

02

## Preparando o ambiente

Neste curso, vamos trabalhar com o **Elasticsearch**, o **Kibana** e o **CURL**.

Essas 3 aplicações rodam de forma independente e possuem, cada uma, uma instalação própria.

Ao longo do curso usaremos a **versão 7.4.2 do Elasticsearch e do Kibana**. Para evitar problemas de incompatibilidade, recomendamos que você **use essa mesma versão** em suas atividades. Nos links a seguir, você pode fazer download do:

- [ElasticSearch 7.4.2](http://elastic.co/pt/downloads/past-releases/elasticsearch-7-4-2) (<http://elastic.co/pt/downloads/past-releases/elasticsearch-7-4-2>);
- [Kibana 7.4.2](http://elastic.co/pt/downloads/past-releases/kibana-7-4-2) (<http://elastic.co/pt/downloads/past-releases/kibana-7-4-2>);
- [CURL](http://curl.haxx.se/download.html) (<http://curl.haxx.se/download.html>).

Após o download, extraia esses arquivos para seus respectivos diretórios.

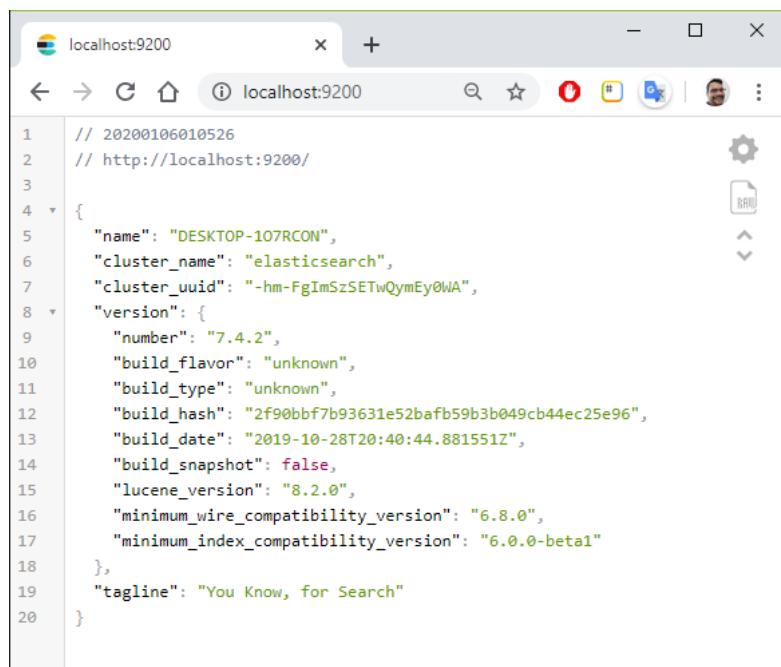
Nos primeiros vídeos do curso, entenderemos como executar esses aplicativos para inicialização e uso do Elasticsearch.

A instalação do Elasticsearch é bem simples. Basta descompactar o arquivo compactado em qualquer pasta que você tenha acesso de escrita.

Para iniciar o processo do Elasticsearch com as configurações padrão (não se preocupe, falaremos delas mais a frente), basta executar o comando `elasticsearch` para sua plataforma que está disponível dentro da pasta “bin”.

**Atenção:** A execução do Elasticsearch depende da instalação prévia da JVM no seu ambiente. Tenha certeza que você tem a versão mais atual da JVM instalada e que o comando `java` está no *path* do seu ambiente. Note também que o Elasticsearch, por padrão, utiliza as portas `9200` e `9300`.

Após rodarmos o arquivo executável de lote, um teste bem rápido que podemos fazer é acessar a URL <http://localhost:9200> (<http://localhost:9200>) no nosso browser favorito. A seguir, o resultado esperado:



```
// 20200106010526
// http://localhost:9200/
{
  "name": "DESKTOP-107RCON",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "-hm-FgImSzSETwQymEy0WA",
  "version": {
    "number": "7.4.2",
    "build_flavor": "unknown",
    "build_type": "unknown",
    "build_hash": "2f90bbf7b93631e52bafb59b3b049cb44ec25e96",
    "build_date": "2019-10-28T20:40:44.881551Z",
    "build_snapshot": false,
    "lucene_version": "8.2.0",
    "minimum_wire_compatibility_version": "6.8.0",
    "minimum_index_compatibility_version": "6.0.0-beta1"
  },
  "tagline": "You Know, for Search"
}
```

Para encerrar o processo, basta utilizar “Ctrl+C”. Note que o valor para o campo *name* varia. Neste momento podemos ignorar esta variação.

## Kibana

Kibana é uma aplicação do "Elastic Stack" que funciona como uma "janela". Ela permite visualizar e analisar os dados no Elasticsearch em tempo real. Com o Kibana, você pode criar visualizações para explorar questões específicas, montar um dashboard para contar uma história visual dos seus dados, compartilhar dashboards como relatórios em PDF e executar comandos na API REST através de um console.

Após a instalação do Kibana, podemos acessar a URL <http://localhost:5601/> (<http://localhost:5601/>).

E teremos o seguinte resultado:

The screenshot shows the Kibana interface running in a web browser. The title bar says "Kibana". The address bar shows the URL "localhost:5601/app/kibana#/home?\_g=0". The main content area is titled "Add Data to Kibana" and contains four sections: "APM", "Logging", "Metrics", and "SIEM". Each section has a brief description and a "Add [solution]" button. On the left side, there is a vertical sidebar with several icons representing different data types and monitoring systems.

Solution	Description	Action Button
APM	APM automatically collects in-depth performance metrics and errors from inside your applications.	Add APM
Logging	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
SIEM	Centralize security events for interactive investigation in ready-to-go visualizations.	Add security events