Análisis y visuazilazicón de datos con Elasticsearch y Kibana

Girona | SIG Libre | Septiembre, 2025

https://ela.st/siglibre-2025

elastic | The Search AI Company

Jorge Sanz

Principal Software Engineer
Kibana Presentation and Maps team

jorge.sanz@elastic.co
@jorgesanz@mapstodon.space
@jsanz

Documento de apoyo

Este material está adaptado del taller impartido en la conferencia FOSS4G Europe en Mostar (Bosnia-Herzegovina) en julio de 2025.

Agenda

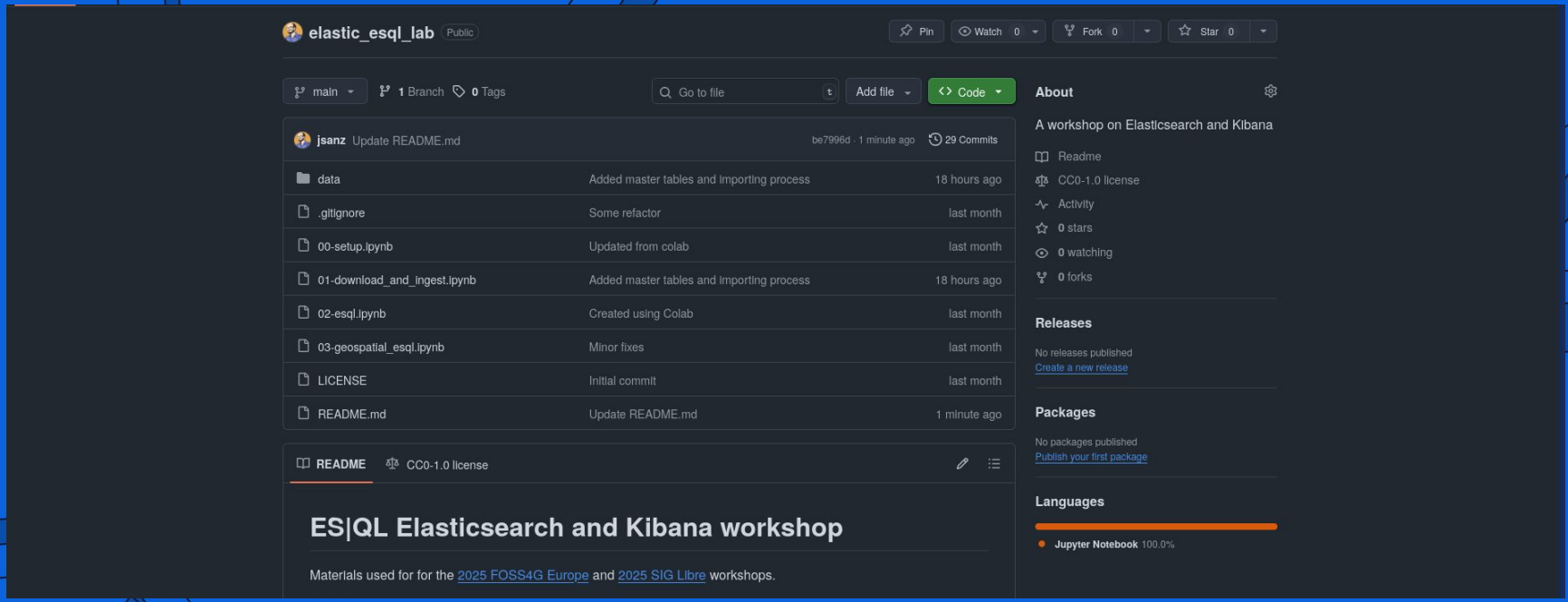
Elastic intro & Elasticsearch and geospatial (~15min)

ES|QL (~45min)

- Source Commands
- Processing Commands: filters, aggregations, calculations
- Geospatial functions

Kibana analytics (~1h)

- Kibana intro
- Discover
- Dashboards
- Lens & ES|QL visualizations
- Maps

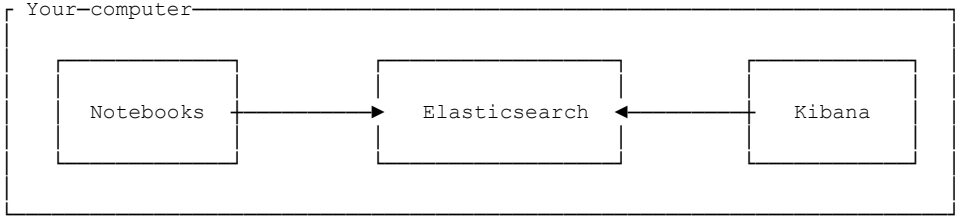


We'll go through the ES|QL basics and geospatial features using Jupyter notebooks then we'll move to Kibana

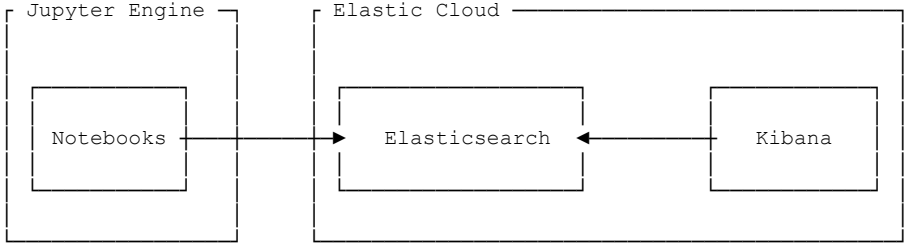
Lab setup

Depending on our connectivity and your preferences

Deploy locally the Notebooks and the Elastic Stack with the `start-local` script



Open the Notebook anywhere and connect to a provided Elastic Stack



00-setup.ipynb

How to download and start an Elastic Stack along with a Jupyter notebook engine.

- Requires a good connectivity to download all the docker images
- Once installed, everything runs in `localhost`
- Fast ingest and download from Elasticsearch
- By default in a *trial* but with instructions to opt out

Alternatively, **we provide an Elastic stack cluster for this workshop** so you don't need to install anything (now).

- Same features as the local instance (Open Source = Basic license)
- Notebooks can run from any Jupyter engine: locally, Google Colab, Binder, etc.

Set up a local environment

Create an Elastic Stack with `start-local`

You can run this workshop in three different ways:

- Run a Elastic stack (Elasticsearch & Kibana) on your computer
- Using an Elastic stack deployment in Elastic Cloud or anywhere else
- With an Elastic Serverless project

The following instructions set up a local environment with Elasticsearch and Kibana.

Create a new folder and inside execute the following commands to download the `start-local` script and execute it:

```
curl -fsSL https://elastic.co/start-local > start-local
bash start-local -v 9.0.3
```

For more details about `start-local` refer to the README on GitHub.

You'll see how images are downloaded, volumes and containers created, etc. An output like this will be rendered at the end of the execution:

```
🎉 Congrats, Elasticsearch and Kibana are installed and running in Docker!

🌐 Open your browser at http://localhost:5601

   Username: elastic
   Password: hODGZcFs

🔌 Elasticsearch API endpoint: http://localhost:9200
🔑 API key: OThOSDJwY0I3QnlxdzlfMnVtZTc6TDlSUlpCVjRoQXdvb0oyODVNaVFEUQ==

Learn more at https://github.com/elastic/start-local
```

Copy the login details from the command output:

- User and password
- API key

Add a Jupyterlab notebook environment

Now you can add the following code to the `elastic-start-local/docker-compose.yml` file, just after the Kibana service is defined and before the `volumes` key.

```
  notebook:
    depends_on:
      elasticsearch:
        condition: service_healthy
      kibana:
```

Elastic intro

Elastic — The Search AI Company

Elastic helps everyone transform data into **answers**, **actions**, and **outcomes** with Search AI.

Founded in
2012

3,000+
employees (~250 in Spain)

40+
Countries with employees

5B+
downloads

Used by over **54%**
of the Fortune 500

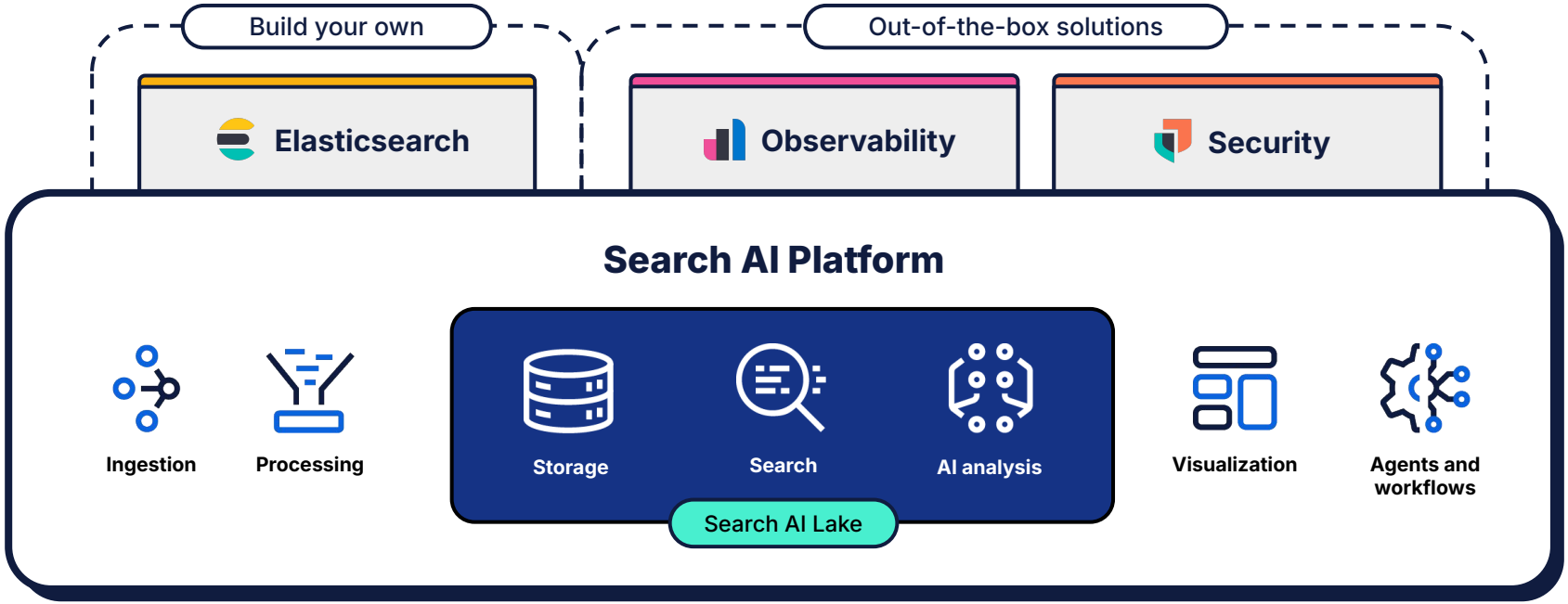
Publicly traded under
ESTC in the NYSE

Data as of Mar 2025

Used by more than 50% of the Fortune 500 enterprises

TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE / TRANSPORTATION	RETAIL
Adobe	BARCLAYS	orange	Uber	VITAS Healthcare	Lawrence Livermore National Laboratory	VOLVO Volvo Group	AutoZone
cisco	ZURICH	dish media	Grab	UCLA Health	OAK RIDGE National Laboratory	Audi	The Home Depot
workday.	USAA	COMCAST	Miles & More Lufthansa	Yale NewHaven Health	De Watergroep	JAGUAR LAND ROVER	ebay
Microsoft	Swift	verizon	ACTIVISION BLIZZARD	MAYO CLINIC	JPL Jet Propulsion Laboratory	BMW	Kroger
INGRAM MICRO	Postbank	T-Mobile	lyft	Pfizer	MENTAT COMPUTE OPTIMIZATION	VW	Walgreens

One **platform**, two out-of-the-box **solutions**, the freedom to **build anything**

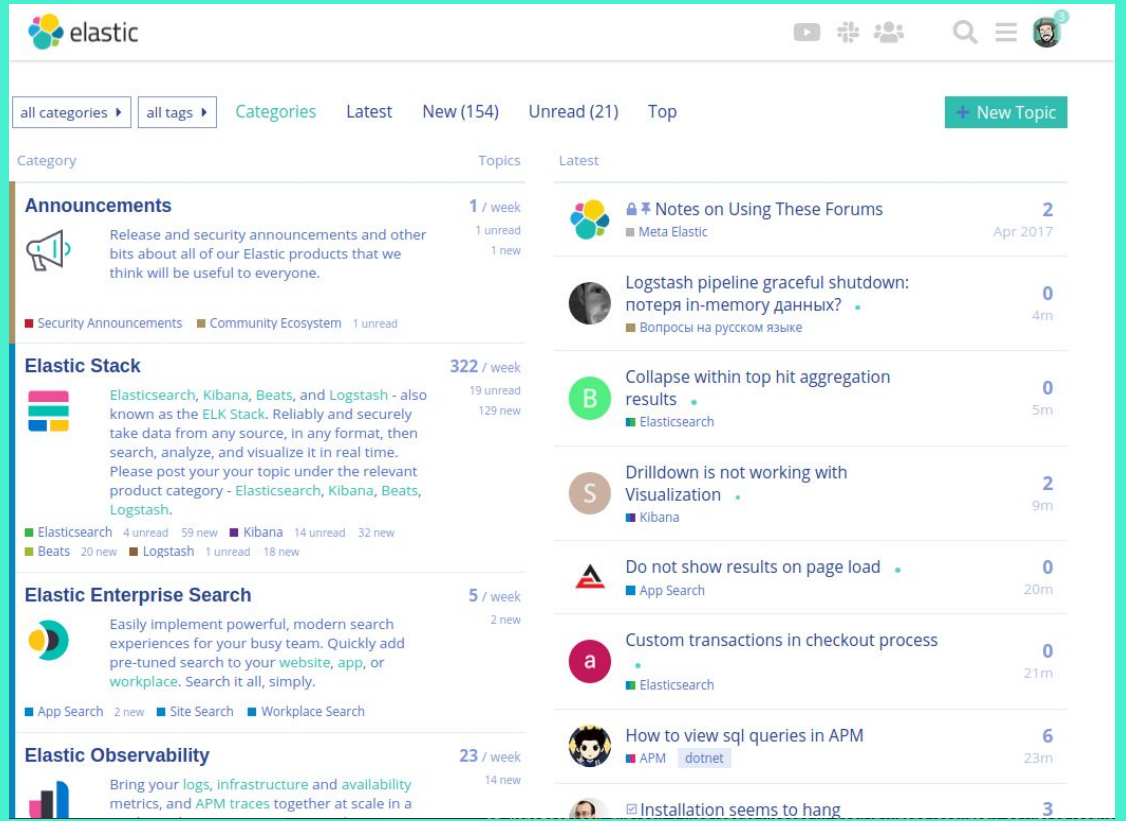


Community

https://github.com/elastic

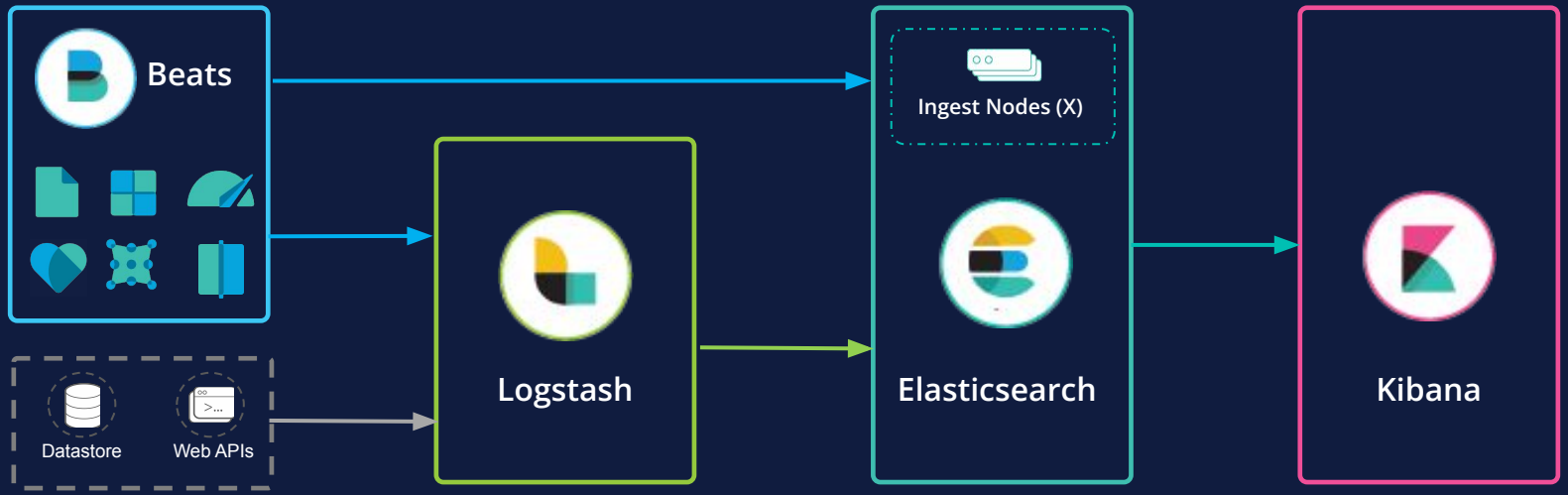
https://ela.st/slack

https://discuss.elastic.co



Elastic Stack

Ingest, Store, Search, Visualise



Elasticsearch and geospatial

Geospatial timeline

2010-2012
Geo search
Points & Shapes

2014
Geo analysis
Aggregations

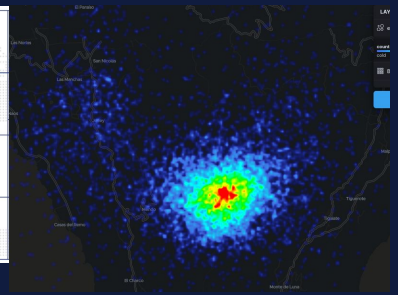
2017-2019
Geo at scale
Encoding
upgrades

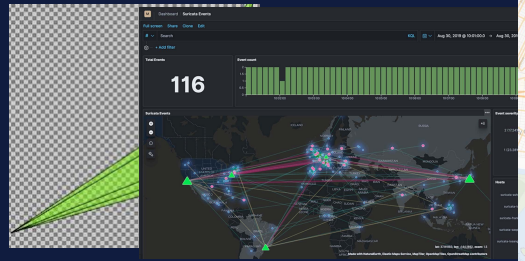
2020-2021
GIS
Maps & analytics

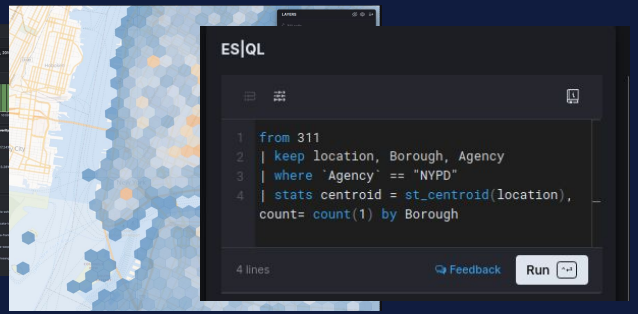
2022-2023
Vector tiles and H3
Fast aggregations
and rendering

2024
ES|QL
Powerful and
expressive language

b	c	f	g
8	9	d	e
2	3	6	7
0	1	4	5







elastic

Elasticsearch geospatial data types

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

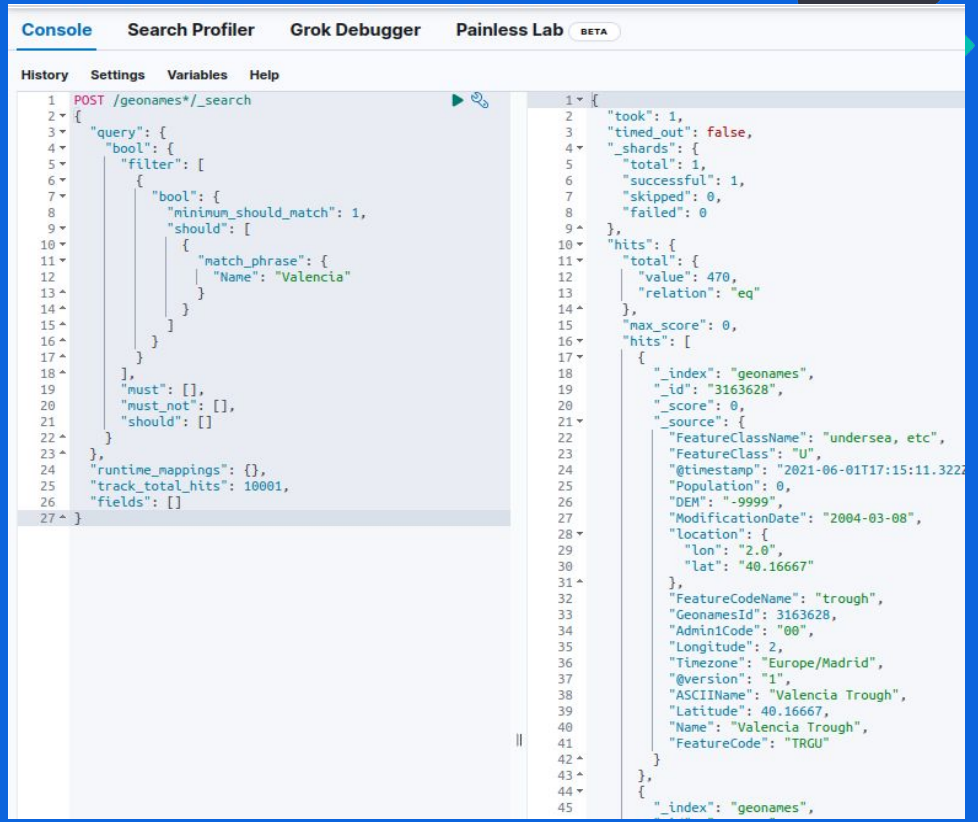
Vector tiles API

Elasticsearch **`_search` API**

- JSON output format
- Search and aggregate

Elasticsearch **`_mvt` API**

- *protobuf* output format
- Use queries and aggregations to generate standard vector tiles



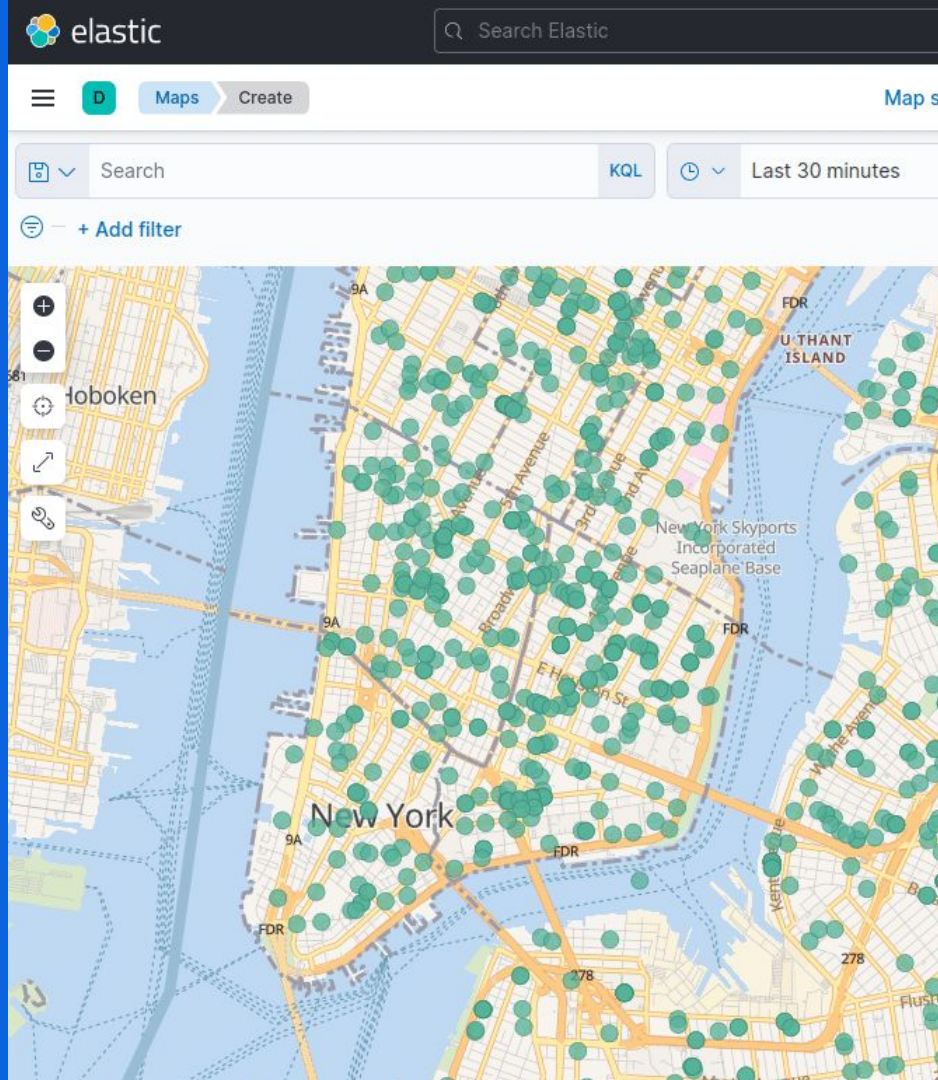
Search

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

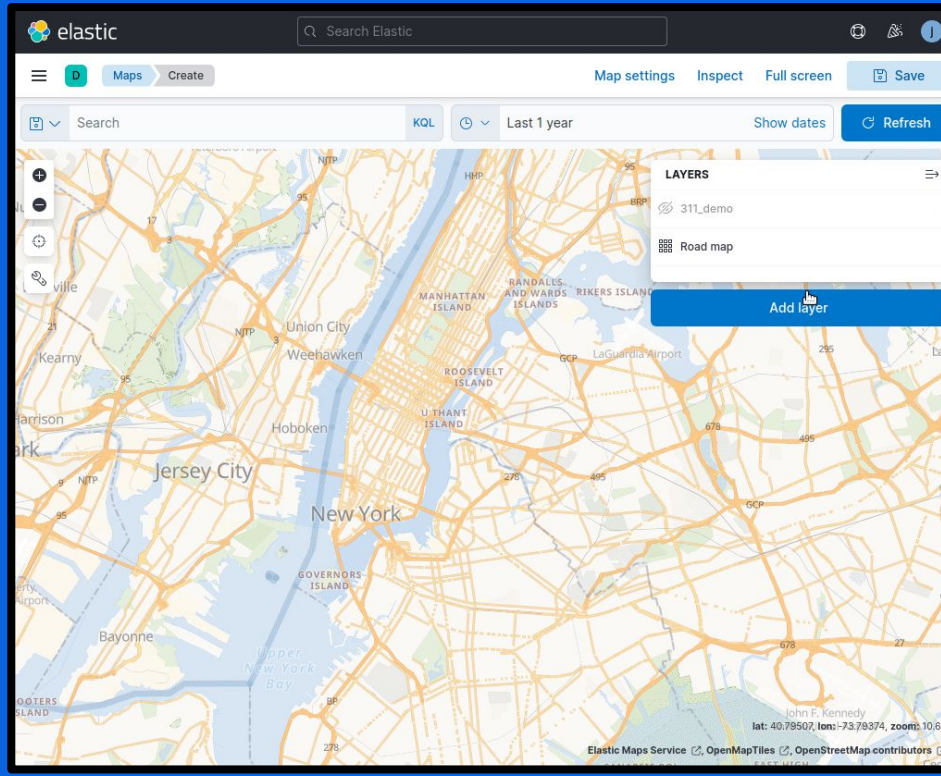
Binning (bucket agg)

- Geo-Distance (rings) 📖
- Geohash grid 📖
- Geotile grid 📖
- Geohex grid 📖 🛒

Derived geometries (metric agg)

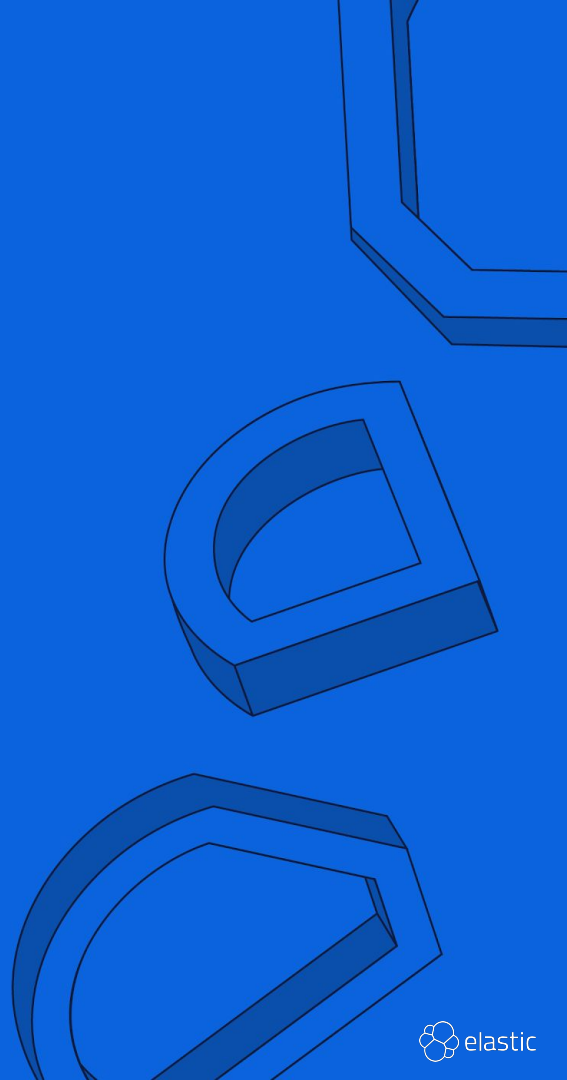
- Geo-centroid 📖
- Geo-bounds 📖
- Geo-line 📖 🛒

Non-geo aggregations: Huge range of bucket and metric aggregations 📖



Introducing ES|QL

What is ES|QL?



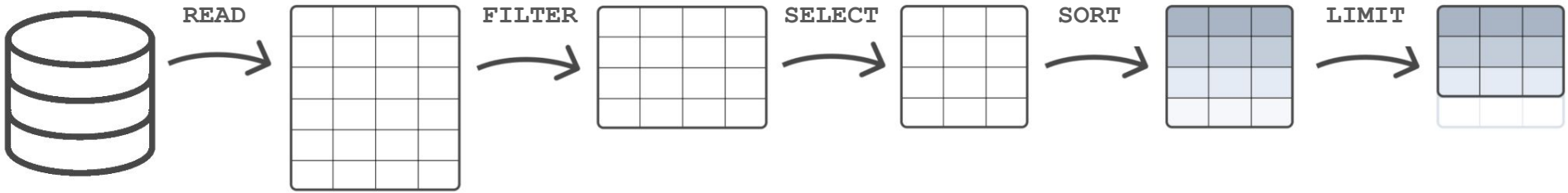
Declarative, Piped, Tabular

```
1  FROM airports
2  | WHERE scalerank < 6
3  | KEEP abbrev, name, location, country, city
4  | SORT abbrev ASC
5  | LIMIT 3
```

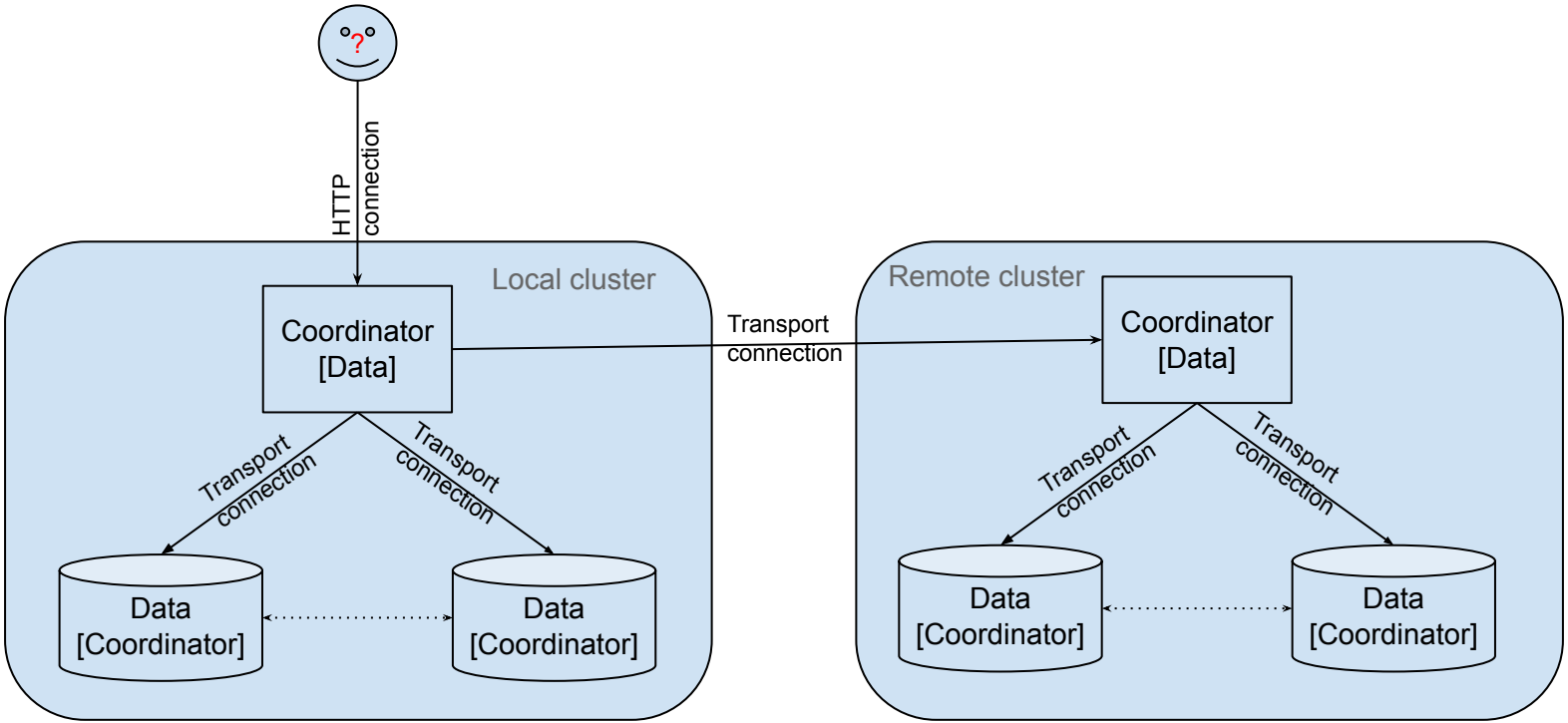
ES|QL

```
3  SELECT abbrev, name, location, country, city
1  FROM airports
2  WHERE scalerank < 6
4  ORDER BY abbrev ASC
5  LIMIT 3
```

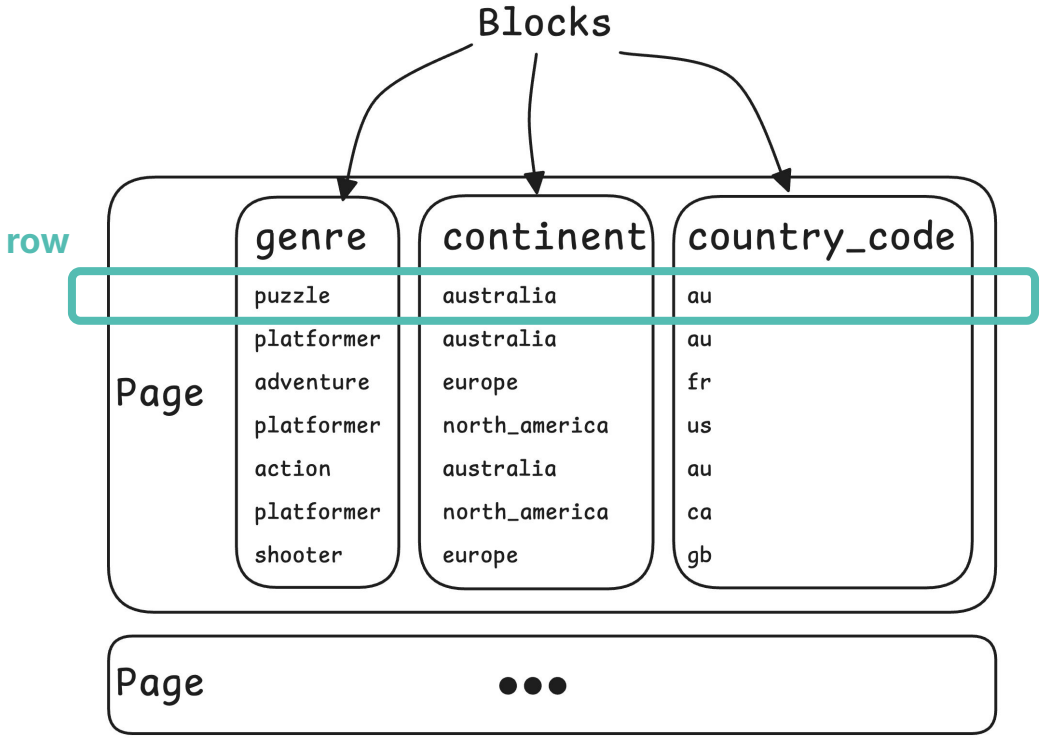
SQL



Distributed



Vectorized


Blocks
row
genre
continent
country_code
puzzle
australia
au
platformer
australia
au
adventure
europe
fr
platformer
north_america
us
action
australia
au
platformer
north_america
ca
shooter
europe
gb
Page
Page
●●●

ES|QL

Elasticsearch Query Language (ES|QL) provides a powerful way to **filter, transform, and analyze** data stored in Elasticsearch.

It is designed to be **easy to learn** and use, by end users, SRE teams, application developers, subject matter experts, and administrators.

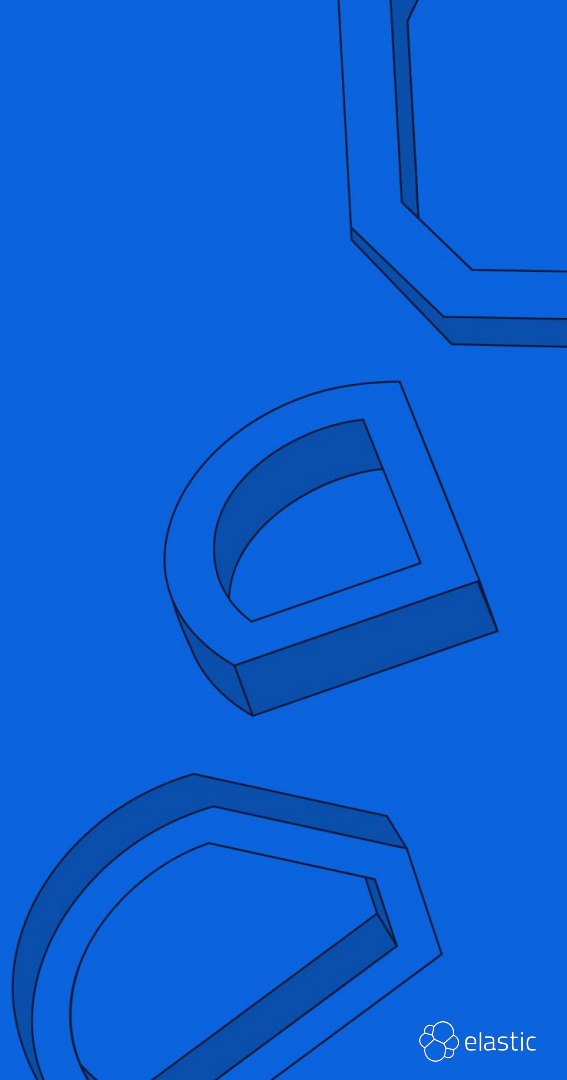
Keywords: speed, simplicity, and efficiency

Distributed & Dedicated Query Engine

`_query`

- No transpilation or translation
- Queries are parsed and optimized for distributed execution
- It operates in blocks, instead of one row at a time
- It takes advantage of specialization and multi-threading
- Benchmarking has shown ES|QL can outperform DSL in many instances

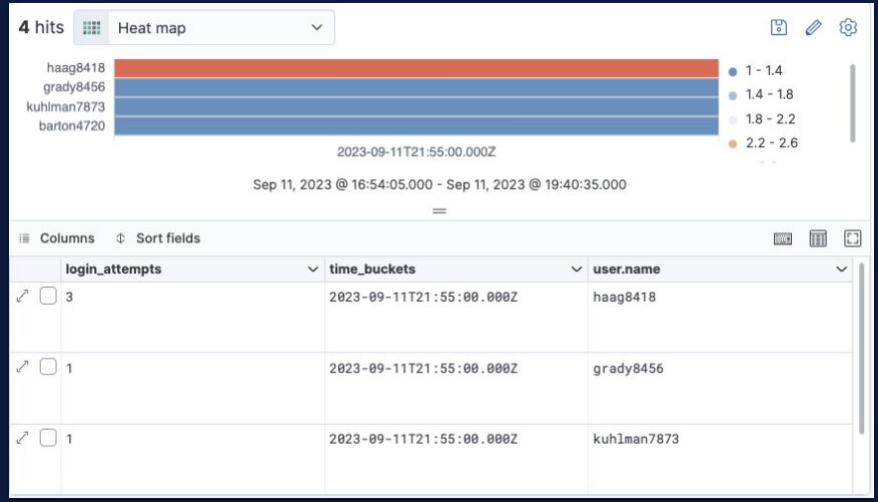
Understanding ES|QL Syntax



elastic

An ES|QL query

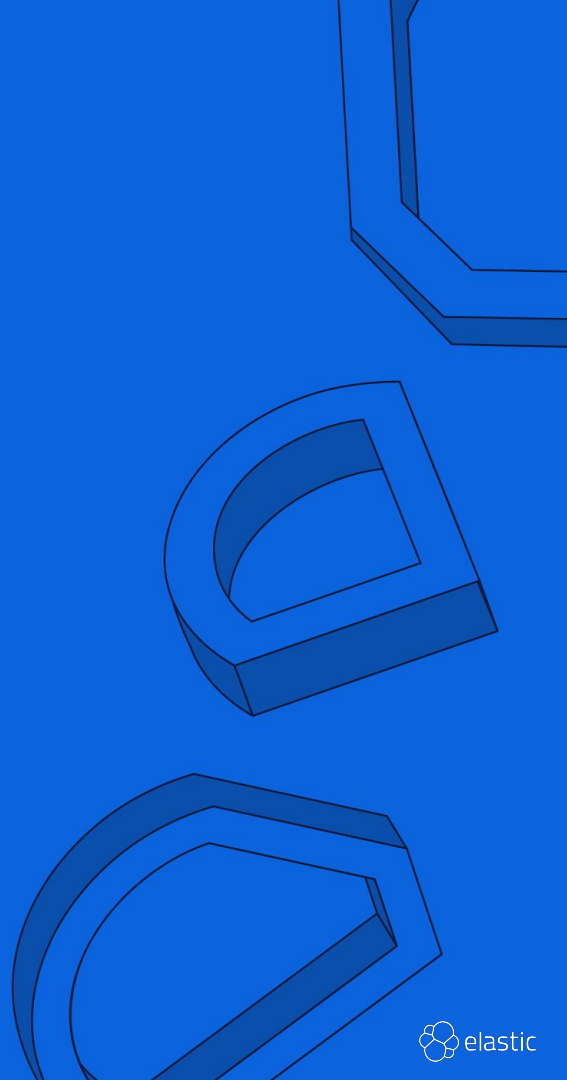
```
FROM apache-logs
| WHERE url.original == ‘/login’
| EVAL time_buckets = auto_bucket (@timestamp, 50,”2023-09-11T21:54:05.000Z”,”2023-09-12T00:40:35.000Z”)
| STATS login_attempts = count(user.name) by time_buckets, user.name
| SORT login_attempts desc
```



Expressive, Powerful, Composable, Extensible, Fast

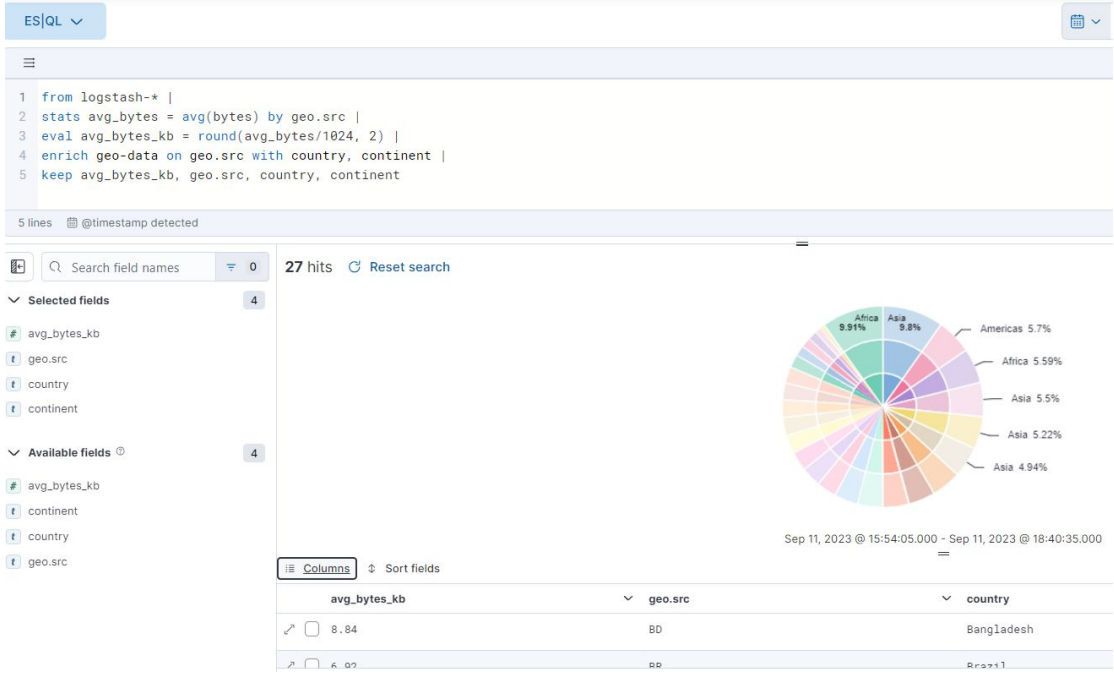
elastic

Unified User Experience



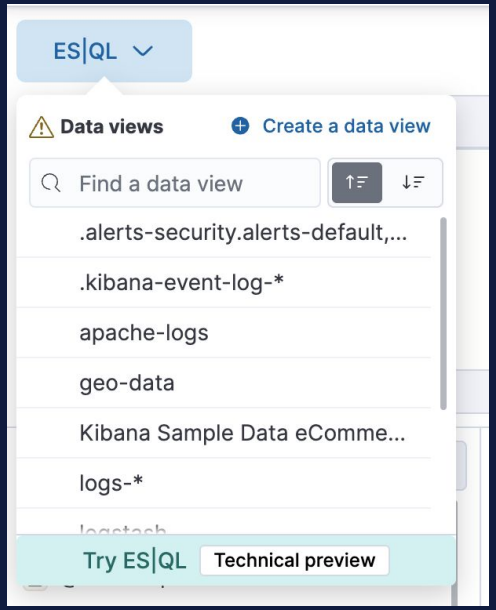
ES|QL UX

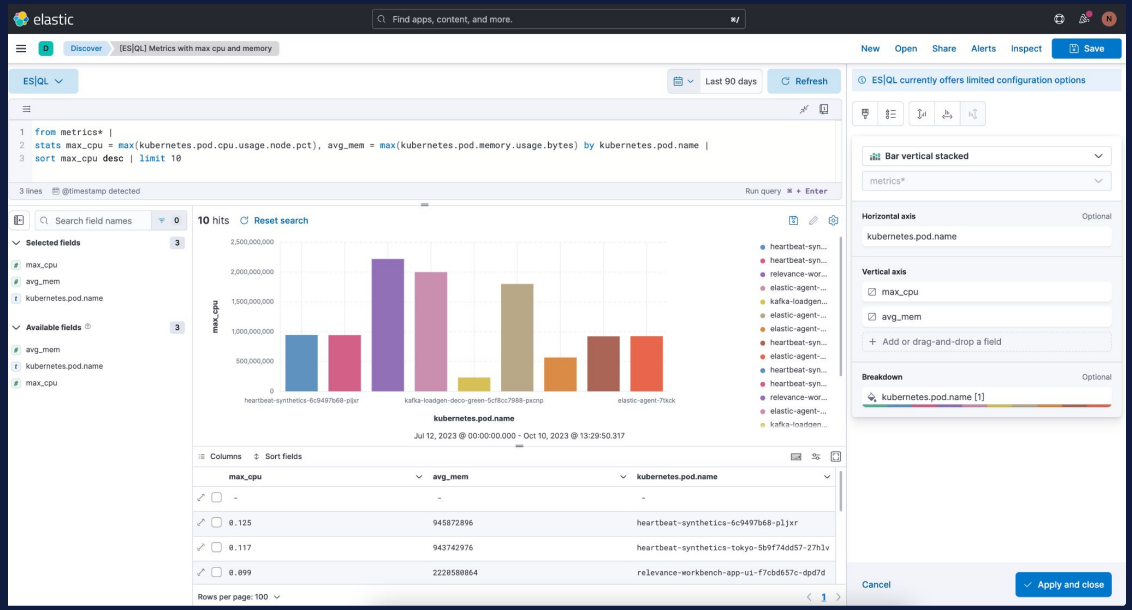
Data Exploration, Transformation and Visualization all in one



elastic

ES|QL in Discover

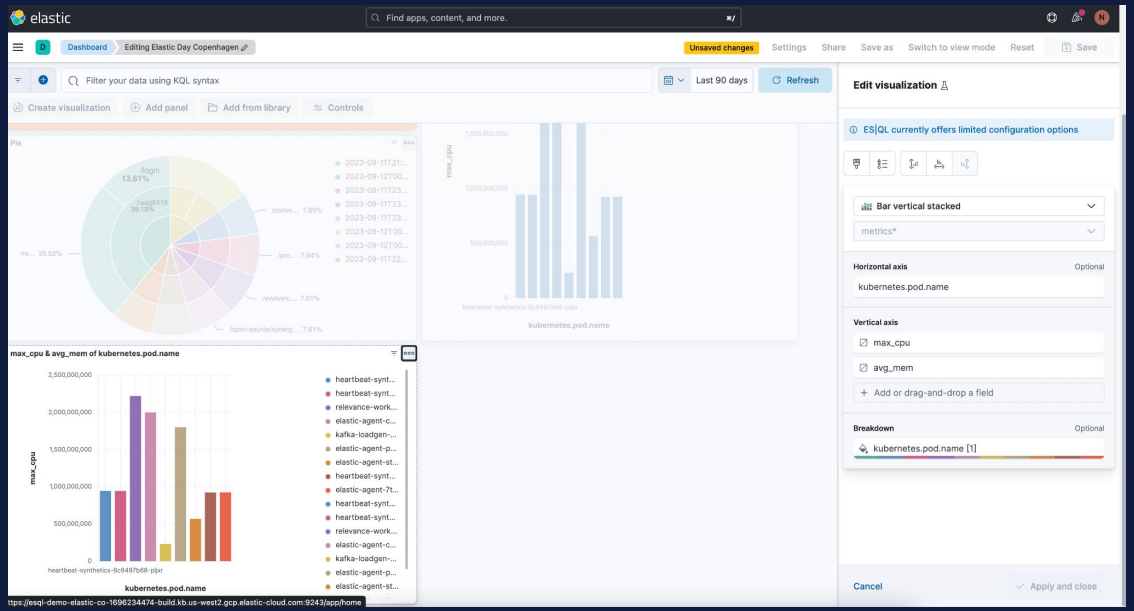




ES|QL is under the data view picker in Discover

The ES|QL experience in Discover includes Lens visualizations and in-line editing.

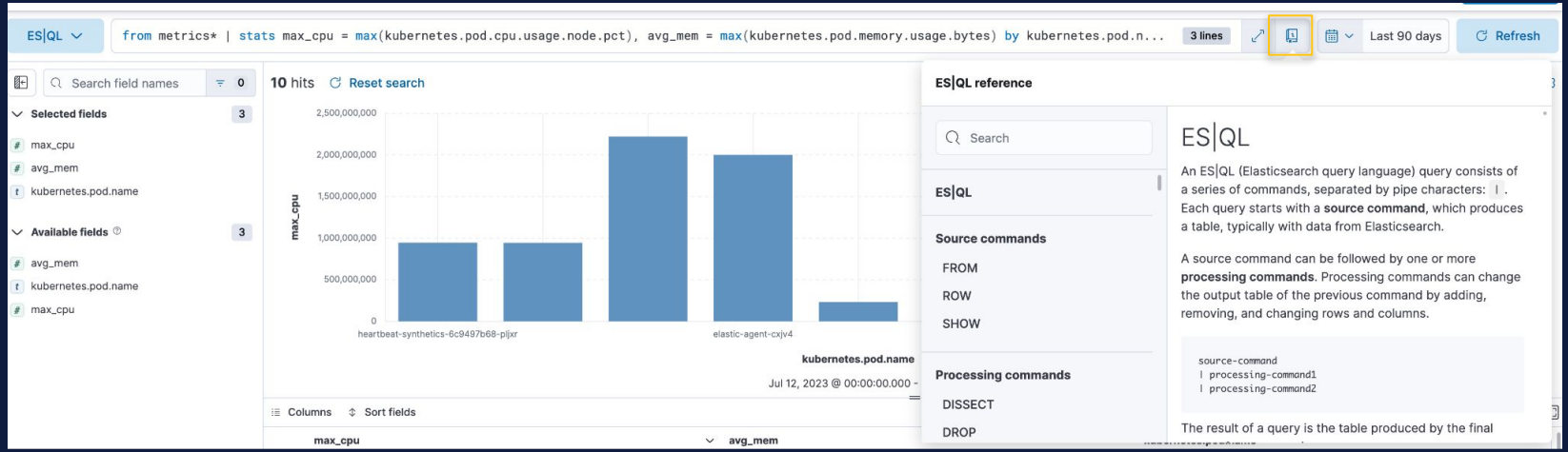
ES|QL in Dashboard

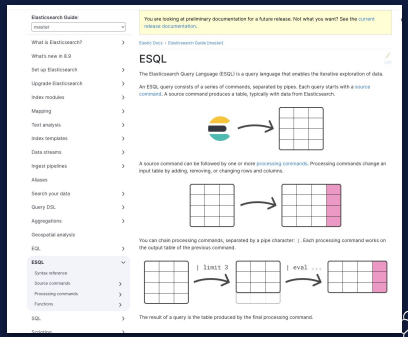


Save ES|QL charts from Discover and use them on Dashboards.
ES|QL charts also have in-line editing in Dashboard

elastic

In Product ES|QL Documentation

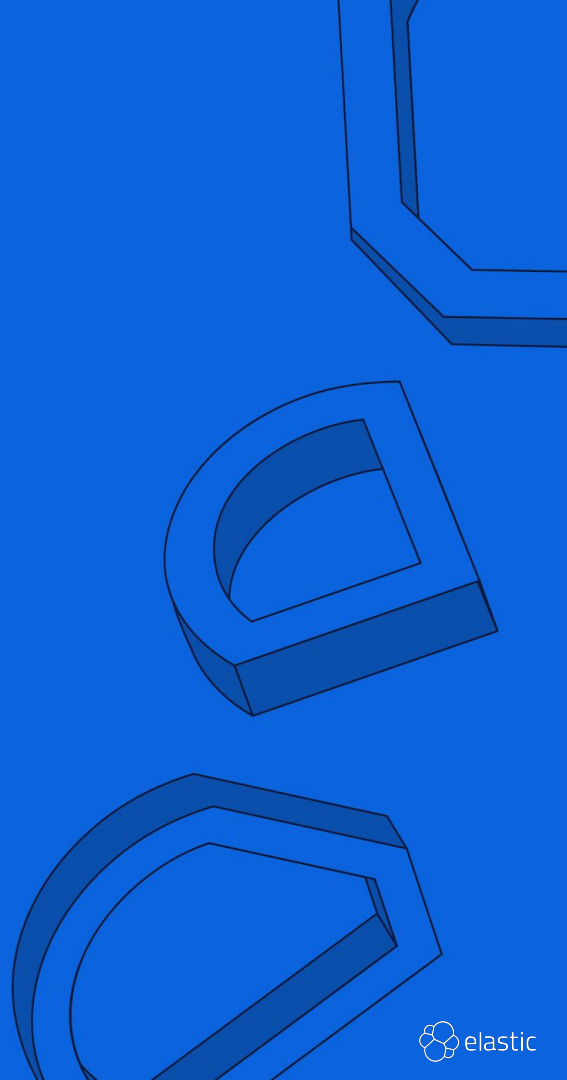




- In-line documentation right at your fingertips!
- Full documentation page: **ES|QL**

elastic

ES|QL Workshop



elastic

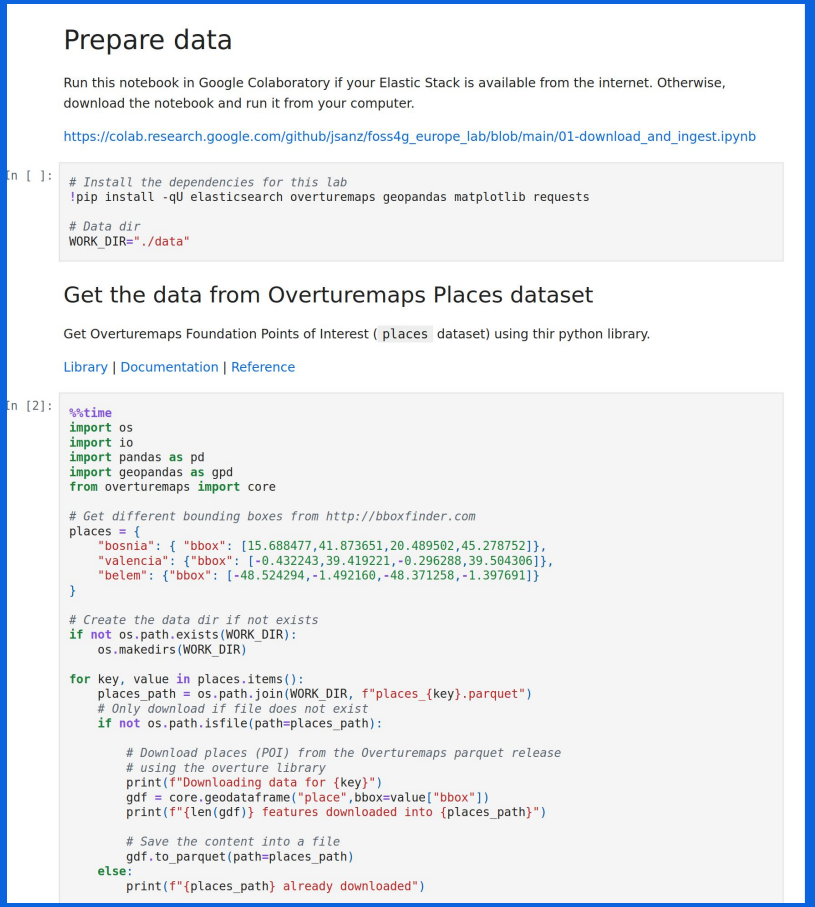
01-download_and_ingest.ipynb

Details on how to download and ingest in Elasticsearch datasets for this workshop:

- Overture Maps Foundation places dataset from parquet files
- Natural Earth countries zipped shapefile
- OSM, Geonames, and GHCD snapshots
- Civio Forest Fires between 1968 and 2023

To get these tasks:

- How to use the OvertureMaps Python API
- How to read parquet files into (Geo)Pandas Dataframes
- How to define Elasticsearch index mappings and bulk uploading efficiently large datasets
- Use the Kibana API to create Data Views
- Some troubleshooting for a misbehaving geospatial feature
- How to restore snapshots from read-only HTTP repositories



Prepare data

Run this notebook in Google Colaboratory if your Elastic Stack is available from the internet. Otherwise, download the notebook and run it from your computer.

https://colab.research.google.com/github/jsanz/foss4g_europe_lab/blob/main/01-download_and_ingest.ipynb

In [ ]:

```
# Install the dependencies for this lab
!pip install -qU elasticsearch overturemaps geopandas matplotlib requests

# Data dir
WORK_DIR="./data"
```

Get the data from Overturemaps Places dataset

Get Overturemaps Foundation Points of Interest (`places` dataset) using thir python library.

Library | Documentation | Reference

In [2]:

```
%%time
import os
import io
import pandas as pd
import geopandas as gpd
from overturemaps import core

# Get different bounding boxes from http://bboxfinder.com
places = {
    "bosnia": { "bbox": [15.688477,41.873651,20.489502,45.278752]},
    "valencia": {"bbox": [-0.432243,39.419221,-0.296288,39.504306]},
    "belem": {"bbox": [-48.524294,-1.492160,-48.371258,-1.397691]}
}

# Create the data dir if not exists
if not os.path.exists(WORK_DIR):
    os.makedirs(WORK_DIR)

for key, value in places.items():
    places_path = os.path.join(WORK_DIR, f"places_{key}.parquet")
    # Only download if file does not exist
    if not os.path.isfile(path=places_path):

        # Download places (POI) from the Overturemaps parquet release
        # using the overture library
        print(f"Downloading data for {key}")
        gdf = core.geodataframe("place",bbox=value["bbox"])
        print(f"{len(gdf)} features downloaded into {places_path}")

        # Save the content into a file
        gdf.to_parquet(path=places_path)
    else:
        print(f"{places_path} already downloaded")
```

elastic

Lab datasets

```
GET _cat/indices?v&h=index,docs.count,dataset.size&s=index
```

index	docs.count	dataset.size
.ds-kibana_sample_data_logs-2025.09.01-000001	14074	7.1mb
airports	891	98.1kb
civio-fires	292181	41.7mb
geonames	11968314	1.9gb
ghcnd_daily_observations	29075053	4gb
kibana_sample_data_ecommerce	4675	3.9mb
kibana_sample_data_flights	13014	5.6mb
ne_countries	257	35.1mb
osm_andorra	284619	55mb
osm_estonia	12787609	2.8gb
osm_italy_centro	43002709	8.4gb
osm_spain_valencia	12355000	2.4gb
osm_usa_arizona	31160000	5.1gb
places-bosnia	166644	61.3mb
places-girona	20899	8.9mb
places-valencia	36193	14.8mb

02-esql.ipynb

With a helper function that takes a ES|QL query and return a (Geo)Dataframe, go through the different aspects of the language to learn its syntax:

- Source commands
- Controlling the output
- Processing commands
  - Filtering
  - Aggregations
  - Joins

Filtering and processing

In [16]:
```
# A basic filter
esql("""
FROM places-* METADATA _index
| RENAME _index as dataset
| WHERE name LIKE "*Burger*"
    AND category IN ("restaurant", "burger_restaurant")
    AND confidence < 0.3
| SORT confidence DESC
| KEEP dataset, name, category, confidence
| LIMIT 5
""")
```

Out[16]:

	dataset	name	category	confidence
0	places-belem	Purple Burgers	burger_restaurant	0.296943
1	places-belem	Prime Burger food truck	burger_restaurant	0.296943
2	places-bosnia	Burgers by Manzoni	burger_restaurant	0.296943
3	places-valencia	TORO Burger Lounge	restaurant	0.296943
4	places-belem	Nick Burger	burger_restaurant	0.296943

In [17]:
```
# STATS allows running aggrecations.
# In this count agg, no other data is available afterwards
esql("""
FROM ne_countries
| STATS counts = count(id)
""")
```

Out[17]:

	counts
0	257

In [18]:
```
# When grouping by other fields, those are also available
# for further operations like sorting or filtering
esql("""
FROM ne_countries
| WHERE type in ("Country", "Sovereign country")
| STATS counts = count(id) BY continent
| WHERE counts > 30
| SORT continent
| KEEP continent, counts
| LIMIT 5
""")
```

Out[18]:

	continent	counts

03-geospatial_esql.ipynb

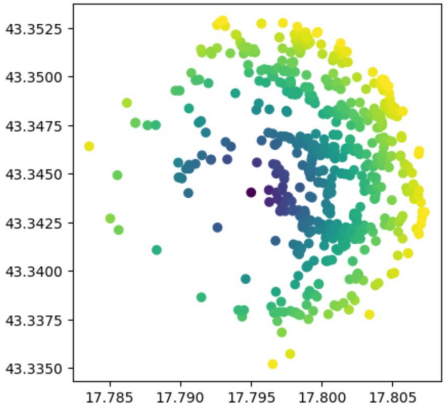
Focusing on the current geospatial features in ES|QL:

- Type conversions
- Distance computations
- Geometry aggregations
- Geometry functions

```
print(query)
esql(query).plot(column="dist_charlie")
```

```
    FROM places-bosnia
    | EVAL dist_charlie = ST_DISTANCE(TO_GEOPOINT("POINT (17.7950102 43.3440312)"), geometry)
    | WHERE dist_charlie < 1000
    | KEEP name, category, dist_charlie, geometry
    | LIMIT 50000
```

Out[12]: <Axes: >



We'll use that query later in Kibana.

Geometry aggregation: `ST_EXTENT_AGG` , and `ST_CENTROID_AGG` and geometry functions `ST_ENVELOPE`, `ST_XMAX`, `ST_YMAX`, etc.

In [13]:

```
# Get the envelope of a geometry, this function only works on single rows
# We use the use_arrow=False param in our helper function to return the
# envelope as a WKT instead of a binary.
query = f"""
    FROM ne_countries
    | WHERE iso_a2 LIKE "BA"
    | EVAL geometry_envelope = ST_ENVELOPE(geometry)
    | KEEP name, geometry_envelope
    | LIMIT 1
    """
```

Kibana

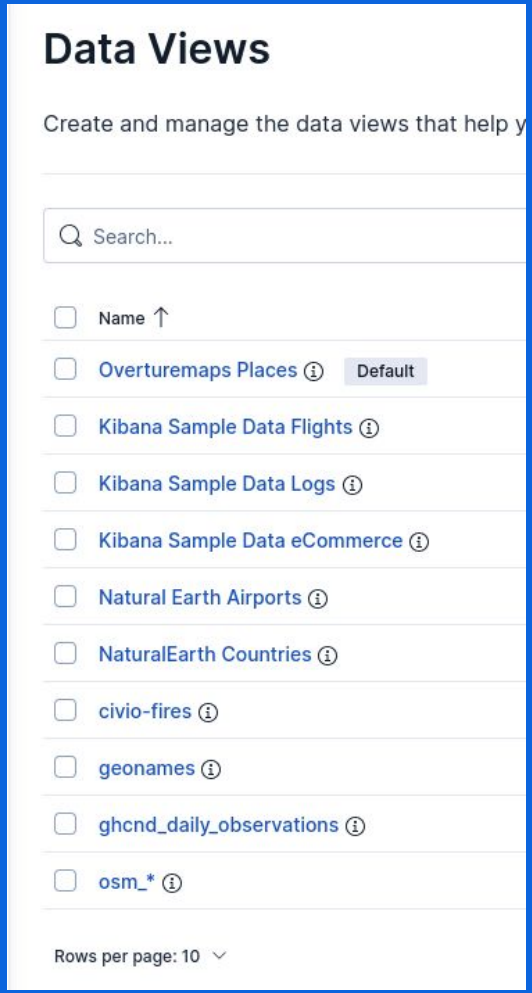
Home for all Elastic graphic applications

Please, now it is a good time to connect to your Kibana instance if running locally, or to the Elastic Cloud Kibana instance provided in the workshop notes.

Lab datasets

Datasets to experiment with

- Kibana sample datasets
  - `kibana_sample_data_commerce`
  - `Kibana_sample_data_flights`
  - `kibana_sample_data_logs`
- Natural Earth airports and countries
  - `airports`
  - `Ne_countries`
- Civio Spain fires: `civio-fires`
- Overturemaps Places: `places*`
- Geonames gazetter: `geonames`
- GHCD daily observations: `ghcd`
- OSM data: `osm*`



elastic

Lab datasets

```
GET _cat/indices?v&h=index,docs.count,dataset.size&s=index
```

index	docs.count	dataset.size
.ds-kibana_sample_data_logs-2025.09.01-000001	14074	7.1mb
airports	891	98.1kb
civio-fires	292181	41.7mb
geonames	11968314	1.9gb
ghcnd_daily_observations	29075053	4gb
kibana_sample_data_ecommerce	4675	3.9mb
kibana_sample_data_flights	13014	5.6mb
ne_countries	257	35.1mb
osm_andorra	284619	55mb
osm_estonia	12787609	2.8gb
osm_italy_centro	43002709	8.4gb
osm_spain_valencia	12355000	2.4gb
osm_usa_arizona	31160000	5.1gb
places-bosnia	166644	61.3mb
places-girona	20899	8.9mb
places-valencia	36193	14.8mb

jorge-sanz.kb.eastus2.azure.elastic-cloud.com/app/home#/ 110%

elastic

Find apps, content, and more. ^/

Home

Welcome home

Elasticsearch

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

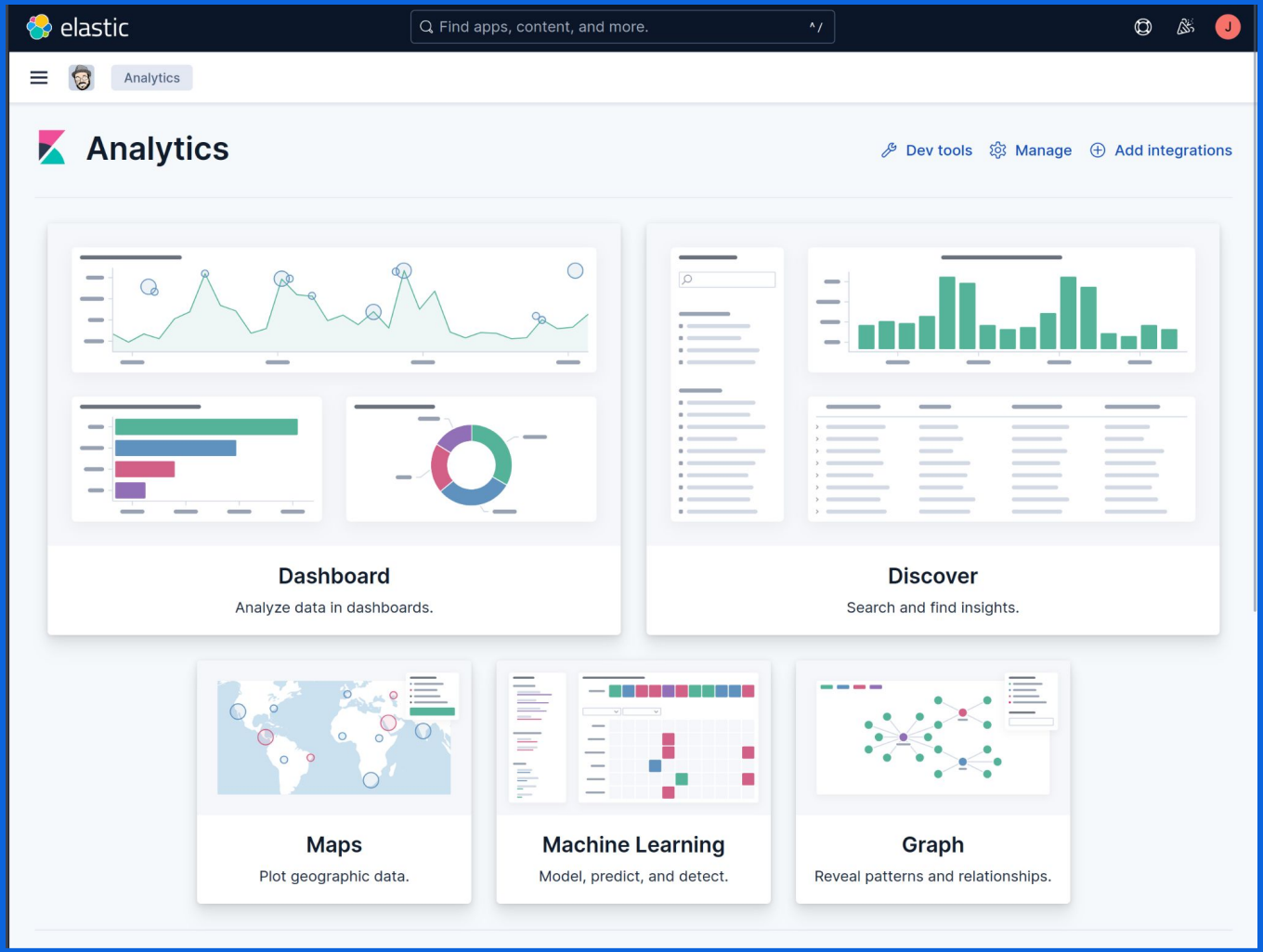
Setup guides | Add integrations | Try sample data | Upload a file

Management

Dev Tools | Stack Management

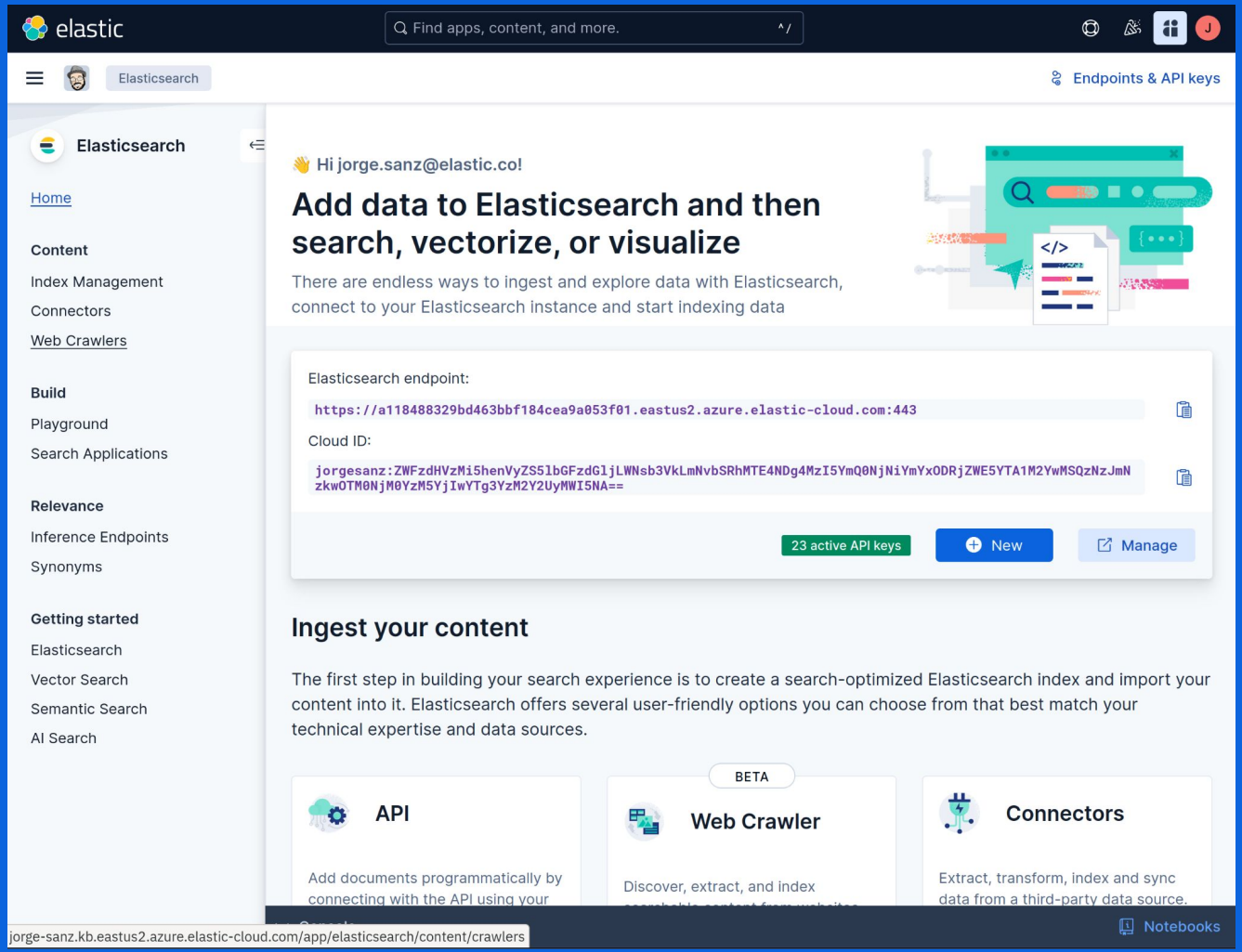
Manage permissions | Monitor the stack | Back up and restore | Manage index lifecycles

ANALYTICS



elastic

Search platform



elastic

Kibana Analytics

Kibana analytics

Applications that power data analysis in Kibana.

Machine learning features are not part of the Basic offering and not covered today.

👀 Data Views

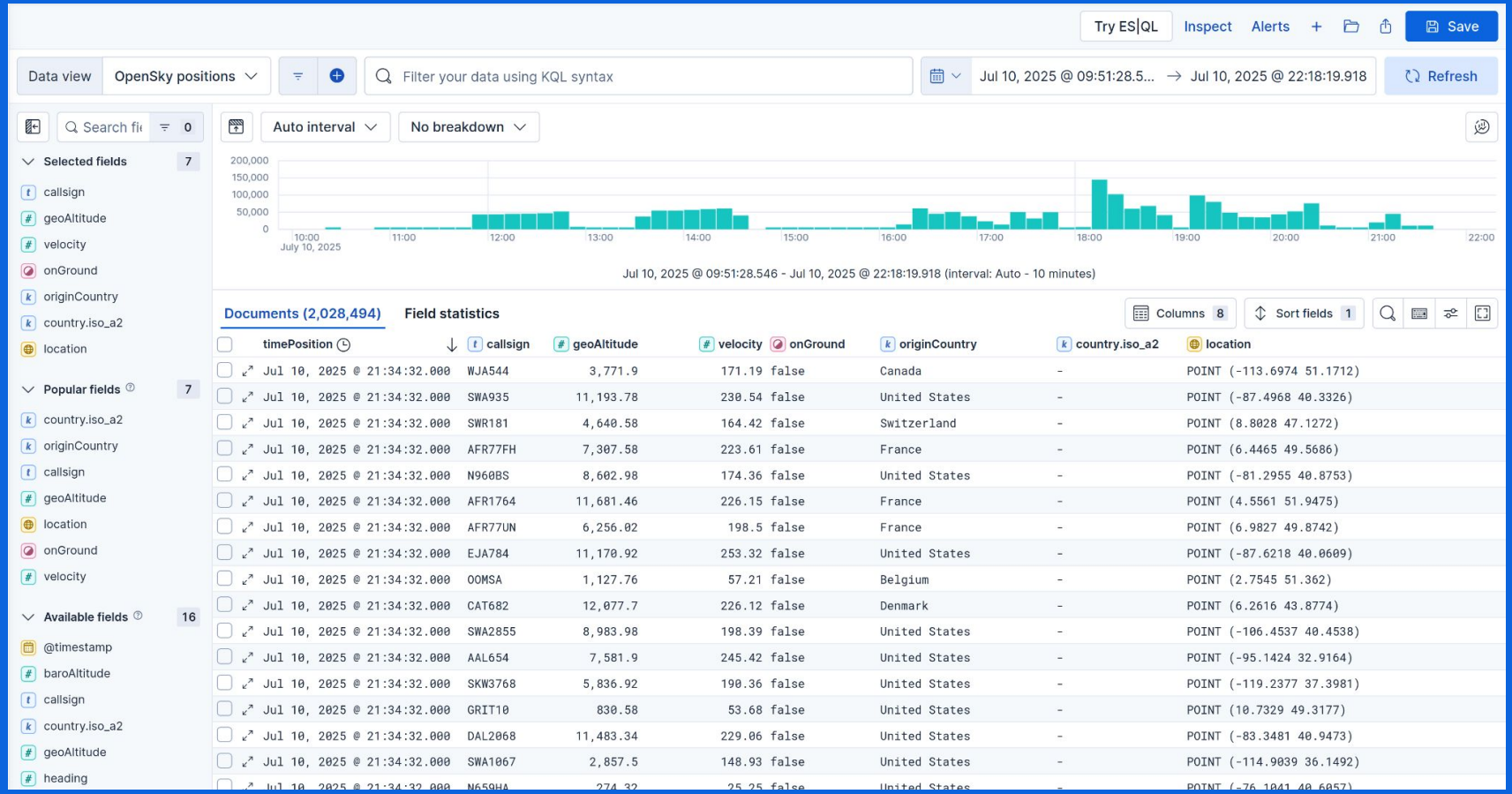
🕵️ Discover

👩‍💻 Dashboards

📊 Visualizations: Lens & ES|QL

🌏 Maps

Discover



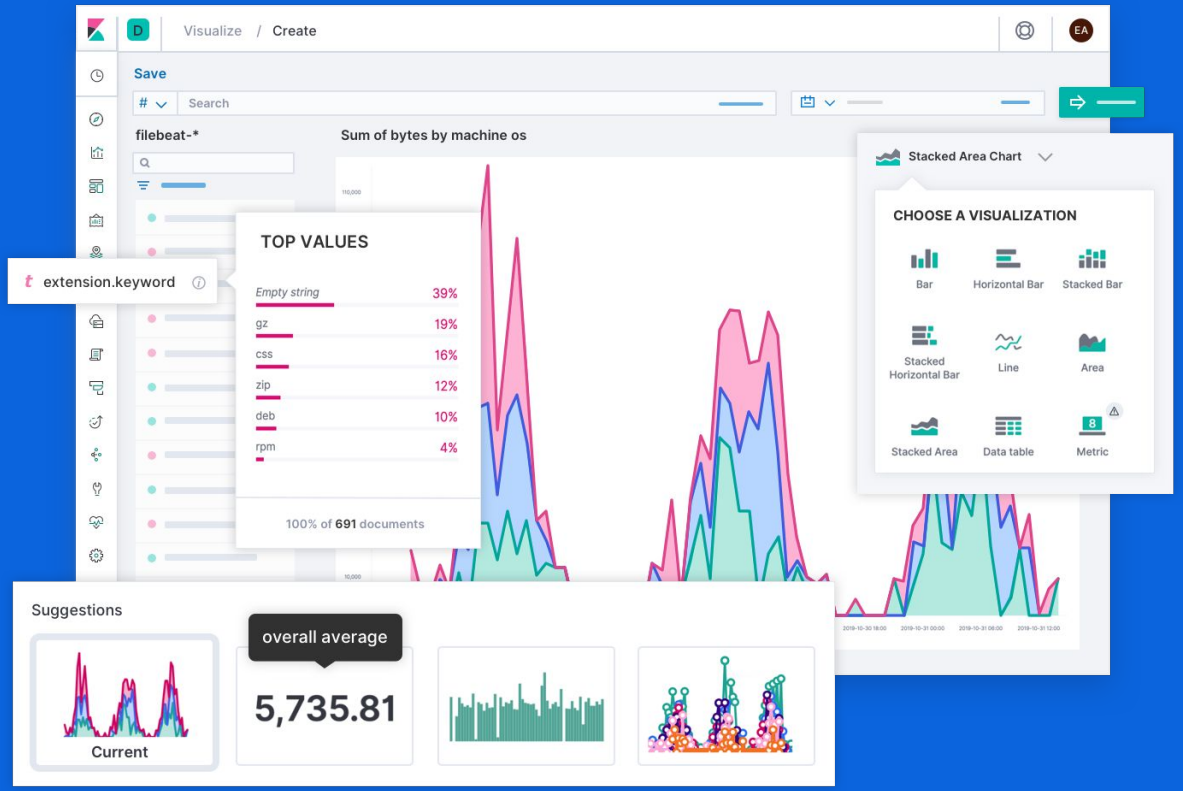
timePosition	callsign	geoAltitude	velocity	onGround	originCountry	country.iso_a2	location
Jul 10, 2025 @ 21:34:32.000	WJA544	3,771.9	171.19	false	Canada	-	POINT (-113.6974 51.1712)
Jul 10, 2025 @ 21:34:32.000	SWA935	11,193.78	230.54	false	United States	-	POINT (-87.4968 40.3326)
Jul 10, 2025 @ 21:34:32.000	SWR181	4,640.58	164.42	false	Switzerland	-	POINT (8.8028 47.1272)
Jul 10, 2025 @ 21:34:32.000	AFR77FH	7,307.58	223.61	false	France	-	POINT (6.4465 49.5686)
Jul 10, 2025 @ 21:34:32.000	N960BS	8,602.98	174.36	false	United States	-	POINT (-81.2955 40.8753)
Jul 10, 2025 @ 21:34:32.000	AFR1764	11,681.46	226.15	false	France	-	POINT (4.5561 51.9475)
Jul 10, 2025 @ 21:34:32.000	AFR77UN	6,256.02	198.5	false	France	-	POINT (6.9827 49.8742)
Jul 10, 2025 @ 21:34:32.000	EJA784	11,170.92	253.32	false	United States	-	POINT (-87.6218 40.0609)
Jul 10, 2025 @ 21:34:32.000	OOMSA	1,127.76	57.21	false	Belgium	-	POINT (2.7545 51.362)
Jul 10, 2025 @ 21:34:32.000	CAT682	12,077.7	226.12	false	Denmark	-	POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000	SWA2855	8,983.98	198.39	false	United States	-	POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000	AAL654	7,581.9	245.42	false	United States	-	POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000	SKW3768	5,836.92	190.36	false	United States	-	POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000	GRIT10	830.58	53.68	false	United States	-	POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000	DAL2068	11,483.34	229.06	false	United States	-	POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000	SWA1067	2,857.5	148.93	false	United States	-	POINT (-114.9039 36.1492)
Jul 10, 2025 @ 21:34:32.000	N659HA	274.32	25.25	false	United States	-	POINT (-76.1041 40.6057)

elastic

Lens

Your data in front of you

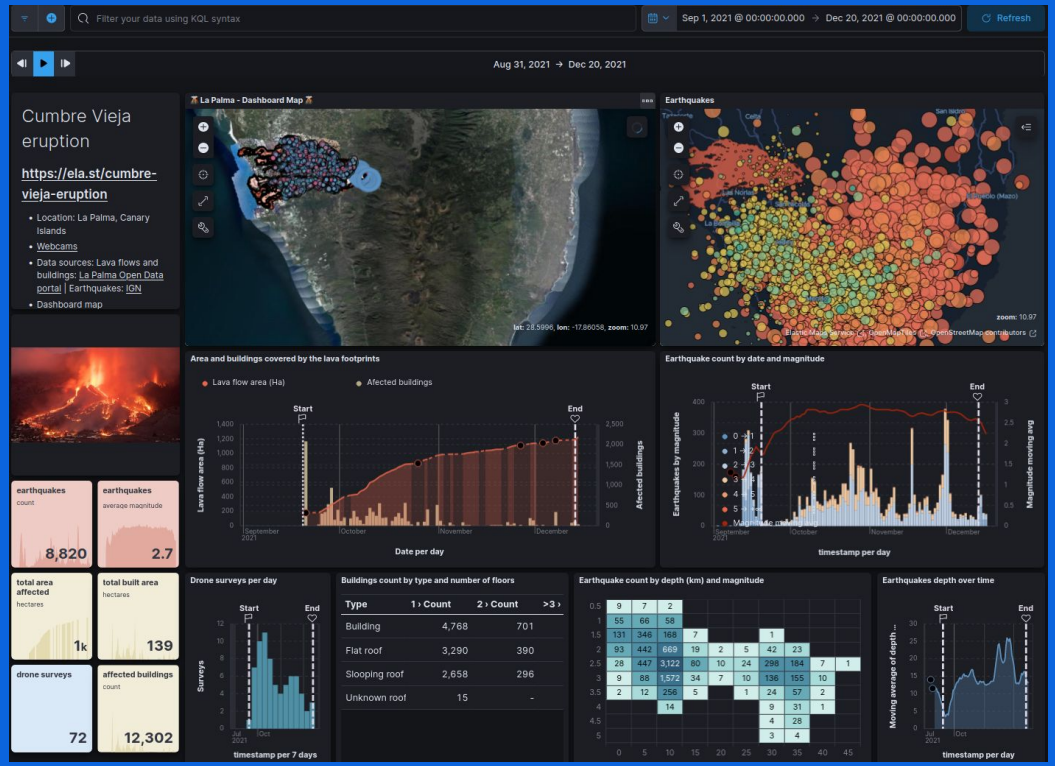
- Explore your fields with a single click
- Drag and drop
- Go from nothing to visual insights with a single mouse gesture.
- Smart suggestions
- Let Lens help guide your analysis with useful chart suggestions



Dashboards

All your information in a single place

- Combine multiple visualizations: **panels**
- Time Range + Search Bar + Filters
- Panels can use filters to perform **drill downs**
- Panels can have custom **time ranges and filters**
- **Share**
- **Export** to PDF or PNG 🛒



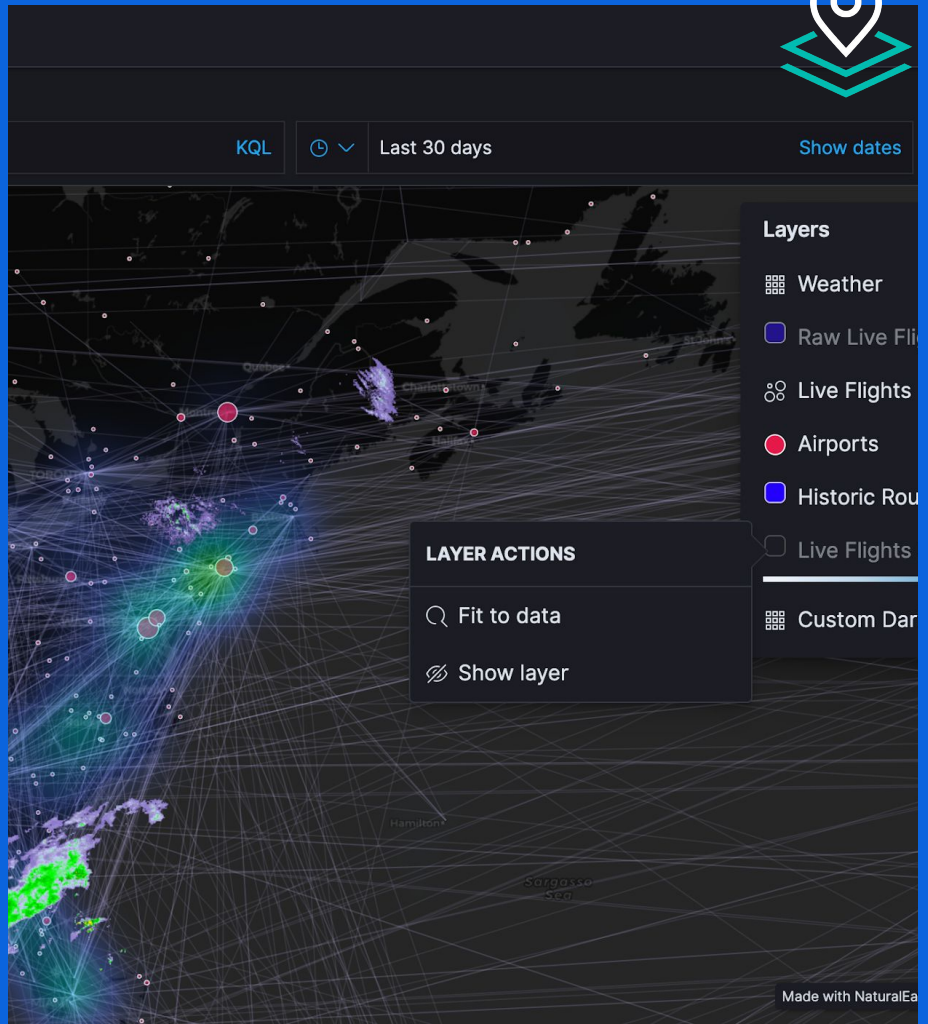
elastic

Elastic Maps

Elastic Maps

Geo Analytics interface within Kibana

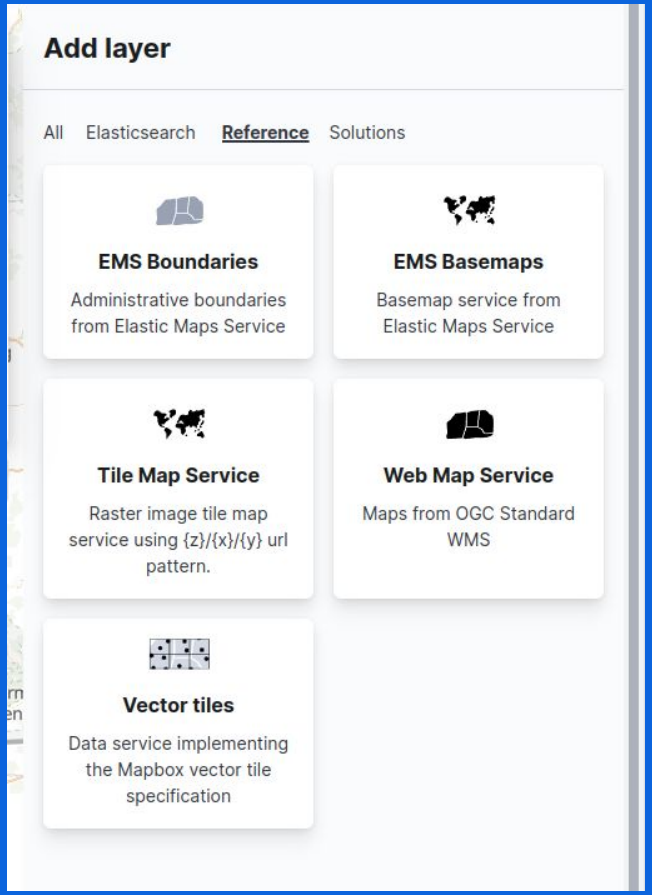
- **Friendly** user experience
- **Aggregations**: heat map, clustering, grids, geoline
- Data driven **styling**
- **Tools** for drawing, filtering, measuring
- Add layers from **external** tile servers
- Used alone or in dashboards
- **Embedded** in other apps



Reference data

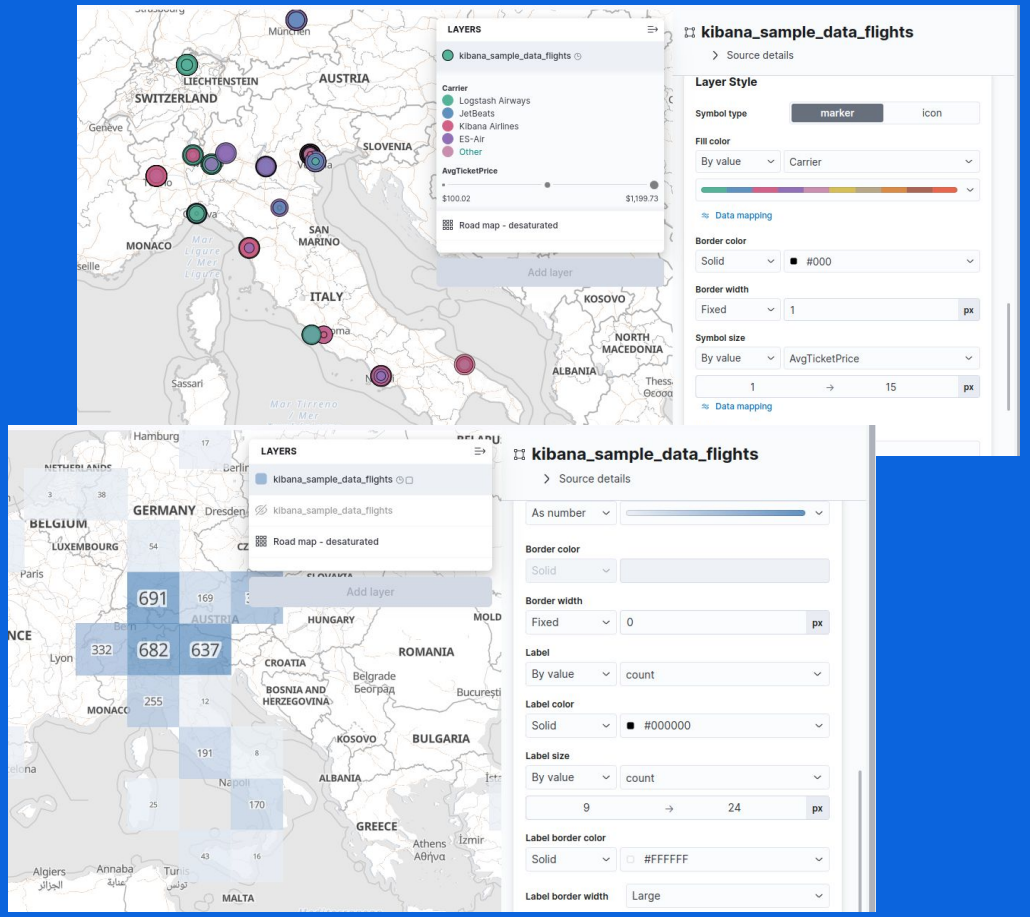
Data that provides context

- Elastic provides **basemaps** (OSM + OpenMapTiles) and **boundaries** (OSM + Natural Earth + Wikidata)
- Third party basemaps providers
  - **WMS**
  - **Tiles Maps Service**
  - **Vector Tiles**



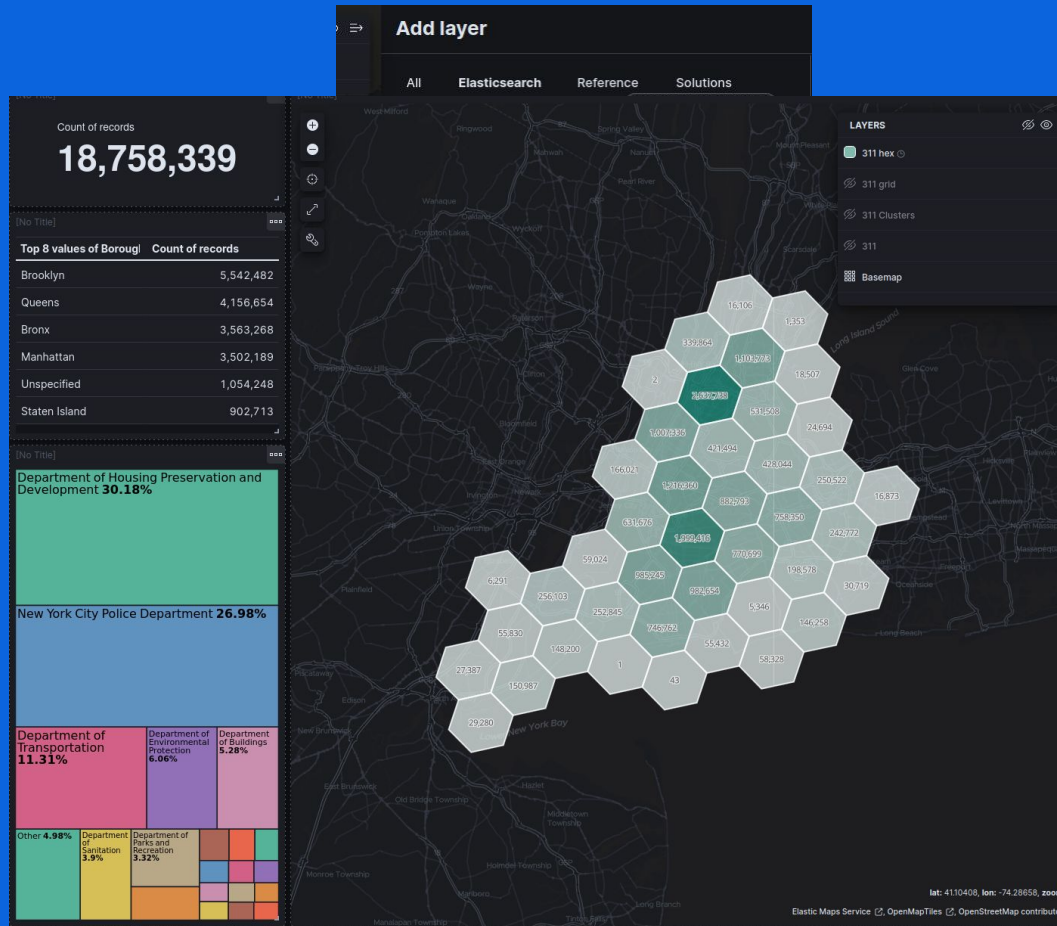
Data Driven Styling

- Quantitative:
  - Size
  - Widths
  - Color ramp
  - Label text
- Qualitative
  - Color palette
  - Label text



Big Data Rendering

- Heatmap
- Clusters
- Tile aggregation
- Hexagon aggregation 🛒

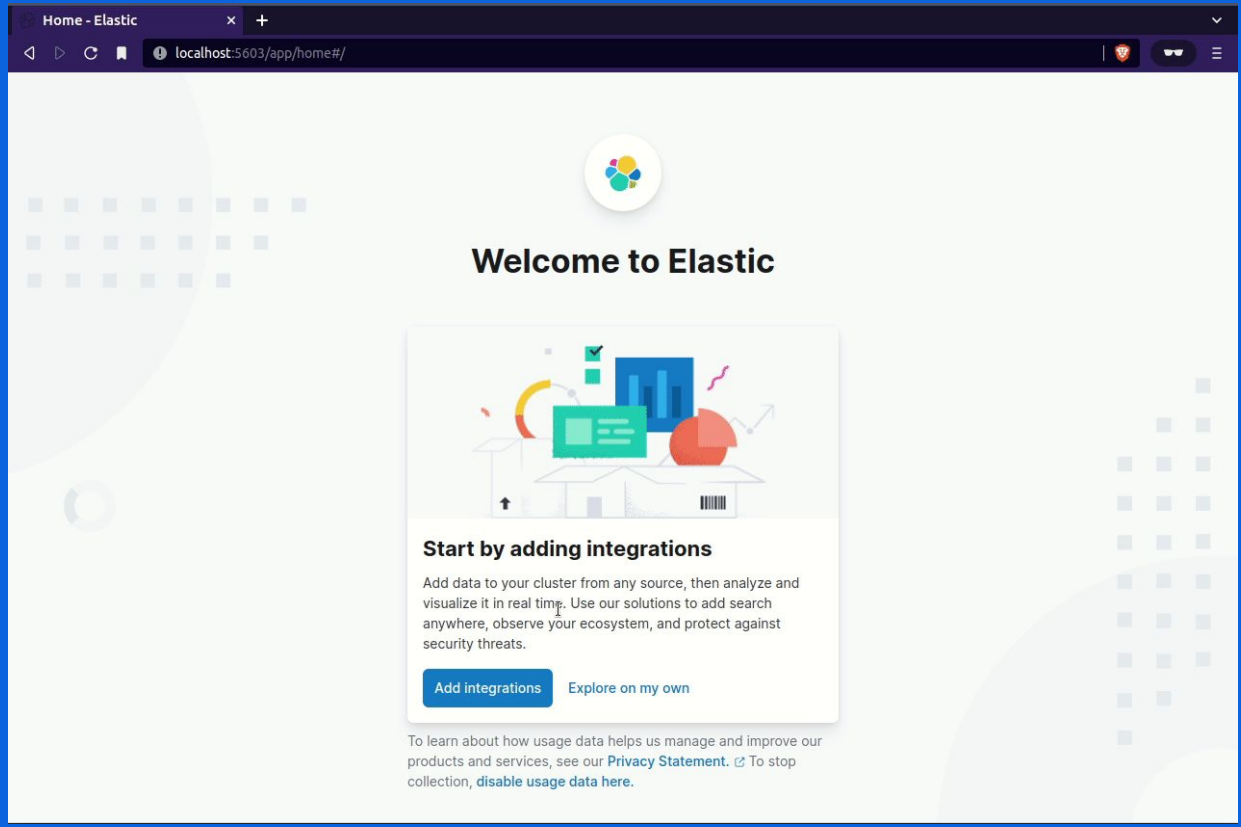


Data Views

Data views

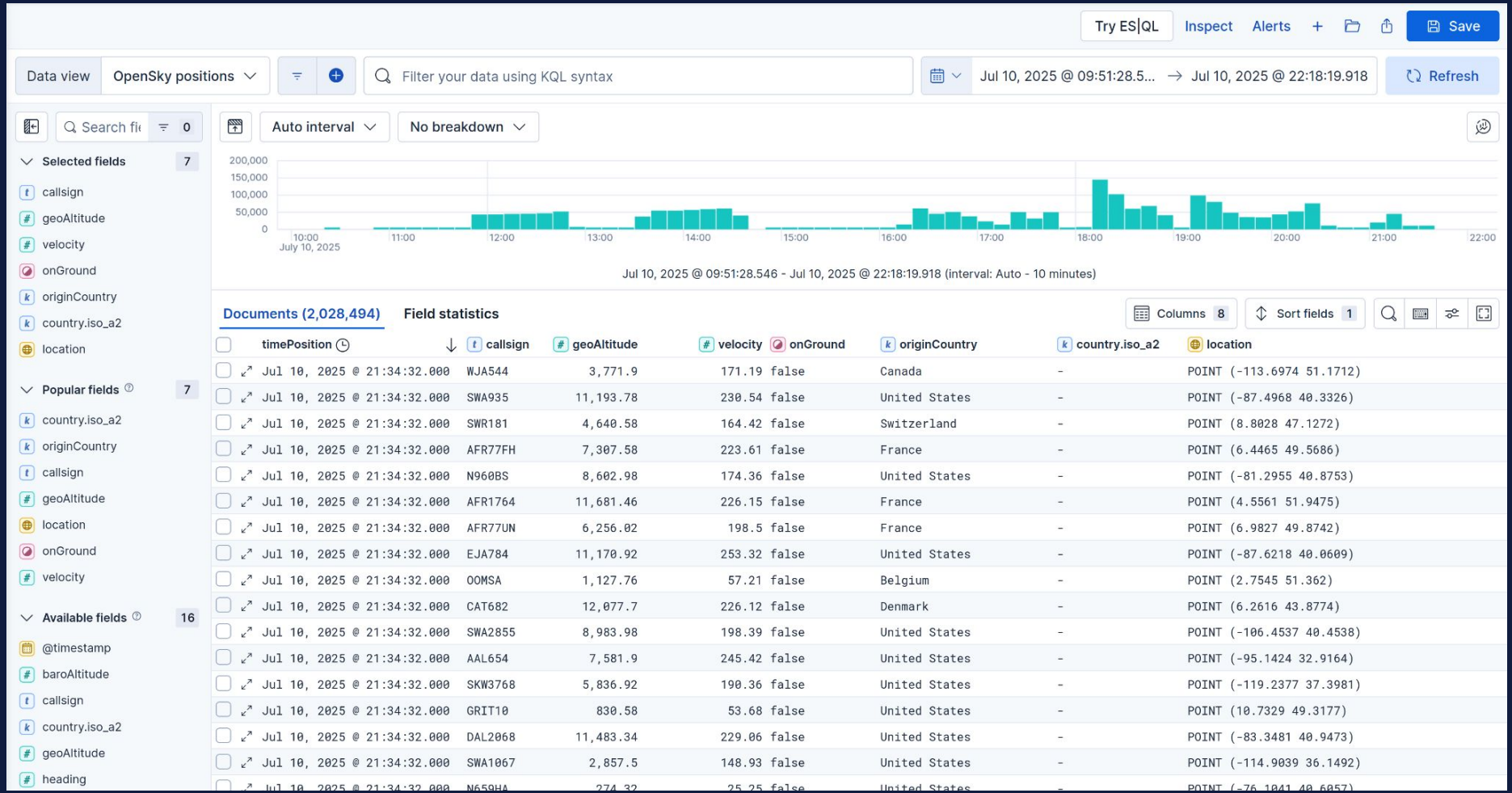
Abstracting index patterns

- A data view is an index pattern (like `places-*`) with some extra metadata
- An optional (but very common) field that defines the time for the document
- Custom formatter for dates, URLs, images, etc.
- Create new computed fields (runtime fields)



elastic

Discover

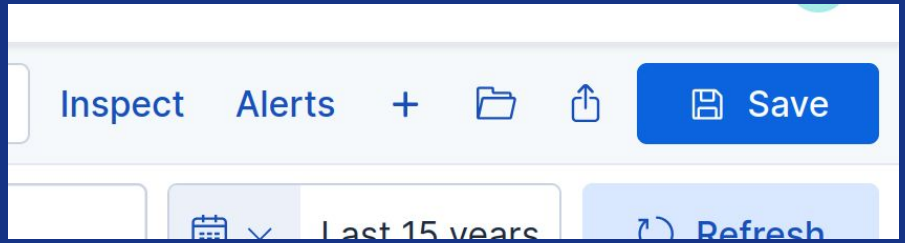


timePosition	callsign	geoAltitude	velocity	onGround	originCountry	country.iso_a2	location
Jul 10, 2025 @ 21:34:32.000	WJA544	3,771.9	171.19	false	Canada	-	POINT (-113.6974 51.1712)
Jul 10, 2025 @ 21:34:32.000	SWA935	11,193.78	230.54	false	United States	-	POINT (-87.4968 40.3326)
Jul 10, 2025 @ 21:34:32.000	SWR181	4,640.58	164.42	false	Switzerland	-	POINT (8.8028 47.1272)
Jul 10, 2025 @ 21:34:32.000	AFR77FH	7,307.58	223.61	false	France	-	POINT (6.4465 49.5686)
Jul 10, 2025 @ 21:34:32.000	N960BS	8,602.98	174.36	false	United States	-	POINT (-81.2955 40.8753)
Jul 10, 2025 @ 21:34:32.000	AFR1764	11,681.46	226.15	false	France	-	POINT (4.5561 51.9475)
Jul 10, 2025 @ 21:34:32.000	AFR77UN	6,256.02	198.5	false	France	-	POINT (6.9827 49.8742)
Jul 10, 2025 @ 21:34:32.000	EJA784	11,170.92	253.32	false	United States	-	POINT (-87.6218 40.0609)
Jul 10, 2025 @ 21:34:32.000	OOMSA	1,127.76	57.21	false	Belgium	-	POINT (2.7545 51.362)
Jul 10, 2025 @ 21:34:32.000	CAT682	12,077.7	226.12	false	Denmark	-	POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000	SWA2855	8,983.98	198.39	false	United States	-	POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000	AAL654	7,581.9	245.42	false	United States	-	POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000	SKW3768	5,836.92	190.36	false	United States	-	POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000	GRIT10	830.58	53.68	false	United States	-	POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000	DAL2068	11,483.34	229.06	false	United States	-	POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000	SWA1067	2,857.5	148.93	false	United States	-	POINT (-114.9039 36.1492)
Jul 10, 2025 @ 21:34:32.000	N659HA	274.32	25.25	false	United States	-	POINT (-76.1041 40.6057)

Search sessions

Persist your common search settings

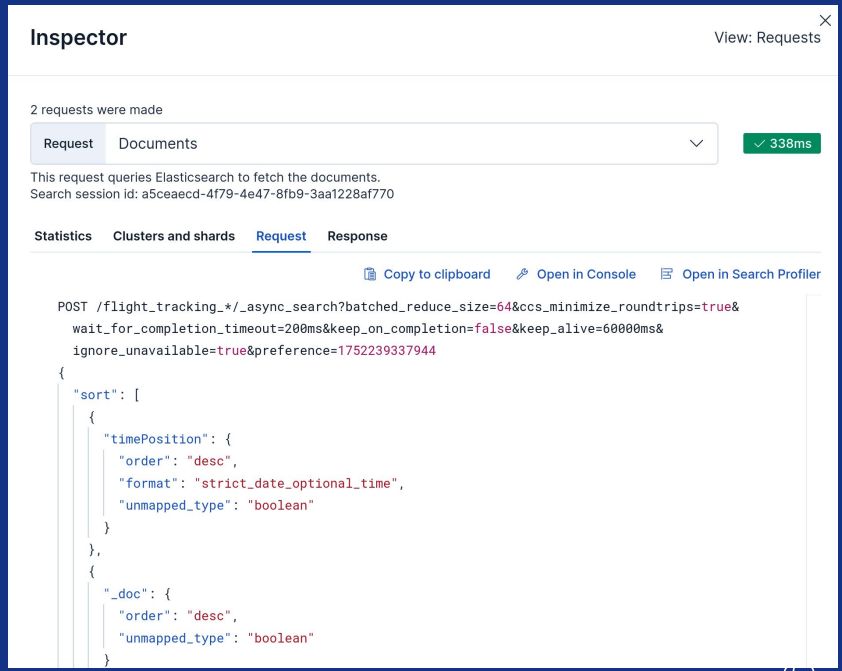
- Save and restore
- Can be added to dashboards
- Can be exported as links or CSV



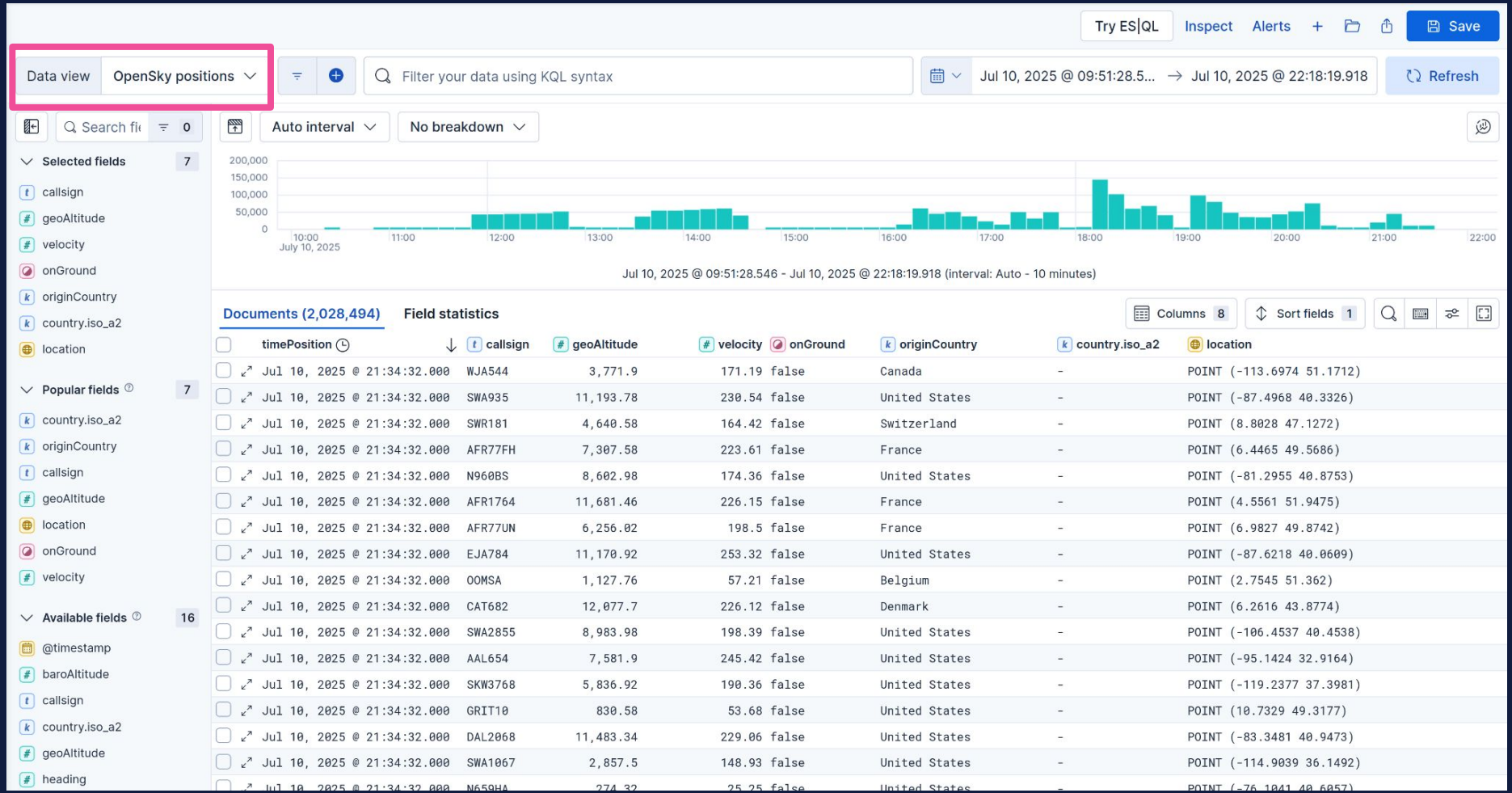
Inspector

Get details of your queries to Elasticsearch

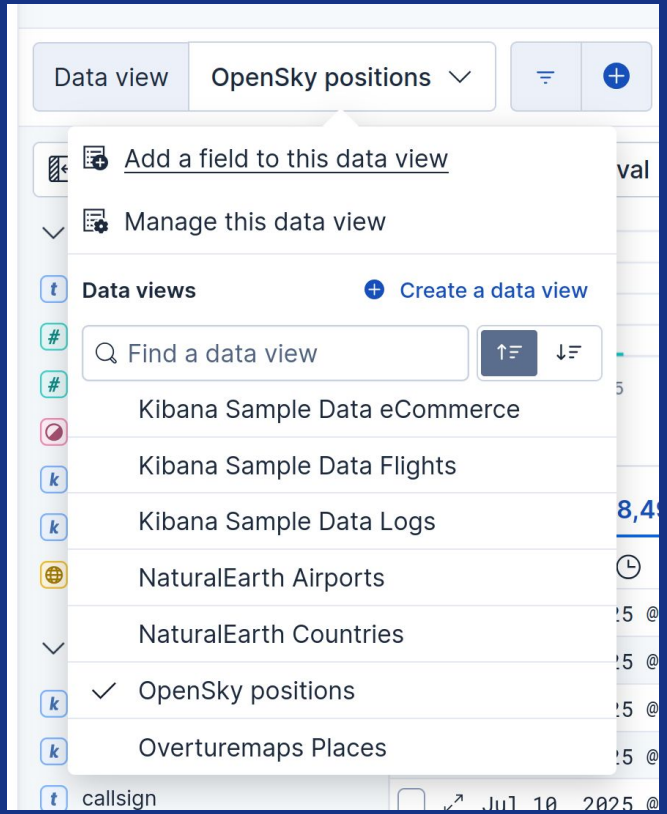
- Metadata about the query execution
- Request to Elasticsearch
- Response details



elastic


Try ES|QL
Inspect
Alerts
Save
Data view
OpenSky positions
Filter your data using KQL syntax
Jul 10, 2025 @ 09:51:28.5...
Jul 10, 2025 @ 22:18:19.918
Refresh
Search fi
0
Auto interval
No breakdown
200,000
150,000
100,000
50,000
0
10:00
July 10, 2025
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
Jul 10, 2025 @ 09:51:28.546 - Jul 10, 2025 @ 22:18:19.918 (interval: Auto - 10 minutes)
Selected fields 7
callsign
geoAltitude
velocity
onGround
originCountry
country.iso_a2
location
Popular fields 7
country.iso_a2
originCountry
callsign
geoAltitude
location
onGround
velocity
Available fields 16
@timestamp
baroAltitude
callsign
country.iso_a2
geoAltitude
heading
Documents (2,028,494)
Field statistics
Columns 8
Sort fields 1
timePosition
callsign
geoAltitude
velocity
onGround
originCountry
country.iso_a2
location
Jul 10, 2025 @ 21:34:32.000 WJA544 3,771.9 171.19 false Canada - POINT (-113.6974 51.1712)
Jul 10, 2025 @ 21:34:32.000 SWA935 11,193.78 230.54 false United States - POINT (-87.4968 40.3326)
Jul 10, 2025 @ 21:34:32.000 SWR181 4,640.58 164.42 false Switzerland - POINT (8.8028 47.1272)
Jul 10, 2025 @ 21:34:32.000 AFR77FH 7,307.58 223.61 false France - POINT (6.4465 49.5686)
Jul 10, 2025 @ 21:34:32.000 N960BS 8,602.98 174.36 false United States - POINT (-81.2955 40.8753)
Jul 10, 2025 @ 21:34:32.000 AFR1764 11,681.46 226.15 false France - POINT (4.5561 51.9475)
Jul 10, 2025 @ 21:34:32.000 AFR77UN 6,256.02 198.5 false France - POINT (6.9827 49.8742)
Jul 10, 2025 @ 21:34:32.000 EJA784 11,170.92 253.32 false United States - POINT (-87.6218 40.0609)
Jul 10, 2025 @ 21:34:32.000 OOMSA 1,127.76 57.21 false Belgium - POINT (2.7545 51.362)
Jul 10, 2025 @ 21:34:32.000 CAT682 12,077.7 226.12 false Denmark - POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000 SWA2855 8,983.98 198.39 false United States - POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000 AAL654 7,581.9 245.42 false United States - POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000 SKW3768 5,836.92 190.36 false United States - POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000 GRIT10 830.58 53.68 false United States - POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000 DAL2068 11,483.34 229.06 false United States - POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000 SWA1067 2,857.5 148.93 false United States - POINT (-114.9039 36.1492)

Data View selector



Try ES|QL | Inspect | Alerts | Save

Data view: OpenSky positions

Filter your data using KQL syntax

Jul 10, 2025 @ 09:51:28.5... → Jul 10, 2025 @ 22:18:19.918

Refresh

Search fi 0

Auto interval | No breakdown

Jul 10, 2025 @ 09:51:28.546 - Jul 10, 2025 @ 22:18:19.918 (interval: Auto - 10 minutes)

Selected fields 7
- callsign
- geoAltitude
- velocity
- onGround
- originCountry
- country.iso_a2
- location

Popular fields 7
- country.iso_a2
- originCountry
- callsign
- geoAltitude
- location
- onGround
- velocity

Available fields 16
- @timestamp
- baroAltitude
- callsign
- country.iso_a2
- geoAltitude
- heading

Documents (2,028,494) | Field statistics

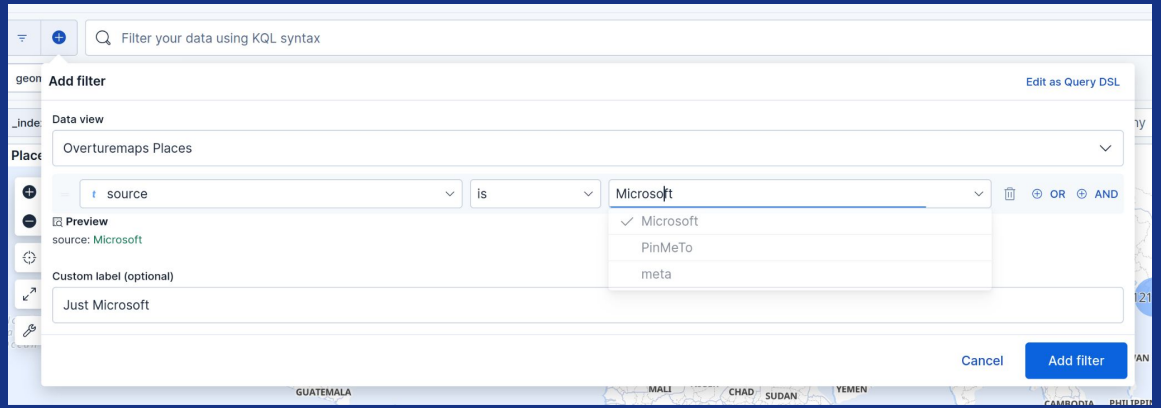
Columns 8 | Sort fields 1

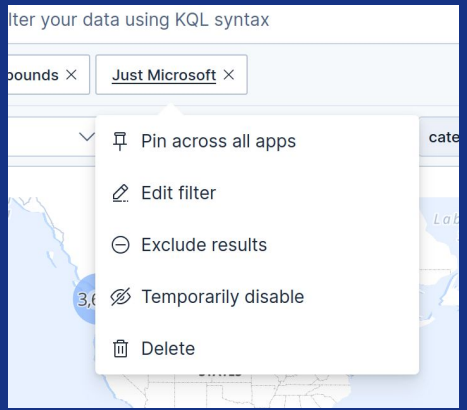
timePosition	callsign	geoAltitude	velocity	onGround	originCountry	country.iso_a2	location
Jul 10, 2025 @ 21:34:32.000	WJA544	3,771.9	171.19	false	Canada	-	POINT (-113.6974 51.1712)
Jul 10, 2025 @ 21:34:32.000	SWA935	11,193.78	230.54	false	United States	-	POINT (-87.4968 40.3326)
Jul 10, 2025 @ 21:34:32.000	SWR181	4,640.58	164.42	false	Switzerland	-	POINT (8.8028 47.1272)
Jul 10, 2025 @ 21:34:32.000	AFR77FH	7,307.58	223.61	false	France	-	POINT (6.4465 49.5686)
Jul 10, 2025 @ 21:34:32.000	N960BS	8,602.98	174.36	false	United States	-	POINT (-81.2955 40.8753)
Jul 10, 2025 @ 21:34:32.000	AFR1764	11,681.46	226.15	false	France	-	POINT (4.5561 51.9475)
Jul 10, 2025 @ 21:34:32.000	AFR77UN	6,256.02	198.5	false	France	-	POINT (6.9827 49.8742)
Jul 10, 2025 @ 21:34:32.000	EJA784	11,170.92	253.32	false	United States	-	POINT (-87.6218 40.0609)
Jul 10, 2025 @ 21:34:32.000	OOMSA	1,127.76	57.21	false	Belgium	-	POINT (2.7545 51.362)
Jul 10, 2025 @ 21:34:32.000	CAT682	12,077.7	226.12	false	Denmark	-	POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000	SWA2855	8,983.98	198.39	false	United States	-	POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000	AAL654	7,581.9	245.42	false	United States	-	POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000	SKW3768	5,836.92	190.36	false	United States	-	POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000	GRIT10	830.58	53.68	false	United States	-	POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000	DAL2068	11,483.34	229.06	false	United States	-	POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000	SWA1067	2,857.5	148.93	false	United States	-	POINT (-114.9039 36.1492)
Jul 10, 2025 @ 21:34:32.000	N659HA	274.32	25.25	false	United States	-	POINT (-76.1041 40.6057)

Filters

Versatile pills for filtering

- Easy filter creation, but DSL also available
- Custom label
- Transferred across dashboards and applications
- Also available on view mode



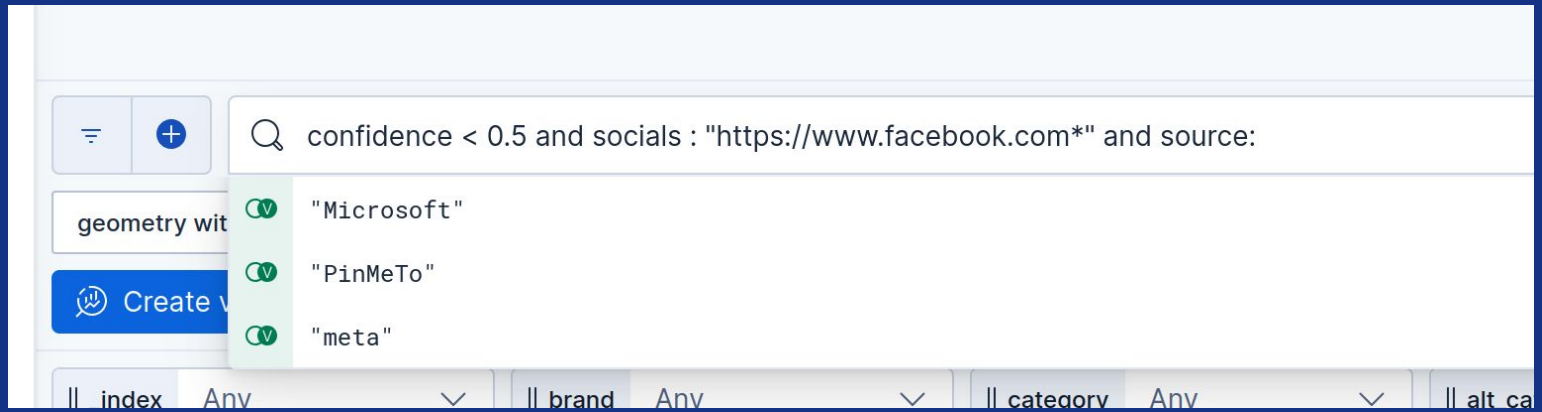


elastic

Query bar

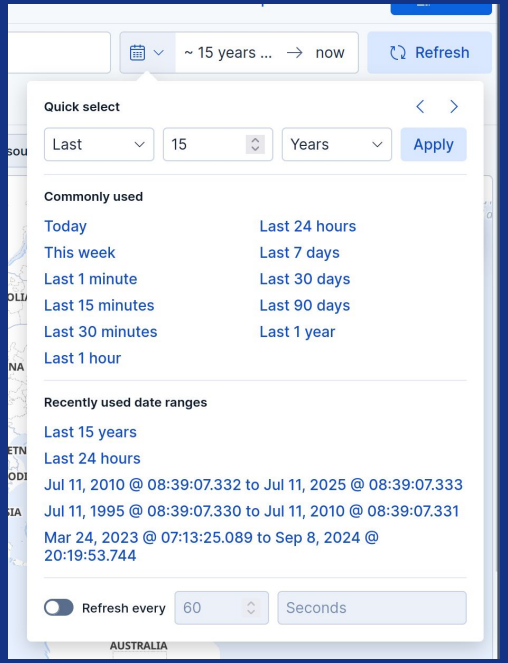
Advanced ad-hoc queries

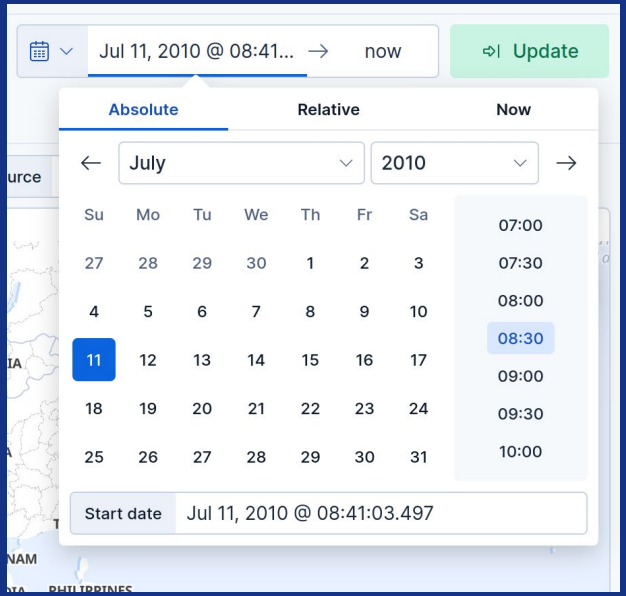
- Kibana Query Language
- Autocomplete for fields and values
- Can be saved in the dashboard definition and used in view mode

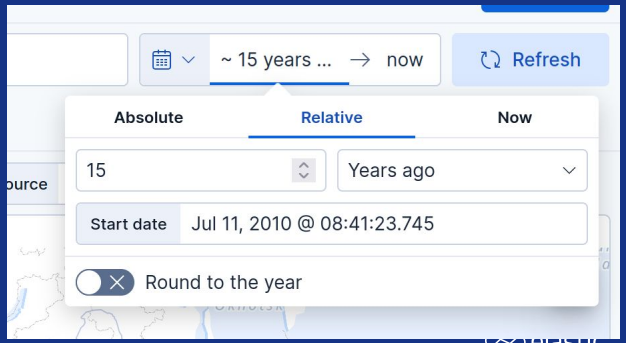


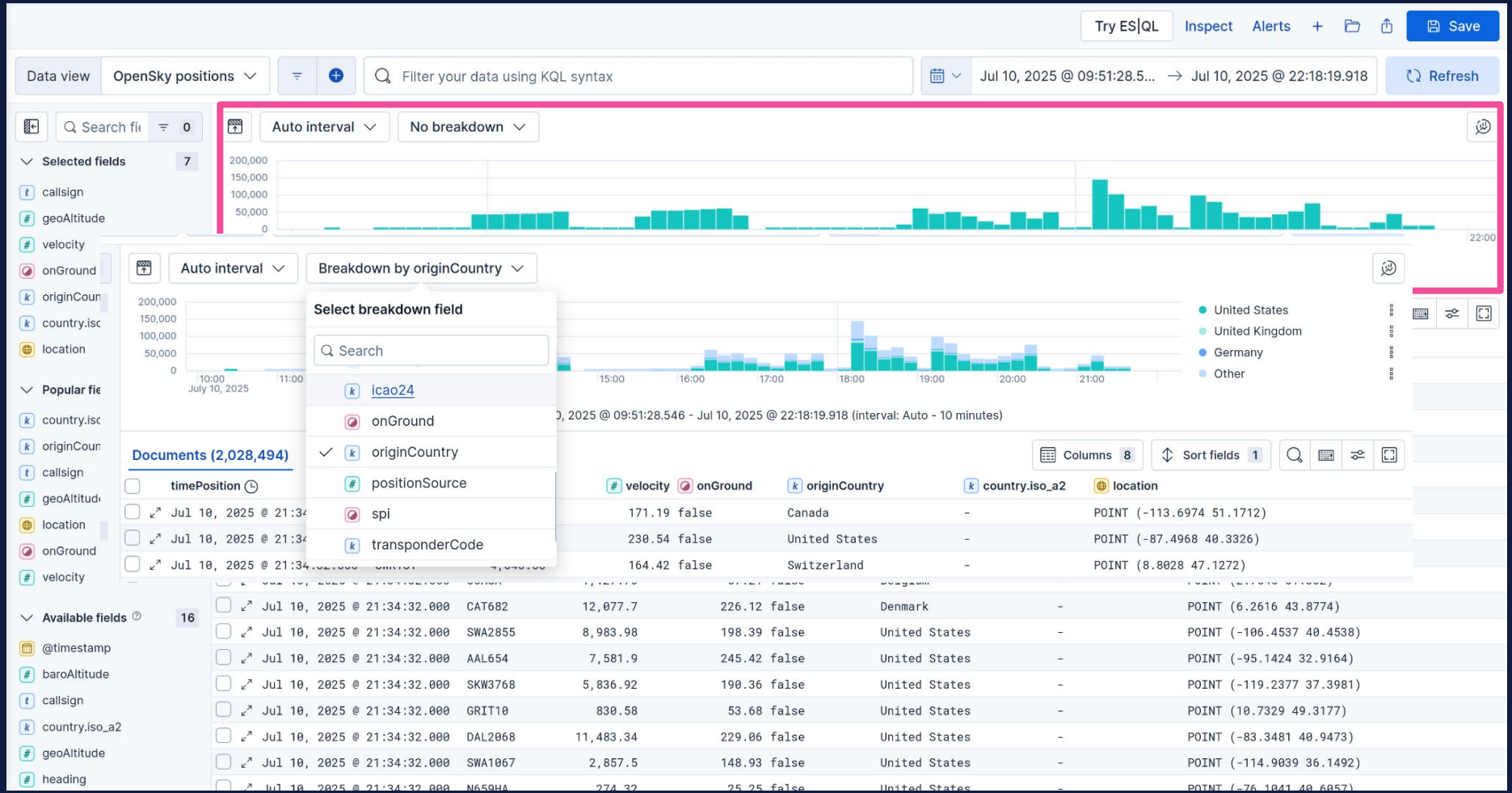
Time picker

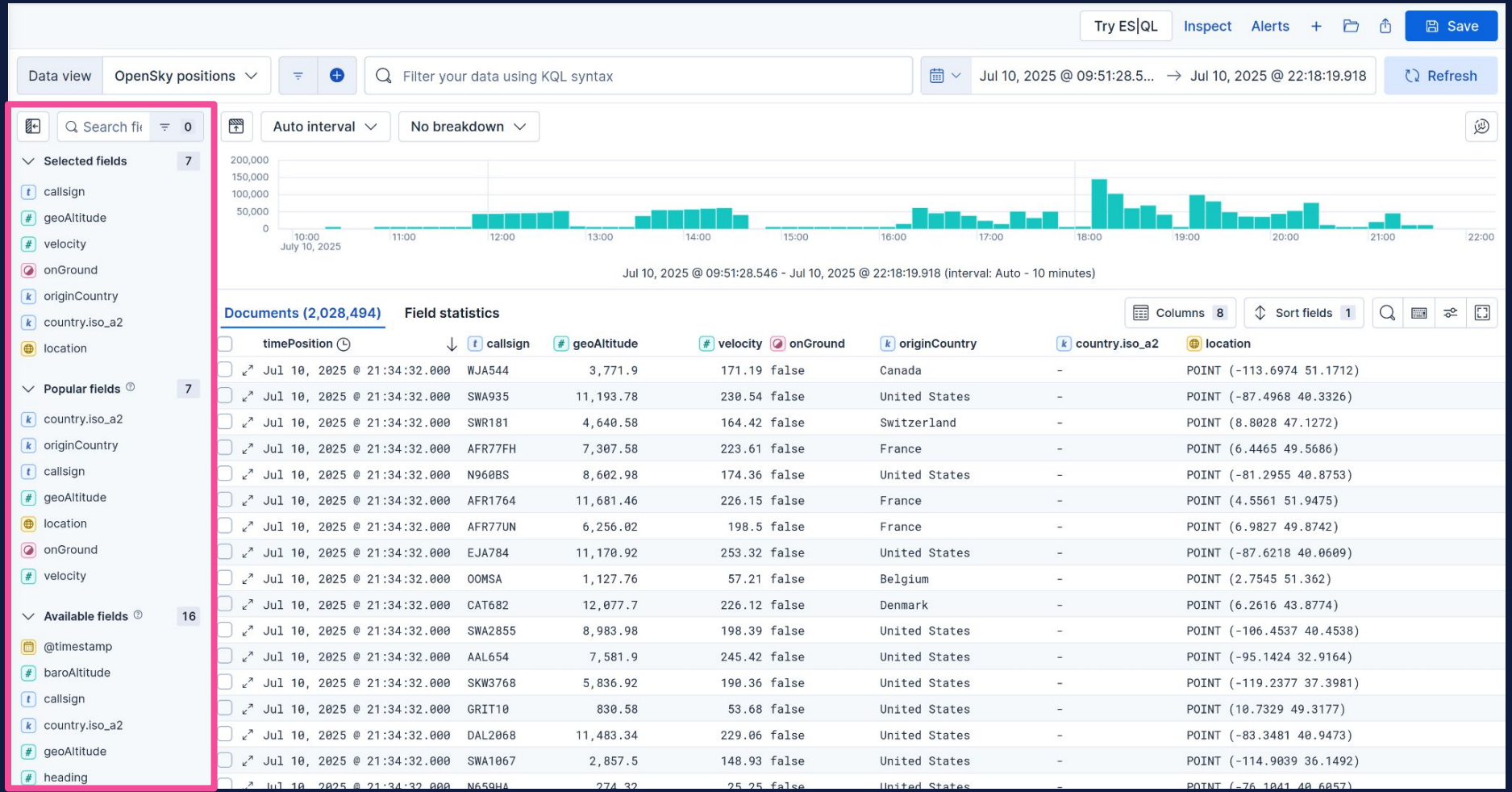
- Flexible time range selector with quick, absolute and relative selections.
- Auto-refresh








Try ES|QL
Inspect
Alerts
Save
Data view
OpenSky positions
Filter your data using KQL syntax
Jul 10, 2025 @ 09:51:28.5...
Jul 10, 2025 @ 22:18:19.918
Refresh
Auto interval
No breakdown
Selected fields 7
callsign
geoAltitude
velocity
onGround
originCoun
country.isc
location
Popular fie
Available fields 16
@timestamp
baroAltitude
callsign
country.iso_a2
geoAltitude
heading
Auto interval
Breakdown by originCountry
Select breakdown field
Search
icao24
onGround
originCountry
positionSource
spi
transponderCode
United States
United Kingdom
Germany
Other
Documents (2,028,494)
Columns 8
Sort fields 1
timePosition
velocity
onGround
originCountry
country.iso_a2
location
Jul 10, 2025 @ 21:34:32.000 CAT682 12,077.7 226.12 false Denmark - POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000 SWA2855 8,983.98 198.39 false United States - POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000 AAL654 7,581.9 245.42 false United States - POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000 SKW3768 5,836.92 190.36 false United States - POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000 GRIT10 830.58 53.68 false United States - POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000 DAL2068 11,483.34 229.06 false United States - POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000 SWA1067 2,857.5 148.93 false United States - POINT (-114.9039 36.1492)



timePosition	callsign	geoAltitude	velocity	onGround	originCountry	country.iso_a2	location
Jul 10, 2025 @ 21:34:32.000	WJA544	3,771.9	171.19	false	Canada	-	POINT (-113.6974 51.1712)
Jul 10, 2025 @ 21:34:32.000	SWA935	11,193.78	230.54	false	United States	-	POINT (-87.4968 40.3326)
Jul 10, 2025 @ 21:34:32.000	SWR181	4,640.58	164.42	false	Switzerland	-	POINT (8.8028 47.1272)
Jul 10, 2025 @ 21:34:32.000	AFR77FH	7,307.58	223.61	false	France	-	POINT (6.4465 49.5686)
Jul 10, 2025 @ 21:34:32.000	N960BS	8,602.98	174.36	false	United States	-	POINT (-81.2955 40.8753)
Jul 10, 2025 @ 21:34:32.000	AFR1764	11,681.46	226.15	false	France	-	POINT (4.5561 51.9475)
Jul 10, 2025 @ 21:34:32.000	AFR77UN	6,256.02	198.5	false	France	-	POINT (6.9827 49.8742)
Jul 10, 2025 @ 21:34:32.000	EJA784	11,170.92	253.32	false	United States	-	POINT (-87.6218 40.0609)
Jul 10, 2025 @ 21:34:32.000	OOMSA	1,127.76	57.21	false	Belgium	-	POINT (2.7545 51.362)
Jul 10, 2025 @ 21:34:32.000	CAT682	12,077.7	226.12	false	Denmark	-	POINT (6.2616 43.8774)
Jul 10, 2025 @ 21:34:32.000	SWA2855	8,983.98	198.39	false	United States	-	POINT (-106.4537 40.4538)
Jul 10, 2025 @ 21:34:32.000	AAL654	7,581.9	245.42	false	United States	-	POINT (-95.1424 32.9164)
Jul 10, 2025 @ 21:34:32.000	SKW3768	5,836.92	190.36	false	United States	-	POINT (-119.2377 37.3981)
Jul 10, 2025 @ 21:34:32.000	GRIT10	830.58	53.68	false	United States	-	POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000	DAL2068	11,483.34	229.06	false	United States	-	POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000	SWA1067	2,857.5	148.93	false	United States	-	POINT (-114.9039 36.1492)
Jul 10, 2025 @ 21:34:32.000	N659HA	274.32	25.25	false	United States	-	POINT (-76.1041 40.6057)

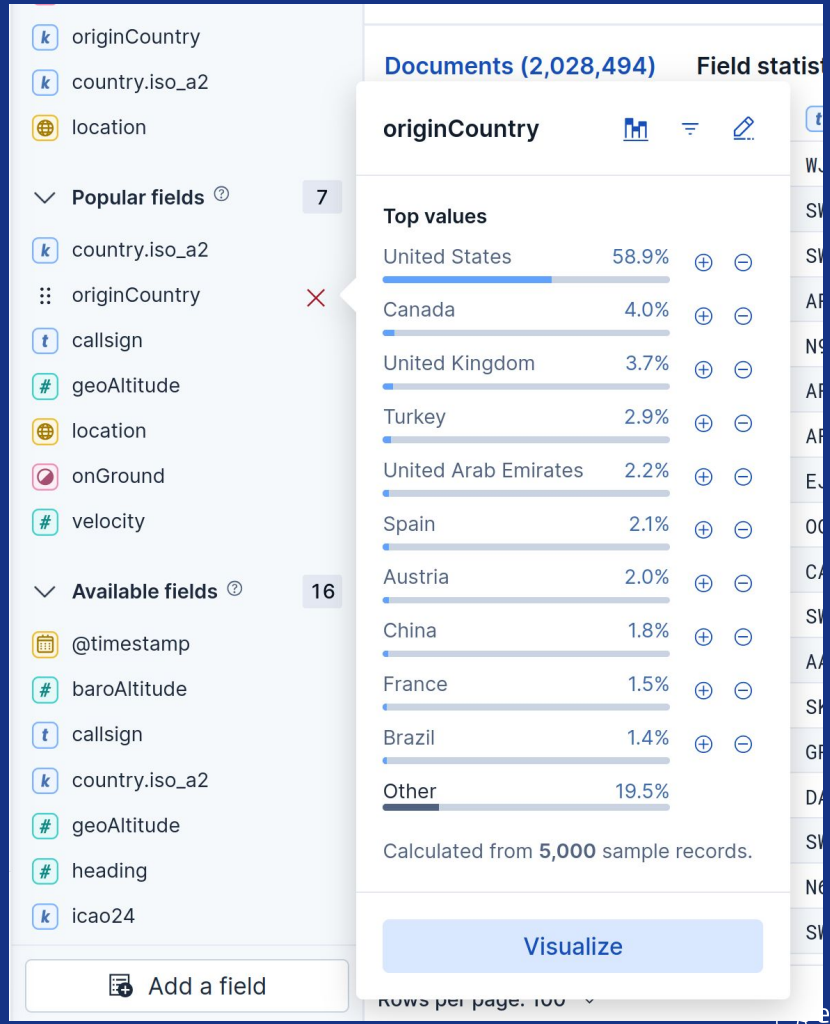
Selecting fields

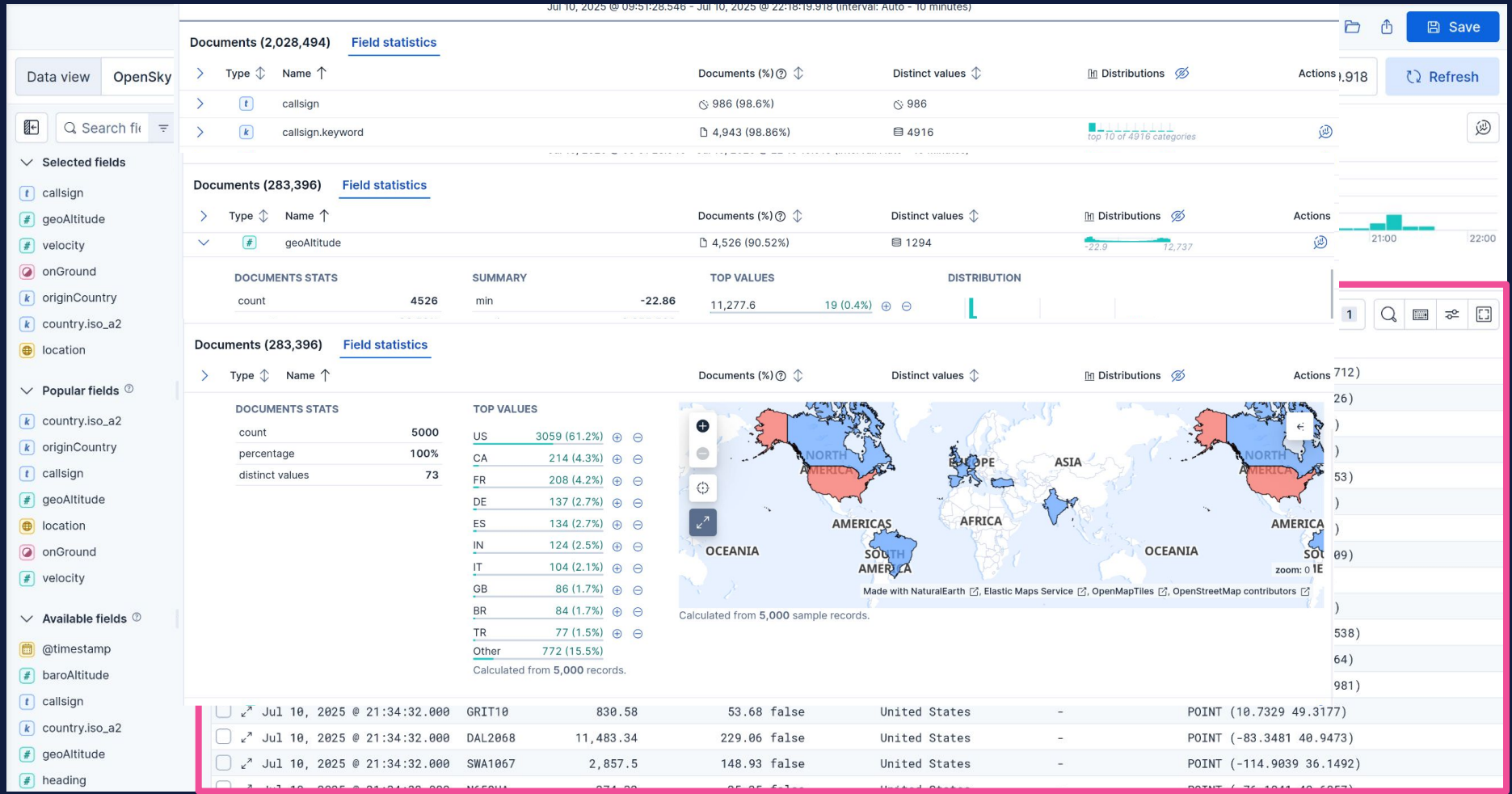
Click on a field to reveal basic information

- Filter in/out for any of the top values
- Visualize: jump to chart authoring for this field

In the quick actions

- Create a filter for this field to be present
- Add the field to the histogram breakdown
- Edit the Data View field

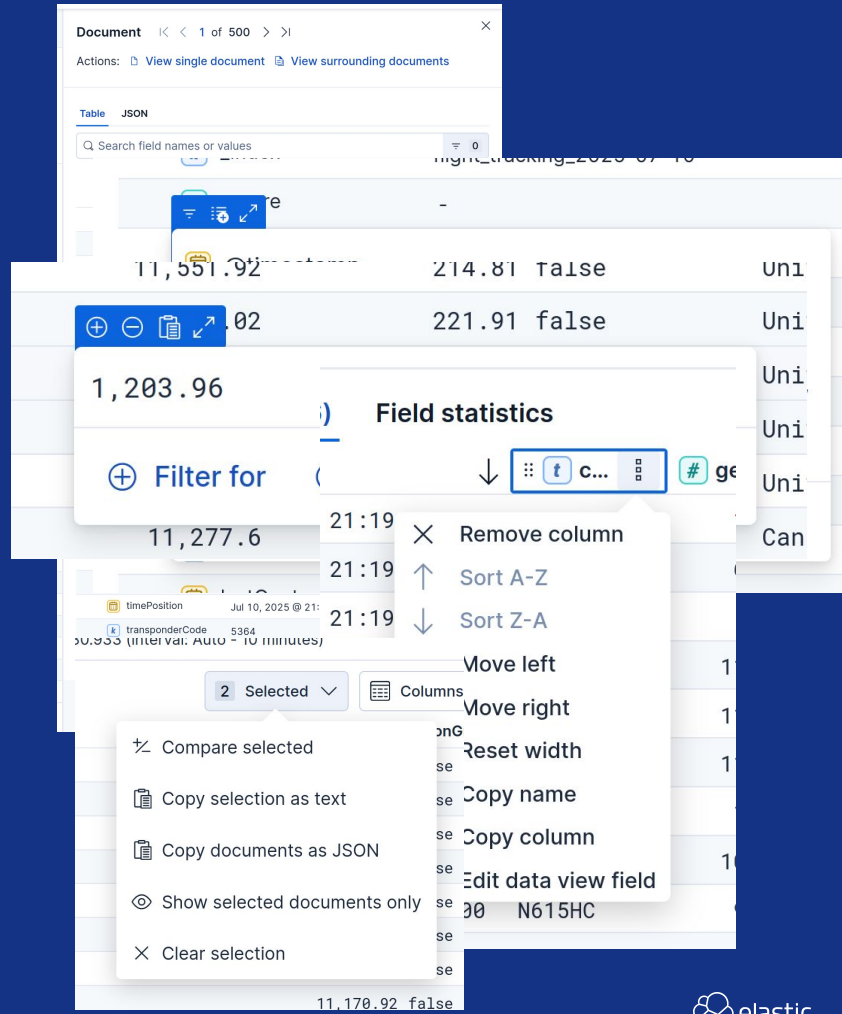



Jul 10, 2025 @ 09:51:28.546 - Jul 10, 2025 @ 22:18:19.918 (interval: Auto - 10 minutes)
Save
Refresh
Data view
OpenSky
Search fie
Selected fields
callsign
geoAltitude
velocity
onGround
originCountry
country.iso_a2
location
Popular fields
country.iso_a2
originCountry
callsign
geoAltitude
location
onGround
velocity
Available fields
@timestamp
baroAltitude
callsign
country.iso_a2
geoAltitude
heading
Documents (2,028,494)
Field statistics
Type
Name
Documents (%)
Distinct values
Distributions
Actions
callsign
986 (98.6%)
986
callsign.keyword
4,943 (98.86%)
4916
top 10 of 4916 categories
Documents (283,396)
Field statistics
geoAltitude
4,526 (90.52%)
1294
-22.9
12,737
DOCUMENTS STATS
count 4526
SUMMARY
min -22.86
TOP VALUES
11,277.6 19 (0.4%)
DISTRIBUTION
Documents (283,396)
Field statistics
DOCUMENTS STATS
count 5000
percentage 100%
distinct values 73
TOP VALUES
US 3059 (61.2%)
CA 214 (4.3%)
FR 208 (4.2%)
DE 137 (2.7%)
ES 134 (2.7%)
IN 124 (2.5%)
IT 104 (2.1%)
GB 86 (1.7%)
BR 84 (1.7%)
TR 77 (1.5%)
Other 772 (15.5%)
Calculated from 5,000 records.
NORTH AMERICA
EUROPE
ASIA
AFRICA
AMERICAS
OCEANIA
SOUTH AMERICA
zoom: 0
Made with NaturalEarth, Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Calculated from 5,000 sample records.
Jul 10, 2025 @ 21:34:32.000 GRIT10 830.58 53.68 false United States - POINT (10.7329 49.3177)
Jul 10, 2025 @ 21:34:32.000 DAL2068 11,483.34 229.06 false United States - POINT (-83.3481 40.9473)
Jul 10, 2025 @ 21:34:32.000 SWA1067 2,857.5 148.93 false United States - POINT (-114.9039 36.1492)

Documents table

View everything about each indexed document

- Toggle document viewer (table or raw JSON)
  - Quick actions on field names
- Click on any value to filter in/out
- Click on any column header to sort/shift
- Select documents to compare or copy them

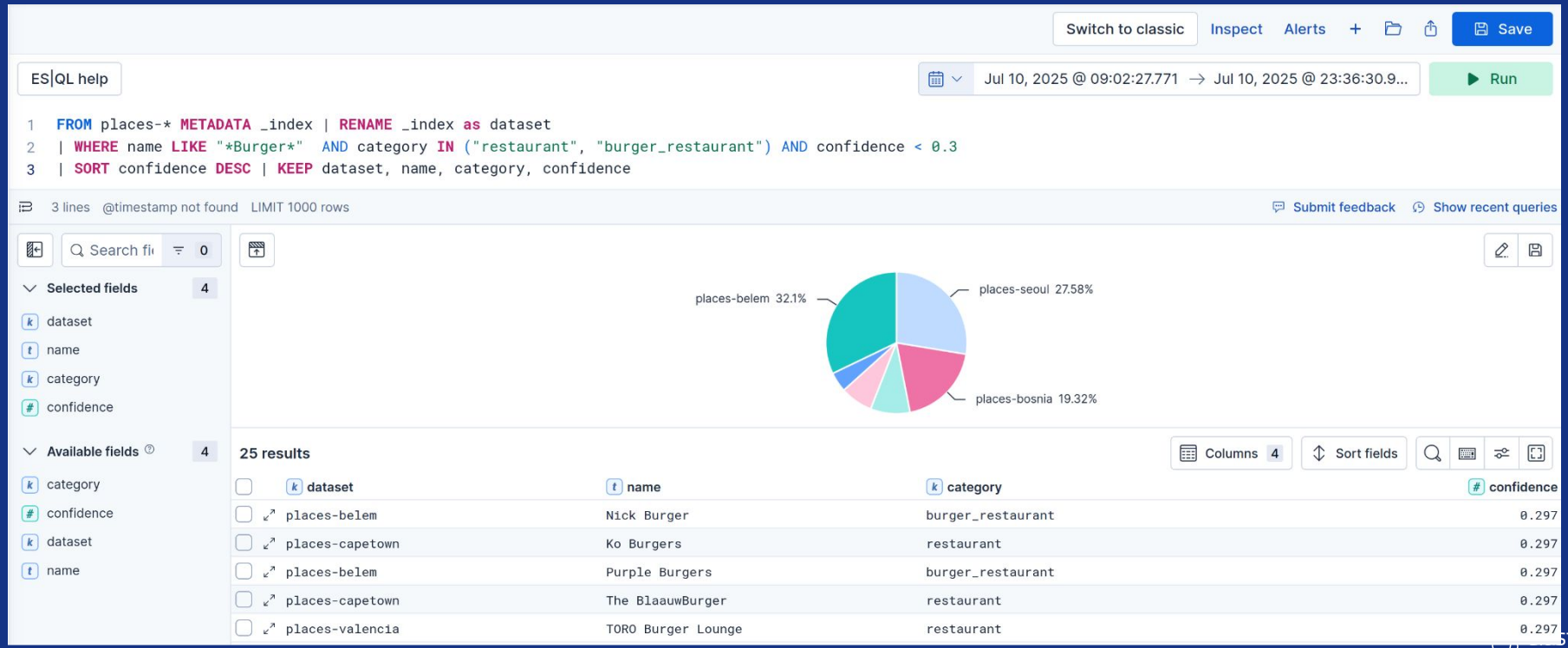


elastic

Discover & ES|QL

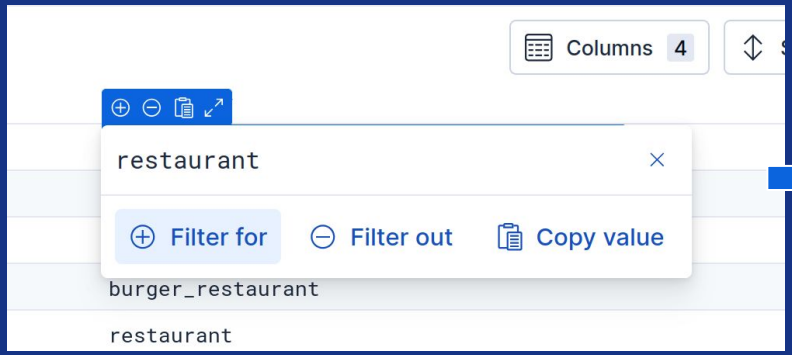
Discover & ES|QL

Rich editor for ES|QL replacing Data Views for data exploration and manipulation

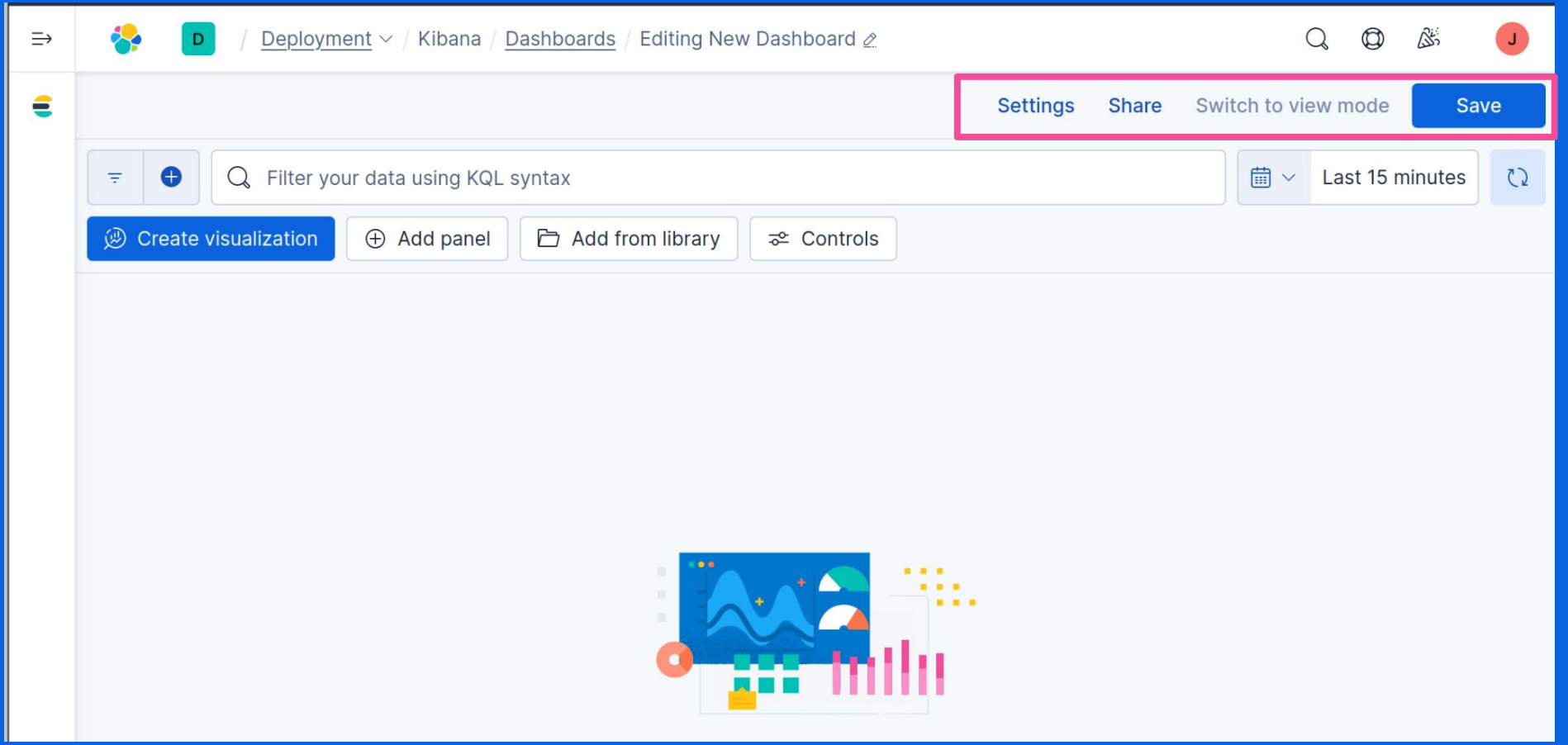


Discover & ES|QL

Interactions in fields and values are translated into new query piped commands

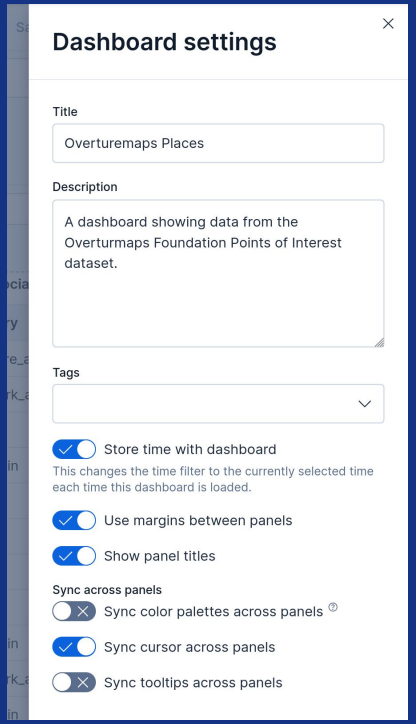


Dashboards


D
Deployment
Kibana
Dashboards
Editing New Dashboard
J
Settings
Share
Switch to view mode
Save
Filter your data using KQL syntax
Last 15 minutes
Create visualization
Add panel
Add from library
Controls

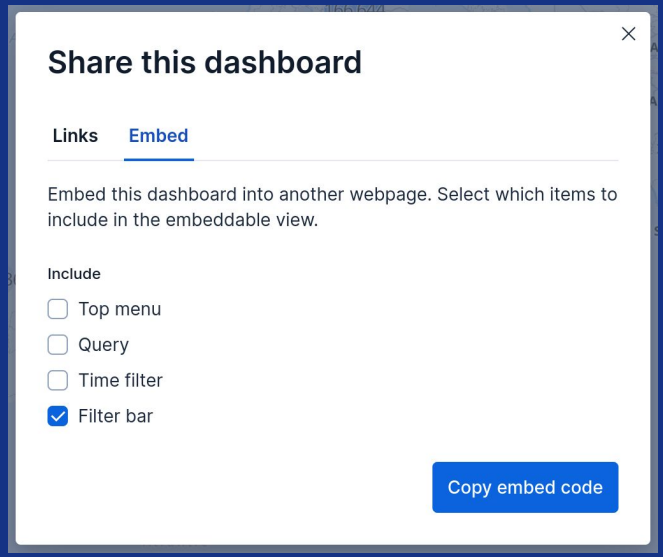
Settings

Metadata and general appearance

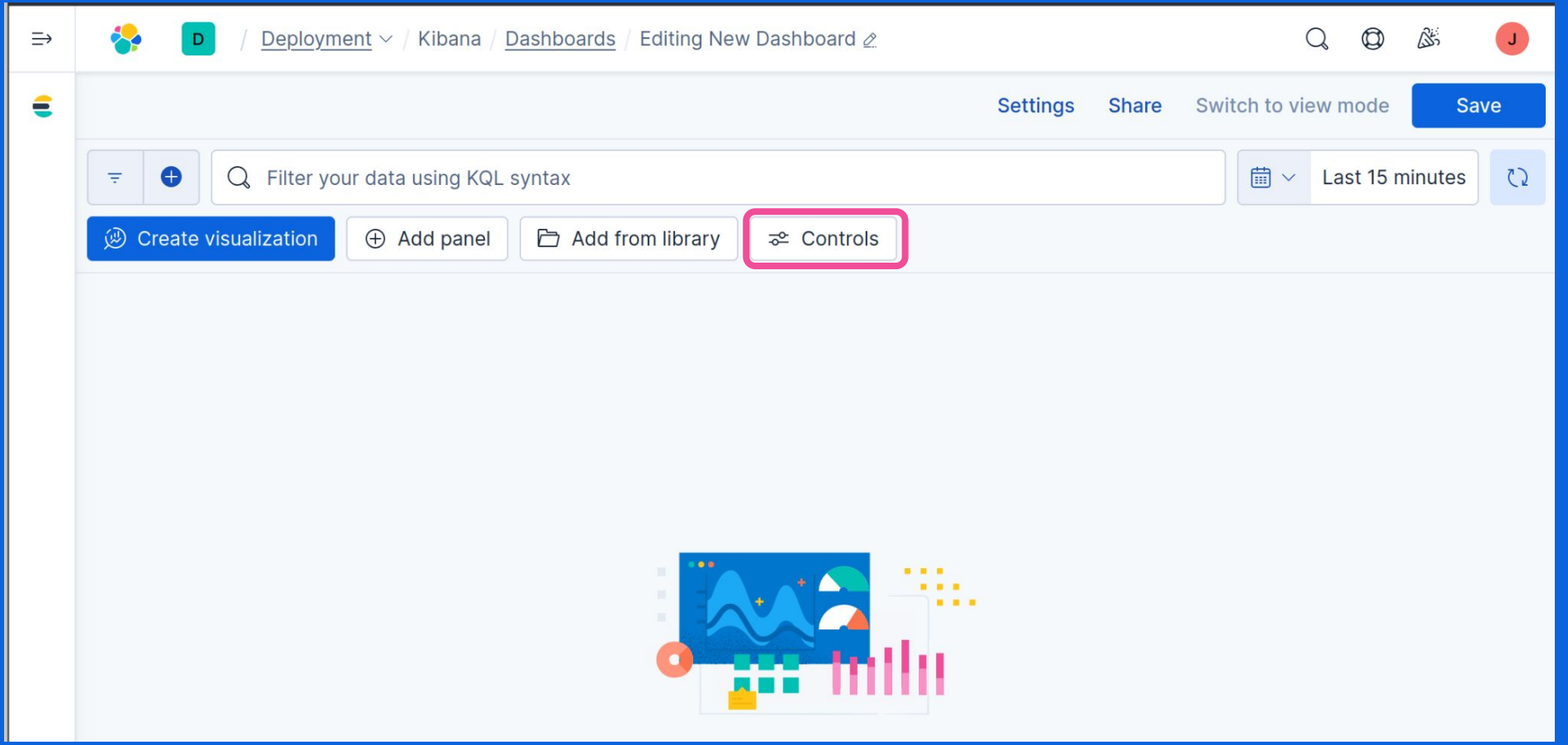


Share

Generate links to your dashboard or get the embed code (iframe)

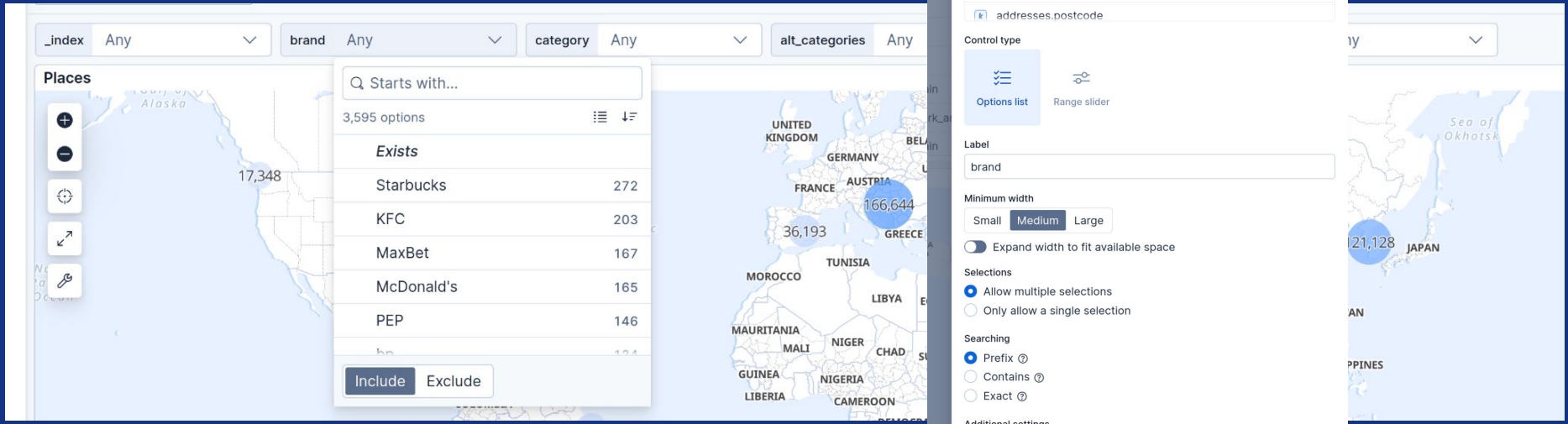


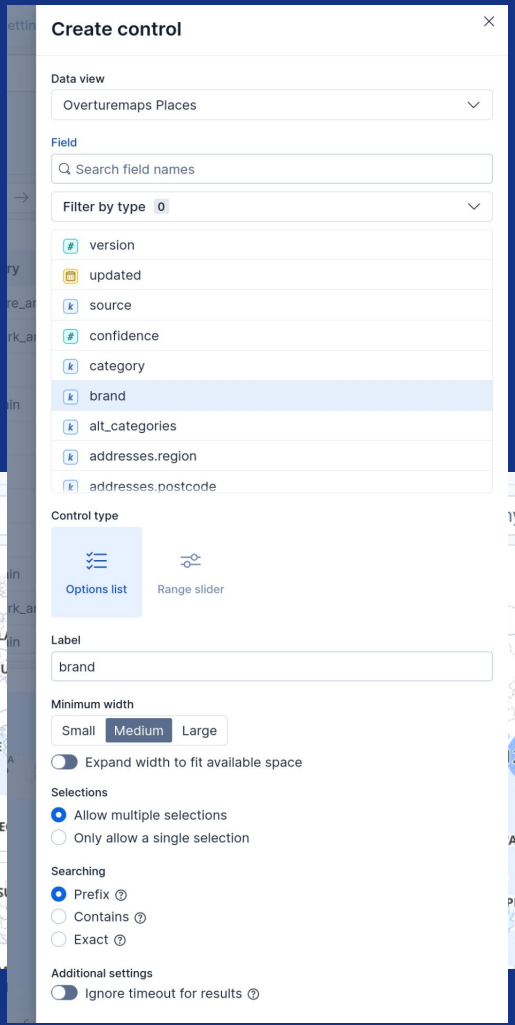
elastic


D
Deployment
Kibana
Dashboards
Editing New Dashboard
J
Settings
Share
Switch to view mode
Save
Filter your data using KQL syntax
Last 15 minutes
Create visualization
Add panel
Add from library
Controls

Controls

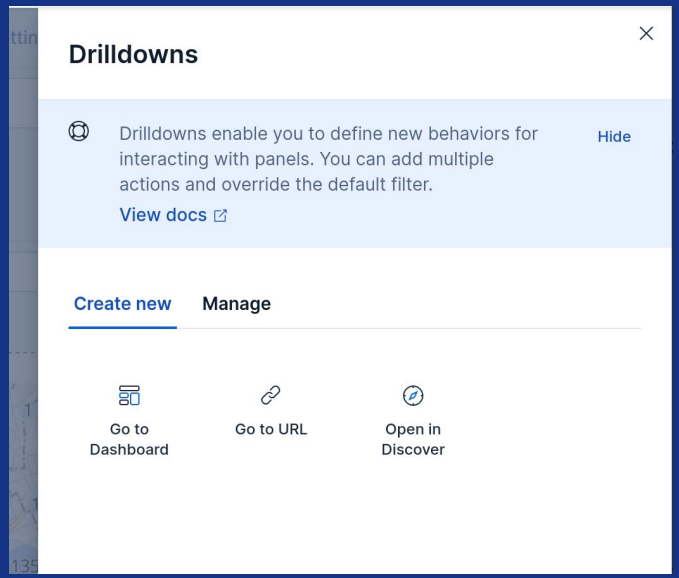
Create powerful option lists or range sliders from any field that filter your dashboard

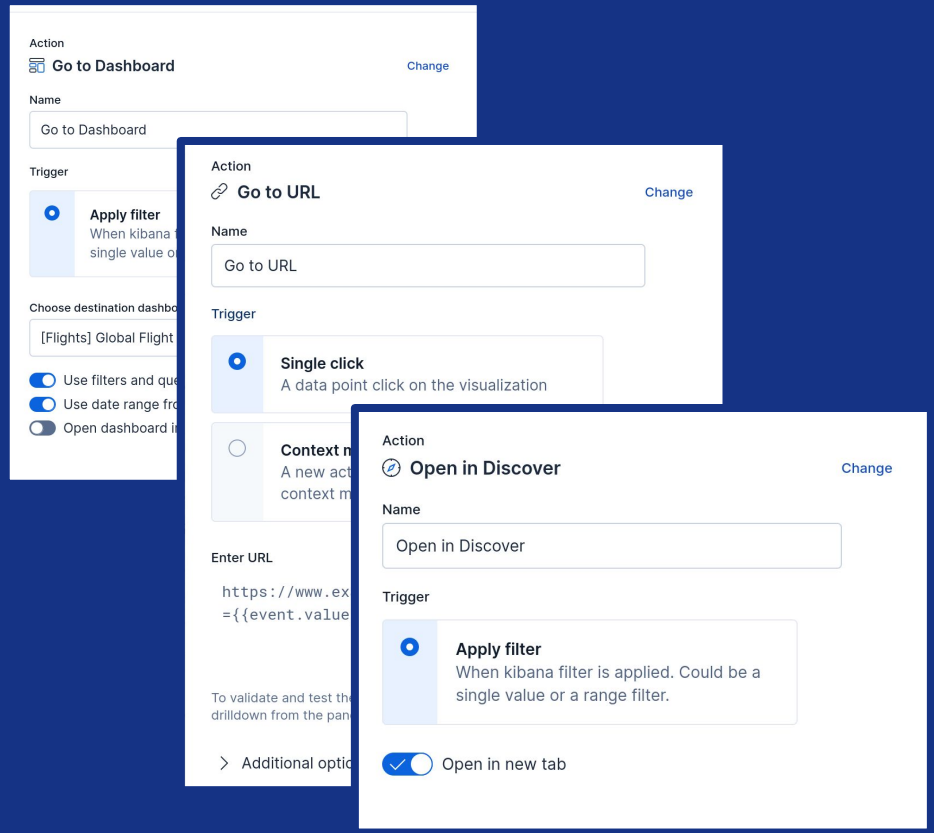




elastic

Drilldowns



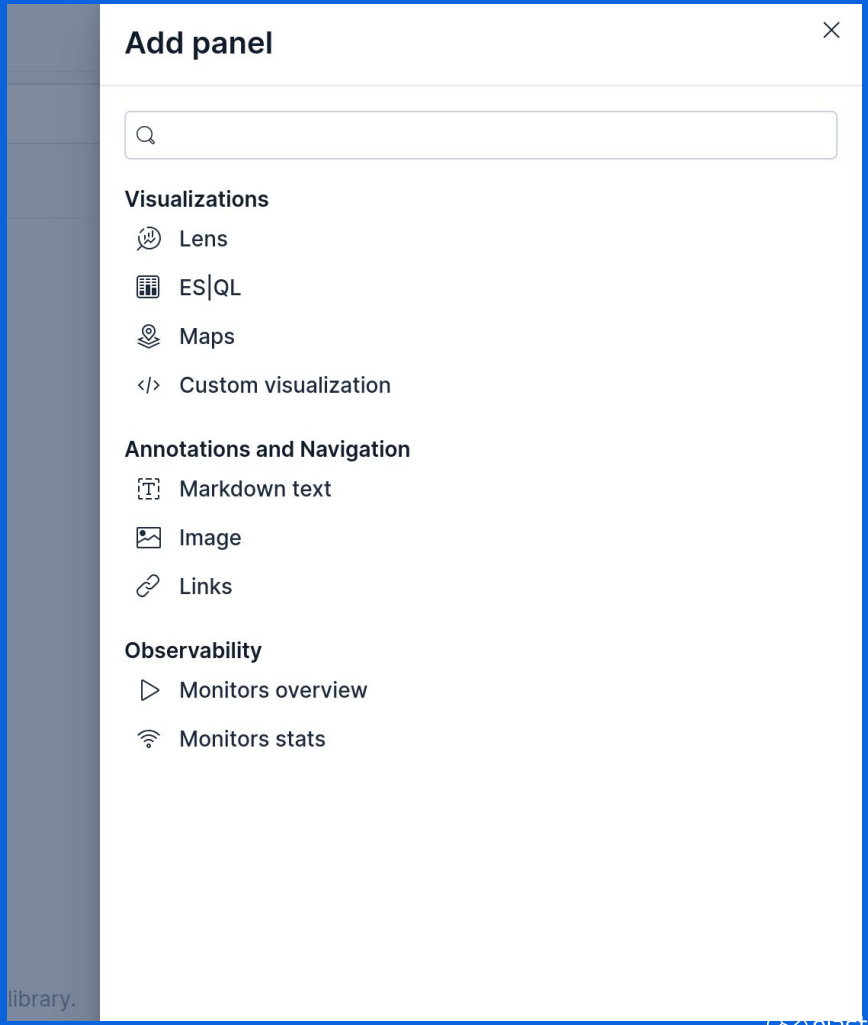


elastic

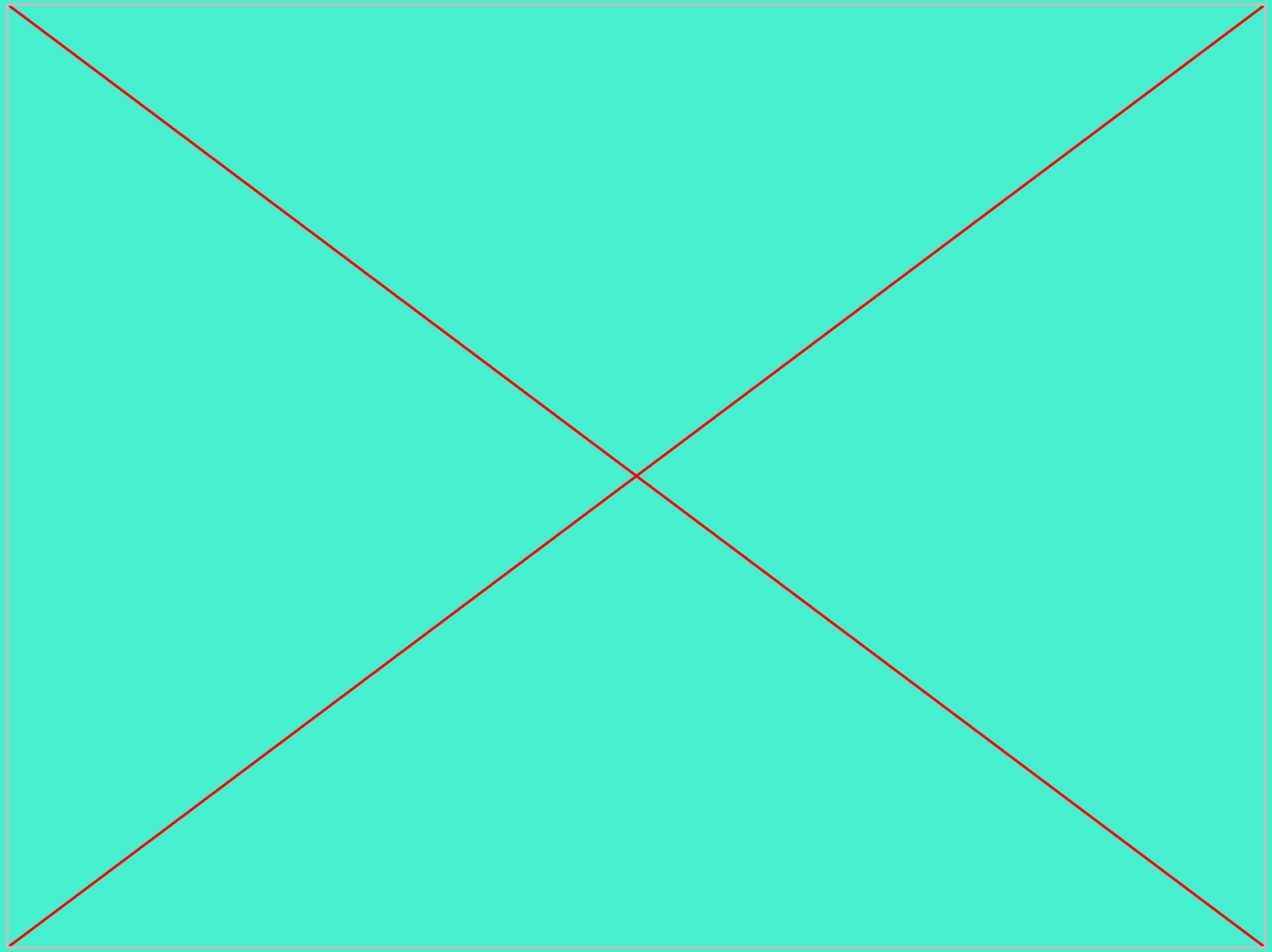
Dashboard panels

Visualizations

- Lens: drag & drop visualization builder
- ES|QL: create visualizations from queries
- Maps: geospatial visualizations
- Custom visualization: use Vega JSON specifications to create advanced visualizations

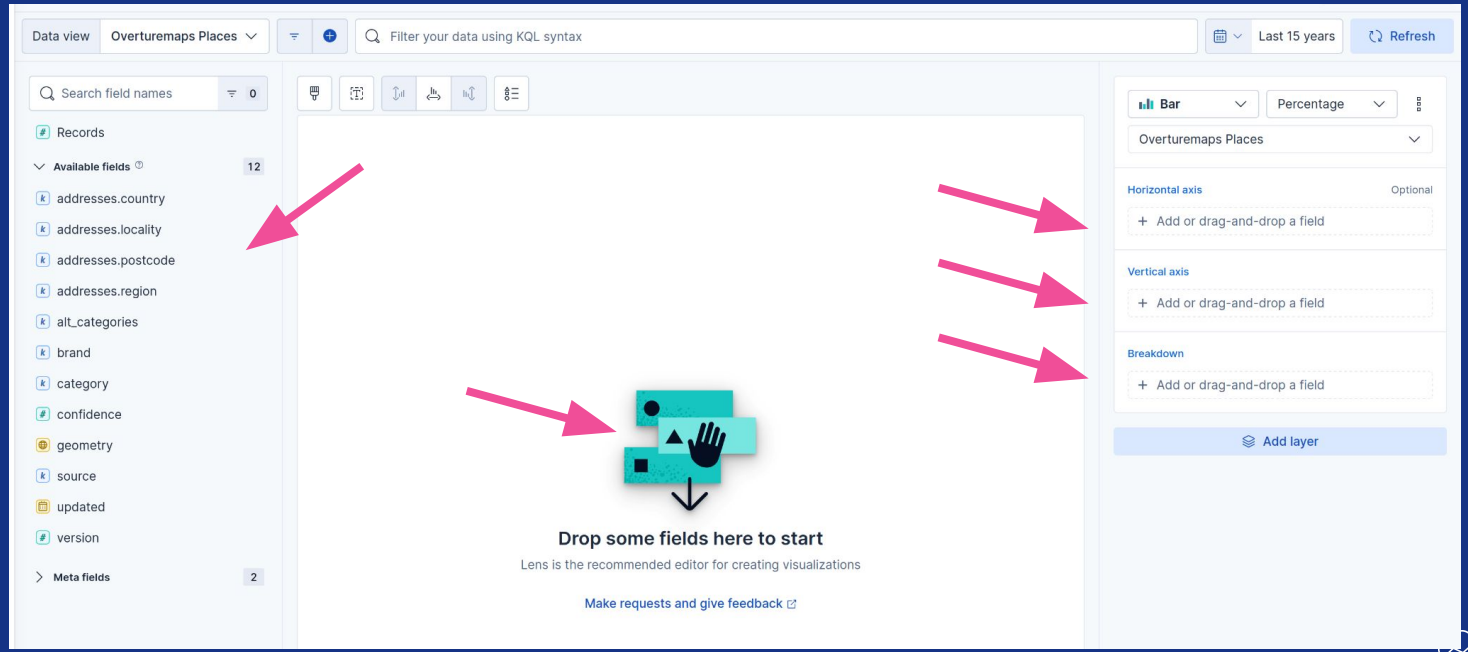


Lens



Lens

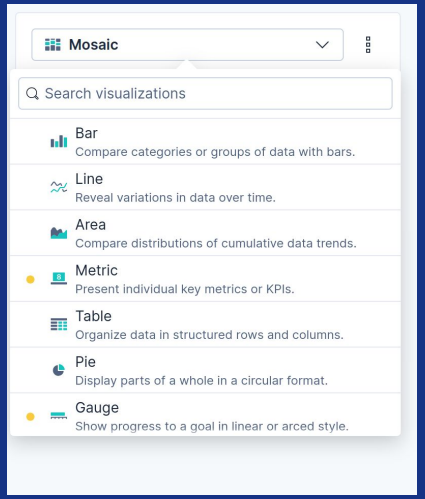
Drag & drop fields into the main area, axis, and breakdown selectors



elastic

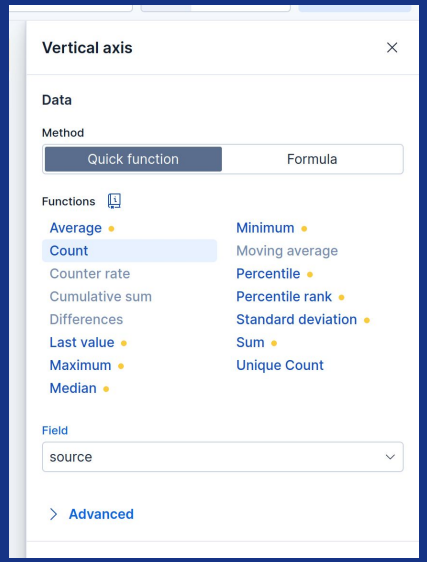
Lens

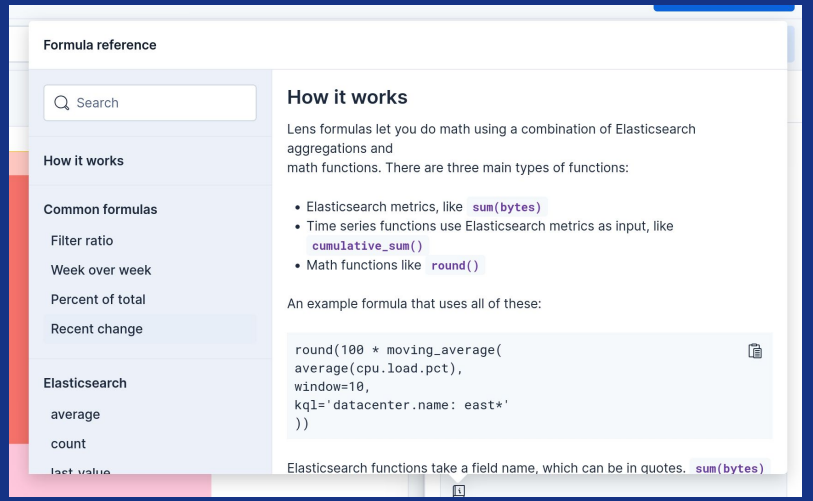
Broad selection of chart types: table, area/bar/line chart, metrics, treemap, waffle, gauge



Lens

Easy metric aggregation selection & custom formula with in-product help

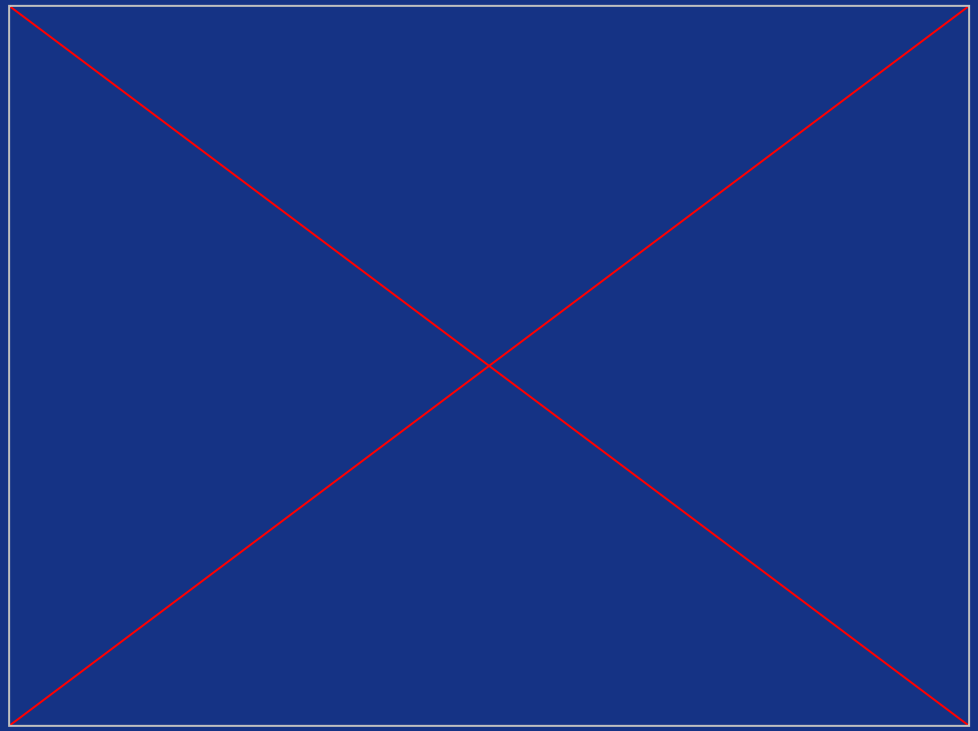




elastic

Lens

Lens visualizations can create filter pills interactively when brushing or clicking on chart elements

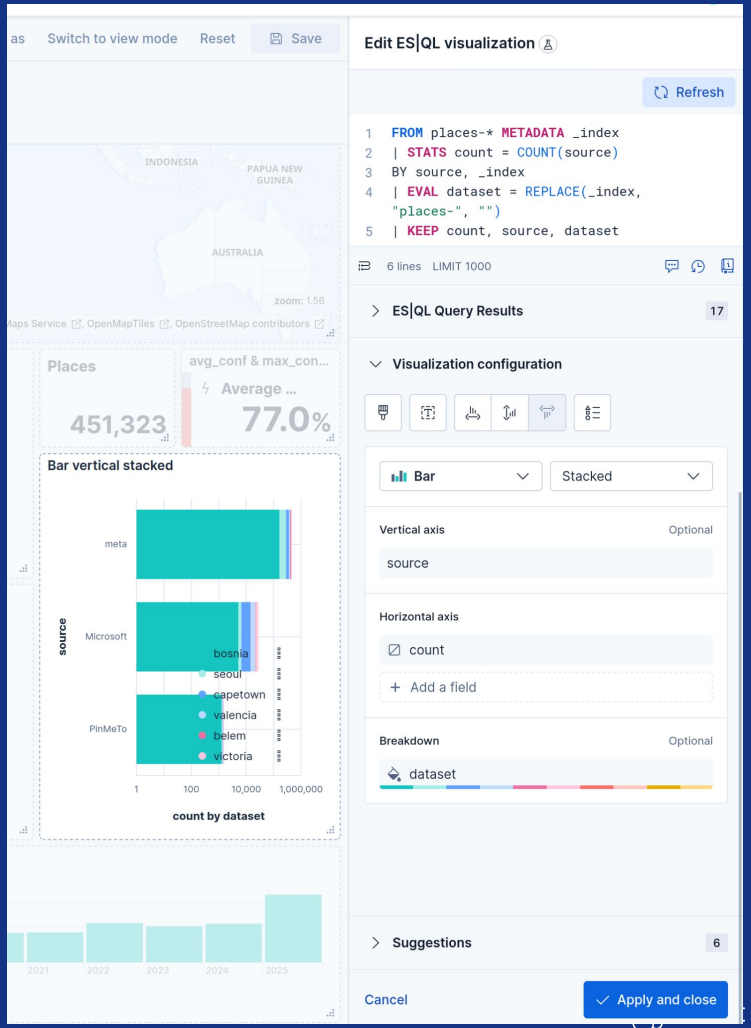


ES|QL visualizations

ES|QL visualizations

From queries to charts

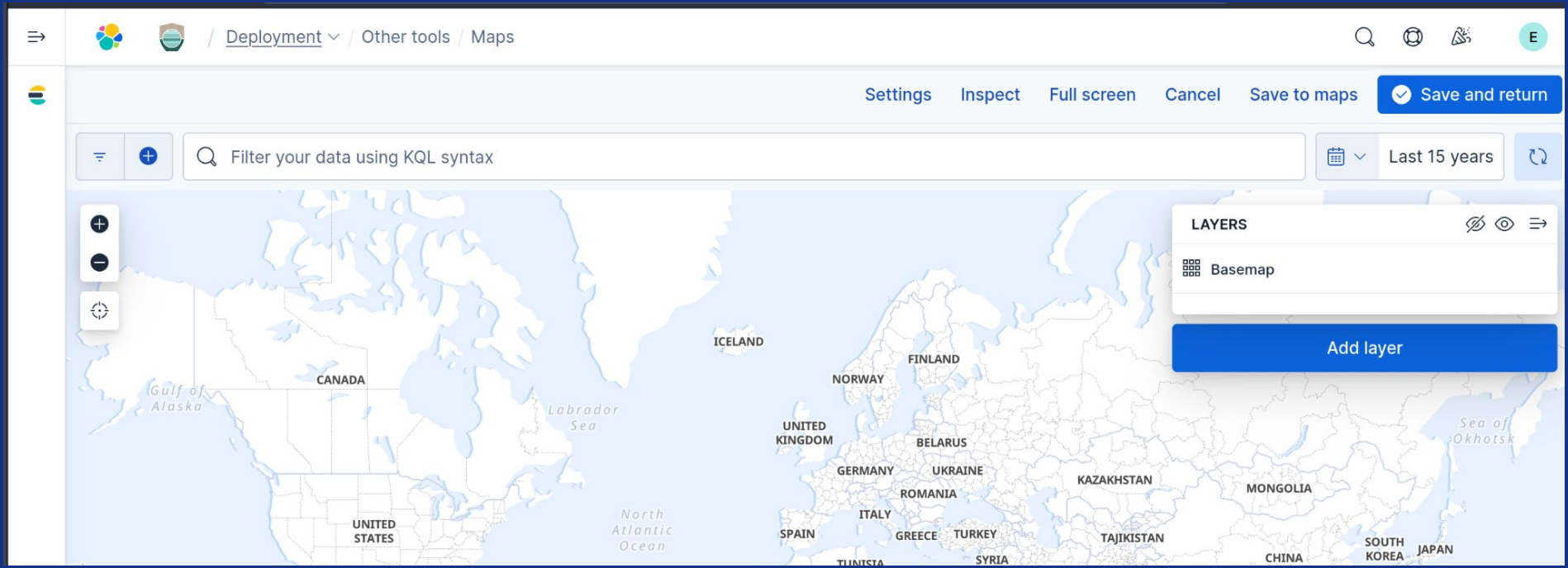
- Create chart without leaving the dashboard
- Complete ES|QL editor with autocomplete, error highlighting, etc.
- Review query results
- Define the visualization with a lens-like interface
  - Chart type, visualization settings, axis, etc
  - Vertical and horizontal axis metrics
  - Optional breakdown
- In future releases:
  - Use variables in the query to create controls that allow interactive visualizations.



Elastic Maps

Interface

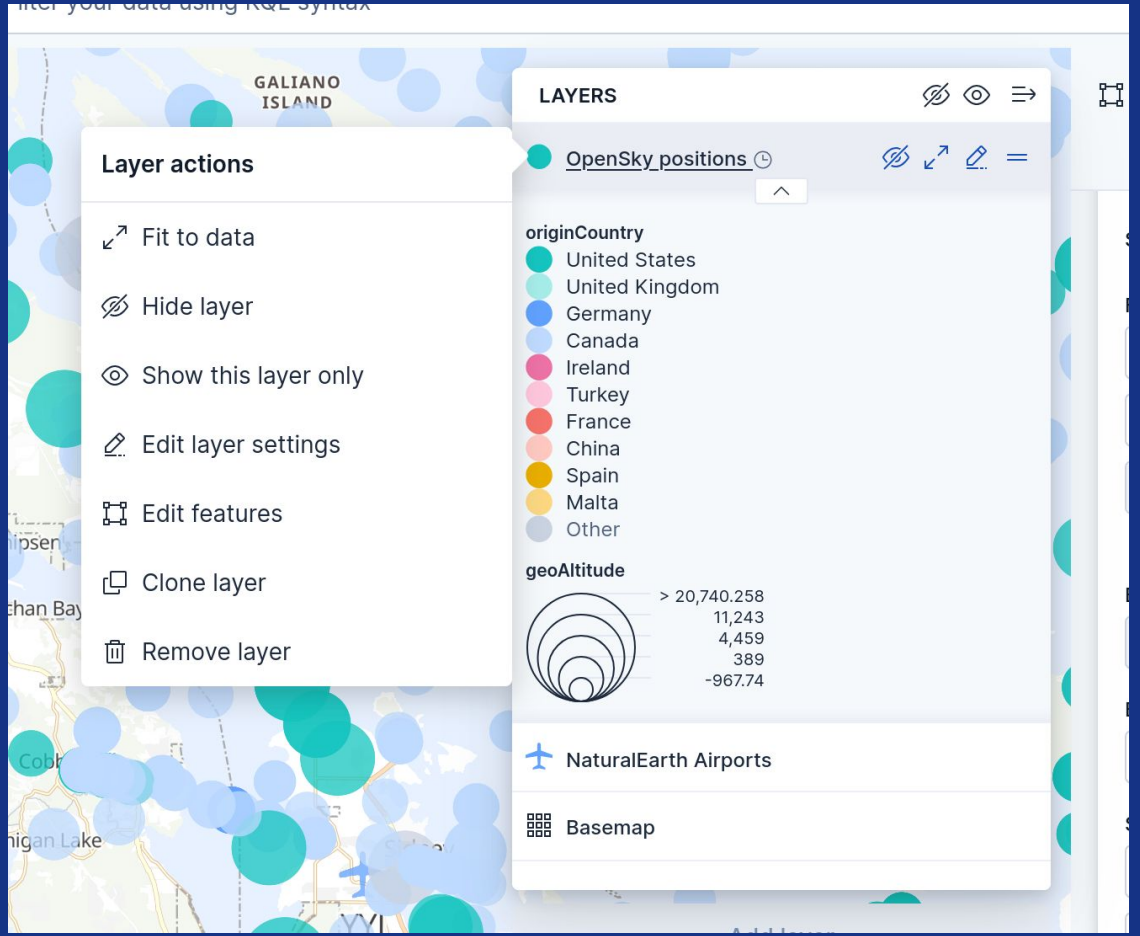
Same elements as in Lens, Dashboards, etc.



Interface

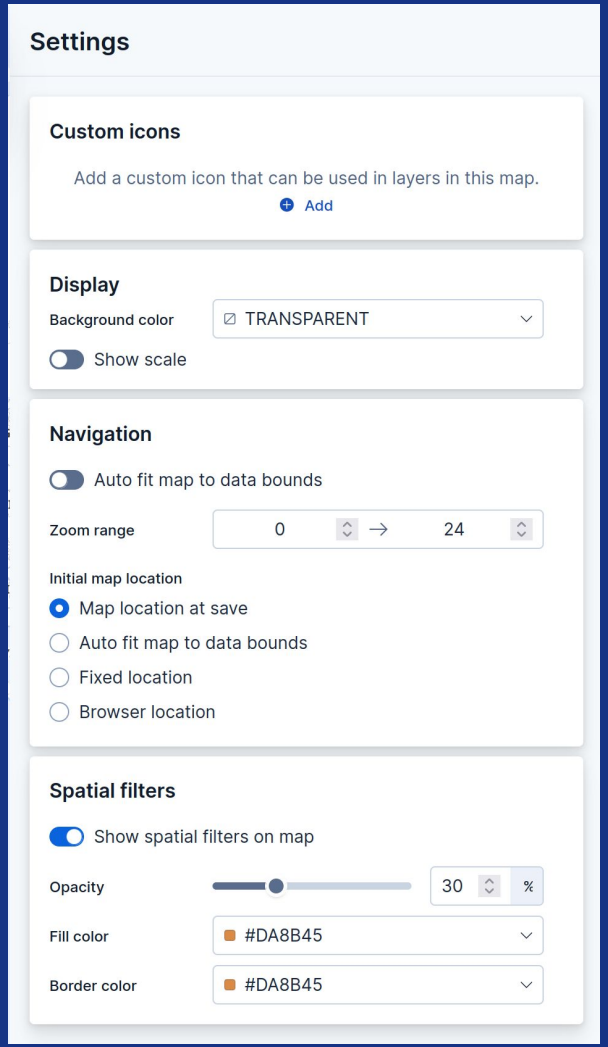
Familiar layers user interface

- Quick actions by the name
- Layers can be reordered, grouped, cloned
- Legend shows all data driven properties
- Actions depend on layer type



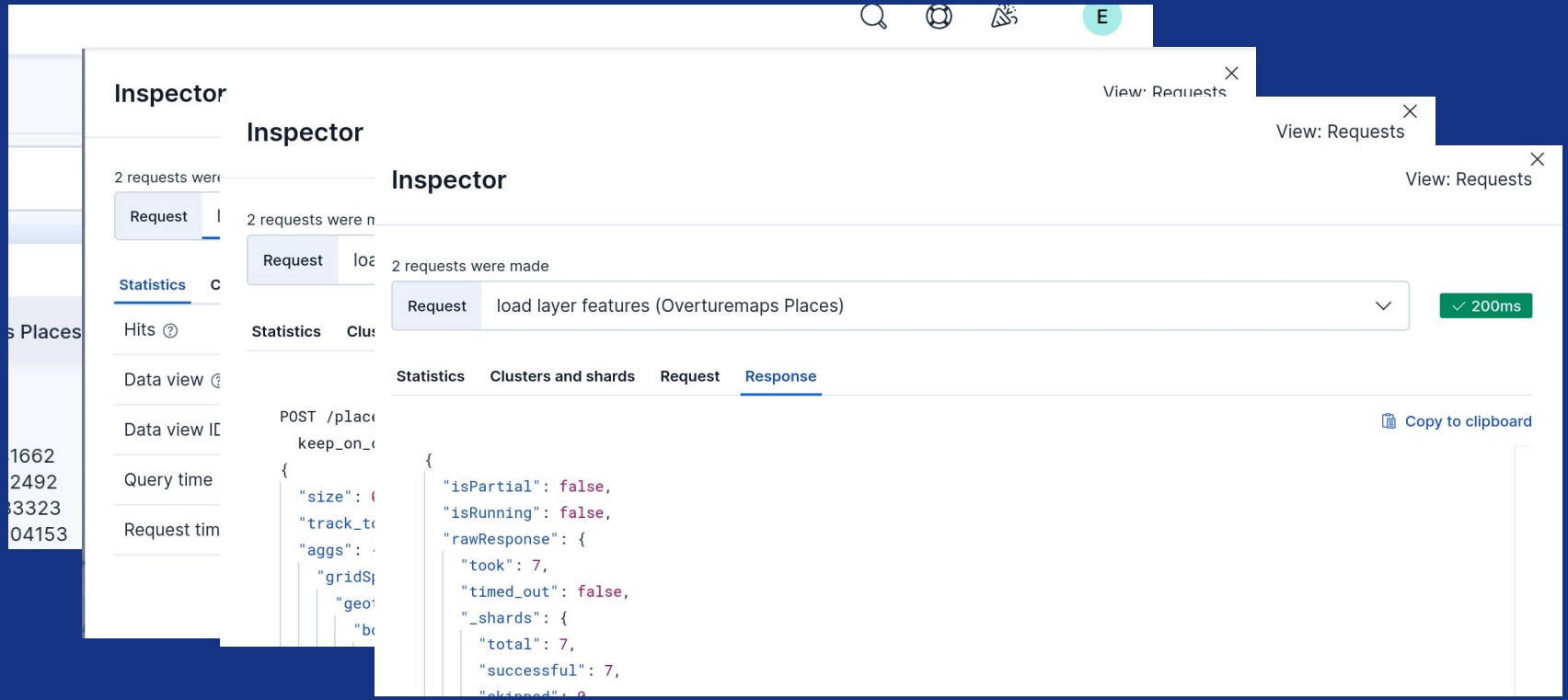
Settings

- Upload custom icons for point symbols
- Change background color if basemap is displayed
- Navigation defaults
- Spatial filters settings



Layer inspect

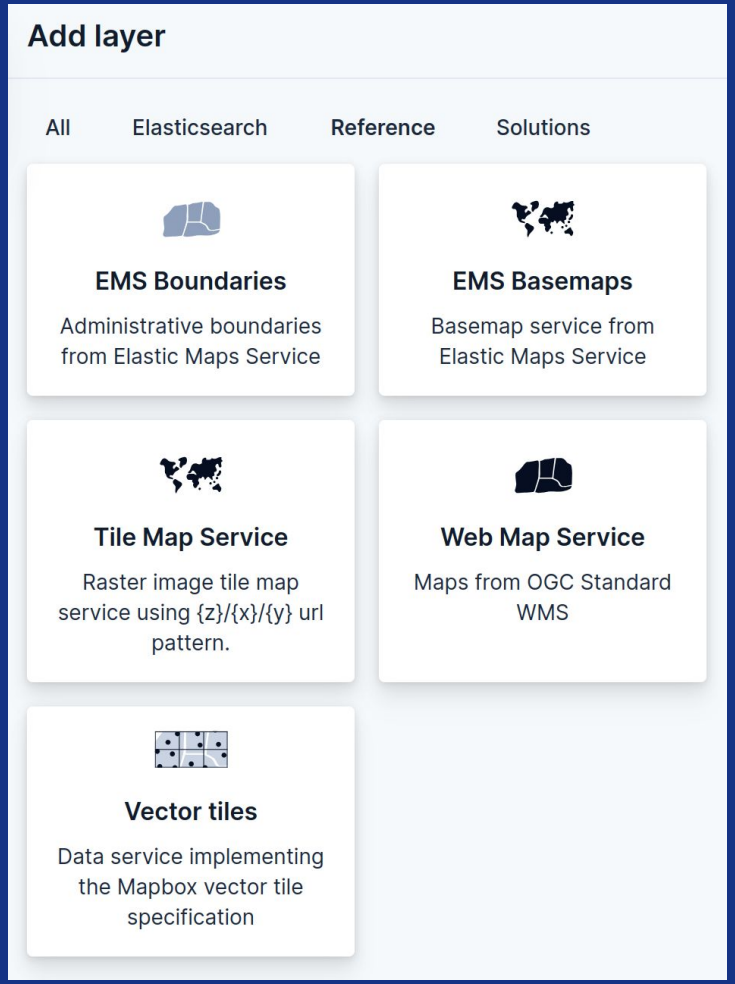
See the queries to Elasticsearch in detail



Reference layers

Data outside from Elasticsearch

- EMS Basemaps
  - Default basemap provided by Elastic
- EMS Boundaries
  - Administrative boundaries ready to join with Elasticsearch data
- Web Map Service and Tile Map Service
  - Custom basemaps (imagery, official cartography, etc.)
- Vector Tiles
  - Vector data to style manually



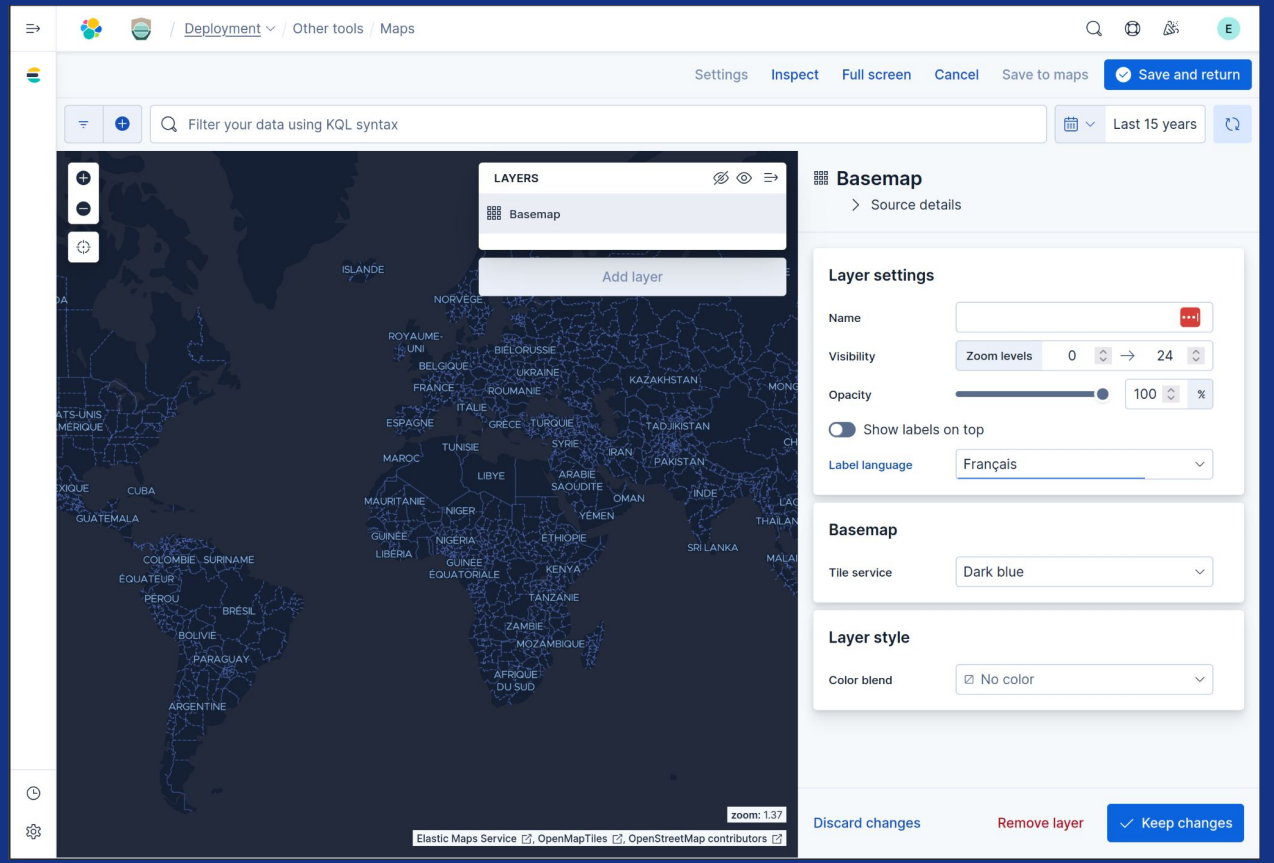
EMS Basemaps

Settings

- Labels language
- Labels on top
- Opacity
- Basemap style
- Colorize

In 9.1

- Globe mode



Data layers

Loading Elasticsearch data in different ways

Documents: load individual index documents using vector tiles or JSON representation

ES|QL: craft queries that return geometries

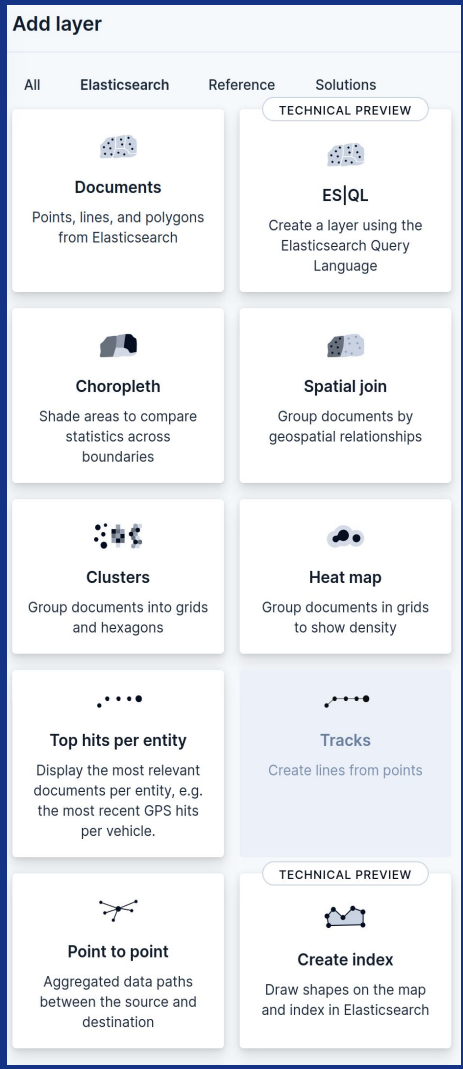
Spatial Join: basic support for client side spatial join

Clusters: aggregate into clusters, grids, and hexagons (non-free)

Heat map

Top hits per entity: display the n-latest documents of time series

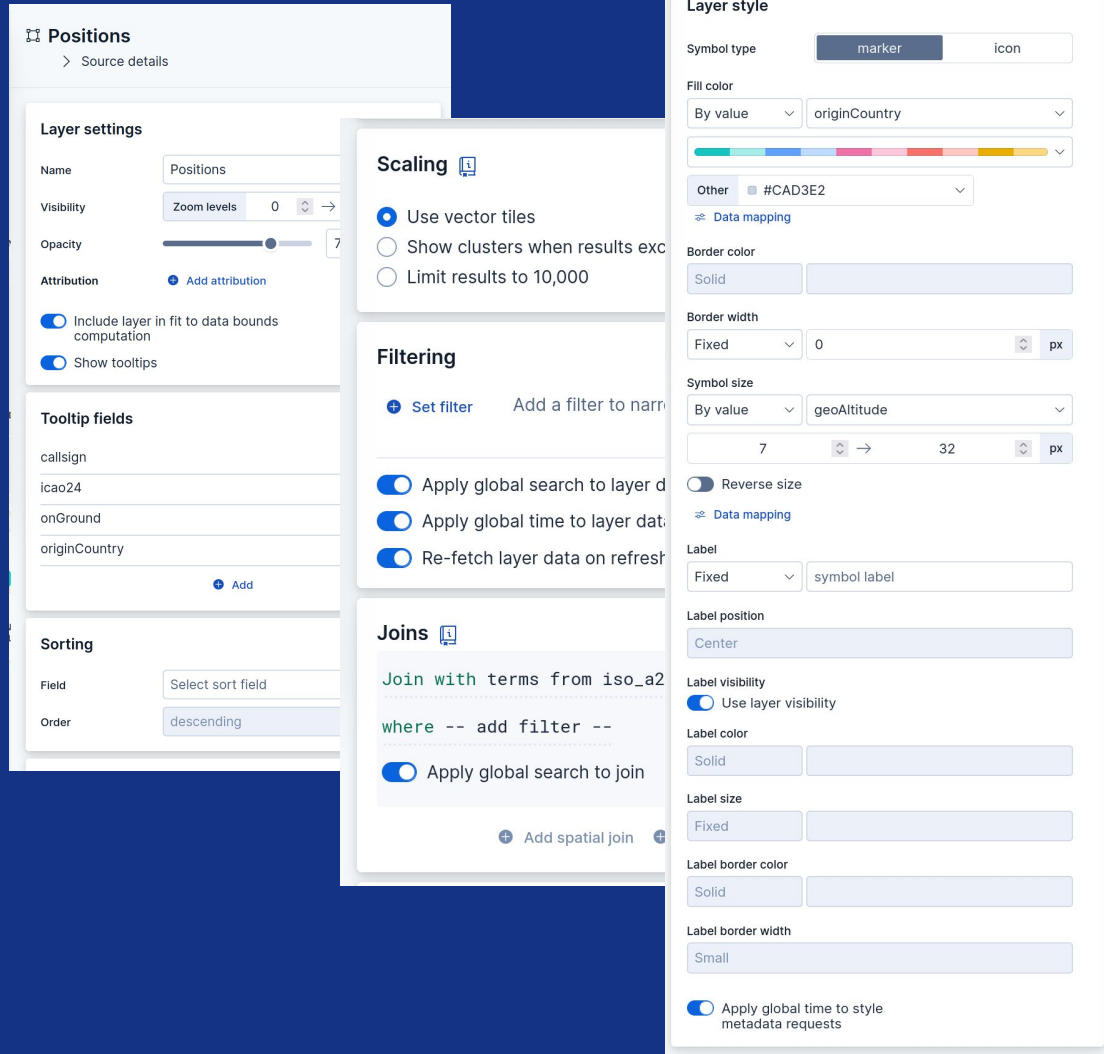
Point to point: connect source and destination fields



Documents

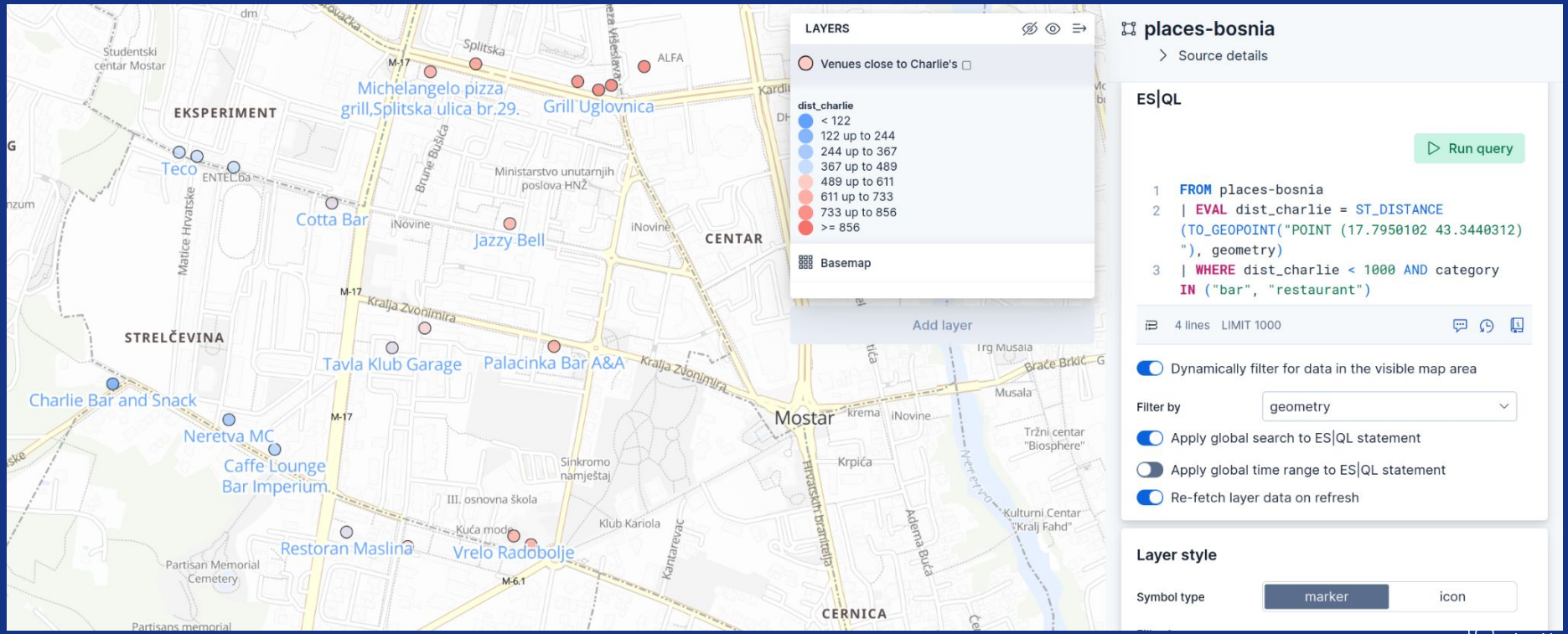
Render individual documents

- Zoom based visibility and Opacity
- Select fields for tooltips
- Sort by a field
- Scaling:
  - Vector tiles
  - First 10K documents
  - Automatically cluster > 10K
- Join with another index
- Styling
  - Symbol, sizes, colors, label



ES|QL

Similar to the documents layer type, but using a query as the source for the layer features



Clusters

Rendering big data

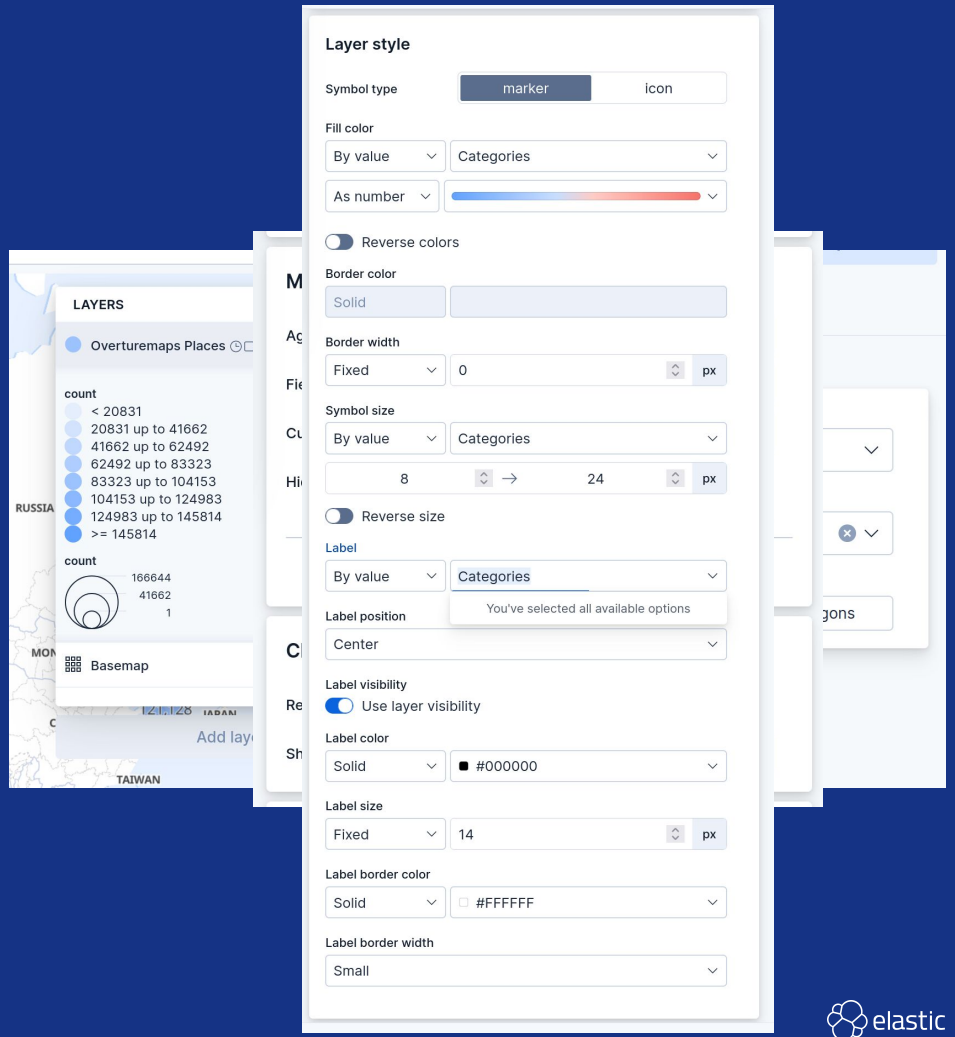
Aggregate into:

- Geotile: clusters or grid
- H3 grid 🛒

Layer settings

- Each metric defines an aggregation function on a field
  - To be used as labels, and data driven properties
- Spatial grid resolution
- Aggregation switch

Layer styling

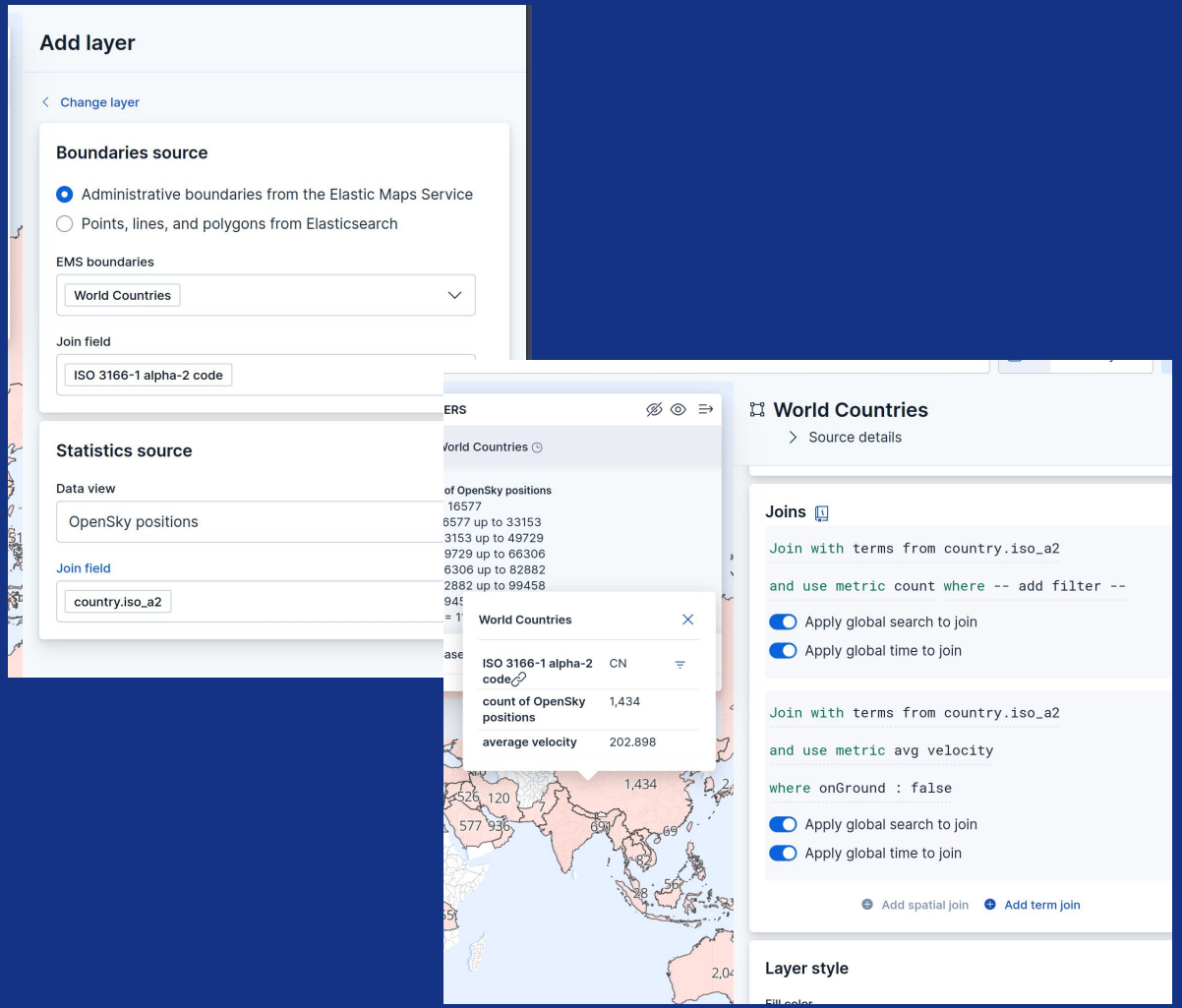


elastic

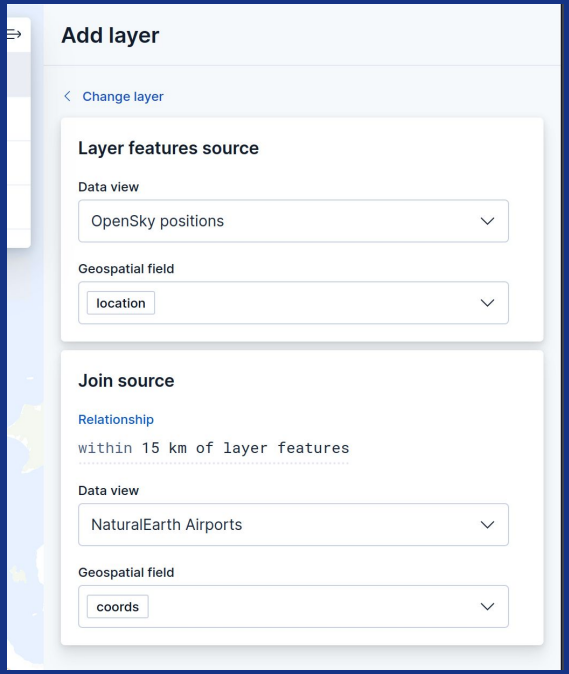
Choropleth

Aggregate and join with reference data

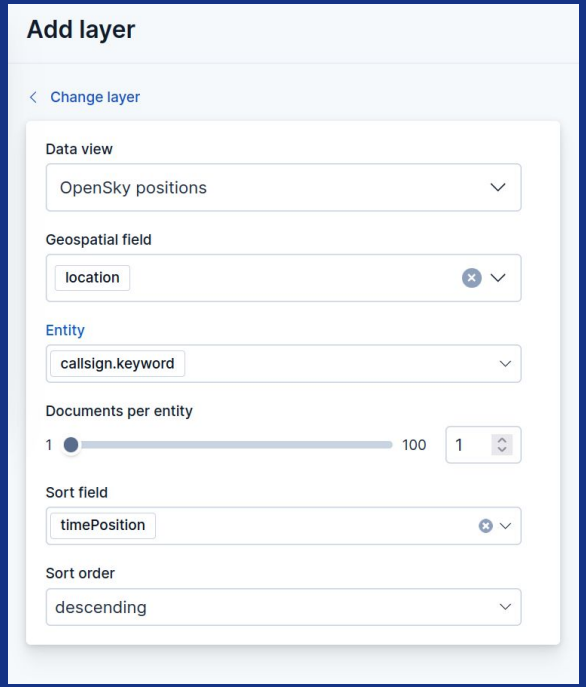
- Use EMS boundaries or an index for the reference data
- Aggregate any metrics using a common field (ISO codes, usually)
  - Available for styling
  - Tooltips
- Apply filters
- Allow removing by threshold
  - Hide outliers



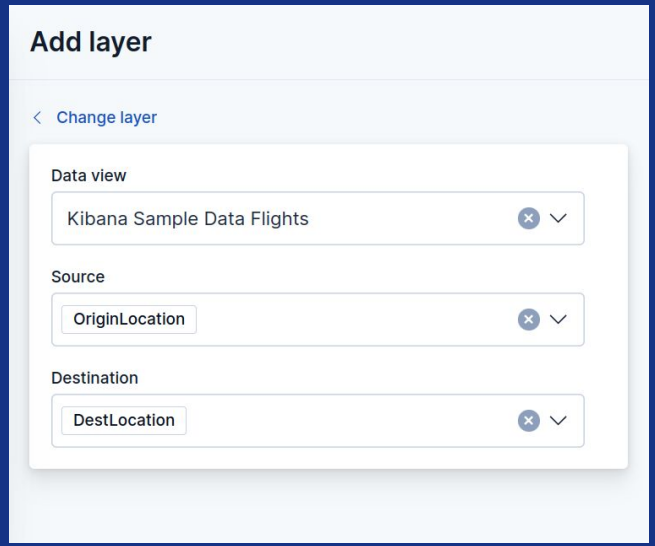
Other types



Spatial Join



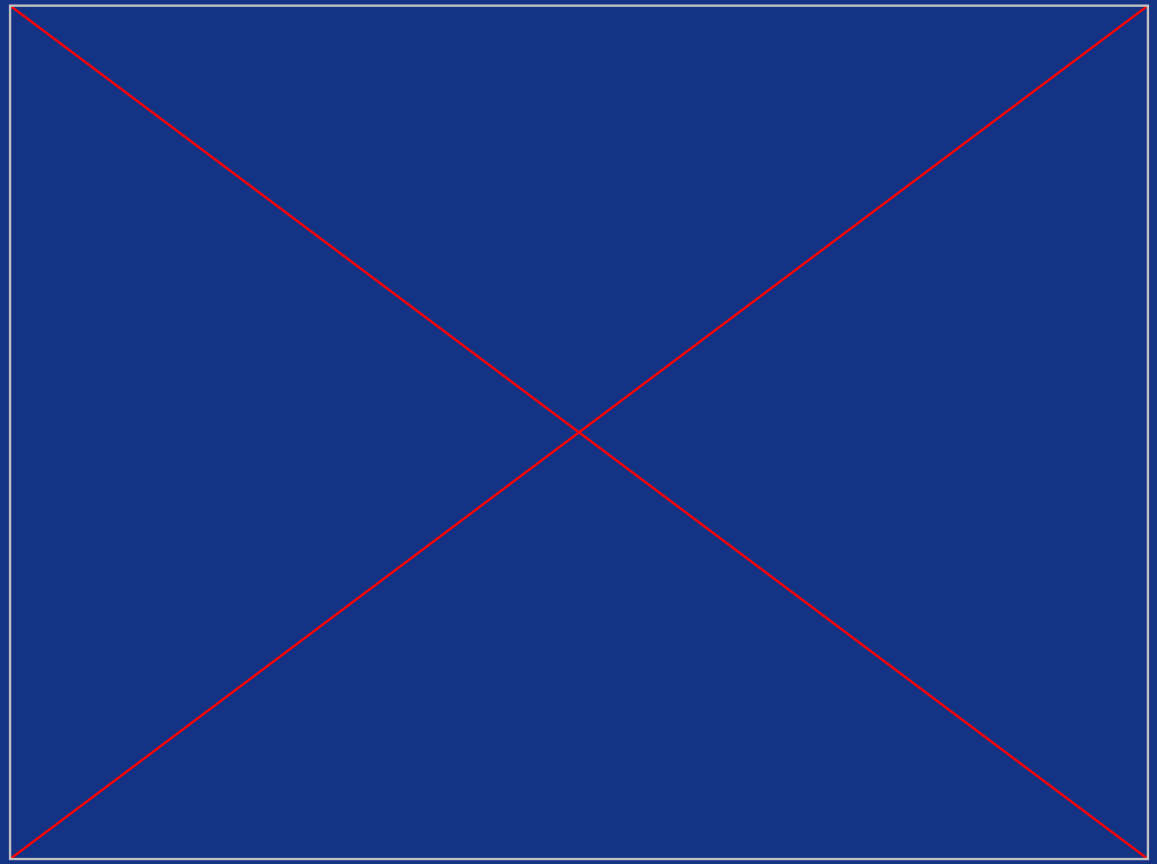
Top hits per entity



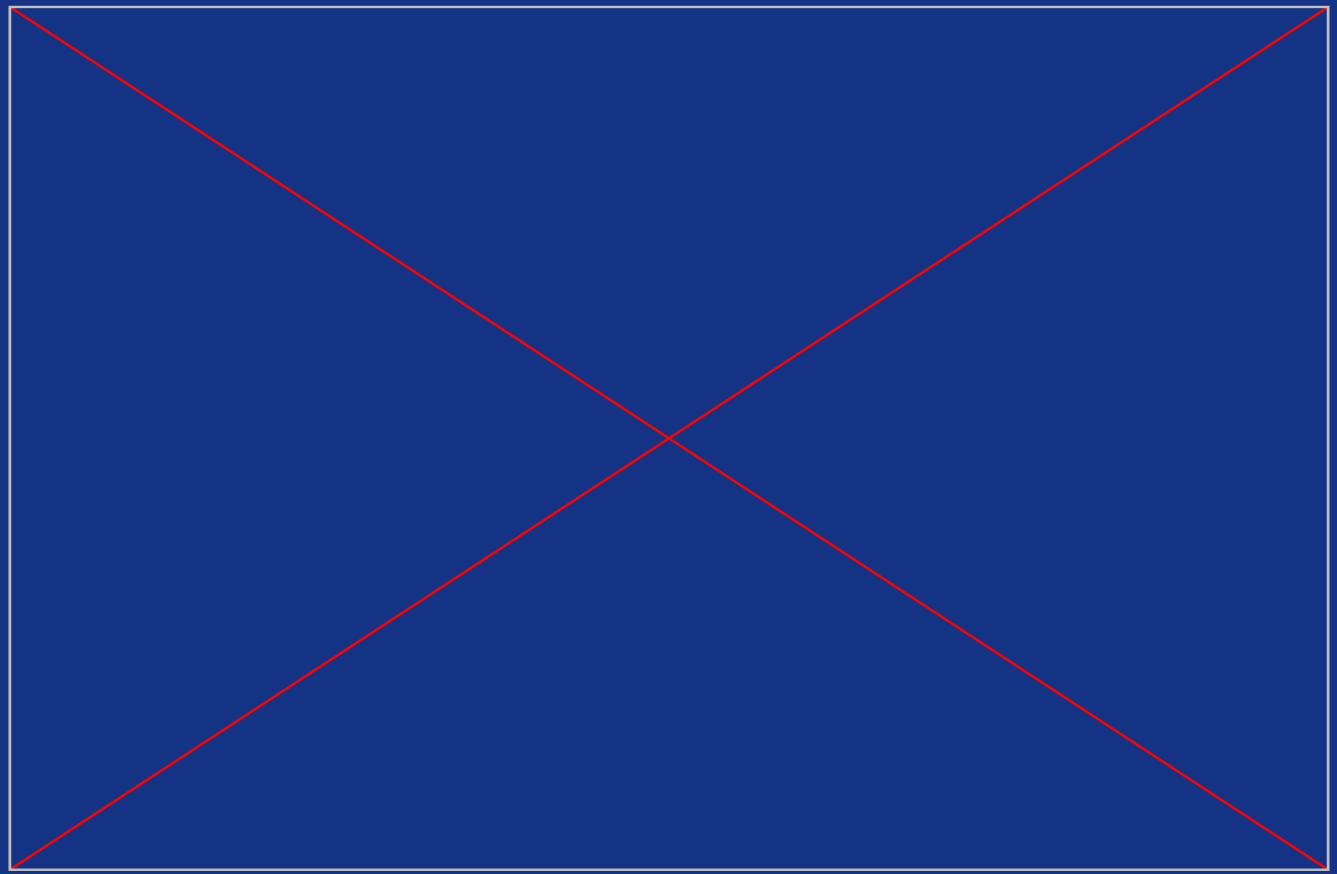
Point to point

elastic

Maps in dashboards: filters



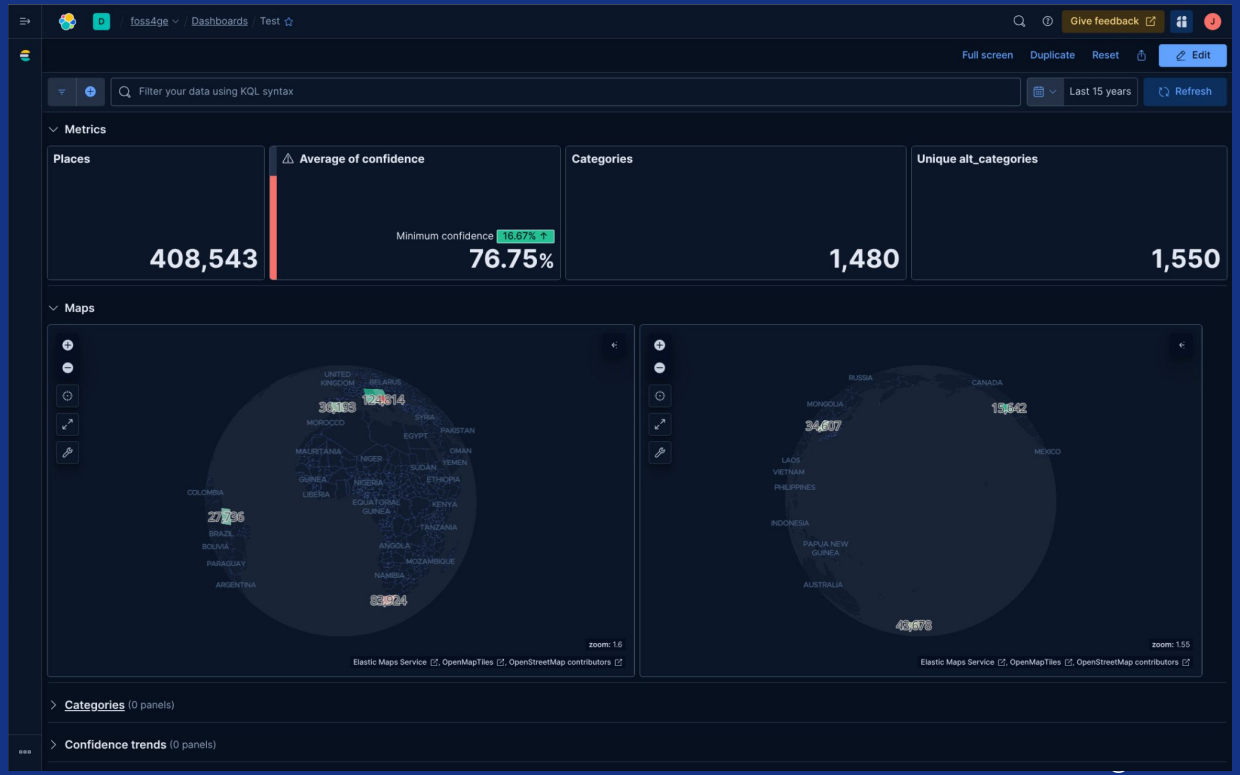
Maps in dashboards: synchronized extents



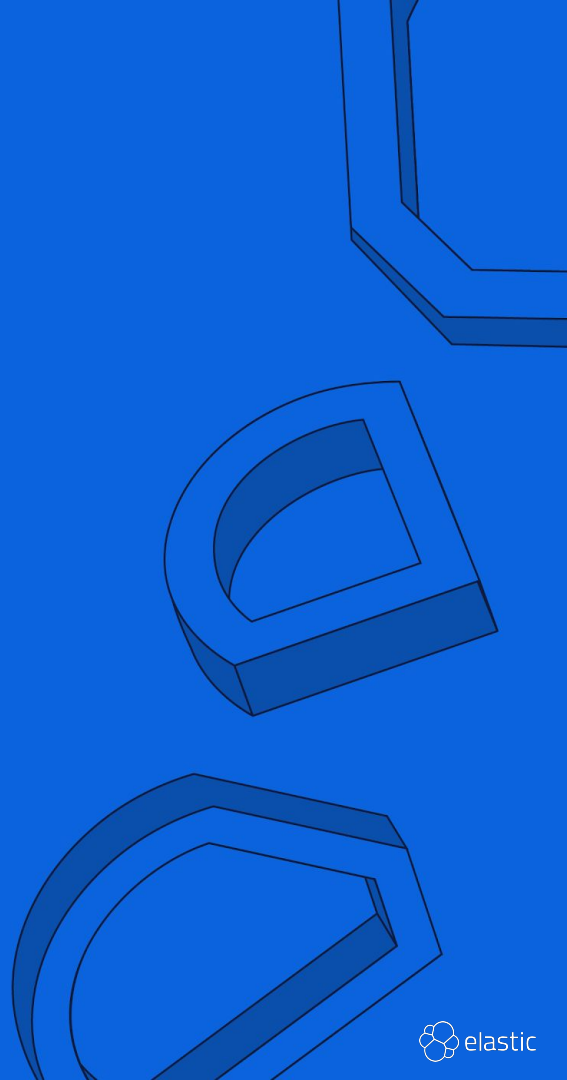
What's new in 9.1?

What's new in 9.1

- Improvements in ES|QL text search functions
- Maps Globe projection
- Collapsible panels on dashboards
- ES|QL controls and `?variables` in queries
- Improvements in metric and table visualization types
- View chart configuration in read-only dashboards



Questions?



¡Gracias!

Girona | SIG Libre | Septiembre, 2025

https://ela.st/siglibre-2025

elastic | The Search AI Company