



Semantix

Elastic Essential I

Aula 1

Quem sou eu?

Eu sou Rodrigo Augusto Rebouças.

Engenheiro de dados da Semantix
Instrutor do Semantix Academy

Você pode me encontrar em:
rodrigo.augusto@semantix.com.br





Semantix

Agenda

Introdução

Consultas

Mapeamento

Agregações

Analísadores

Ingestão de dados

Monitoramento e Dashboards



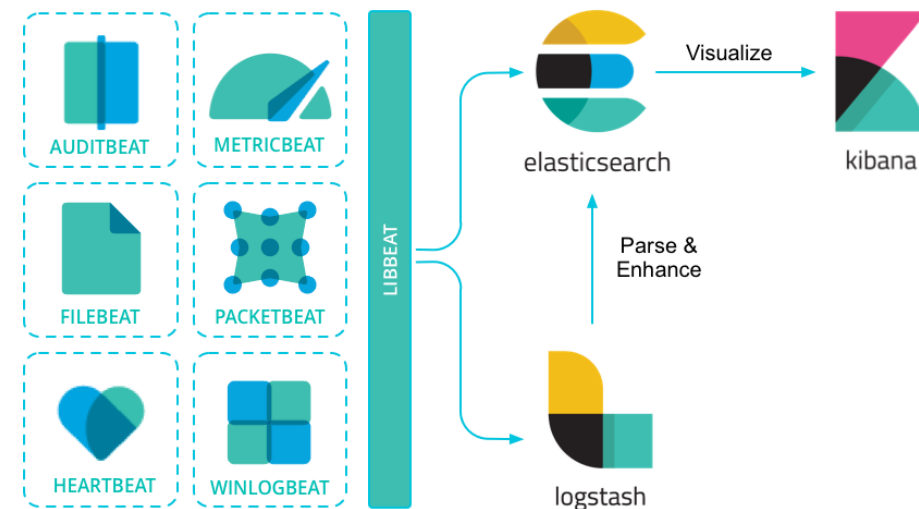
Introdução

Stack Elastic

Arquitetura Elastic

- Problema de busca
- Elasticsearch
 - Engine de search e analytics altamente escalável
 - Banco de dados
- Logstash
 - Transporte entre a origem e destino
- Kibana
 - GUI (Graphical User Interface) da Elastic
 - Visualização dos dados
 - Gerenciamento do Elasticsearch

- Beats
 - Coletores de dados
 - Distribuído
 - Lado do cliente
 - Não servidor



Banco Relacional x Elasticsearch

Banco Relacional	ElasticSearch
Banco de dados	Index
Tabela	Type
Schema	Mapping
Registro (linha)	Documento
Coluna	Atributo

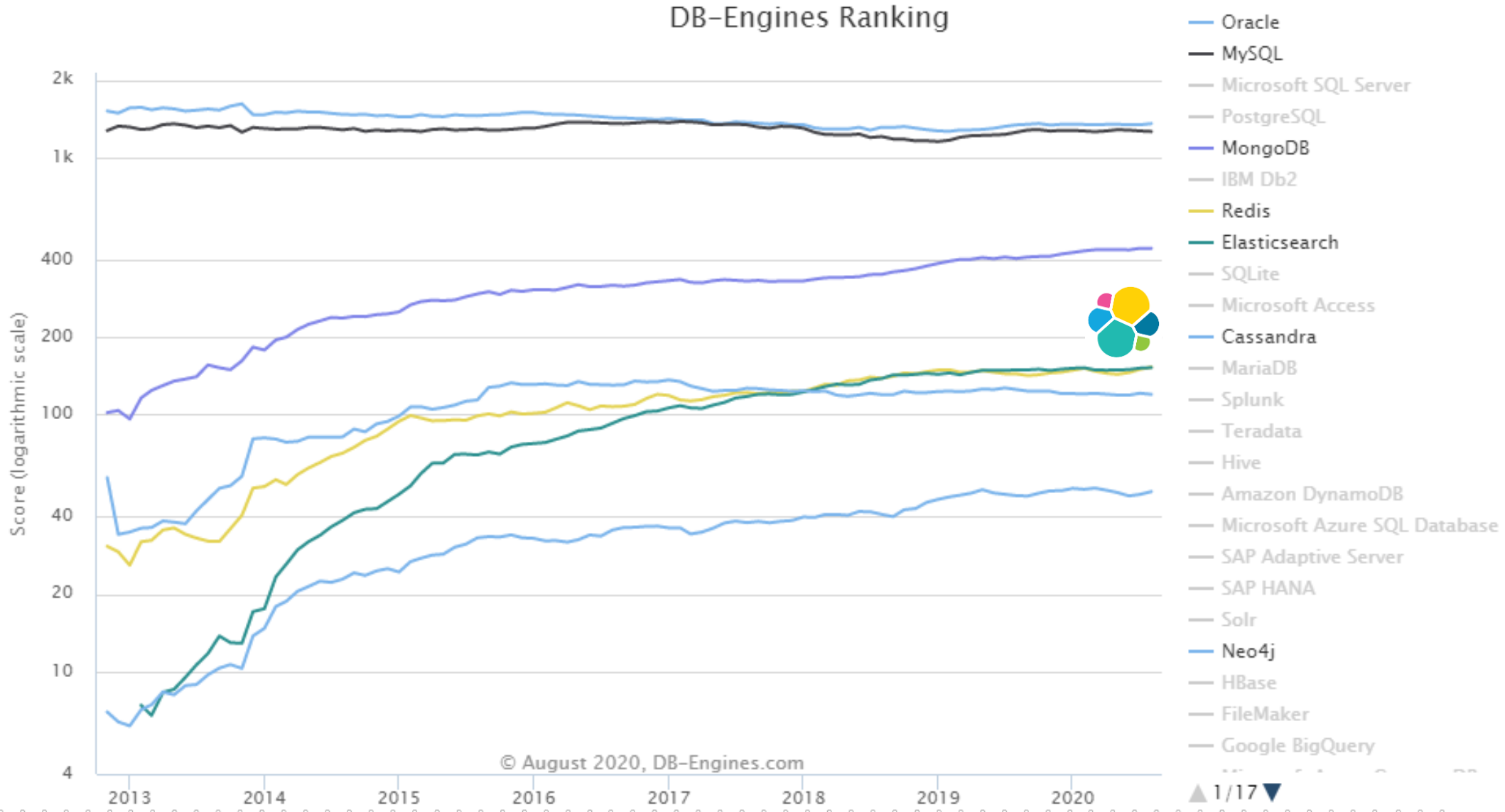
- A partir da versão 7 do Elastic, os documentos são todos do tipo _doc
 - Versão 6
 - Apenas um único tipo de nome
 - Versão 6.8: usar ?include_type_name=false
 - Versão 7 (Atual 7.9.2)
 - include_type_name aviso de depreciado
 - Versão 8
 - include_type_name será removido

Índice

- Shards
 - Índice é dividido por shards
 - Armazenam os dados
- Alias
 - link virtual para um índice real (apelido)
 - Associar um alias a mais de um índice (grupos)
- Analyzer
 - Buscar por Full Text e Valores exatos
- Mapping
 - Definição da estrutura do seu índice

Ranking Banco de dados

○ <https://db-engines.com/>





Instalação



Instalação Elastic Stack

○ Ferramentas

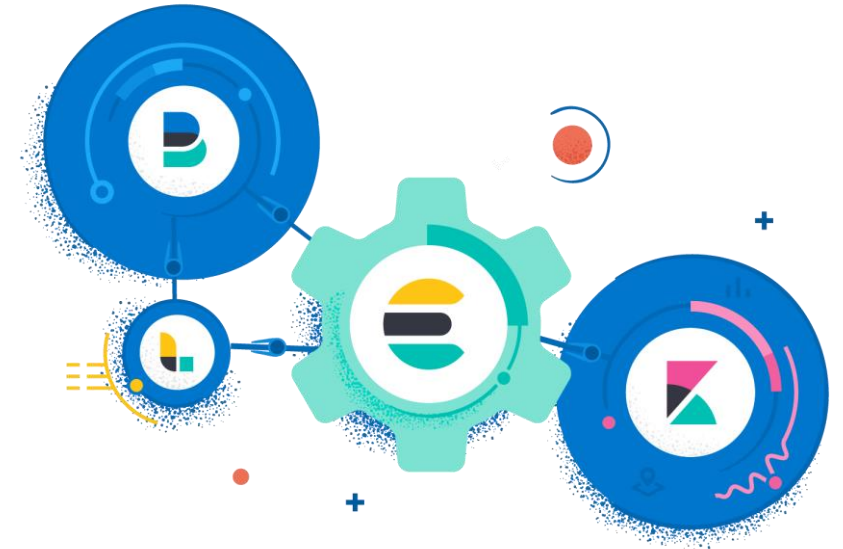
- Elasticsearch
- Kibana
- Beats
- Logstash

○ Link versão atual:

- <https://www.elastic.co/pt/downloads/<ferramenta>>

○ Link para outras versões

- <https://www.elastic.co/pt/downloads/past-releases/<ferramenta>-<versão>>
- Exemplo:
 - <https://www.elastic.co/pt/downloads/past-releases/elasticsearch-6-8-0>



Instalação Elastic Stack

○ Site Oficial

- <https://www.elastic.co/pt/downloads/>

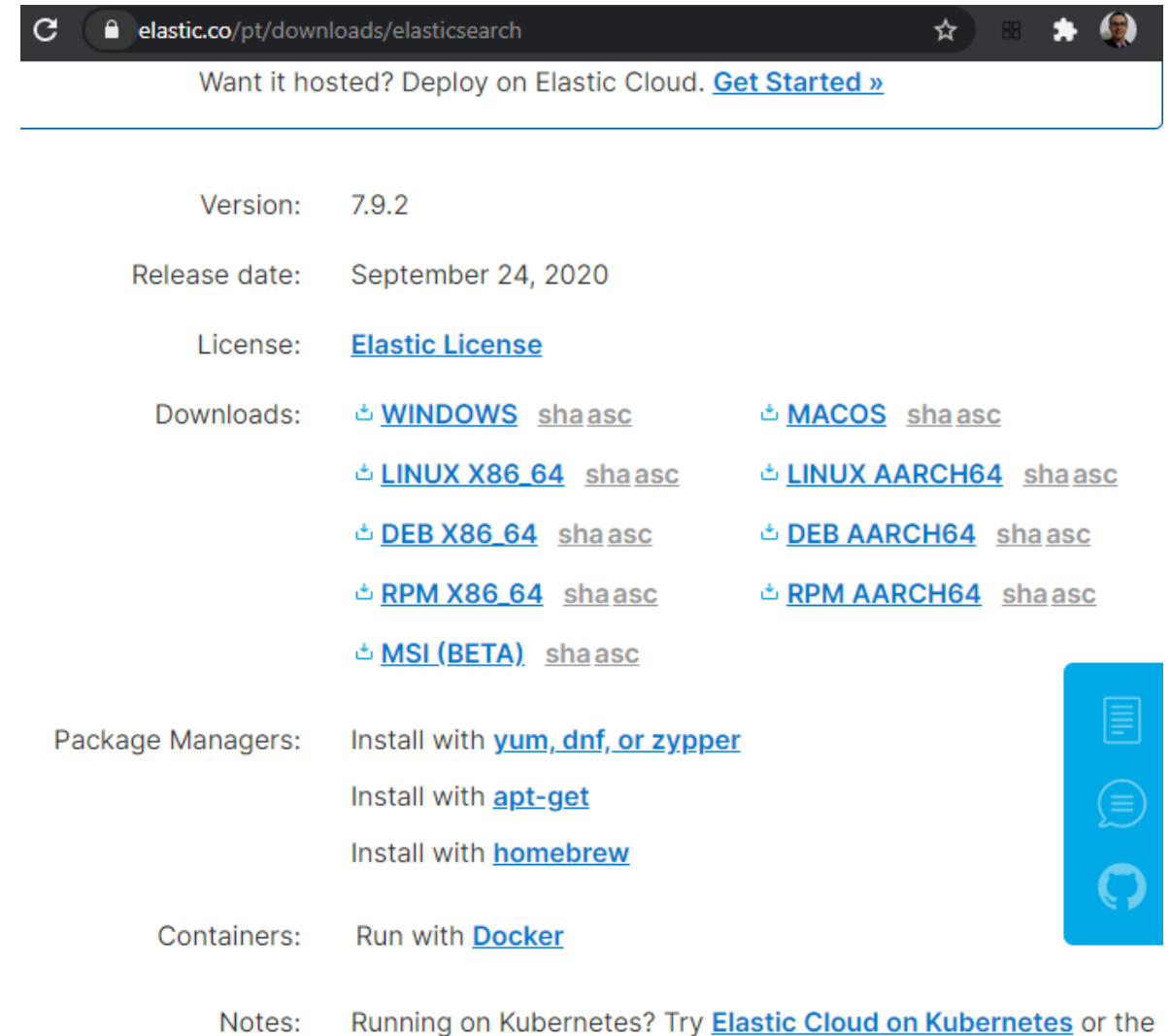
○ Localmente

- Linux
- Windows
- Mac

○ Docker

○ Cloud - Serviço da Elastic

- Desenvolvimento
- Produção
- <https://www.elastic.co/pt/pricing/>



The screenshot shows the Elastic.co download page for Elasticsearch. At the top, there's a navigation bar with the Elastic logo and a user profile icon. Below the navigation bar, a banner asks if the user wants to host it on Elastic Cloud, with a 'Get Started' link. The main content area lists the version (7.9.2), release date (September 24, 2020), and license (Elastic License). Under the 'Downloads' section, there are links for various operating systems and architectures: Windows, MacOS, Linux X86_64, Linux AARCH64, DEB X86_64, DEB AARCH64, RPM X86_64, RPM AARCH64, and MSI (BETA). The 'Package Managers' section provides instructions for installing using yum, dnf, zypper, apt-get, and homebrew. The 'Containers' section mentions running with Docker. Finally, the 'Notes' section suggests trying Elastic Cloud on Kubernetes or the

Version: 7.9.2

Release date: September 24, 2020

License: [Elastic License](#)

Downloads:

- [WINDOWS](#) [sha](#) [asc](#)
- [MACOS](#) [sha](#) [asc](#)
- [LINUX X86_64](#) [sha](#) [asc](#)
- [LINUX AARCH64](#) [sha](#) [asc](#)
- [DEB X86_64](#) [sha](#) [asc](#)
- [DEB AARCH64](#) [sha](#) [asc](#)
- [RPM X86_64](#) [sha](#) [asc](#)
- [RPM AARCH64](#) [sha](#) [asc](#)
- [MSI \(BETA\)](#) [sha](#) [asc](#)

Package Managers:

- Install with [yum, dnf, or zypper](#)
- Install with [apt-get](#)
- Install with [homebrew](#)

Containers: Run with [Docker](#)

Notes: Running on Kubernetes? Try [Elastic Cloud on Kubernetes](#) or the



Instalação - Docker

Preparação Ambiente – Instalação Docker e Docker-compose

○ Instalação

- Docker: <https://docs.docker.com/get-docker/>
- Docker-compose: <https://docs.docker.com/compose/install/>
- SO
 - Windows
 - Docker Desktop (Hyper-V ou Hyper-V com WSL2)
 - Docker Toolbox (VirtualBox)
 - Linux - Seguir o passo a passo (PassosInstalacaoDockerLinux.txt)
 - Mac - Docker Desktop

An abstract graphic on the left side of the slide. It features two overlapping profiles of human heads facing each other. The profiles are filled with a dense pattern of blue concentric lines. Inside the profiles, there are faint, semi-transparent images of data visualizations, including bar charts and line graphs. The background is a light blue gradient.

Preparação do Ambiente

Preparação Ambiente – Cluster Elastic

- Download da imagem: <https://www.docker.elastic.co/>
 - `docker pull docker.elastic.co/elasticsearch/elasticsearch:7.9.2`
 - `docker pull docker.elastic.co/kibana/kibana:7.9.2`
 - `docker pull docker.elastic.co/logstash/logstash:7.9.2`
- Setar o `vm.max_map_count` com no mínimo 262144
- Criar `docker-compose.yml` e os arquivos de configuração para facilitar o gerenciamento do elastic

Preparação Ambiente – Configurar Máquina Elastic

- Setar o `vm.max_map_count` com no mínimo 262144
 - Linux
 - Permanentemente
 - `grep vm.max_map_count /etc/sysctl.conf`
 - `vm.max_map_count=262144`
 - Em execução
 - `sysctl -w vm.max_map_count=262144`
 - Mac
 - `screen ~/Library/Containers/com.docker.docker/Data/vms/0/tty`
 - `sysctl -w vm.max_map_count=262144`
- https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html#_set_vm_max_map_count_to_at_least_262144

Preparação Ambiente – Configurar Máquina Elastic

- Setar o `vm.max_map_count` com no mínimo 262144
 - Windows ou Mac – Docker Desktop
 - `docker-machine ssh`
 - `sudo sysctl -w vm.max_map_count=262144`
 - Windows - Docker Desktop com WSL2
 - `wsl -d docker-desktop`
 - `sysctl -w vm.max_map_count=262144`
- https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html#_set_vm_max_map_count_to_at_least_262144

Preparação Ambiente – Arquivos de configuração

- Baixar o diretório elastic na guia arquivos da plataforma
- Estrutura de arquivos
 - elastic
 - docker-compose.yml
 - settings
 - elasticsearch.yml
 - kibana.yml
 - Logstash.yml
 - Pipeline
 - logstash.conf

Opções Docker Compose

- Iniciar todos os serviços em background (-d)

\$ docker-compose up -d

- Parar os serviços

\$ docker-compose stop

- Iniciar os serviços

\$ docker-compose start

- Término do treinamento

- Matar os serviços

\$ docker-compose down

- Apagar todos os volumes sem uso

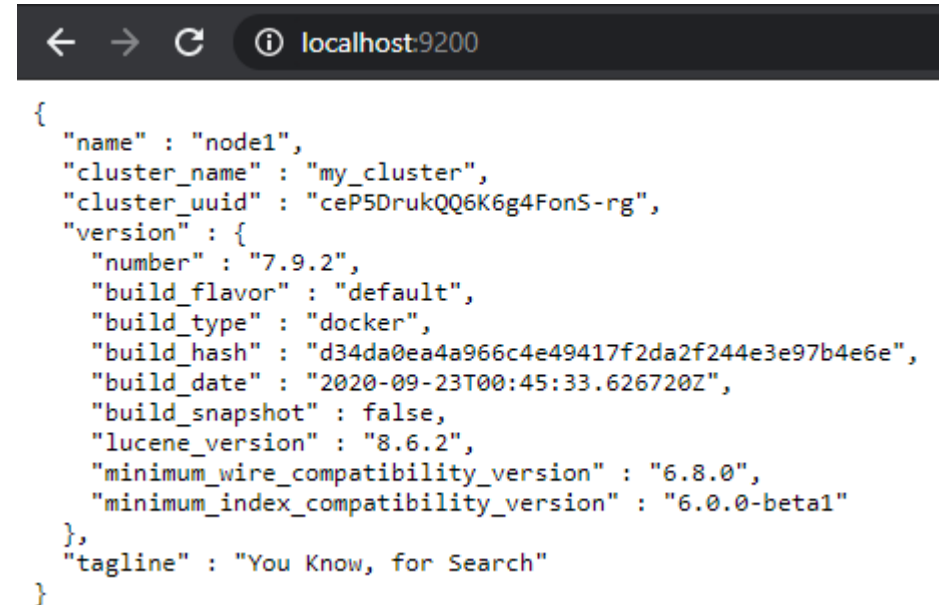
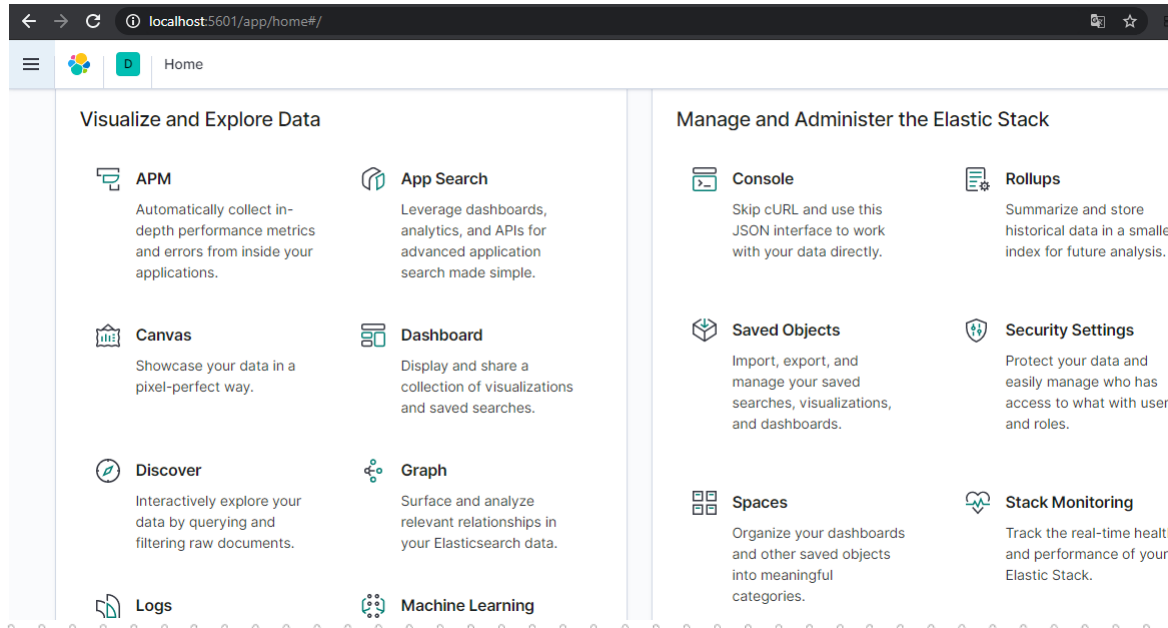
\$ docker volume prune

Acessos Ambiente docker

- Visualizar os container
 - Ativos
 - `$ docker ps`
 - Todos
 - `$ docker ps -a`
- Executar comandos no container
 - `$ docker exec -it <container> <comando>`
- Visualizar os logs
 - `$ docker logs <container>`
 - `$ Docker-compose logs`
- Enviar arquivos
 - `$ docker cp <diretório> <container>:/<diretório>`
- Acesso o container Elasticsearch
 - `docker exec -it elastic_elasticsearch_1 bash`
- Acesso o container Kibana
 - `docker exec -it elastic_kibana_1 bash`
- Acesso o container Logstash
 - `docker exec -it elastic_Logstash_1 bash`

Verificar Funcionamento do cluster Elastic

- Verificar se os nós estão funcionando
 - `$ curl -X GET "localhost:9200/_cat/nodes?v&pretty"`
- Acessar os serviços pela Web
 - Kibana: <http://localhost:5601/>
 - Elasticsearch: <http://localhost:9200/>





Configuração dos Containers

Serviços Docker – Elasticsearch

```
elasticsearch:
  image: docker.elastic.co/elasticsearch/elasticsearch:7.9.2

  ports:
    - "9200:9200"
  volumes:
    - es-data:/usr/share/elasticsearch/data
    - ./settings/elasticsearch.yml:/usr/share/elasticsearch/
config/elasticsearch.yml:ro
    - ./data:/data
  environment:
    - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
  ulimits:
    memlock:
      soft: -1
      hard: -1
  networks:
    - elastic
```

○ \$ cat docker-compose.yml

version: '2.2'

services:

elasticsearch:

...

kibana:

...

logstash:

...

Serviços Docker – Kibana

```
kibana:
  image: docker.elastic.co/kibana/kibana:7.9.2
  volumes:
    - ./settings/kibana.yml:/usr/share/kibana/config/kibana.
    yml:ro
  ports:
    - "5601:5601"
  depends_on:
    - elasticsearch
  networks:
    - elastic
```

○ \$ cat docker-compose.yml

version: '2.2'

services:

elasticsearch:

...

kibana:

...

logstash:

...

Serviços Docker – Logstash

```
logstash:
  image: docker.elastic.co/logstash/logstash:7.9.2
  volumes:
    - ./pipeline/logstash.conf:/usr/share/logstash/pipeline/
logstash.conf:ro
    - ./settings/logstash.yml:/usr/share/logstash/config/log
stash.yml:ro
  ports:
    - "9600:9600"
    - "5044:5044"
  depends_on:
    - elasticsearch
  networks:
    - elastic
```

○ \$ cat docker-compose.yml

version: '2.2'

services:

elasticsearch:

...

kibana:

...

logstash:

...

Exercícios Instalação

1. Baixar a pasta elastic na Guia [Arquivos](#) do treinamento
2. Instalação do docker e docker-compose
3. Executar os seguintes comandos, para baixar as imagens de Elastic:
 - `docker pull docker.elastic.co/elasticsearch/elasticsearch:7.9.2`
 - `docker pull docker.elastic.co/kibana/kibana:7.9.2`
 - `docker pull docker.elastic.co/logstash/logstash:7.9.2`
4. Setar o `vm.max_map_count` com no mínimo 262144
5. Iniciar o cluster Elastic através do docker-compose
6. Listas as imagens em execução
7. Verificar os logs dos containers em execução
8. Verificar as informações do cluster através do browser:
 - <http://localhost:9200/>
9. Acessar o Kibana através do browser:
 - <http://localhost:5601/>



Semantix

Obrigado!

Alguma pergunta?



Você pode me encontrar em:
rodrigo.augusto@semantix.com.br

GET SMARTER