Introducción al stack de Elastic y sus capacidades geoespaciales

Jorge Sanz
2022-06-09, Kibana, Elastic,
xurxosanz jsanz jorge.sanz@elastic.co

https://ela.st/siglibre2022-taller

elastic

Objetivos de la sesión

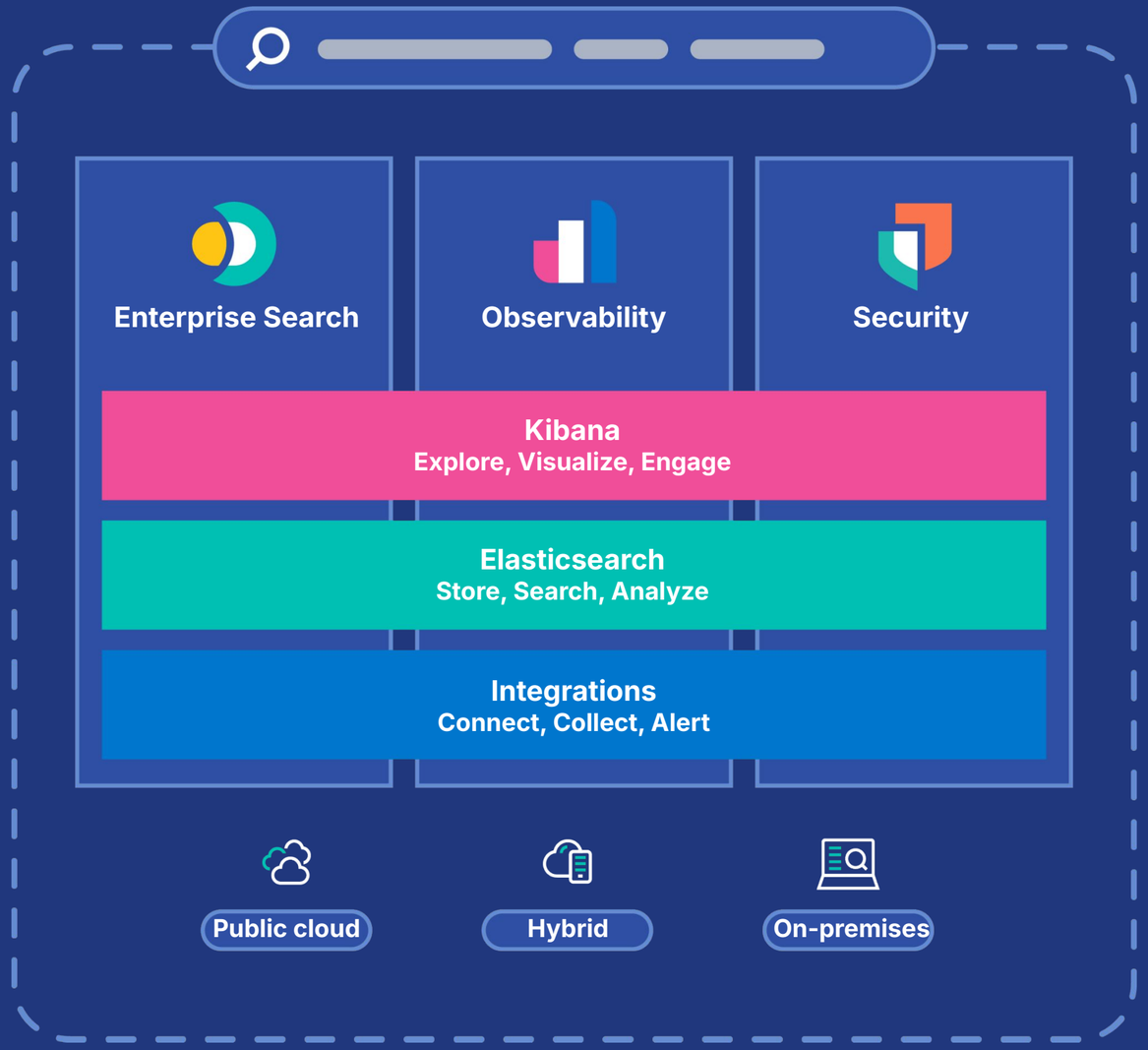
- **Ejecutar** el stack de Elastic de manera sencilla
- Qué son **Kibana** y sus diferentes componentes
- Cómo usar **Elastic Maps** para visualizar datos geoespaciales
- Cuáles son las características **geoespaciales** básicas de Elasticsearch
- Cómo encaja Elastic en la **arquitectura** de una aplicación geoespacial

elastic

Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

La plataforma Elastic



elastic

Elasticsearch

Todos los datos son bienvenidos

elastic

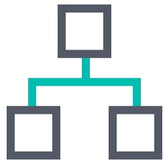
Componentes de Elasticsearch

Cluster

Node

Shard

Index



Mapping

Document

Field

elastic

Communicating with Elasticsearch

- All communication through HTTP endpoints 📖

```
→ http --verify=/tmp/ca.crt --auth elastic:changeme https://localhost:9203/
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 531
content-type: application/json

{
    "cluster_name": "docker-cluster",
    "cluster_uuid": "kIQy28mqRlyOvBis_FELXg",
    "name": "es01",
    "tagline": "You Know, for Search",
    "version": {
        "build_date": "2022-04-20T10:35:10.180408517Z",
        "build_flavor": "default",
        "build_hash": "b174af62e8dd9f4ac4d25875e9381ffe2b9282c5",
        "build_snapshot": false,
        "build_type": "docker",
        "lucene_version": "9.1.0",
        "minimum_index_compatibility_version": "7.0.0",
        "minimum_wire_compatibility_version": "7.17.0",
        "number": "8.2.0"
    }
}
```

Communicating with Elasticsearch

- All communication through HTTP endpoints 📖
- JSON

```
→ http --verify=/tmp/ca.crt --auth elastic:changeme\
 "https://localhost:9203/flight_tracking*/_search?size=1"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 582
content-type: application/json

{
    "_shards": {
        "failed": 0,
        "skipped": 0,
        "successful": 2,
        "total": 2
    },
    "hits": {
        "hits": [
            {
                "_id": "_VcQtIAB4XM3OLHfsxTV",
                "_index": "flight_tracking_2022-05-11",
                "_score": 1.0,
                "_source": {
                    "@timestamp": 1652288434988,
                    "baroAltitude": 8206.74,
                    "callsign": "PDT6046",
                    "geoAltitude": 8564.88,
                    "heading": 56.6,
                    "icao24": "a808c4",
                    "lastContact": 1652288393000,
                    "location": {
                        "lat": 34.129,
                        "lon": -82.6954
                    },
                    "onGround": false,
                    "originCountry": "United States",
                    "spi": false,
```

Communicating with Elasticsearch

- All communication through HTTP endpoints 📖
- JSON
- REST methods: GET, PUT, POST, DELETE

```
○ echo -n '{"hello": "world"}' | http --verify=/tmp/ca.crt --auth elastic:changeme \
    POST "https://localhost:9203/my_test/_doc"
HTTP/1.1 201 Created
Location: /my_test/_doc/KLCJxoAB0CoZ6d_Z8ZDc
X-elastic-product: Elasticsearch
content-length: 159
content-type: application/json

{
    "_id": "KLCJxoAB0CoZ6d_Z8ZDc",
    "_index": "my_test",
    "_primary_term": 1,
    "_seq_no": 0,
    "_shards": {
        "failed": 0,
        "successful": 1,
        "total": 2
    },
    "_version": 1,
    "result": "created"
}


~
→ http --verify=/tmp/ca.crt --auth elastic:changeme DELETE \
 "https://localhost:9203/my_test"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 21
content-type: application/json

{
    "acknowledged": true
}
```

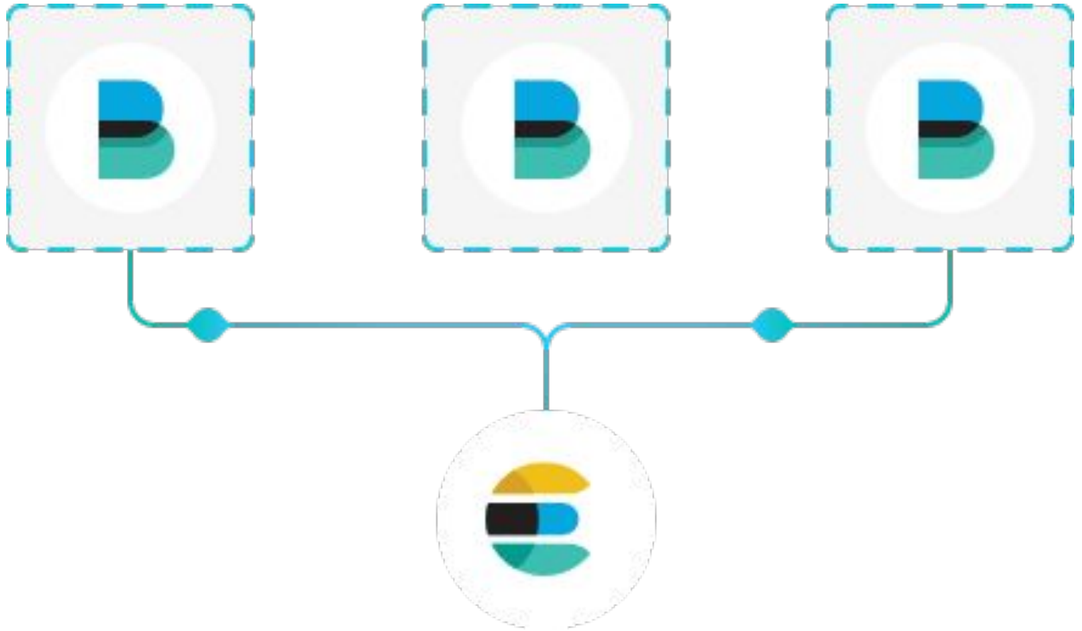
Communicating with Elasticsearch

- All communication through HTTP endpoints 📖
- JSON
- REST methods: GET, PUT, POST, DELETE
- _cat API for human readable display 📖

```
~
→ http --verify=/tmp/ca.crt --auth elastic:changeme\
 "https://localhost:9203/_cat/health?v&h=cluster,status,node.total,pri,shards"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 88
content-type: text/plain; charset=UTF-8

cluster        status node.total pri shards
docker-cluster green           2  15     30


~
→ http --verify=/tmp/ca.crt --auth elastic:changeme\
 "https://localhost:9203/_cat/nodes?v&h=name,ip,ram.percent,cpu,node.role"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 130
content-type: text/plain; charset=UTF-8

name ip         ram.percent cpu node.role
es01 172.27.0.3         100   7 cdfhilmrstw
es02 172.27.0.4          96   7 cdfhilmrstw


~
→ http --verify=/tmp/ca.crt --auth elastic:changeme\
 "https://localhost:9203/_cat/indices?v&h=index,health,docs.count,store.size"
HTTP/1.1 200 OK
X-elastic-product: Elasticsearch
content-length: 224
content-type: text/plain; charset=UTF-8

index                       health docs.count store.size
flight_tracking_2022-05-12 green      299029    108.6mb
flight_tracking_2022-05-11 green      438453    155.2mb
flight_tracking_2022-05-15 green        4070      3.4mb
```

Beats

Lightweight data shippers



Ship data from the source	Ship and centralize in Elasticsearch	Ship to Logstash for transformation and parsing
Ship to Elastic Cloud	Libbeat: API framework to build custom beats	70+ community Beats

elastic

Beats

All the modules

FileBeat
Log Files

MetricBeat
Metrics

PacketBeat
Network Data

WinLogBeat
Window Events

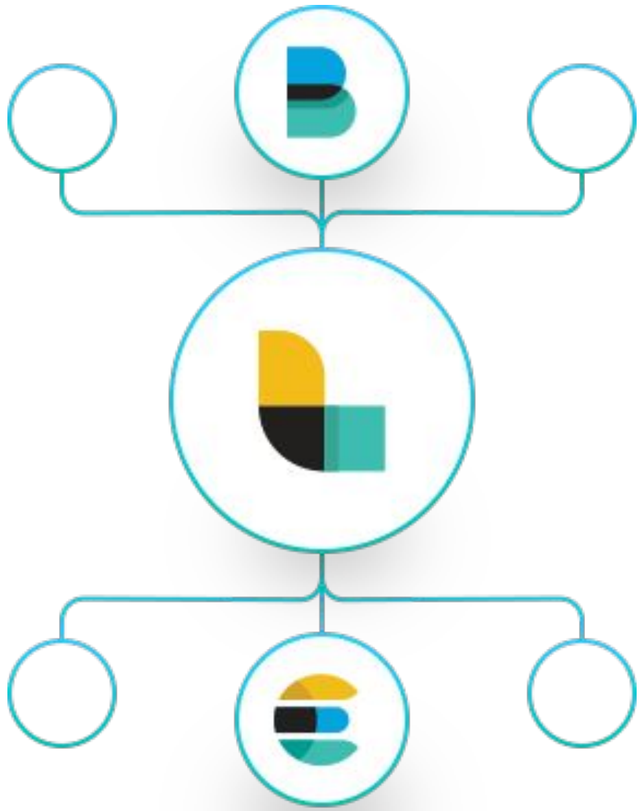
HeartBeat
Uptime Monitoring

AuditBeat
Audit Data

FunctionBeat
Serverless Shipper

Plus, more than 70 community Beats and growing...

elastic



Logstash

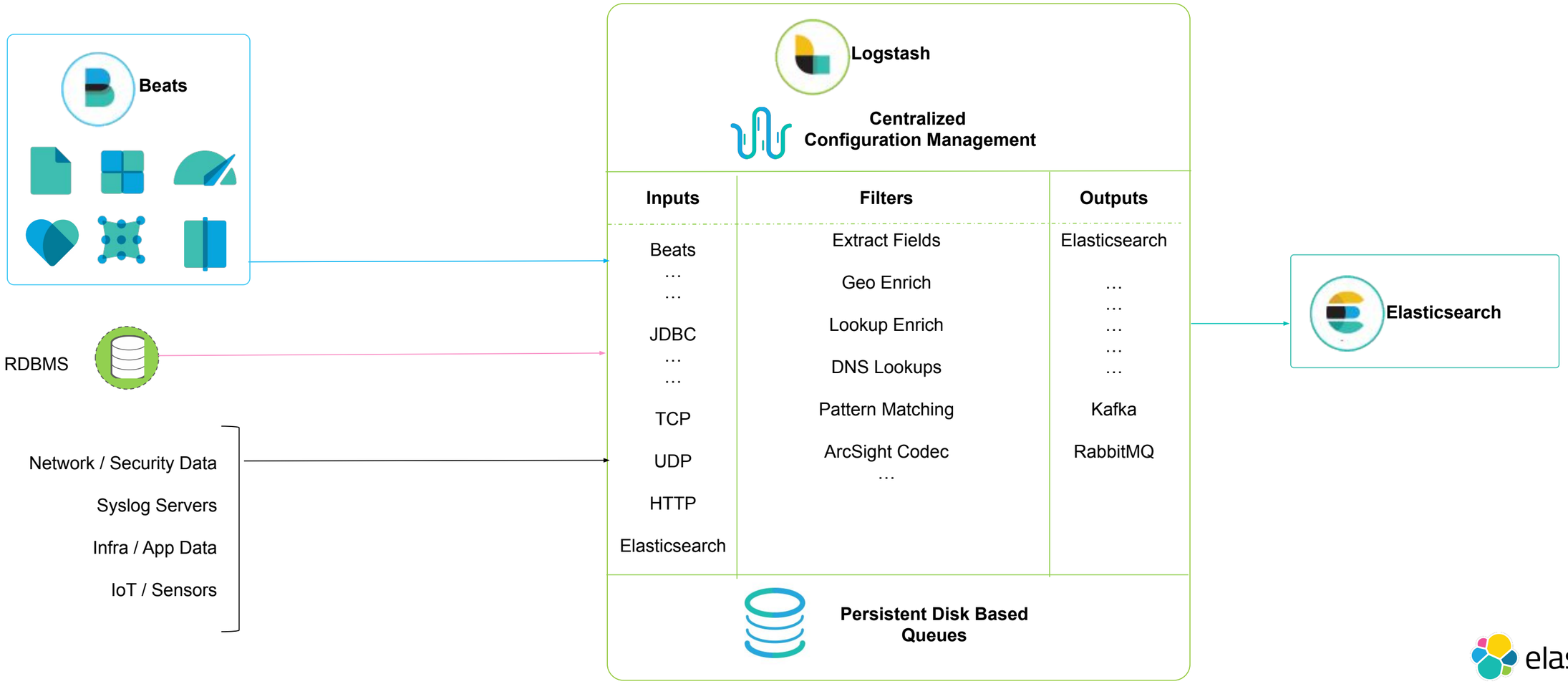
ETL for Elasticsearch

Ingest data of all shapes, sizes, and sources	Parse and dynamically transform data	Transport data to any output
Secure and encrypt data inputs	Build your own pipelines	Lots of plugins

elastic

Logstash

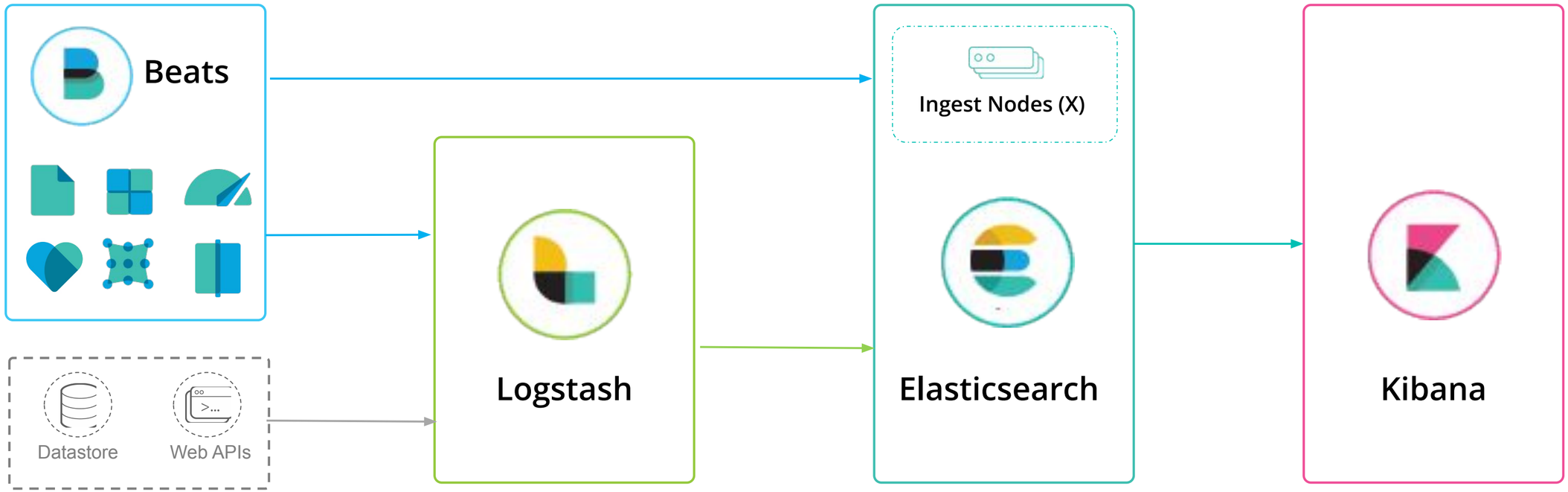
Normalize and Enrich Data before Indexing



elastic

Elastic **Stack**

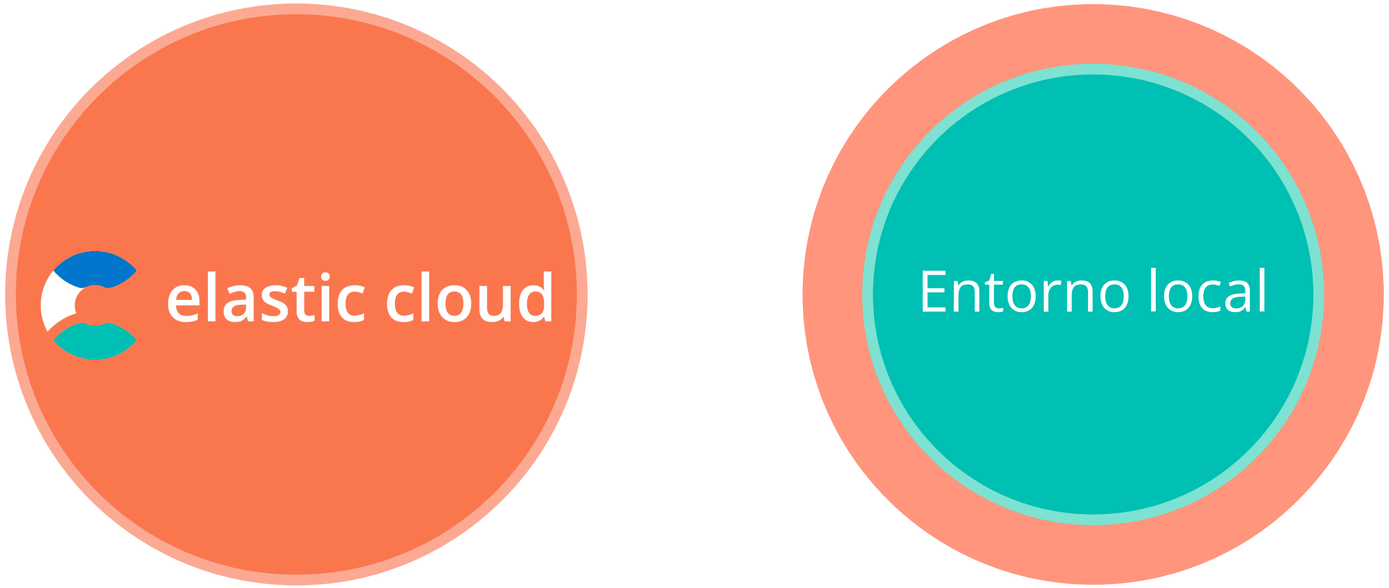
Ingest, Store, Search, Visualise



Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

Dónde podéis ejecutar el laboratorio



Cuenta de prueba en Elastic Cloud

- Crea una cuenta gratuita de dos semanas en **cloud.elastic.co**
- Crear un *deployment* nuevo (**detalles**)
  - los valores por defecto están bien
  - para este taller puedes eliminar del despliegue Integrations Server y Enterprise Search
- Para cargar los datos de prueba (open sky):
  - Puedes subir datos en tiempo real con la imagen docker o script opensky-loader (**detalles**)
  - Puedes usar un **dataset estático** en formato GeoJSON o generar uno nuevo (**detalles**)

Usando Docker Compose en OSGeo Live

- Prerrequisito: instalar Docker y Docker Compose
- Descargar laboratorio: https://github.com/jsanz/elastic-workshop

```
git clone https://github.com/jsanz/elastic-workshop.git
```

- Ajustar parámetros en `.env`
  - Puerto de OpenSky viewer (puerto 80 no disponible en OSGeo Live)
    - `OPENSKY_VIEWER_PORT=8080`
  - (Opcional) contraseñas de usuario
    - `ELASTIC_PASSWORD=changeme`
    - `KIBANA_PASSWORD=changeme`

elastic

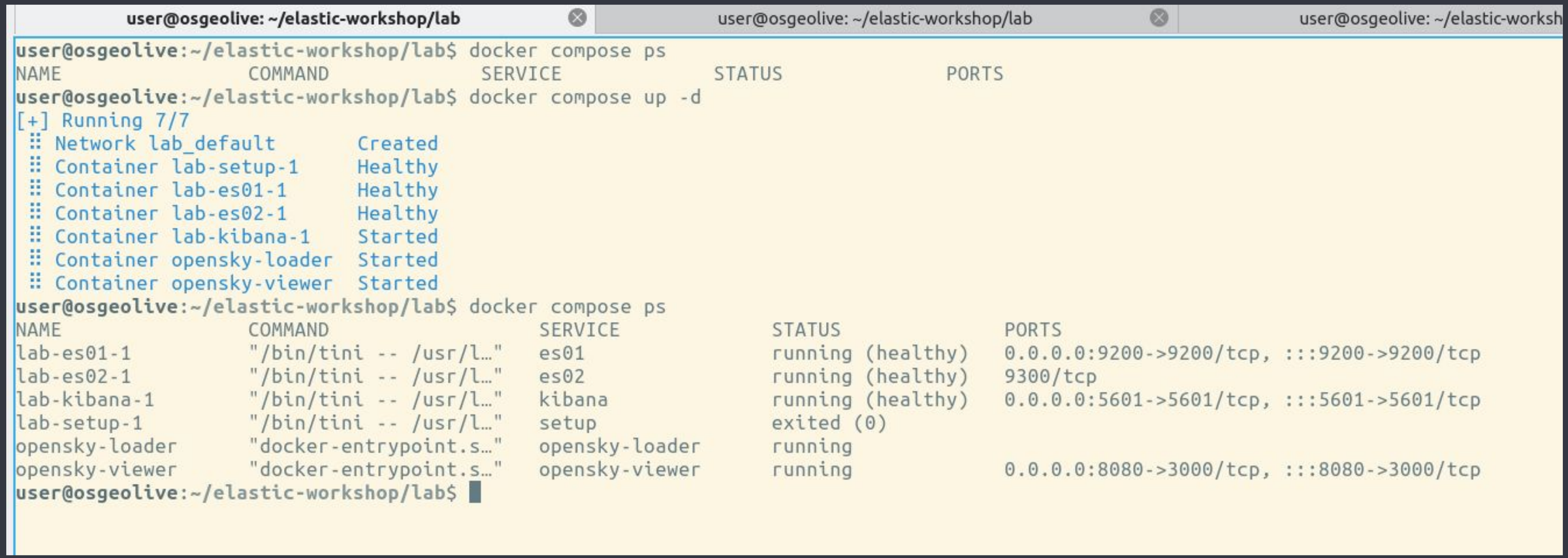
Arrancar aplicaciones


```
$ cd elastic-workshop/lab
$ sudo sysctl -w vm.max_map_count=262144 # ajusta la memoria virtual
$ docker compose pull # descarga las imágenes del stack
$ docker compose build # construye las imágenes opensky
$ docker compose up -d # arranca todos los contenedores
```

Otros comandos útiles

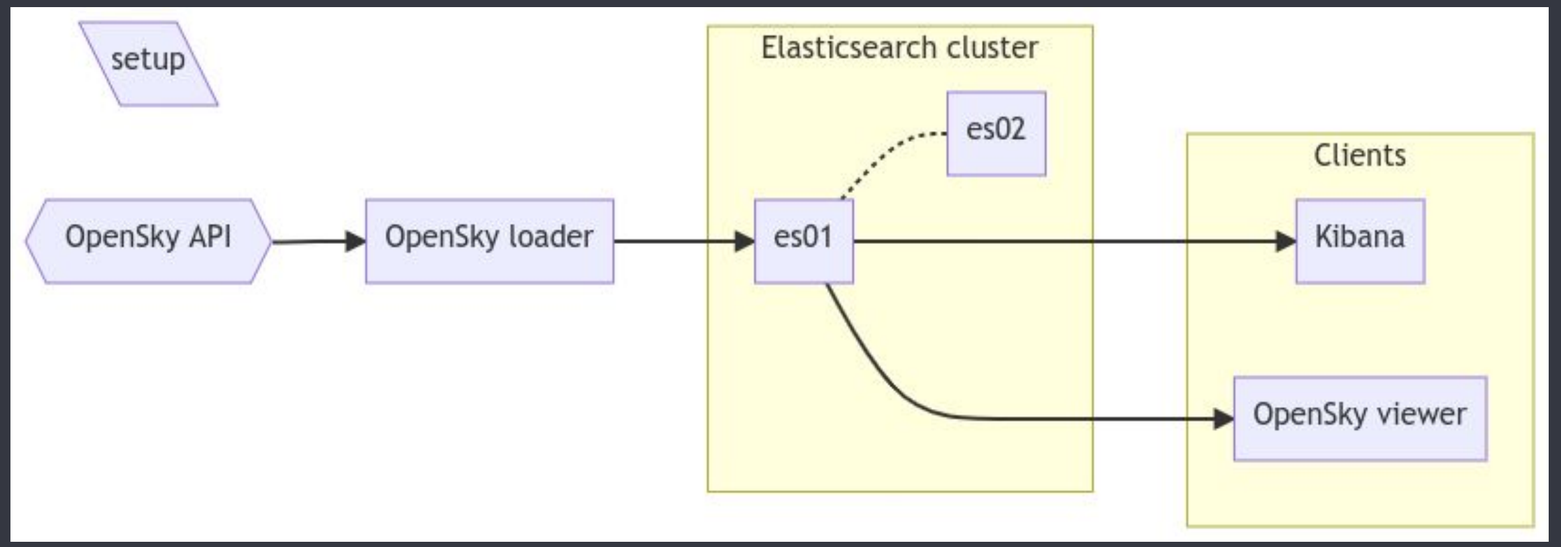
```
$ docker compose ps # muestra información de estado
$ docker compose logs -f kibana # mostrar logs
$ docker compose down # apaga todos los contenedores y servicios
$ docker compose restart opensky-viewer # resetea un contenedor
$ docker compose stop opensky-viewer # para un contenedor
$ docker volume ls # lista los volúmenes (discos duros de docker)
$ docker volume rm [nombre-volume] # borra un volumen
```

Comprobar estado de los contenedores



¿Qué tenemos?

- `es01` y `es02`: cluster de Elasticsearch, `https://localhost:9200`
- `opensky-loader`: cargador de datos
- `kibana`: `http://localhost:5601`
- `opensky-viewer`: visualizador de datos, `http://localhost:8080`



Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

Kibana

Algunos conceptos básicos del funcionamiento de Kibana

Developer Tools

Consola

Permite ejecutar consultas a Elasticsearch con autocompletado, indentación, histórico, etc.

Search profiler

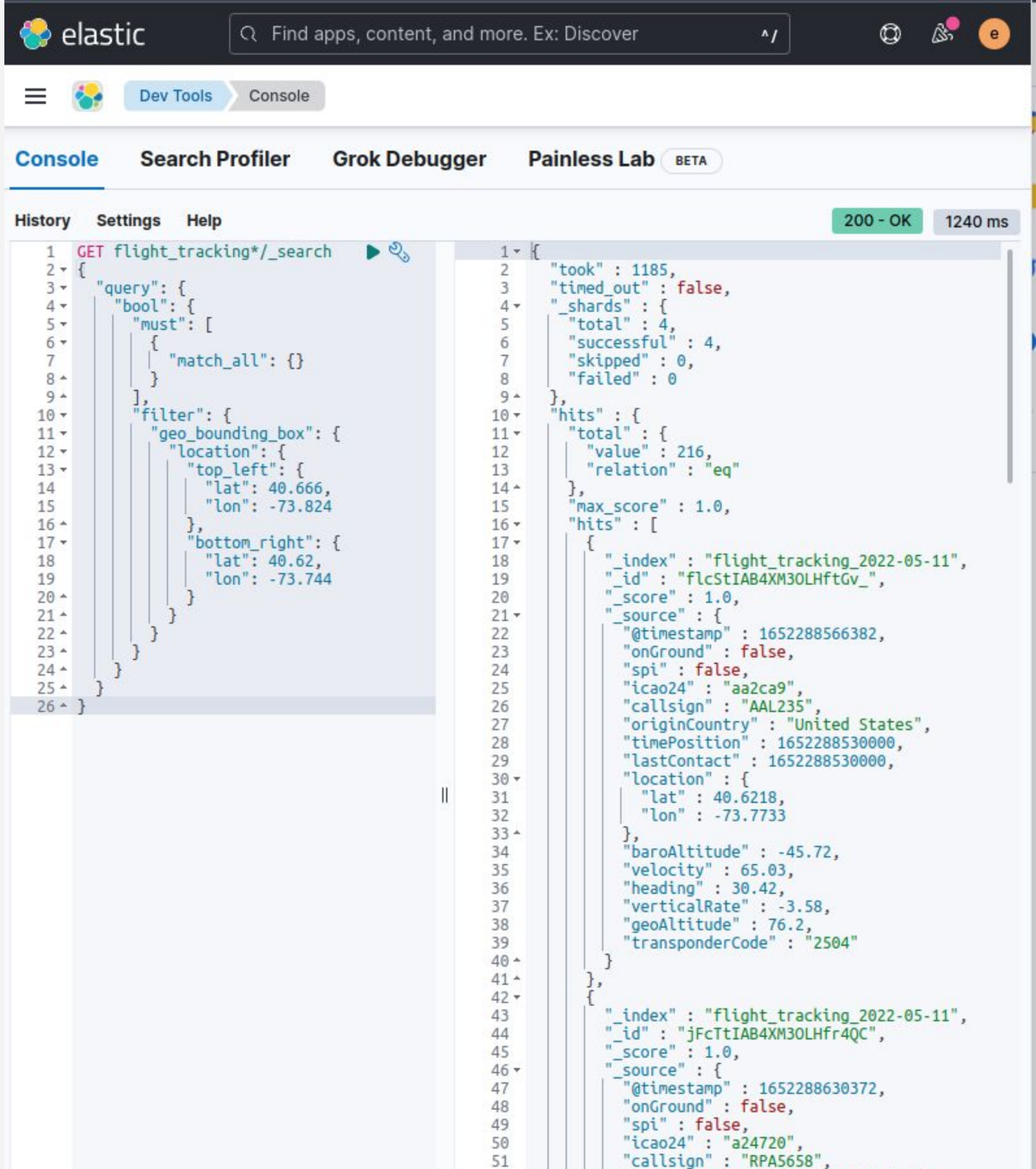
Estadísticas de rendimiento de consultas

Grok debugger

Ayuda para crear expresiones grok para Logstash y otras herramientas de carga

Painless lab

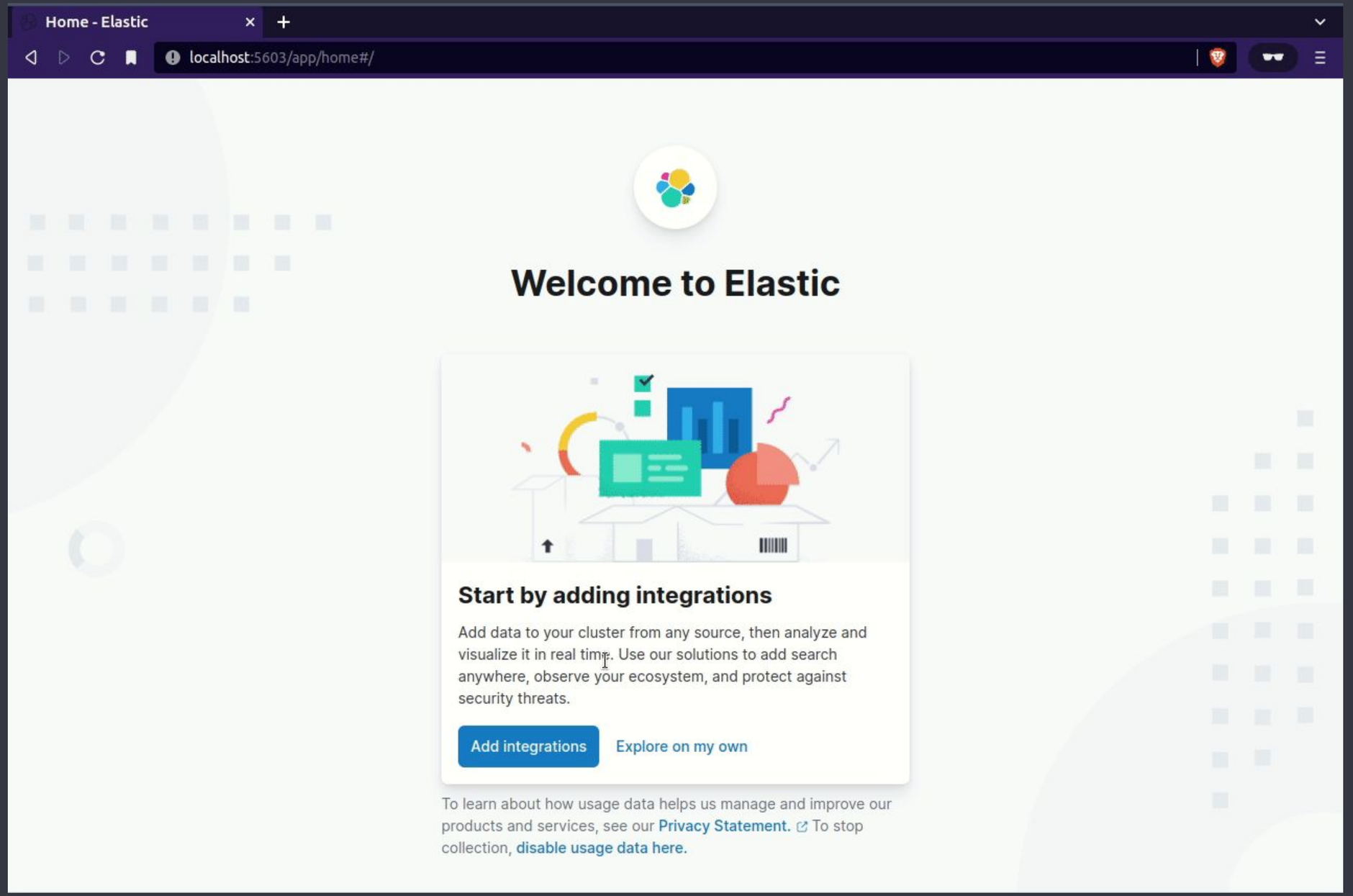
Entorno para probar scripts escritos en painless



Data Views

- Componente lógico que **agrupa** índices usando un **patrón**
  - `my_application_logs_*`
- Definir **formato** a campos: números, monedas, imágenes, URL, ...
- Definir **campo temporal** para filtros (opcional)
- **Campos dinámicos (runtime)** para cálculos en tiempo de consulta

Crear un Data View

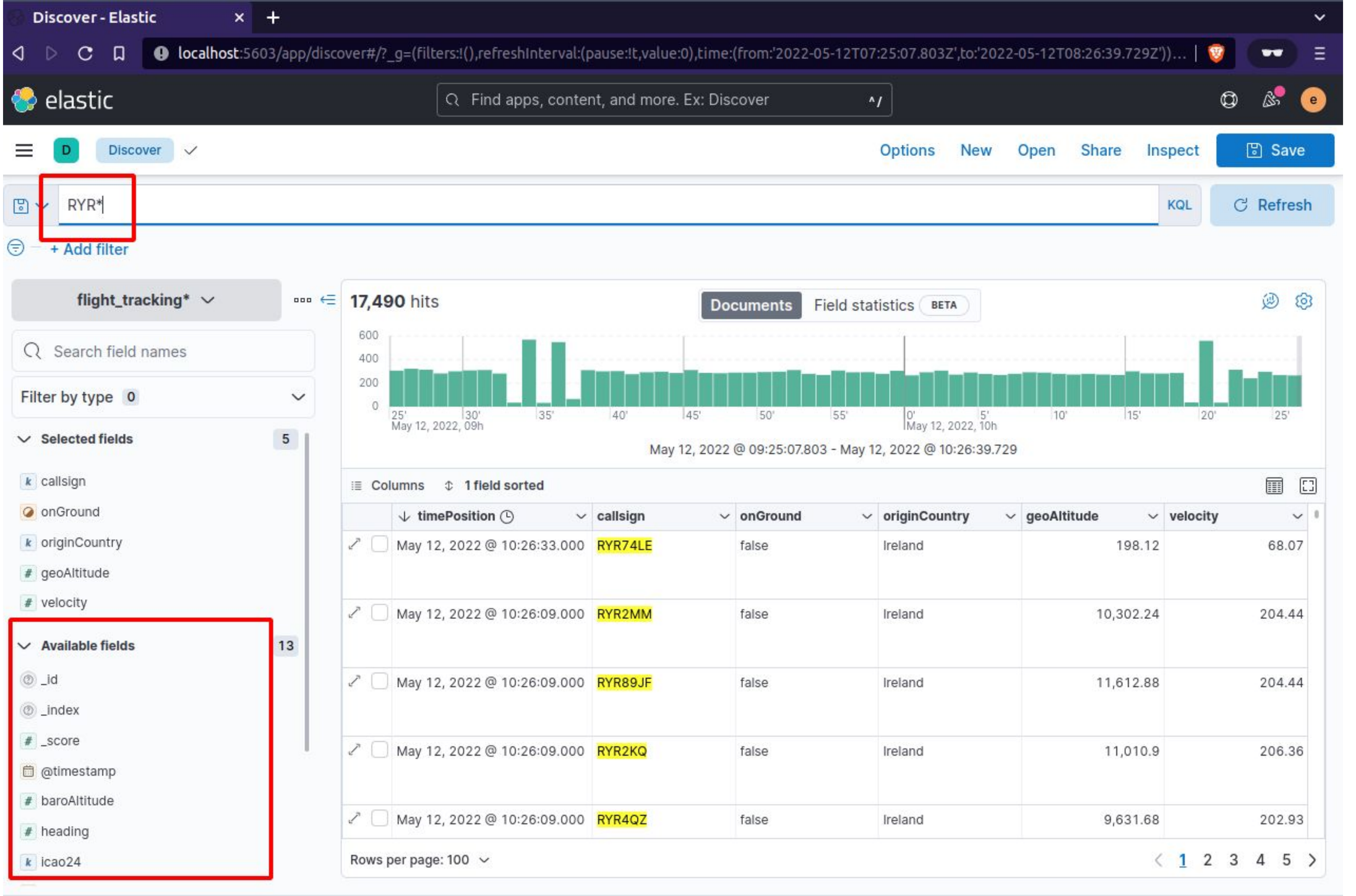


elastic

Discover

- Herramienta de **exploración** rápida
- **Rango temporal** y **actualización** automática*
- **Barra de búsqueda** usando Kibana Query Language o Lucene*
- **Filtros***
- Campos como **columnas**
- **Estadísticas** de los campos
- **Inspect** tool: estadísticas, petición completa y respuesta
- **Guardar** tu búsqueda para usarla más tarde en cuadros de mando

* común a muchos otros elementos de Kibana


Discover - Elastic
localhost:5603/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2022-05-12T07:25:07.803Z',to:'2022-05-12T08:26:39.729Z'))...
elastic
Find apps, content, and more. Ex: Discover
Discover
Options
New
Open
Share
Inspect
Save
RYR*
KQL
Refresh
+ Add filter
flight_tracking*
Search field names
Filter by type 0
Selected fields 5
callsign
onGround
originCountry
geoAltitude
velocity
Available fields 13
_id
_index
_score
@timestamp
baroAltitude
heading
icao24
17,490 hits
Documents
Field statistics
BETA
600
400
200
0
25'
May 12, 2022, 09h
30'
35'
40'
45'
50'
55'
0'
May 12, 2022, 10h
5'
10'
15'
20'
25'
May 12, 2022 @ 09:25:07.803 - May 12, 2022 @ 10:26:39.729
Columns
1 field sorted
timePosition
callsign
onGround
originCountry
geoAltitude
velocity
May 12, 2022 @ 10:26:33.000 RYR74LE false Ireland 198.12 68.07
May 12, 2022 @ 10:26:09.000 RYR2MM false Ireland 10,302.24 204.44
May 12, 2022 @ 10:26:09.000 RYR89JF false Ireland 11,612.88 204.44
May 12, 2022 @ 10:26:09.000 RYR2KQ false Ireland 11,010.9 206.36
May 12, 2022 @ 10:26:09.000 RYR4QZ false Ireland 9,631.68 202.93
Rows per page: 100
1 2 3 4 5

Lens

Tus datos delante tuyo

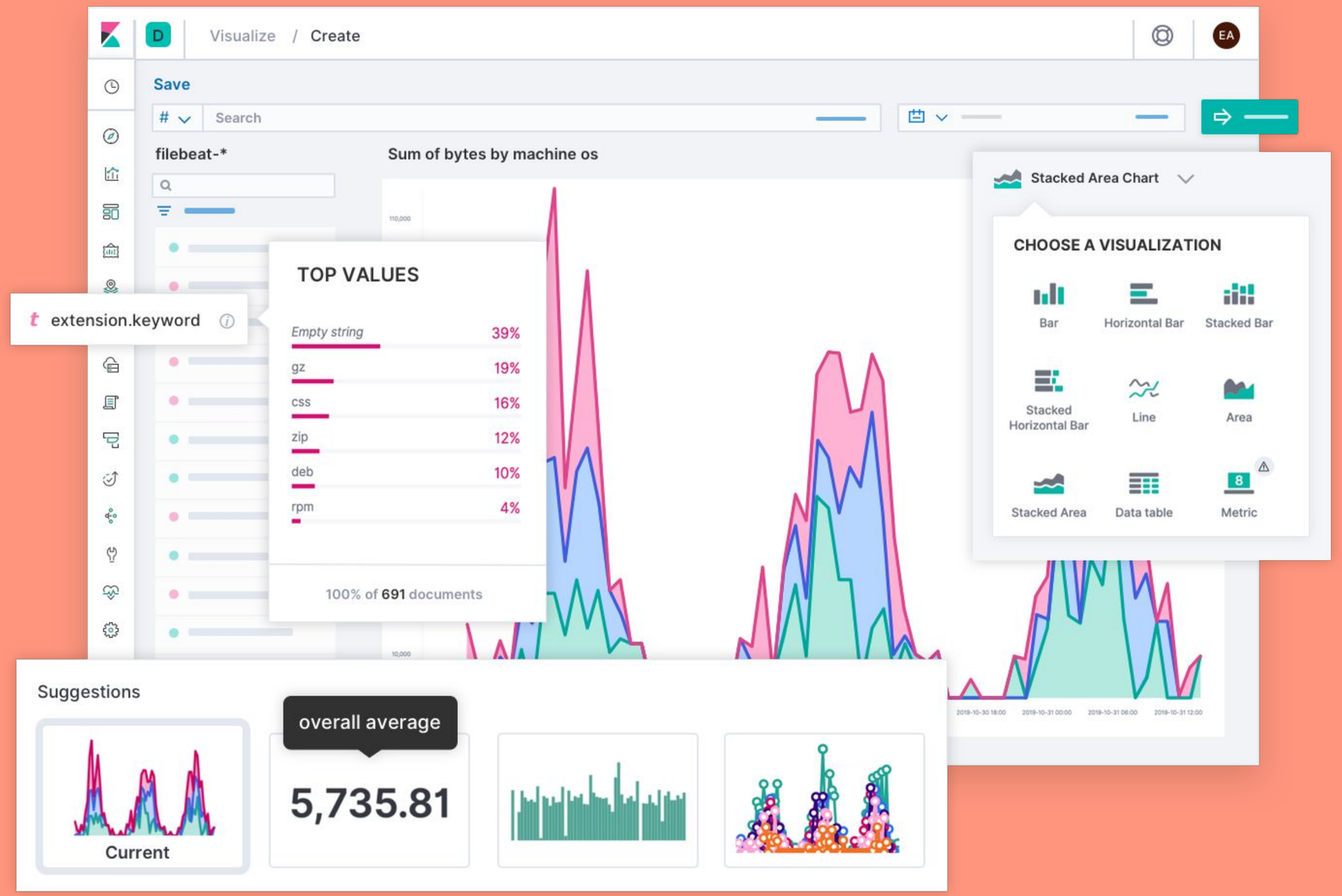
Exploración de campos con un clic

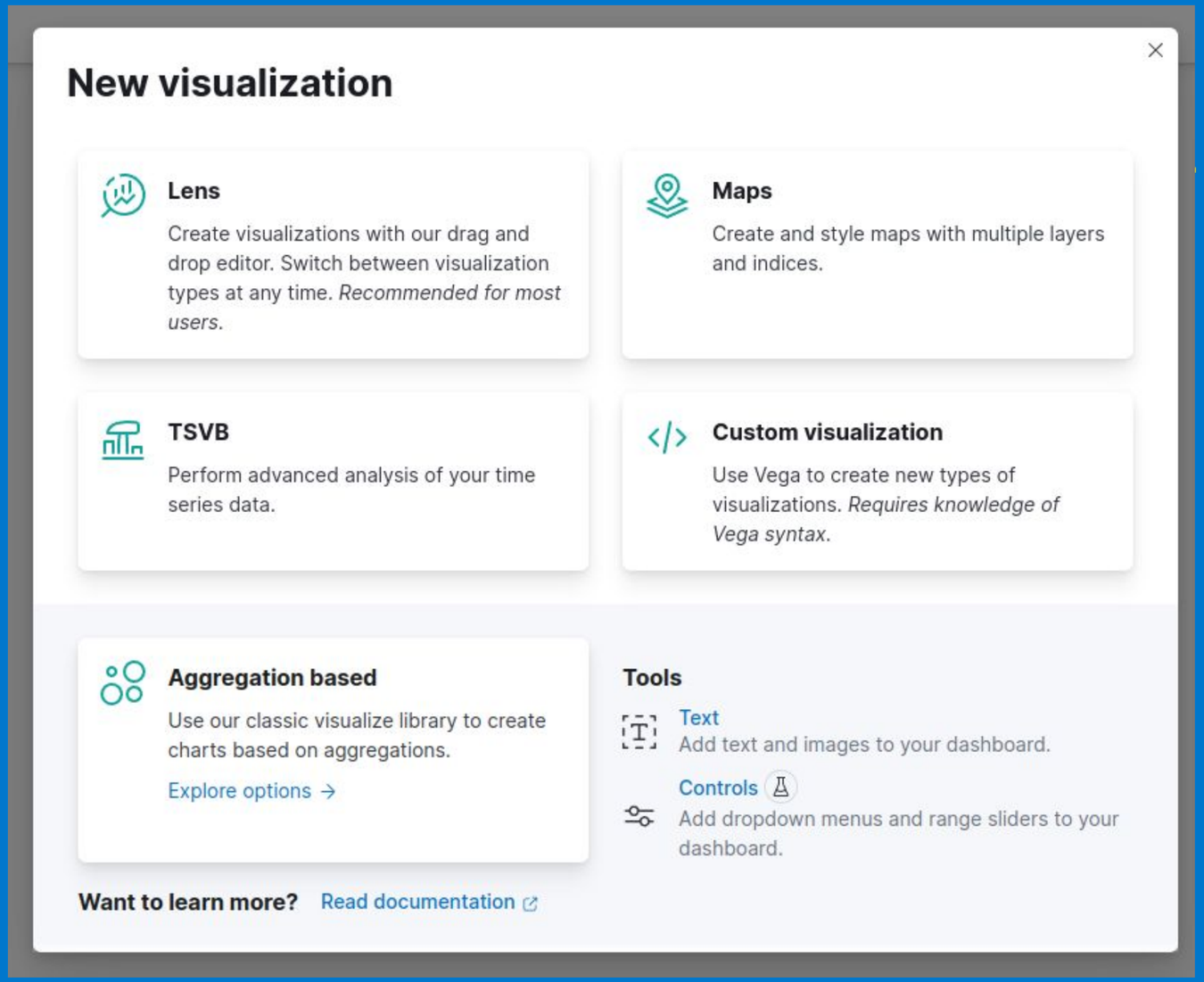
Arrastrar y soltar

De cero a gráficas útiles con un simple gesto de ratón

Sugerencias inteligentes

Lens analiza tus datos y te sugiere gráficas apropiadas a su distribución



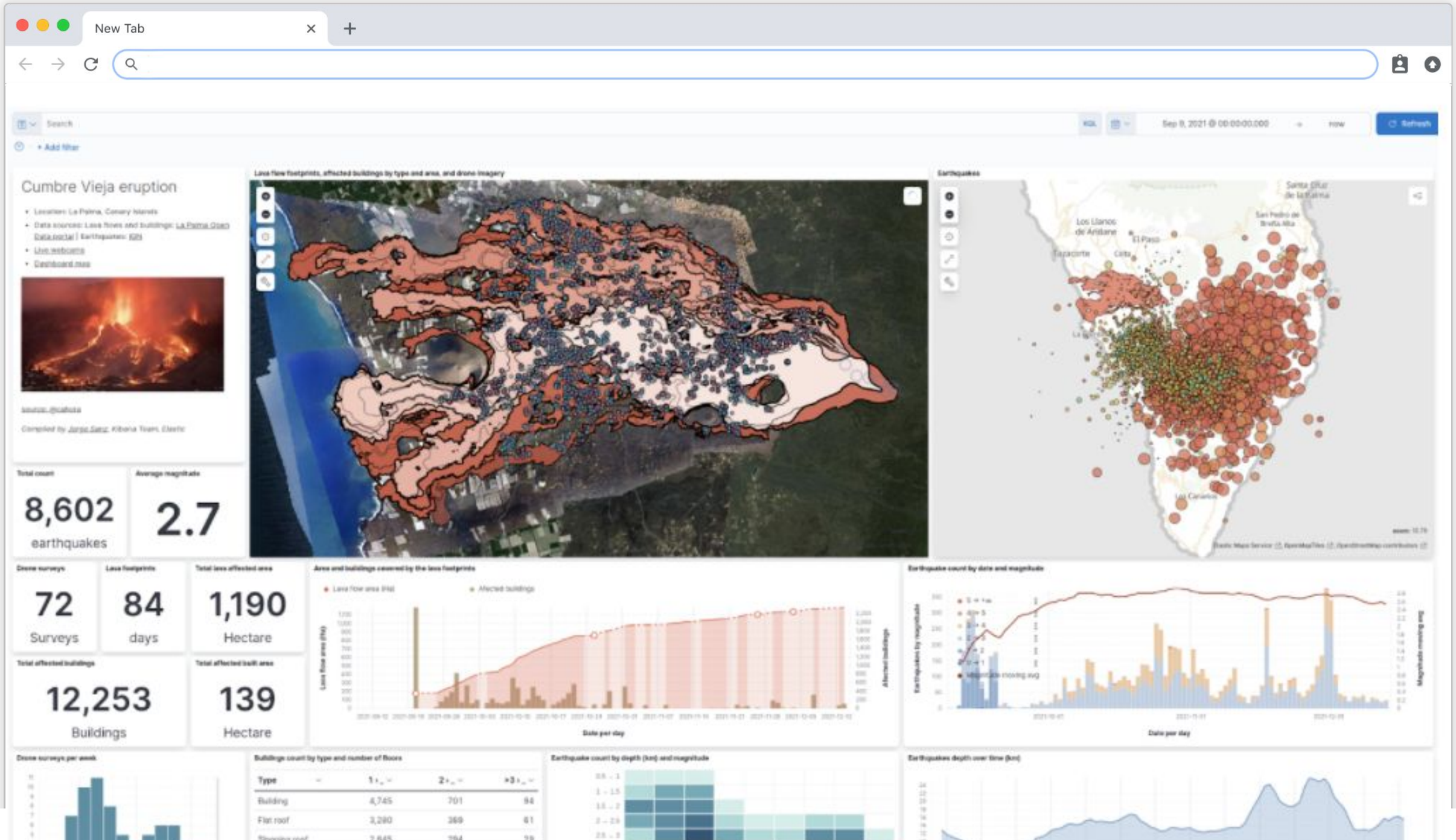


... y más

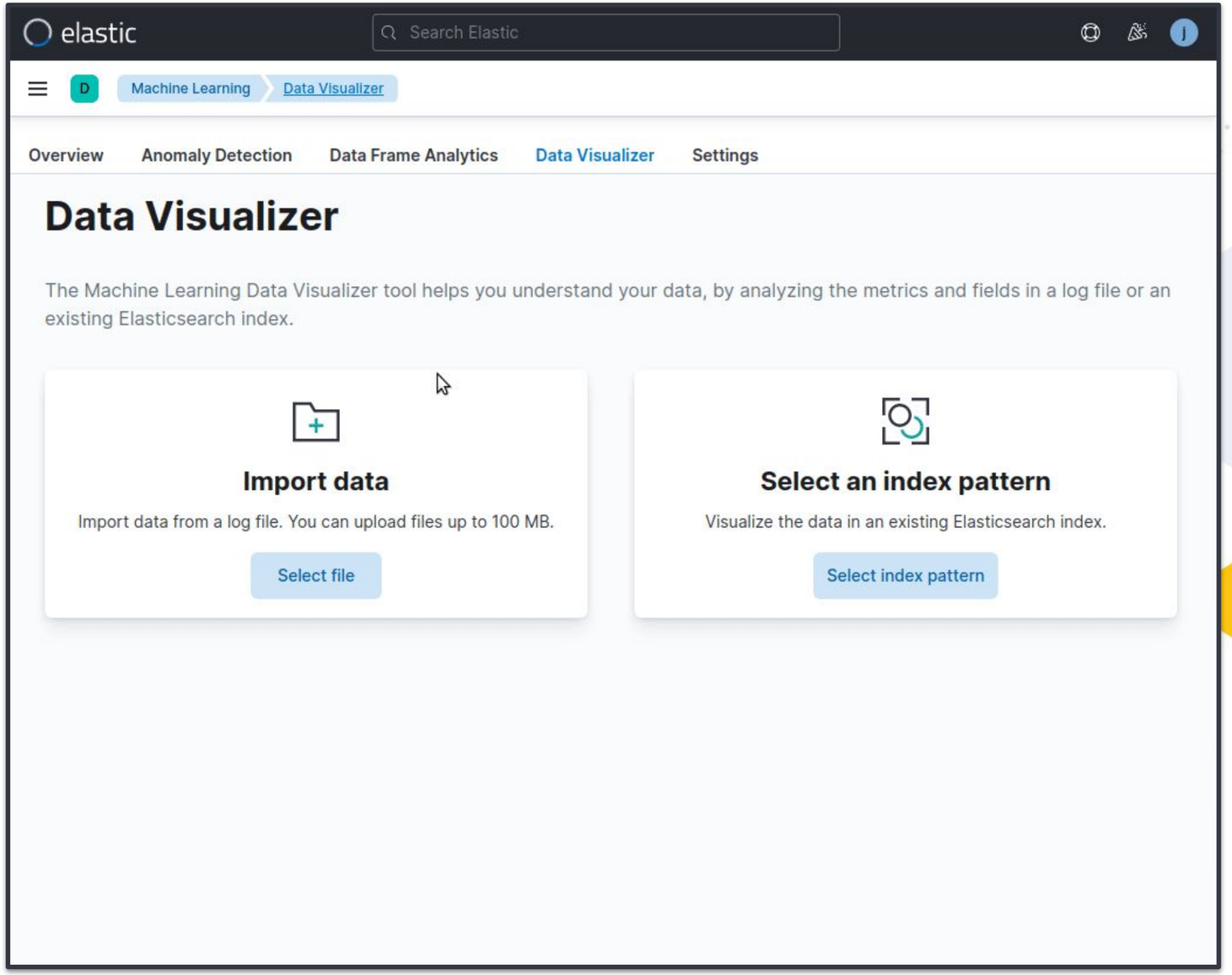
elastic

Dashboards

- Combinación de múltiples visualizaciones: **paneles**
- Time Range + Search Bar + Filters
- Los paneles permiten definir filtros para hacer **drill down**
- Los paneles pueden tener rangos temporales **personalizados**
- **Compartir**
- **Exportar** como PDF o PNG


New Tab
Search
Sep 9, 2021 @ 00:00:00.000
now
Refresh
+ Add filter
Cumbre Vieja eruption
Location: La Palma, Canary Islands
Data sources: Lava flows and buildings: La Palma Open Data portal | Earthquakes: IGN
Live webcams
Dashboard map
source: @cabosa
Compiled by Jorge Sanz, Kibana Team, Elastic
Lava flow footprints, affected buildings by type and area, and drone imagery
Earthquakes
Los Llanos de Aridane
El Paso
Tazacorte
Tijarafe
Santa Cruz de la Palma
San Pedro de Breña Alta
Total count
8,602
earthquakes
Average magnitude
2.7
Drone surveys
72
Surveys
Lava footprints
84
days
Total lava affected area
1,190
Hectare
Total affected buildings
12,253
Buildings
Total affected built area
139
Hectare
Area and buildings covered by the lava footprints
Lava flow area (Ha)
Affected buildings
Date per day
Earthquake count by date and magnitude
Earthquakes by magnitude
Magnitude moving avg
Date per day
Drone surveys per week
Buildings count by type and number of floors
Type
1
2
>3
Building
4,745
701
94
Flat roof
3,280
369
61
Earthquake count by depth (km) and magnitude
Earthquakes depth over time (km)

Ingest with Kibana: CSV file upload



elastic

Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

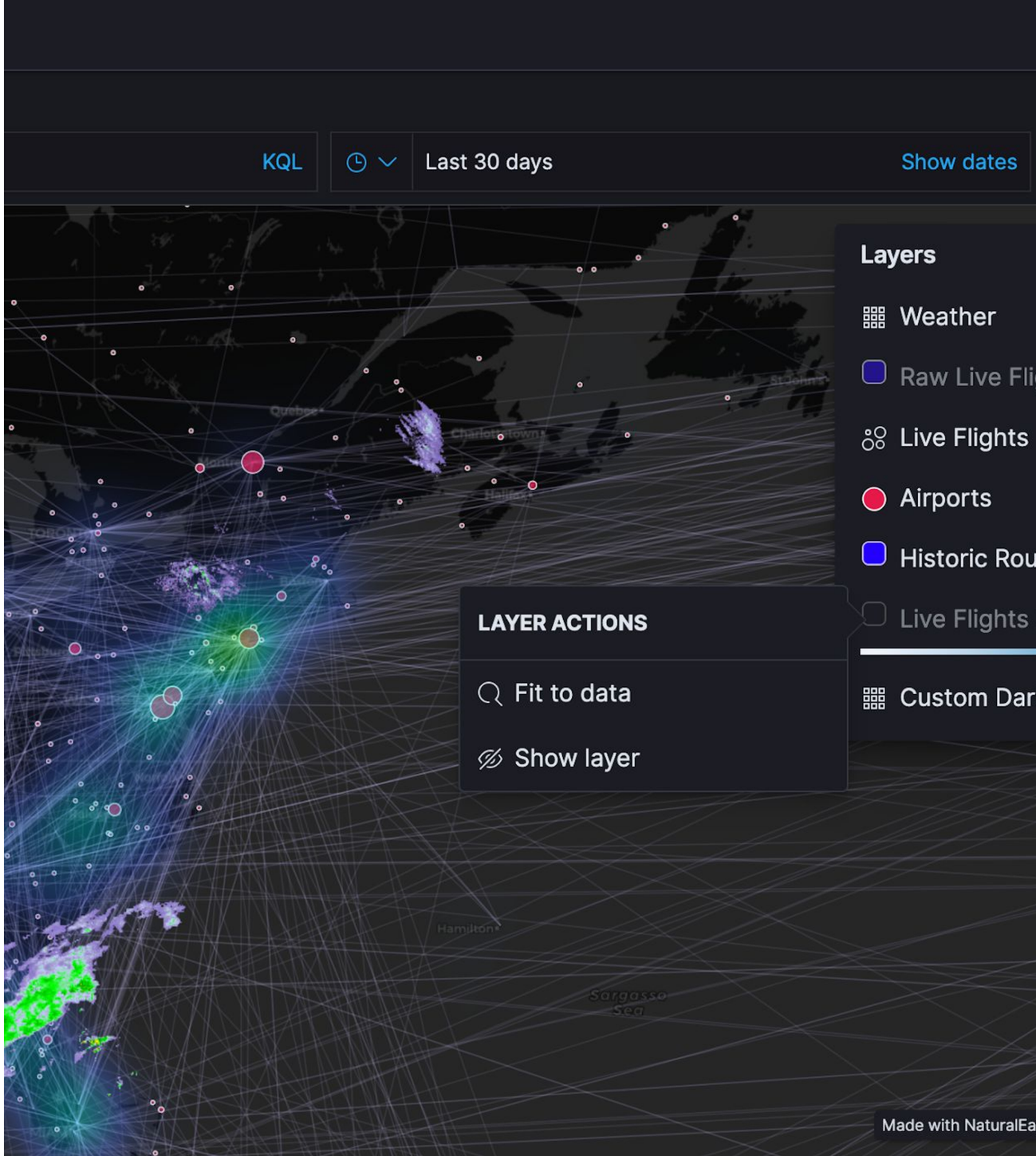
Elastic Maps

Acercando los Sistemas de Información Geográfica a Kibana

elastic

Elastic Maps

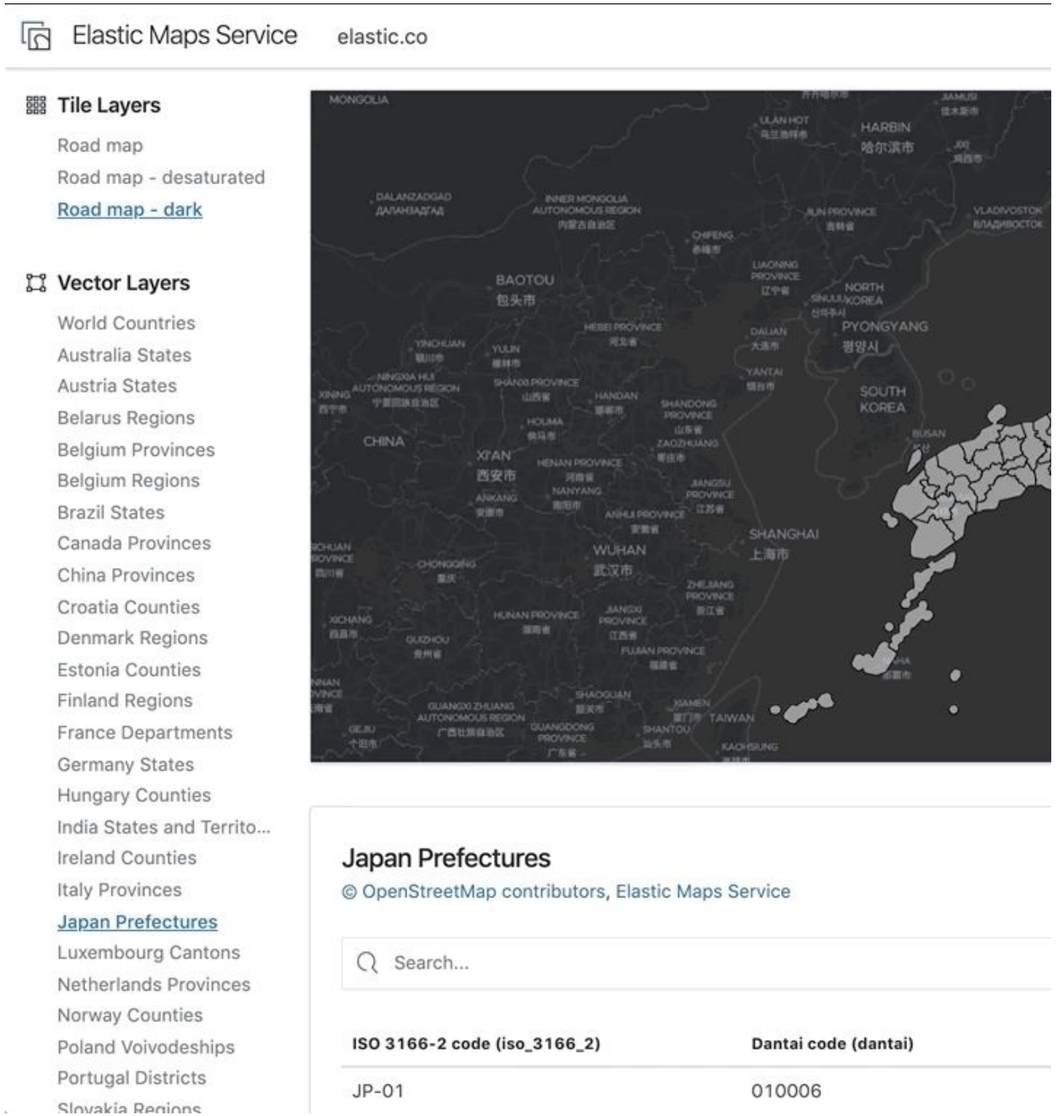
- Interfaz amigable
- MapLibre
- `geo_point` y `geo_shape`
- Agregaciones: heat map, clustering, grids, geoline
- Estilos desde los datos
- Herramientas para dibujar, filtrar, medir
- Uso independiente o en dashboards y canvas
- Componente para otras aplicaciones de Kibana



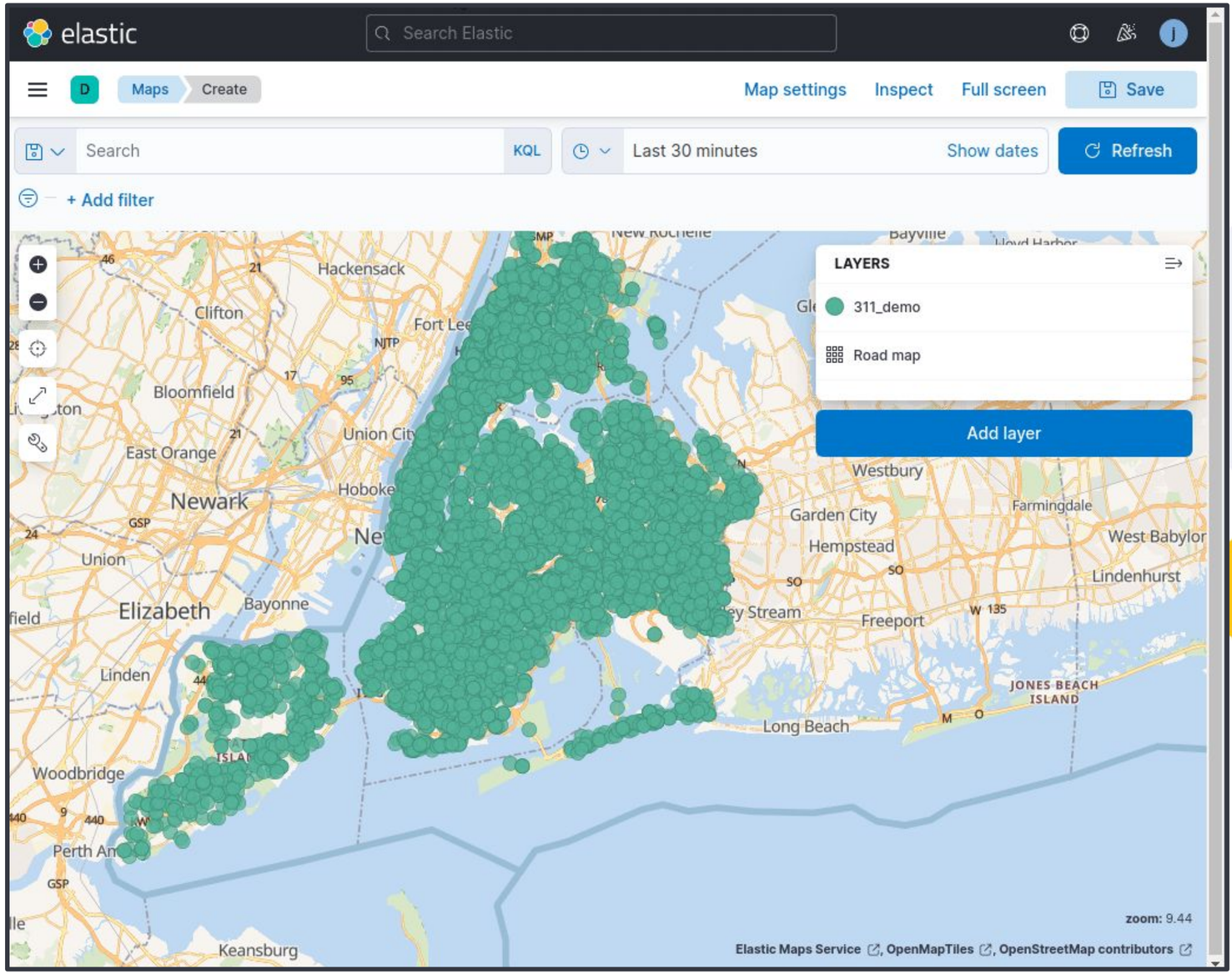
Elastic Maps Service

maps.elastic.co

- 18 niveles de zoom
  - Mapas de todo el mundo o de tu ciudad
- Tres estilos de mapas base
  - Muestra tus datos sobre un mapa base claro, oscuro, o colorido
- Límites Administrativos
  - Más de 60 capas de regiones administrativas de países de todo el mundo



Ingest with Kibana: GeoJSON and Shapefile upload



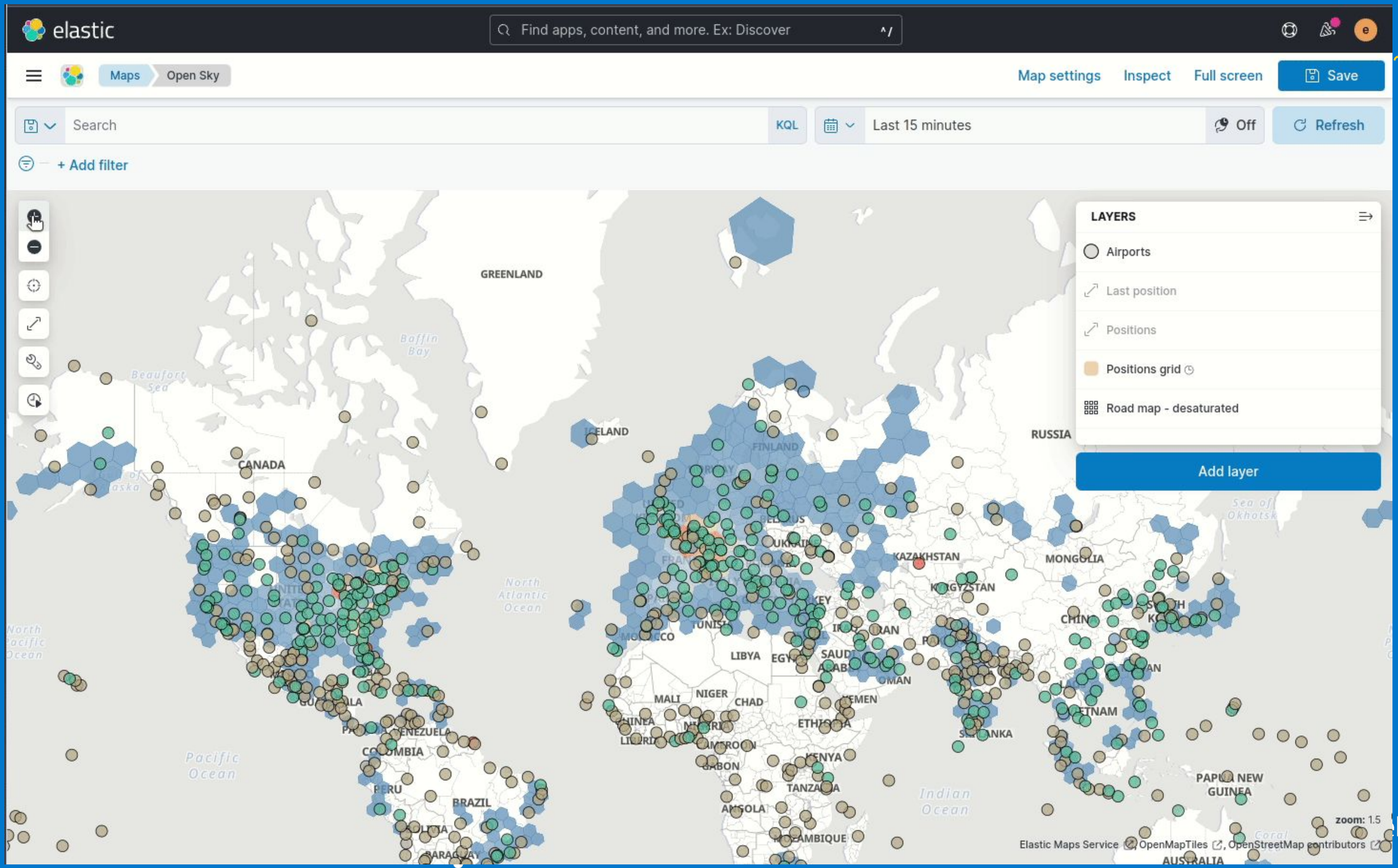
- Docs 📖
- Tutorial 📖

elastic

Hora de practicar

- Crea un **mapa** nuevo
- Sube datos a tu *cluster*
  - **Aeropuertos** (desde DevTools o GeoJSON detalles)
  - **Posiciones** (vía cargador o fichero estático)
- Capa **aeropuertos**
- Capa de **grid (hex, tile o cluster) de posiciones** (zoom 0 a 6)
- Capa de **posiciones individuales** (zoom 7 en adelante)
- Añadir **tooltips**, jugar con la **simbología**, etc
- Añadir capa con la agregación de línea (**tracks**)

elastic


elastic
Find apps, content, and more. Ex: Discover
Maps
Open Sky
Map settings
Inspect
Full screen
Save
Search
KQL
Last 15 minutes
Off
Refresh
+ Add filter
LAYERS
Airports
Last position
Positions
Positions grid
Road map - desaturated
Add layer
GREENLAND
CANADA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
LIBYA
MALI
NIGER
CHAD
KENYA
TANZANIA
ANGOLA
BRAZIL
PERU
COLOMBIA
VENEZUELA
Pacific Ocean
North Atlantic Ocean
Indian Ocean
Baffin Bay
Beaufort Sea
Sea of Okhotsk
zoom: 1.5
Elastic Maps Service
OpenMapTiles
OpenStreetMap contributors

Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

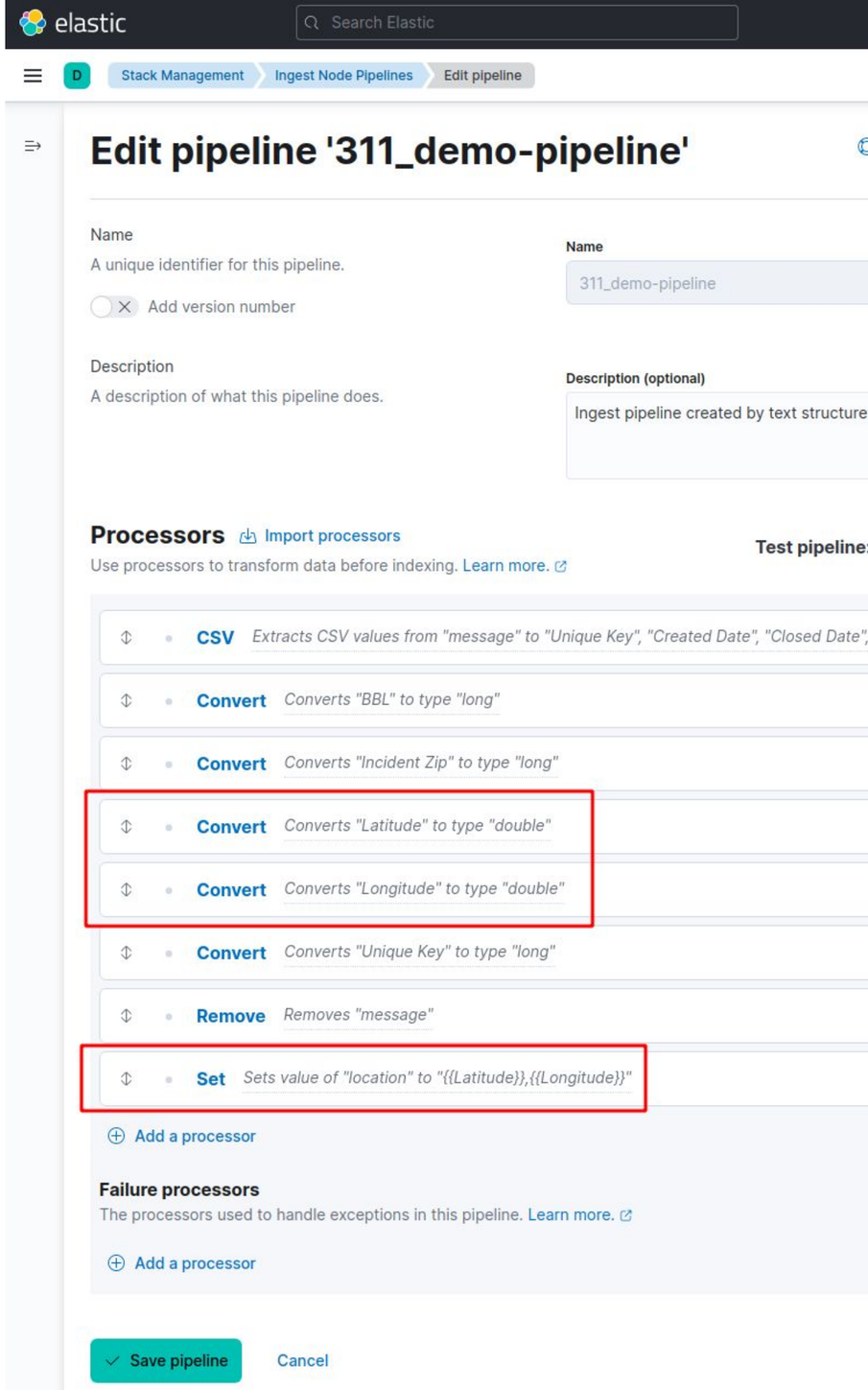
Elasticsearch geospatial data types

- `geo_point` 📖
  - A single pair of latitude and longitude **coordinates**
  - Can be inserted as an object, WKT, array, geohash
- `geo_shape` 📖
  - Supports any **lat/lon** geometry type, incl. envelope and circle
  - Inserted with GeoJSON or WKT notation
- `shape` 📖
  - Supports any **cartesian** geometry type
  - Inserted with GeoJSON or WKT notation

Geo Enrichment

Adding a geo dimension to your data

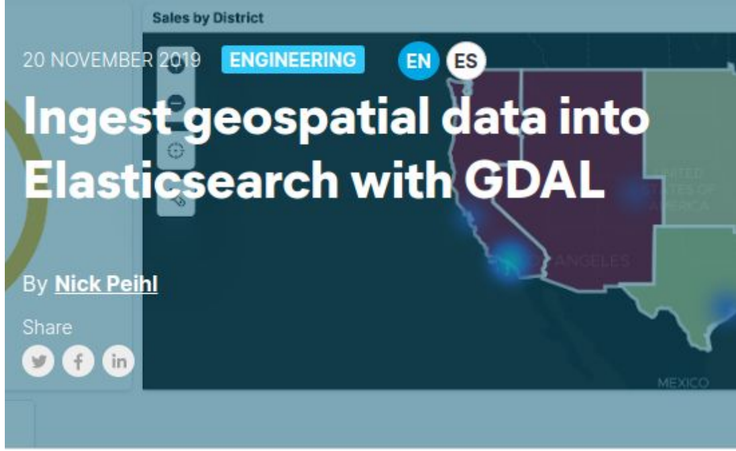
- Transform data at ingest time
- Enrich IP addressed with estimated location
- Lookup location based on another index e.g. postcodes
- Tag documents by matching with polygons in another index e.g. local authority boundaries
- Convenient UI in Kibana



Ingest with ogr2ogr

https://gdal.org/drivers/vector/elasticsearch.html

- `ogr2ogr` can read and write into Elasticsearch
- Support for custom mapping definitions
- Blog posts:
  - How to ingest geospatial data into Elasticsearch with GDAL
  - Import OSM data into Elasticsearch with ogr2ogr and Docker



Have you used **Elastic Maps** in Kibana yet? I am very excited about mu
layer support. Heat maps, vector layers from the Elastic Maps Service,
individual documents all in the same interface! What a fantastic way to
and visualize your data.

But what about geospatial data that's not in Elasticsearch? Maybe you
overlay a shapefile of regional sales territories with sales aggregations.
you have a CSV file of distribution center locations, and you want to ge
data into Elasticsearch, but configuring Filebeat or Logstash is not idea
ingesting static datasets. Well, we have the perfect solution for you: GD

GDAL (Geospatial Data Abstraction Library) contains command line too
can convert geospatial data between over 75 different geospatial file fo
including **Elasticsearch**. GDAL can be **compiled from source** or **install**
package managers. GDAL can also be installed via **Homebrew OSGeo**
(ex. `brew tap osgeo/osgeo4mac && brew install osgeo-gdal`). Note, yo
have GDAL v3.1 or later to ingest data into Elasticsearch 7.x.

Connecting to Elasticsearch

Once you've installed GDAL, open your command line or terminal windo
try connecting to your Elasticsearch cluster using the `ogrinfo` tool. We
the URL with "ES:" to tell GDAL to use the Elasticsearch driver.

```
ogrinfo ES:http://localhost:9200
```

Search

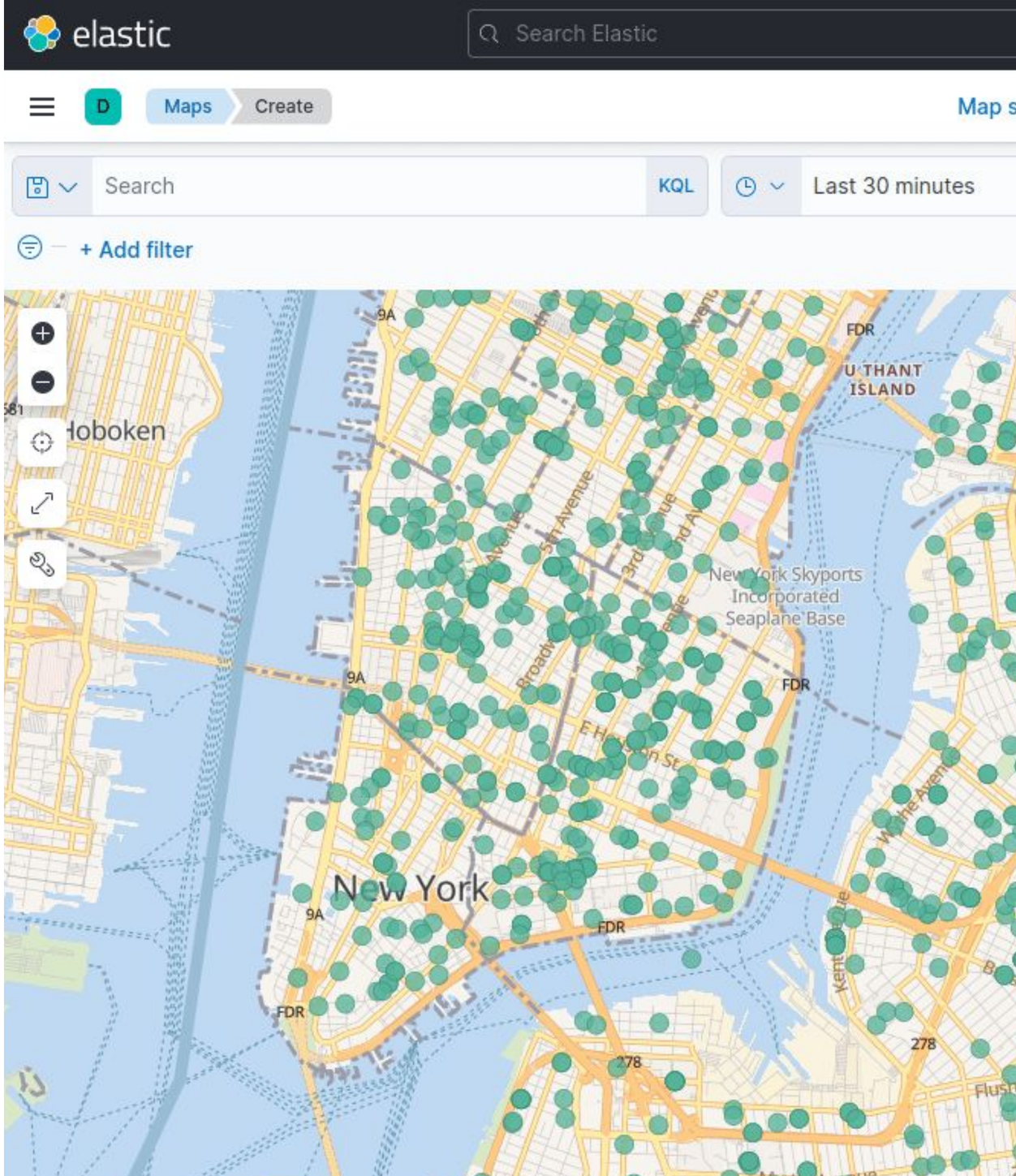
Filter documents with geospatial relationships

Geo Filters

- Bounding box
- Point and radius
- Polygon
- An indexed geo_shape

Plus every other Elasticsearch filter

- Boolean
- Range (numeric, date, IP)
- Unstructured text (stemming, fuzzy ...)



Aggregate

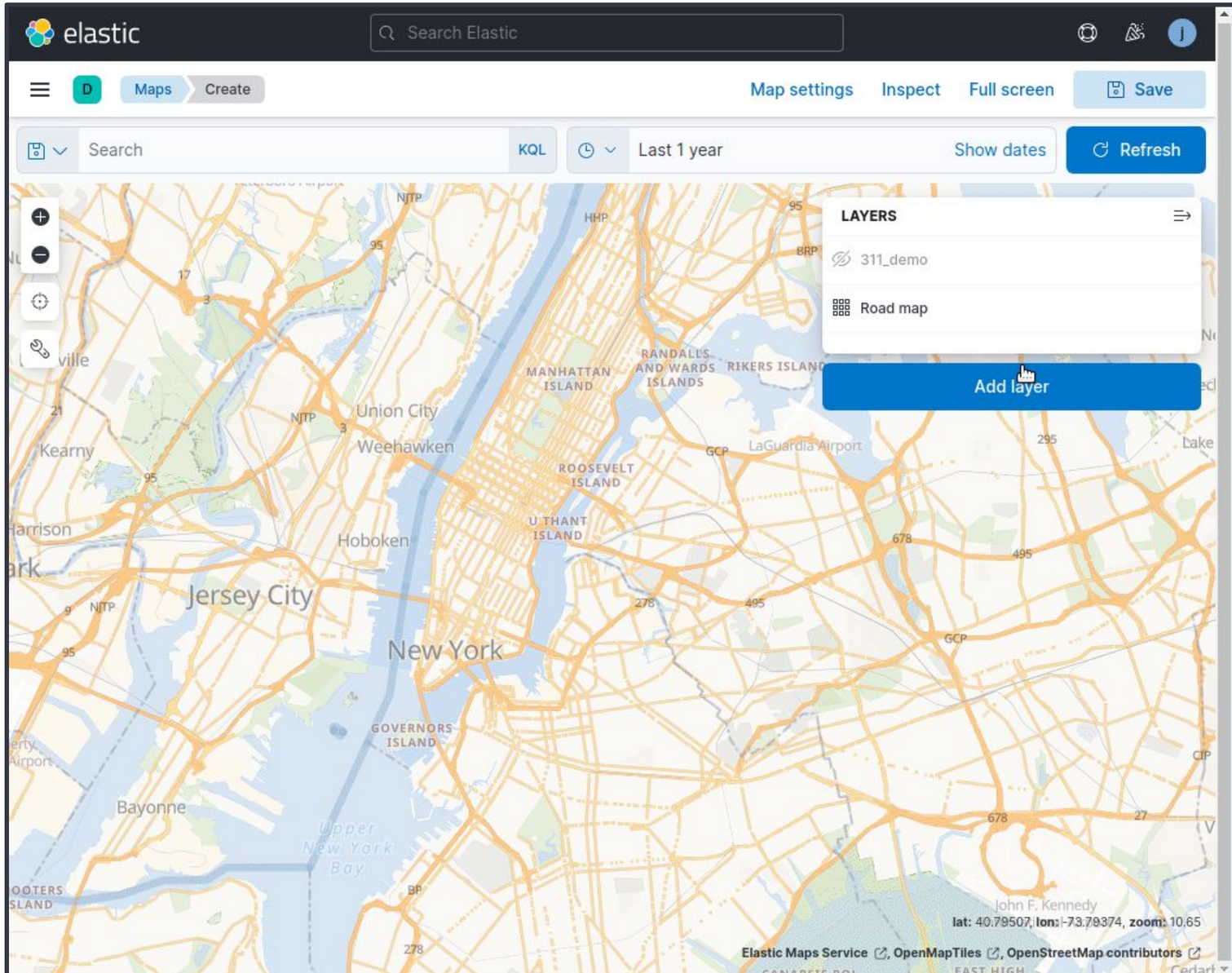
Geo Bucket

- Distance (rings) 📖
- Hash 📖
- Geotile 📖
- Geohex 📖

Geo Metric

- Centroid 📖
- Bounds 📖
- Geoline 📖

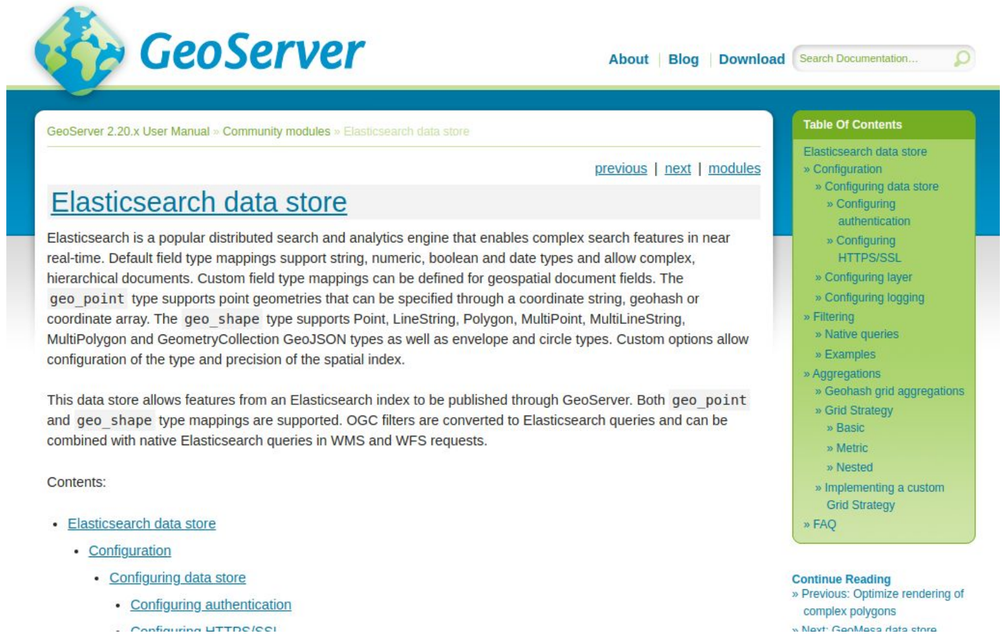
Many more 📖



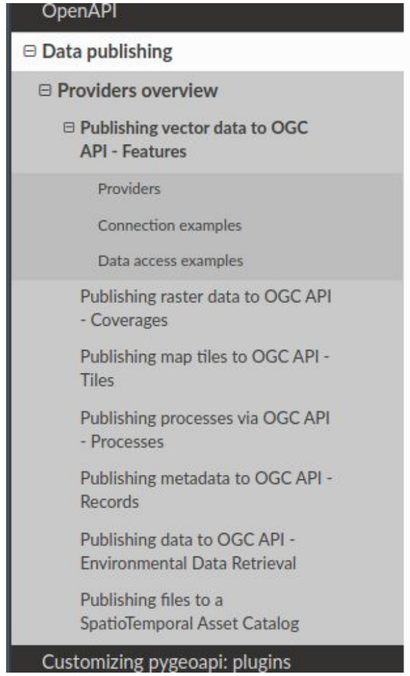
OGC servers and Elasticsearch

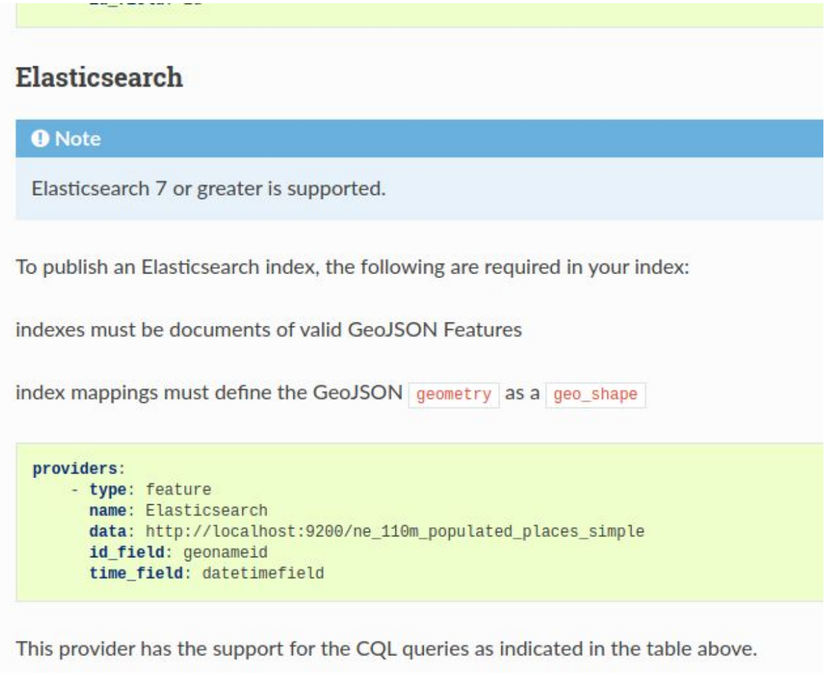
Expose Elasticsearch indices as OGC services

GeoServer



pygeoapi





elastic

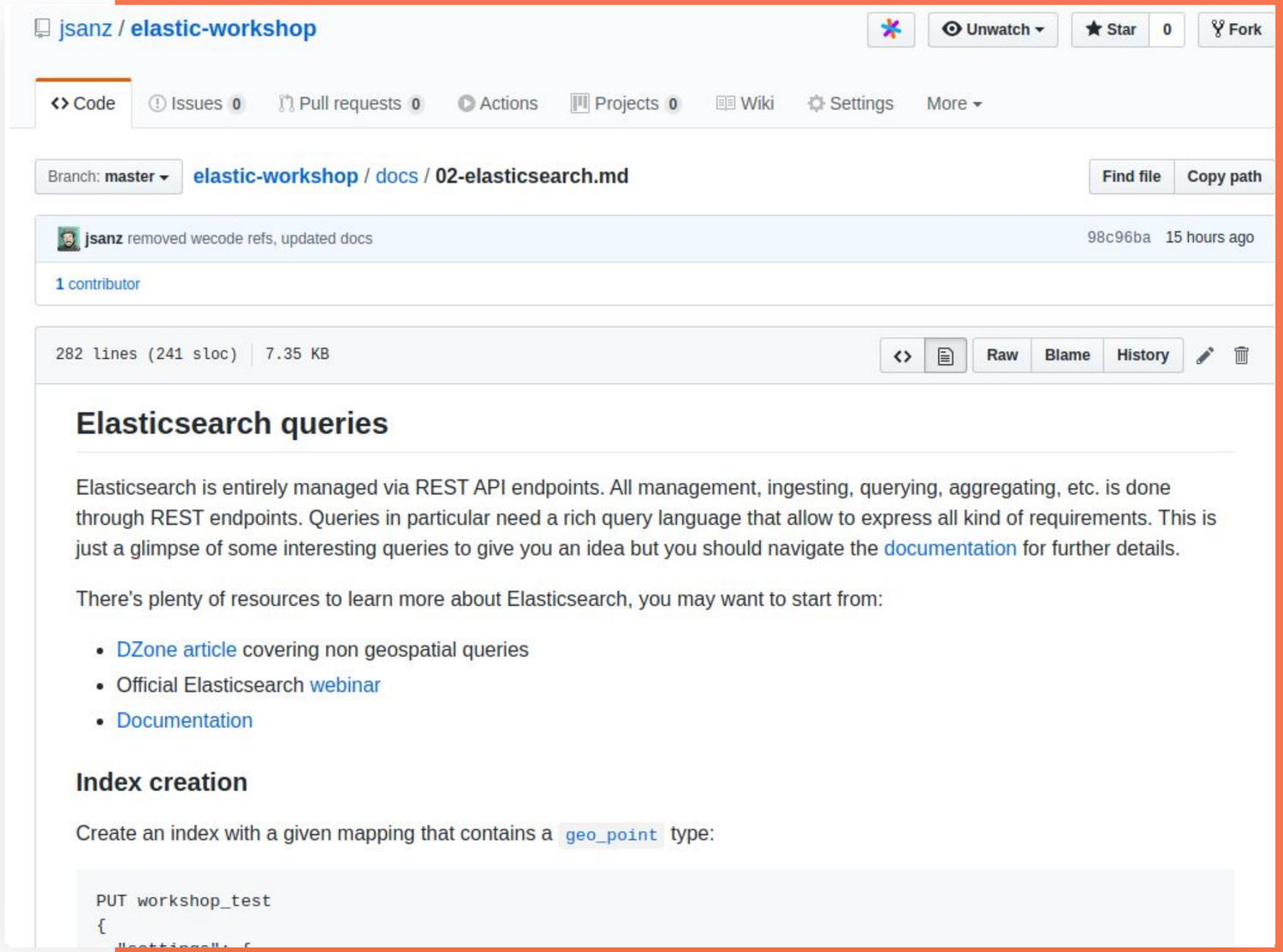
Hora de practicar

- Accede a las Dev Tools de Kibana
- Prueba las diferentes consultas del guión
    - Consultas básicas con Elasticsearch
    - Consultas geoespaciales

elastic

DSL Elasticsearch

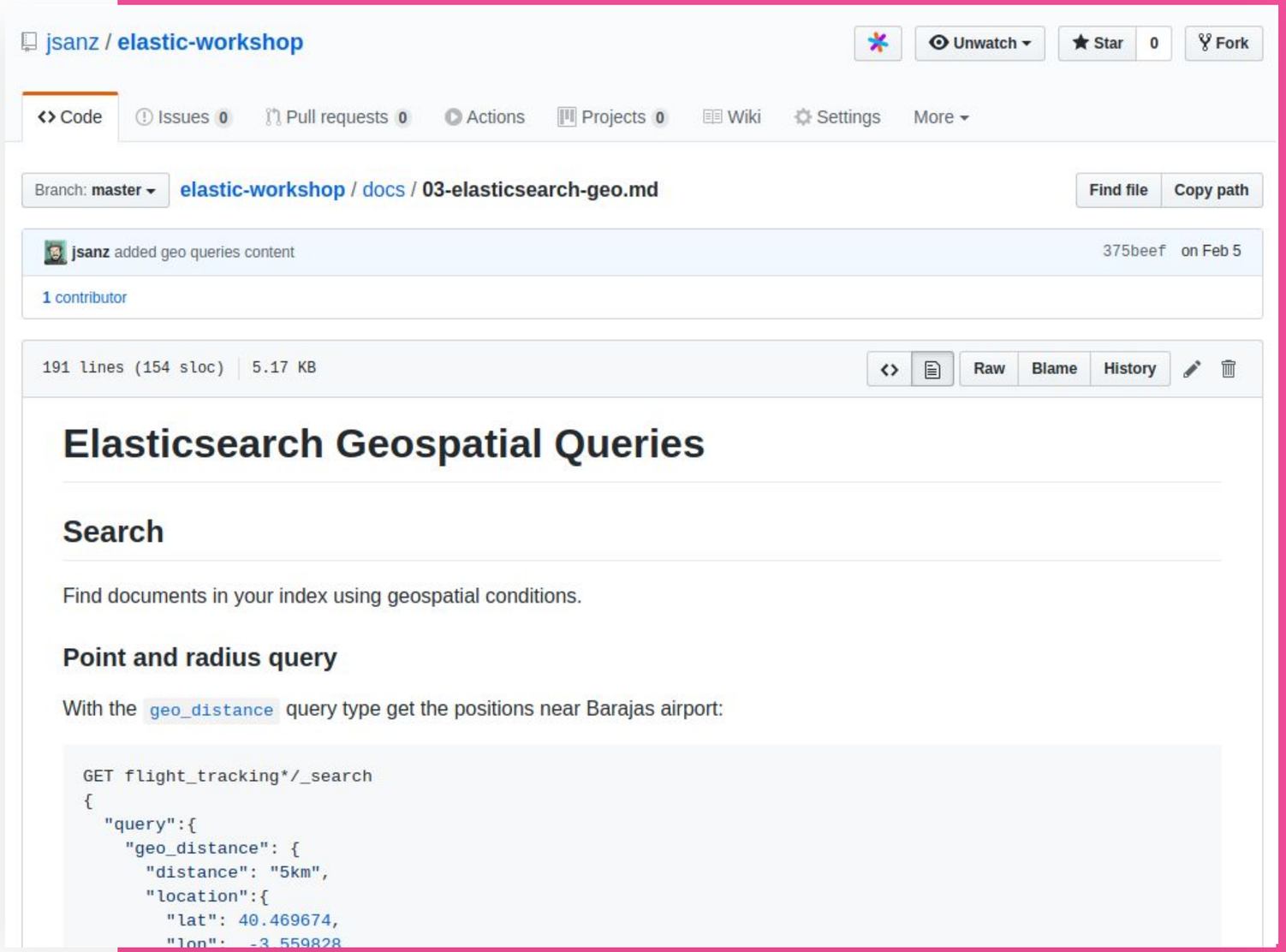
- Kibana DevTools Console
  - curl, postman, ...
- Crear índices
  - Definir tipos, incluyendo campos geoespaciales
- Insertar
  - Añadir datos a tu índice
- Búsquedas
  - Obteniendo documentos
- Agregaciones
  - Agrupa tus datos



Elasticsearch geo

Consultas geoespaciales

- Búsquedas
  - Encontrar documentos por punto/radio, bounding box, polígonos arbitrarios
- Agregación de métricas
  - Encontrar el centroide o la caja envolvente de tu búsqueda
- Agregación en grupos
  - Agrupa tus resultados por características geográficas como anillos o cuadrículas

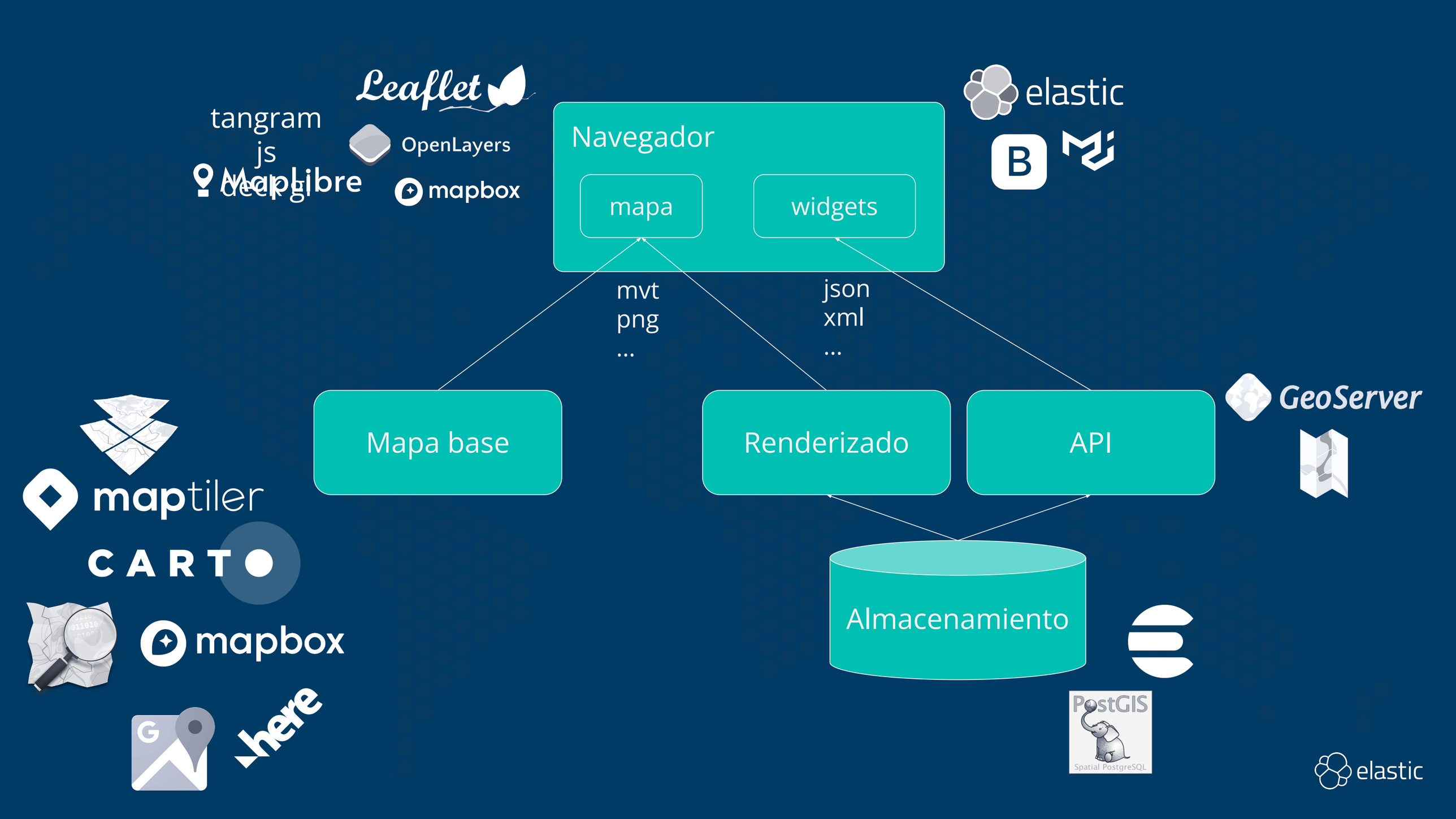


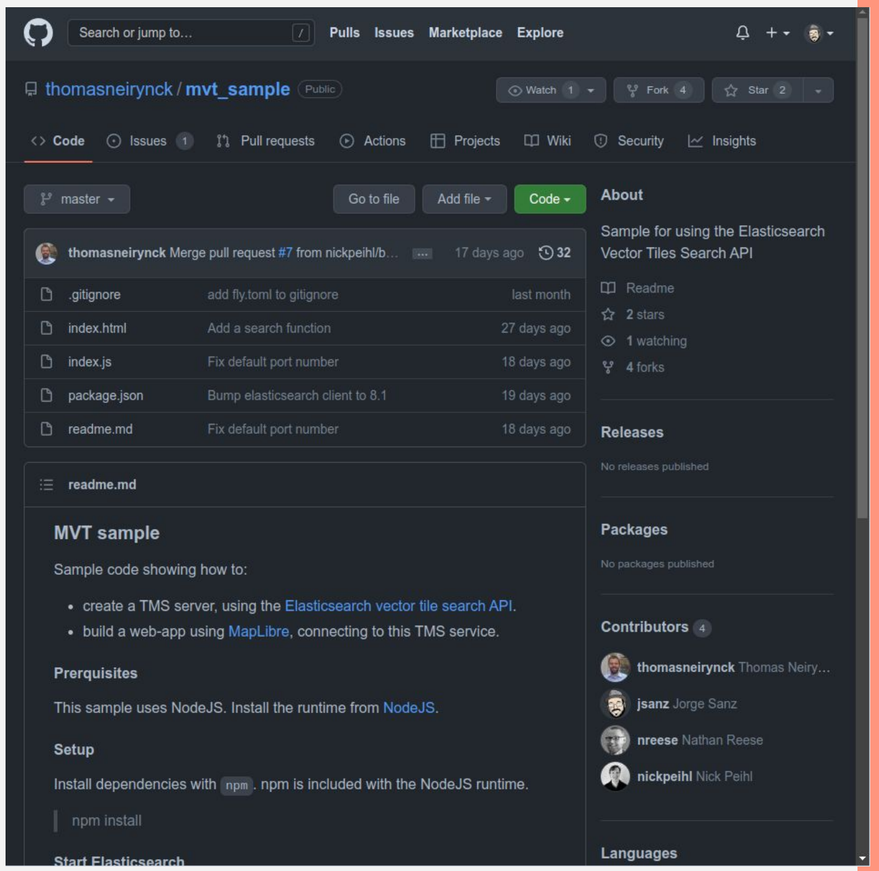
Agenda

1. Introducción al stack de Elastic
2. Preparación del laboratorio
3. Introducción a Kibana
4. Elastics Maps
5. Elasticsearch Geo
6. Web mapping con Elasticsearch

Pequeña intro al *webmapping*

elastic

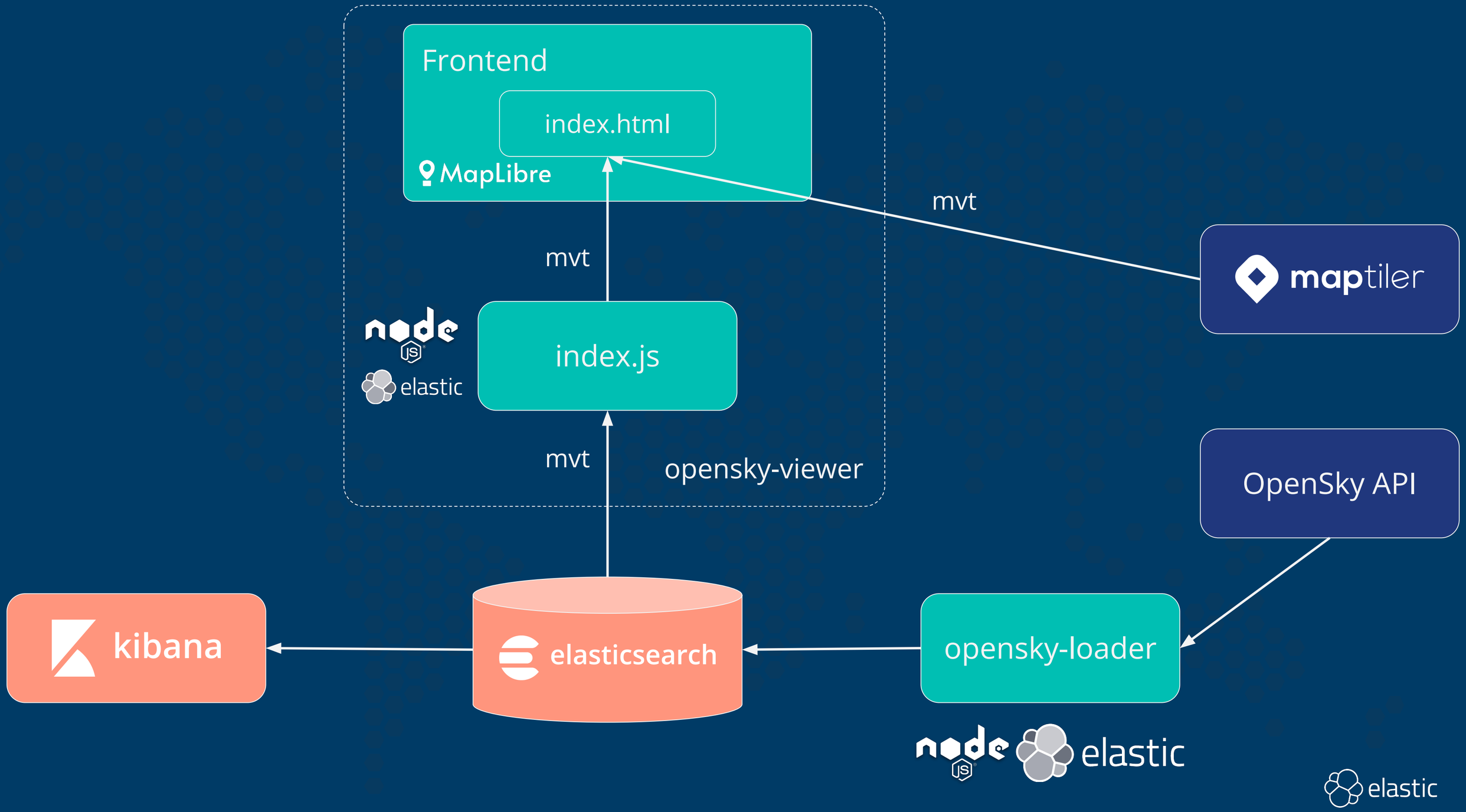

tangram
js
deck.gl
MapLibre
Leaflet
OpenLayers
mapbox
elastic
Navegador
mapa
widgets
mvt
png
...
json
xml
...
Mapa base
Renderizado
API
GeoServer
maptiler
CARTO
mapbox
here
Almacenamiento
PostGIS
Spatial PostgreSQL
elastic



- Un servidor de teselas: nodejs
- Un visor genérico: Maplibre

https://github.com/thomasneirynck/mvt_sample

elastic


Frontend
index.html
MapLibre
mvt
mvt
maptiler
node
elastic
index.js
mvt
opensky-viewer
OpenSky API
kibana
elasticsearch
opensky-loader
node
elastic
elastic

Hora de practicar: cargador de datos

- /lab/opensky-loader/index.js
- Aplicación nodejs con el cliente de elasticsearch
- Revisar el flujo de carga de datos
- Cómo se crea el índice
- Cómo se formatean los datos antes de subirlos
- Cómo se cargan los datos usando la Bulk API

elastic

Hora de practicar: visualizador

`https://github.com/thomasneirynck/mvt_sample`

Backend

- `/lab/opensky-viewer/index.js`
- La ruta raíz sirve el *frontend*
- Controlador para la ruta /tile
- Revisar parámetros
- Construcción de la query a Elasticsearch
- Cabeceras adicionales

Frontend

- `/lab/opensky-viewer/index.html`
- Maplibre y un formulario sencillo
- Capas para polígonos, líneas y puntos
- Revisar *source*: el servidor del *backend*
- Revisar estilos
- Revisar *callback* para el contador de geometrías

elastic

¡Gracias!

Jorge Sanz
2022-06-09, Kibana, Elastic,
xurxosanz jsanz jorge.sanz@elastic.co

https://ela.st/siglibre2022-taller

elastic