



Primeros pasos con Kibana

Enrique V. Kortright

3 de febrero de 2021

<https://github.com/evkortright/primeros-pasos-con-kibana>

Meetup del grupo de usuarios de Elastic (EUG) de Costa Rica

Conéctese con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



<https://community.elastic.co/>

User Group Virtual:

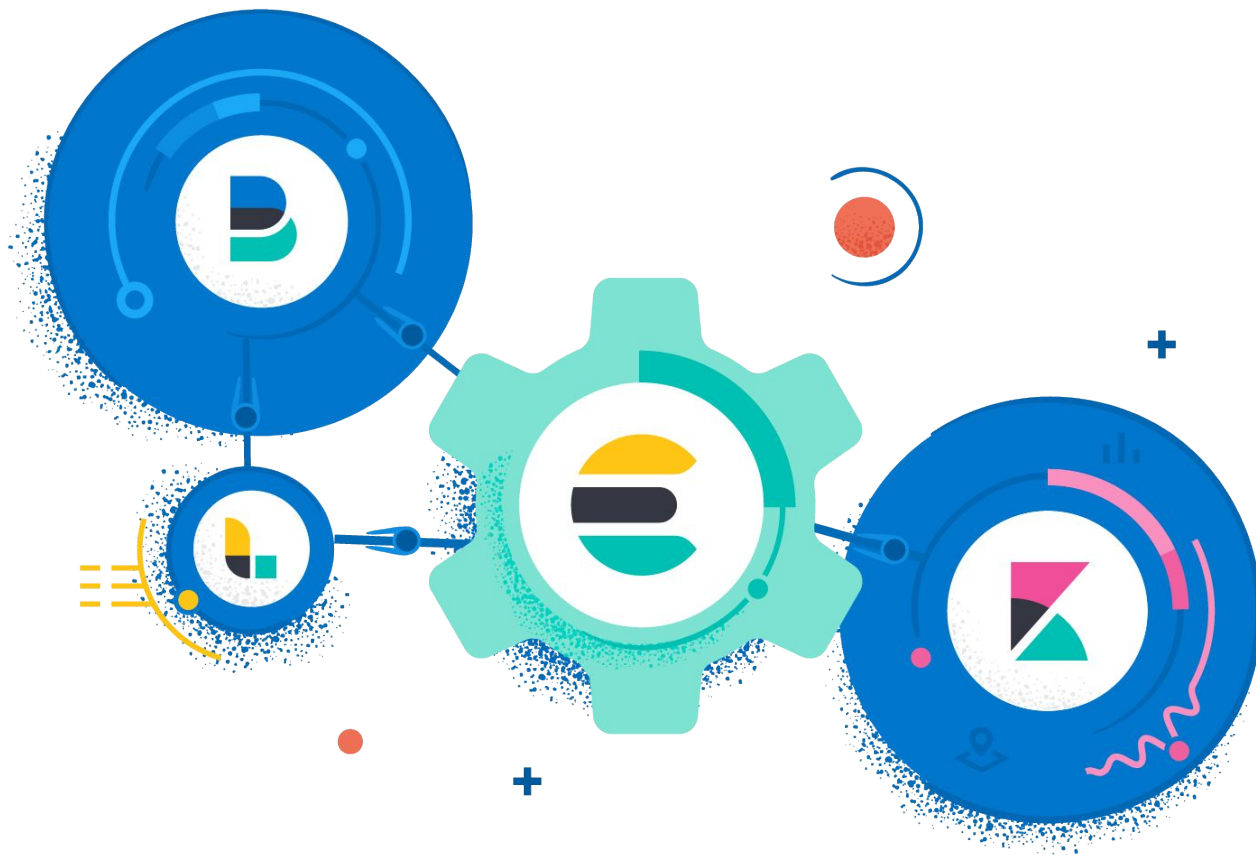


<https://community.elastic.co/amer-virtual/>

Agenda

- ¿Que es Kibana? Repaso del primer episodio
- Flujo de trabajo de un analista de datos
- Explora
- Visualiza
- Analiza
- Actua
- Preguntas y respuestas
- Episodios futuro: Logstash/Beats

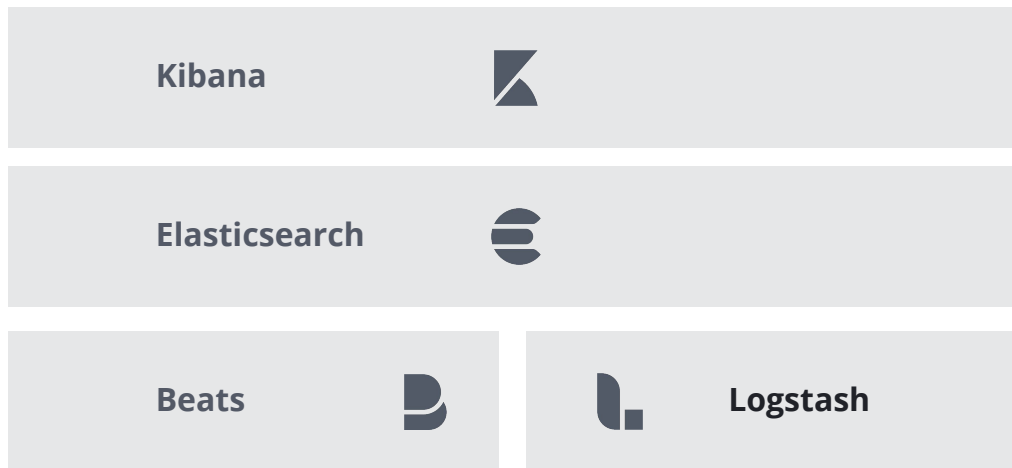
Elasticsearch es parte del Elastic Stack



El Stack de Elastic

Casos de uso

Logging	Metrics	APM	Uptime	Security Analytics	FUTURE
App Search	Site Search	Enterprise Search	Maps	Business Analytics	



Visualiza, analiza,
administra y
alerta

Guarda, busca y
procesa

Captura, enriquece,
transforma y carga

SaaS

Elastic Stack

- Elasticsearch
 - es un almacén de documentos de JSON
 - es una máquina de búsqueda de alto rendimiento
 - Maneja y procesa los datos a través de una serie de APIs de REST
- Kibana
 - es la interfaz de usuario (UI)
 - proporciona operaciones de administración y monitoreo de un cluster de Elasticsearch
 - proporciona funciones de visualización en tiempo casi-real
 - proporciona UIs para trabajos de aprendizaje de máquina
 - proporciona UIs especializadas para áreas que incluyen observabilidad, seguridad, aprendizaje de máquina, visualización de datos geoespaciales, infográficos usando Canvas, grafos de relaciones entre objetos y otras más
- Logstash
 - es la herramienta de transformación, enriquecimiento y carga de datos
 - puede jalar y empujar datos almacenados en fuentes muy diversas como bases de datos
- Beats
 - son agentes ligeros (generalmente) desplegados en el punto de origen de datos
 - se encargan de capturar logs, métricas o trazas y enviarlos a Elasticsearch directamente o a través de Logstash

- [API conventions](#)
- [cat APIs](#)
- [Cluster APIs](#)
- [Cross-cluster replication APIs](#)
- [Data stream APIs](#)
- [Document APIs](#)
- [Enrich APIs](#)
- [Graph Explore API](#)
- [Index APIs](#)
- [Index lifecycle management APIs](#)
- [Ingest APIs](#)
- [Info API](#)
- [Licensing APIs](#)
- [Machine learning anomaly detection APIs](#)
- [Machine learning data frame analytics APIs](#)
- [Migration APIs](#)
- [Reload Search Analyzers API](#)
- [Repositories Metering APIs](#)
- [Rollup APIs](#)
- [Search APIs](#)
- [Searchable snapshots APIs](#)
- [Security APIs](#)
- [Snapshot and restore APIs](#)
- [Snapshot lifecycle management APIs](#)
- [Transform APIs](#)
- [Usage API](#)
- [Watcher APIs](#)

Plan de esta serie de primeros pasos

- En el primer episodio nos enfocamos en **Elasticsearch**
 - Creación, lectura, actualización, y borrado de datos (CRUD) individualmente o a granel
 - El lenguaje de dominio específico (DSL) de Elasticsearch
 - El lenguaje de búsqueda para hacer consultas
 - Diseño de una gran experiencia de búsqueda
- En este segundo episodio vamos a explorar **Kibana**
- En el tercer episodio nos enfocamos en **Logstash y Beats**

Explora - conoce tus datos



Explora - conoce tus datos

- Tus datos estan ya en Elasticsearch
- Es hora de explorarlos y entenderlos
- Elasticsearch nos da el mapeo
 - Índice, campos y tipos de datos
- Kibana nos da un app de exploración de datos
- Sígueme en este ejercicio en el que exploramos dos de los juegos de datos que vienen incluidos en Kibana
 - Vamos a usar el app de Explore
 - Vamos a usar el lenguaje de consulta Kibana Query Language (KQL)
 - Vamos a usar filtros en donde podemos inyectar código de DSL (¿te acuerdas del DSL en nuestro primer episodio?)

Explore App

- Puntos salientes:
 - KQL es un lenguaje de expresiones booleanas
 - Tiene una función de autocompletar avanzada y completa
 - Permite explorar documentos en grupo e individualmente
 - Permite explorar cada campo y ver la distribución de valores
 - Podemos usar filtros para dividir nuestra lógica en bloques de construcción
 - Podemos guardar la búsqueda y usarla en otras apps de Kibana
 -

Ejercicios de exploración

- Tomando el índice de vuelos que viene como ejemplo en Kibana, encuentra lo siguiente:
 - ¿Cuántos vuelos hay en el índice en total?
 - ¿Cual es la distribución de valores del campo Carrier (aerolinea)?
 - ¿Cual es la distribución de valores del campo Dest (destino del vuelo)?
 - Usando KQL, ¿cuantos vuelos tuvieron retraso?
 - ¿Cuantos vuelos tuvieron un retraso de más de dos horas?
- Define los siguientes filtros
 - Vuelos que tienen como destino Canadá
 - Vuelos cancelados
 - Vuelos con retraso de más de 15 minutos
 - Vuelos de más de dos mil millas
 - Vuelos que tienen como destino *o como origen* Canadá
 - Para este filtro necesitas definir la consulta en DSL
- Guarda el conjunto de filtros en forma de búsqueda

Visualiza, analiza y actua



Visualiza y analiza

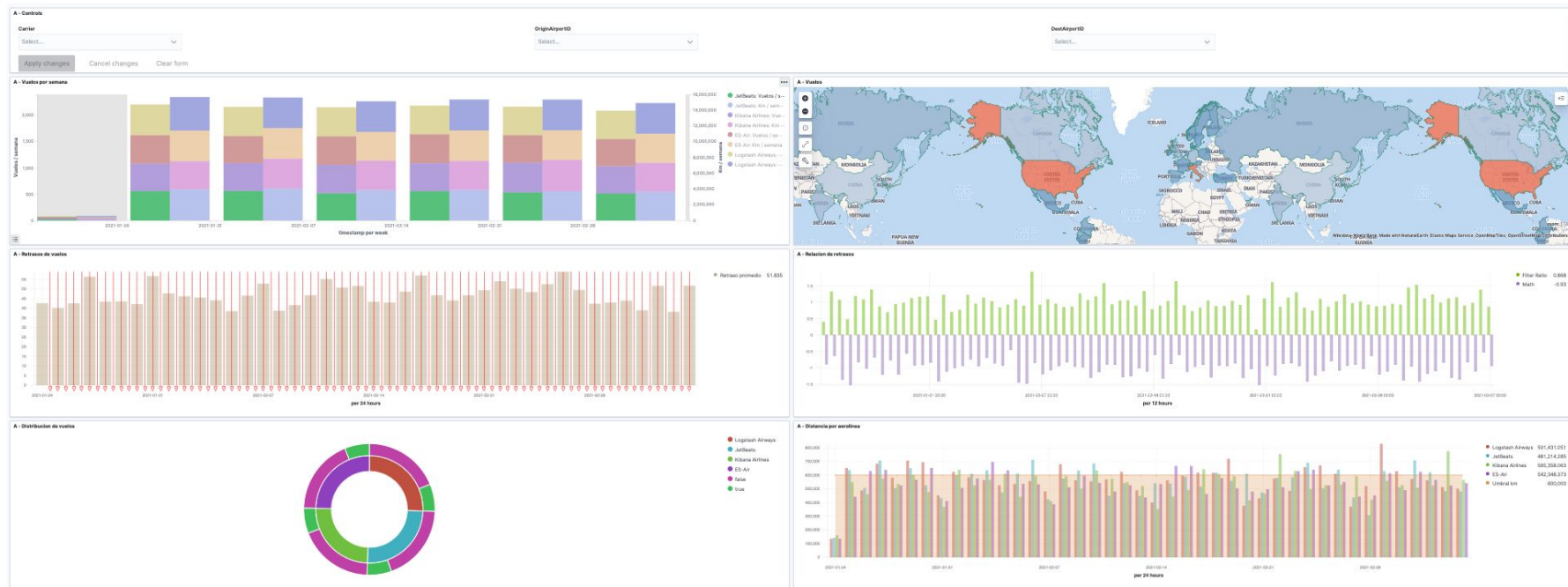
- Kibana ofrece una gran variedad de herramientas de visualización de datos, incluyendo
 - Lens, una herramienta de "arrastrar y colocar" fácil de usar es un buen lugar para comenzar
 - Un juego de visualizaciones más avanzadas que incluye tablas, diagramas de pie, histogramas de tiempo, histogramas, gráficos de líneas, mapas de calor, nubes de palabras, indicadores, controles y markdown
 - Una herramienta especializada para series de tiempo, el Time Series Visual Builder (gráfico) y el Timelion (expresiones)
 - Una herramienta de mapas geográficos construido en el servicio de mapas de Elastic
 - Canvas, una herramienta para crear infografías con información dinámica
 - Vega, una herramienta para hospedar visualizaciones de Vega-Lite -- una gramática de diagramas construidos usando 3D.js
 - Una herramienta que usa aprendizaje de máquina para encontrar anomalías

Ejercicios de visualización y análisis

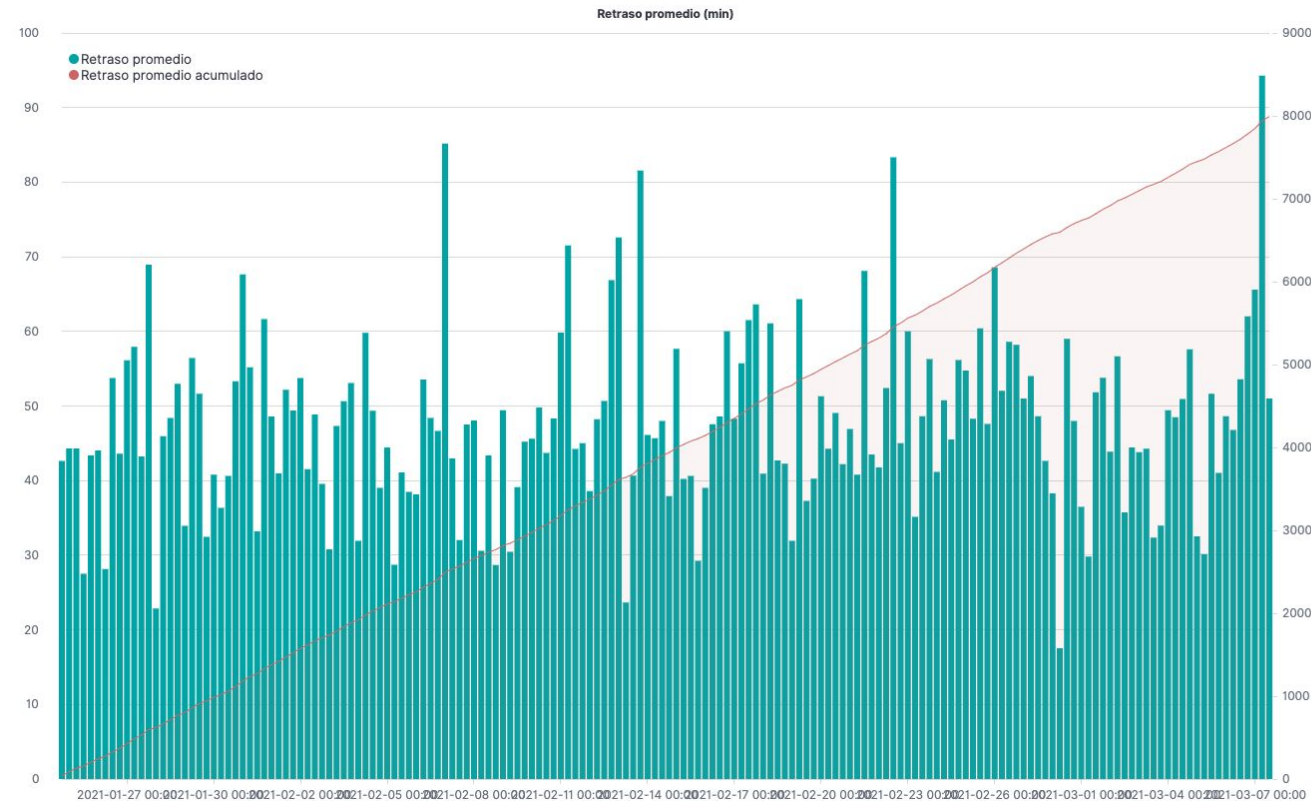
- La mejor manera de comenzar con visualización en Kibana es resolviendo problemas
- Encuentra
 - La distribución de vuelos de cada aerolínea
 - La fracción de retrasos de cada aerolínea
 - Los vuelos semanales de todas las aerolíneas
 - Los vuelos semanales de cada aerolínea
 - Las distancia en km que vuela cada aerolínea cada día
 - Las aerolíneas que exceden el umbral de 600,000 km diarios
 - Si hay condiciones adversas de clima cuando hay retrasos en un vuelo
 - La relación de retrasos de Logstash Airlines con respecto a las demas aerolineas
 - La relación de retrasos de Logstash Airlines con respecto a ES-Air
 - Los vuelos de cada aerolínea en un mapa
 - Puntos de anomalías en los vuelos que tenemos capturados en el índice
 - Continúa la alimentación de datos al trabajo de ML y genera una alerta por email para anomalías críticas

Tableros en Kibana

- Podemos crear tableros en Kibana usando la mayoría de las visualizaciones
- Ejercicio: Añade las visualizaciones que creaste a un nuevo tablero



Timelion para series de tiempo



Interval

6h

Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

Timelion expression

```
.es(index=kibana_sample_data_flights,timefield=timestamp,
metric=avg:FlightDelayMin,).bars().label('Retraso
promedio'),
.es(index=kibana_sample_data_flights,timefield=timestamp,
metric=avg:FlightDelayMin,).lines(fill=0.75, width=1)
.cumsum().yaxis(2).label('Retraso promedio acumulado')
.title('Retraso promedio (min)')
```

× Discard

▶ Update

Infografías con Canvas

- En Kibana podemos usar Canvas para crear infografías con información dinámica
 - Se pueden anidar visualizaciones igual que en un tablero normal
 - Canvas además proporciona su propio juego de visualizaciones
- * Este ejemplo fue adaptado del ejemplo en Kibana

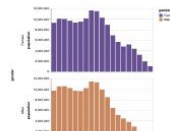


Visualización con Vega-Lite

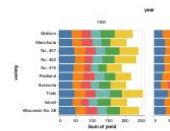
- Vega y Vega-Lite son gramáticas de visualización construidas sobre 3D.js
- Kibana proporciona un puente entre Vega-Lite y una consulta a ES expresada en DSL

Multi-View Displays

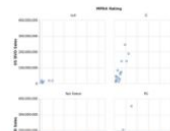
Faceting (Trellis Plot / Small Multiples)



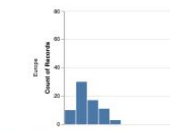
Trellis Bar Chart



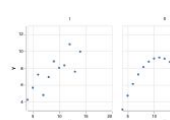
Trellis Stacked Bar Chart



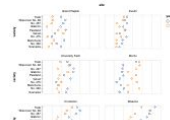
Trellis Scatter Plot (wrapped)



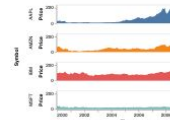
Trellis Histograms



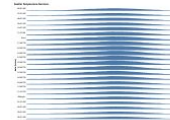
Trellis Scatter Plot Showing Anscombe's Quartet



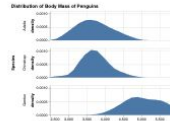
Becker's Barley Trellis Plot



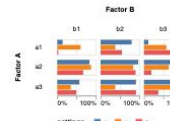
Trellis Area



Trellis Area Plot Showing Annual Temperatures in Seattle

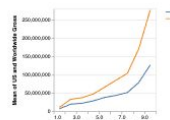


Faceted Density Plot

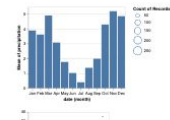


Compact Trellis Grid of Bar Charts

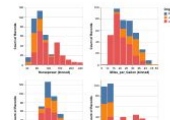
Repeat & Concatenation



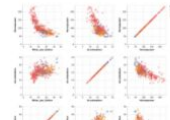
Repeat and Layer to Show Different Movie Measures



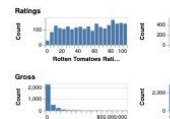
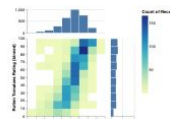
Vertical Concatenation



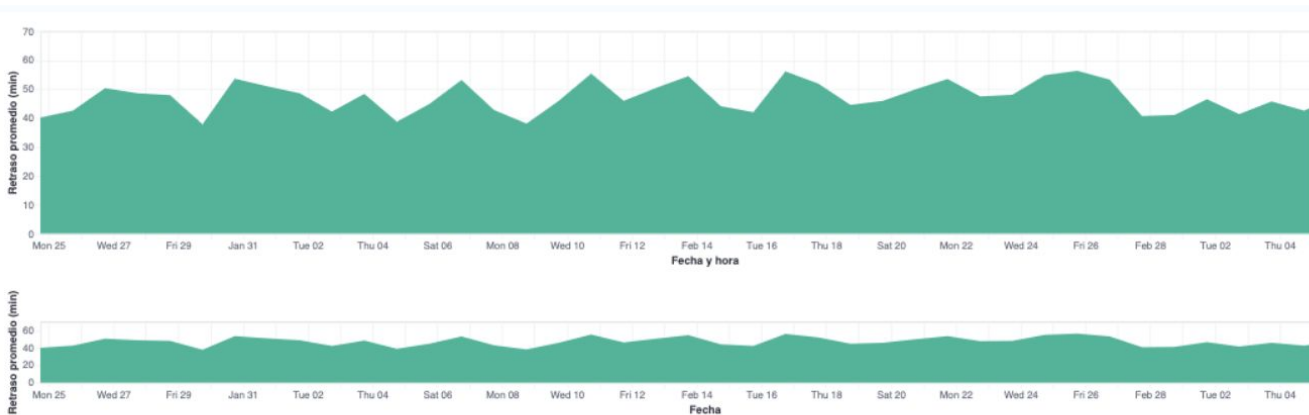
Horizontally Repeated Charts



Interactive Scatterplot Matrix



Ejemplo: Gráfica interactiva con Kibana y Vega-Lite



```
1- {
2   "$schema": "https://vega.github.io/schema/vega-lite/v4.json",
3   "data": {
4     "name": "data1",
5     "url": {
6       "index": "kibana_sample_data_flights",
7       "size": 0,
8       "body": {
9         "aggs": {
10           "por_dia": {
11             "date_histogram": {
12               "field": "timestamp",
13               "interval": "day"
14             },
15             "aggs": {
16               "retraso_promedio": {
17                 "avg": {
18                   "field": "FlightDelayMin"
19                 }
20             }
21           }
22         }
23       },
24       "format": {
25         "property": "aggregations.por_dia.buckets"
26       }
27     },
28     "vconcat": [{
29       "width": 480,
30       "mark": "area",
31       "encoding": {
32         "x": {
33           "field": "key",
34           "type": "temporal",
35           "scale": { "domain": { "selection": "brush" } },
36           "axis": { "title": "Fecha y hora" }
37         },
38         "y": { "field": "retraso_promedio.value", "type": "quantitative",
39           "axis": { "title": "Retraso promedio (min)" } }
40       }
41     ]
42   }
```

Otras apps de Kibana



Casos de uso de Kibana

- Búsqueda
- Observabilidad
- Seguridad
- Administración del Elastic Stack
- Ingesta
- Manejo de datos

The screenshot displays the Kibana Home interface. At the top, there's a 'Home' header with navigation links for 'Add data', 'Manage', and 'Dev tools'. The main content area is divided into several sections:

- Enterprise Search:** Build a powerful search experience. Connect your users to relevant data. Unify your team content.
- Observability:** Monitor infrastructure metrics. Trace application requests. Measure SLAs and react to issues.
- Security:** Prevent threats autonomously. Detect and respond. Investigate incidents.
- Kibana:** Analyze data in dashboards. Search and find insights. Design pixel-perfect presentations. Plot geographic data. Model, predict, and detect. Reveal patterns and relationships.

Below these, there's a section titled 'Ingest your data' with options to 'Add data', 'Add Elastic Agent', and 'Upload a file'. At the bottom, the 'Manage your data' section includes 'Manage permissions', 'Monitor the stack', 'Back up and restore', and 'Manage index lifecycles'.

Directorio de apps

Directory

[All](#) [Data Exploration & Visualization](#) [Administrative](#)



APM

Automatically collect in-depth performance metrics and errors from inside your applications.



Add Elastic Agent

Add and manage your fleet of Elastic Agents and integrations.



Add data

Ingest data from popular apps and services.



Advanced Settings

Customize your Kibana experience — change the date format, turn on dark mode, and more.



App Search

Leverage dashboards, analytics, and APIs for advanced application search made simple.



Back up and restore

Save snapshots to a backup repository, and restore to recover index and cluster state.



Canvas

Showcase your data in a pixel-perfect way.



Dashboard

Display and share a collection of visualizations and saved searches.



Discover

Interactively explore your data by querying and filtering raw documents.



Graph

Surface and analyze relevant relationships in your Elasticsearch data.



Grok Debugger

Simulate and debug grok patterns for data transformation on ingestion.



Interact with the Elasticsearch API

Skip cURL and use a JSON interface to work with your data in Console.



Logs

Stream logs in real time or scroll through historical views in a console-like experience.



Machine Learning

Automatically model the normal behavior of your time series data to detect anomalies.



Manage index lifecycles

Define lifecycle policies to automatically perform operations as an index ages.



Manage permissions

Control who has access and what tasks they can perform.



Maps

Explore geospatial data from Elasticsearch and the Elastic Maps Service.



Metrics

Explore infrastructure metrics and logs for common servers, containers, and services.



Monitor the stack

Track the real-time health and performance of your deployment.



Painless Lab (beta)

Simulate and debug painless code.



Reporting

Manage your reports generated from Discover, Visualize, and Dashboard.



Rollups

Summarize and store historical data in a smaller index for future analysis.



Saved Objects

Import, export, and manage your saved searches, visualizations, and dashboards.



Search Profiler

Quickly check the performance of any Elasticsearch query.



Spaces

Organize your dashboards and other saved objects into meaningful categories.



Stack Management

Your center console for managing the Elastic Stack.



Transforms

Use transforms to pivot existing Elasticsearch indices into summarized or entity-centric indices.



Upload a file

Import your own CSV, NDJSON, or log file.

Sigue aprendiendo



Cursos gratuitos

Free training

Whether you're just getting started or exploring new features, learning Elastic has never been easier with our free introductory training offerings.



Quick Starts

Start your Elastic journey with these bite-sized modules focused on logging, metrics, APM, Workplace Search, and App Search.

[View Quick Starts →](#)



Fundamentals training

Build your observability, security, and Elastic Stack skills anytime, anywhere with these on-demand courses.

[View Fundamentals courses →](#)

Planes de estudio de certificación

Paths to Elastic certification

The demand for Elasticsearch and Kibana experts increases every day. Our certifications let everyone know that you're just what they're looking for.



Elasticsearch engineers

From spinning up your first cluster to mastering advanced management techniques, the Elastic Certified Engineer path will make you an Elasticsearch expert.

- [Elasticsearch Engineer I >](#)
- [Elasticsearch Engineer II >](#)
- [Elastic Certified Engineer >](#)



Data analysts

Enter training a Kibana novice and leave ready to put your data visualization and advanced analytics skills to the test in our Kibana certification.

- [Data Analysis with Kibana >](#)
- [Elastic Certified Analyst >](#)



Observability engineers

Learn to unify your observability data — logs, metrics, APM — with the Elastic Stack. Then make it operational with dashboards, alerting, and machine learning.

- [Elastic Observability Engineer >](#)
- [Elastic Certified Observability Engineer >](#)

Especializaciones

- Búsqueda avanzada
- Ciencia de datos
- Logging
- Analíticos de seguridad
- Métricas
- Monitoreo de aplicaciones
- Administración del Stack de Elastic

Elasticsearch Advanced Search

Search is the heart of Elasticsearch. It's also about returning from the index to the user. While returning the results is the main goal, the user also wants to know how the results were generated. The user wants to know the search process. The user wants to know the search process. The user wants to know the search process.

Don't leave a stone unturned. [Get the book](#)

[Elasticsearch Advanced Search](#)
[Elasticsearch Advanced Search](#)
[Elasticsearch Advanced Search](#)
[Elasticsearch Advanced Search](#)
[Elasticsearch Advanced Search](#)



Data Science

Data science is the process of using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions.

Don't leave a stone unturned. [Get the book](#)

[Data Science](#)
[Data Science](#)
[Data Science](#)
[Data Science](#)
[Data Science](#)



Logging

Logging is the process of recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events. It's about recording events.

Don't leave a stone unturned. [Get the book](#)

[Logging](#)
[Logging](#)
[Logging](#)
[Logging](#)
[Logging](#)



Security Analytics

Security analytics is the process of using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions. It's about using data to make decisions.

Don't leave a stone unturned. [Get the book](#)

[Security Analytics](#)
[Security Analytics](#)
[Security Analytics](#)
[Security Analytics](#)
[Security Analytics](#)

Metrics

Metrics are the numbers that tell you how your system is doing. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers. It's about numbers.

Don't leave a stone unturned. [Get the book](#)

[Metrics](#)
[Metrics](#)
[Metrics](#)
[Metrics](#)
[Metrics](#)



APM

APM is the process of monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance. It's about monitoring application performance.

Don't leave a stone unturned. [Get the book](#)

[APM](#)
[APM](#)
[APM](#)
[APM](#)
[APM](#)

Elastic Stack Management

Elastic Stack Management is the process of managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack. It's about managing the Elastic Stack.

Don't leave a stone unturned. [Get the book](#)

[Elastic Stack Management](#)
[Elastic Stack Management](#)
[Elastic Stack Management](#)
[Elastic Stack Management](#)
[Elastic Stack Management](#)



Preguntas y respuestas



Recursos y el siguiente episodio



Recursos adicionales

- <https://github.com/evkortright/pagina-de-búsqueda>
- <https://github.com/evkortright/primeros-pasos-con-kibana.git>
- enrique.kortright@elastic.co
- <https://www.linkedin.com/in/enrique-kortright-b182ba/>
- <https://discuss.elastic.co/>

En nuestro siguiente episodio...

- En el tercer episodio vamos a aprender cómo capturar y cargar grandes cantidades y enviarlas a Elasticsearch
 - El módulo de Import de Machine Learning es solo para conjuntos muy pequeños de datos
 - Vamos a explorar Logstash y los varios Beats que completan el Elastic Stack
- ¡No te lo pierdas!

Conéctese con la comunidad de Elastic

Existen User Groups en Costa Rica,
Mexico, Colombia, Argentina y Uruguay -
encuentra el tuyo:



User Group Virtual:



<https://community.elastic.co/>
<https://community.elastic.co/amer-virtual/>