

Análisis y visualización de datos con Elasticsearch y Kibana

Girona | SIG Libre | Septiembre, 2025

<https://ela.st/siglibre-2025>





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



The screenshot shows the GitHub interface for the repository 'elastic_esql_lab'. The repository is public and has 1 branch and 0 tags. The file list includes 'data', '.gitignore', '00-setup.ipynb', '01-download_and_ingest.ipynb', '02-esql.ipynb', '03-geospatial_esql.ipynb', 'LICENSE', and 'README.md'. The 'README.md' file is selected, showing the title 'ES|QL Elasticsearch and Kibana workshop' and a description: 'Materials used for the 2025 FOSS4G Europe and 2025 SIG Libre workshops.' The right sidebar shows repository statistics: 0 stars, 0 forks, 0 watching, and 0 releases. The 'Languages' section shows that the repository is 100.0% Jupyter Notebook.

elastic_esql_lab Public

main 1 Branch 0 Tags

Go to file Add file Code

jsanz Update README.md be7996d · 1 minute ago 29 Commits

data	Added master tables and importing process	18 hours ago
.gitignore	Some refactor	last month
00-setup.ipynb	Updated from colab	last month
01-download_and_ingest.ipynb	Added master tables and importing process	18 hours ago
02-esql.ipynb	Created using Colab	last month
03-geospatial_esql.ipynb	Minor fixes	last month
LICENSE	Initial commit	last month
README.md	Update README.md	1 minute ago

README CC0-1.0 license

ES|QL Elasticsearch and Kibana workshop

Materials used for the [2025 FOSS4G Europe](#) and [2025 SIG Libre](#) workshops.

About

A workshop on Elasticsearch and Kibana

- Readme
- CC0-1.0 license
- Activity
- 0 stars
- 0 watching
- 0 forks

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)

Languages

- Jupyter Notebook 100.0%

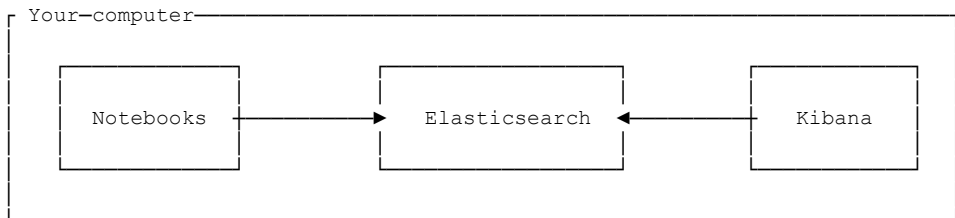
We'll go through the ES|QL basics and geospatial features using **Jupyter notebooks** then we'll move to Kibana



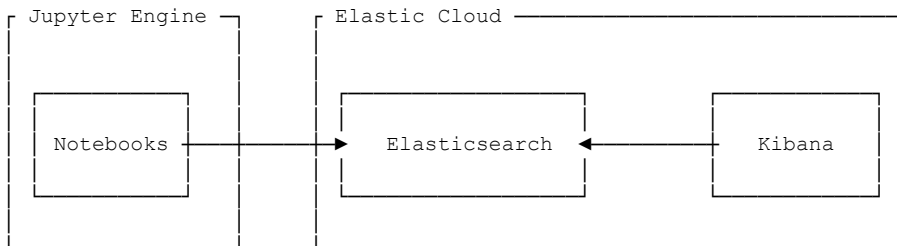
Lab setup

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: `0Th0SDJwY0I3QnLxdzlfMnVtZTC6TDlSulpCVjRoQXdbv0oy0DVNaVFEUQ==`

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



5B+
downloads



3,000+
employees (~250 in Spain)



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



40+
Countries with employees

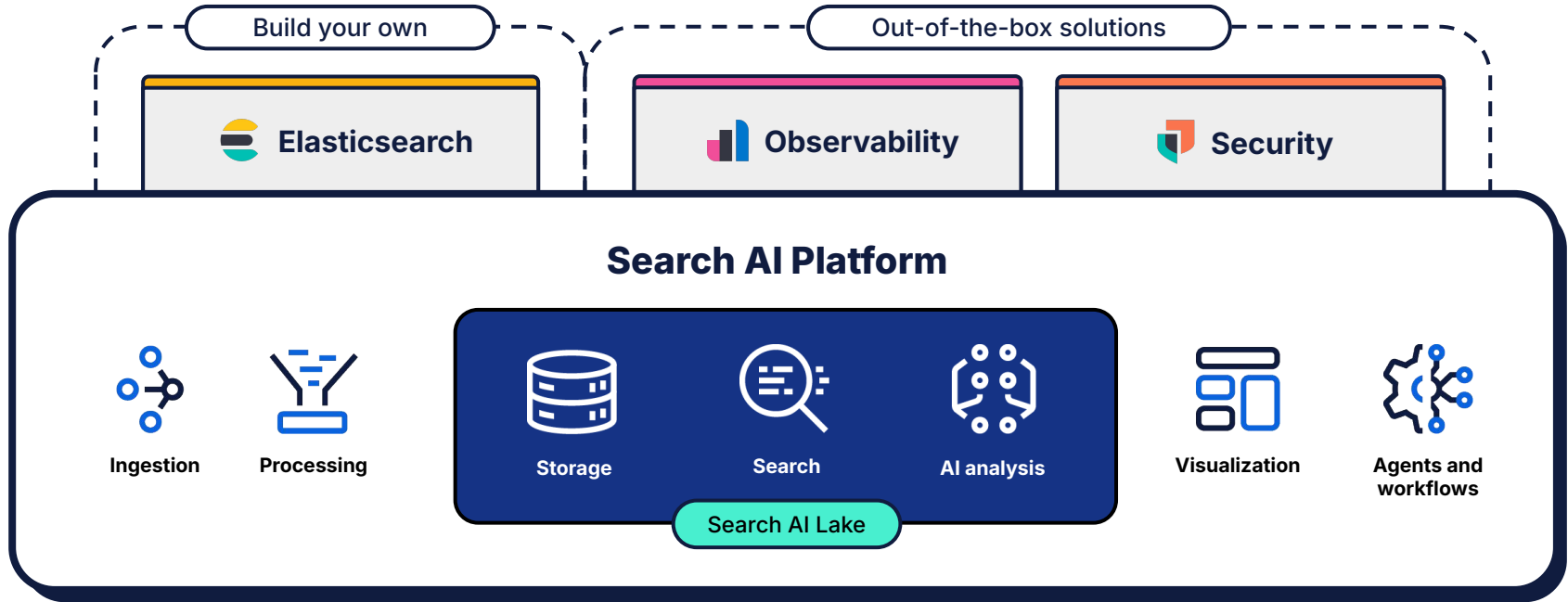


Publicly traded under
ESTC in the NYSE

Used by more than 50% of the Fortune 500 enterprises

TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE / TRANSPORTATION	RETAIL
							
							
							
							
							

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>

The screenshot shows the Elastic community forum interface. At the top, there's a navigation bar with the Elastic logo, a search icon, and a user profile icon. Below the navigation bar, there are filters for 'all categories', 'all tags', and tabs for 'Categories', 'Latest', 'New (154)', 'Unread (21)', and 'Top'. A '+ New Topic' button is also present. The main content area is divided into two columns. The left column lists categories: 'Announcements' (1 / week, 1 unread, 1 new), 'Elastic Stack' (322 / week, 19 unread, 129 new), 'Elastic Enterprise Search' (5 / week, 2 new), and 'Elastic Observability' (23 / week, 14 new). Each category has a brief description and a list of sub-topics. The right column shows a list of topics under the 'Latest' tab, including 'Notes on Using These Forums', 'Logstash pipeline graceful shutdown: потеря в-памяти данных?', 'Collapse within top hit aggregation results', 'Drilldown is not working with Visualization', 'Do not show results on page load', 'Custom transactions in checkout process', 'How to view sql queries in APM', and 'Installation seems to hang'.

elastic

all categories all tags Categories Latest New (154) Unread (21) Top + New Topic

Category Topics Latest

Announcements 1 / week
1 unread 1 new
Release and security announcements and other bits about all of our Elastic products that we think will be useful to everyone.
■ Security Announcements ■ Community Ecosystem 1 unread

Elastic Stack 322 / week
19 unread 129 new
Elasticsearch, Kibana, Beats, and Logstash - also known as the ELK Stack. Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time. Please post your your topic under the relevant product category - Elasticsearch, Kibana, Beats, Logstash.
■ Elasticsearch 4 unread 59 new ■ Kibana 14 unread 32 new
■ Beats 20 new ■ Logstash 1 unread 18 new

Elastic Enterprise Search 5 / week
2 new
Easily implement powerful, modern search experiences for your busy team. Quickly add pre-tuned search to your website, app, or workplace. Search it all, simply.
■ App Search 2 new ■ Site Search ■ Workplace Search

Elastic Observability 23 / week
14 new
Bring your logs, infrastructure and availability metrics, and APM traces together at scale in a

Notes on Using These Forums 2
Apr 2017
■ Meta Elastic

Logstash pipeline graceful shutdown: потеря в-памяти данных? 0
4m
■ Вопросы на русском языке

Collapse within top hit aggregation results 0
5m
■ Elasticsearch

Drilldown is not working with Visualization 2
9m
■ Kibana

Do not show results on page load 0
20m
■ App Search

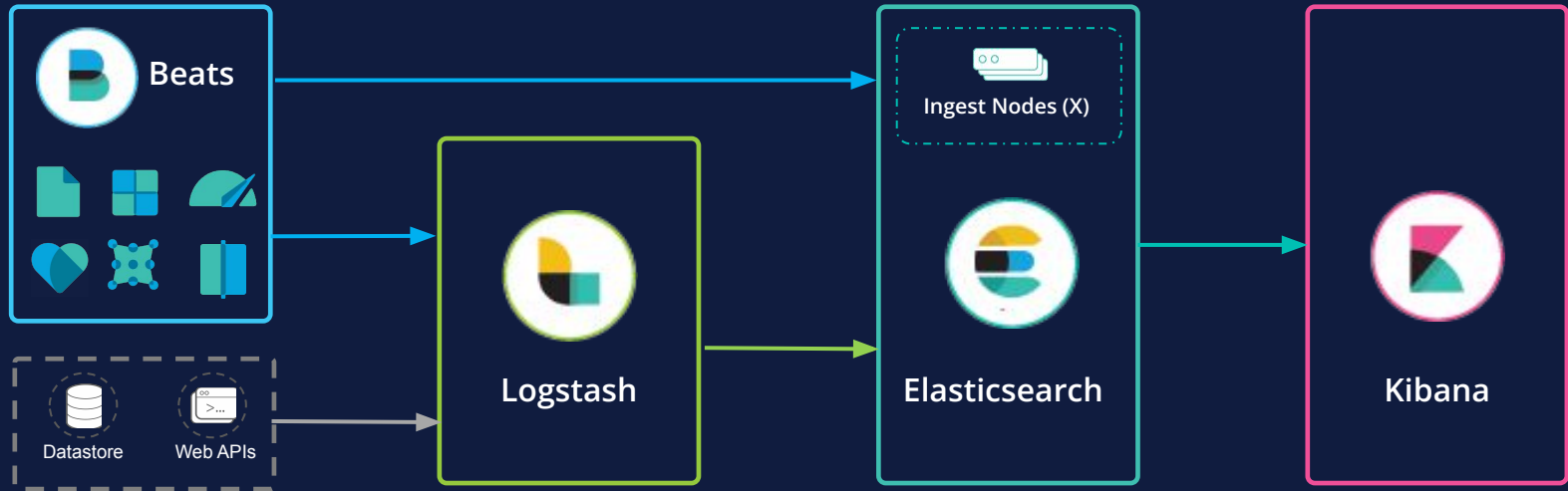
Custom transactions in checkout process 0
21m
■ Elasticsearch

How to view sql queries in APM 6
23m
■ APM ■ dotnet

Installation seems to hang 3

Elastic Stack

Ingest, Store, Search, Visualise

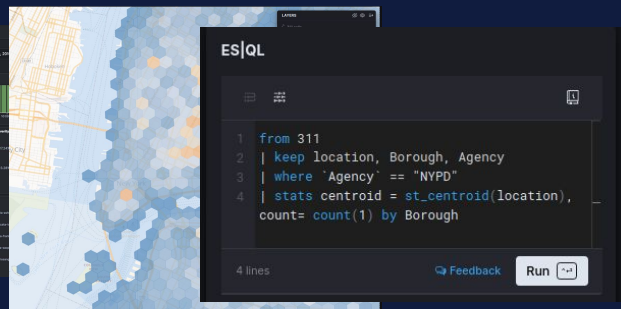
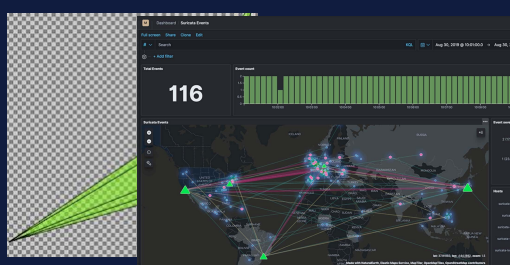
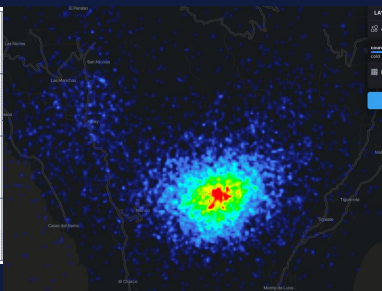


Elasticsearch and geospatial

Geospatial timeline



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



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

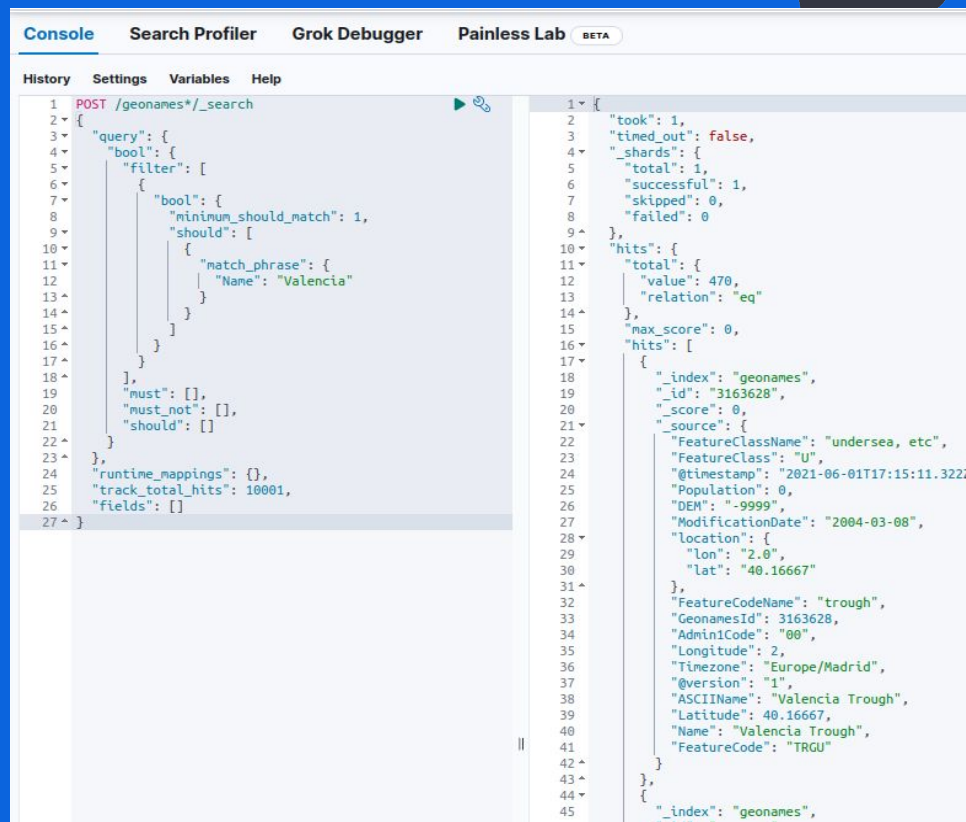
Vector tiles API

Elasticsearch `_search` API

- JSON output format
- Search and aggregate

Elasticsearch `_mvt` API

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



The screenshot displays the Elastic Stack DevTools interface. The top navigation bar includes 'Console', 'Search Profiler', 'Grok Debugger', and 'Painless Lab BETA'. The 'Console' tab is active, showing a search query in the left pane and the corresponding JSON response in the right pane.

Search Query (Left Pane):

```
1 POST /geonames*/_search
2 {
3   "query": {
4     "bool": {
5       "filter": [
6         {
7           "bool": {
8             "minimum_should_match": 1,
9             "should": [
10              {
11                "match_phrase": {
12                  "Name": "Valencia"
13                }
14              }
15            ]
16          }
17        }
18      ],
19      "must": [],
20      "must_not": [],
21      "should": []
22    }
23  },
24  "runtime_mappings": {},
25  "track_total_hits": 10001,
26  "fields": []
27 }
```

Search Results (Right Pane):

```
1 {
2   "took": 1,
3   "timed_out": false,
4   "shards": {
5     "total": 1,
6     "successful": 1,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": {
12      "value": 470,
13      "relation": "eq"
14    },
15    "max_score": 0,
16    "hits": [
17      {
18        "_index": "geonames",
19        "_id": "3163628",
20        "_score": 0,
21        "_source": {
22          "FeatureClassName": "undersea, etc",
23          "FeatureClass": "U",
24          "@timestamp": "2021-06-01T17:15:11.322Z",
25          "Population": 0,
26          "DEM": "-9999",
27          "ModificationDate": "2004-03-08",
28          "location": {
29            "lon": "2.0",
30            "lat": "40.16667"
31          },
32          "FeatureCodeName": "trough",
33          "GeonamesId": 3163628,
34          "Admin1Code": "00",
35          "Longitude": 2,
36          "Timezone": "Europe/Madrid",
37          "@version": "1",
38          "ASCIIName": "Valencia Trough",
39          "Latitude": 40.16667,
40          "Name": "Valencia Trough",
41          "FeatureCode": "TRGU"
42        }
43      },
44      {
45        "_index": "geonames",
```

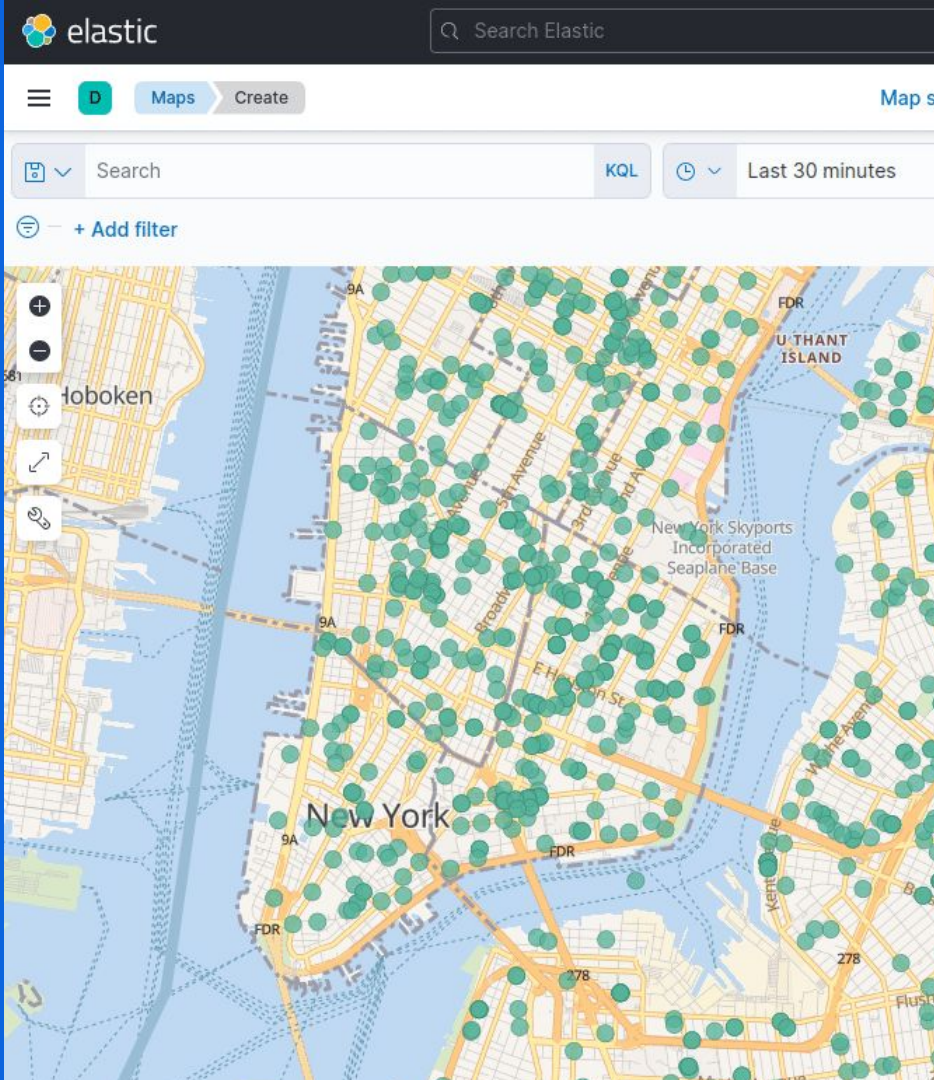
Search

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

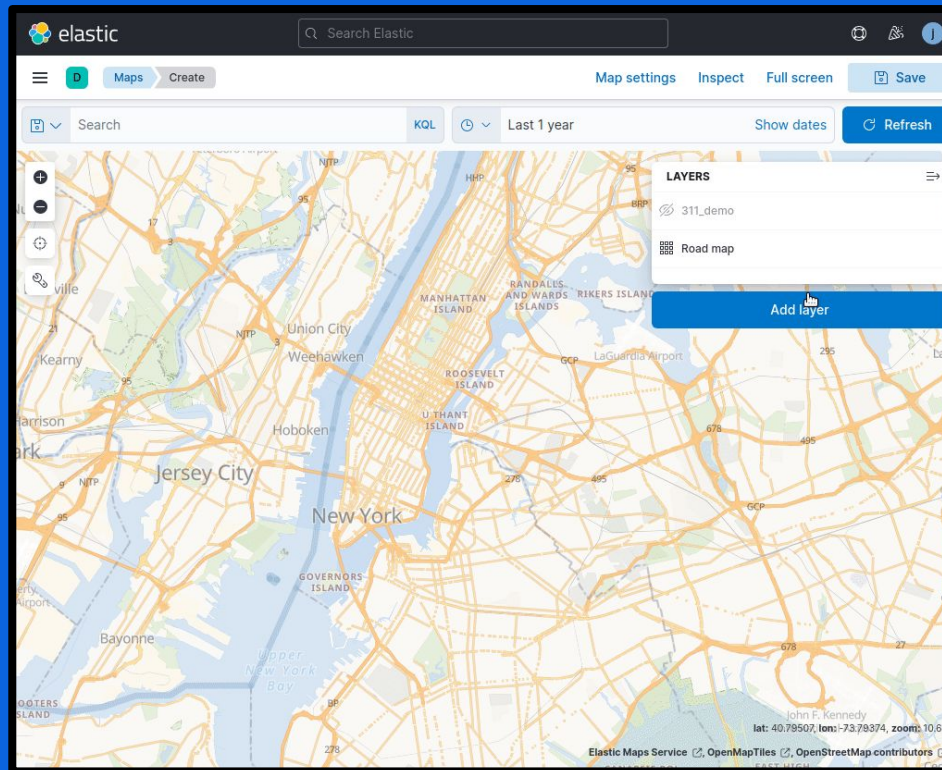
Binning (bucket agg)

- 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?

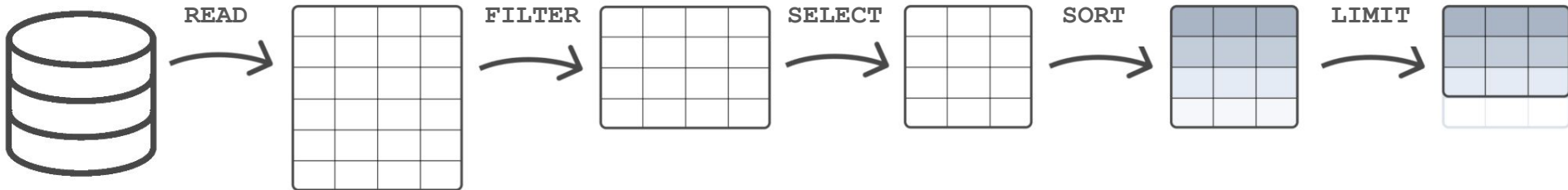
Declarative, Piped, Tabular

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

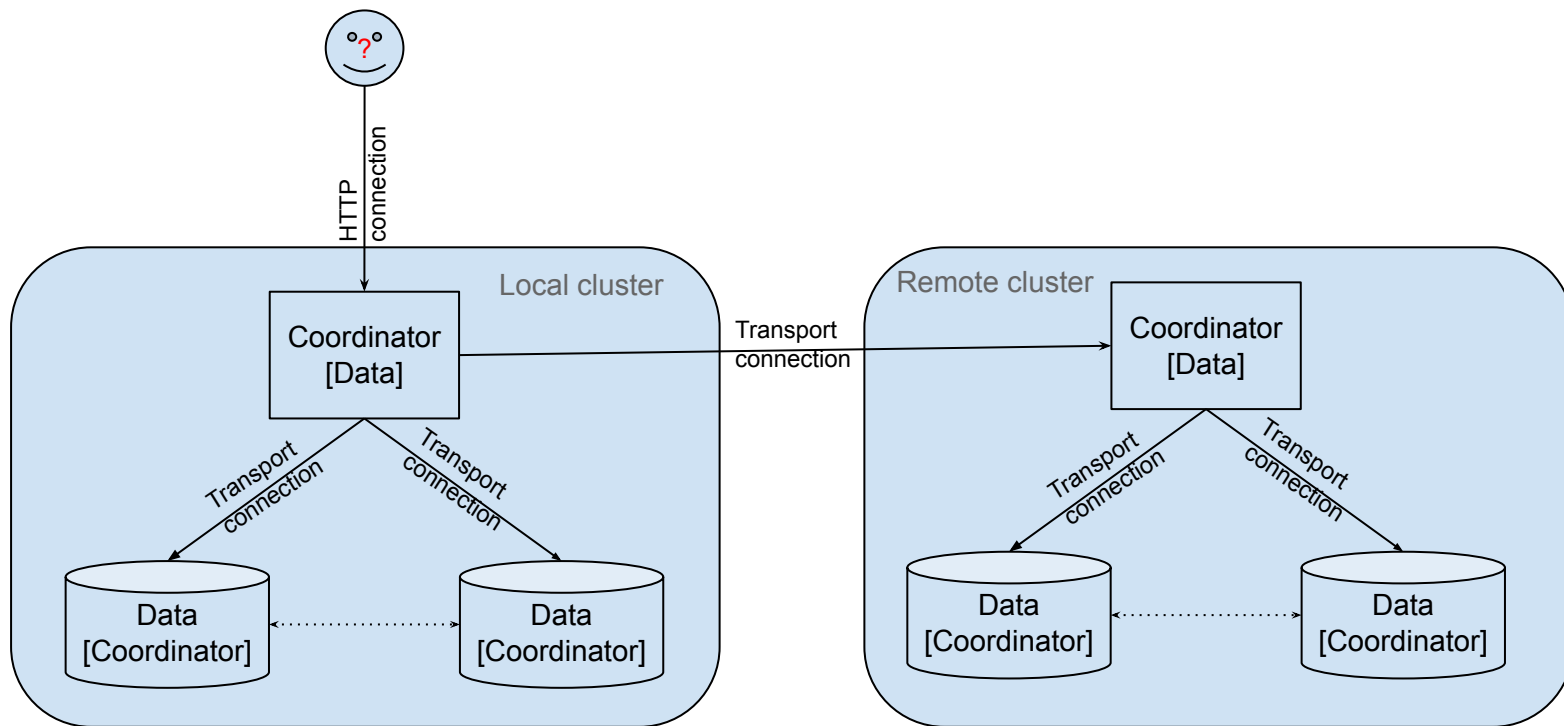
ES|QL

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

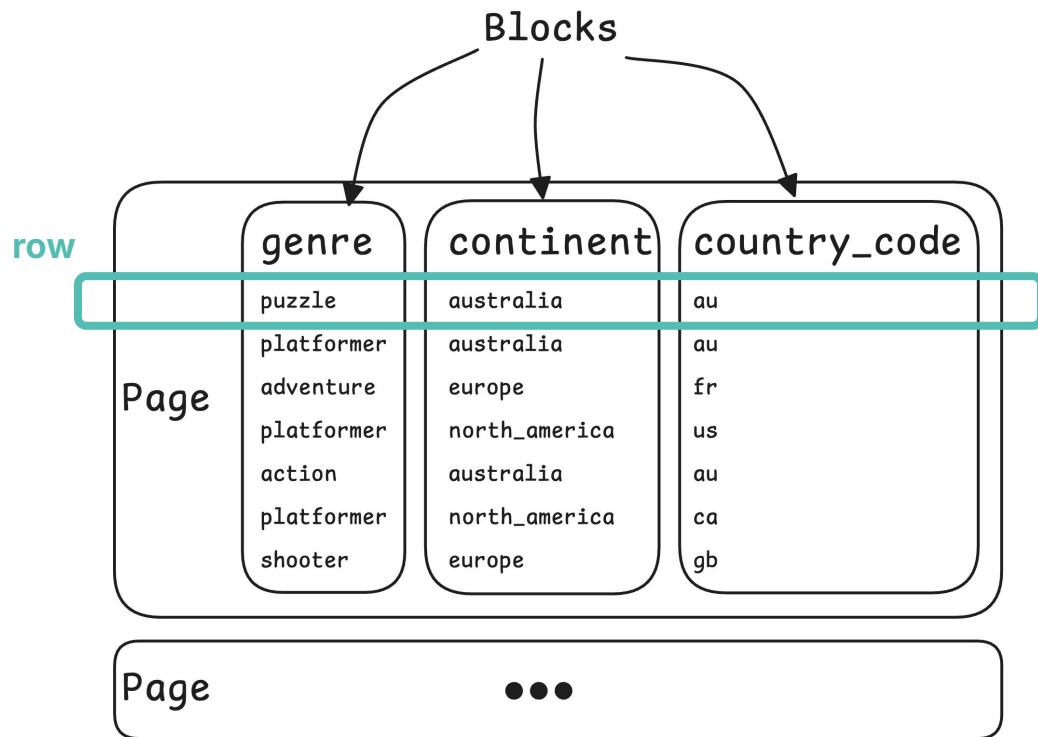
SQL



Distributed



Vectorized



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**

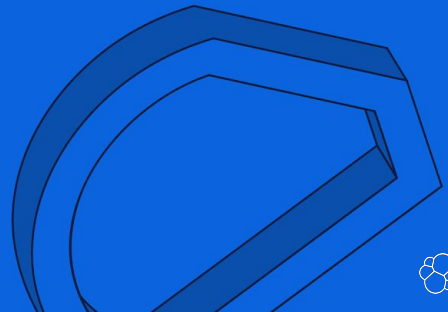
Distributed & Dedicated Query Engine

`_query`



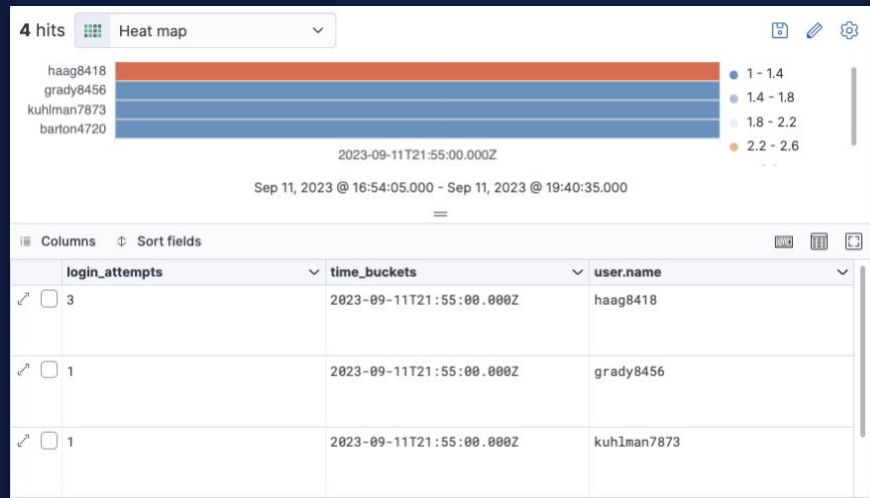
- No transpilation or translation
- Queries are parsed and optimized for distributed execution
- It operates in blocks, instead of one row at a time
- It takes advantage of specialization and multi-threading
- Benchmarking has shown ES|QL can outperform DSL in many instances

Understanding ES|QL Syntax



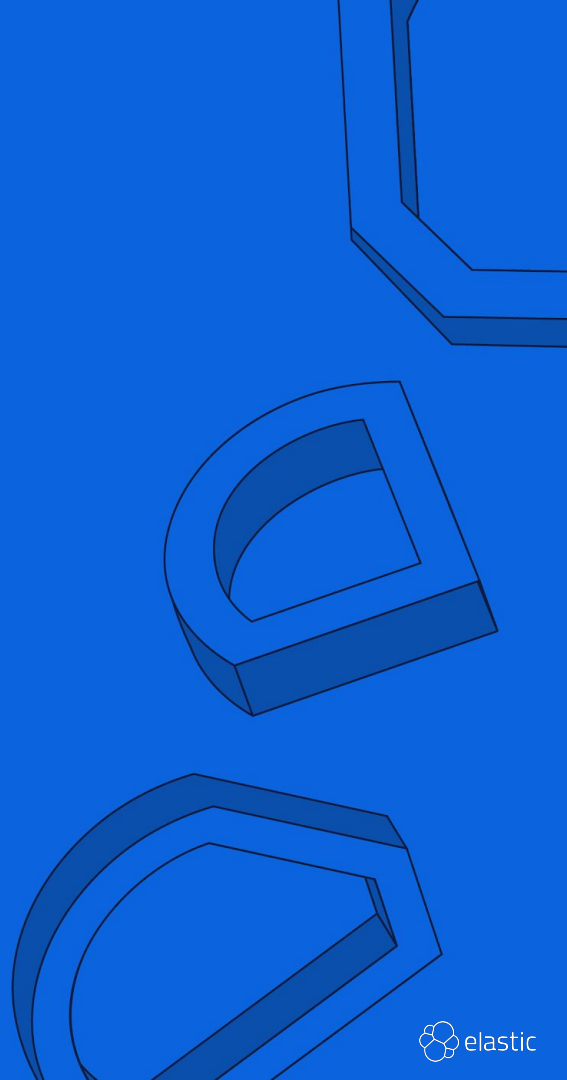
An ES|QL query

```
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
```



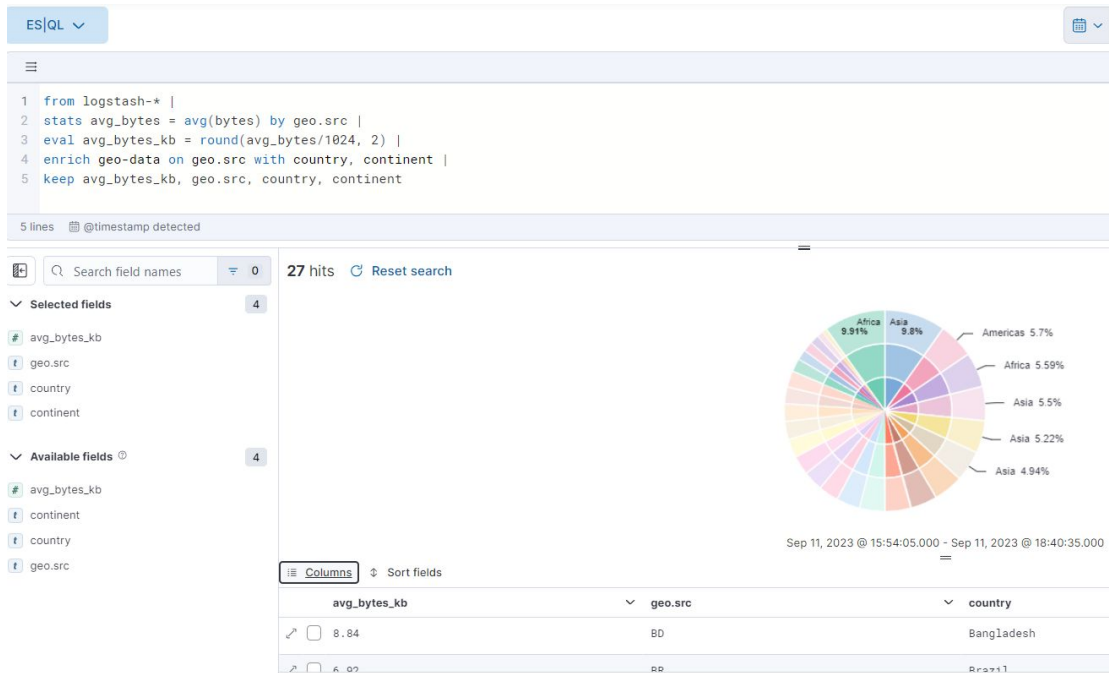
Expressive, Powerful, Composable, Extensible, Fast

Unified User Experience

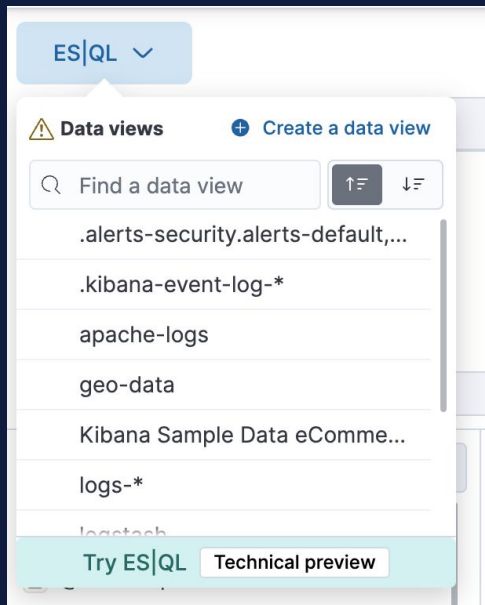


ES|QL UX

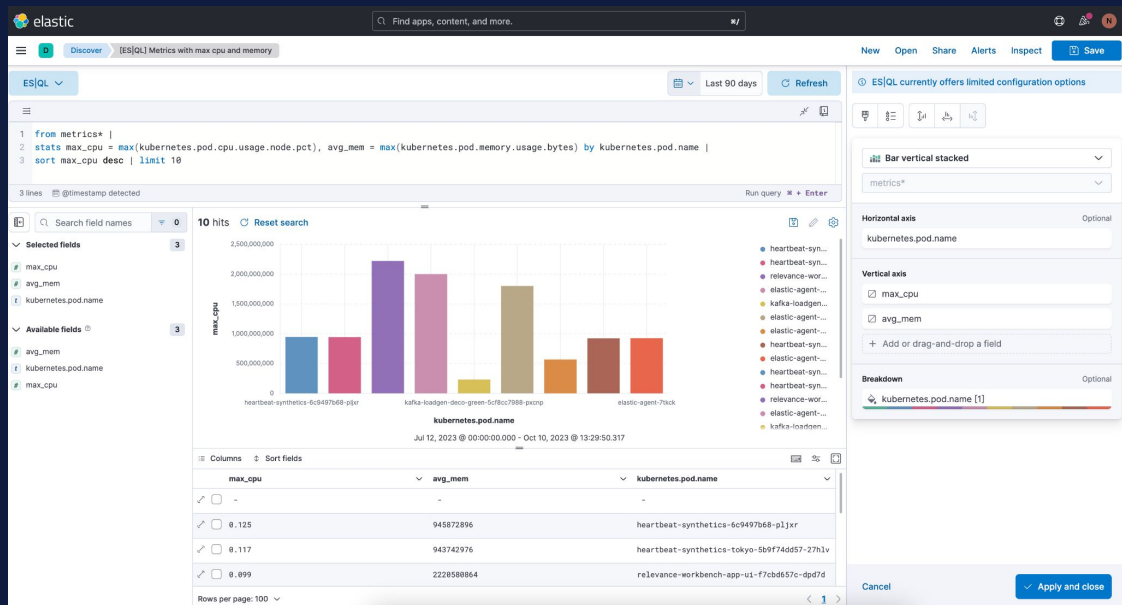
Data Exploration,
Transformation and
Visualization all in one



ES|QL in Discover

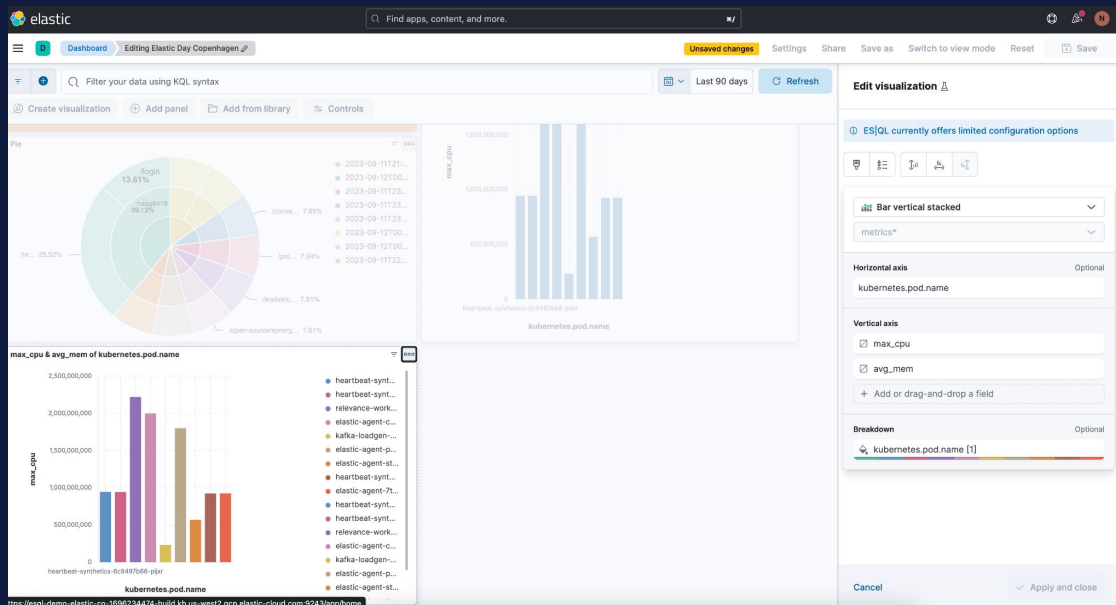


ES|QL is under the data view picker in Discover



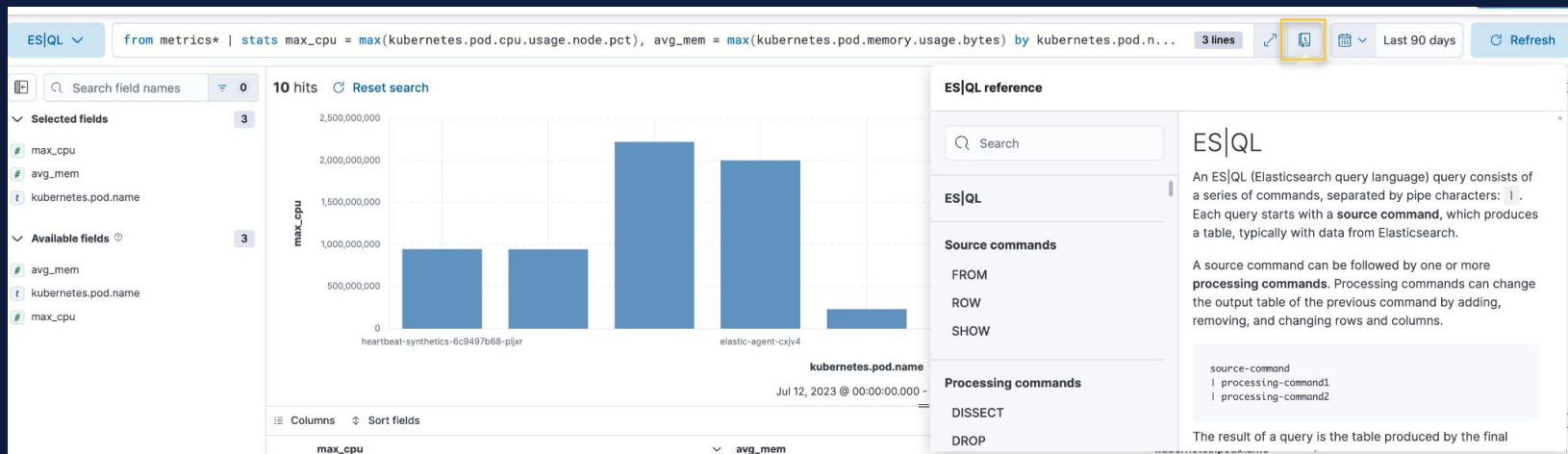
The ES|QL experience in Discover includes Lens visualizations and in-line editing.

ES|QL in Dashboard

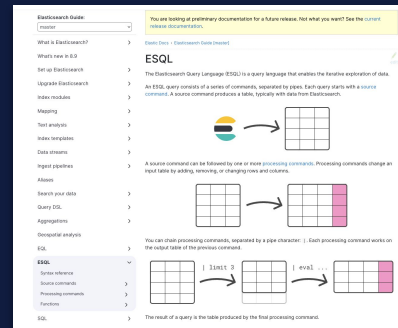


Save ES|QL charts from Discover and use them on Dashboards.
ES|QL charts also have in-line editing in Dashboard

In Product ES|QL Documentation



- In-line documentation right at your fingertips!
- Full documentation page: [ES|QL](#)



ES|QL Workshop

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 their 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")
```

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
ghcnv2_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 aggregations.
        # 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

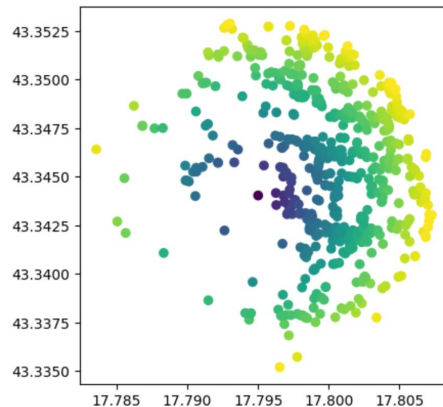
Focusing on the current geospatial features in ES|QL:

- 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
# query as a WKT instead of a binary.
query = """
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*`

Data Views

Create and manage the data views that help y

Search...

☐ Name ↑

☐ Overturemaps Places ⓘ **Default**

☐ Kibana Sample Data Flights ⓘ

☐ Kibana Sample Data Logs ⓘ

☐ Kibana Sample Data eCommerce ⓘ

☐ Natural Earth Airports ⓘ

☐ NaturalEarth Countries ⓘ

☐ civio-fires ⓘ

☐ geonames ⓘ

☐ ghcdnd_daily_observations ⓘ

☐ osm_* ⓘ

Rows per page: 10 ▾

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
ghcnv2_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

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

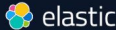
 Manage permissions

 Monitor the stack

 Back up and restore

 Manage index lifecycles

ANALYTICS



Q Find apps, content, and more.



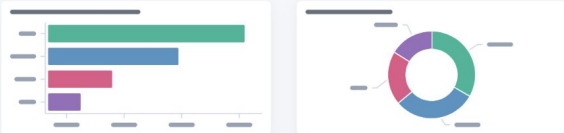


Analytics



Analytics

 Dev tools  Manage  Add integrations



Dashboard

Analyze data in dashboards.



Discover

Search and find insights.



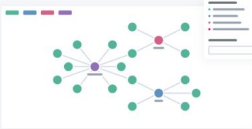
Maps

Plot geographic data.



Machine Learning

Model, predict, and detect.



Graph

Reveal patterns and relationships.



Find apps, content, and more.

 ^/



J



Elasticsearch



Elasticsearch

[Home](#)
Content
Index Management
Connectors
Web Crawlers

Build
Playground
Search Applications

Relevance
Inference Endpoints
Synonyms

Getting started
Elasticsearch
Vector Search
Semantic Search
AI Search



Hi [jorge.sanz@elastic.co!](#)

Add data to Elasticsearch and then search, vectorize, or visualize

There are endless ways to ingest and explore data with Elasticsearch, connect to your Elasticsearch instance and start indexing data



Elasticsearch endpoint:
`https://a118488329bd463bbf184cea9a053f01.eastus2.azure.elastic-cloud.com:443`

Cloud ID:
`jorgesanz:ZWFzdHVzM15henVzS5lbGFzdGljLWNsb3VklmNvbSRhMTE4NDg4MzI5YmQ0NjNiYmYxODRjZWESYTA1M2YwMSQzNzJmNzkwOTM0NjM0YzM5YjIwYTg3YzM2Y2UyMWI5NA==`

23 active API keys

 New

 Manage

Ingest your content

The first step in building your search experience is to create a search-optimized Elasticsearch index and import your content into it. Elasticsearch offers several user-friendly options you can choose from that best match your technical expertise and data sources.



API
Add documents programmatically by connecting with the API using your

BETA



Web Crawler
Discover, extract, and index



Connectors
Extract, transform, index and sync data from a third-party data source.

jorge-sanz.kb.eastus2.azure.elastic-cloud.com/app/elasticsearch/content/crawlers

 Notebooks





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



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 filter 0

Auto interval

No breakdown

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

200,000

150,000

100,000

50,000

0

10:00

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

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

Documents (2,028,494)

Field statistics

Columns 8

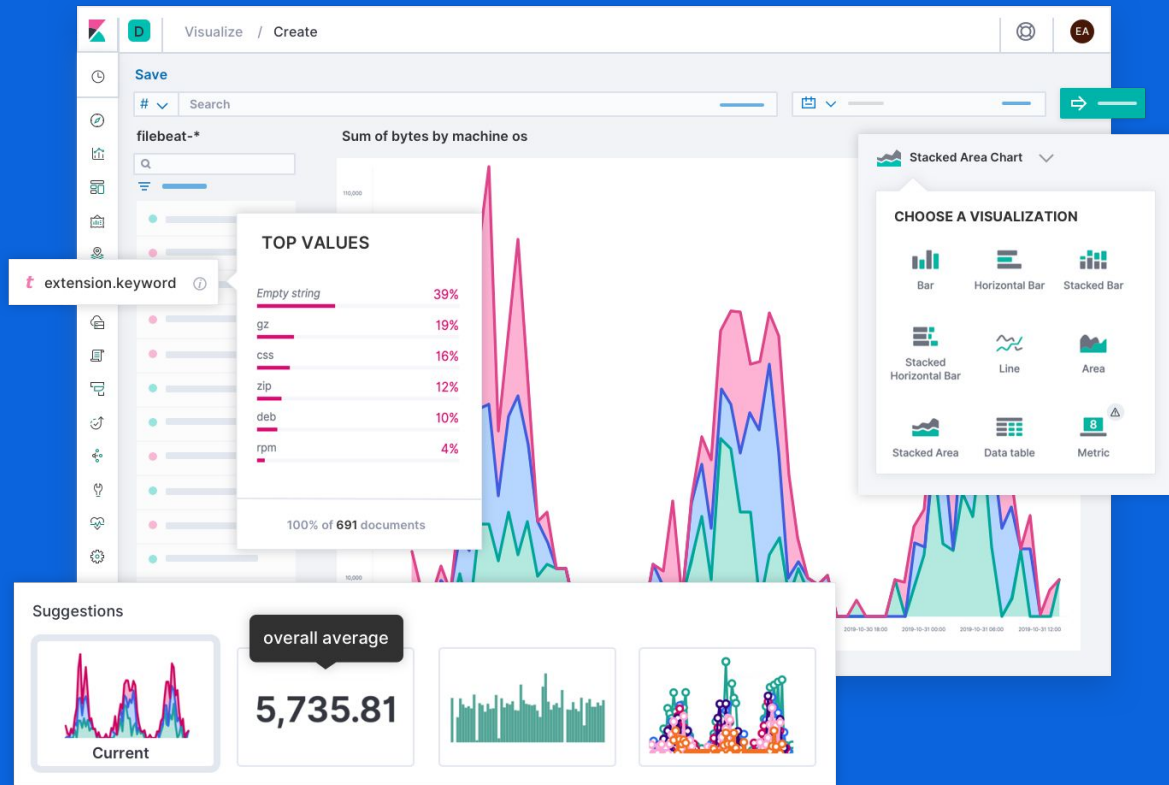
Sort fields 1

	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 (-114.9839 36.1492)
☐	Jul 10, 2025 @ 21:34:32.000	N659HA	274.32	25.25	false	United States	-	POINT (-76.1841 48.6052)

Lens

Your data in front of you

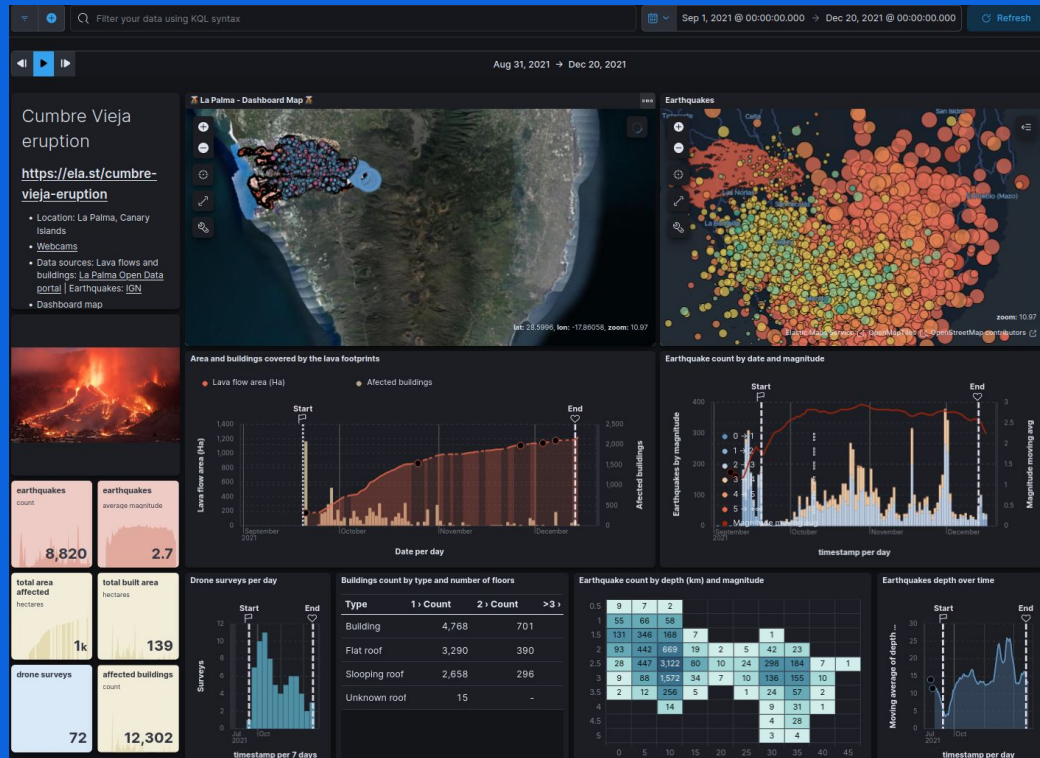
- Explore your fields with a single click
- Drag and drop
- Go from nothing to visual insights with a single mouse gesture.
- Smart suggestions
- Let Lens help guide your analysis with useful chart suggestions



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 



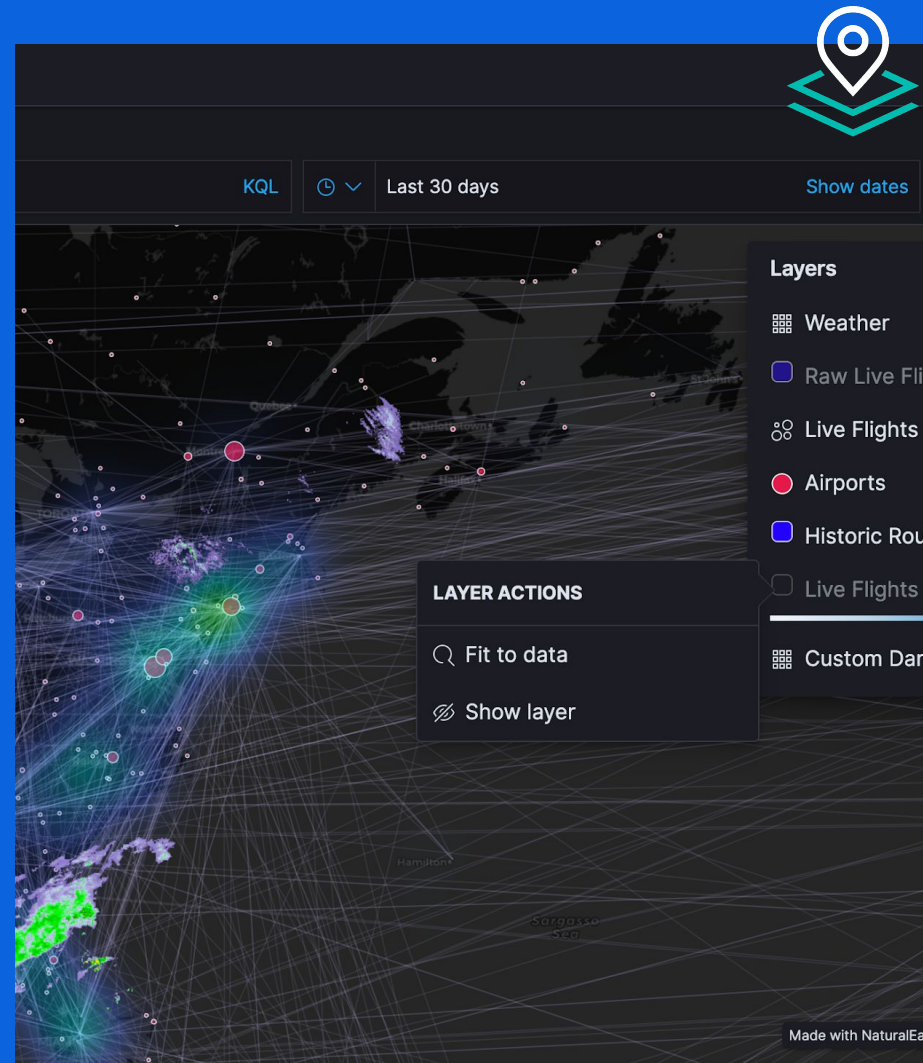


Elastic Maps

Elastic Maps

Geo Analytics interface within Kibana

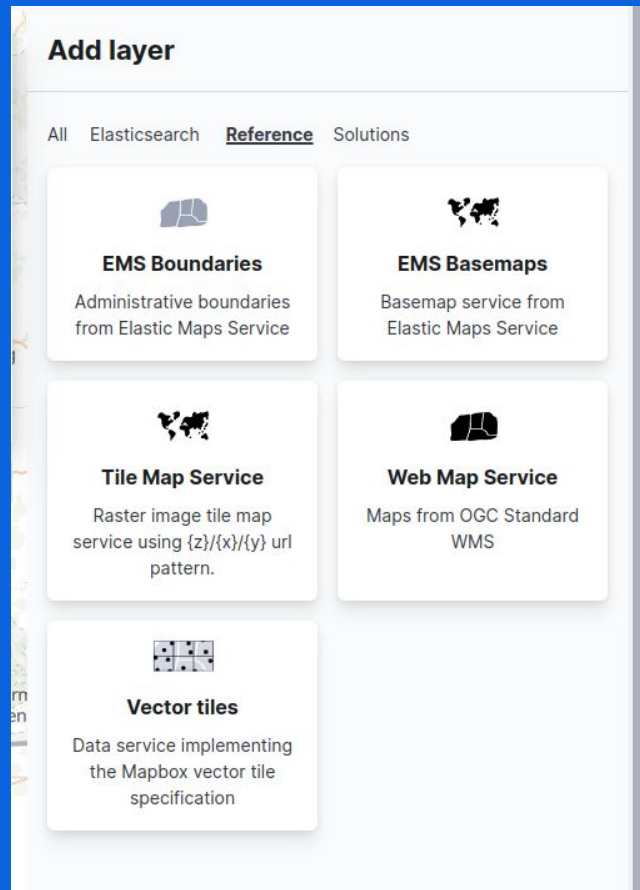
- **Friendly** user experience
- **Aggregations**: heat map, clustering, grids, geoline
- Data driven **styling**
- **Tools** for drawing, filtering, measuring
- Add layers from **external** tile servers
- Used alone or in dashboards
- **Embedded** in other apps



Reference data

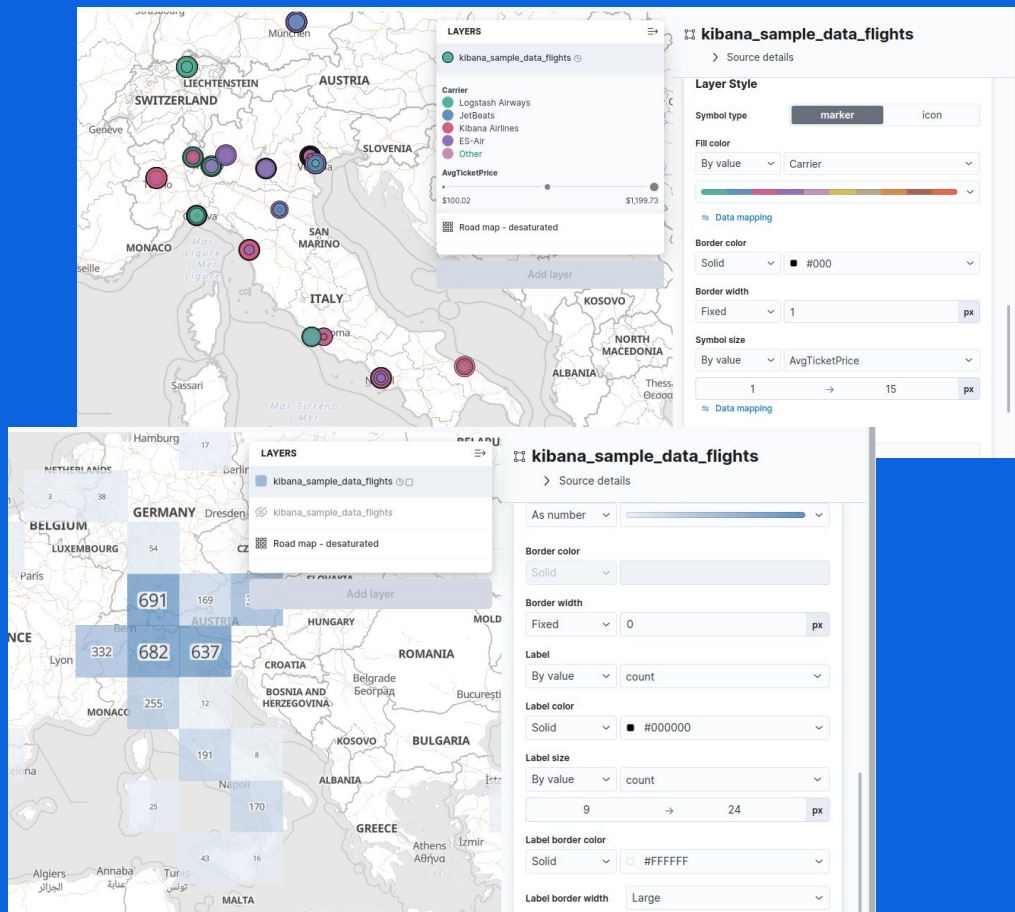
Data that provides context

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



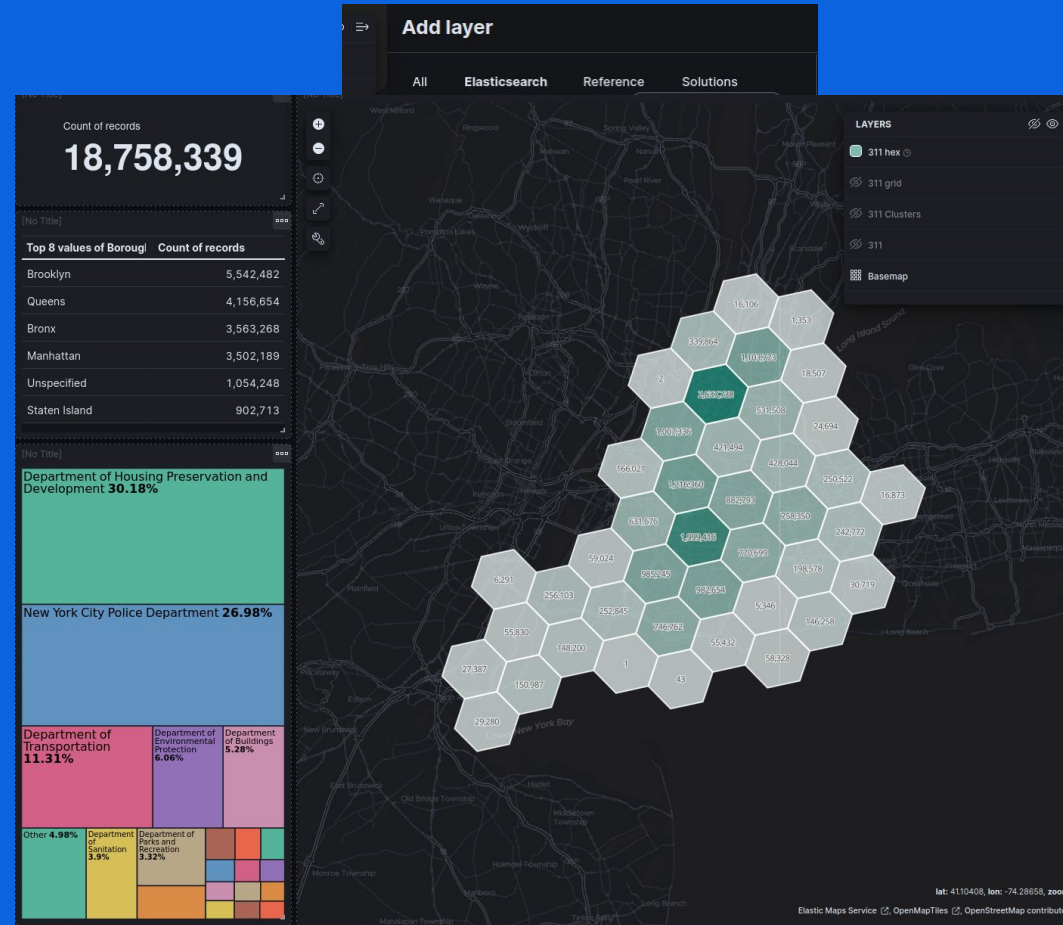
Data Driven Styling

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



Big Data Rendering

- Heatmap
- Clusters
- Tile aggregation
- Hexagon aggregation 

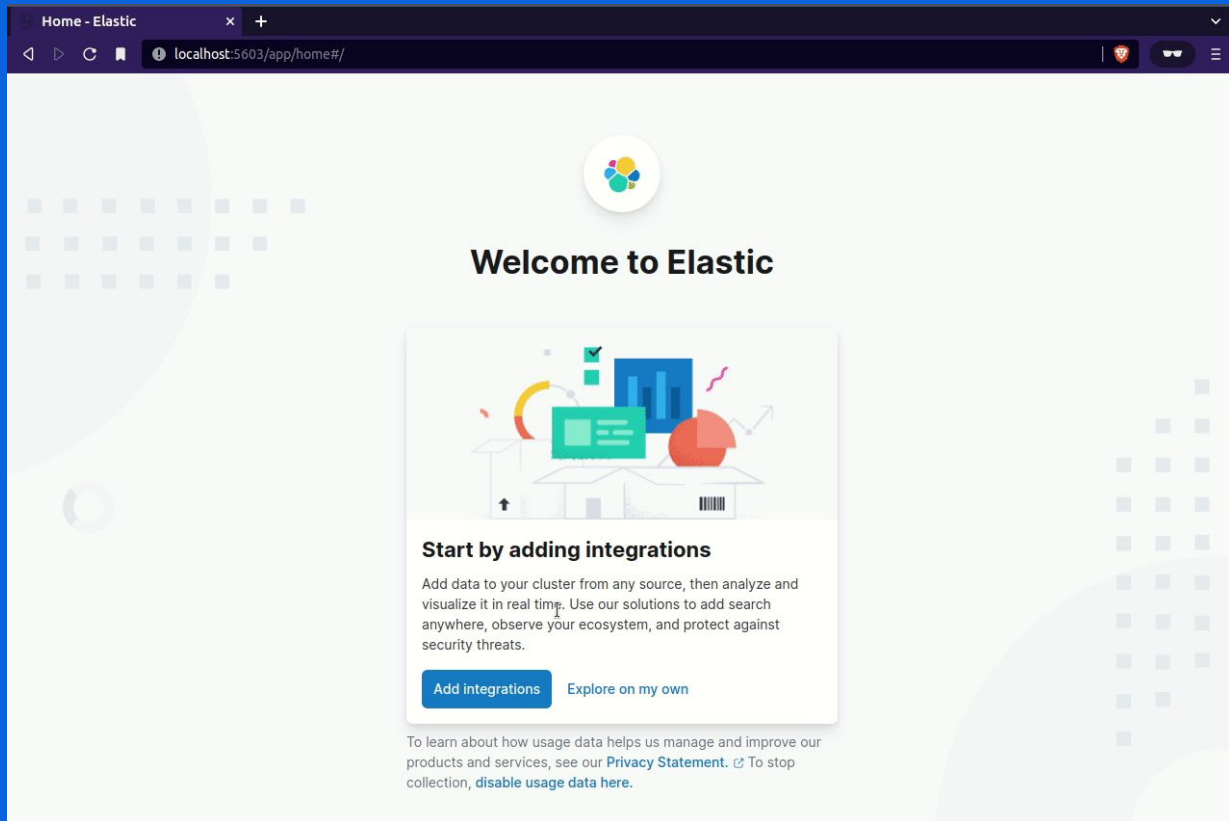


Data Views

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)



Discover

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 for 0



Auto interval ▾

No breakdown ▾



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

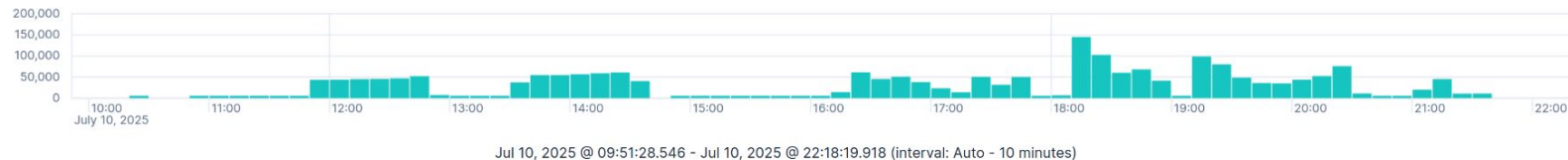
📍 baroAltitude

📅 callsign

📍 country.iso_a2

📍 geoAltitude

📍 heading



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

Documents (2,028,494)

Field statistics

Columns 8

Sort fields 1

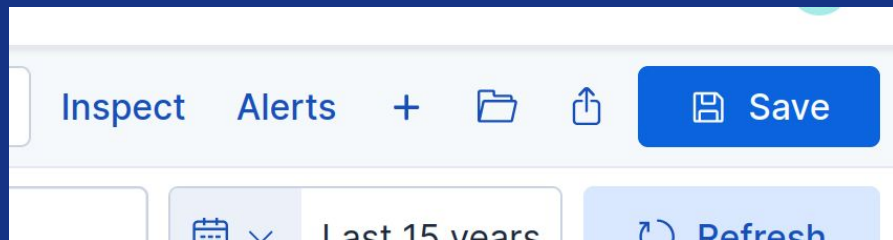


☐	timePosition 🕒	📅 callsign	📍 geoAltitude	📈 velocity	📍 onGround	📍 originCountry	📍 country.iso_a2	📍 location
☐	↗️ Jul 10, 2025 @ 21:34:32.000	WJA544	3,771.9	171.19	false	Canada	-	POINT (-113.6974 51.1712)
☐	↗️ Jul 10, 2025 @ 21:34:32.000	SWA935	11,193.78	230.54	false	United States	-	POINT (-87.4968 40.3326)
☐	↗️ 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)

Search sessions

Persist your common search settings

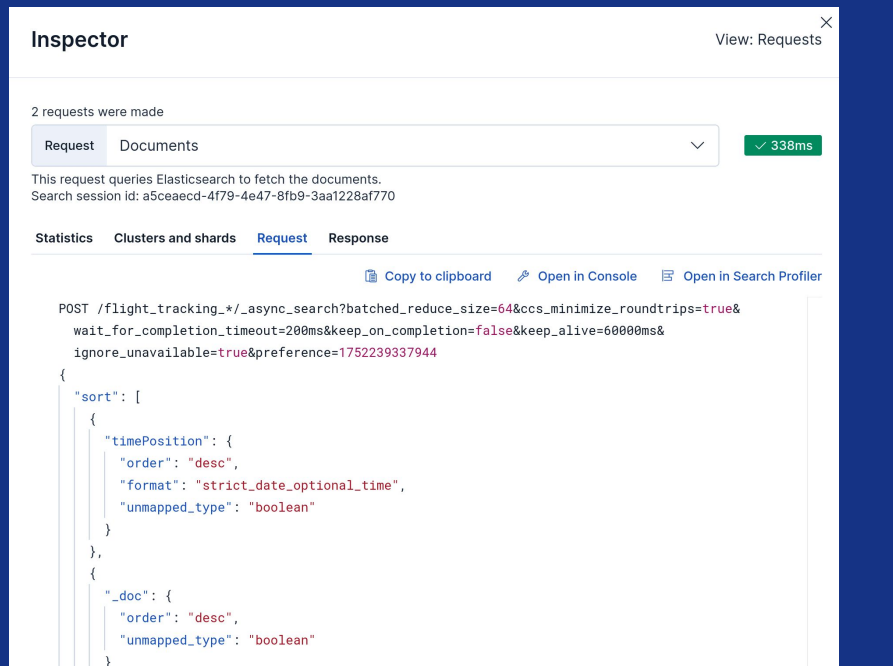
- Save and restore
- Can be added to dashboards
- Can be exported as links or CSV



Inspector

Get details of your queries to Elasticsearch

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



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 for



0



Auto interval ▾

No breakdown ▾



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

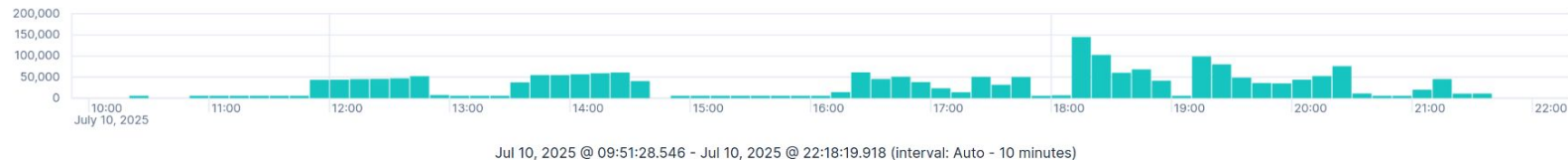
baroAltitude

callsign

country.iso_a2

geoAltitude

heading



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

Documents (2,028,494)

Field statistics

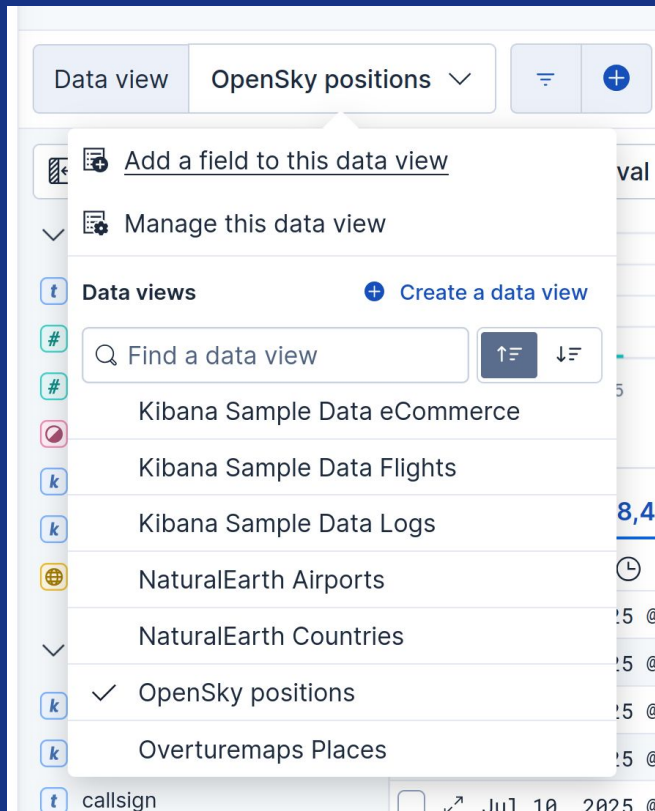
Columns 8

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)

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 for

≡

0



Auto interval ▾

No breakdown ▾



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



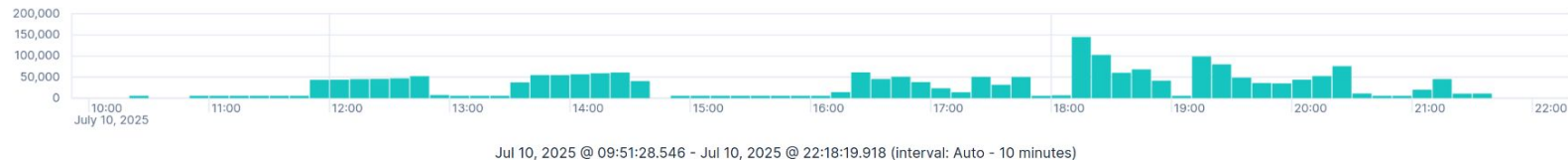
country.iso_a2



geoAltitude



heading



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

Documents (2,028,494)

Field statistics

Columns 8

Sort fields 1

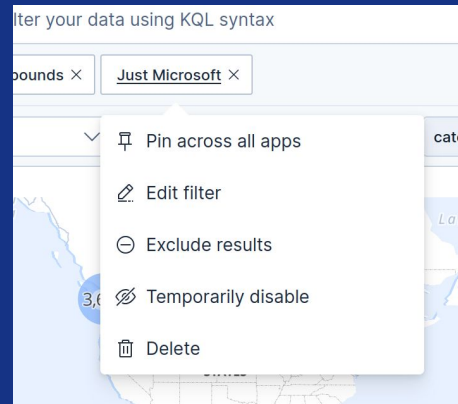
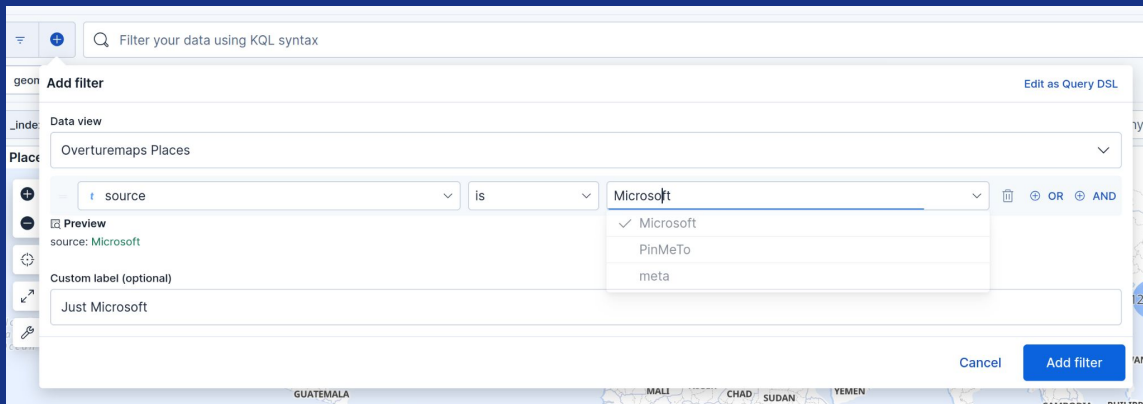


☐	timePosition	☐	callsign	☐	geoAltitude	☐	velocity	☐	onGround	☐	originCountry	☐	country.iso_a2	☐	location
☐	↗ Jul 10, 2025 @ 21:34:32.000		WJA544		3,771.9		171.19		false		Canada		-		POINT (-113.6974 51.1712)
☐	↗ Jul 10, 2025 @ 21:34:32.000		SWA935		11,193.78		230.54		false		United States		-		POINT (-87.4968 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

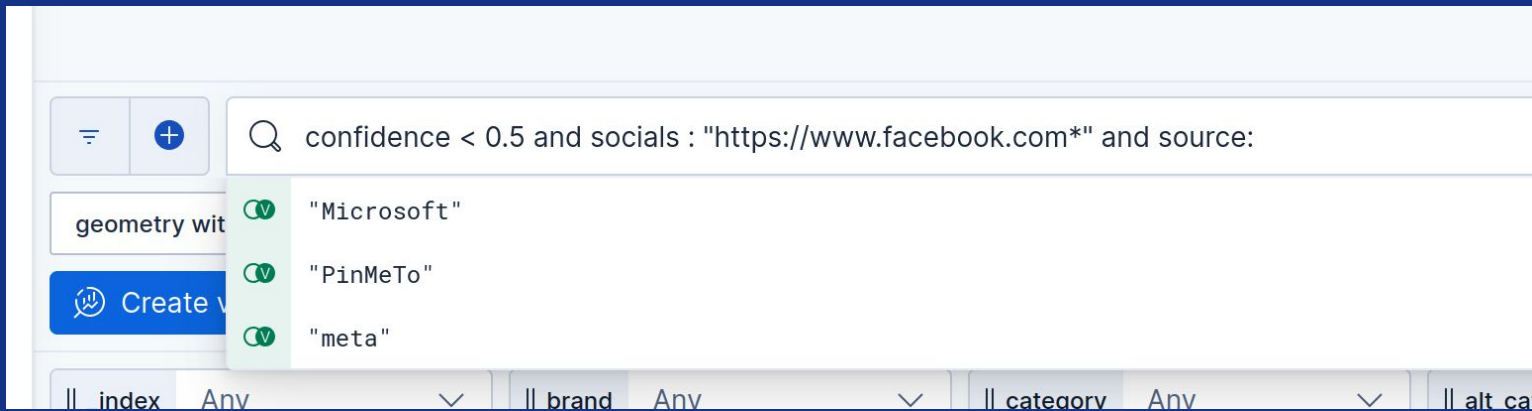
- Easy filter creation, but DSL also available
- Custom label
- Transferred across dashboards and applications
- Also available on view mode



Query bar

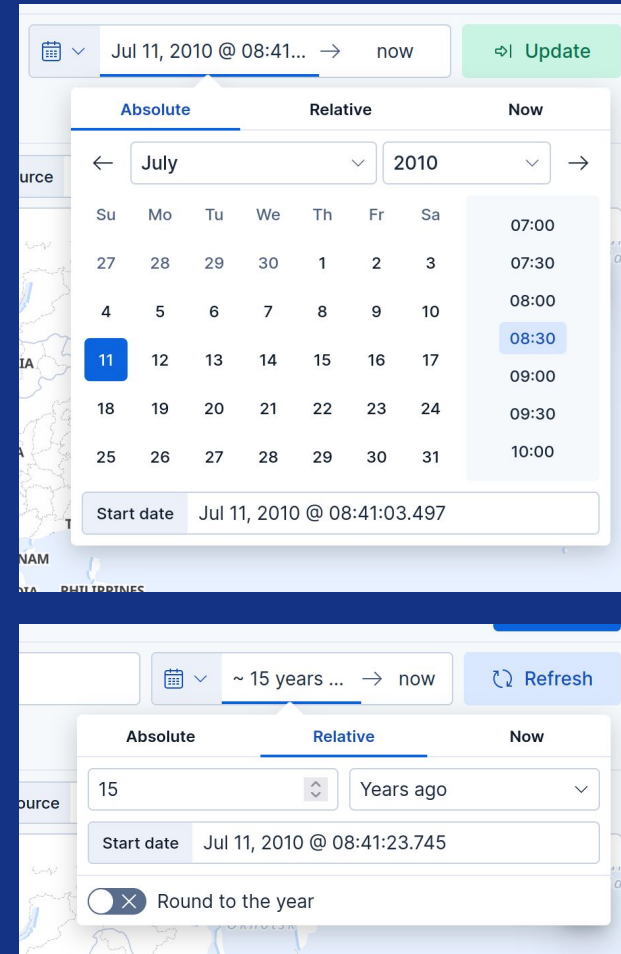
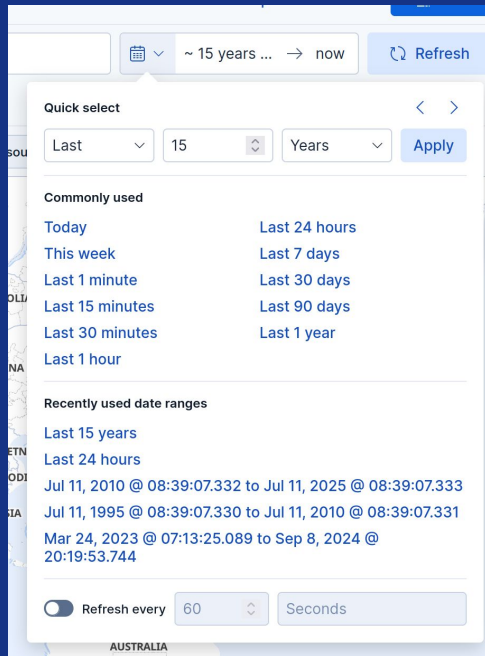
Advanced ad-hoc queries

- 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



Search fields 0



Auto interval ▾



No breakdown ▾

Selected fields 7

callsign

geoAltitude

velocity

onGround

originCountry

country.iso

location

Popular fields

country.iso

originCountry

callsign

geoAltitude

location

onGround

velocity

Available fields 16

@timestamp

baroAltitude

callsign

country.iso_a2

geoAltitude

heading

200,000

150,000

100,000

50,000

0

10:00

11:00

July 10, 2025

Auto interval ▾

Breakdown by originCountry ▾

Select breakdown field

Search

k icao24

onGround

✓ k originCountry

positionSource

spi

k transponderCode



Auto interval ▾

Breakdown by originCountry ▾

Select breakdown field

Search

k icao24

onGround

✓ k originCountry

positionSource

spi

k transponderCode

Documents (2,028,494)

timePosition

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

Jul 10, 2025 @ 21:34:32.000

CAT682

SWA2855

AAL654

SKW3768

GRIT10

DAL2068

SWA1067

N659HA

12,077.7

8,983.98

7,581.9

5,836.92

830.58

11,483.34

2,857.5

274.32

226.12

198.39

245.42

190.36

53.68

229.06

148.93

25.25

false

false

false

false

false

false

false

false

Denmark

United States

United States

United States

United States

United States

United States

United States

-

-

-

-

-

-

-

-

POINT (6.2616 43.8774)

POINT (-106.4537 40.4538)

POINT (-95.1424 32.9164)

POINT (-119.2377 37.3981)

POINT (10.7329 49.3177)

POINT (-83.3481 40.9473)

POINT (-114.9039 36.1492)

POINT (-76.1041 40.6057)

United States

United Kingdom

Germany

Other

Columns 8

Sort fields 1



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



Q Search filter

0



Auto interval ▾

No breakdown ▾



Selected fields 7

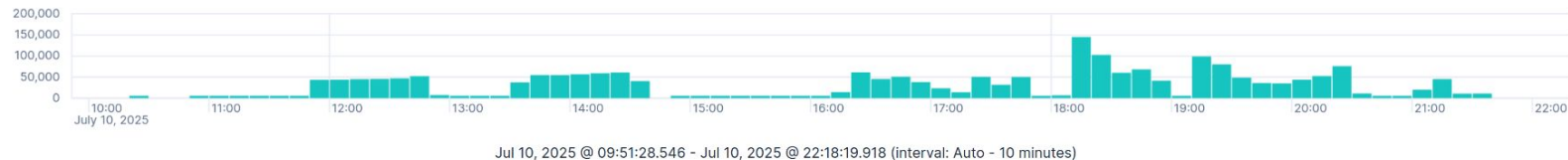
callsign
geoAltitude
velocity
onGround
originCountry
country.iso_a2
location

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)

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

The screenshot shows the Elasticsearch field selection interface. On the left, a list of fields is displayed, categorized into 'Popular fields' (7) and 'Available fields' (16). The 'originCountry' field is selected, and its details are shown in a modal on the right. The modal displays the field name 'originCountry' and a 'Field statistics' section. The 'Top values' section shows a horizontal bar chart of the top 10 values for 'originCountry'.

Value	Percentage	Actions
United States	58.9%	+ -
Canada	4.0%	+ -
United Kingdom	3.7%	+ -
Turkey	2.9%	+ -
United Arab Emirates	2.2%	+ -
Spain	2.1%	+ -
Austria	2.0%	+ -
China	1.8%	+ -
France	1.5%	+ -
Brazil	1.4%	+ -
Other	19.5%	

Calculated from 5,000 sample records.

Visualize

Rows per page: 100

Documents (2,028,494) [Field statistics](#)

>	Type	Name	Documents (%)	Distinct values	Distributions	Actions
>	t	callsign	986 (98.6%)	986		
>	k	callsign.keyword	4,943 (98.86%)	4916		

Documents (283,396) [Field statistics](#)

>	Type	Name	Documents (%)	Distinct values	Distributions	Actions
>	#	geoAltitude	4,526 (90.52%)	1294		

DOCUMENTS STATS

count	4526
-------	------

SUMMARY

min	-22.86
-----	--------

TOP VALUES

11,277.6	19 (0.4%)
----------	-----------

DISTRIBUTION

Documents (283,396) [Field statistics](#)

>	Type	Name	Documents (%)	Distinct values	Distributions	Actions
---	------	------	---------------	-----------------	---------------	---------

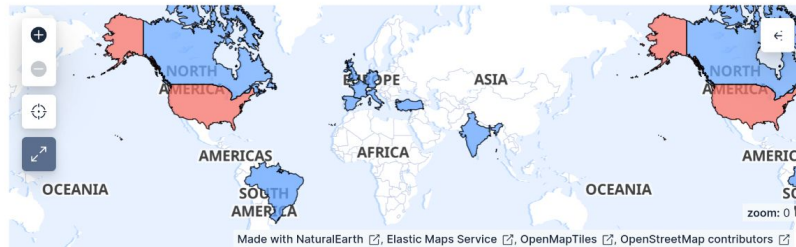
DOCUMENTS STATS

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.



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

The screenshot displays the Elastic Documents table interface with several overlays demonstrating its functionality:

- Document Viewer:** A top window shows document navigation controls, including a table/JSON toggle and search fields.
- Field Statistics:** A pop-up for the 'c...' field shows a distribution of values (e.g., 1,203.96, 221.91, false) and a 'Filter for' button.
- Column Context Menu:** A menu for the 'timePosition' column offers actions like 'Remove column', 'Sort A-Z', 'Sort Z-A', 'Move left', 'Move right', 'Reset width', 'Copy name', 'Copy column', 'Edit data view field', and 'Clear selection'.
- Selection Menu:** A menu for '2 Selected' documents provides options such as 'Compare selected', 'Copy selection as text', 'Copy documents as JSON', 'Show selected documents only', and 'Clear selection'.

The background shows a table of documents with columns for numerical values, boolean flags, and timestamps.

Discover & ES|QL

Discover & ES|QL

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

Switch to classicInspectAlerts+Save

ES|QL helpJul 10, 2025 @ 09:02:27.771 → Jul 10, 2025 @ 23:36:30.9...Run

```
1 FROM places-* METADATA _index | RENAME _index as dataset
2 | WHERE name LIKE "*Burger*" AND category IN ("restaurant", "burger_restaurant") AND confidence < 0.3
3 | SORT confidence DESC | KEEP dataset, name, category, confidence
```

3 lines @timestamp not found LIMIT 1000 rowsSubmit feedbackShow recent queries

Selected fields4

datasetnamecategoryconfidence

Available fields4

categoryconfidencedatasetname

25 results

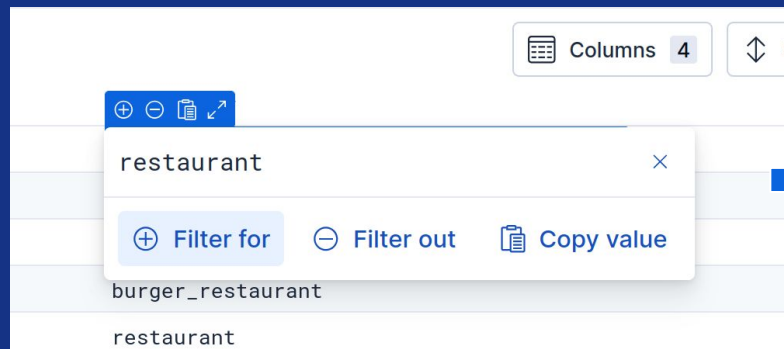
☐	dataset	name	category	confidence
☐	places-belem	Nick Burger	burger_restaurant	0.297
☐	places-capetown	Ko Burgers	restaurant	0.297
☐	places-belem	Purple Burgers	burger_restaurant	0.297
☐	places-capetown	The BlaauwBurger	restaurant	0.297
☐	places-valencia	TORO Burger Lounge	restaurant	0.297

Columns4Sort fields

places-belem 32.1%places-seoul 27.58%places-bosnia 19.32%

Discover & ES|QL

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



Dashboards



D

/ [Deployment](#) / [Kibana](#) / [Dashboards](#) / Editing New Dashboard



Settings

Share

Switch to view mode

Save



Filter your data using KQL syntax



Last 15 minutes



Create visualization



Add panel



Add from library

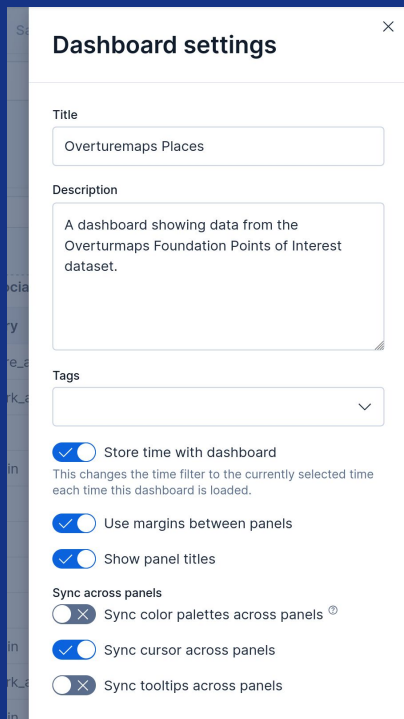


Controls



Settings

Metadata and general appearance

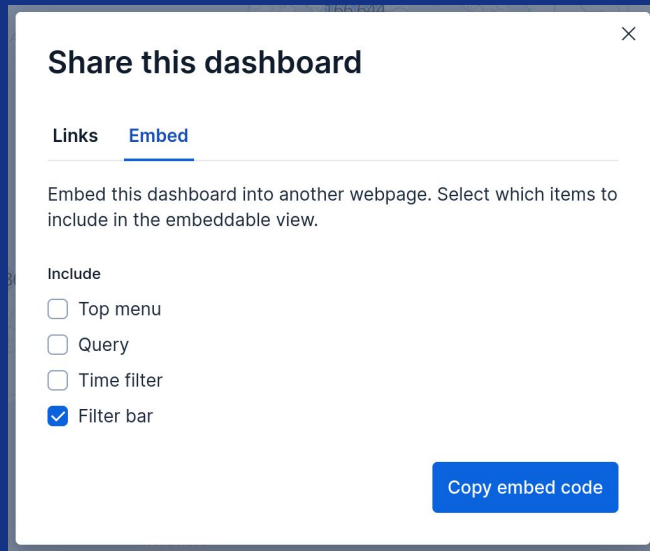


The 'Dashboard settings' dialog box is shown with a close button (X) in the top right corner. It contains the following sections:

- Title:** A text input field containing 'Overturemaps Places'.
- Description:** A text area containing 'A dashboard showing data from the Overturemaps Foundation Points of Interest dataset.'
- Tags:** A dropdown menu with a downward arrow.
- Options:**
 - ☒ Store time with dashboard
This changes the time filter to the currently selected time each time this dashboard is loaded.
 - ☒ Use margins between panels
 - ☒ Show panel titles
- Sync across panels:**
 - ☐ Sync color palettes across panels [Ⓢ]
 - ☒ Sync cursor across panels
 - ☐ Sync tooltips across panels

Share

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



The 'Share this dashboard' dialog box is shown with a close button (X) in the top right corner. It contains the following sections:

- Links** and **Embed** tabs. The 'Embed' tab is selected and underlined.
- Instructions:** 'Embed this dashboard into another webpage. Select which items to include in the embeddable view.'
- Include:**
 - ☐ Top menu
 - ☐ Query
 - ☐ Time filter
 - ☒ Filter bar
- Copy embed code:** A blue button at the bottom right.



D

/ [Deployment](#) / [Kibana](#) / [Dashboards](#) / [Editing New Dashboard](#)



[Settings](#)

[Share](#)

[Switch to view mode](#)

[Save](#)



Filter your data using KQL syntax



Last 15 minutes



Create visualization



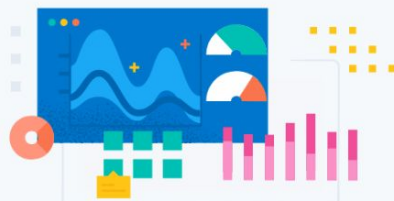
Add panel



Add from library

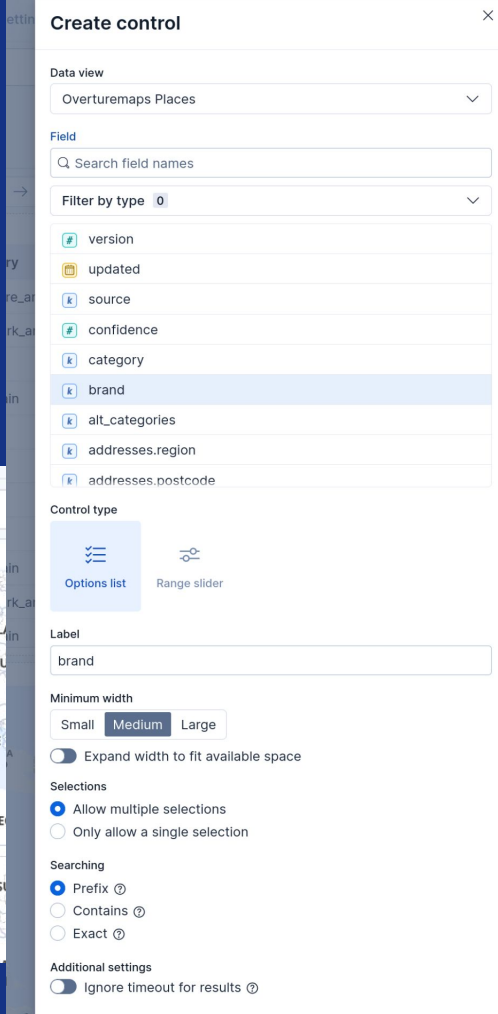
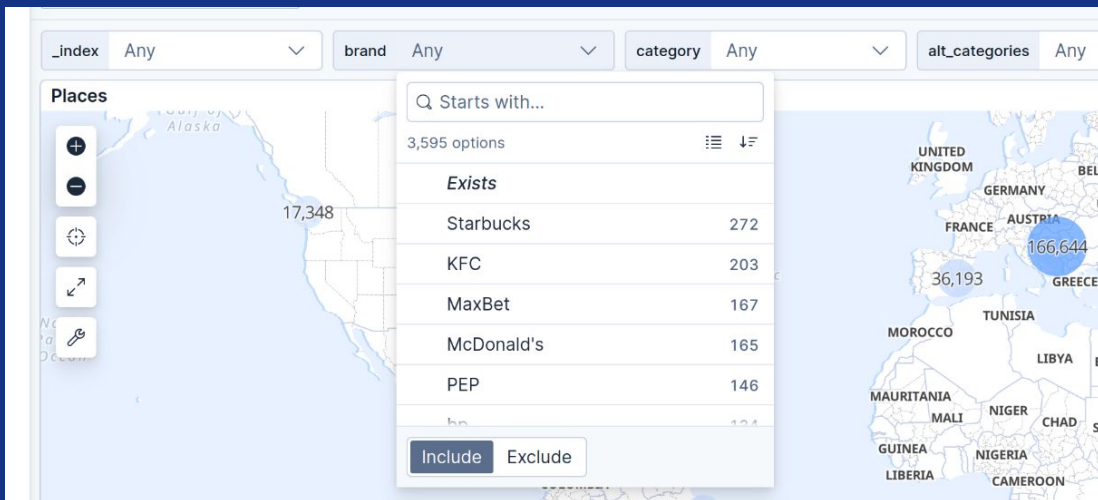


Controls



Controls

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



Drilldowns

Drilldowns



Drilldowns enable you to define new behaviors for interacting with panels. You can add multiple actions and override the default filter.

Hide

[View docs](#)

Create new

Manage



Go to
Dashboard



Go to URL



Open in
Discover

Action
 Go to Dashboard

[Change](#)

Name

Go to Dashboard

Trigger



Apply filter

When kibana filter is applied. Could be a single value or a range filter.

Choose destination dashboard

[Flights] Global Flight

☒ Use filters and query

☒ Use date range from

☐ Open dashboard in

Action

Go to URL

[Change](#)

Name

Go to URL

Trigger



Single click

A data point click on the visualization



Context menu

A new action context menu

Enter URL

https://www.elastic.co
={{event.value}}

To validate and test the drilldown from the panel

> Additional options

Action

Open in Discover

[Change](#)

Name

Open in Discover

Trigger



Apply filter

When kibana filter is applied. Could be a single value or a range filter.

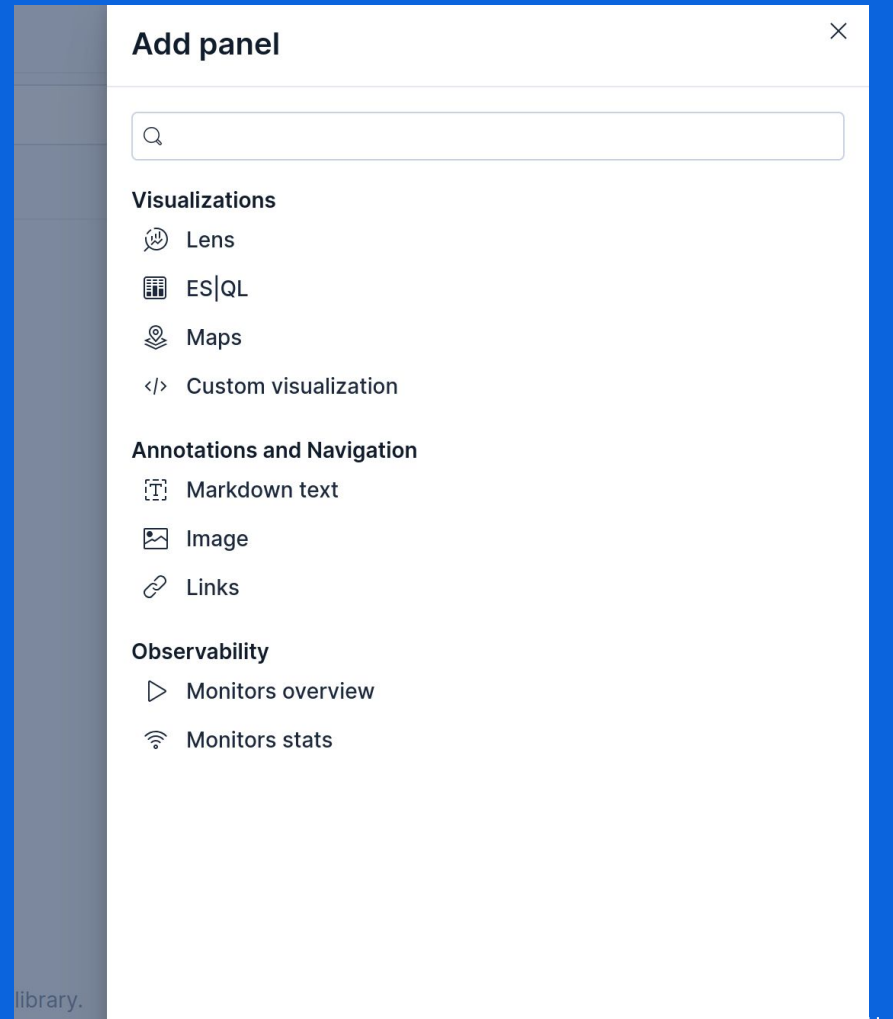
☒

Open in new tab

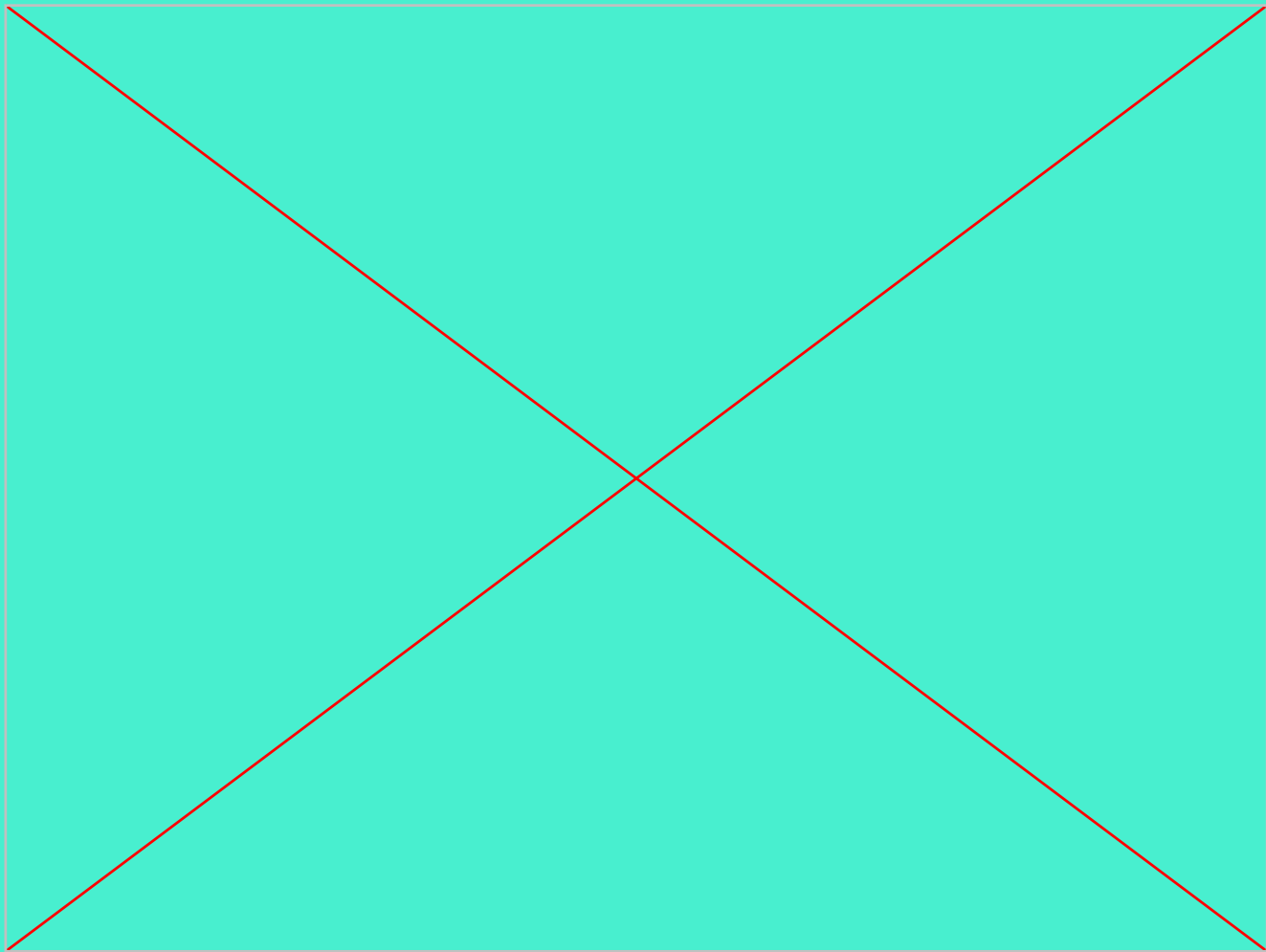
Dashboard panels

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

The screenshot displays the Elastic Lens interface. On the left, the 'Available fields' list contains 12 fields: addresses.country, addresses.locality, addresses.postcode, addresses.region, alt_categories, brand, category, confidence, geometry, source, updated, and version. A pink arrow points from this list to the main visualization area. The main area features a large teal square with a hand icon and the text 'Drop some fields here to start'. Below this, it says 'Lens is the recommended editor for creating visualizations' and 'Make requests and give feedback'. A pink arrow points from the main area to the right-hand selectors. The right-hand side contains three selectors: 'Horizontal axis', 'Vertical axis', and 'Breakdown'. Each selector has a '+ Add or drag-and-drop a field' button. A pink arrow points from the 'Horizontal axis' selector to the 'Add layer' button at the bottom. The 'Add layer' button is a blue button with a plus icon and the text 'Add layer'.

Data view | Overturemaps Places | Filter your data using KQL syntax | Last 15 years | Refresh

Search field names | 0

Records

Available fields 12

- addresses.country
- addresses.locality
- addresses.postcode
- addresses.region
- alt_categories
- brand
- category
- confidence
- geometry
- source
- updated
- version

Meta fields 2

Drop some fields here to start

Lens is the recommended editor for creating visualizations

Make requests and give feedback

Horizontal axis | Optional

+ Add or drag-and-drop a field

Vertical axis

+ Add or drag-and-drop a field

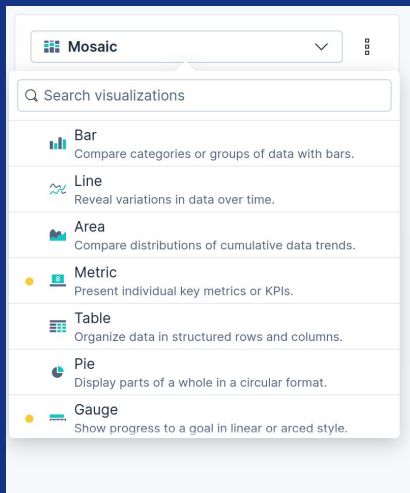
Breakdown

+ Add or drag-and-drop a field

Add layer

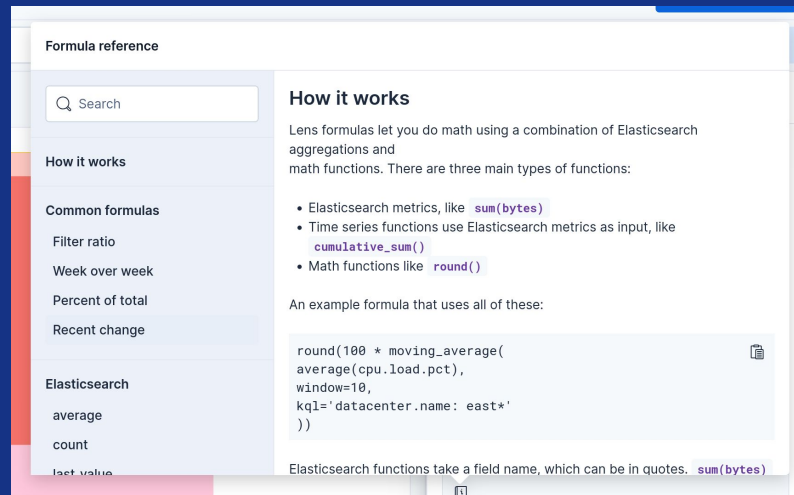
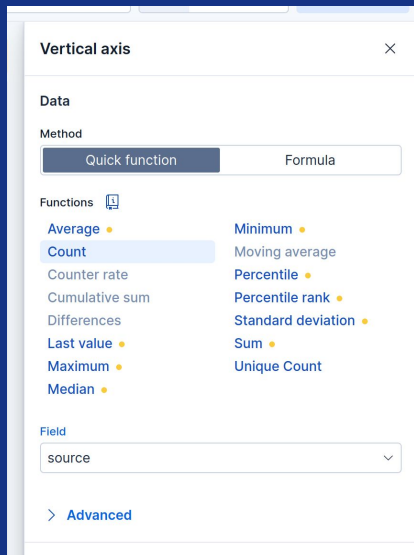
Lens

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



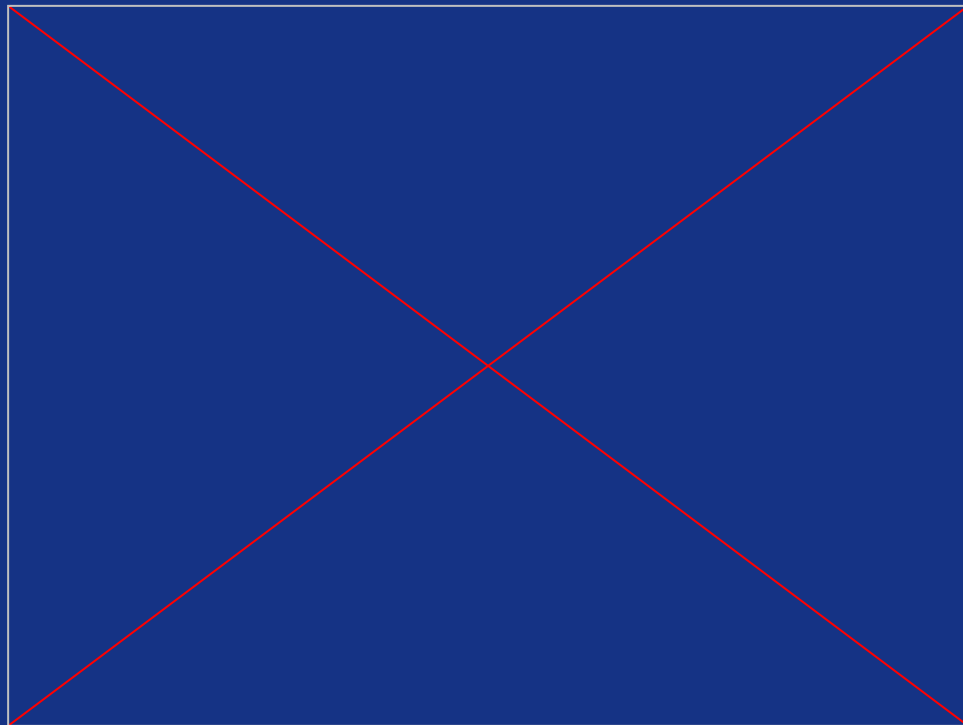
Lens

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



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.

The screenshot displays the ES|QL visualization interface. At the top, there are tabs for 'as', 'Switch to view mode', 'Reset', and 'Save'. The main area is divided into three sections: a map, a summary card, and a chart.

Map: Shows a map of Southeast Asia with labels for INDONESIA, PAPUA NEW GUINEA, and AUSTRALIA. The zoom level is 1.56.

Summary Card: Titled 'Places', it shows a count of 451,323 and an average of 77.0%.

Chart: A 'Bar vertical stacked' chart titled 'count by dataset'. The y-axis is labeled 'source' and the x-axis is labeled 'count by dataset'. The chart shows three bars for 'meta', 'Microsoft', and 'PinMeTo'. The 'meta' bar is the largest, followed by 'Microsoft' and 'PinMeTo'. The bars are stacked with different colors: teal for 'meta', light blue for 'Microsoft', and pink for 'PinMeTo'. A legend on the right side of the chart identifies the colors: teal for 'meta', light blue for 'Microsoft', pink for 'PinMeTo', and a small red dot for 'bosnia', a small blue dot for 'capetown', a small green dot for 'valencia', a small orange dot for 'betem', and a small purple dot for 'victoria'.

ES|QL Query Results: The query is displayed in the top right panel:

```
1 FROM places-* METADATA _index
2 | STATS count = COUNT(source)
3 BY source, _index
4 | EVAL dataset = REPLACE(_index,
5 | KEEP count, source, dataset
```

The results show 6 lines and a limit of 1000.

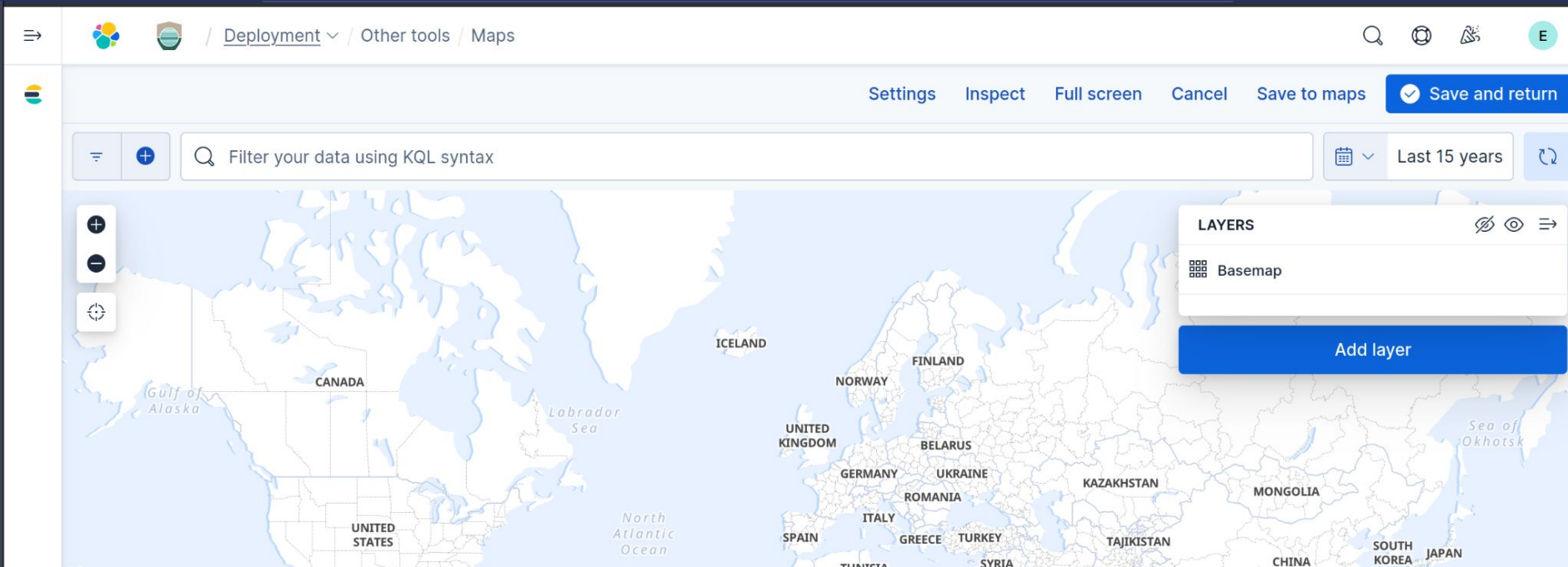
Visualization configuration: The configuration panel on the right allows setting the chart type to 'Bar' and the visualization to 'Stacked'. The vertical axis is set to 'source' and the horizontal axis is set to 'count'. A breakdown is shown for the 'dataset' field, with a color-coded bar representing the distribution of the dataset.

Suggestions: The bottom right panel shows suggestions for the visualization, including 'Cancel' and 'Apply and close' buttons.

Elastic Maps

Interface

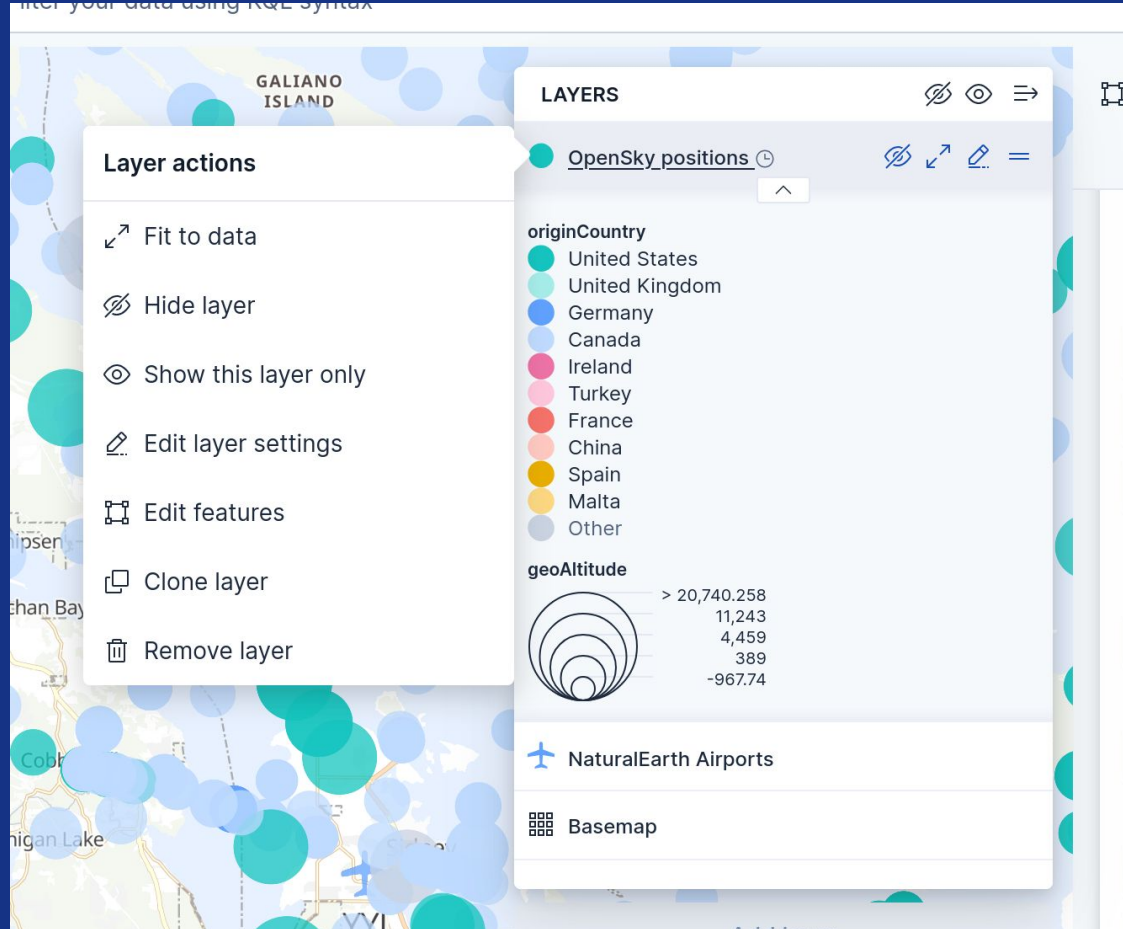
Same elements as in Lens, Dashboards, etc.



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

Settings

Custom icons

Add a custom icon that can be used in layers in this map.

[+ Add](#)

Display

Background color

☒ TRANSPARENT

☐ Show scale

Navigation

☐ Auto fit map to data bounds

Zoom range

0

→

24

Initial map location

☒ Map location at save

☐ Auto fit map to data bounds

☐ Fixed location

☐ Browser location

Spatial filters

☒ Show spatial filters on map

Opacity



30

%

Fill color

#DA8B45

Border color

#DA8B45

Layer inspect

See the queries to Elasticsearch in detail

Inspector

2 requests were made

Request

Statistics

Hits

Data view

Data view II

Query time

Request time

Inspector

2 requests were made

Request

Statistics

Clusters and shards

Request

Response

Inspector

2 requests were made

Request

Statistics

Clusters and shards

Request

Response

load layer features (Overturemaps Places)

✓ 200ms

Copy to clipboard

```
{
  "isPartial": false,
  "isRunning": false,
  "rawResponse": {
    "took": 7,
    "timed_out": false,
    "_shards": {
      "total": 7,
      "successful": 7,
      "skipped": 0
    }
  }
}
```

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

Add layer

All Elasticsearch Reference Solutions



EMS Boundaries

Administrative boundaries from Elastic Maps Service



EMS Basemaps

Basemap service from Elastic Maps Service



Tile Map Service

Raster image tile map service using {z}/{x}/{y} url pattern.



Web Map Service

Maps from OGC Standard WMS



Vector tiles

Data service implementing the Mapbox vector tile specification

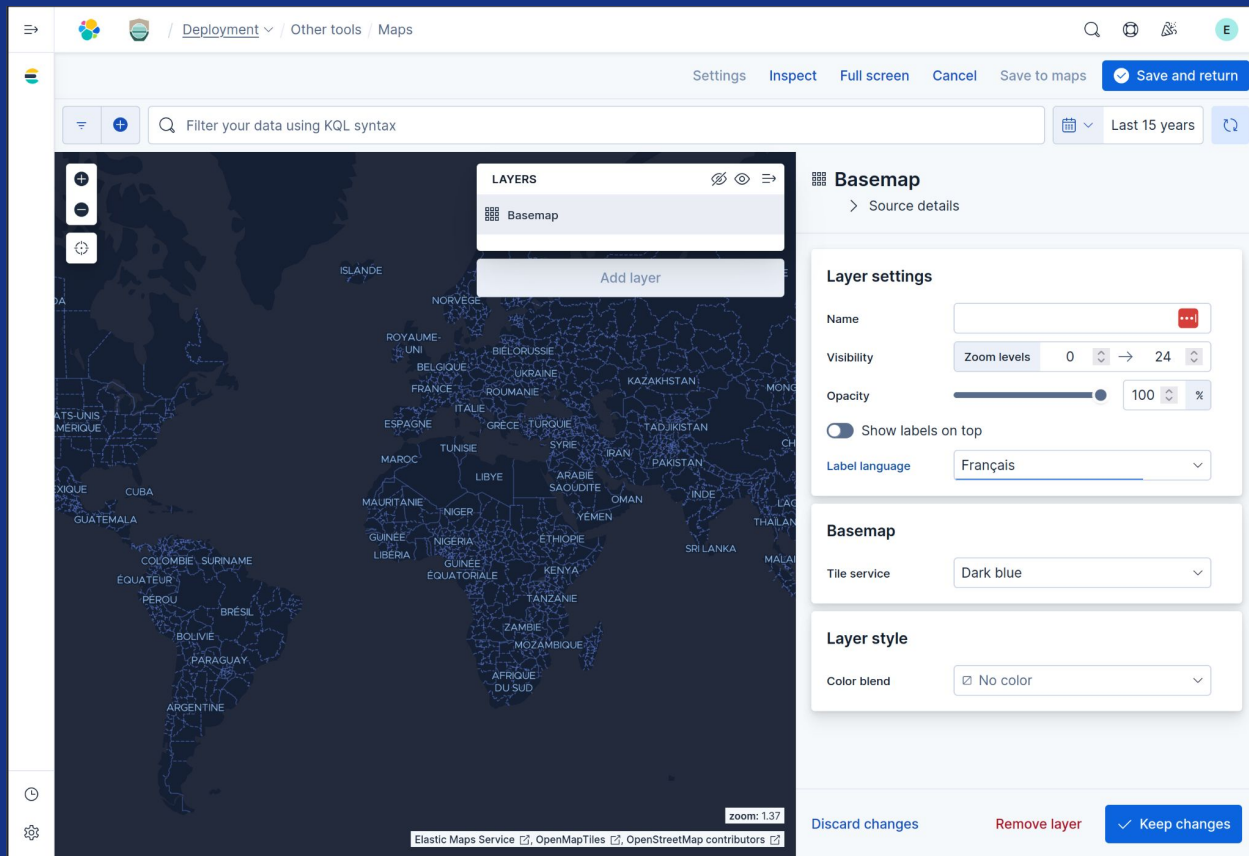
EMS Basemaps

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

Add layer

AllElasticsearchReferenceSolutions

TECHNICAL PREVIEW

**Documents**
Points, lines, and polygons from Elasticsearch

**ES|QL**
Create a layer using the Elasticsearch Query Language

**Choropleth**
Shade areas to compare statistics across boundaries

**Spatial join**
Group documents by geospatial relationships

**Clusters**
Group documents into grids and hexagons

**Heat map**
Group documents in grids to show density

**Top hits per entity**
Display the most relevant documents per entity, e.g. the most recent GPS hits per vehicle.

**Tracks**
Create lines from points

**Point to point**
Aggregated data paths between the source and destination

TECHNICAL PREVIEW

**Create index**
Draw shapes on the map and index in Elasticsearch

Documents

Render individual documents

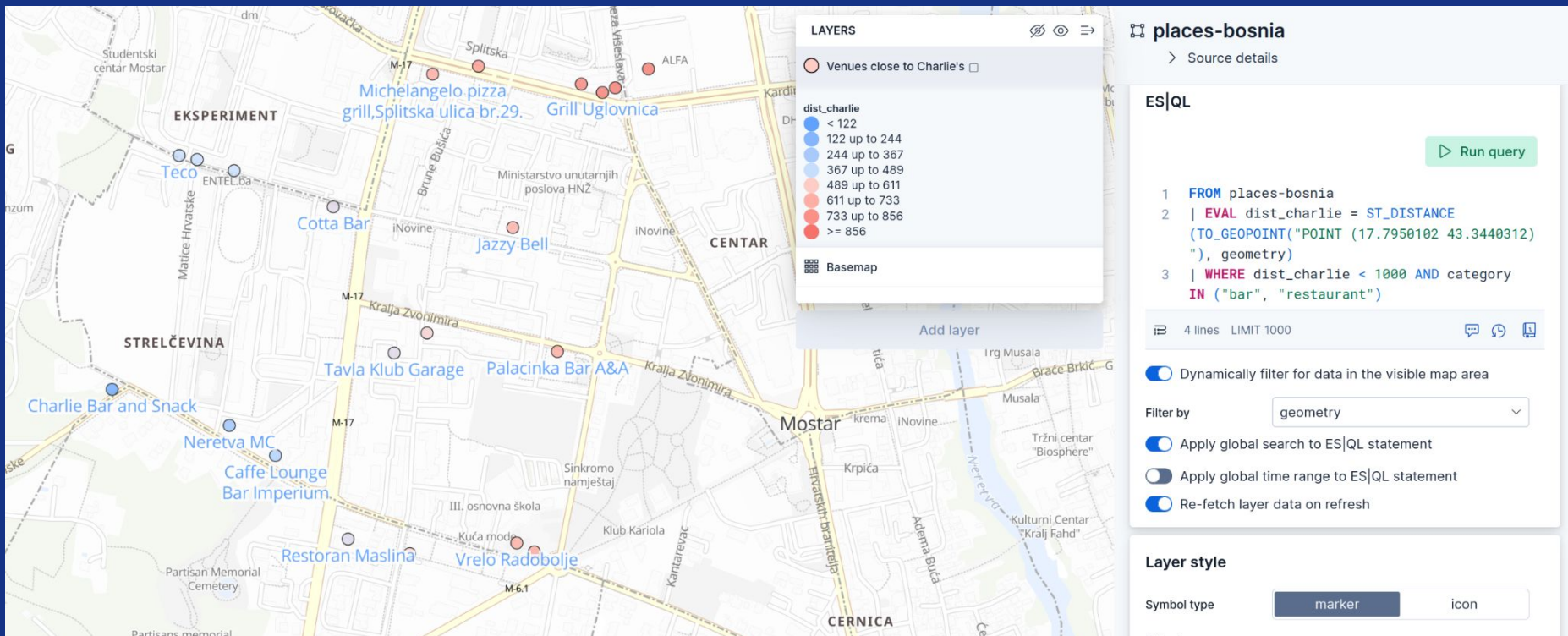
- Zoom based visibility and Opacity
- Select fields for tooltips
- Sort by a field
- Scaling:
 - Vector tiles
 - First 10K documents
 - Automatically cluster > 10K
- Join with another index
- Styling
 - Symbol, sizes, colors, label

The screenshot displays the Mapbox Studio configuration interface for a layer named "Positions". The interface is divided into several sections:

- Positions**
 - > Source details
- Layer settings**
 - Name: Positions
 - Visibility: Zoom levels 0 → 7
 - Opacity: Slider set to 7
 - Attribution: Add attribution
 - Include layer in fit to data bounds computation: ☒
 - Show tooltips: ☒
- Tooltip fields**
 - callsign
 - icao24
 - onGround
 - originCountry
 - + Add
- Sorting**
 - Field: Select sort field
 - Order: descending
- Scaling**
 - ☒ Use vector tiles
 - ☐ Show clusters when results exceed 10,000
 - ☐ Limit results to 10,000
- Filtering**
 - + Set filter Add a filter to narrow down results
 - ☒ Apply global search to layer data
 - ☒ Apply global time to layer data
 - ☒ Re-fetch layer data on refresh
- Joins**
 - Join with terms from iso_a2
 - where -- add filter --
 - ☒ Apply global search to join
 - + Add spatial join
- Layer style**
 - Symbol type: marker icon
 - Fill color: By value originCountry
 - Other: #CAD3E2
 - Data mapping
 - Border color: Solid
 - Border width: Fixed 0 px
 - Symbol size: By value geoAltitude
 - Reverse size: ☐
 - Data mapping
 - Label: Fixed symbol label
 - Label position: Center
 - Label visibility: ☒ Use layer visibility
 - Label color: Solid
 - Label size: Fixed
 - Label border color: Solid
 - Label border width: Small
 - ☒ Apply global time to style metadata requests

ES|QL

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



Clusters

Rendering big data

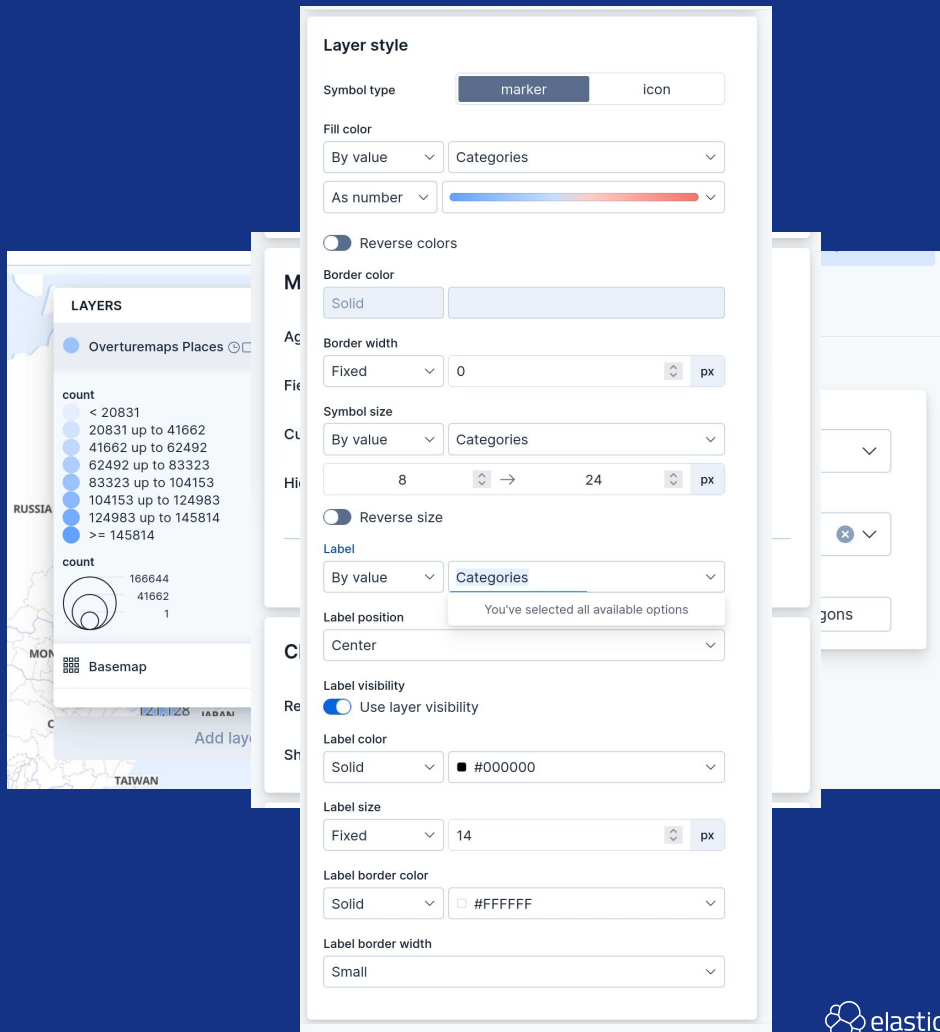
Aggregate into:

- 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



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

The screenshot displays the Mapbox Studio interface for configuring a choropleth layer. The 'Add layer' dialog is open, showing the 'Boundaries source' set to 'Administrative boundaries from the Elastic Maps Service' and the 'Join field' set to 'ISO 3166-1 alpha-2 code'. The 'Statistics source' is set to 'OpenSky positions' and the 'Join field' is set to 'country.iso_a2'. A data table for 'World Countries' is shown, listing various metrics for different countries. The 'Joins' panel is also visible, showing the configuration for joining data from 'country.iso_a2' and applying filters.

Add layer

< Change layer

Boundaries source

☒ Administrative boundaries from the Elastic Maps Service
☐ Points, lines, and polygons from Elasticsearch

EMS boundaries

World Countries

Join field

ISO 3166-1 alpha-2 code

Statistics source

Data view

OpenSky positions

Join field

country.iso_a2

World Countries

Source details

Joins

Join with terms from country.iso_a2

and use metric count where -- add filter --

☒ Apply global search to join
☒ Apply global time to join

Join with terms from country.iso_a2

and use metric avg velocity

where onGround : false

☒ Apply global search to join
☒ Apply global time to join

+ Add spatial join + Add term join

Layer style

Fill color

ISO 3166-1 alpha-2	code	count of OpenSky positions	average velocity
CN		1,434	202.898
US		1,434	202.898
IN		1,434	202.898
BR		1,434	202.898
RU		1,434	202.898
JP		1,434	202.898
GB		1,434	202.898
FR		1,434	202.898
DE		1,434	202.898
IT		1,434	202.898
ES		1,434	202.898
PT		1,434	202.898
GR		1,434	202.898
TR		1,434	202.898
PL		1,434	202.898
CZ		1,434	202.898
SK		1,434	202.898
HR		1,434	202.898
SI		1,434	202.898
RO		1,434	202.898
BG		1,434	202.898
MD		1,434	202.898
UA		1,434	202.898
BY		1,434	202.898
BE		1,434	202.898
NL		1,434	202.898
SE		1,434	202.898
NO		1,434	202.898
DK		1,434	202.898
FI		1,434	202.898
IS		1,434	202.898
EE		1,434	202.898
LV		1,434	202.898
LT		1,434	202.898
RU		1,434	202.898
UA		1,434	202.898
BY		1,434	202.898
BE		1,434	202.898
NL		1,434	202.898
SE		1,434	202.898
NO		1,434	202.898
DK		1,434	202.898
FI		1,434	202.898
IS		1,434	202.898
EE		1,434	202.898
LV		1,434	202.898
LT		1,434	202.898

Other types

→ **Add layer**

< Change layer

Layer features source

Data view
OpenSky positions

Geospatial field
location

Join source

Relationship
within 15 km of layer features

Data view
NaturalEarth Airports

Geospatial field
coords

Spatial Join

Add layer

< Change layer

Data view
OpenSky positions

Geospatial field
location

Entity
callsign.keyword

Documents per entity
1 100 1

Sort field
timePosition

Sort order
descending

Top hits per entity

Add layer

< Change layer

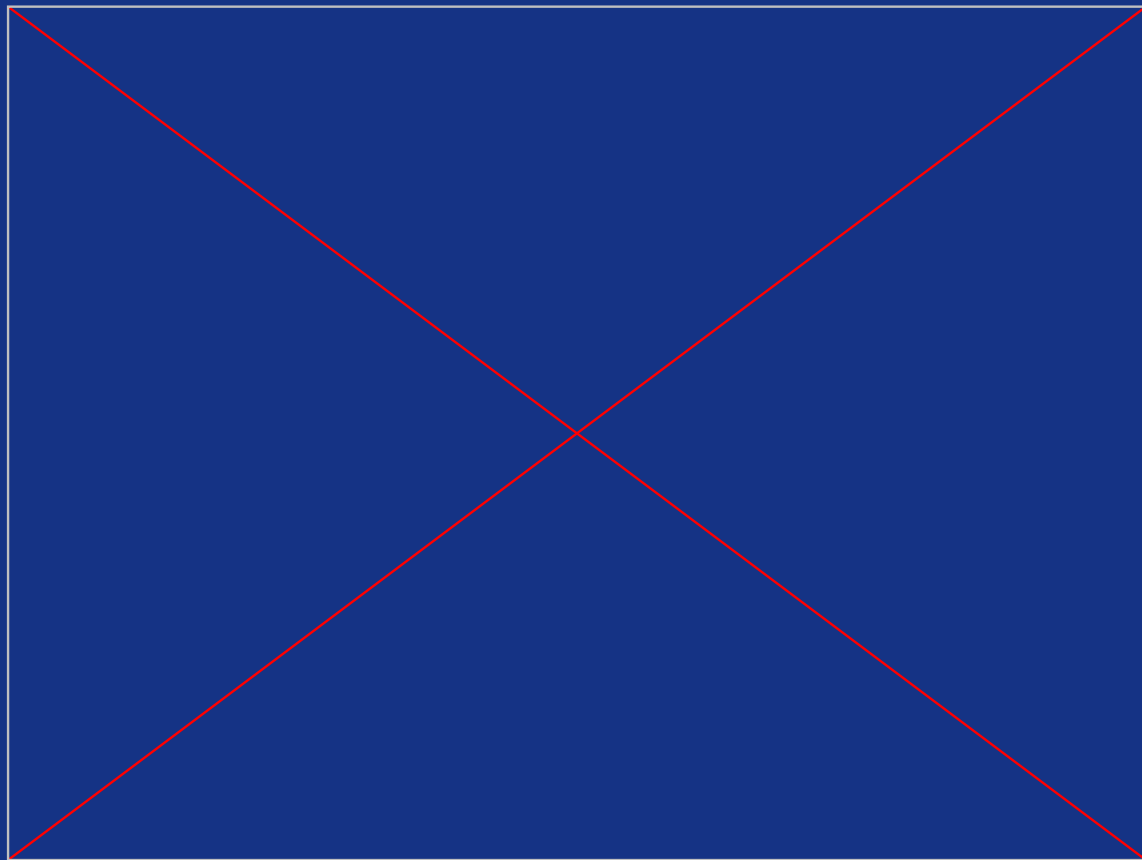
Data view
Kibana Sample Data Flights

Source
OriginLocation

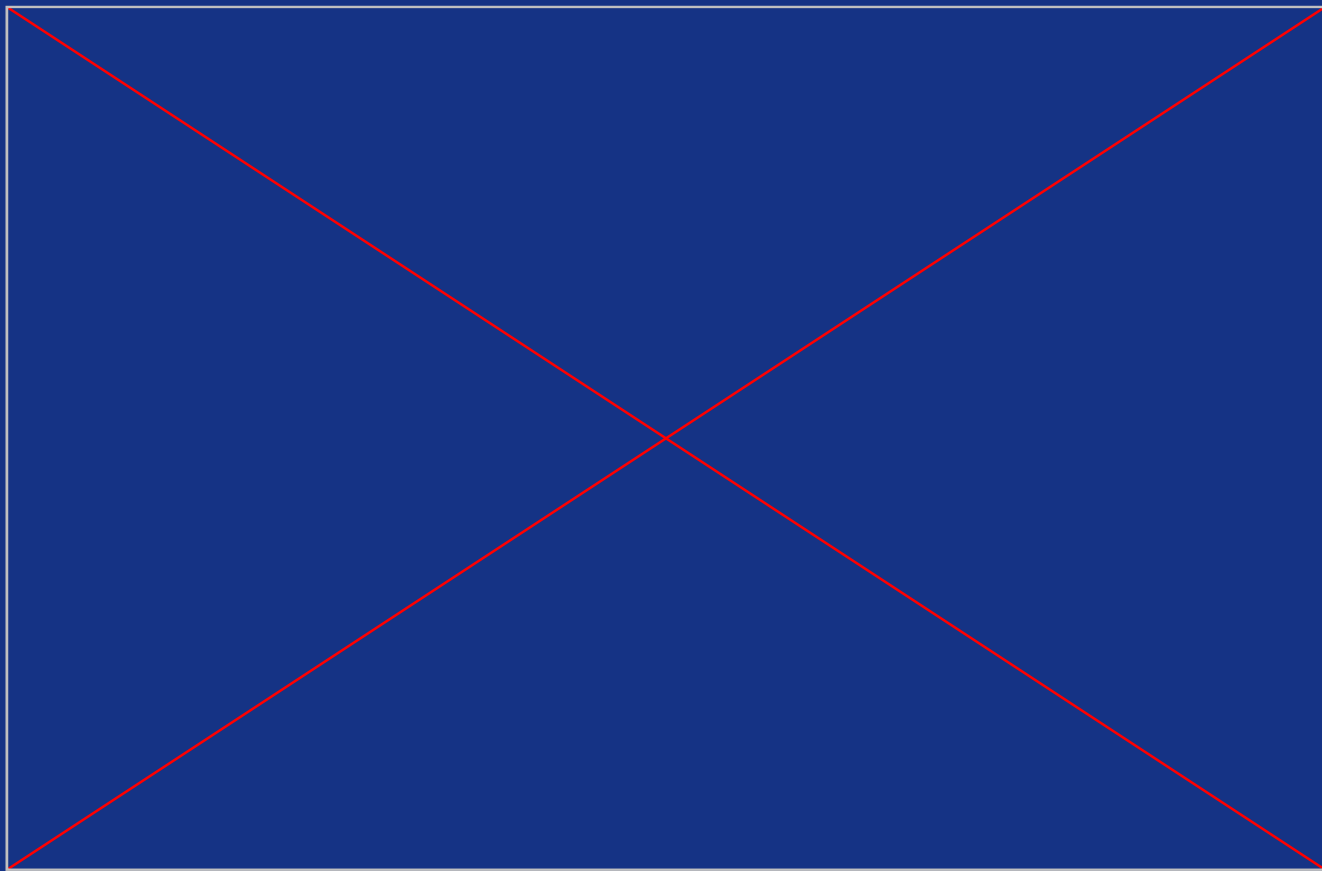
Destination
DestLocation

Point to point

Maps in dashboards: filters



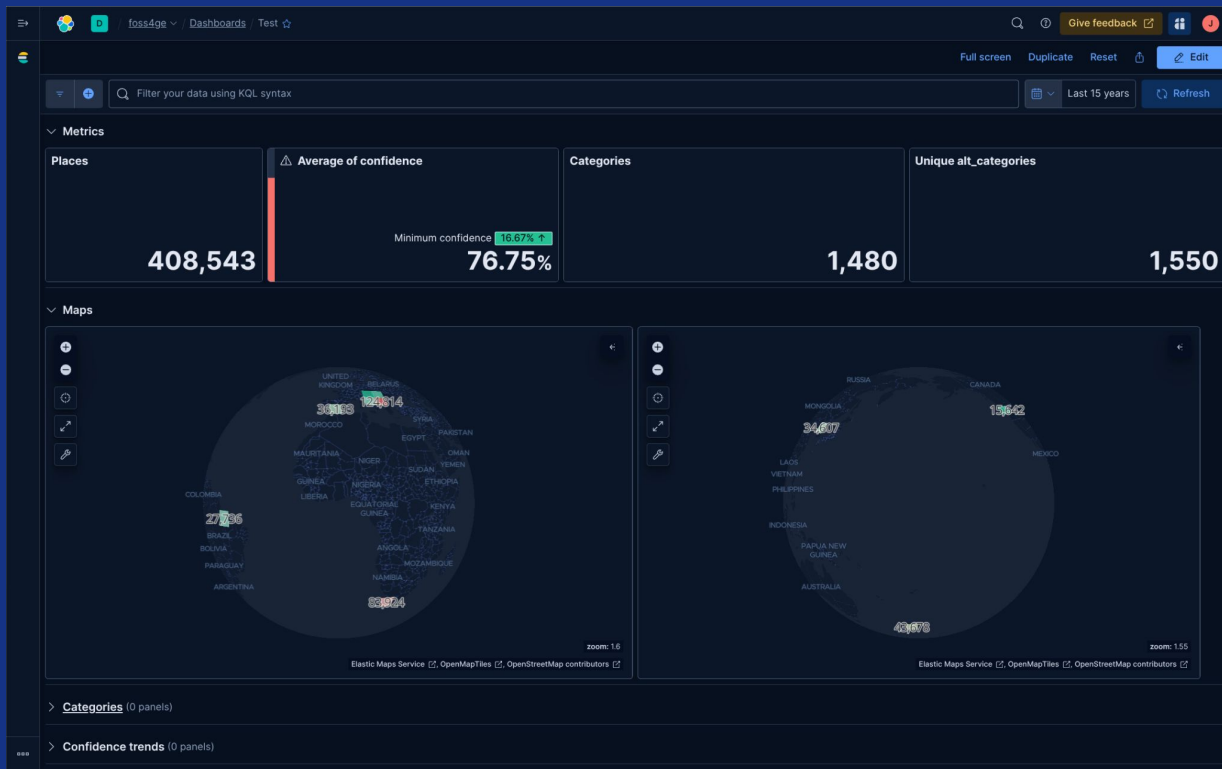
Maps in dashboards: synchronized extents



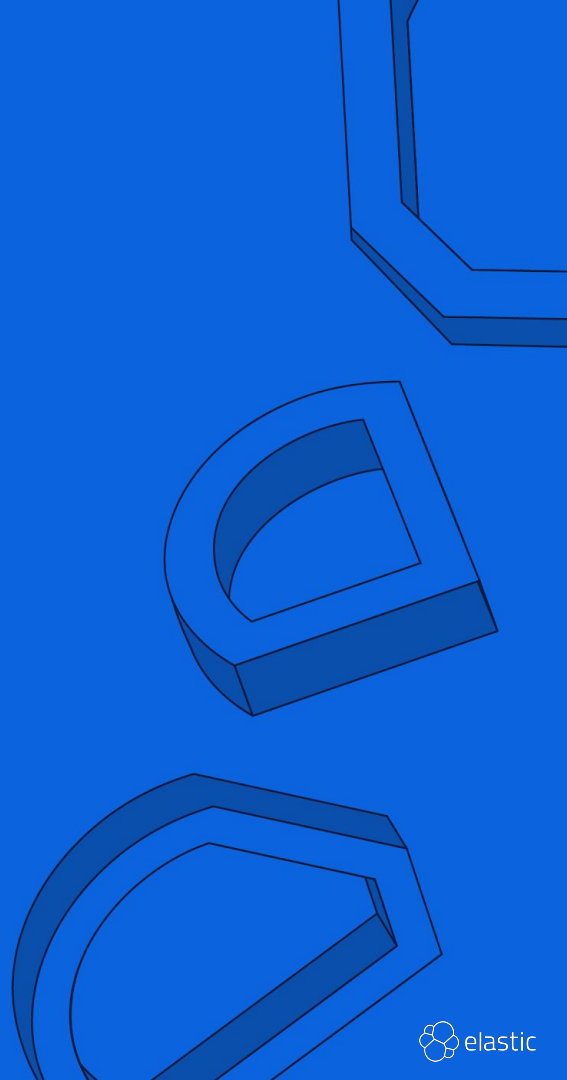
What's new in 9.1?

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>

