

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 "/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
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
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_logstash_1
elastic_kibana_1
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

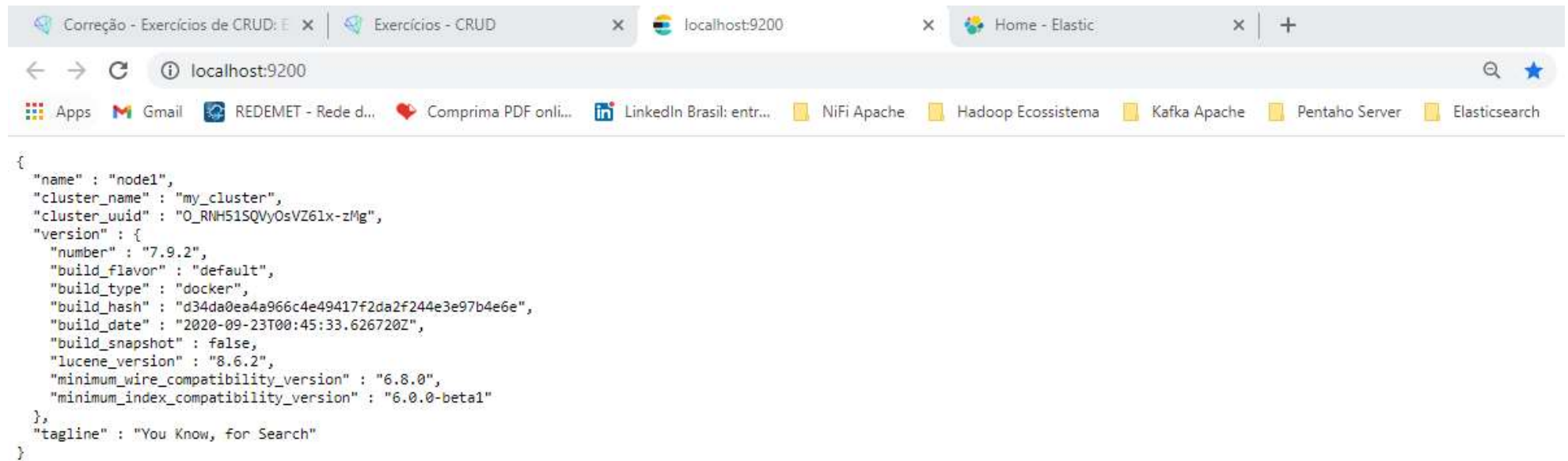
 elastic_elasticsearch_1
docker.elastic.co/elasticsearch/elasticsearch:7.9.2
RUNNING PORT: 9200

```
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 the Kibana web interface in a browser window. The browser's address bar displays `localhost:5601/app/home/`. The page features a left-hand navigation sidebar with a hamburger menu icon, a user profile icon, and a 'Home' button. The sidebar lists several categories: 'Recently viewed' (empty), 'Kibana' (with sub-items: Discover, Dashboard, Canvas, Maps, Machine Learning, Visualize), 'Enterprise Search' (with sub-items: App Search, Workplace Search), and 'Observability' (with sub-items: Overview, Logs). The main content area is titled 'Home' and contains several interactive cards. These include 'Logs' (with an 'Add log data' button), 'Metrics' (with an 'Add metric data' button), and 'Security' (with an 'Add events' button). Below these are three larger cards: 'Add sample data', 'Upload data from log file', and 'Use Elasticsearch data'. At the bottom, there are two more sections: 'Explore Data' (featuring 'App Search') and 'Manage and Administer the Elastic Stack' (featuring 'Console' and 'Rollups').

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

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

Upload data from log file

Use Elasticsearch data

Explore Data

App Search

Manage and Administer the Elastic Stack

Console

Rollups

Exercitando Logstash

Down nos serviços do ElasticSearch

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ docker-compose down
Stopping elastic_kibana_1      ... done
Stopping elastic_elasticsearch_1 ... done
Removing elastic_logstash_1    ... done
Removing elastic_kibana_1      ... done
Removing elastic_elasticsearch_1 ... done
Removing network elastic_elastic
semantix@NTBSTX7158:~/treinamentos/elastic
```

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

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ cd filebeat-7.9.2-linux-x86_64/
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ls
LICENSE.txt  data      filebeat.reference.yml  logs      modules.d
NOTICE.txt   fields.yml filebeat.yml             metricbeat-8.0.0-linux-x86_64.tar.gz
README.md    filebeat  kibana                   module
```

Configurar o filebeat.yml

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

Entrada dos dados

```
- type: log

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

# Paths that should be crawled and fetched. Glob based paths.
paths:
  - /home/semantix/treinamentos/elastic/dataset/paris-925.logs
  # - /var/log/*.log
  #- c:\programdata\elasticsearch\logs\*
```

Saída será logstash

```
# ----- Logstash Output -----
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # list of root certificates for HTTPS server verifications
```

Salvar o arquivo

2. Configurar e executar o logstash com as seguintes configurações

Entrada:

```
beats {
```

```
  port => 5044
```

```
}
```

Saída:

```
elasticsearch {
```

```
  hosts => [ "elasticsearch:9200" ]
```

```
  index => "seu_nome-%{+YYYY.MM.dd}"
```

```
}
```

Configuração do logstash.conf

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ ls
config_vm.sh          filebeat-7.9.2-linux-x86_64.tar.gz
data                  heartbeat-7.9.2-linux-x86_64
dataset               heartbeat-7.9.2-linux-x86_64.tar.gz
docker-compose-windows.yml  metricbeat-7.9.2-linux-x86_64
docker-compose.yml    metricbeat-7.9.2-linux-x86_64.tar.gz
elastic-7.5.1         pipeline
extra_config          settings
filebeat-7.9.2-linux-x86_64
semantix@NTBSTX7158:~/treinamentos/elastic
$ sudo vi pipeline/logstash.conf
```

```
input {
  beats {
    port => 5044
  }
}

output {
  stdout {
    codec => "json"
  }
  elasticsearch {
    hosts => ["elasticsearch:9200"]
    index => "rodrigo_%{+yyyy.MM.dd}"
  }
}
```

Vai gravar os arquivos no elasticsearch sequencialmente com nome e ano

Recriando os serviços do elasticsearch após as alterações

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ docker-compose up -d
Creating network "elastic_elastic" with driver "bridge"
Creating elastic_elasticsearch_1 ... done
Creating elastic_kibana_1         ... done
Creating elastic_logstash_1       ... done
```

3. Verificar a quantidade de documentos do índice criado pelo Logstash e visualizar seus 10 primeiros documentos

Inicializando o filebeat

```
semantix@NTBSTX7158:~/treinamentos/elastic
$ cd filebeat-7.9.2-linux-x86_64/
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ls
LICENSE.txt  data          filebeat.reference.yml  logs          modules.d
NOTICE.txt   fields.yml    filebeat.yml            metricbeat-8.0.0-linux-x86_64.tar.gz
README.md    filebeat     kibana                  module
```

Testando a configuração e a saída

```
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo ./filebeat test config
[sudo] password for semantix:
Config OK
semantix@NTBSTX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo ./filebeat test output
logstash: localhost:5044...
  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
```

Apontando a saída para o logstash porta 5044.

<http://localhost:9600>

o status deve estar green

```
{ "host": "554f7f4e3311", "version": "7.9.2", "http_address": "0.0.0.0:9600", "id": "80ef0758-2c3d-4bfe-8dd7-9002fcc3ec8b", "name": "554f7f4e3311", "ephemeral_id": "a7e1f175-5eec-41e1-aefd-0e6c4d2ea6bf", "status": "green", "snapshot": false, "pipeline": { "workers": 8, "batch_size": 125, "batch_delay": 50 }, "build_date": "2020-09-23T03:12:32Z", "build_sha": "0d3d0617adaa8c0c770469c9c32e18514b5d8f15", "build_snapshot": false }
```

A pastas logs e data são úteis quando o serviço cai por algum motivo.

Tendo os dados nessas pastas o serviço saberá onde parou

```
semantix@NTB8TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ ls
LICENSE.txt  data      filebeat.reference.yml  logs
NOTICE.txt  fields.yml filebeat.yml             metricbeat-8.0.0-linux-x86_64.tar.gz
README.md   filebeat  kibana                  module
```

Removendo as pastas por elas já continham os dados do arquivo paris-925.logs do exercício anterior.

```
semantix@NTB8TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo rm -rf data/
semantix@NTB8TX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64
$ sudo rm -rf logs/
```

Iniciando o envio do arquivo paris-925.logs

```
semantix@NT8STX7158:~/treinamentos/elastic/filebeat-7.9.2-linux-x86_64  
$ sudo ./filebeat -e_
```

```
2020-10-15T17:40:13.031-0300 INFO [registrar] registrar/registrar.go:109 States Loaded from registrar: 0  
2020-10-15T17:40:13.031-0300 INFO [crawler] beater/crawler.go:71 Loading Inputs: 1  
2020-10-15T17:40:13.031-0300 INFO log/input.go:157 Configured paths: [/home/semantix/treinamentos/elastic/dataset/paris-925.logs]  
2020-10-15T17:40:13.031-0300 INFO [crawler] beater/crawler.go:141 Starting input (ID: 3976361801678345579)  
2020-10-15T17:40:13.032-0300 INFO [crawler] beater/crawler.go:108 Loading and starting Inputs completed. Enabled inputs: 1  
2020-10-15T17:40:13.032-0300 INFO cfgfile/reload.go:164 Config reloader started  
2020-10-15T17:40:13.032-0300 INFO log/harvester.go:299 Harvester started for file: /home/semantix/treinamentos/elastic/dataset/paris-925.logs  
2020-10-15T17:40:13.032-0300 INFO cfgfile/reload.go:224 Loading of config files completed  
.  
2020-10-15T17:40:16.009-0300 INFO [add_cloud_metadata] add_cloud_metadata/add_cloud_metadata.go:89 add_cloud_metadata: hosting provider type not detected.  
2020-10-15T17:40:16.045-0300 INFO [publisher_pipeline_output] pipeline/output.go:143 Connecting to backoff(async(tcp://localhost:5044))  
2020-10-15T17:40:16.045-0300 INFO [publisher] pipeline/retry.go:219 retryer: send unwait signal to consumer  
2020-10-15T17:40:16.045-0300 INFO [publisher] pipeline/retry.go:223 done  
2020-10-15T17:40:16.045-0300 INFO [publisher_pipeline_output] pipeline/output.go:151 Connection to backoff(async(tcp://localhost:5044)) established
```

Ficar atento se aparece “open_files”:1.

```
2020-10-15T17:40:16.045-0300 INFO [publisher] pipeline/retry.go:219 retryer: send  
ait signal to consumer  
2020-10-15T17:40:16.045-0300 INFO [publisher] pipeline/retry.go:223 done  
2020-10-15T17:40:16.045-0300 INFO [publisher_pipeline_output] pipeline/output.go:1  
onnection to backoff(async(tcp://localhost:5044)) established  
2020-10-15T17:40:43.030-0300 INFO [monitoring] log/log.go:145 Non-zero metrics in  
ast 30s {"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 1440, "time": {"ms": 1449  
tal": {"ticks": 11530, "time": {"ms": 11540}, "value": 11530}, "user": {"ticks": 10090, "time": {"ms": 10  
}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 12}, "info": {"ephemeral_id": "f8371372-t  
dd3-bb16-776094405632", "uptime": {"ms": 30073}}, "memstats": {"gc_next": 50266944, "memory_alloc":  
904, "memory_total": 1091596352, "rss": 113721344}, "runtime": {"goroutines": 33}}, "filebeat": {"eve  
{"active": 4117, "added": 106518, "done": 102401}, "harvester": {"files": {"19e10c58-7f84-4c94-9e00-  
2edd765": {"last_event_published_time": "2020-10-15T17:40:42.940Z", "last_event_timestamp": "202  
15T17:40:42.940Z", "name": "/home/semantix/treinamentos/elastic/dataset/paris-925.logs", "read  
t": 24628322, "size": 67644119, "start_time": "2020-10-15T17:40:13.032Z"}, "open_files": 1, "runnin  
"started": 1}}, "libbeat": {"config": {"module": {"running": 0}, "reloads": 1, "scans": 1}, "output": {"  
s": {"acked": 102400, "active": 4096, "batches": 52, "total": 106496}, "read": {"bytes": 300}, "type": "l  
sh", "write": {"bytes": 9608558}}, "pipeline": {"clients": 1, "events": {"active": 4117, "filtered": 1,  
ished": 106516, "retry": 2048, "total": 106518}, "queue": {"acked": 102400}}, "registrar": {"states":  
rent": 1, "update": 102401}, "writes": {"success": 51, "total": 51}}, "system": {"cpu": {"cores": 8}, "ld  
"1": 4.95, "15": 0.46, "5": 1.19, "norm": {"1": 0.6188, "15": 0.0575, "5": 0.1488}}}}}
```


Vendo todos os índices



Dev Tools



Console

Search Profiler

Grok Debugger

Painless Lab

BETA

History Settings Help

200 - OK

35 ms

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

```
1 green open .kibana-event-log-7.9.2-000001
   DaaVr7GYSvSnRolmFWifkQ 1 0 15 0 33kb
   33kb
2 green open .apm-agent-configuration
   dAoyJer0Tdazqd1oF8Ni-g 1 0 0 0 208b
   208b
3 yellow open populacao
   Yx8AjG78TheE4sfL1KUeYQ 1 1 319 0 47.4kb 47
   .4kb
4 yellow open metricbeat-7.9.2-2020.10.13-000001
   R5RclsviRKOpSgwkS7aLZA 1 1 750 0 836.5kb 836
   .5kb
5 green open .kibana_1
   GKYWqFgoTt-fdaaWkOLOHA 1 0 76 27 10.4mb 10
   .4mb
6 yellow open concessionaria2
   WA7Km5vKS8m8lxTcMSa07g 1 1 16 0 5.2kb 5
   .2kb
7 yellow open cliente
   1YAASDR0SHi4sEgaw3ZVdg 1 1 3 0 9.6kb 9
   .6kb
8 yellow open filebeat-7.9.2-2020.10.13-000001
   uolS0o1MQfelWbfVQiA10w 1 1 300000 0 76.2mb 76
   2mb
```

D

Dev Tools

Pressione Esc para sair do modo tela cheia

Console

Search Profiler

Grok Debugger

Painless Lab

BETA

History

Settings

Help

200 - OK

24 ms

1	GET	health status index	docs.deleted	store.size	pri.store.size	uuid	pri	rep	docs.count	
2	_cat/indices?v	green	open	.kibana-event-log-7.9.2-000001	33kb	33kb	DaaVr7GYSvSnR0lmFWifkQ	1	0	15
3	#	green	open	.apm-agent-configuration	208b	208b	dAoyJer0Tdazqd1oF8Ni-g	1	0	0
4	----	yellow	open	metricbeat-7.9.2-2020.10.13-000001	836.5kb	836.5kb	R5RclsviRK0pSgwkS7aLZA	1	1	750
5	----	yellow	open	populacao	47.4kb	47.4kb	Yx8AjG78TheE4sfL1KUeYQ	1	1	319
6	----	green	open	.kibana_1	10.4mb	10.4mb	GKYWqFgoTt-fdaaWkOLOHA	1	0	76
7	----	yellow	open	concessionaria2	5.2kb	5.2kb	WA7Km5vKS8m8lxTcMSa07g	1	1	16
8	----	yellow	open	cliente	9.6kb	9.6kb	1YAASDR0SHi4sEgaw3ZVdg	1	1	3
9	----	green	open	produto	5.7kb	5.7kb	f7RRtCiMQm2uXDLd3NIGwA	1	0	4
10	GET	green	open	.apm-custom-link	208b	208b	xFrQo6FURz0tRf8CXwAx4w	1	0	0
11	hear	green	open	produto1	5kb	5kb	AWFFrDYERLiRB5j87fFaXA	1	0	4
12	t-7	yellow	open	bolsa	100 26h	100 26h	gh9yWSYyRJih27X4IoLi6Q	1	1	1111

O indice rodrigo tem 120897 documentos



Search Profiler




Painless Lab

200 - OK

History Settings Help

Line	Color	Status	File Name	Size	Path	Count	Offset	Checksum
1	green	open	produto	9.6kb	f7RRtCiMQm2uXDLd3NIGwA	1	0	4
2	green	open	.apm-custom-link	5.7kb	xFrQo6FURz0tRf8CXwAx4w	1	0	0
3	green	open	produto1	208b	AWFFrDYERLiRB5j87fFaXA	1	0	4
4	yellow	open	bolsa	5kb	gh9yWSYyRJih27X4IoLi6Q	1	1	1111
5	yellow	open	filebeat-7.9.2-2020.10.13-000001	190.2kb	uolS0o1MQfelWbfVQiA10w	1	1	300000
6	yellow	open	contador	76.2mb	8ys77PDUTFSGuf67sjpqXQ	1	1	30
7	yellow	open	produto2	14.1kb	YfikZBywRVW-So9hdXFULA	1	1	4
8	green	open	.kibana_task_manager_1	5.7kb	dC79hVu7Rz-R8otb-PrjUg	1	0	6
9	yellow	open	heartbeat-7.9.2-2020.10.13-000001	176.1kb	fIvwSaqqRGaH0J0oToZ8Bw	1	1	74
10	green	open	produto4	59.8kb	euyMLow3RIudmseeeye7cAw	1	0	4
11	yellow	open	rodrigo-2020.10.15	5.7kb	fbYG7oUkT_0axd9s7PTc_g	1	1	120897
12				151.4mb				

Total de documentos criados

 Dev Tools

Console Search Profiler Grok Debugger Painless Lab BETA






History Settings Help

1 GET rodrigo-2020.10.15/_count
2
3 GET _cat/indices?v
4
5
6
7 # -----
8 ---- #
9 GET heartbeat-7.9.2-2020.10.13-000001/_search
10
11 GET metricbeat-7.9.2-2020.10.13-000001/_search
12
13 GET filebeat-7.9.2-2020.10.13-000001/_search
14
15 # -----
16 ---- #
17 GET bolsa/_search
18 {
19 "size": 0

1 {
2 "count" : 300000,
3 "_shards" : {
4 "total" : 1,
5 "successful" : 1,
6 "skipped" : 0,
7 "failed" : 0
8 }
9 }
10 I

200 - OK 1004 ms

Search mostra os 10 primeiros documentos

Dev Tools

Console Search Profiler Grok Debugger Painless Lab BETA

History Settings Help

```
1 GET rodrigo-2020.10.15/_search
2
3 GET _cat/indices?v
4
5
6
7 # -----
8 ---- #
9 GET heartbeat-7.9.2-2020.10.13-000001/_search
10
11 GET metricbeat-7.9.2-2020.10.13-000001/_search
12
13 GET filebeat-7.9.2-2020.10.13-000001/_search
14
15 # -----
16 ---- #
17 GET bolsa/_search
18 {
19   "size": 10
```

```
22 _source : {
23   "ecs" : {
24     "version" : "1.5.0"
25   },
26   "@version" : "1",
27   "container" : {
28     "id" : "dataset"
29   },
30   "log" : {
31     "file" : {
32       "path" : "/home/semantix/treinamentos/elastic/dataset/paris-925.logs"
33     },
34     "offset" : 7305194
35   },
36   "agent" : {
37     "id" : "c808b565-395a-4af9-a10d-225151994b27",
38     "type" : "filebeat",
39     "version" : "7.9.2",
40     "name" : "NTBSTX7158",
41     "hostname" : "NTBSTX7158",
42     "ephemeral_id" : "f8371372-f620-4dd3-bb16-776094405632"
43   },
```

200 - OK20 ms



Dev Tools



Console

Search Profiler

Grok Debugger

Painless Lab

BETA

History Settings Help

200 - OK

20 ms

```
1 GET rodrigo-2020.10.15/_search
2
3 GET _cat/indices?v
4
5
6
7 # -----
8 ---- #
9 GET heartbeat-7.9.2-2020.10.13-000001
10 /_search
11 GET metricbeat-7.9.2-2020.10.13-000001
12 /_search
13 GET filebeat-7.9.2-2020.10.13-000001
14 /_search
15 # -----
16 ---- #
17 GET bolsa/_search
18 {
19   "size": 0
```

```
34   "offset" : 7305194
35 },
36
37   "agent" : {
38     "id" : "c808b565-395a-4af9-a10d-225151994b27",
39     "type" : "filebeat",
40     "version" : "7.9.2",
41     "name" : "NTBSTX7158",
42     "hostname" : "NTBSTX7158",
43     "ephemeral_id" : "f8371372-f620-4dd3-bb16-776094405632"
44   },
45   "message" : "162.243.110.66 - - [30/Aug/2014:08:54:24 +0000] \"GET /?page=16 HTTP/1.1\" 200 31344 \"http://www.semi-complete.com/?page=15\" \"Mozilla/5.0 (compatible; spbot/4.0.7; +http://OpenLinkProfiler.org/bot)\"",
46   "tags" : [
47     "beats_input_codec_plain_applied"
48   ],
49   "input" : {
50     "type" : "log"
51   },
52   "@timestamp" : "2020-10-15T20:40:26.451Z",
53   "host" : {
```