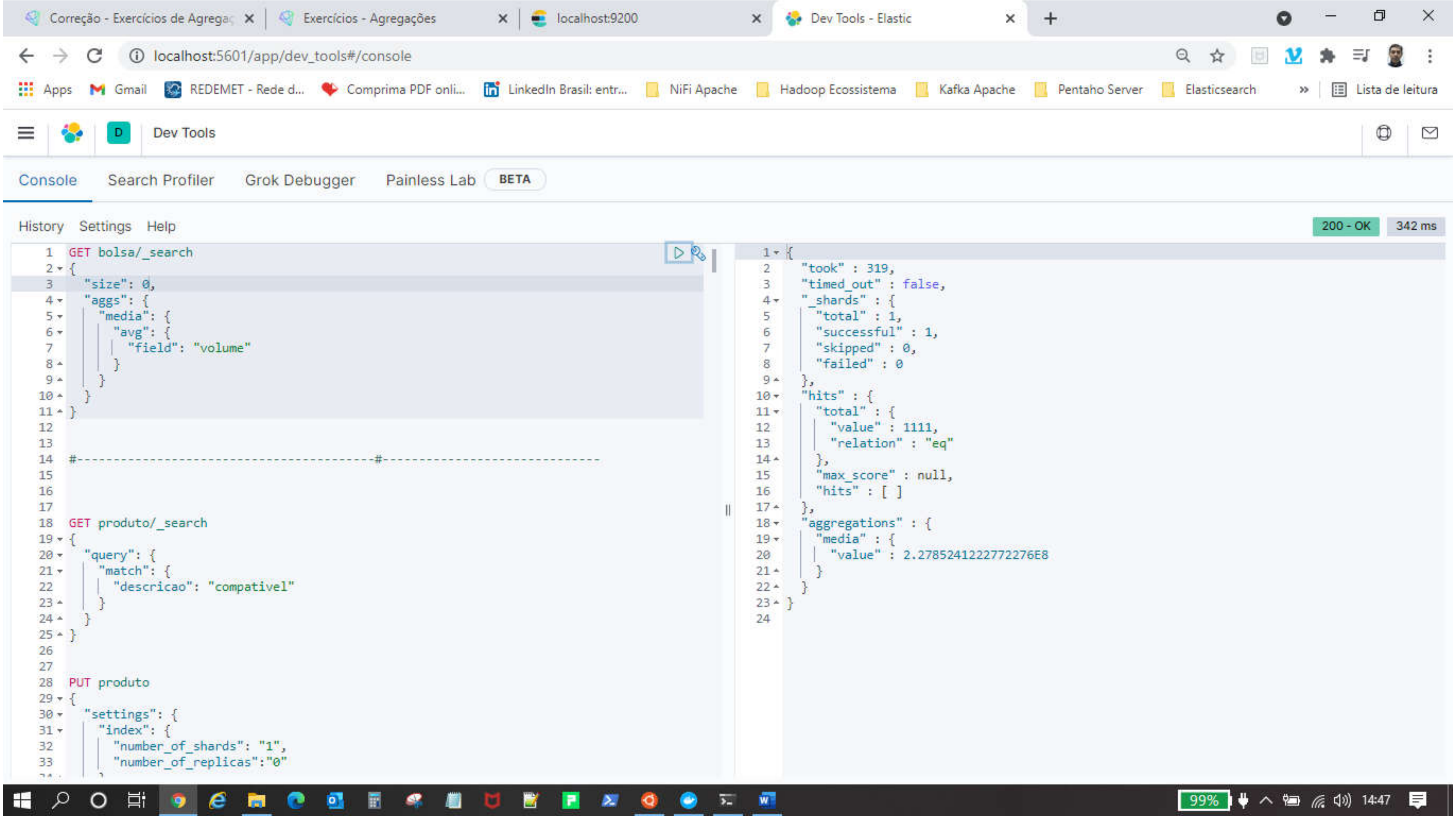
Exercitando Agregações

Acessar o MENU -> Dev Tools



Realizar os exercícios no índice bolsa

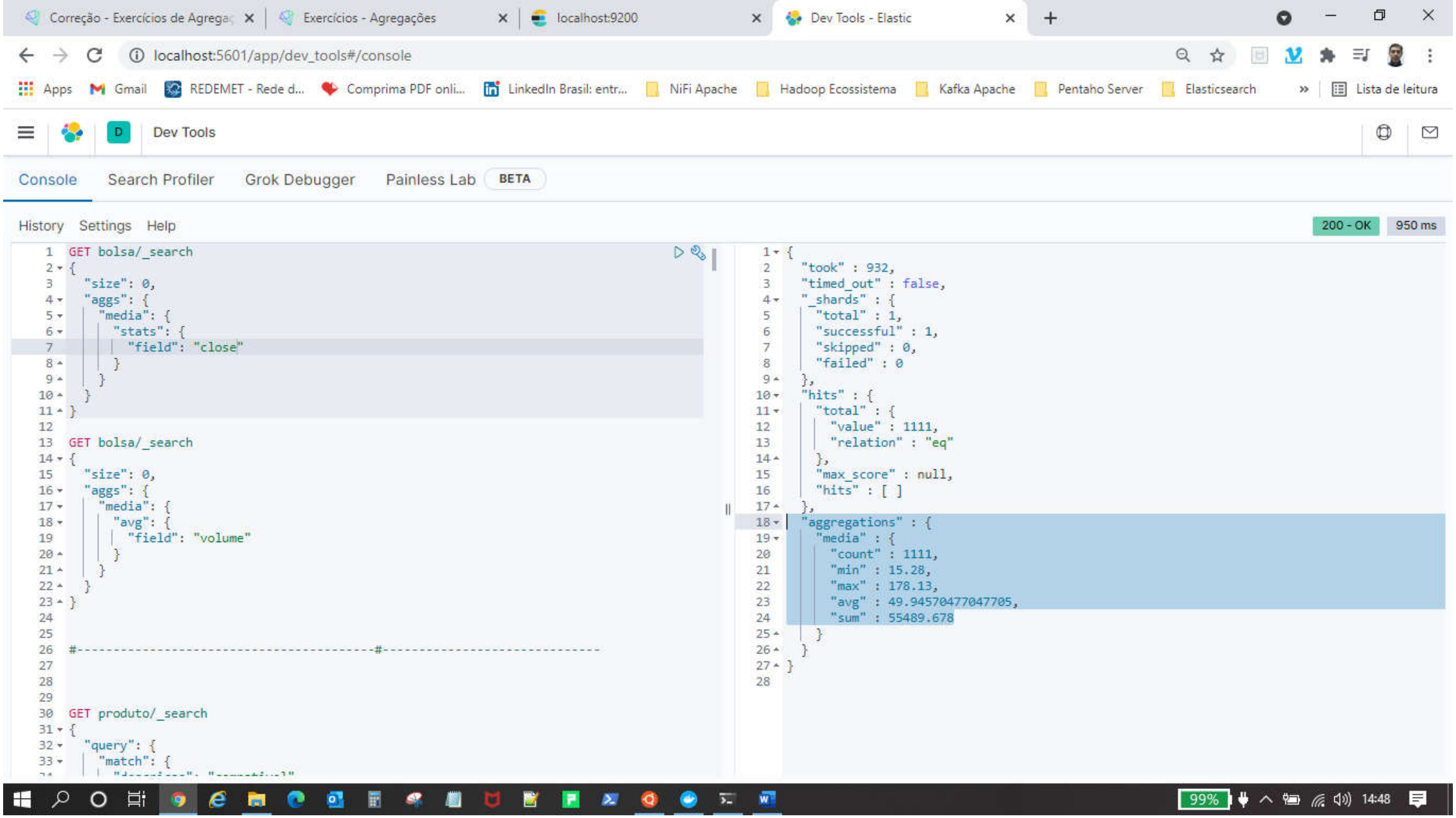
1. Calcular a média do campo volume



```
GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "media": {
      "avg": {
        "field": "volume"
      }
    }
  }
}


#---------------------------------------#-----------------------------



GET produto/_search
{
  "query": {
    "match": {
      "descricao": "compativel"
    }
  }
}


PUT produto
{
  "settings": {
    "index": {
      "number_of_shards": "1",
      "number_of_replicas":"0"
```

```
{
  "took" : 319,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1111,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "media" : {
      "value" : 2.2785241222772276E8
    }
  }
}
```

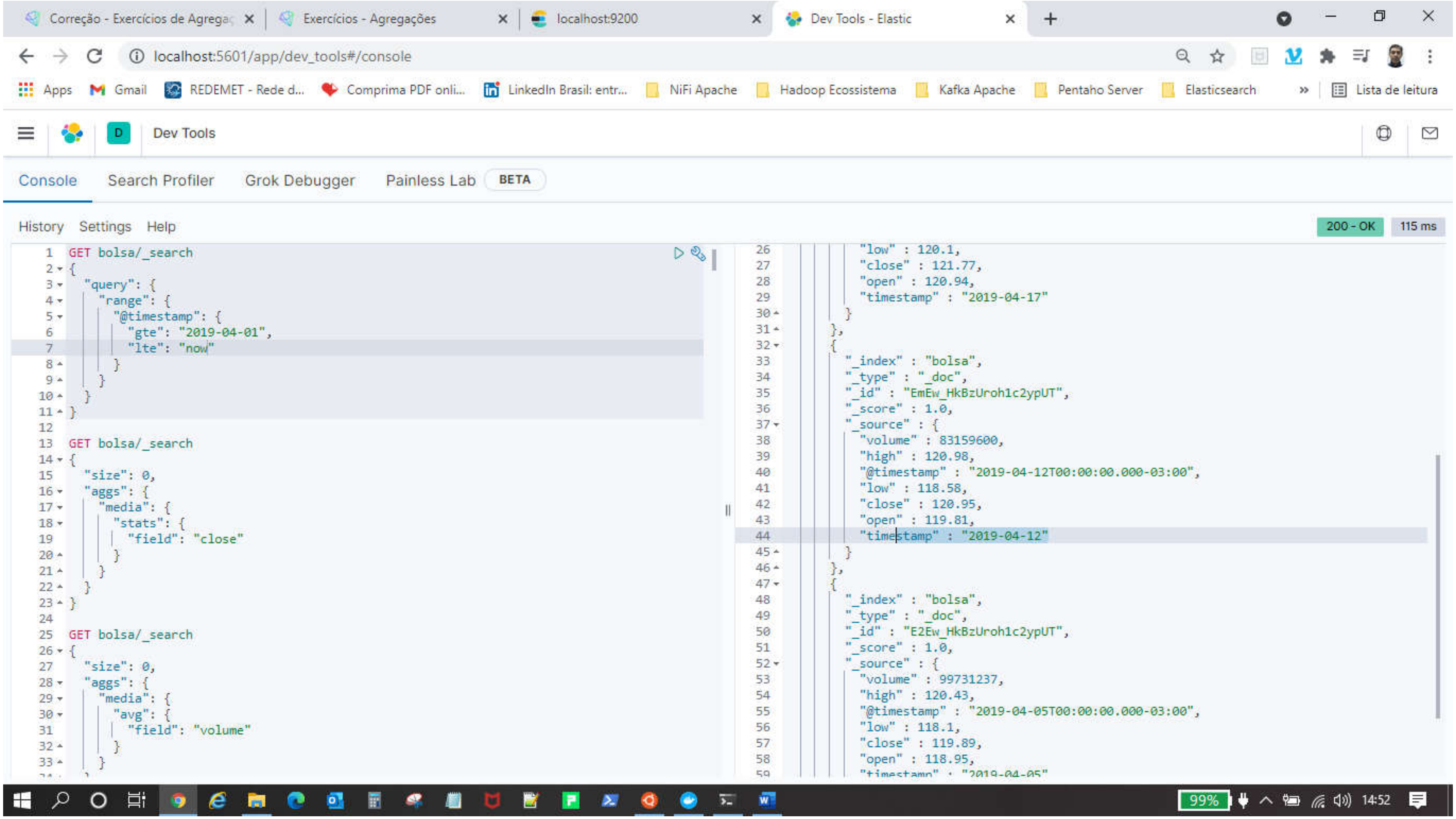
2. Calcular a estatística do campo close



```
GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "media": {
      "stats": {
        "field": "close"
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "media": {
      "avg": {
        "field": "volume"
      }
    }
  }
}


#----------------------------------------#----------------------------



GET produto/_search
{
  "query": {
    "match": {
```

```
{
  "took" : 932,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1111,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "media" : {
      "count" : 1111,
      "min" : 15.28,
      "max" : 178.13,
      "avg" : 49.94570477047705,
      "sum" : 55489.678
    }
  }
}
```

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

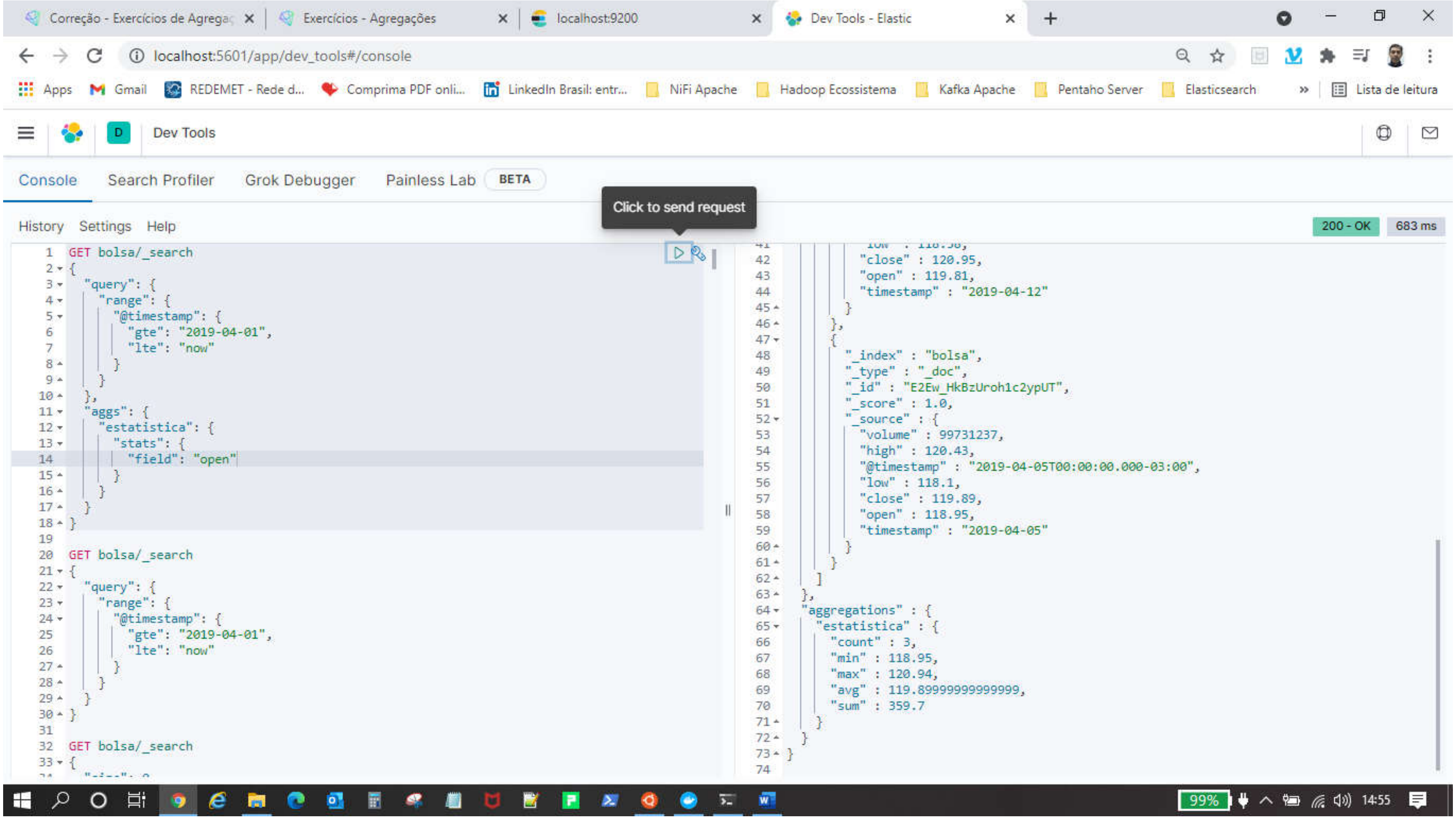


```
GET bolsa/_search
{
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "media": {
      "stats": {
        "field": "close"
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "media": {
      "avg": {
        "field": "volume"
      }
    }
```

```
          "low" : 120.1,
          "close" : 121.77,
          "open" : 120.94,
          "timestamp" : "2019-04-17"
        }
      },
      {
        "_index" : "bolsa",
        "_type" : "_doc",
        "_id" : "EmEw_HkBzUroh1c2ypUT",
        "_score" : 1.0,
        "_source" : {
          "volume" : 83159600,
          "high" : 120.98,
          "@timestamp" : "2019-04-12T00:00:00.000-03:00",
          "low" : 118.58,
          "close" : 120.95,
          "open" : 119.81,
          "timestamp" : "2019-04-12"
        }
      },
      {
        "_index" : "bolsa",
        "_type" : "_doc",
        "_id" : "E2Ew_HkBzUroh1c2ypUT",
        "_score" : 1.0,
        "_source" : {
          "volume" : 99731237,
          "high" : 120.43,
          "@timestamp" : "2019-04-05T00:00:00.000-03:00",
          "low" : 118.1,
          "close" : 119.89,
          "open" : 118.95,
          "timestamp" : "2019-04-05"
```

4. Calcular a estatística do campo open do período do dia 2019-04-01 até agora

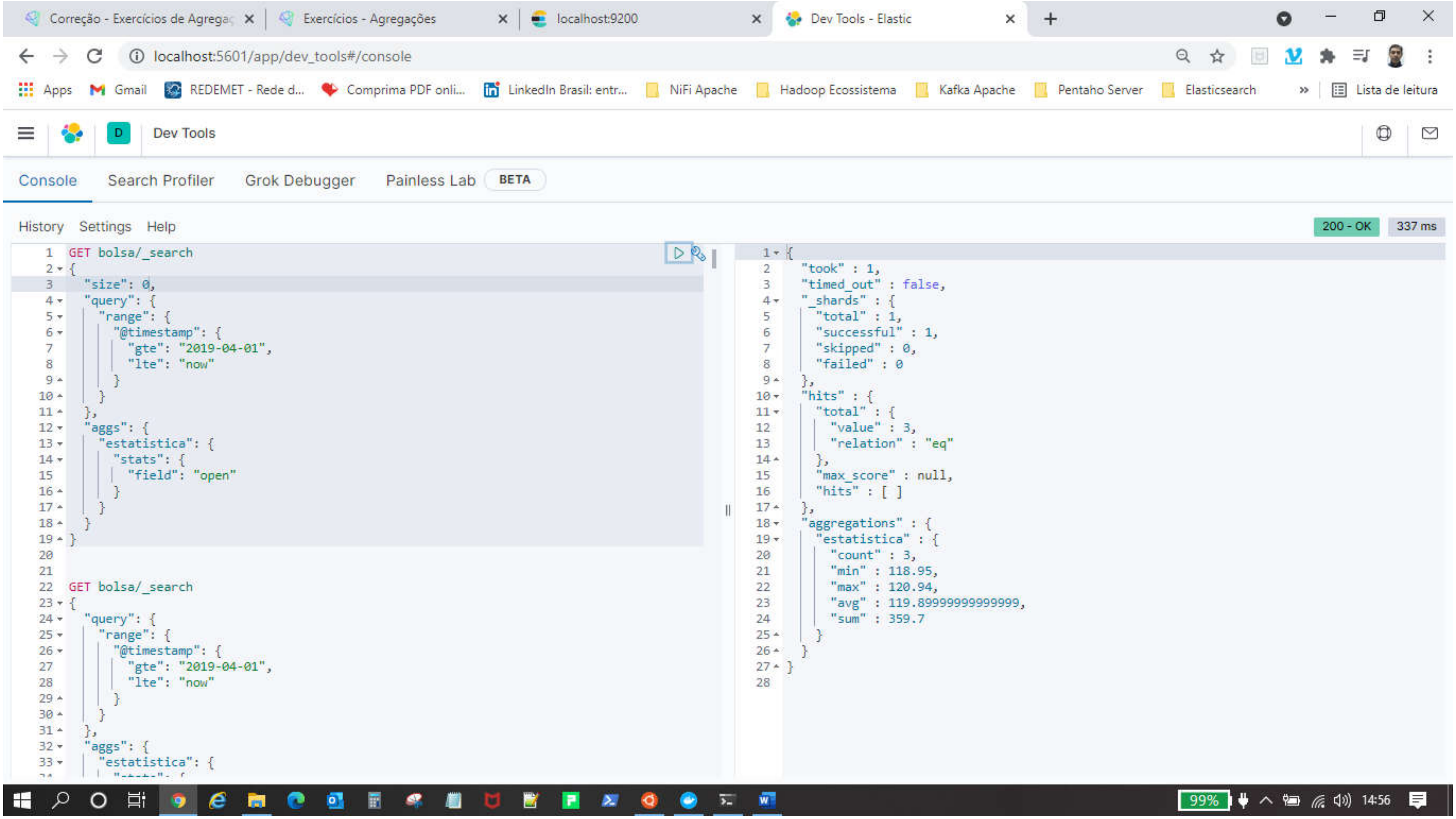
Mostra os documentos pesquisados e a estatística dela



```
GET bolsa/_search
{
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  },
  "aggs": {
    "estatistica": {
      "stats": {
        "field": "open"
      }
    }
  }
}

GET bolsa/_search
{
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  }
}

GET bolsa/_search
{
```

```
        "close" : 120.95,
        "open" : 119.81,
        "timestamp" : "2019-04-12"
      }
    },
    {
      "_index" : "bolsa",
      "_type" : "_doc",
      "_id" : "E2Ew_HkBzUroh1c2ypUT",
      "_score" : 1.0,
      "_source" : {
        "volume" : 99731237,
        "high" : 120.43,
        "@timestamp" : "2019-04-05T00:00:00.000-03:00",
        "low" : 118.1,
        "close" : 119.89,
        "open" : 118.95,
        "timestamp" : "2019-04-05"
      }
    }
  ]
},
"aggregations" : {
  "estatistica" : {
    "count" : 3,
    "min" : 118.95,
    "max" : 120.94,
    "avg" : 119.89999999999999,
    "sum" : 359.7
  }
}
}
```

Se colocar size 0 mostra apenas a estatística dos documentos pesquisados.



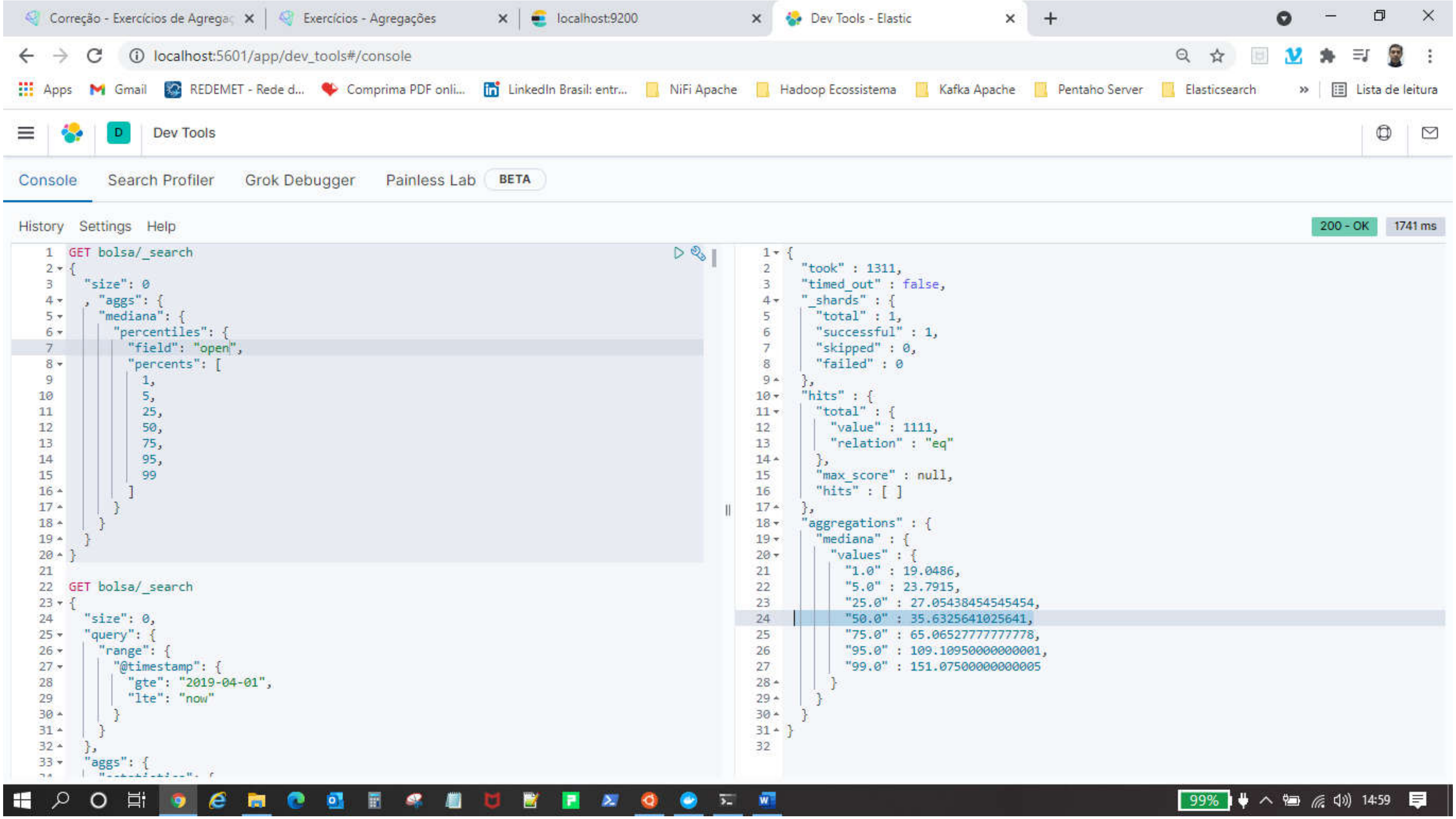
```
GET bolsa/_search
{
  "size": 0,
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  },
  "aggs": {
    "estatistica": {
      "stats": {
        "field": "open"
      }
    }
  }
}


GET bolsa/_search
{
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  },
  "aggs": {
    "estatistica": {
```

```
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 3,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "estatistica" : {
      "count" : 3,
      "min" : 118.95,
      "max" : 120.94,
      "avg" : 119.89999999999999,
      "sum" : 359.7
    }
  }
}
```

5. Calcular a mediana do campo open

Não existe mediana

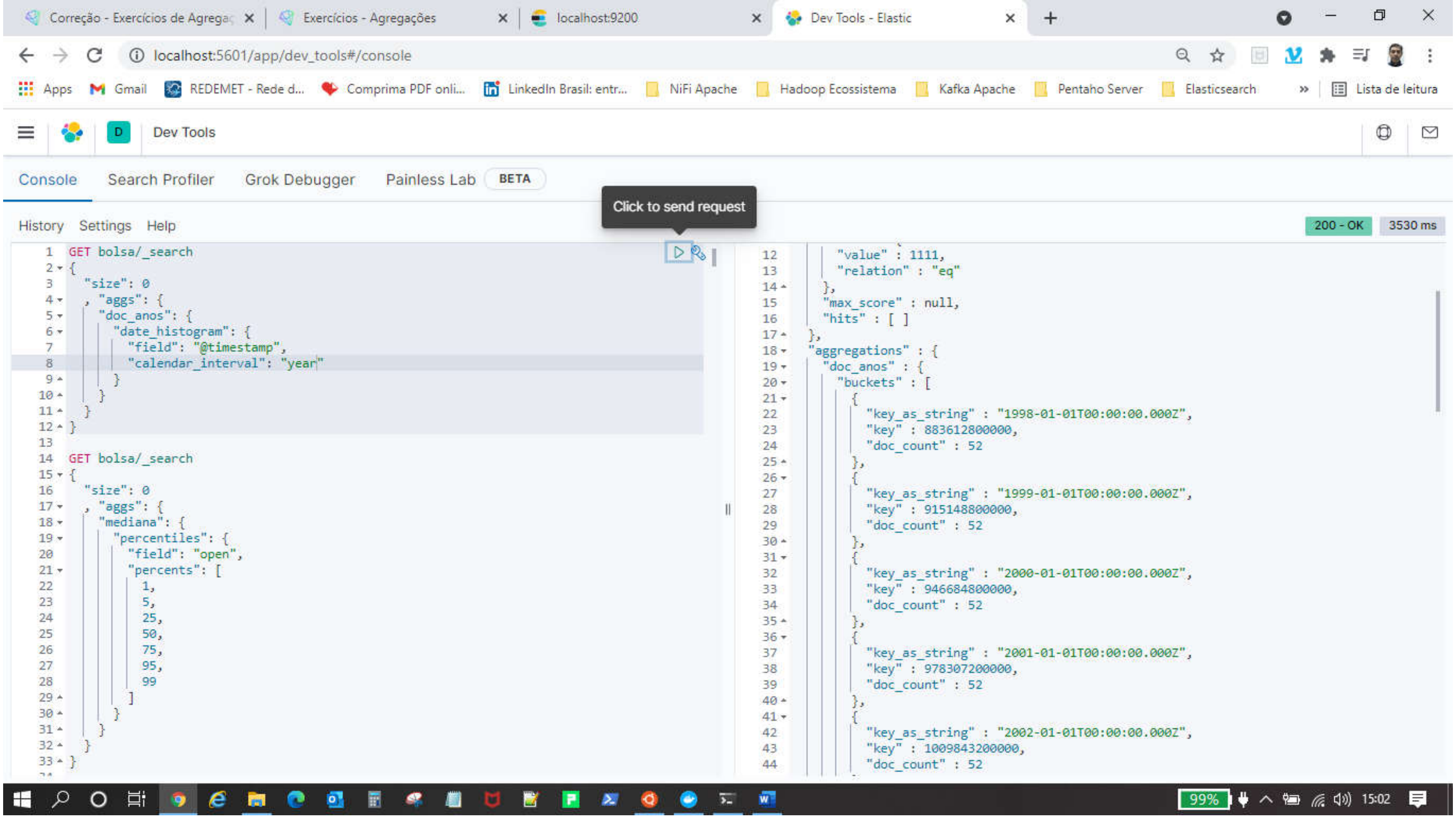
A media aparare no 50% = 35,63



```
GET bolsa/_search
{
  "size": 0
  , "aggs": {
    "mediana": {
      "percentiles": {
        "field": "open",
        "percents": [
          1,
          5,
          25,
          50,
          75,
          95,
          99
        ]
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0,
  "query": {
    "range": {
      "@timestamp": {
        "gte": "2019-04-01",
        "lte": "now"
      }
    }
  },
  "aggs": {
```

```
{
  "took" : 1311,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1111,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "mediana" : {
      "values" : {
        "1.0" : 19.0486,
        "5.0" : 23.7915,
        "25.0" : 27.05438454545454,
        "50.0" : 35.6325641025641,
        "75.0" : 65.06527777777778,
        "95.0" : 109.10950000000001,
        "99.0" : 151.07500000000005
      }
    }
  }
}
```

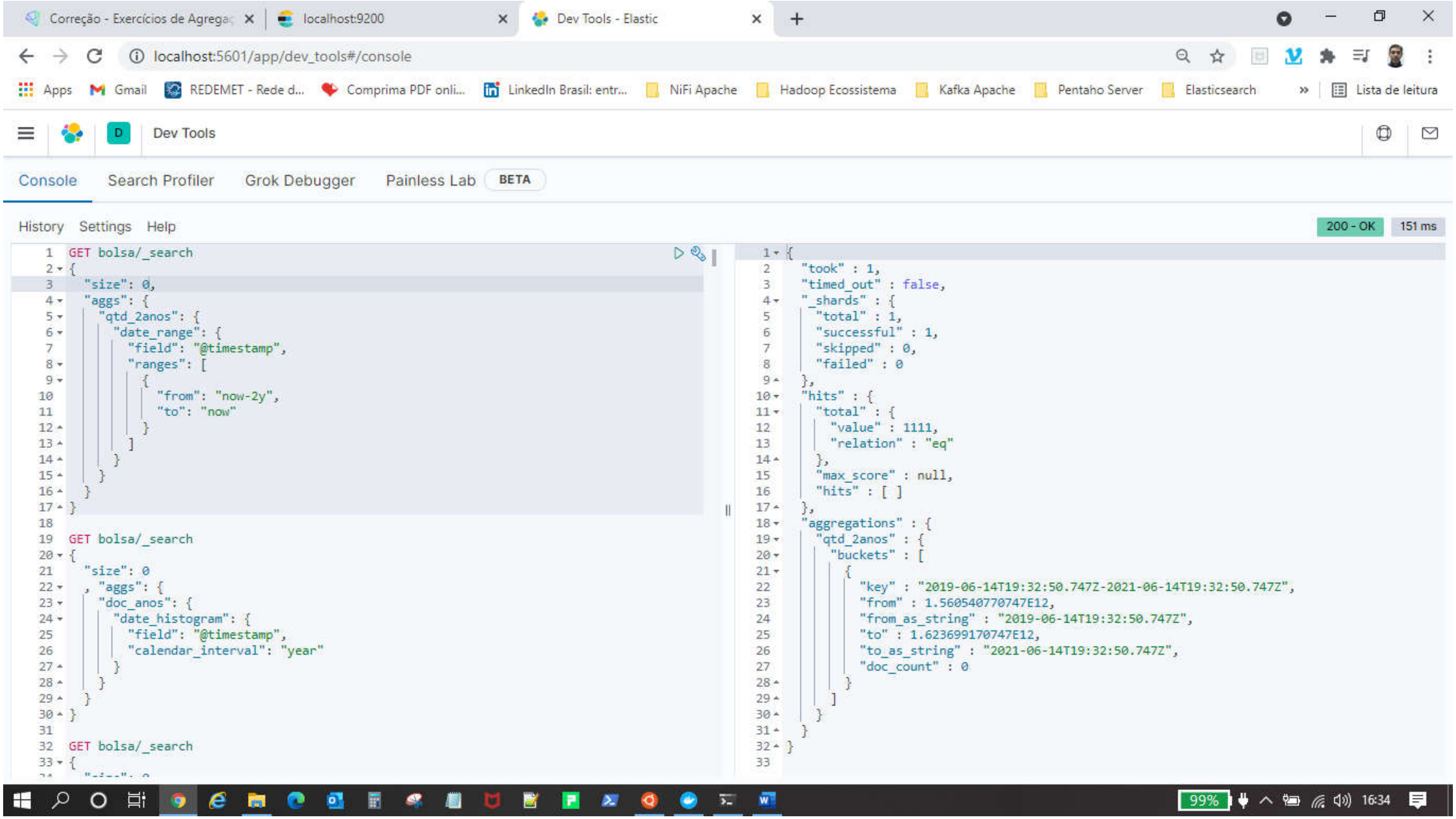
6. Contar a quantidade de documentos agrupados por ano



```
GET bolsa/_search
{
  "size": 0
  , "aggs": {
    "doc_anos": {
      "date_histogram": {
        "field": "@timestamp",
        "calendar_interval": "year"
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0
  , "aggs": {
    "mediana": {
      "percentiles": {
        "field": "open",
        "percents": [
          1,
          5,
          25,
          50,
          75,
          95,
          99
        ]
      }
    }
  }
}
```

```
      "value" : 1111,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "doc_anos" : {
      "buckets" : [
        {
          "key_as_string" : "1998-01-01T00:00:00.000Z",
          "key" : 883612800000,
          "doc_count" : 52
        },
        {
          "key_as_string" : "1999-01-01T00:00:00.000Z",
          "key" : 915148800000,
          "doc_count" : 52
        },
        {
          "key_as_string" : "2000-01-01T00:00:00.000Z",
          "key" : 946684800000,
          "doc_count" : 52
        },
        {
          "key_as_string" : "2001-01-01T00:00:00.000Z",
          "key" : 978307200000,
          "doc_count" : 52
        },
        {
          "key_as_string" : "2002-01-01T00:00:00.000Z",
          "key" : 1009843200000,
          "doc_count" : 52
```

7. Contar a quantidade de documentos de 2 anos atrás até hoje



```
GET bolsa/_search
{
  "size": 0,
  "aggs": {
    "qtd_2anos": {
      "date_range": {
        "field": "@timestamp",
        "ranges": [
          {
            "from": "now-2y",
            "to": "now"
          }
        ]
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0
  , "aggs": {
    "doc_anos": {
      "date_histogram": {
        "field": "@timestamp",
        "calendar_interval": "year"
      }
    }
  }
}

GET bolsa/_search
{
  "size": 0
```

```
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1111,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  },
  "aggregations" : {
    "qtd_2anos" : {
      "buckets" : [
        {
          "key" : "2019-06-14T19:32:50.747Z-2021-06-14T19:32:50.747Z",
          "from" : 1.560540770747E12,
          "from_as_string" : "2019-06-14T19:32:50.747Z",
          "to" : 1.623699170747E12,
          "to_as_string" : "2021-06-14T19:32:50.747Z",
          "doc_count" : 0
        }
      ]
    }
  }
}
```