

VISUALIZACIONES Y DASHBOARDS

KIBANA





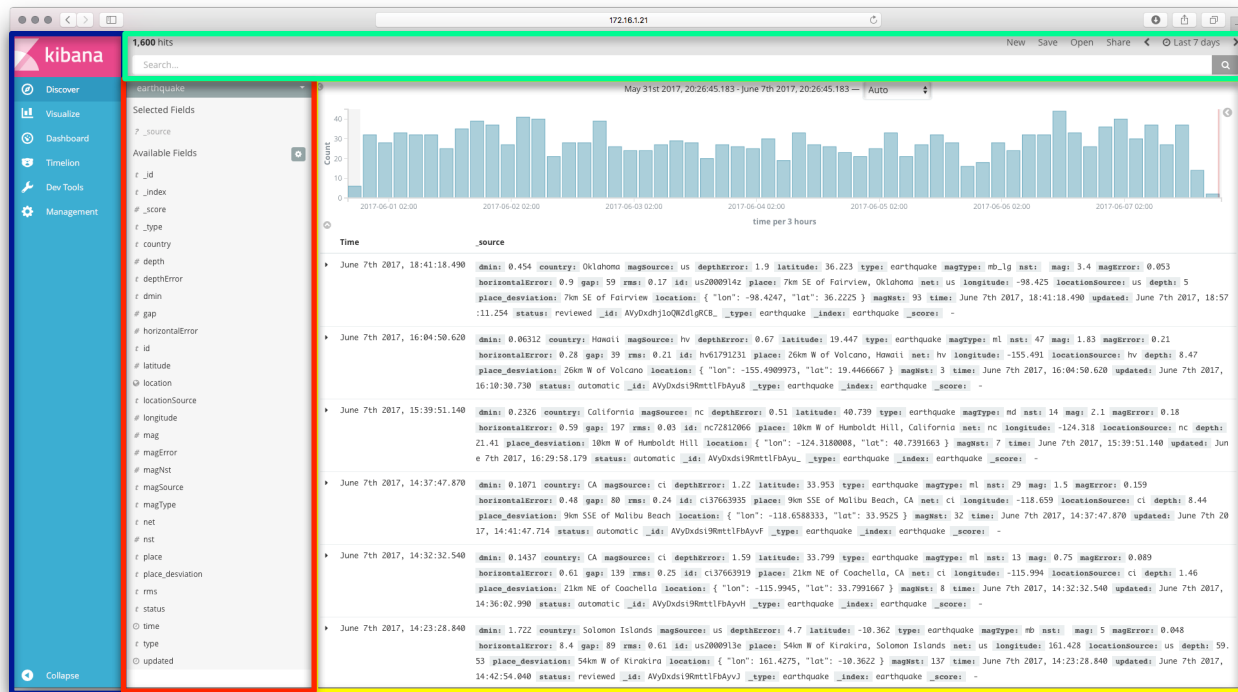
1.

DISCOVER

KIBANA

Opciones y filtrado

Menu



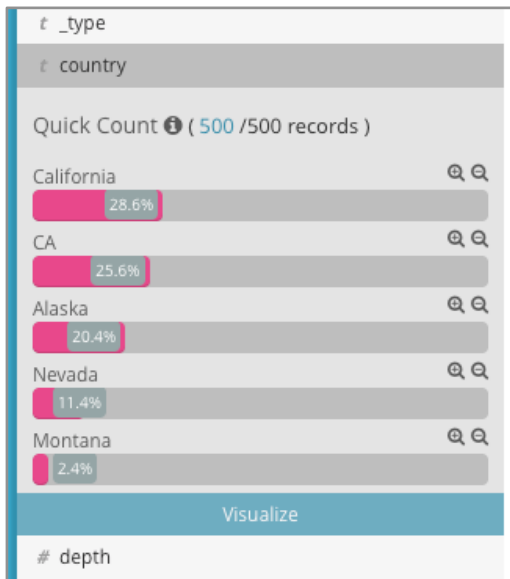
Campos

Logs en bruto

KIBANA. DISCOVER

Campos

- Lista de los campos disponibles según el filtro aplicado.
- Top 5 por campo.
- Enlaces directos al filtrado y a las visualizaciones.



KIBANA. DISCOVER

Logs en bruto

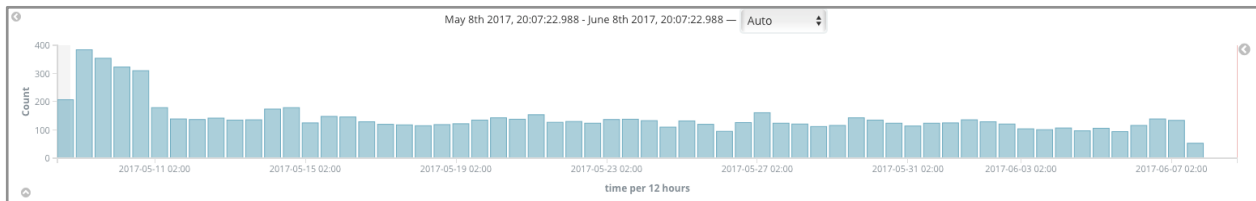
- Logs desplegados con sus respectivos campos.
- Se puede filtrar por cada campo usando: 🔍 🔍
- Buena forma de analizar logs por detalle o buscar anomalías.

Time	_source
June 7th 2017, 18:41:18.490	<pre>dmin: 0.454 country: Oklahoma magSource: gap: 59 rms: 0.17 id: us2000914z place: location: { "lon": -98.4247, "lat": 36.2225 _type: earthquake _index: earthquake _scor</pre>
Table	JSON
🔍 _id	AVyDxdhj1oQWZdlgRCB_
🔍 _index	earthquake
# _score	-
🔍 _type	earthquake
🔍 country	Oklahoma
# depth	5
🔍 depthError	1.9
🔍 dmin	0.454
# gap	59
# horizontalError	0.9
🔍 id	us2000914z
# latitude	36.223
🔍 location	{ "lon": -98.4247, "lat": 36.2225 }

KIBANA. DISCOVER

Eventos en el tiempo

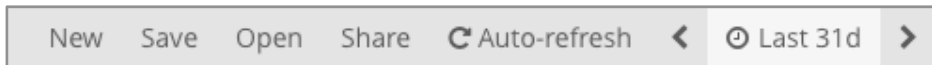
- Muestra la cantidad de eventos en el tiempo.
- Se puede filtrar seleccionando una zona.
- Se identifican anomalías con picos o claros.



KIBANA. DISCOVER

Opciones

- ***New/Save/Open***: Interacción con búsquedas.
- ***Share***: Compartir la visualización.
- ***Auto-refresh***: Refresco automático de los datos.
- ***Intervalo de tiempo***: En el que mostrar los datos.
Permite hacer intervalos *rápidos* (1 hora, 1 día, 1 semana...), *relativos* (desde hace x días/semanas...) o *absoluto* (intervalo de fecha y hora exacta).



KIBANA. DISCOVER

Cantidad de eventos y filtro

- En la esquina superior izquierda: número de eventos que casan con el filtrado y tiempo.
- Búsqueda: Consulta a realizar sobre los datos. Se puede realizar más de un filtrado.

A screenshot of the Kibana Discover search bar. It consists of a light gray rectangular box. The top half of the box has a slightly darker gray background and contains the text "7,865 hits" in a dark gray font. The bottom half of the box is white and contains a search input field with the placeholder text "Search..." in a light gray font.

7,865 hits

Search...



2.

BÚSQUEDAS

KIBANA. BÚSQUEDAS

Búsquedas **básicas**: *campo:valor*
country:“Alaska”

Búsquedas **AND**: *campo1:valor1 AND campo2:valor2*
type:“quarry blast” AND country:“Mexico”

Búsquedas **OR**: *campo1:valor1 OR campo2:valor2*
type:“quarry blast” OR type:“explosion”

KIBANA. BÚSQUEDAS

Búsquedas **negadas**: *!campo:valor*
!country:California

Búsquedas **numéricas**: *campo:[>|<]valor*
mag:>6

Búsquedas **expresiones regulares**: *campo:*valor**
*place:*Alaska*



3.

VISUALIZACIONES

VISUALIZACIONES

Select visualization type

Basic Charts



Area



Heat Map



Horizontal Bar



Line



Pie



Vertical Bar

Data



Data Table

1,234

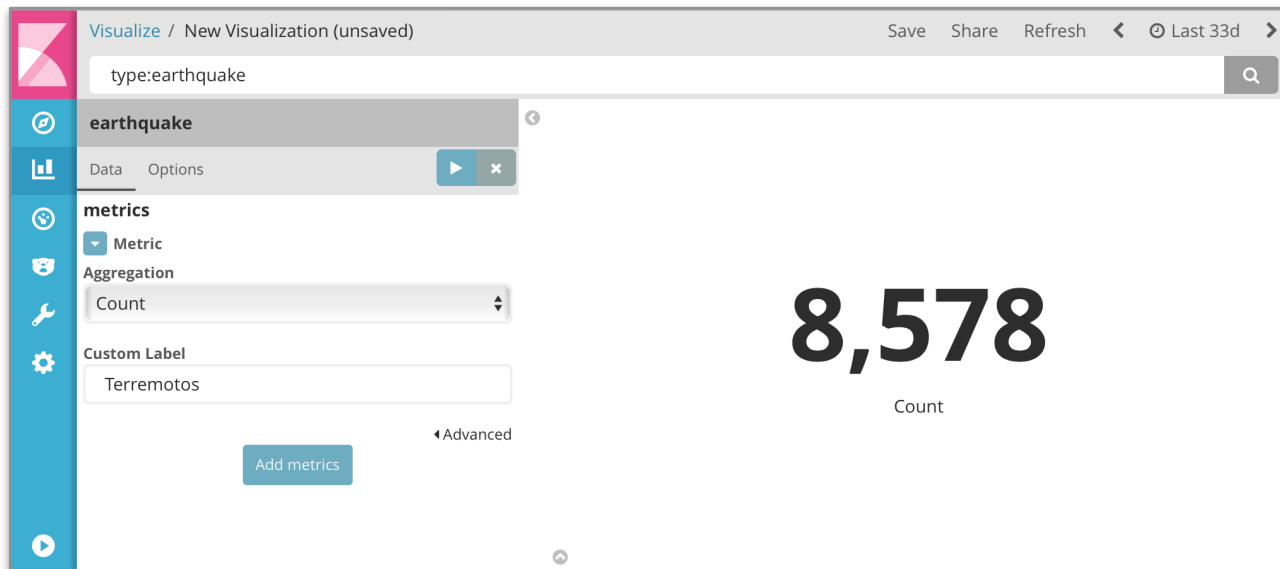
Metric

Maps

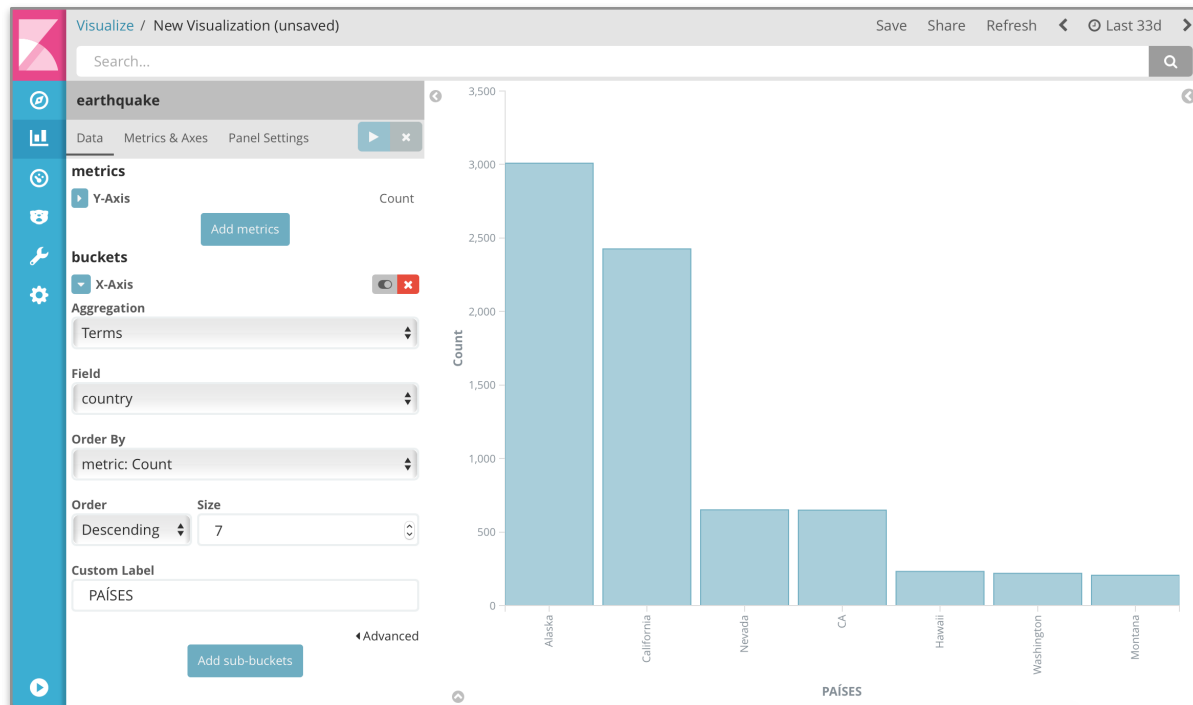


Tile Map

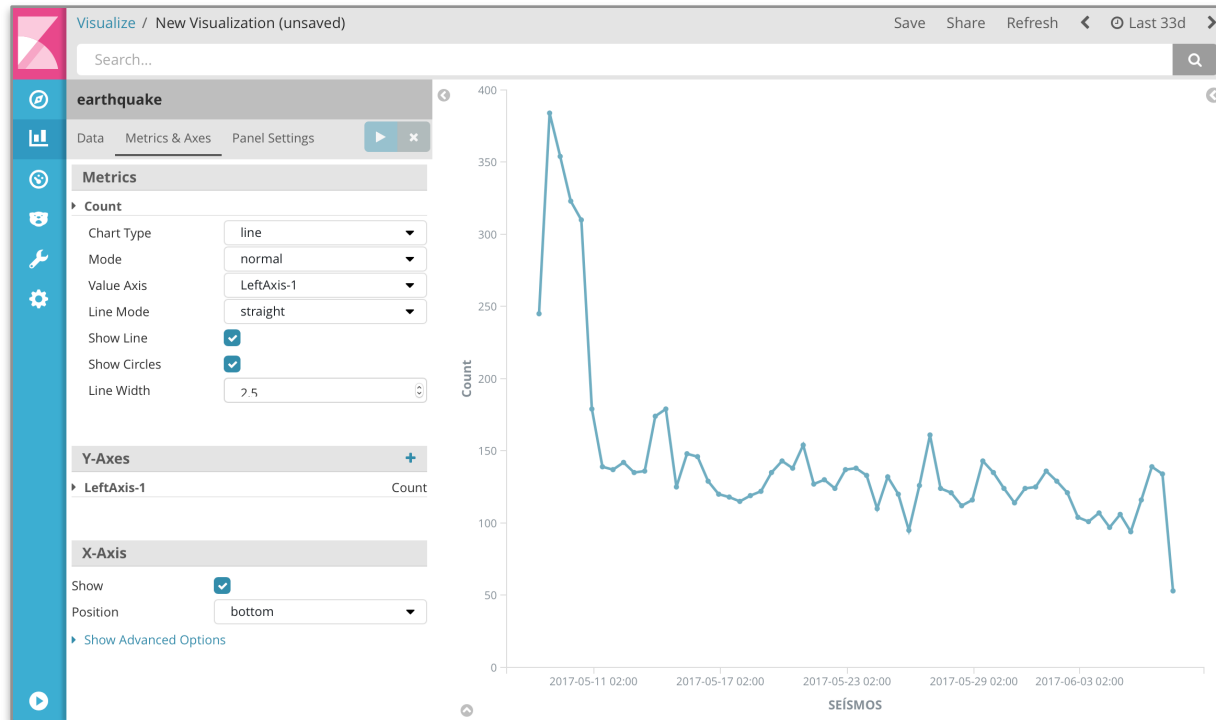
VISUALIZACIONES METRICS



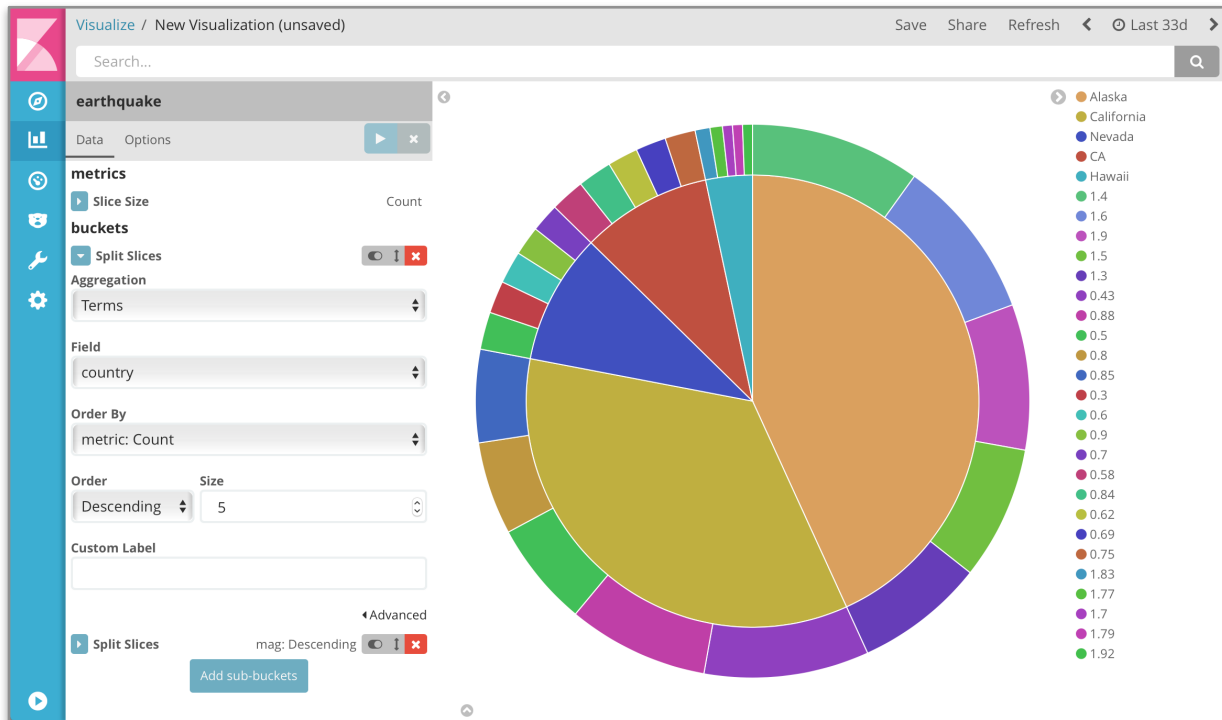
VISUALIZACIONES BARRAS



VISUALIZACIONES LÍNEAS



VISUALIZACIONES TARTAS



VISUALIZACIONES TABLAS

Visualize / New Visualization (unsaved) Save Share Refresh Last 33d

Search...

earthquake

Data Options

metrics

Metric

Count

Add metrics

buckets

Split Rows

place: Descending

Split Rows

Sub Aggregation

Terms

Field

mag

Order By

metric: SEÍSMOS

Order

Descending

Size

5

Custom Label

MAGNITUD

Add sub-buckets

Advanced

LUGAR

MAGNITUD

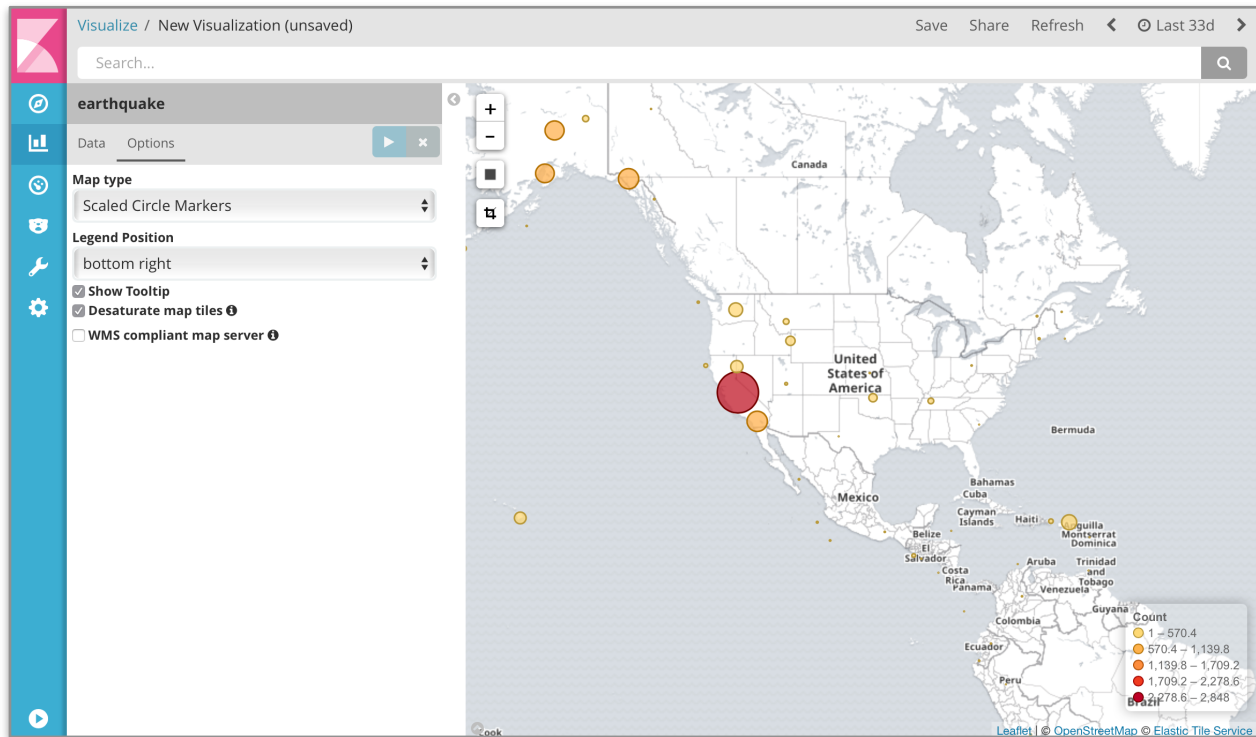
SEÍSMOS

6km NW of The Geysers, California	0.43	13
6km NW of The Geysers, California	0.88	10
6km NW of The Geysers, California	0.69	7
6km NW of The Geysers, California	0.45	6
6km NW of The Geysers, California	0.85	5
9km NE of Aguanga, California	0.33	3
9km NE of Aguanga, California	0.48	3
9km NE of Aguanga, California	0.55	3
9km NE of Aguanga, California	0.6	3
9km NE of Aguanga, California	0.31	2

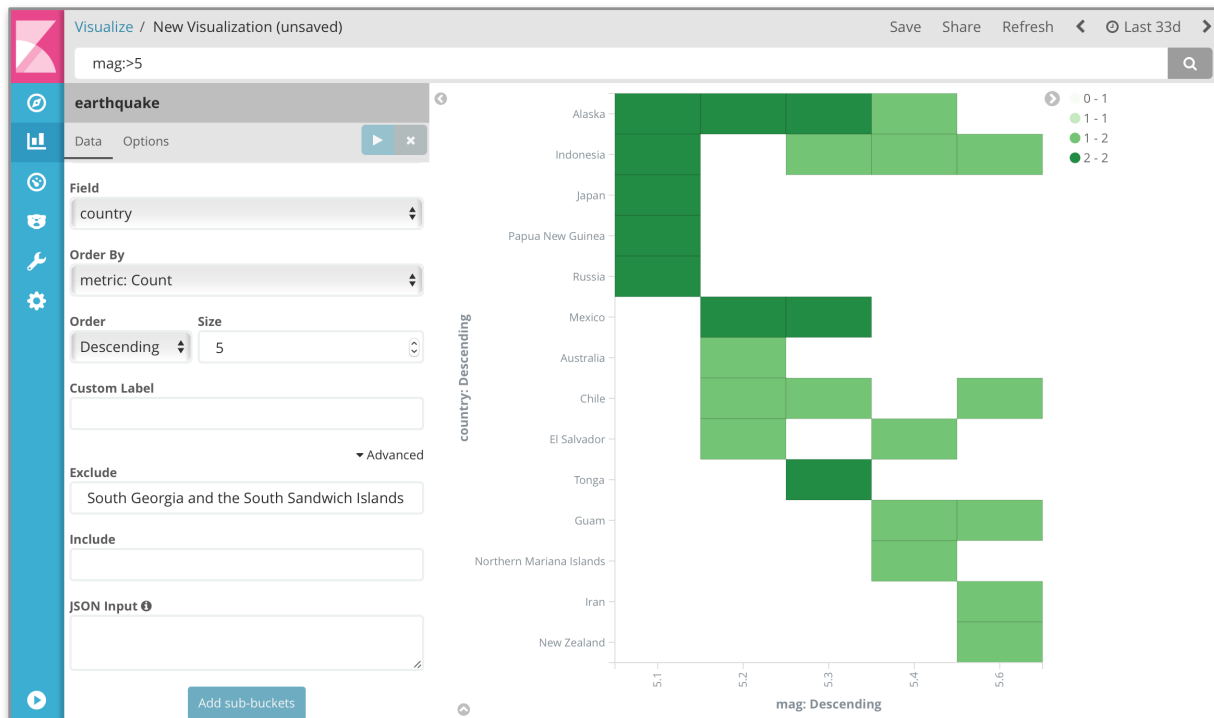
Export: Raw Formatted

1 2 3 »

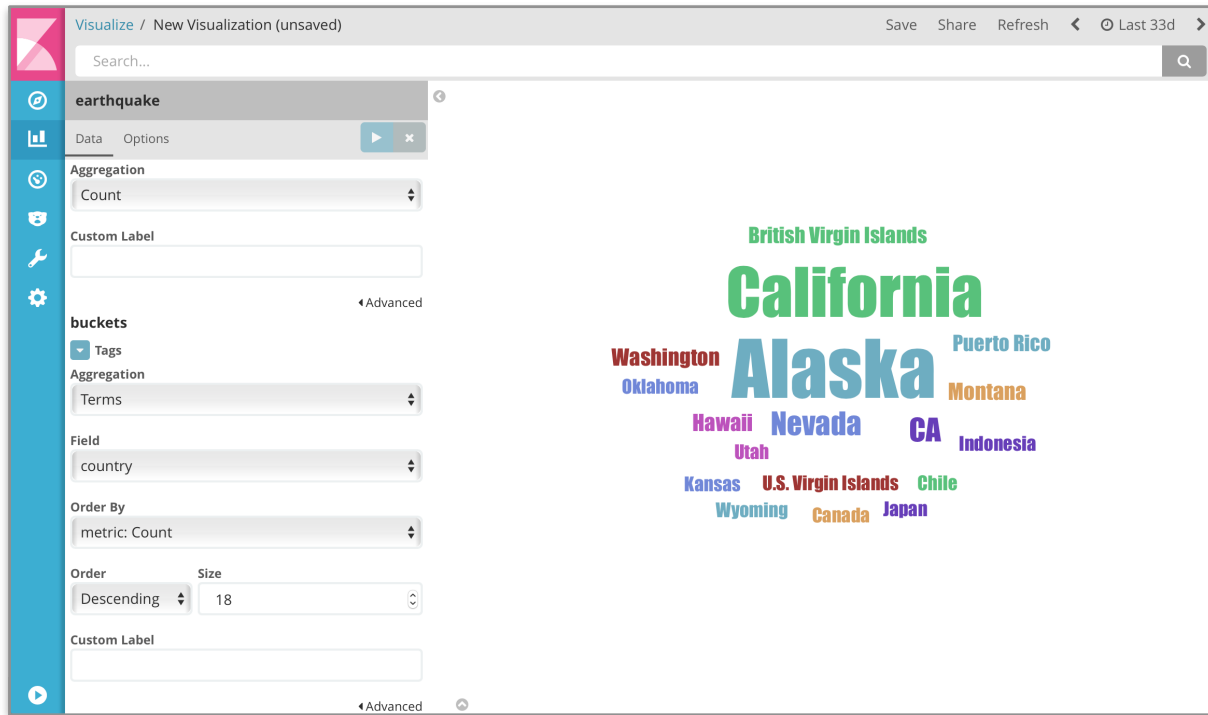
VISUALIZACIONES GEOLOCALIZACIÓN



VISUALIZACIONES MAPAS DE CALOR



VISUALIZACIONES NUBE DE PALABRAS

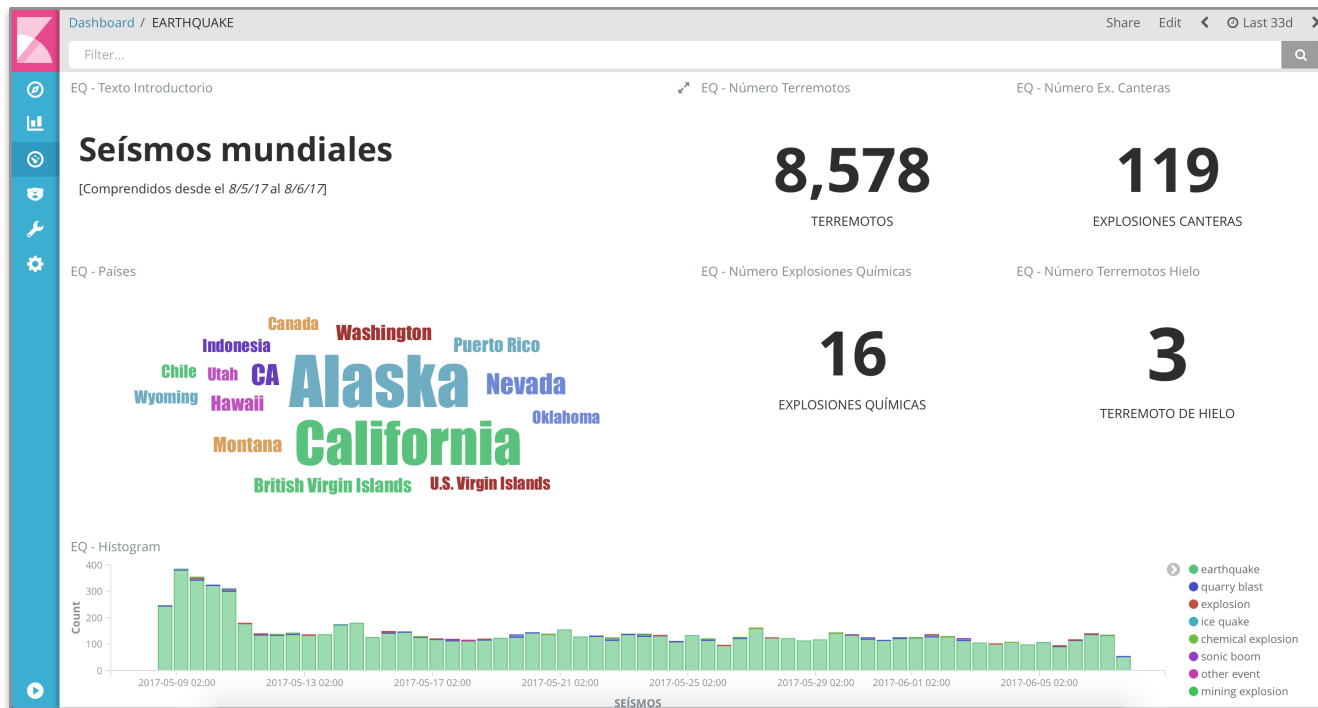




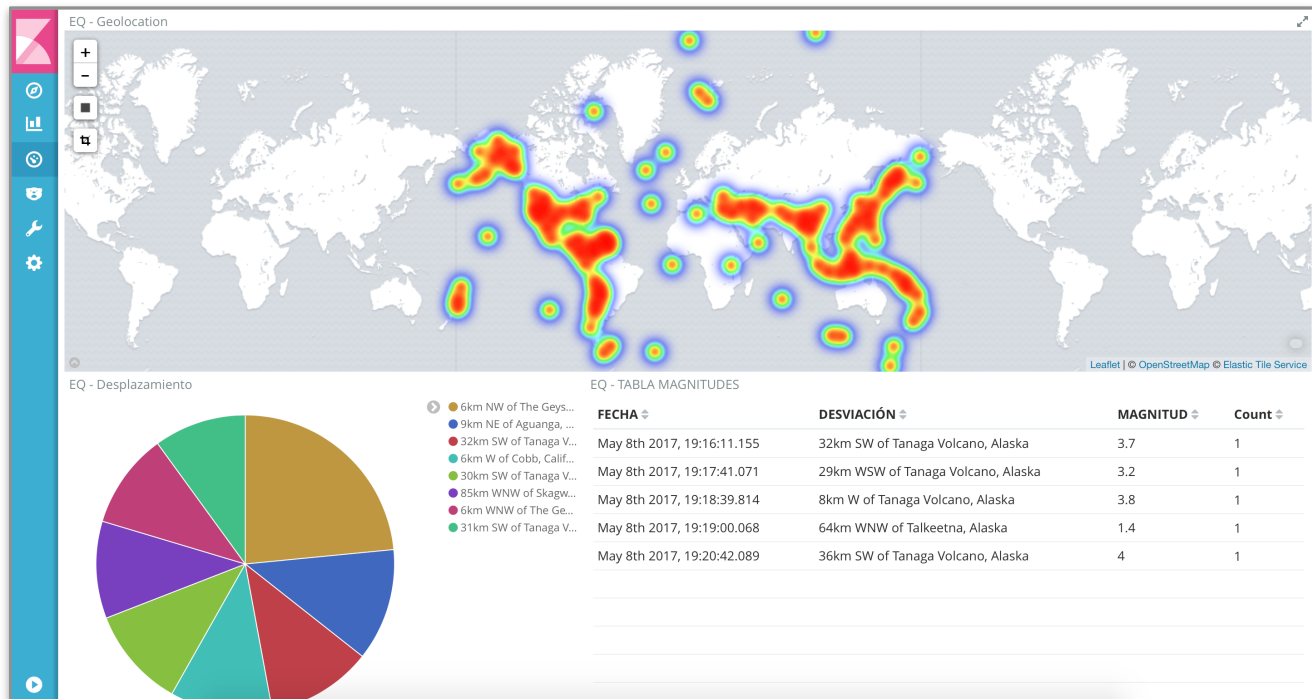
4.

DASHBOARDS

DASHBOARDS



DASHBOARDS





5.

DEV TOOLS

DEV TOOLS

Interfaz de Usuario para interactuar con la **REST API** de Elasticsearch. Dividida en dos áreas:

- Editor: donde se realizan las consultas.
- Panel de respuestas: donde se recibe la información devuelta por elasticsearch

Más cómodo que realizar las consultas con CURL.

DEV TOOLS





6.

MANAGEMENT

MANAGEMENT

Panel de **configuración** y administración de distintas características de Elasticsearch.

- ***Index Patterns***: Plantillas que siguen los índices cuando de indexa la información (formato, tipo de datos...)
- ***Saved Objects***: Dashboards, visualizaciones y búsquedas creadas.
- ***Advanced Settings***: parámetros de configuración avanzados de Elasticsearch

MANAGEMENT

Management / Kibana

Index Patterns

Saved Objects

Advanced Settings

+

★ twitter

earthquake

metricbeat.*

earthquake

ⓘ Configured time field: time

This page lists every field in the **earthquake** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's [Mapping API](#).

fields (34) | scripted fields (0) | source filters (0)

Q Filter

All field types ▾

name ↕	type ^	format ↕	searchable ⓘ ↕	aggregatable ⓘ ↕	analyzed ⓘ ↕	excluded ⓘ ↕	controls
_source	_source						
@timestamp	date						
time ⓘ	date		✓	✓			
updated	date		✓	✓			
location	geo_point		✓	✓			
latitude	number		✓	✓			
nst	number		✓	✓			
mag	number		✓	✓			
magError	number		✓	✓			
horizontalError	number		✓	✓			