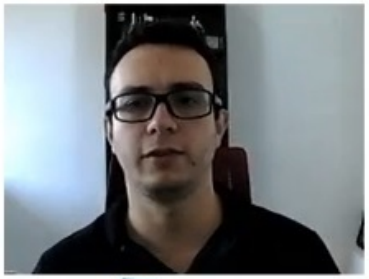
Introdução

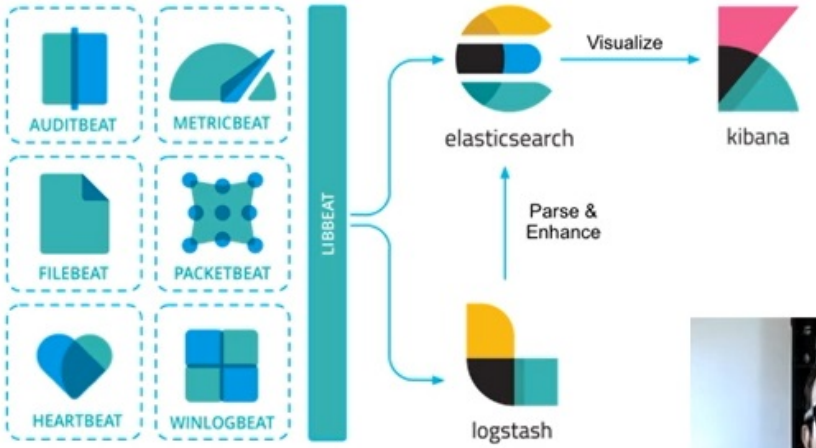
Stack Elastic

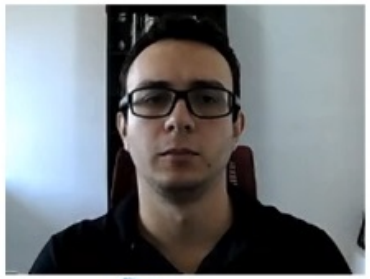


Samantix

Arquitetura Elastic

- Problema de busca
- Elasticsearch
  - Engine de search e analystics 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





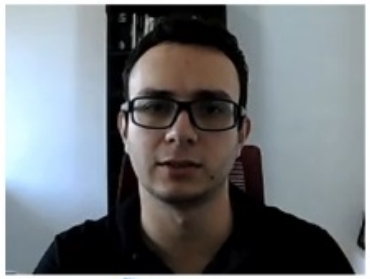
00:16

Samantix

Banco Relacional x ElasticSearch

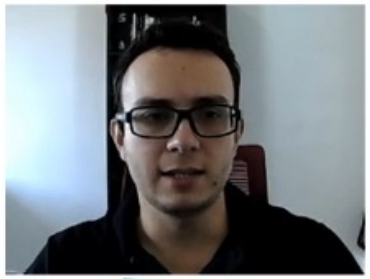
Banco Relacional	ElasticSearch
Banco de dados	Index
~~Tabela~~	~~Type~~
Schema	Mapping
Registro (linha)	Documento
Coluna	Atributo

- 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



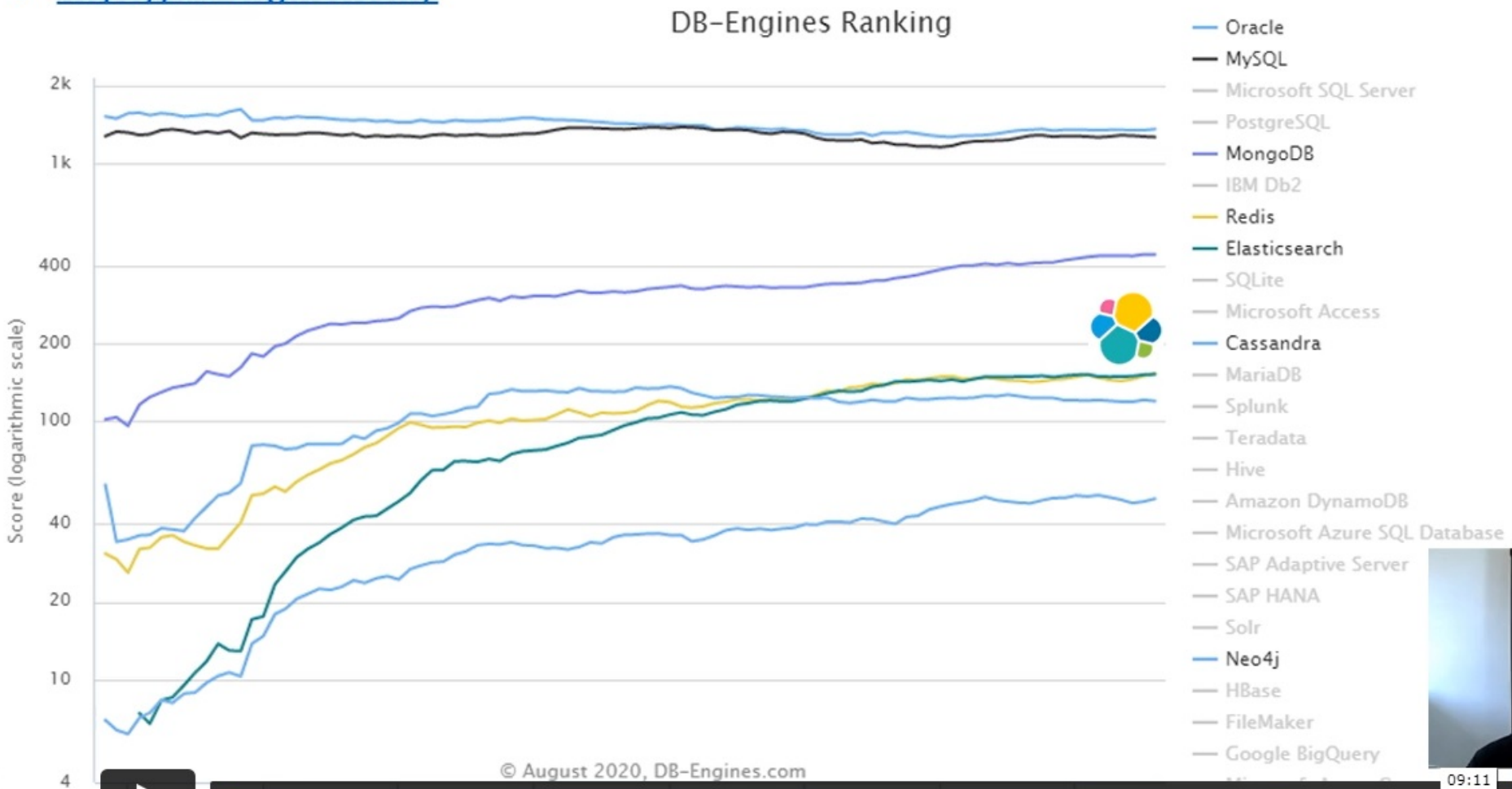
Índice

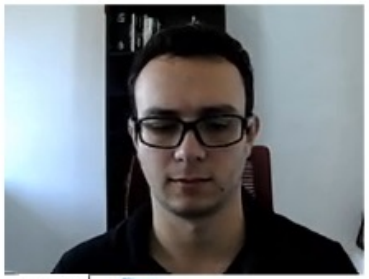
- Shards
  - Índice é dividido por shards
  - Armazenam os dados
- Alias
  - link virtual para um índice real (apelido)
  - Associar um alias a mais de um índice (grupos)
- Analyzer
  - Buscar por Full Text e Valores exatos
- Mapping
  - Definição da estrutura do seu índice



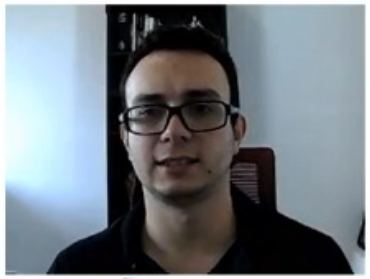
Ranking Banco de dados

- https://db-engines.com/





Instalação

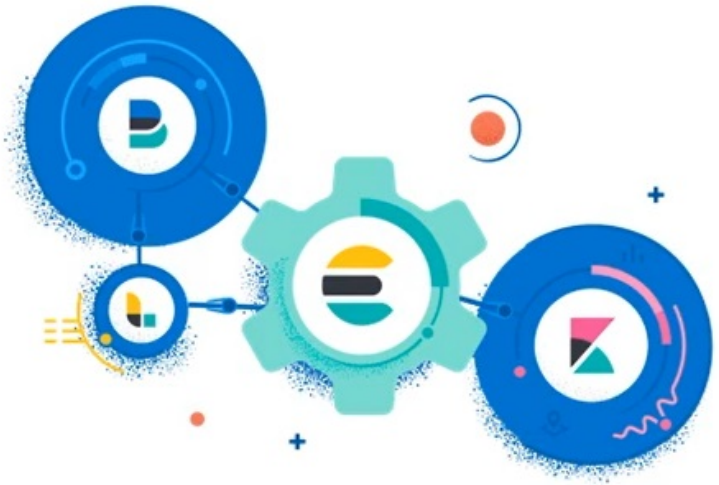


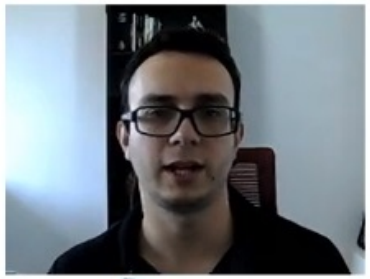
00:01

Samantix

Instalação Elastic Stack

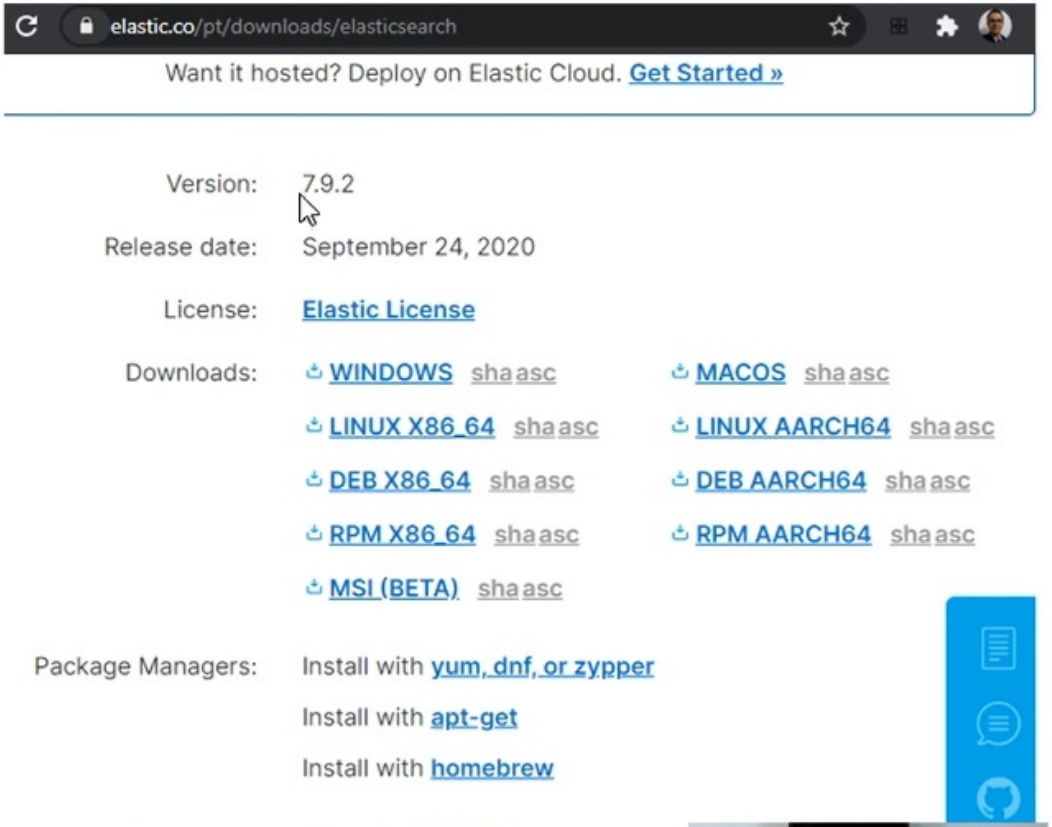
- Ferramentas
  - Elasticsearch
  - Kibana
  - Beats
  - Logstash
- Link versão atual:
  - https://www.elastic.co/pt/downloads/<ferramenta>
- Link para outras versões
  - https://www.elastic.co/pt/downloads/past-releases/<ferramenta>-<versão>
  - Exemplo:
    - https://www.elastic.co/pt/downloads/past-releases/elasticsearch-6-8-0

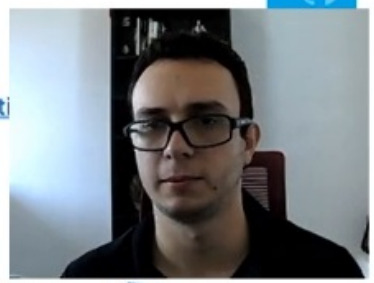




Instalação Elastic Stack

- 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/

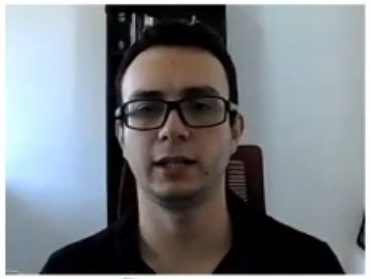




01:05

Samantix

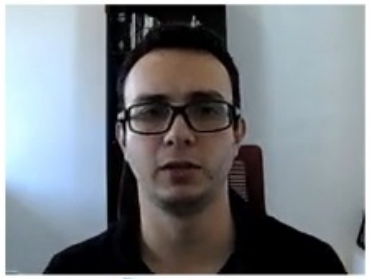
Preparação do Ambiente



Samantix

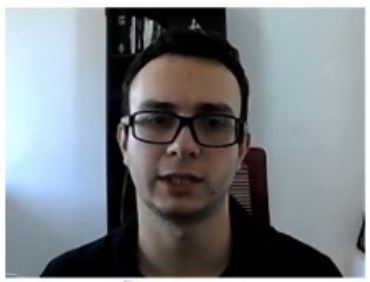
Preparação Ambiente – Cluster Elastic

- 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
    - sysctl -w vm.max_map_count=26214
- https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html#_set_vm_max_map_count_to_at_least_262144

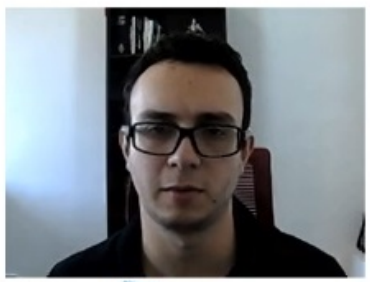


Semantix

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

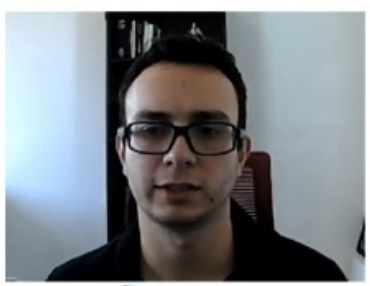
- https://www.elastic.co/guide/en/elasticsearch/reference/current/docker.html#_set_vm_max_map_count_to_at_least_262144



Semantix

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



Semantix

Opções Docker Compose

- Iniciar todos os serviços em background (-d)

  $ docker-compose up –d

- Parar os serviços

  $ docker-compose stop

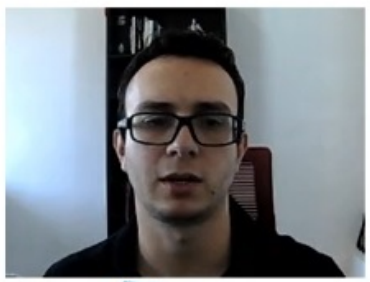
- Iniciar os serviços

  $ docker-compose start

- Término do treinamento
  - Matar os serviços

    $ docker-compose dowm
  - Apagar todos os volumes sem uso

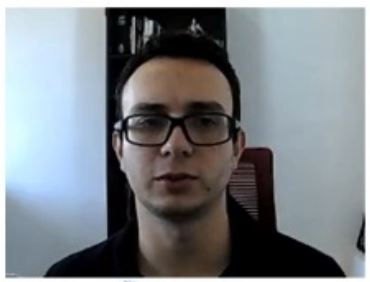
    $ docker volume prune



Semantix

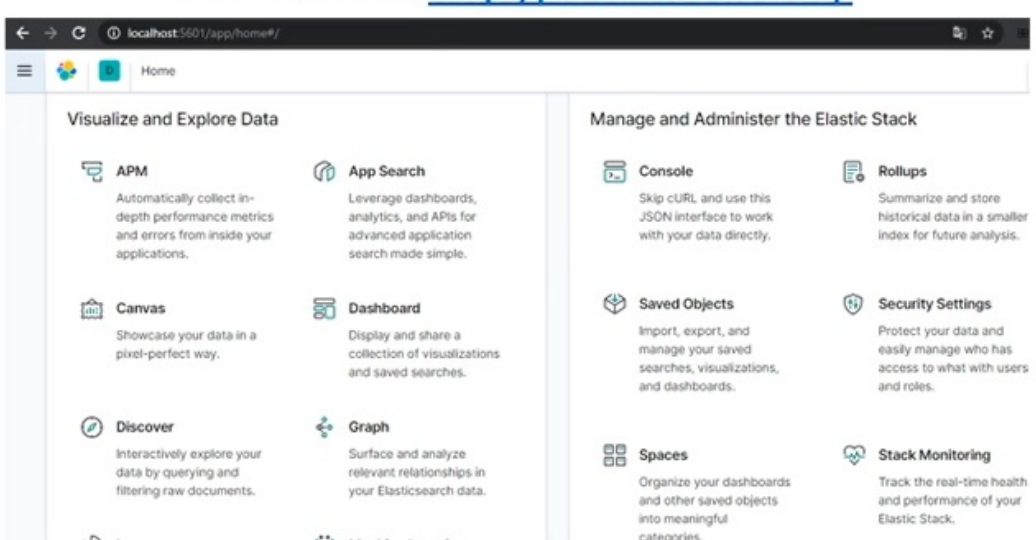
Acessos Ambiente docker

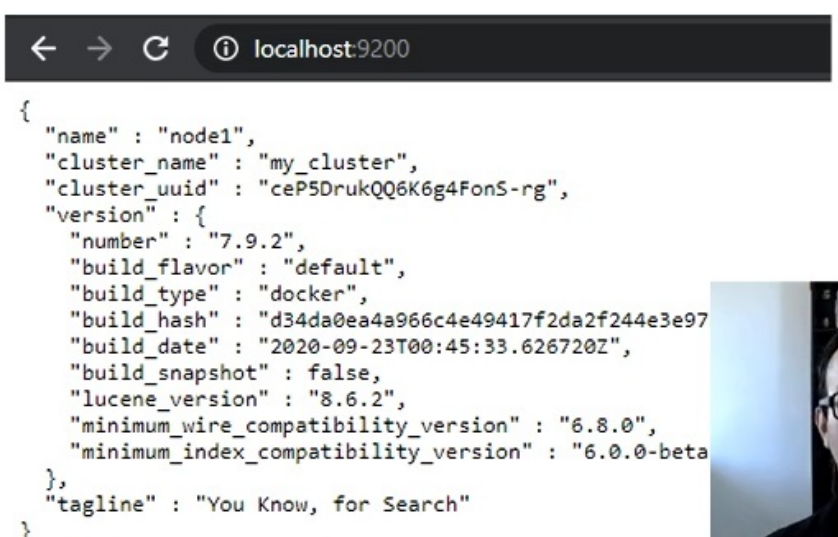
- Visualizar os container
  - Ativos
    - $ docker ps
  - Todos
    - $ docker ps –a
- Executar comandos no container
  - $ docker exec -it <container> <comando>
- Visualizar os logs
  - $ docker logs <container>
  - $ Docker-compose logs
- Enviar arquivos
  - $ docker cp <diretório> <container>:/<diretório>
- 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

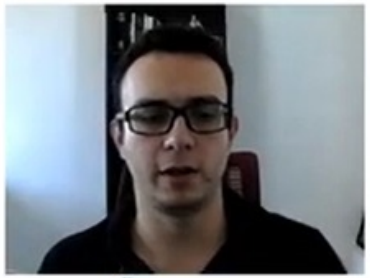
- Verificar se os nós estão funcionando
  - $ curl -X GET "localhost:9200/_cat/nodes?v&pretty“
- Acessar os serviços pela Web
  - Kibana: http://localhost:5601/
  - Elasticsearch: http://localhost:9200/





Semantix

Configuração dos Containers



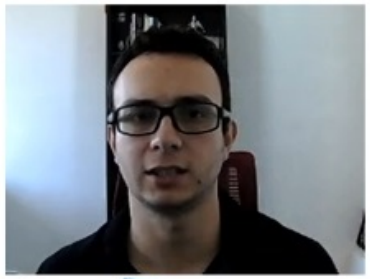
Serviços Docker – Elasticsearch

```
  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:
                ...
```

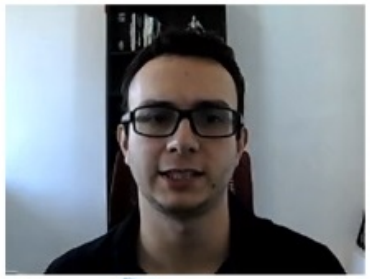


Serviços Docker – Kibana

```
  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:
                ...
```

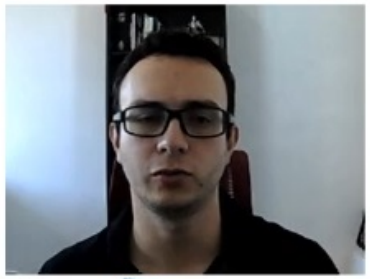


Serviços Docker – Logstash

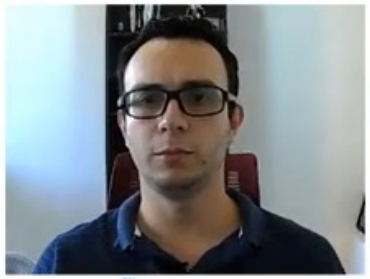
```
  logstash:
    image: docker.elastic.co/logstash/logstash:7.9.2
    volumes:
      - ./pipeline/logstash.conf:/usr/share/logstash/pipeline/
logstash.conf:ro
      - ./settings/logstash.yml:/usr/share/logstash/config/log
stash.yml:ro
    ports:
      - "9600:9600"
      - "5044:5044"
    depends_on: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

- $ cat docker-compose.yml

```
version: '2.2'
services:
        elasticsearch:
                ...
        kibana:
                ...
        logstash:
                ...
```



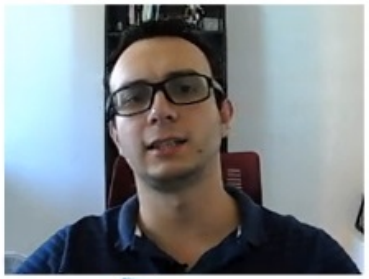
Comunicação com Elasticsearch



API Rest

- Comunicação Protocolo HTTP
  - HEAD
  - GET
  - POST
  - PUT
  - DELETE
- Requisições HTTP para a API de elasticsearch por meio do envio de objetos JSON

- Estrutura de uma requisição HTTP:
  - <ação> endereço_api:porta/índice/<opções>
- Exemplo
  - PUT localhost:9200/cliente/_create

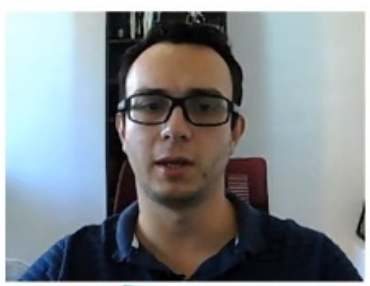


Integração Linguagens

- Clientes Elastic
  - https://www.elastic.co/guide/en/elasticsearch/client/index.html
- Clientes Elastic que a Comunidade Contribuem
  - https://www.elastic.co/guide/en/elasticsearch/client/community/current/index.html

Curl
C#
Go
Java
JavaScript
Perl
PHP
Python
Ruby
SQL

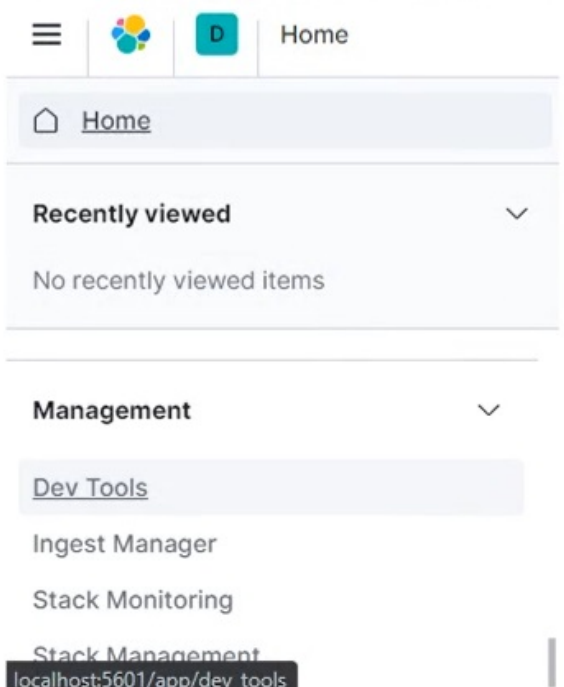
```
curl -H "Content-Type: application/json" -XGET
'http://localhost:9200/social-*/_search' -d '{
  "query": {
    "match": {
      "message": "myProduct"
    }
  },
  "aggregations": {
    "top_10_states": {
      "terms": {
        "field": "state",
        "size": 10
      }
    }
```

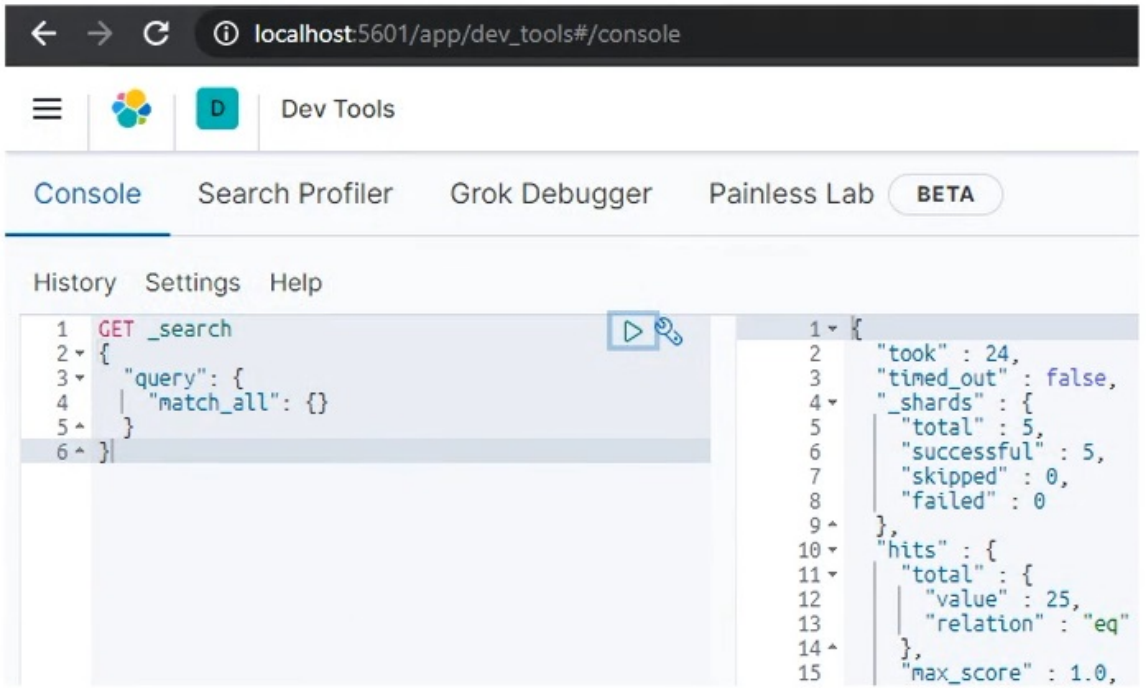


Semantix

Interface Kibana - Comunicação HTTP

- Acessar
  - http://localhost:5601
  - Menu/Management/ Dev Tools
    - http://localhost:5601/app/dev_tools





Semantix

Dev Tools - Elastic

localhost:5601/app/dev_tools#/console

Dev Tools

Console | Search Profiler | Grok Debugger | Painless Lab BETA

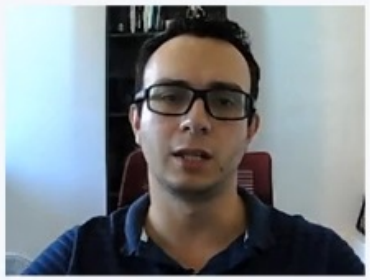
History | Settings | Help

200 - OK 18 ms

```
GET cliente/_doc/1
GET cliente/_count
GET cliente/_search
GET /

GET cliente/_source/1
```

```
{
  "_index" : "cliente",
  "_type" : "_doc",
  "_id" : "1",
  "_version" : 3,
  "_seq_no" : 2,
  "_primary_term" : 1,
  "found" : true,
  "_source" : {
    "nome" : "Lucas",
    "idade" : 20,
    "conhecimento" : "Windows, Office, Hadoop, Elastic"
  }
}
```



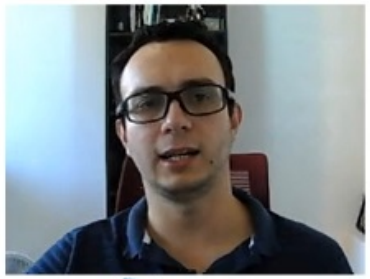
Operações básicas

CRUD

Samantix

CRUD

- **C**reate
- **R**ead
- **U**pdate
- **D**elete



00:10

Samantix

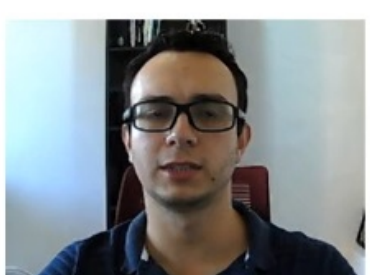
CRUD HEAD

- Retorna apenas o cabeçalho do HTTP
  - Saber se o documento existe
- Exemplo
  - Curl
    - Ferramenta de linha de comando
    - Biblioteca para transferir dados com URLs
    - Exemplo
      - curl –XHEAD –v http://localhost:9200/cliente/_doc/1
  - Kibana
    - Opção: Dev Tools
    - Exemplo
      - HEAD cliente/_doc/1

CRUD PUT

- Criar ou reindexar um documento inteiro (_version)
- Exemplo

```
PUT cliente/_doc/1
{
    "nome" : "Lucas",
    "idade" : 20,
    "conhecimento" : "Windows, Office, Hadoop, Elastic"
}
PUT cliente/_create/1
{
    "nome" : "Lucas",
    "idade" : 20,
    "conhecimento" : "Windows, Office, Hadoop, Elastic, Sqoop"
}
```



CRUD POST

- Criar um documento com _id ou atualizar um documento parcial
- Exemplo

```
POST cliente/_update/1
{
    "doc" : {
        "nome" : "João"
    }
}
POST cliente/_doc
{
    "nome" : "Marcos"
}
```

Semantix

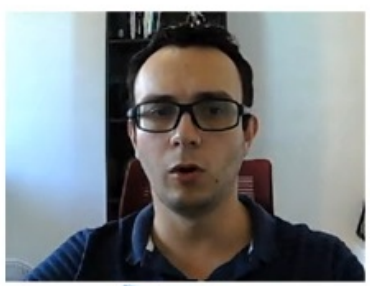
CRUD DELETE

- Deletar um documento
  - Exemplo

    DELETE cliente/_doc/1

- Deletar um índice
  - Exemplo

    DELETE cliente



Semantix

CRUD GET

- Exemplos
  - Informações sobre o nó do elasticseach (http://localhost:9200/)
    - GET /
  - Buscar todos os documentos em um índice
    - GET cliente/_search
  - Buscar um documento em um índice
    - GET cliente/_doc/1
  - Buscar a quantidade de documentos em um índice
    - GET cliente/_count
  - Buscar os dados de um documento em um índie
    - GET cliente/_source/1
      - SQL -> select * from cliente where id=1

Semantix

Beats

Família de beats

Samantix

Beats Família

- Enviam dados de centenas ou milhares de máquinas e sistemas
  - Logstash
  - Elasticsearch
- Download
  - https://www.elastic.co/pt/downloads/beats/

Filebeat

Arquivos de log

Metricbeat

Métricas

Packetbeat

Dados de rede

Winlogbeat

Logs de evento do Windows

Auditbeat

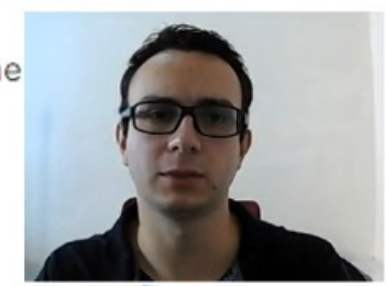
Dados de auditoria

Heartbeat

Monitorame

Functionbeat

Agente de envio sem servidor



Semantix

Logstash

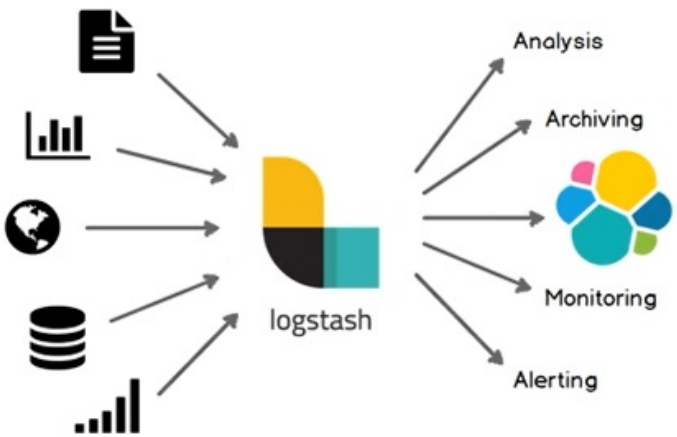
Conceitos

Plugins

00:00

Samantix

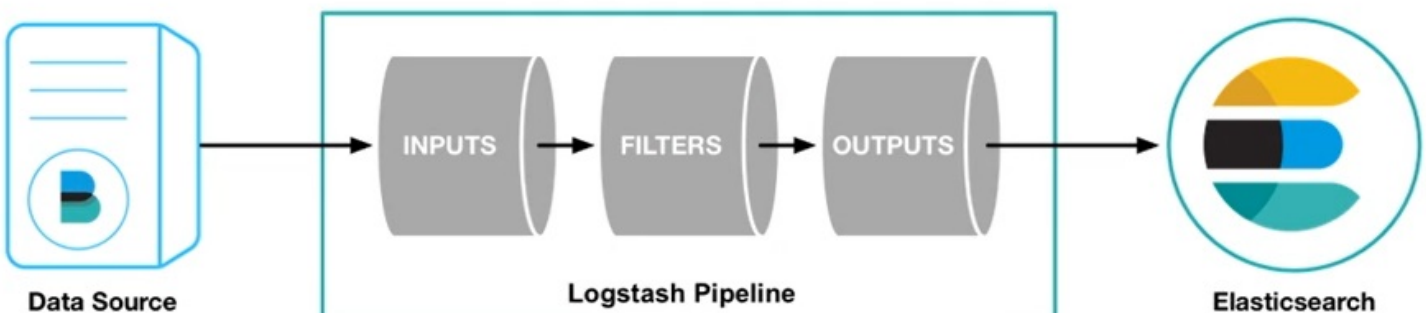
Logstash Conceitos

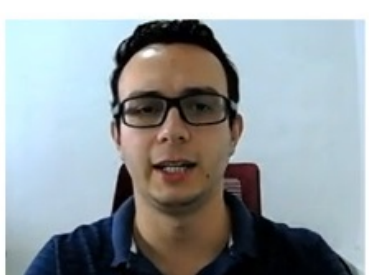


- Alterar o logstash.conf
- Plugin
  - Input
  - Filter
  - Output

- Estrutura do json

```
input{
}
filter{
}
output {
}
```





Semantix

Logstash Instalação e Configuração

- Version Elasticsearch 7.9.2
- Documentação da Elastic:
  https://www.elastic.co/guide/en/logstash/current/getting-started-with-logstash.html
- Estrutura pastas

  docker-compose.yml

  - pipeline/logstash.conf
  - settings
    - elasticsearch.yml
    - kibana.yml
    - logstash.yml

Semantix

Logstash Instalação e Configuração

- Adicionar o serviço do logstash no docker-compose.yml

```
services:
    elasticsearch: ...
    kibana: ...
    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/logstash.yml:ro
        ports:
          - "9600:9600“
          - “5044:5044“
        networks:
          - elastic
```

Semantix

Logstash Configuração

- pipeline/logstash.conf

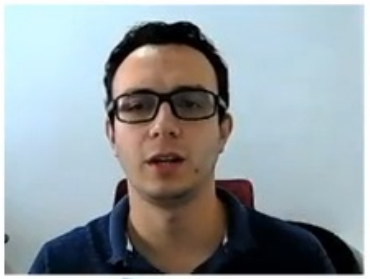
```
input {
        beats {
        port => 5044
        }
}
output {
        stdout {
        codec => "json"
        }
        elasticsearch {
                hosts => ["elasticsearch:9200"]
        }
}
```

- settings/logstash.yml

```
http.host: "0.0.0.0"
xpack.monitoring.elasticsearch.hosts: [
"http://elasticsearch:9200" ]
```

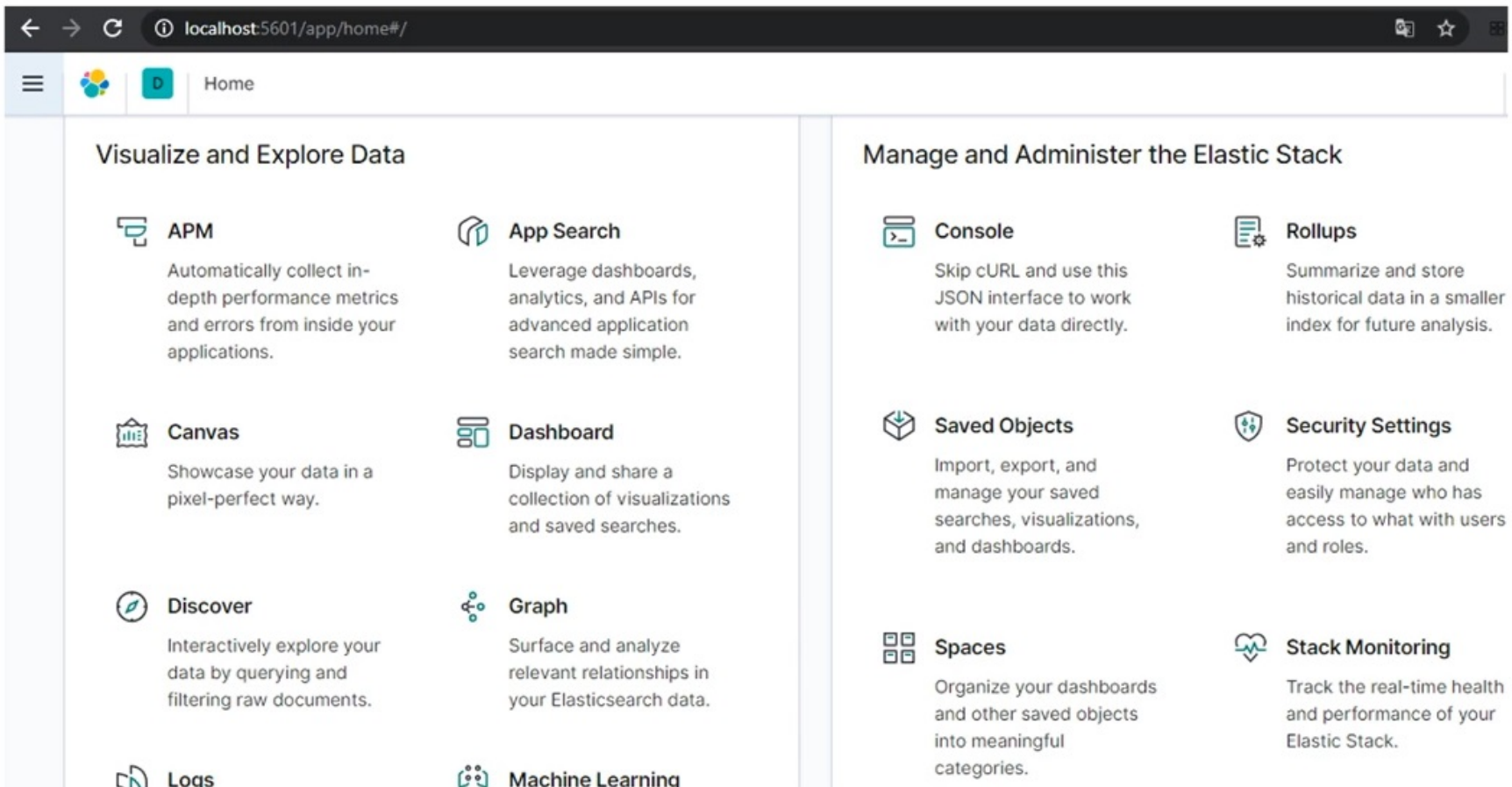
Semantix

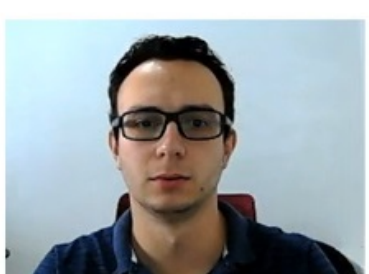
Kibana



Semantix

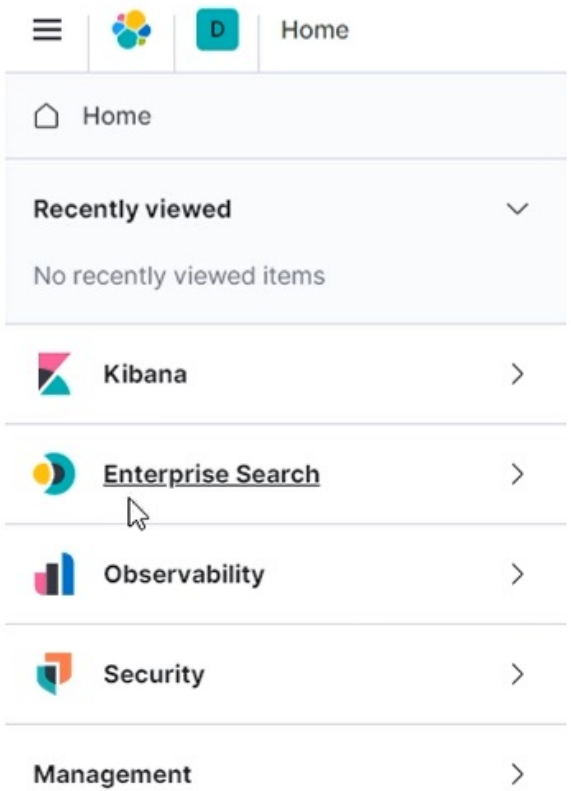
Interface Kibana

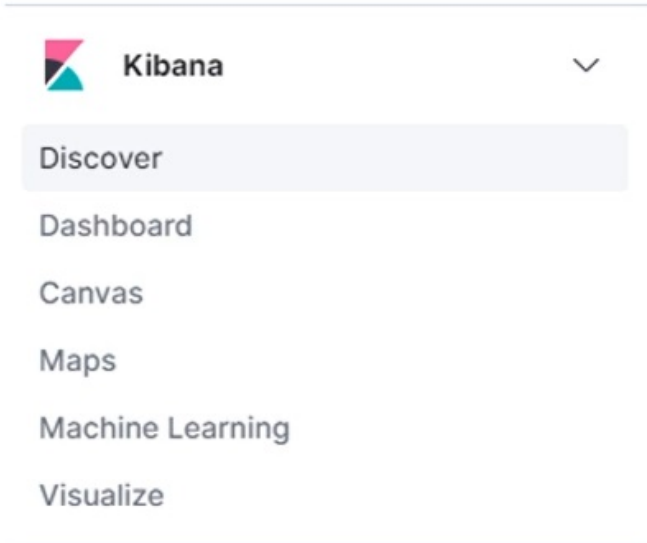




Semantix

Menu Kibana

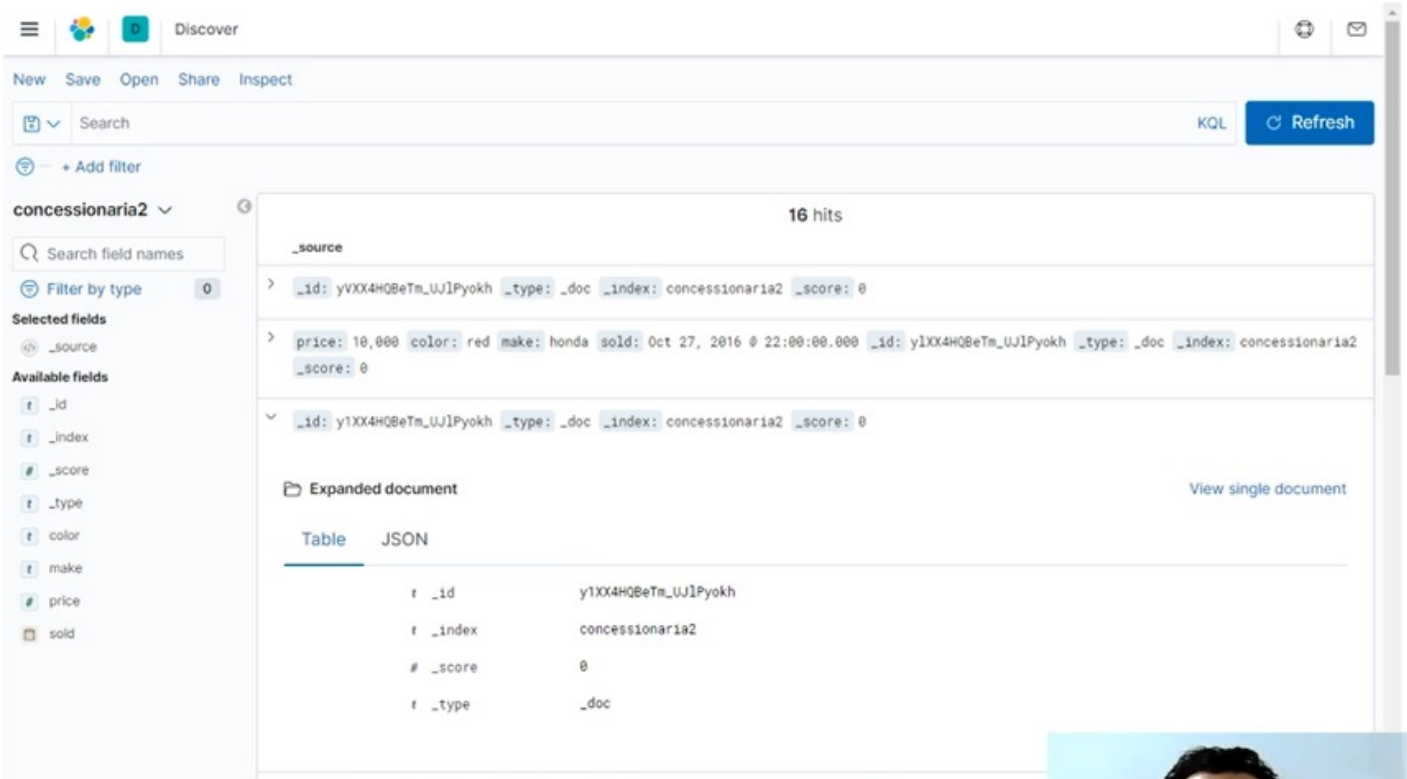




Semantix

Guia Discover

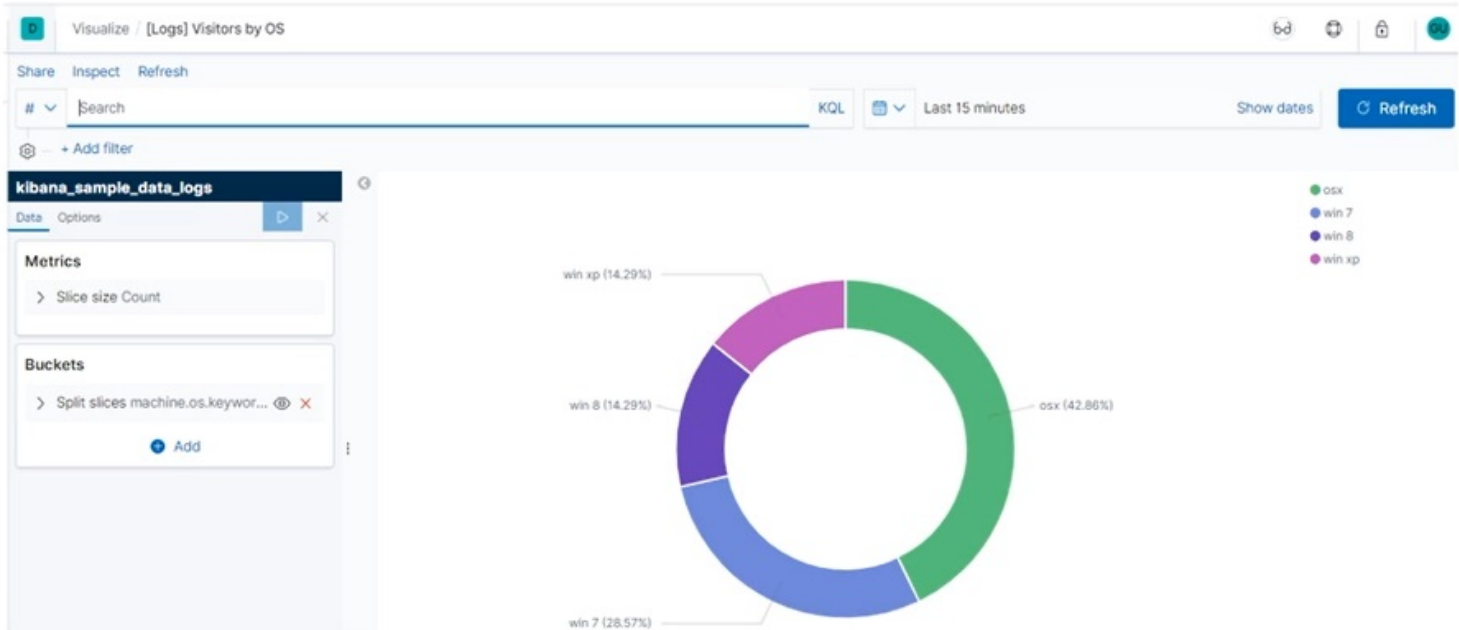
- Acessar, pesquisar e filtrar dados do índice selecionado
- Detalhes de campos da pesquisa
- Salvar pesquisas para usar no discover, visualizações e dashboards

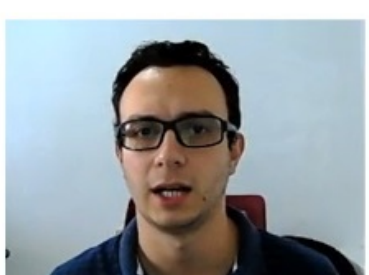


Semantix

Guia Visualize

- Criar, editar e salvar visualizações dos dados
  - Consultas
  - Filtros
  - Agregações

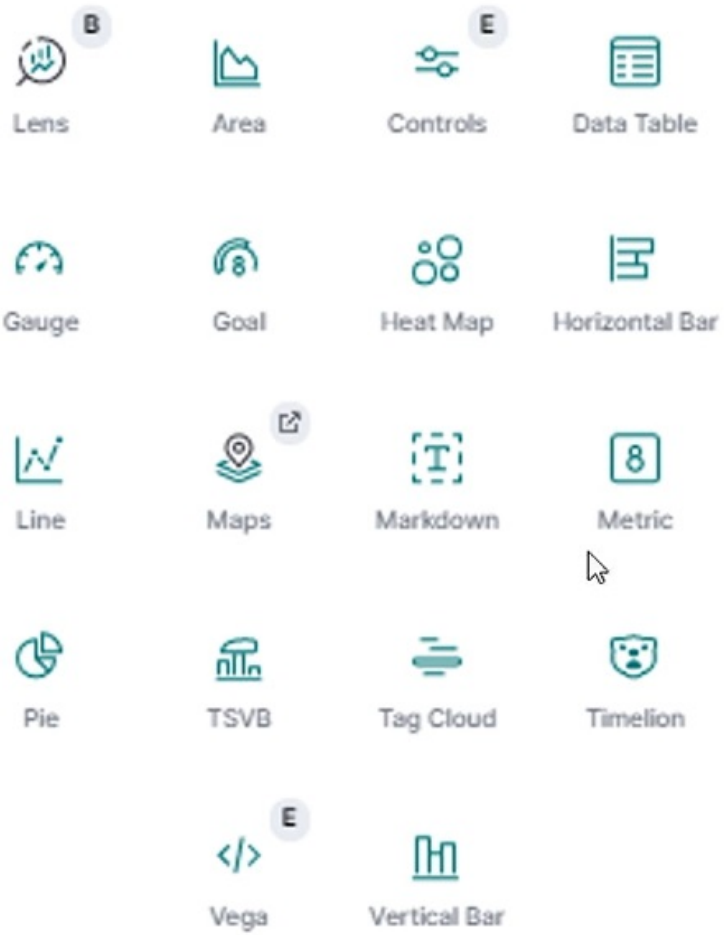


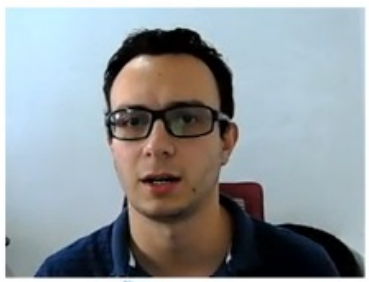


Semantix

Guia Visualize

- Tipos de Visualizações

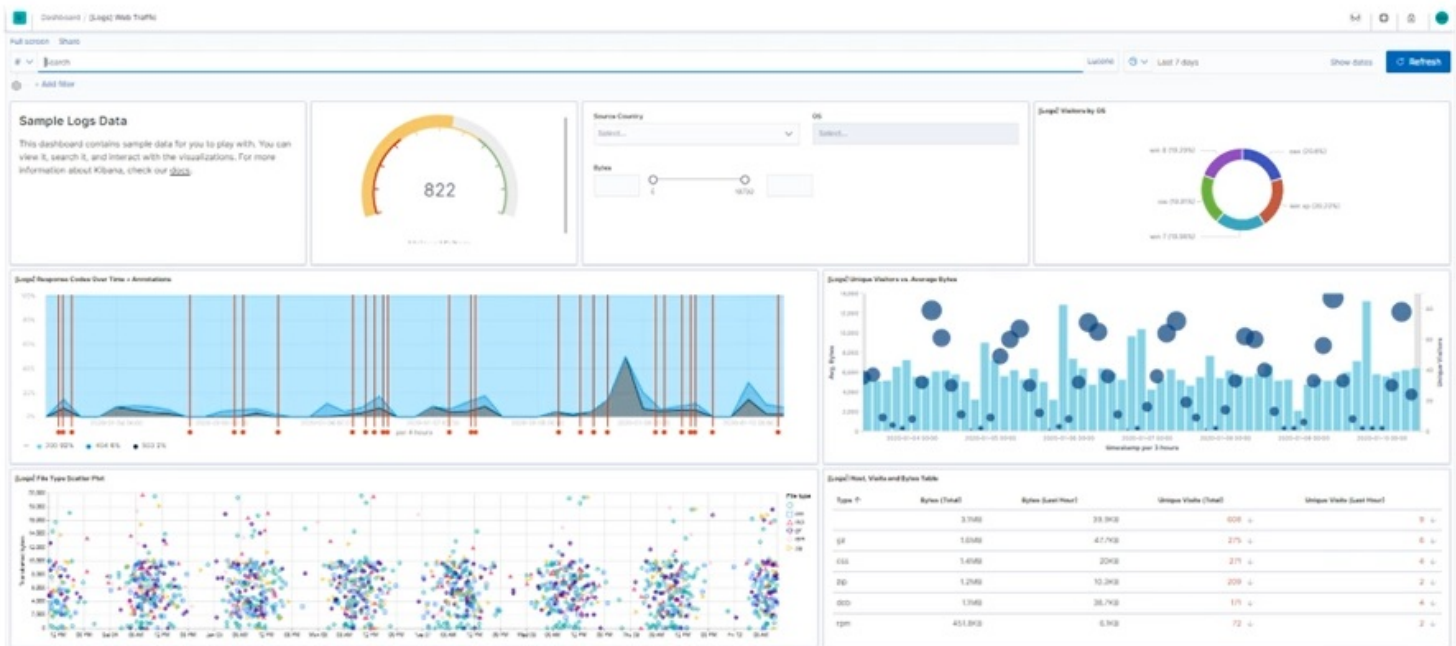




Semantix

Guia Dashboard

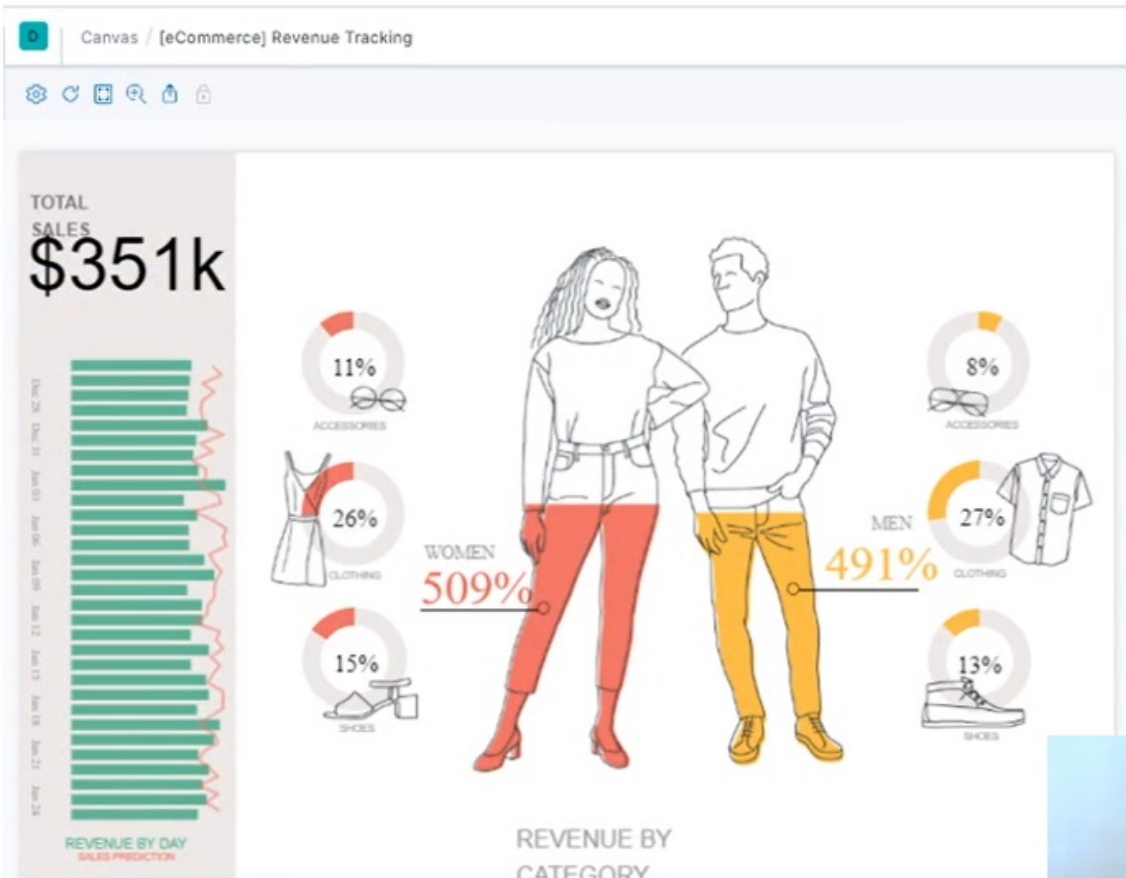
- Combinar várias visualizações de dados em um único lugar

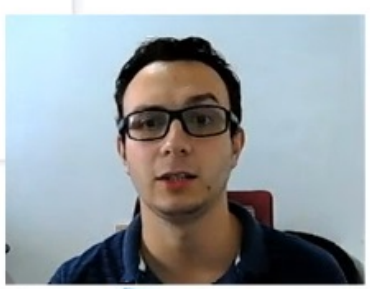


Semantix

Guia Canvas

- Visualização e apresentação de dados
  - Páginas
  - Combinação
    - Cores
    - Imagens
    - Texto

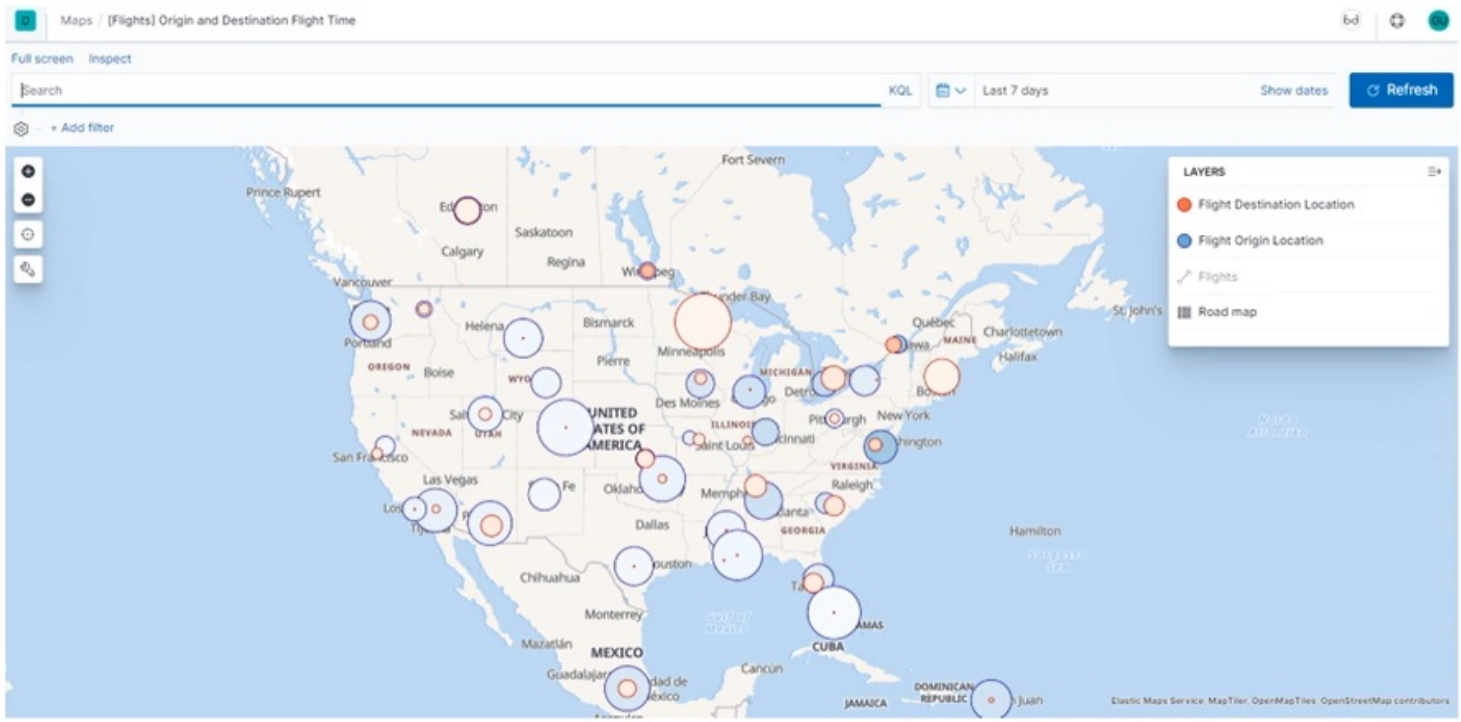




Semantix

Guia Maps

- Analisar dados geográfico em tempo real
  - Mapas com várias camadas e índices
  - Carregar arquivos GeoJSON



Semantix

Guia Machine Learning

- Gerenciamento de Jobs
  - Detector de anomalias
- Carregamento de dados

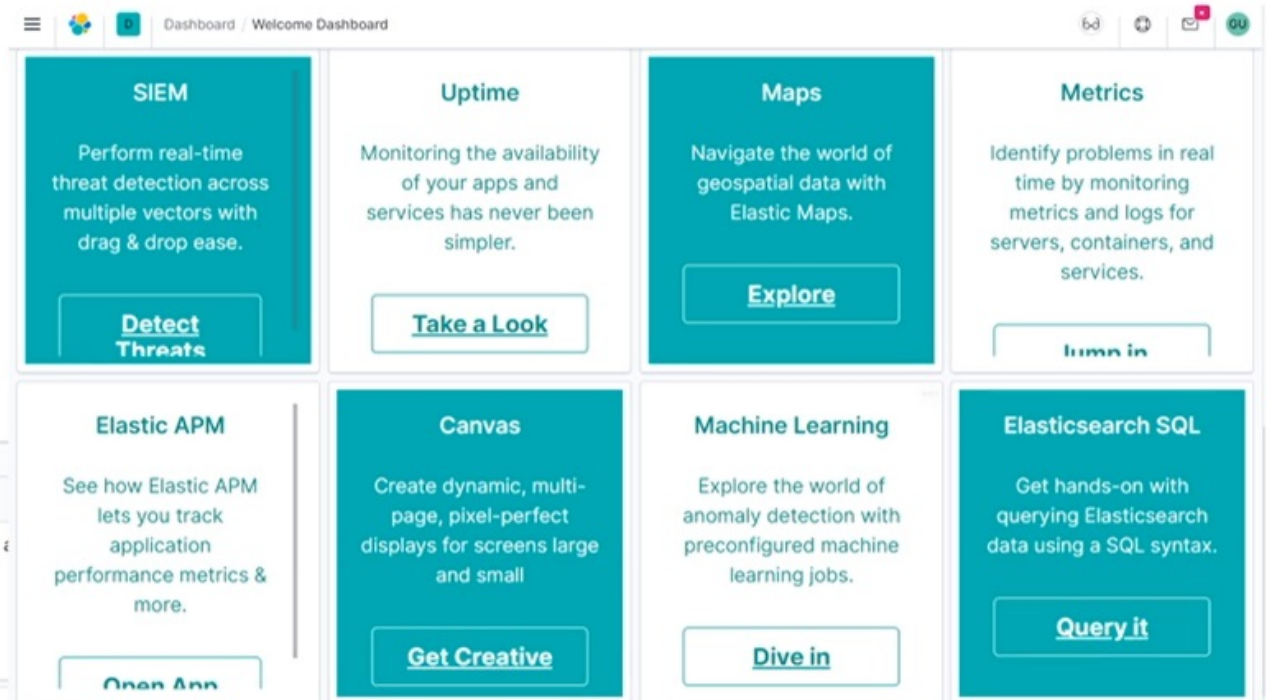
Semantix

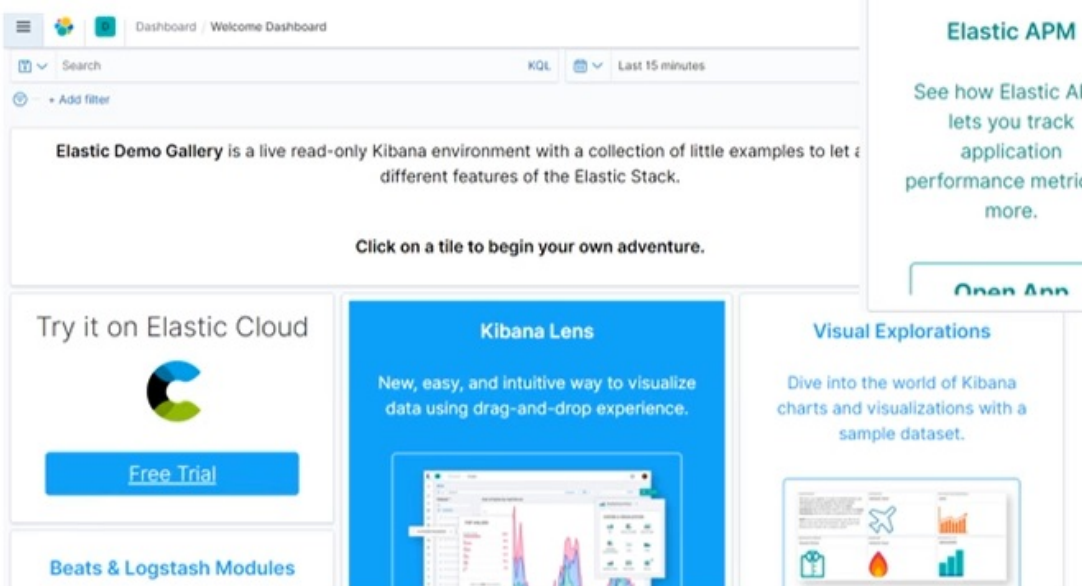
Bônus

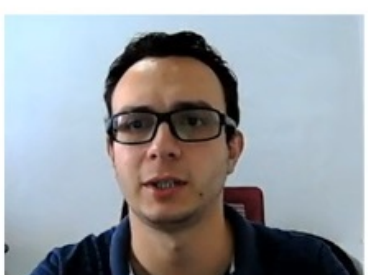
Semantix

Treinar Features do Elastic

- https://demo.elastic.co/







Semantix