

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

 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

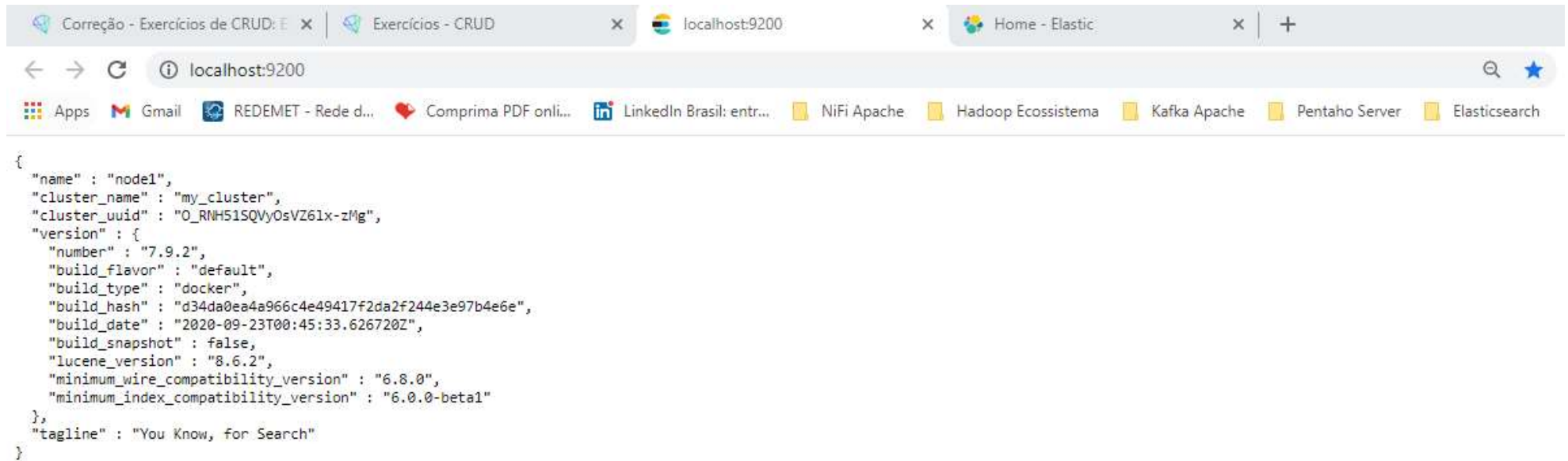
RUNNING PORT: 9200

```
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 tabs for '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** (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 cards and 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 adding data: '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 a card for 'App Search' (Leverage dashboards, analytics, and APIs for advanced application).
- Manage and Administer the Elastic Stack**: Includes cards for '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 Beats

Filebeat

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

Acessar a pasta dataset para utilizar o arquivo paris-925.logs

```
feliciani@LAPTOP-V176DRSL:~$ cd /mnt/e/projetos/docker-elasticsearch
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch$ cd elastic
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ ls
data  dataset  docker-compose.yml  pipeline  settings
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ ls dataset
blogs.csv  cars.bulk  paris-925.logs  populacaoLA.csv  weekly_MSFT.csv
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$
```

Verificar o conteúdo do arquivo paris-925.logs

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ head dataset/paris-925.logs
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$
```


O arquivo contém um sequencia de logs que será enviado para o elasticsearch

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ head dataset/paris-925.logs
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/sad-medic.png HTTP/1.1" 200 430406 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Bold.ttf HTTP/1.1" 200 38720 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/css/fonts/Roboto-Regular.ttf HTTP/1.1" 200 41820 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:45 +0000] "GET /presentations/logstash-monitorama-2013/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [26/Aug/2014:21:13:43 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard.png HTTP/1.1" 200 321631 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$
```

Baixando o Filebeat da mesma versão do elasticsearch para Linux

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.9.2-linux-x86_64.tar.gz
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload    Total   Spent    Left   Speed
100 29.7M  100 29.7M    0     0  1451k      0  0:00:20  0:00:20 --:--:-- 1490k
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$
```

Descompactando o arquivo

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ ls
data  dataset  docker-compose.yml  filebeat-7.9.2-linux-x86_64  filebeat-7.9.2-linux-x86_64.tar.gz  pipeline  settings
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ sudo tar -xzf filebeat-7.9.2-linux-x86_64.tar.gz
```

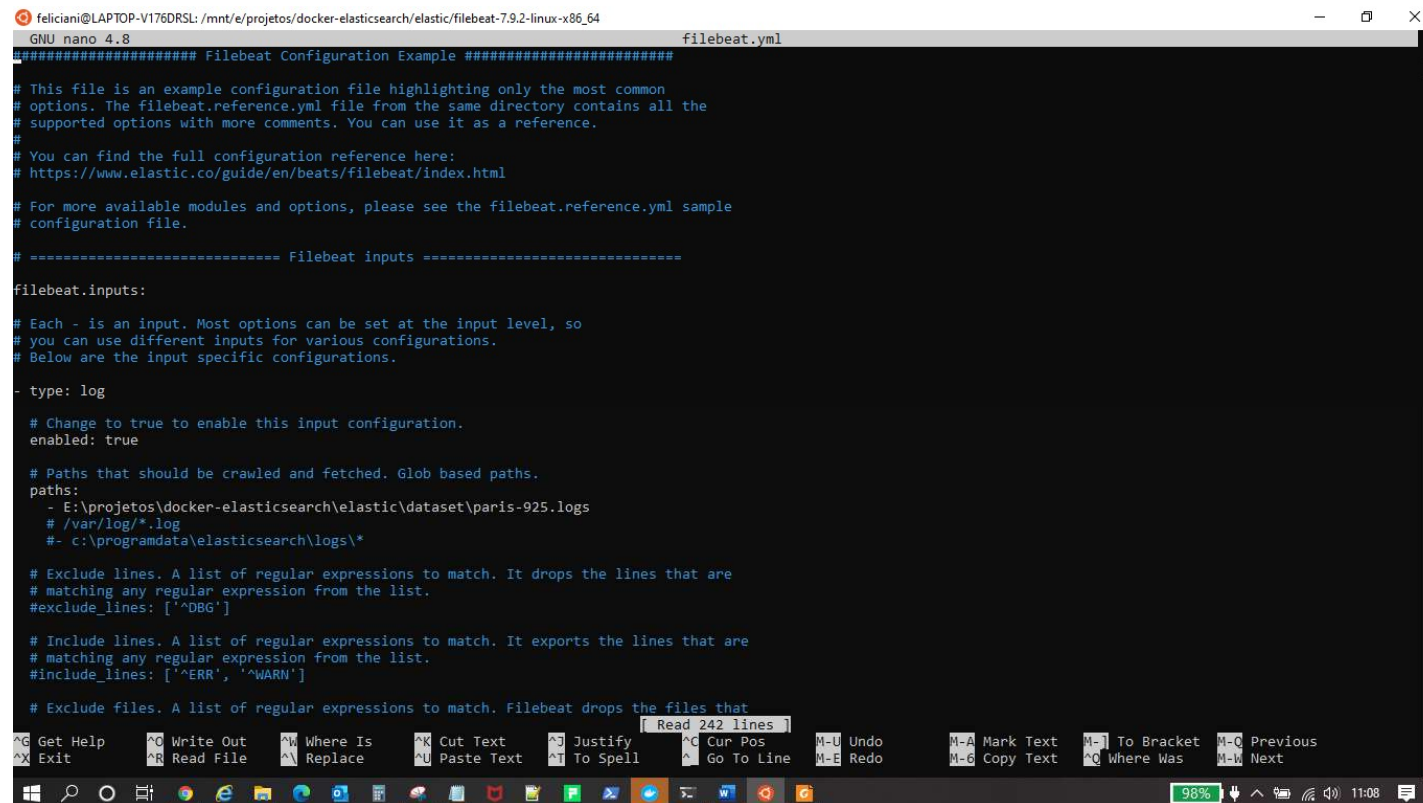
Arquivos contidos na pasta descompactada

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ cd filebeat-7.9.2-linux-x86_64/
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/filebeat-7.9.2-linux-x86_64$ ls
LICENSE.txt NOTICE.txt README.md fields.yml filebeat filebeat.reference.yml filebeat.yml kibana module modules.d
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/filebeat-7.9.2-linux-x86_64$
```

Acessar o arquivo filebeat.yml para configurar a entrada e a saída dos dados

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/filebeat-7.9.2-linux-x86_64$ nano filebeat.yml
```

Foi habilitada o input para **ENABLE** e foi colocado o endereço de origem dos dados (E:\projetos\docker-elasticsearch\elastic\dataset\paris-925.logs) e a saída será o elastic <http://localhost:9200>



```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/filebeat-7.9.2-linux-x86_64$ nano filebeat.yml
GNU nano 4.8 filebeat.yml
##### Filebeat Configuration Example #####

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html
#
# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

# ----- Filebeat inputs -----

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

# Change to true to enable this input configuration.
enabled: true

# Paths that should be crawled and fetched. Glob based paths.
paths:
  - E:\projetos\docker-elasticsearch\elastic\dataset\paris-925.logs
  # /var/log/*.log
  #- c:\programdata\elasticsearch\logs\*

# Exclude lines. A list of regular expressions to match. It drops the lines that are
# matching any regular expression from the list.
#exclude_lines: ['^DBG']

# Include lines. A list of regular expressions to match. It exports the lines that are
# matching any regular expression from the list.
#include_lines: ['^ERR', '^WARN']

# Exclude files. A list of regular expressions to match. Filebeat drops the files that
# match any regular expression from the list.
#exclude_files: ['.*\.*']

[ Read 242 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^M Undo ^M-A Mark Text ^M-] To Bracket ^M-0 Previous
^X Exit ^R Read File ^N Replace ^U Paste Text ^T To Spell ^G Go To Line ^M-E Redo ^M-C Copy Text ^M-6 Copy Text ^M-^ Where Was ^M-W Next
```


Testando o arquivo

```
semantix@NT85TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ./filebeat test config
Config OK
semantix@NT85TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
```

Testando a conexão

```
semantix@NT85TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ./filebeat test output
elasticsearch: http://localhost:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1, 127.0.0.1
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
  version: 7.9.2
semantix@NT85TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
```

Enviando os logs

```
semantix@NT85TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo ./filebeat -e
```

```
2020-10-13T17:28:38.962-0300 INFO [registrar] registrar/registrar.go:109 States Loaded from registrar: 0
2020-10-13T17:28:38.962-0300 INFO [crawler] beater/crawler.go:71 Loading Inputs: 1
2020-10-13T17:28:38.963-0300 INFO log/input.go:157 Configured paths: [/home/semantix/treinamentos/elastic/dataset/paris-925.logs]
2020-10-13T17:28:38.963-0300 INFO [crawler] beater/crawler.go:141 Starting input (ID: 3976361801678345579)
2020-10-13T17:28:38.963-0300 INFO [crawler] beater/crawler.go:108 Loading and starting Inputs completed. Enabled inputs: 1
2020-10-13T17:28:38.963-0300 INFO cfgfile/reload.go:164 Config reloader started
2020-10-13T17:28:38.963-0300 INFO log/harvester.go:299 Harvester started for file: /home/semantix/treinamentos/elastic/dataset/paris-925.logs
```



```

y successfully loaded.
2020-10-13T17:28:42.119-0300    INFO    [index-management]    idxmgmt/std.go:407    Set setup
.template.name to '{filebeat-7.9.2 {now/d}-000001}' as ILM is enabled.
2020-10-13T17:28:42.119-0300    INFO    [index-management]    idxmgmt/std.go:412    Set setup
.template.pattern to 'filebeat-7.9.2-*' as ILM is enabled.
2020-10-13T17:28:42.120-0300    INFO    [index-management]    idxmgmt/std.go:446    Set setti
ngs.index.lifecycle.rollover_alias in template to {filebeat-7.9.2 {now/d}-000001} as ILM is enabl
ed.
2020-10-13T17:28:42.120-0300    INFO    [index-management]    idxmgmt/std.go:450    Set setti
ngs.index.lifecycle.name in template to {filebeat {"policy":{"phases":{"hot":{"actions":{"rollove
r":{"max_age":"30d","max_size":"50gb"}}}}}}}} as ILM is enabled.
2020-10-13T17:28:42.124-0300    INFO    template/load.go:169    Existing template will be overwri
tten, as overwrite is enabled.
2020-10-13T17:28:42.838-0300    INFO    template/load.go:109    Try loading template filebeat-7.9
.2 to Elasticsearch
2020-10-13T17:28:43.129-0300    INFO    template/load.go:101    template with name 'filebeat-7.9.
2' loaded.
2020-10-13T17:28:43.129-0300    INFO    [index-management]    idxmgmt/std.go:298    Loaded in
dex template.
2020-10-13T17:28:43.723-0300    INFO    [index-management]    idxmgmt/std.go:309    Write ali
as successfully generated.
2020-10-13T17:28:43.723-0300    INFO    [publisher_pipeline_output]    pipeline/output.go:151 C
onnection to backoff(elasticsearch(http://localhost:9200)) established

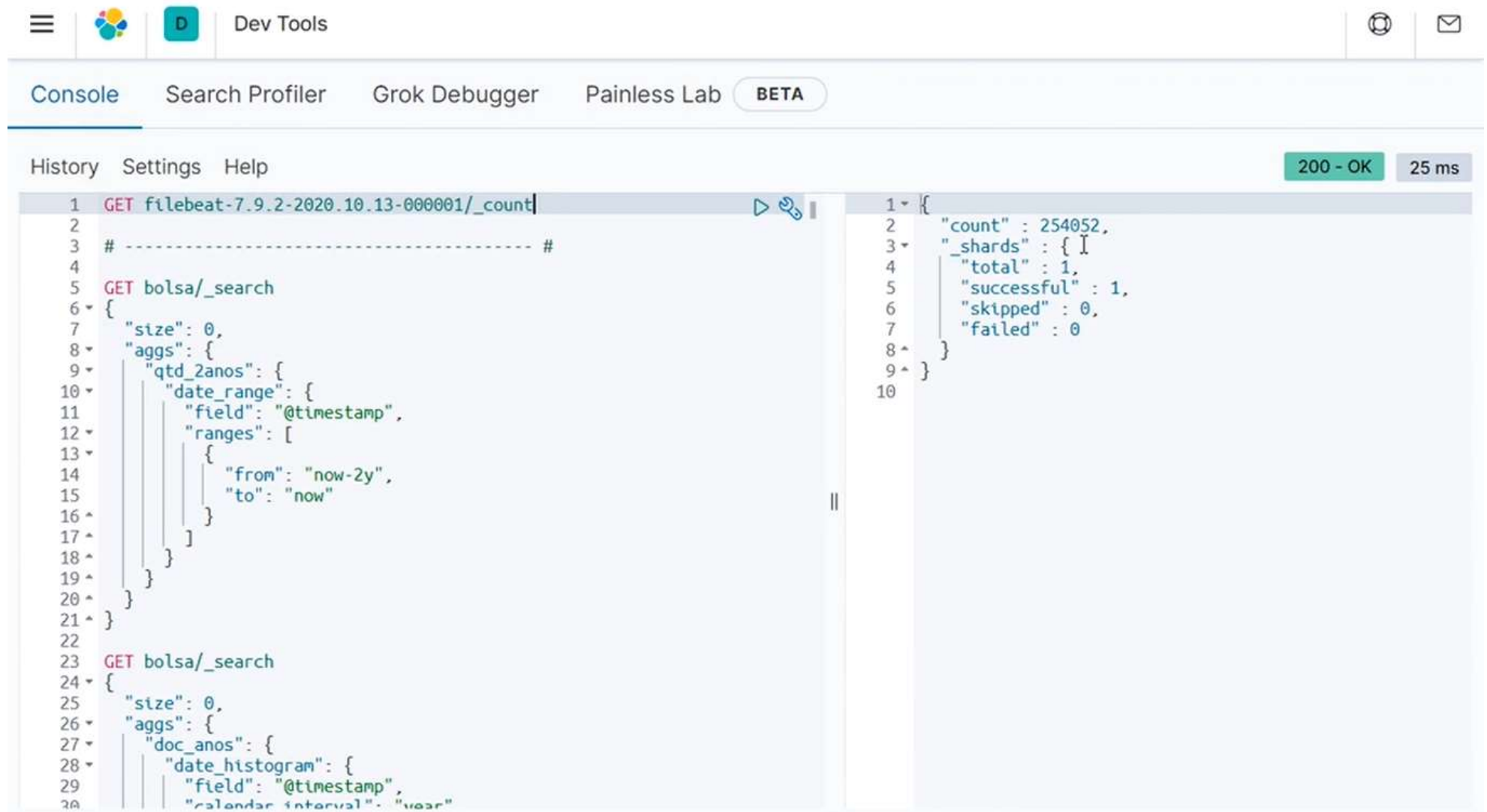
```

Acessar o MENU -> Dev Tools

The screenshot shows a web browser window with multiple tabs. The active tab is 'Dev Tools - Elastic'. The address bar shows the URL 'localhost:5601/app/dev_tools#/console'. The browser's bookmark bar contains 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 Elastic Dev Tools interface has a sidebar on the left with a menu. The menu items are: 'Home', 'Recently viewed' (with a dropdown arrow and 'No recently viewed items'), 'Security' (with a dropdown arrow and sub-items: 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases', 'Administration'), and 'Management' (with a dropdown arrow and sub-items: 'Dev Tools', 'Ingest Ma', 'Stack Monitoring', 'Stack Management'). The 'Dev Tools' item under 'Management' is highlighted, and a tooltip 'Dev Tools' is visible. The main content area is mostly blank, with some faint text visible in the background: '500GB, Sistema: Windows 10, Windows 8, Windows 7' and 'ativel com Windows, Mac e Linux'. The Windows taskbar at the bottom shows various application icons, a battery level of 98%, and the time 14:21.

2. Verificar a quantidade de documentos do índice criado pelo Filebeat e visualizar seus 10 primeiros documentos

O Filebeat enviou 2540052 documentos



The screenshot shows the DevTools interface with the Console tab selected. The top bar includes icons for navigation and a 'Dev Tools' label. The console header shows 'History', 'Settings', and 'Help' tabs, along with a status bar indicating '200 - OK' and '25 ms'.




The console displays a REST client request and its response:

```
1 GET filebeat-7.9.2-2020.10.13-000001/_count
2
3 # ----- #
4
5 GET bolsa/_search
6 {
7   "size": 0,
8   "aggs": {
9     "qtd_2anos": {
10      "date_range": {
11        "field": "@timestamp",
12        "ranges": [
13          {
14            "from": "now-2y",
15            "to": "now"
16          }
17        ]
18      }
19    }
20  }
21 }
22
23 GET bolsa/_search
24 {
25   "size": 0,
26   "aggs": {
27     "doc_anos": {
28       "date_histogram": {
29         "field": "@timestamp",
30         "calendar_interval": "year"
```

The response is a JSON object:

```
1 {
2   "count" : 254052,
3   "_shards" : {
4     "total" : 1,
5     "successful" : 1,
6     "skipped" : 0,
7     "failed" : 0
8   }
9 }
10
```


Verificando os dados dos logs enviados

 Dev Tools

Console Search Profiler Grok Debugger Painless Lab BETA

History Settings Help

200 - OK 27 ms

```
1 GET filebeat-7.9.2-2020.10.13-000001/_search
2
3 # ----- #
4
5 GET bolsa/_search
6 {
7   "size": 0,
8   "aggs": {
9     "qtd_2anos": {
10      "date_range": {
11        "field": "@timestamp",
12        "ranges": [
13          {
14            "from": "now-2y",
15            "to": "now"
16          }
17        ]
18      }
19    }
20  }
21 }
22
23 GET bolsa/_search
24 {
25   "size": 0,
26   "aggs": {
27     "doc_anos": {
28       "date_histogram": {
29         "field": "@timestamp",
30         "calendar_interval": "year"
```

```
13   "relation": "get"
14 }
15 "max_score": 1.0,
16 "hits": [
17 {
18   "_index": "filebeat-7.9.2-2020.10.13-000001",
19   "_type": "_doc",
20   "_id": "WbemI3UB8SR3RpBfn_xP",
21   "_score": 1.0,
22   "_source": {
23     "@timestamp": "2020-10-13T20:28:41.930Z"
24     "message": "66.249.73.135 - - [26/Aug/2014:21:20:03 +0000] \"GET /blog/geekery/eventdb-ideas.html HTTP/1.1\" 200 11418 \"-\" \"Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)\"",
25     "input": {
26       "type": "log"
27     },
28     "ecs": {
29       "version": "1.5.0"
30     },
31     "host": {
32     "os": {
```



Dev Tools



Console

Search Profiler

Grok Debugger

Painless Lab

BETA

History Settings Help

200 - OK

27 ms

1 GET filebeat-7.9.2-2020.10.13-000001/_search

2

3 # ----- #

4 GET bolsa/_search

5 {

6 "size": 0,

7 "aggs": {

8 "qtd_2anos": {

9 "date_range": {

10 "field": "@timestamp",

11 "ranges": [

12 {

13 "from": "now-2y",

14 "to": "now"

15 }]

16 }

17 }

18 }

19 }

20 }

21 }

22 GET bolsa/_search

23 {

24 "size": 0,

25 "aggs": {

26 "doc_anos": {

27 "date_histogram": {

28 "field": "@timestamp",

29 "calendar_interval": "year"

30 }

36 "kernel" : "4.19.84-microsoft

-standard",

37 "codename" : "bionic",

38 "platform" : "ubuntu"

39 }

40 "id" :

"fd1a27fcd918430c94067fac07f4aef6",

41 "containerized" : false,

42 "ip" : [

43 "172.30.86.59",

44 "fe80::215:5dff:fe89:97d4"

45],

46 "mac" : [

47 "5a:02:af:d7:35:e9",

48 "4a:0e:c5:d8:1f:bd",

49 "00:15:5d:89:97:d4"

50],

51 "name" : "NTBSTX7158",

52 "hostname" : "NTBSTX7158",

53 "architecture" : "x86_64"

54 }

55 "agent" : {

56 "name" : "NTBSTX7158",

57 "type" : "filebeat",

58 "version" : "7.9.2",

59 "hostname" : "NTBSTX7158",

60 "ephemeral_id" : "f6159851-a70a-4b0c

-bd97-bff4fdec33c4",

61 "id" : "d5a9fc17-d2ad-4688-8127

f6159851-a70a-4b0c-bd97-bff4fdec33c4"

Utilizando Metricbeat

Baixando o Metricbeat

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.9.2-linux-x86_64.tar.gz
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left    Speed
100 37.0M  100 37.0M    0     0 1326k      0  0:00:28  0:00:28 --:--:-- 1690k
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$
```

Entrando na pasta do Metricbeat

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ ls
data      docker-compose.yml  filebeat-7.9.2-linux-x86_64.tar.gz  metricbeat-7.9.2-linux-x86_64.tar.gz  settings
dataset   filebeat-7.9.2-linux-x86_64  metricbeat-7.9.2-linux-x86_64      pipeline
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic$ cd metricbeat-7.9.2-linux-x86_64/
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/metricbeat-7.9.2-linux-x86_64$
```

Verificando os módulos

```
semantix@NT8STX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat modules list
```

```
mssql
munin
mysql
nats
nginx
openmetrics
oracle
php_fpm
postgresql
prometheus
rabbitmq
redis
redisenterprise
sql
stan
statsd
tomcat
traefik
uwsgi
vsphere
windows
```


Habilitando o módulo do docker

```
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat modules enable docker
Enabled docker
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$
```

docker aparece ENABLE

```
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat modules list
Enabled:
docker
system

Disabled:
activemq
aerospike
apache
```

Testando a configuração

```
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat test config
Config OK
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$
```

Output também está OK

```
semantix@NTB5TX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat test output
elasticsearch: http://localhost:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1, 127.0.0.1
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
  version: 7.9.2
```

Verificando os módulos

```
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/metricbeat-7.9.2-linux-x86_64$ cd modules.d
feliciani@LAPTOP-V176DRSL:/mnt/e/projetos/docker-elasticsearch/elastic/metricbeat-7.9.2-linux-x86_64/modules.d$ ls
```

Docker está enable e a grande maioria disable

```
activemq.yml.disabled  golang.yml.disabled  nats.yml.disabled
aerospike.yml.disabled googlecloud.yml.disabled nginx.yml.disabled
apache.yml.disabled   graphite.yml.disabled openmetrics.yml.disabled
appsearch.yml.disabled haproxy.yml.disabled oracle.yml.disabled
aws.yml.disabled      http.yml.disabled    php_fpm.yml.disabled
azure.yml.disabled    ibmq.yml.disabled    postgresql.yml.disabled
beat-xpack.yml.disabled iis.yml.disabled     prometheus.yml.disabled
beat.yml.disabled     istio.yml.disabled   rabbitmq.yml.disabled
ceph-mgr.yml.disabled jolokia.yml.disabled redis.yml.disabled
ceph.yml.disabled     kafka.yml.disabled  redisenterprise.yml.disabled
cloudfoundry.yml.disabled kibana-xpack.yml.disabled sql.yml.disabled
cockroachdb.yml.disabled kibana.yml.disabled  stan.yml.disabled
consul.yml.disabled   kubernetes.yml.disabled statsd.yml.disabled
coredns.yml.disabled  kvm.yml.disabled     system.yml
couchbase.yml.disabled linux.yml.disabled   tomcat.yml.disabled
couchdb.yml.disabled  logstash-xpack.yml.disabled traefik.yml.disabled
docker.yml            logstash.yml.disabled uwsgi.yml.disabled
dropwizard.yml.disabled memcached.yml.disabled vsphere.yml.disabled
elasticsearch-xpack.yml.disabled mongodb.yml.disabled windows.yml.disabled
elasticsearch.yml.disabled mssql.yml.disabled  zookeeper.yml.disabled
envoyproxy.yml.disabled munin.yml.disabled
etcd.yml.disabled     mysql.yml.disabled
```

Conteúdo do Docker.yml

```
$ cat docker.yml
# Module: docker
# Docs: https://www.elastic.co/guide/en/beats/metricbeat/7.9/metricbeat-module-docker.html

- module: docker
  #metricsets:
  # - container
  # - cpu
  # - diskio
  # - event
  # - healthcheck
  # - info
  # - memory
  # - network
  period: 10s
  hosts: ["unix:///var/run/docker.sock"]

  # If set to true, replace dots in labels with '_'.
  #labels.dedot: false

  # To connect to Docker over TLS you must specify a client and CA certificate.
  #ssl:
  #certificate_authority: "/etc/pki/root/ca.pem"
  #certificate: "/etc/pki/client/cert.pem"
```

Procurando o arquivo para editar e colocar o local host

```
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64/modules.d
$ sudo find / -name docker.sock
[sudo] password for semantix:
find: '/mnt/g': Function not implemented
/mnt/wsl/docker-desktop/shared-sockets/guest-services/docker.sock
^C
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64/modules.d
$ vi docker.yml
```

Configurado para monitorar container, cpu, info, memory, período, host e enable true

```
# Module: docker
# Docs: https://www.elastic.co/guide/en/beats/metricbeat/7.9/metricbeat-module-docker.html

- module: docker
  metricsets:
    - container
    - cpu
  # - diskio
  # - event
  # - healthcheck
  - info
  - memory
  # - network
  period: 10s
  hosts: ["unix:///mnt/wsl/docker-desktop/shared-sockets/guest-services/docker.sock"]
  enabled: true
  # If set to true, replace dots in labels with '_'.
  #labels.dedot: false

  # To connect to Docker over TLS you must specify a client and CA certificate.
  #ssl:
```

Testar para ver se tudo continua OK, após a edição acima

```
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat test config
Config OK
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ ./metricbeat test output
elasticsearch: http://localhost:9200...
parse url... OK
connection...
parse host... OK
dns lookup... OK
addresses: 127.0.0.1, 127.0.0.1
dial up... OK
TLS... WARN secure connection disabled
talk to server... OK
version: 7.9.2
```

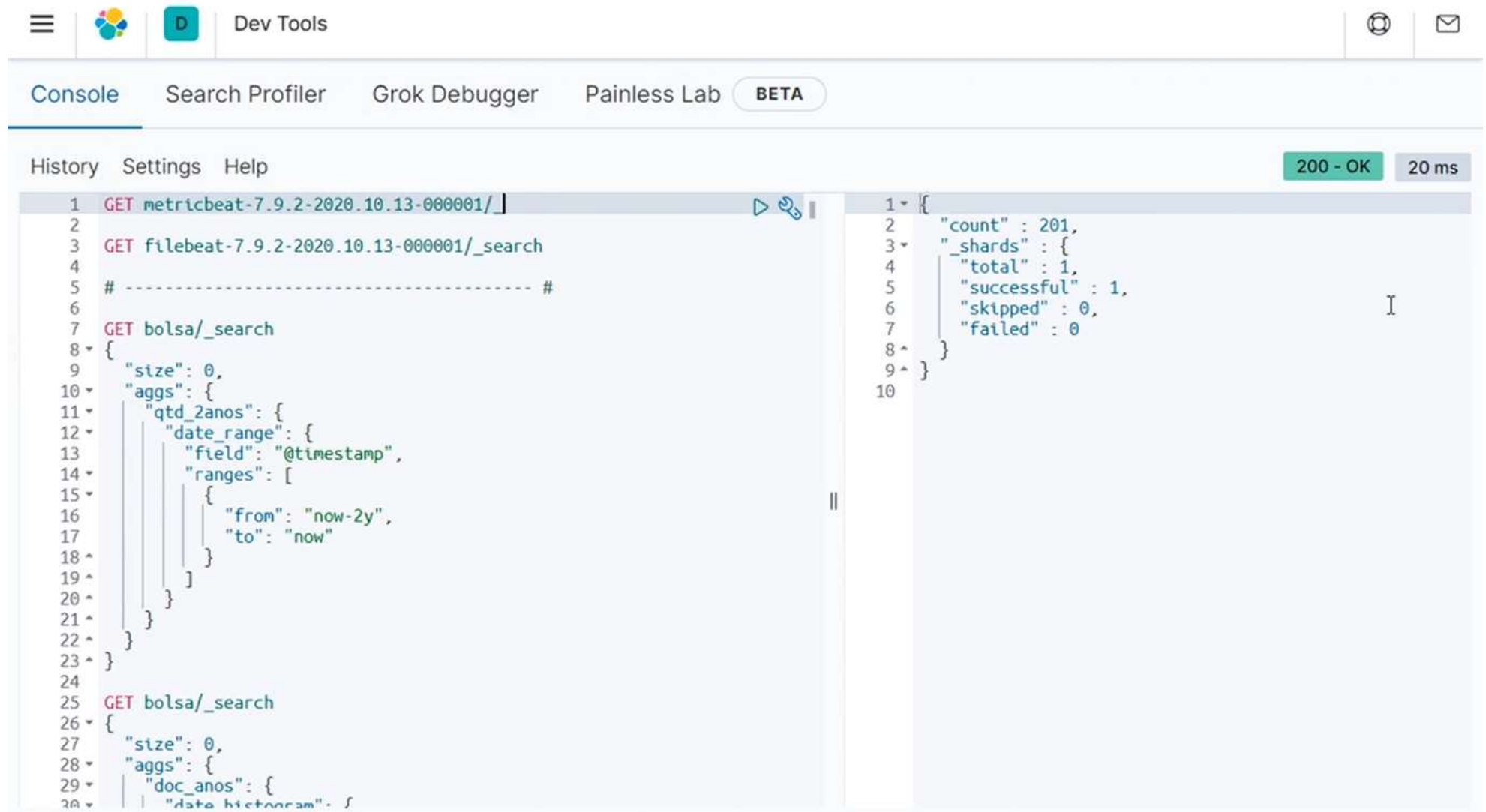

Iniciando a coleta

```
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ sudo chown root modules.d/docker.yml
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ sudo chown root metricbeat.yml
semantix@NTBSTX7158:~/treinamentos/elastic/metricbeat-7.9.2-linux-x86_64
$ sudo ./metricbeat -e
```

```
y successfully loaded.
2020-10-13T18:00:09.593-0300 INFO [index-management] idxmgmt/std.go:407 Set setup
.template.name to '{metricbeat-7.9.2 {now/d}-000001}' as ILM is enabled.
2020-10-13T18:00:09.593-0300 INFO [index-management] idxmgmt/std.go:412 Set setup
.template.pattern to 'metricbeat-7.9.2-*' as ILM is enabled.
2020-10-13T18:00:09.593-0300 INFO [index-management] idxmgmt/std.go:446 Set setti
ngs.index.lifecycle.rollover_alias in template to {metricbeat-7.9.2 {now/d}-000001} as ILM is ena
bled.
2020-10-13T18:00:09.593-0300 INFO [index-management] idxmgmt/std.go:450 Set setti
ngs.index.lifecycle.name in template to {metricbeat {policy:{phases:{hot:{actions:{rollo
ver":{"max_age":"30d","max_size":"50gb"}}}}}}}} as ILM is enabled.
2020-10-13T18:00:09.596-0300 INFO template/load.go:169 Existing template will be overwri
tten, as overwrite is enabled.
2020-10-13T18:00:09.812-0300 INFO template/load.go:189 Try loading template metricbeat-7
.9.2 to Elasticsearch
2020-10-13T18:00:10.058-0300 INFO template/load.go:101 template with name 'metricbeat-7.
9.2' loaded.
2020-10-13T18:00:10.058-0300 INFO [index-management] idxmgmt/std.go:298 Loaded in
dex template.
2020-10-13T18:00:10.528-0300 INFO [index-management] idxmgmt/std.go:309 Write ali
as successfully generated.
2020-10-13T18:00:10.530-0300 INFO [publisher_pipeline_output] pipeline/output.go:151 C
onnection to backoff(elasticsearch(http://localhost:9200)) established
```

4. Verificar a quantidade de documentos do índice criado pelo Metricbeat e visualizar seus 10 primeiros documentos

Recebeu 201 documentos



The screenshot shows the Kibana Dev Tools interface. At the top, there's a navigation bar with icons for menu, Kibana logo, a 'D' icon, and 'Dev Tools'. Below this is a tab bar with 'Console', 'Search Profiler', 'Grok Debugger', 'Painless Lab', and a 'BETA' button. The 'Console' tab is active, showing a history of commands and their results. The first command is a GET request to the metricbeat index, which returned a JSON response indicating 201 documents. The second command is a GET request to the filebeat index, which returned a JSON response indicating 1 document. The third command is a GET request to the bolsa index, which returned a JSON response indicating 0 documents. The fourth command is a GET request to the bolsa index, which returned a JSON response indicating 0 documents.




History Settings Help

200 - OK 20 ms

```
1 GET metricbeat-7.9.2-2020.10.13-000001/
2
3 GET filebeat-7.9.2-2020.10.13-000001/_search
4
5 # ----- #
6
7 GET bolsa/_search
8 {
9   "size": 0,
10  "aggs": {
11    "qtd_2anos": {
12      "date_range": {
13        "field": "@timestamp",
14        "ranges": [
15          {
16            "from": "now-2y",
17            "to": "now"
18          }
19        ]
20      }
21    }
22  }
23 }
24
25 GET bolsa/_search
26 {
27   "size": 0,
28   "aggs": {
29     "doc_anos": {
30       "date_histogram": {
```

```
1 {
2   "count" : 201,
3   "_shards" : {
4     "total" : 1,
5     "successful" : 1,
6     "skipped" : 0,
7     "failed" : 0
8   }
9 }
10
```

Serach mostrando os 10 primeiros documentos

 Dev Tools

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

History Settings Help

200 - OK 20 ms

```
1 GET metricbeat-7.9.2-2020.10.13-000001/_search
2
3 GET filebeat-7.9.2-2020.10.13-000001/_search
4
5 # ----- #
6
7 GET bolsa/_search
8 {
9   "size": 0,
10  "aggs": {
11    "qtd_2anos": {
12      "date_range": {
13        "field": "@timestamp",
14        "ranges": [
15          {
16            "from": "now-2y",
17            "to": "now"
18          }
19        ]
20      }
21    }
22  }
23 }
24
25 GET bolsa/_search
26 {
27   "size": 0,
28   "aggs": {
29     "doc_anos": {
30       "date_histogram": {
```

```
1 {
2   "took" : 2,
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" : 222,
13      "relation" : "eq"
14    },
15    "max_score" : 1.0,
16    "hits" : [
17      {
18        "_index" : "metricbeat-7.9.2-2020.10.13-000001",
19        "_type" : "_doc",
20        "_id" : "F7zDI3UB8SR3RpBfaZ0l",
21        "_score" : 1.0,
22        "_source" : {
23          "@timestamp" : "2020-10-13T21:00:05.503Z"
24        },
25        "event" : {
26          "dataset" : "system.cpu",
27          "module" : "system",
28          "duration" : 91200
29        }
30      }
31    ]
32  }
33 }
```


5. Monitorar o site <https://www.elastic.co/pt/> (Links para um site externo.) com uso do Heartbeat

Baixando o Heartbeat e descompactando

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ curl -L -O https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.9.2-linux-x86_64.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 23.6M  100 23.6M    0     0 10.1M      0  0:00:02  0:00:02 --:--:-- 10.1M
semantix@NTBSTX7158:~/treinamentos/elastic
$ tar xzvf heartbeat-7.9.2-linux-x86_64.tar.gz
heartbeat-7.9.2-linux-x86_64/LICENSE.txt
heartbeat-7.9.2-linux-x86_64/README.md
heartbeat-7.9.2-linux-x86_64/heartbeat.yml
heartbeat-7.9.2-linux-x86_64/NOTICE.txt
heartbeat-7.9.2-linux-x86_64/.build_hash.txt
heartbeat-7.9.2-linux-x86_64/kibana/
heartbeat-7.9.2-linux-x86_64/heartbeat.reference.yml
heartbeat-7.9.2-linux-x86_64/monitors.d/
heartbeat-7.9.2-linux-x86_64/monitors.d/sample.http.yml.disabled
heartbeat-7.9.2-linux-x86_64/monitors.d/sample.icmp.yml.disabled
heartbeat-7.9.2-linux-x86_64/monitors.d/sample.tcp.yml.disabled
heartbeat-7.9.2-linux-x86_64/heartbeat
heartbeat-7.9.2-linux-x86_64/fields.yml
```

Conteúdo da pasta

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ cd heartbeat-7.9.2-linux-x86_64/
semantix@NTBSTX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
$ ls
LICENSE.txt  README.md  heartbeat  heartbeat.yml  monitors.d
NOTICE.txt   fields.yml  heartbeat.reference.yml  kibana
semantix@NTBSTX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
```

Editando o arquivo

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

Site que será monitorado (<http://elastic.co/pt/>)

```
# Directory + glob pattern to search for configuration files
path: ${path.config}/monitors.d/*.yaml
# If enabled, heartbeat will periodically check the config.monitors path for changes
reload.enabled: false
# How often to check for changes
reload.period: 5s

# Configure monitors inline
heartbeat.monitors:
- type: http
  # ID used to uniquely identify this monitor in elasticsearch even if the config changes
  id: my-monitor
  # Human readable display name for this service in Uptime UI and elsewhere
  name: My Monitor
  # List of urls to query
  urls: ["http://elastic.co/pt/"]
  # Configure task schedule
  schedule: '@every 10s'
  # Total test connection and data exchange timeout
```

Testando a configuração e a saída

```
semantix@NT8STX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
$ ./heartbeat test config
Config OK
semantix@NT8STX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
$ ./heartbeat test output
elasticsearch: http://localhost:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1, 127.0.0.1
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
  version: 7.9.2
```

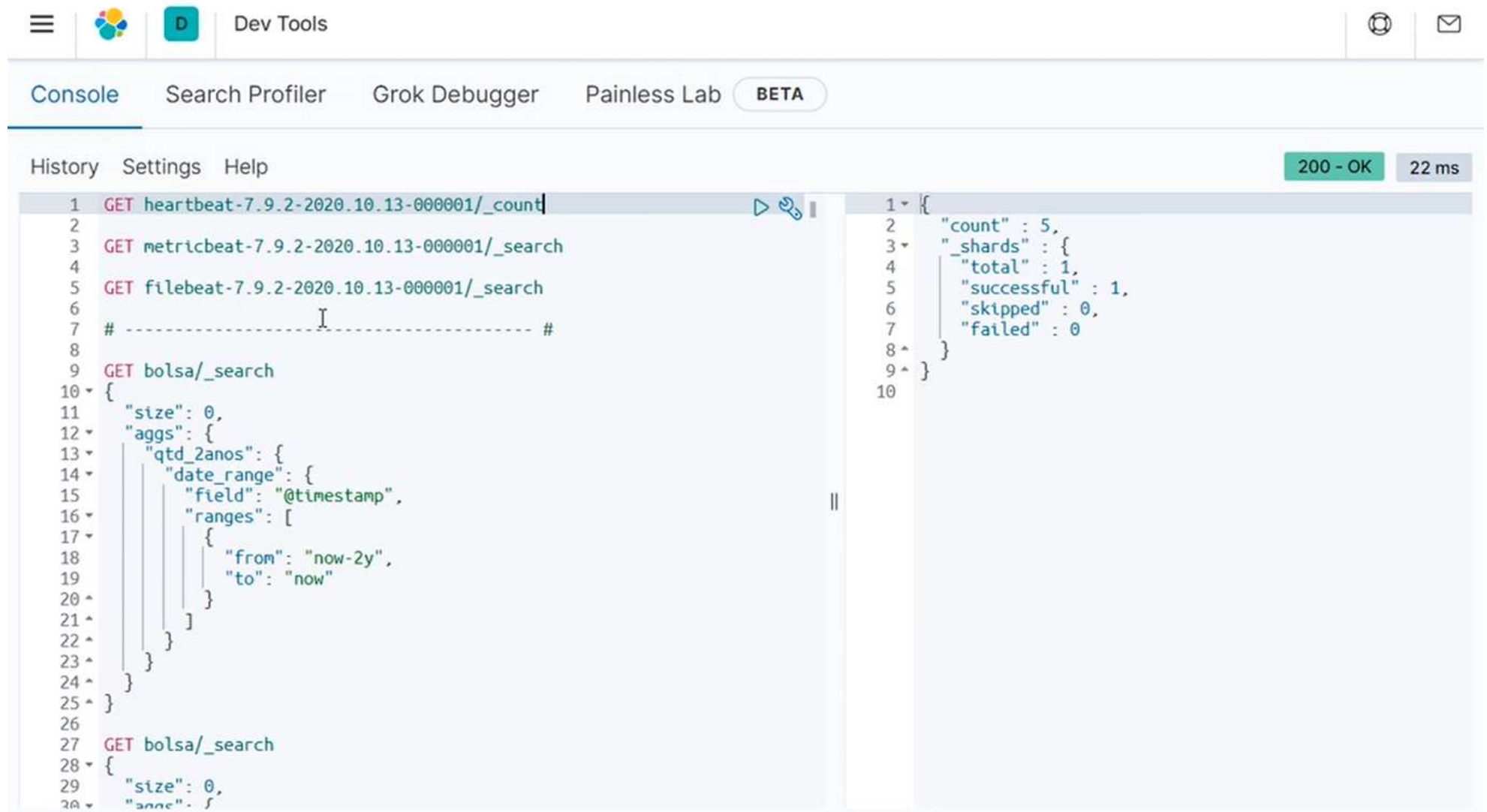
Iniciando o monitoramento

```
semantix@NT8STX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
$ sudo chown root heartbeat.yml
[sudo] password for semantix:
semantix@NT8STX7158:~/treinamentos/elastic/heartbeat-7.9.2-linux-x86_64
$ sudo ./heartbeat -e_
```

```
y successfully loaded.
2020-10-13T18:19:24.662-0300 INFO [index-management] idxmgmt/std.go:407 Set setup
.template.name to '{heartbeat-7.9.2 {now/d}-000001}' as ILM is enabled.
2020-10-13T18:19:24.662-0300 INFO [index-management] idxmgmt/std.go:412 Set setup
.template.pattern to 'heartbeat-7.9.2-*' as ILM is enabled.
2020-10-13T18:19:24.662-0300 INFO [index-management] idxmgmt/std.go:446 Set setti
ngs.index.lifecycle.rollover_alias in template to {heartbeat-7.9.2 {now/d}-000001} as ILM is enab
led.
2020-10-13T18:19:24.662-0300 INFO [index-management] idxmgmt/std.go:450 Set setti
ngs.index.lifecycle.name in template to {heartbeat {"policy":{"phases":{"hot":{"actions":{"rollov
er":{"max_age":"30d","max_size":"50gb"}}}}}}}} as ILM is enabled.
2020-10-13T18:19:24.663-0300 INFO template/load.go:169 Existing template will be overwri
tten, as overwrite is enabled.
2020-10-13T18:19:24.713-0300 INFO template/load.go:189 Try loading template heartbeat-7.
9.2 to Elasticsearch
2020-10-13T18:19:24.828-0300 INFO template/load.go:181 template with name 'heartbeat-7.9
.2' loaded.
2020-10-13T18:19:24.828-0300 INFO [index-management] idxmgmt/std.go:298 Loaded in
dex template.
2020-10-13T18:19:25.282-0300 INFO [index-management] idxmgmt/std.go:309 Write ali
as successfully generated.
2020-10-13T18:19:25.282-0300 INFO [publisher_pipeline_output] pipeline/output.go:151 C
onnection to backoff(elasticsearch(http://localhost:9200)) established
```


6. Verificar a quantidade de documentos do índice criado pelo Heartbeat e visualizar seus 10 primeiros documentos

Chegaram 5 documentos



The screenshot shows the DevTools Console with the 'Console' tab selected. The interface includes a top bar with a hamburger menu, a logo, a 'D' icon, and the text 'Dev Tools'. Below this is a navigation bar with 'Console', 'Search Profiler', 'Grok Debugger', 'Painless Lab', and a 'BETA' button. The main area has tabs for 'History', 'Settings', and 'Help'. On the right side of the main area, there are two status boxes: a green one saying '200 - OK' and a grey one saying '22 ms'.




The console displays a REST client request and its response:

```
1 GET heartbeat-7.9.2-2020.10.13-000001/_count
2
3 GET metricbeat-7.9.2-2020.10.13-000001/_search
4
5 GET filebeat-7.9.2-2020.10.13-000001/_search
6
7 # -----
8
9 GET bolsa/_search
10 {
11   "size": 0,
12   "aggs": {
13     "qtd_2anos": {
14       "date_range": {
15         "field": "@timestamp",
16         "ranges": [
17           {
18             "from": "now-2y",
19             "to": "now"
20           }
21         ]
22       }
23     }
24   }
25 }
26
27 GET bolsa/_search
28 {
29   "size": 0,
30   "aggs": {
```

The response is a JSON object:

```
1 {
2   "count" : 5,
3   "_shards" : {
4     "total" : 1,
5     "successful" : 1,
6     "skipped" : 0,
7     "failed" : 0
8   }
9 }
10
```

Search mostra os dados

 Dev Tools

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

History Settings Help

200 - OK 29 ms

```
1 GET heartbeat-7.9.2-2020.10.13-000001/_search
2
3 GET metricbeat-7.9.2-2020.10.13-000001/_search
4
5 GET filebeat-7.9.2-2020.10.13-000001/_search
6
7 # ----- #
8
9 GET bolsa/_search
10 {
11   "size": 0,
12   "aggs": {
13     "qtd_2anos": {
14       "date_range": {
15         "field": "@timestamp",
16         "ranges": [
17           {
18             "from": "now-2y",
19             "to": "now"
20           }
21         ]
22       }
23     }
24   }
25 }
26
27 GET bolsa/_search
28 {
29   "size": 0,
30   "aggs": {
```

```
58 },
59   "event": {
60     "dataset": "uptime"
61   },
62   "ecs": {
63     "version": "1.5.0"
64   },
65   "url": {
66     "domain": "elastic.co",
67     "port": 80,
68     "path": "/pt/",
69     "full": "http://elastic.co/pt/",
70     "scheme": "http"
71   },
72   "summary": {
73     "up": 1,
74     "down": 0
75   },
76   "tcp": {
77     "rtt": {
78       "connect": {
79         "us": 22940
80       }
81     }
82   },
83   "http": {
84     "response": {
85       "headers": {
86         "Location": "https://www.elastic.co/pt/",
```