



Introdução

Stack Elastic

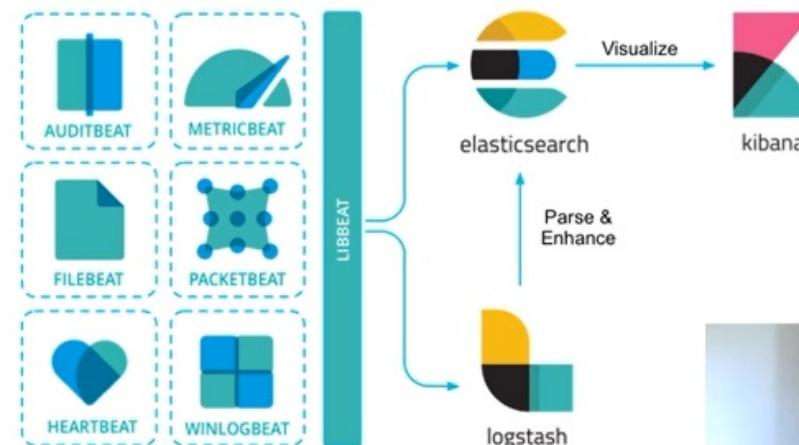


00:01

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



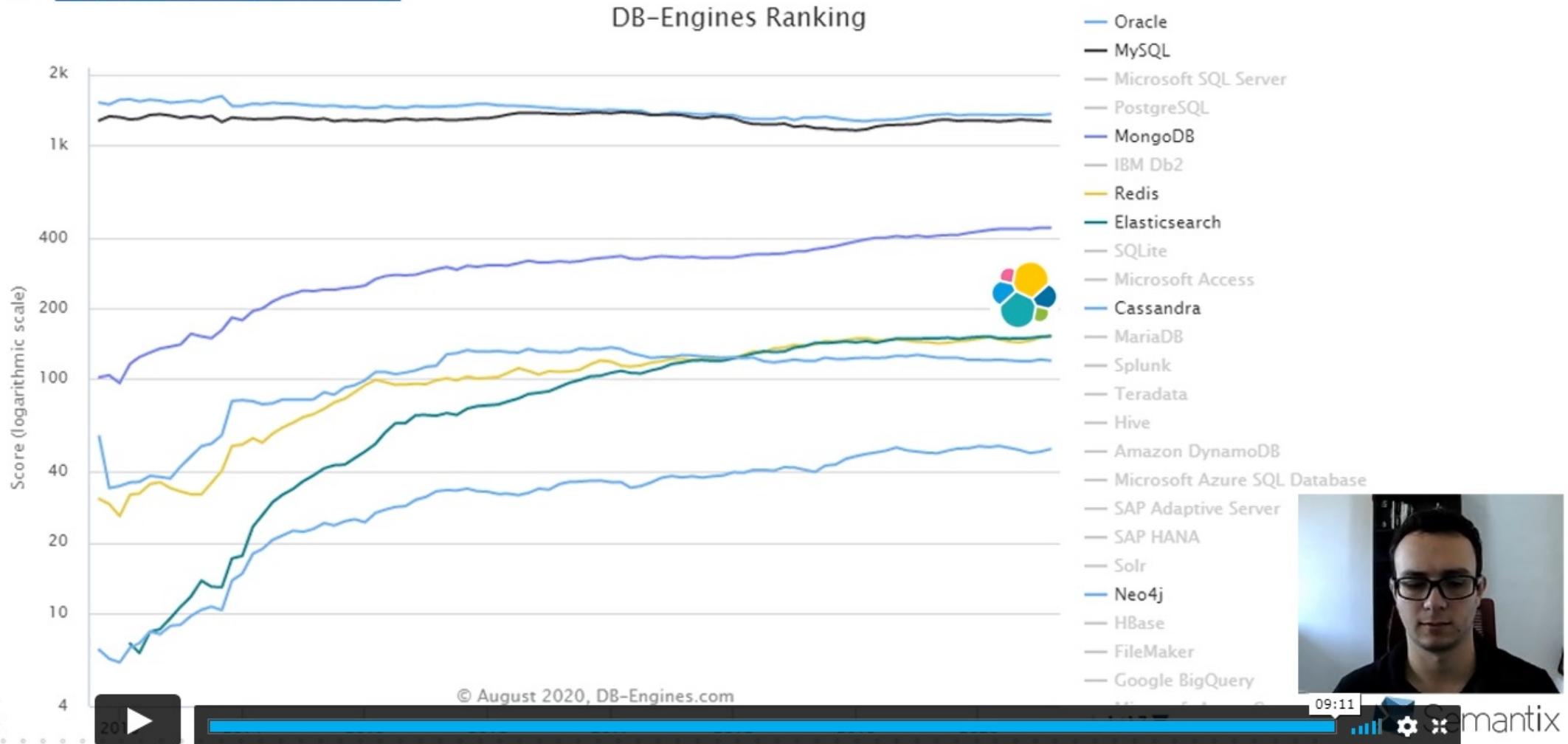
Índice

- 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



00:01

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/>

C elastic.co/pt/downloads/elasticsearch

Want it hosted? Deploy on Elastic Cloud. [Get Started »](#)

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](#)

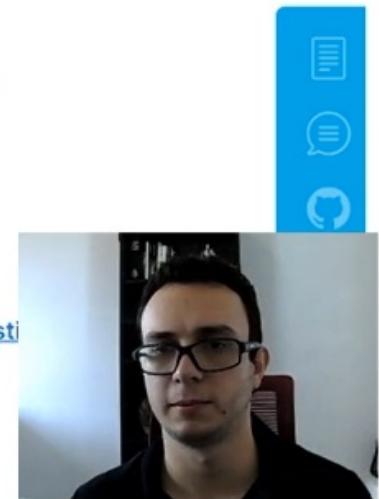
Package Managers: [Install with yum, dnf, or zypper](#)

[Install with apt-get](#)

[Install with homebrew](#)

Containers: [Run with Docker](#)

Notes: Running on Kubernetes? Try [Elasticsearch Operator](#)





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
 - 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



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
```



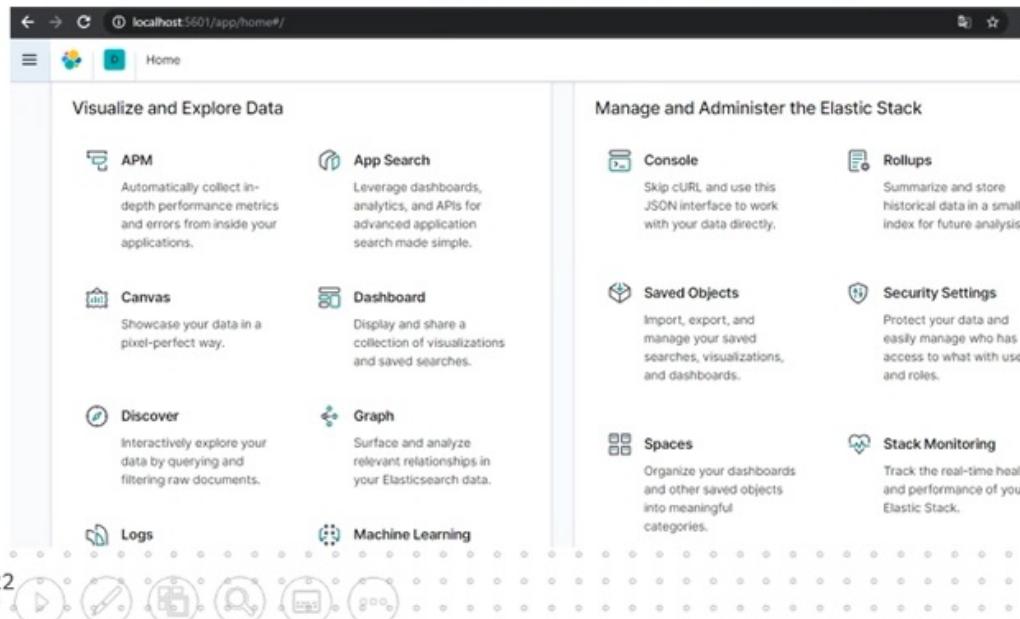
Acessos Ambiente docker

- 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



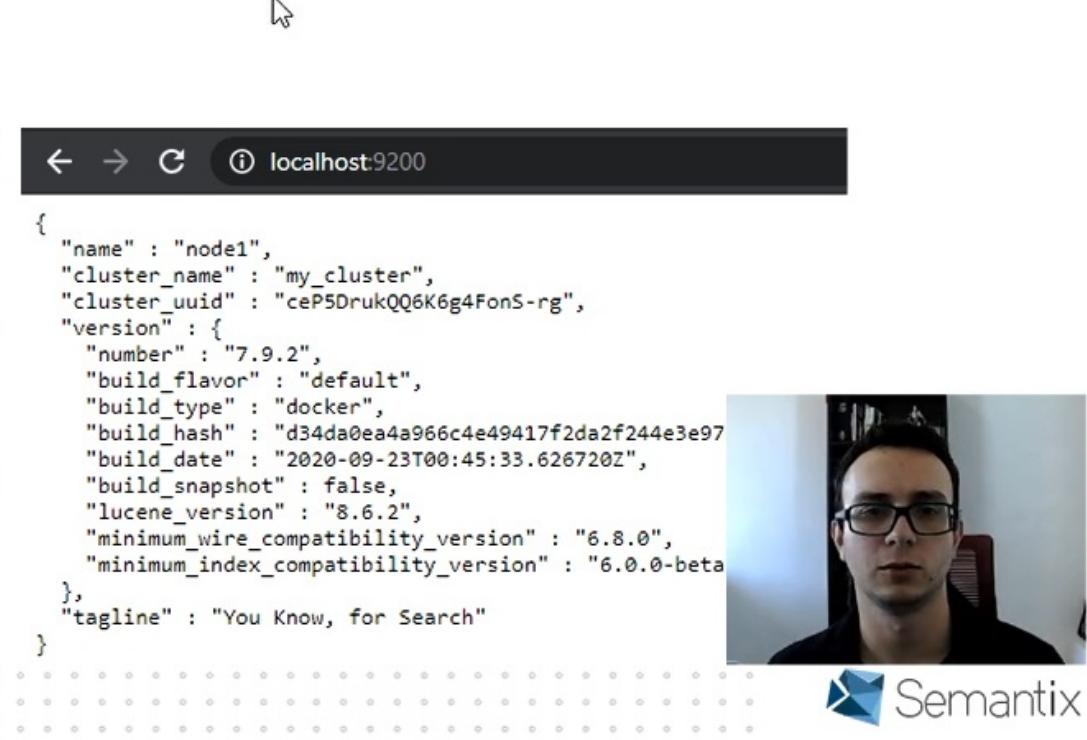
Verificar Funcionamento do cluster Elastic

- 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/>



The screenshot shows the Kibana home page at localhost:5601/app/home/. It features a grid of cards for different services:

- Visualize and Explore Data**:
 - APM: Automatically collect in-depth performance metrics and errors from inside your applications.
 - Canvas: Showcase your data in a pixel-perfect way.
 - Discover: Interactively explore your data by querying and filtering raw documents.
 - Logs: View log data.
 - Machine Learning: Analyze machine learning models.
- Manage and Administer the Elastic Stack**:
 - Console: Skip cURL and use this JSON interface to work with your data directly.
 - Dashboard: Display and share a collection of visualizations and saved searches.
 - Saved Objects: Import, export, and manage your saved searches, visualizations, and dashboards.
 - Spaces: Organize your dashboards and other saved objects into meaningful categories.
 - Rollups: Summarize and store historical data in a smaller index for future analysis.
 - Security Settings: Protect your data and easily manage who has access to what with users and roles.
 - Stack Monitoring: Track the real-time health and performance of your Elastic Stack.



The screenshot shows the Elasticsearch home page at localhost:9200. It displays the cluster state in JSON format:

```
{
  "name" : "node1",
  "cluster_name" : "my_cluster",
  "cluster_uuid" : "ceP5DrukQQ6K6g4FonS-rg",
  "version" : {
    "number" : "7.9.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "d34da0ea4a966c4e49417f2da2f244e3e97",
    "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-beta"
  },
  "tagline" : "You Know, for Search"
}
```

To the right of the JSON output is a video feed of a person wearing glasses and a dark shirt.



Configuração dos Containers



00:01

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



00:00

- 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
      }
    }
}
```



Interface Kibana - Comunicação HTTP

○ Acessar

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

The screenshot shows the Kibana interface. At the top, there's a navigation bar with icons for Home, Dev Tools, and a gear. Below it is a main menu with sections like Home, Recently viewed (empty), Management (with Dev Tools selected), and Ingest Manager/Stack Monitoring. At the bottom, there's a footer with a navigation bar and a URL indicator: localhost:5601/app/dev_tools.

The screenshot shows the Kibana Dev Tools console. The top navigation bar includes tabs for Console, Search Profiler, Grok Debugger, and Painless Lab (BETA). Below the tabs are History, Settings, and Help buttons. The main area displays a search query and its results. The query is:

```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
```

The results pane shows the response structure:

```
1 {
2   "took" : 24,
3   "timed_out" : false,
4   "_shards" : {
5     "total" : 5,
6     "successful" : 5,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : {
12      "value" : 25,
13      "relation" : "eq"
14    },
15    "max_score" : 1.0,
16    "hits" : [
17      {
18        "_index" : "logstash-2015.01.01",
19        "_score" : 1.0,
20        "_type" : "log",
21        "_id" : "ZDgXWjwAABQHJyL",
22        "_source" : {
23          "host": {
24            "host_name": "elasticsearch-01",
25            "ip": "192.168.1.101"
26          },
27          "offset": 1000000000000000000,
28          "offset_end": 1000000000000000000,
29          "offset_start": 1000000000000000000,
30          "offset_type": "bytes"
31        }
32      }
33    ]
34  }
35 }
```





```
1 GET cliente/_doc/1
2 GET cliente/_count
3 GET cliente/_search
4 GET /
5
6 GET cliente/_source/1
```



```
1 { "_index": "cliente",
2   "_type": "_doc",
3   "_id": "1",
4   "_version": 3,
5   "_seq_no": 2,
6   "_primary_term": 1,
7   "found": true,
8   "source": {
9     "name": "Lucas",
10    "idade": 20,
11    "conhecimento": "Windows, Office, Hadoop, Elastic"
12  }
13 }
14
15
```





Operações básicas

CRUD



CRUD

- Create
- Read
- Update
- Delete



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"
```

```
}
```



CRUD DELETE

- Deletar um documento

- Exemplo

```
DELETE cliente/_doc/1
```



- Deletar um índice

- Exemplo

```
DELETE cliente
```



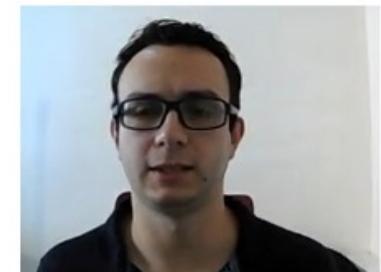
- Exemplos
 - Informações sobre o nó do elasticseach (<http://localhost:9200/>)
 - GET /
 - Buscar todos os documentos em um índice
 - GET cliente/_search
 - Buscar um documento em um índice
 - GET cliente/_doc/1
 - Buscar a quantidade de documentos em um índice
 - GET cliente/_count
 - Buscar os dados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





Beats

Família de beats



00:02

Beats Família

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



Filebeat

Arquivos de log

Winlogbeat

Logs de evento do Windows

Metricbeat

Métricas

Auditbeat

Dados de auditoria

Functionbeat

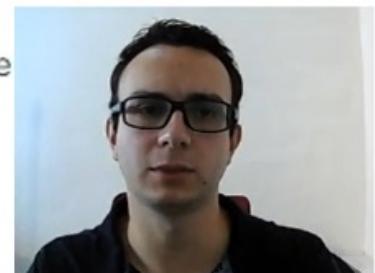
Agente de envio sem servidor

Packetbeat

Dados de rede

Heartbeat

Monitorame





Logstash

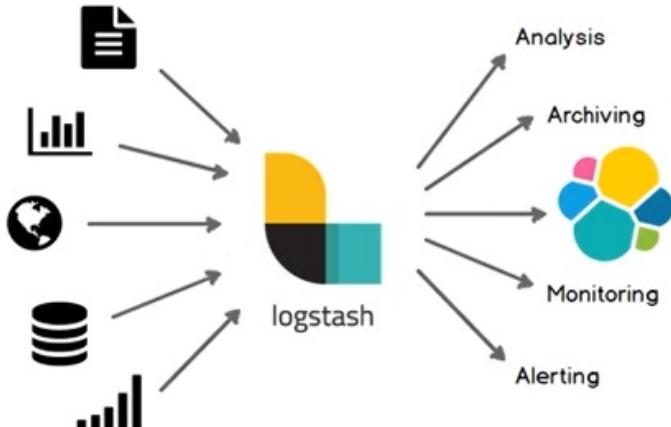
Conceitos

Plugins



00:00

Logstash Conceitos



- Alterar o logstash.conf

- Estrutura do json

```
input{
```

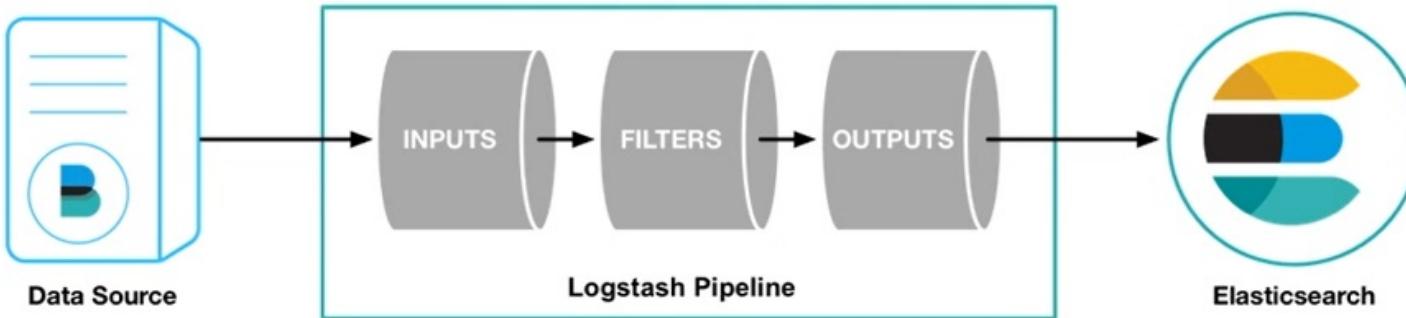
```
}
```

```
filter{
```

```
}
```

```
output {
```

```
}
```



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



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



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" ]
```





Kibana



Semantix

Interface Kibana

localhost:5601/app/home#/

Home

Visualize and Explore Data

- APM**
Automatically collect in-depth performance metrics and errors from inside your applications.
- Canvas**
Showcase your data in a pixel-perfect way.
- Discover**
Interactively explore your data by querying and filtering raw documents.
- Logs**
- App Search**
Leverage dashboards, analytics, and APIs for advanced application search made simple.
- Dashboard**
Display and share a collection of visualizations and saved searches.
- Graph**
Surface and analyze relevant relationships in your Elasticsearch data.
- Machine Learning**

Manage and Administer the Elastic Stack

- Console**
Skip cURL and use this JSON interface to work with your data directly.
- Saved Objects**
Import, export, and manage your saved searches, visualizations, and dashboards.
- Spaces**
Organize your dashboards and other saved objects into meaningful categories.
- Rollups**
Summarize and store historical data in a smaller index for future analysis.
- Security Settings**
Protect your data and easily manage who has access to what with users and roles.
- Stack Monitoring**
Track the real-time health and performance of your Elastic Stack.



Menu Kibana

≡ |  |  | Home

 Home

Recently viewed ▼

No recently viewed items

 Kibana >

 Enterprise Search > Mouse cursor over the link

 Observability >

 Security >

Management >

 Kibana ▼

 Discover

Dashboard

Canvas

Maps

Machine Learning

Visualize



 Semantix

Guia Discover

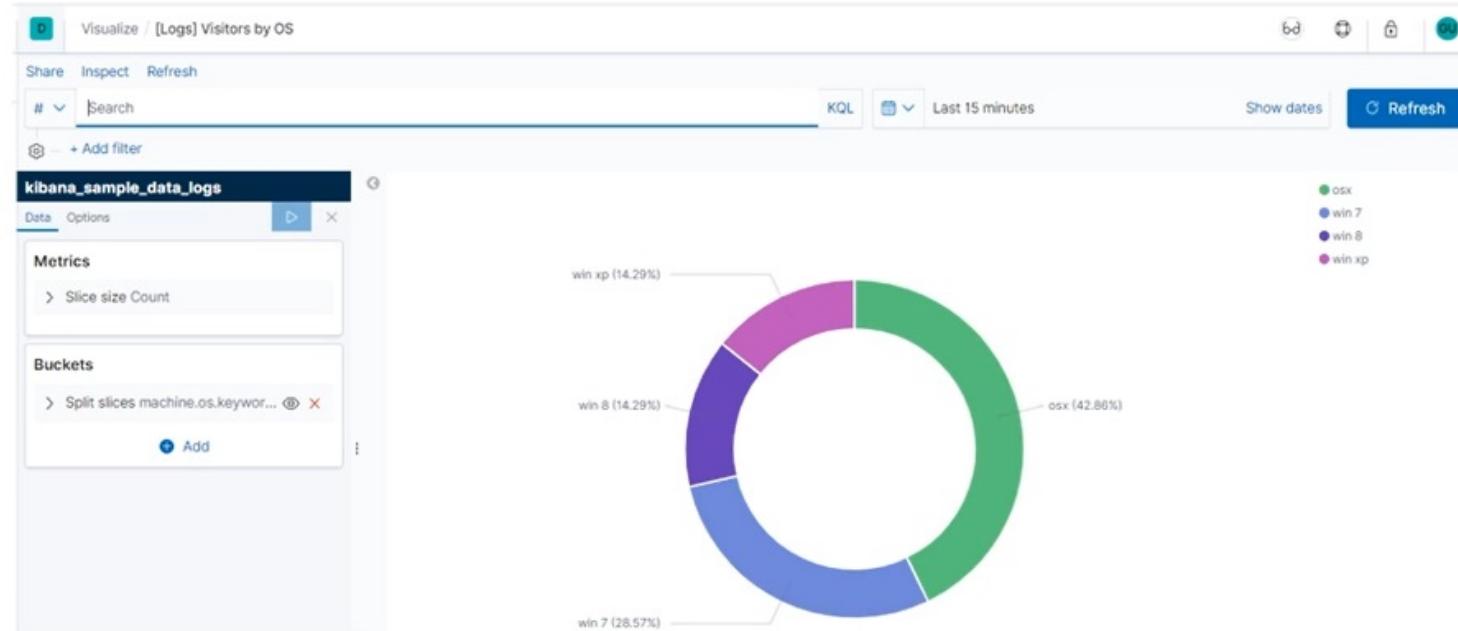
- Acessar, pesquisar e filtrar dados do índice selecionado
- Detalhes de campos da pesquisa
- Salvar pesquisas para usar no discover, visualizações e dashboards

The screenshot shows the Elasticsearch Discover interface. At the top, there are navigation icons and the title 'Discover'. Below the title, a menu bar includes 'New', 'Save', 'Open', 'Share', and 'Inspect'. On the right side of the menu bar are 'KQL' and 'Refresh' buttons. The main area is titled 'concessionaria2' with a dropdown arrow. A search bar contains the placeholder 'Search field names'. To the right of the search bar is a 'Filter by type' button with a count of '0'. Below these are two sections: 'Selected fields' and 'Available fields'. The 'Selected fields' section contains '_source'. The 'Available fields' section lists '_id', '_index', '_score', '_type', 'color', 'make', 'price', and 'sold'. On the right, the search results are displayed with a total of '16 hits'. Each result is a collapsed card showing '_id', '_index', '_score', and '_type'. An 'Expanded document' button is available to view the full document details. The expanded view shows a table with columns '_id', '_index', '_score', and '_type', containing the same information as the collapsed cards.



Guia Visualize

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



Guia Visualize

○ Tipos de Visualizações



Lens



Area



Controls



Data Table



Gauge



Goal



Heat Map



Horizontal Bar



Line



Maps



Markdown



Metric



Pie



TSVB



Tag Cloud



Timelion



Vega

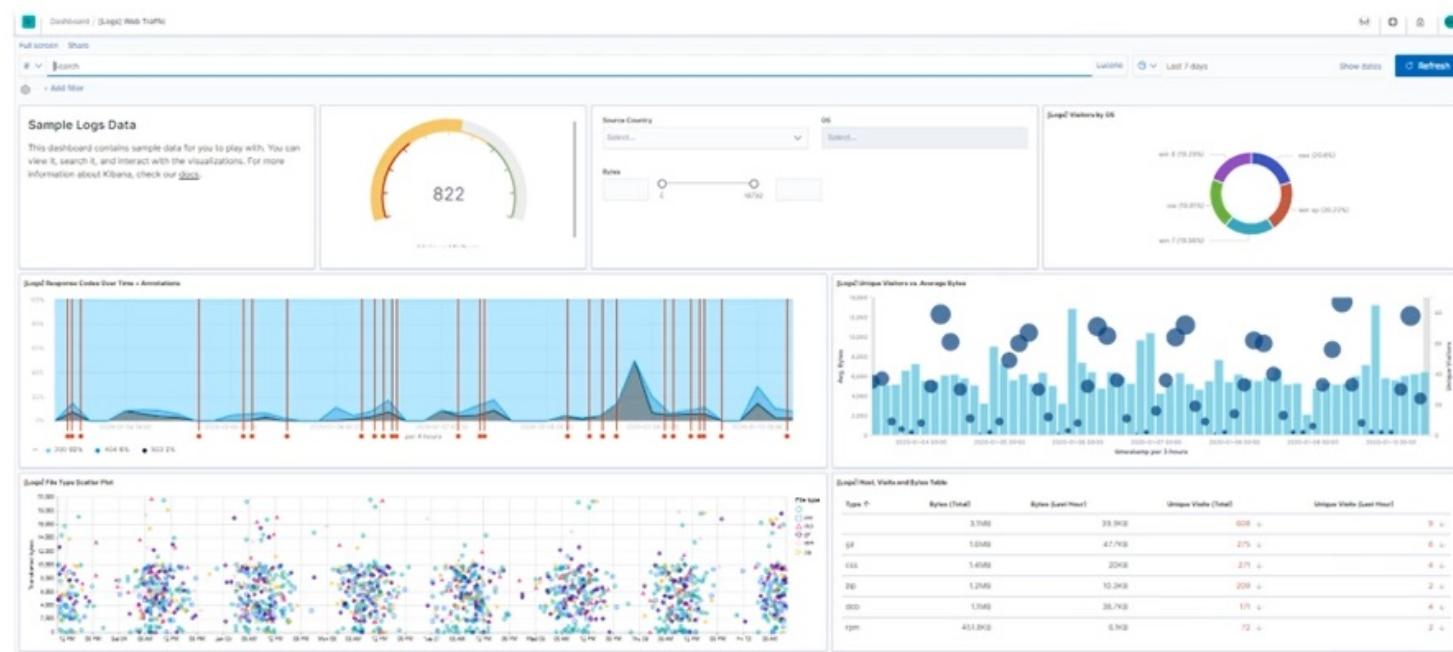


Vertical Bar



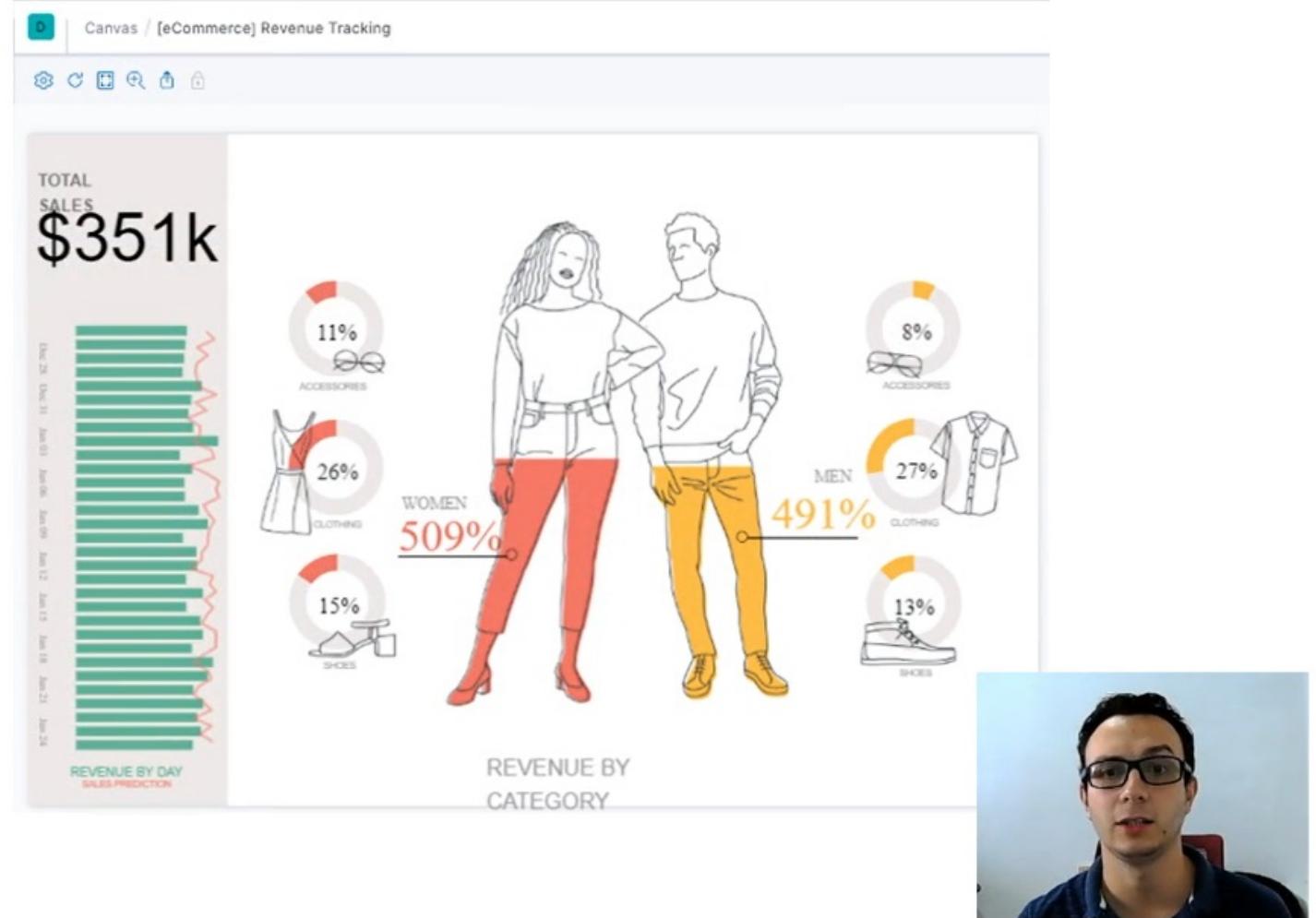
Guia Dashboard

- Combinar várias visualizações de dados em um único lugar



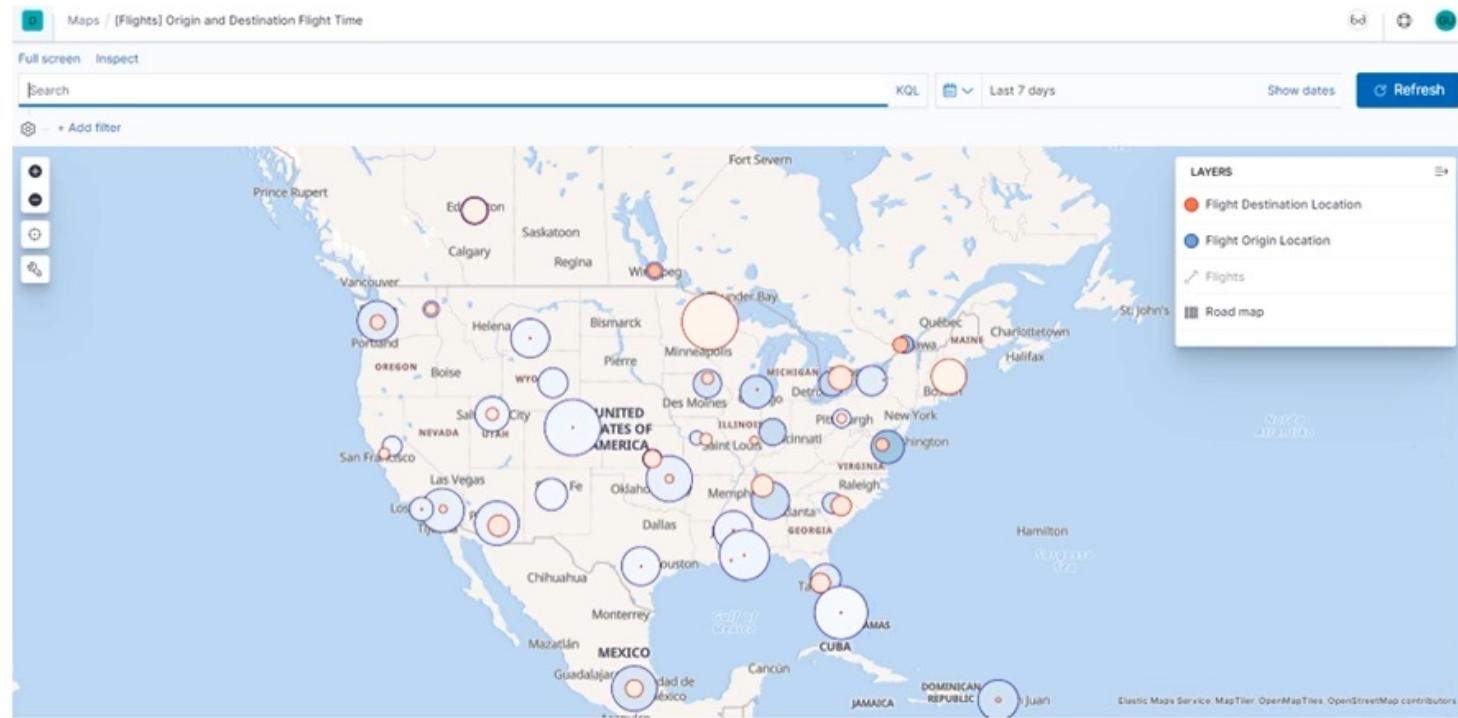
Guia Canvas

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



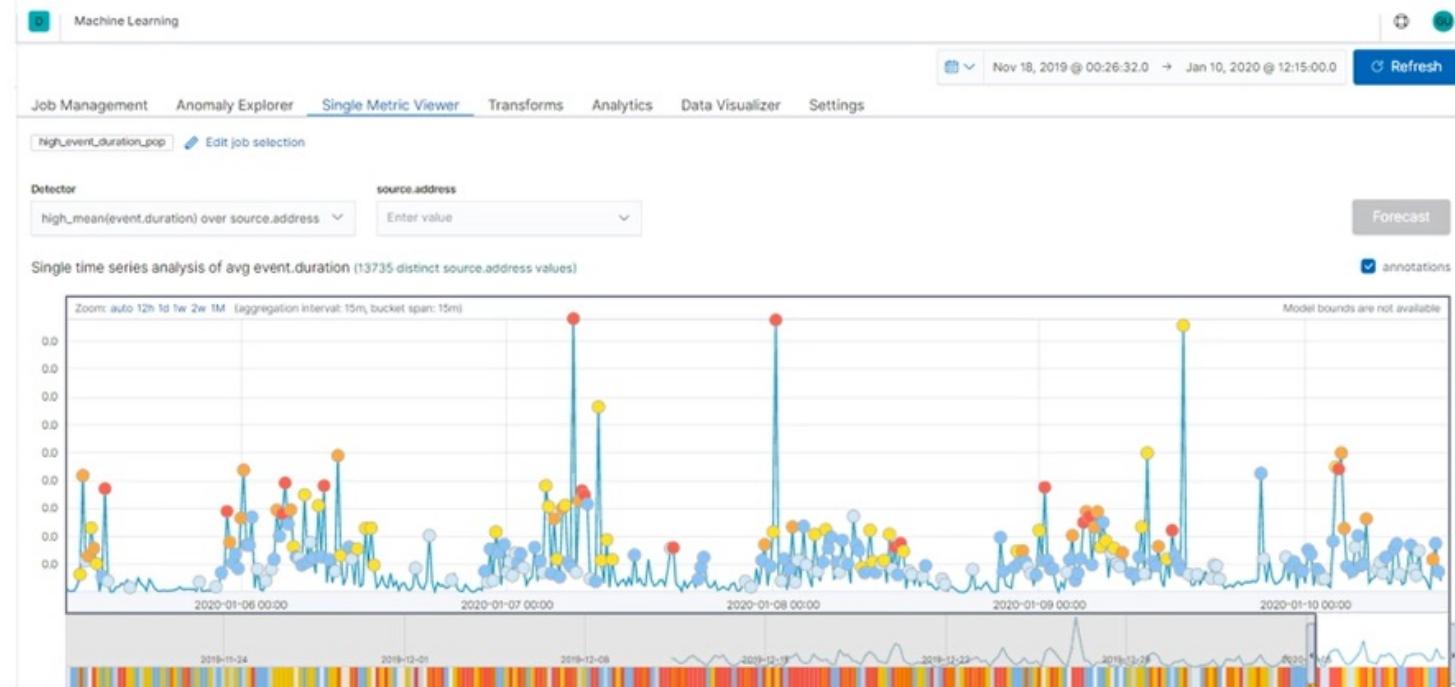
Guia Maps

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



Guia Machine Learning

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





Bônus



Treinar Features do Elastic

- <https://demo.elastic.co/>

The screenshot shows the 'Elastic Demo Gallery' Kibana environment. At the top, there's a search bar and a 'KQL' button. Below it, a message says: 'Elastic Demo Gallery is a live read-only Kibana environment with a collection of little examples to let you explore different features of the Elastic Stack.' A call-to-action 'Click on a tile to begin your own adventure.' is present. On the left, a section titled 'Try it on Elastic Cloud' features a 'Free Trial' button and a logo. Other sections include 'Beats & Logstash Modules' and 'Kibana Lens' which describes a 'New, easy, and intuitive way to visualize data using drag-and-drop experience.' with a preview image.

The screenshot shows the 'Welcome Dashboard' of the Elastic Stack. It features a grid of cards:

- SIEM**: Perform real-time threat detection across multiple vectors with drag & drop ease. [Detect Threats](#)
- Uptime**: Monitoring the availability of your apps and services has never been simpler. [Take a Look](#)
- Maps**: Navigate the world of geospatial data with Elastic Maps. [Explore](#)
- Metrics**: Identify problems in real time by monitoring metrics and logs for servers, containers, and services. [Jump in](#)
- Elastic APM**: See how Elastic APM lets you track application performance metrics & more. [Open App](#)
- Canvas**: Create dynamic, multi-page, pixel-perfect displays for screens large and small. [Get Creative](#)
- Machine Learning**: Explore the world of anomaly detection with preconfigured machine learning jobs. [Dive in](#)
- Elasticsearch SQL**: Get hands-on with querying Elasticsearch data using a SQL syntax. [Query it](#)

