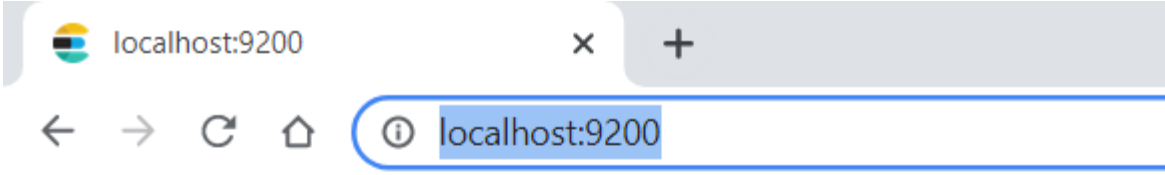




## Vamos praticar!

Aqui estão as etapas para instalar o ELK Stack no ambiente local.

1. Baixe o binário do site oficial e execute o arquivo BAT ou SH, dependendo de seu sistema operacional: <https://www.elastic.co/es/downloads/elasticsearch>
2. Descompacte o arquivo ZIP.
3. Execute o comando dentro da pasta bin **elasticsearch**.
4. Então, no navegador, valide a inicialização correta, chamando a URL <http://localhost:9200>.



```
{
  "name" : "CPX-TJYF5AX53PK",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "JOVI_YsgSzeuWpcNDCgUlw",
  "version" : {
    "number" : "7.17.0",
    "build_flavor" : "default",
    "build_type" : "zip",
    "build_hash" : "bee86328705acaa9a6daede7140defd4d9ec56bd",
    "build_date" : "2022-01-28T08:36:04.875279988Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

5. Baixe o binário do site oficial e execute o BAT ou SH, dependendo de seu sistema operacional: <https://www.elastic.co/downloads/logstash>
6. Descompacte o arquivo ZIP.



7. Execute o comando dentro da pasta bin logstash -f ../config/logstash-sample.conf.

8. Poderemos então ver esta mensagem dentro de nosso console de execução.

```
[2022-02-07T20:20:41,782][INFO ][logstash.outputs.elasticsearch][main] Installing Elasticsearch template {:name=>"logstash"}
[2022-02-07T20:20:43,286][INFO ][logstash.javapipeline][main] Pipeline Java execution initialization time {"seconds"=>1.51}
[2022-02-07T20:20:43,319][INFO ][logstash.inputs.beats][main] Starting input listener {:address=>"0.0.0.0:5044"}
[2022-02-07T20:20:43,343][INFO ][logstash.javapipeline][main] Pipeline started {"pipeline.id"=>"main"}
[2022-02-07T20:20:43,447][INFO ][logstash.agent][main] Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
```

9. Baixe o binário do site oficial e execute o BAT ou SH, dependendo de seu sistema operacional.: <https://www.elastic.co/es/downloads/kibana>

10. Descompacte o arquivo ZIP.

11. Dentro da pasta config, modifique o arquivo kibana.yml indicando a fonte de dados de nosso visualizador:

```
elasticsearch.hosts: ["http://localhost:9200"]
```

12. Execute o comando dentro da pasta bin kibana.

13. Então, no browser, valide a inicialização correta, chamando a URL <http://localhost:5601>



Home - Elastic

×

+

←

→


↻

🏠

📘

localhost:5601/app/home#/

🔗

elastic

🔍


Search Elastic

☰

D


Home

# Welcome home




## Enterprise Search

Create search experiences with a refined set of APIs and tools.



## Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.



## Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.