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/

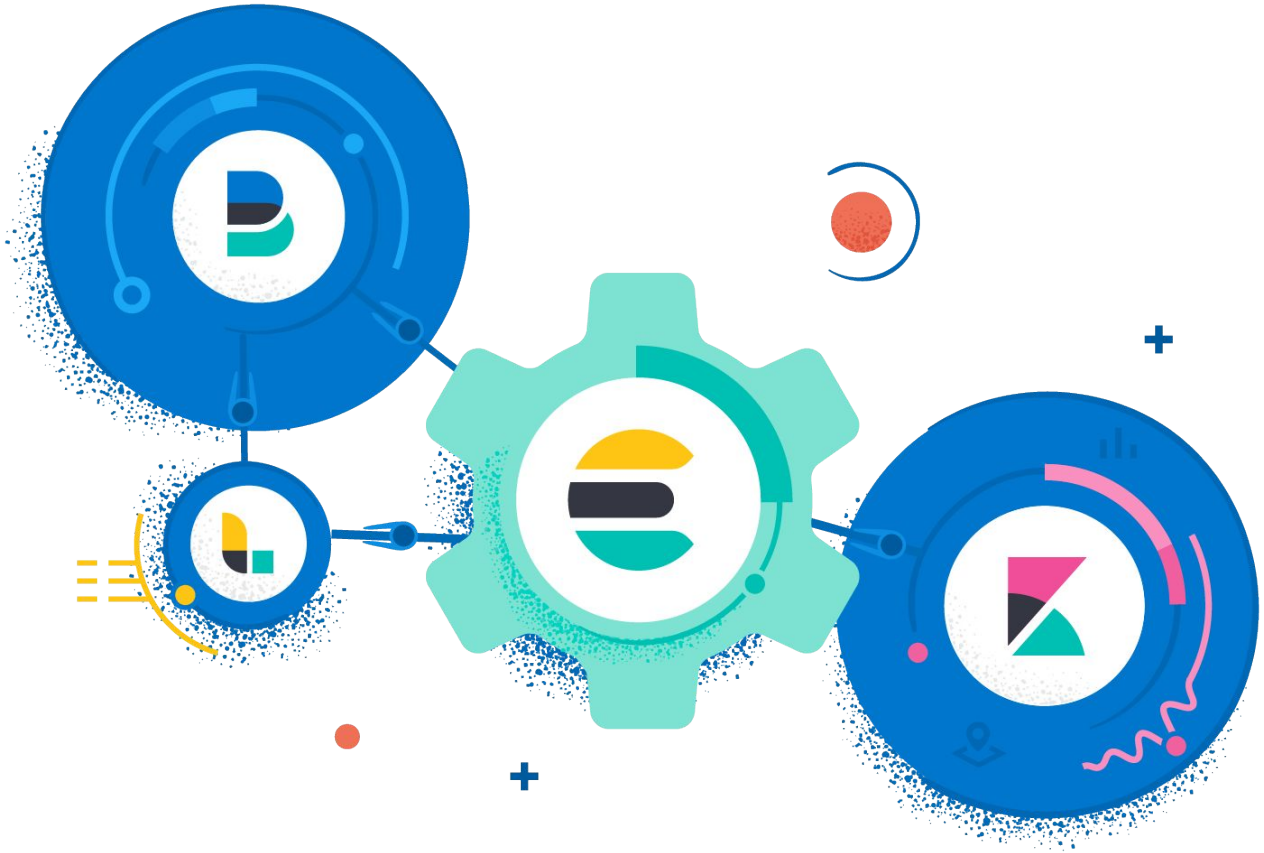
User Group Virtual:

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

Agenda

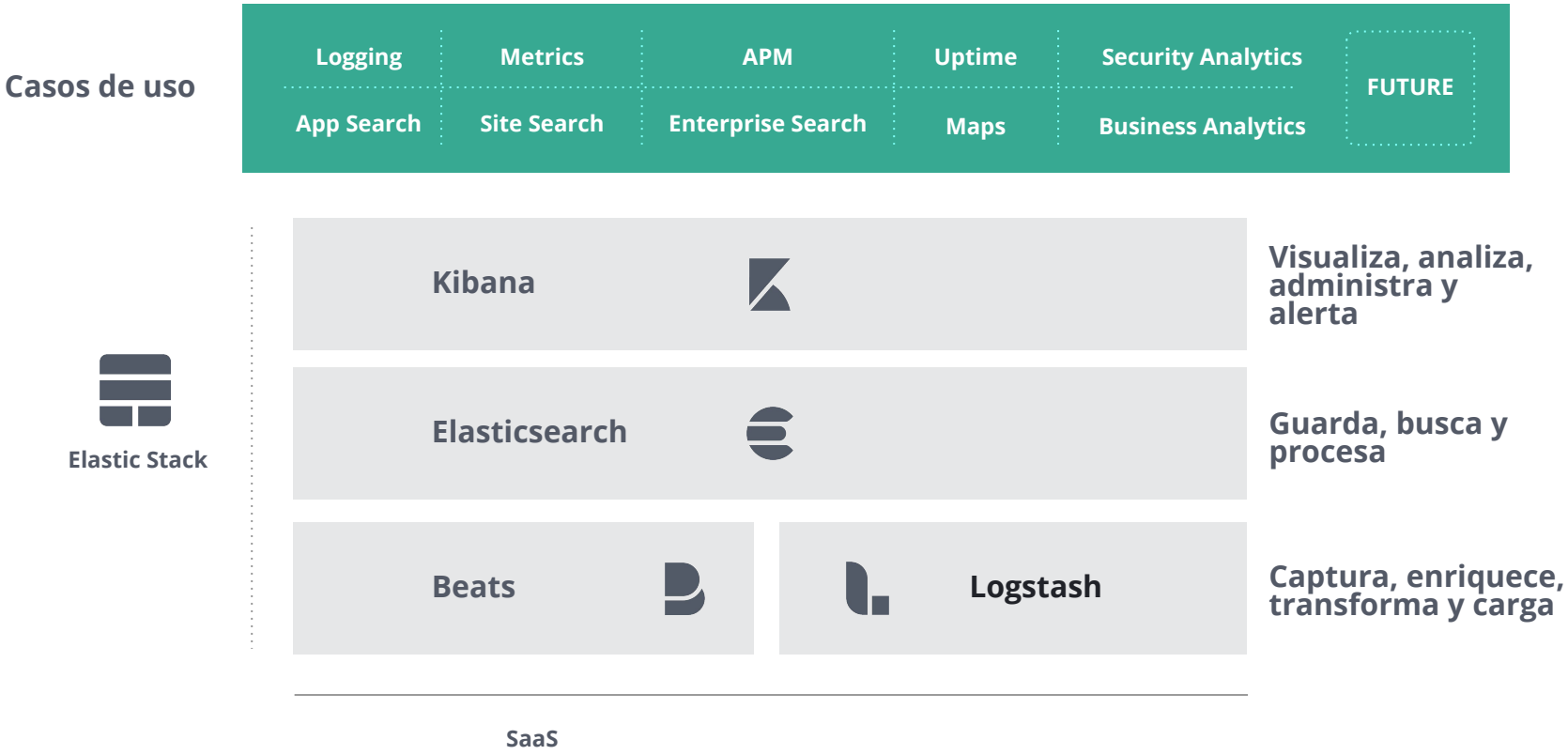
- ¿Que es Kibana? Repaso del primer episodio
- Flujo de trabajo de un analista de datos
- Explora
- Visualiza
- Analiza
- Actua
- Preguntas y respuestas
- Episodios futuro: Logstash/Beats

Elasticsearch es parte del Elastic Stack



elastic

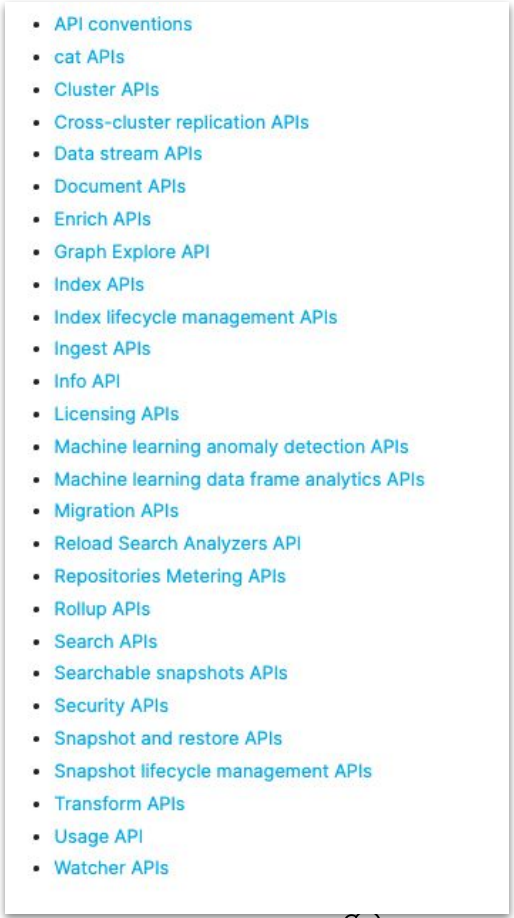
El Stack de Elastic



elastic

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 traves de Logstash



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

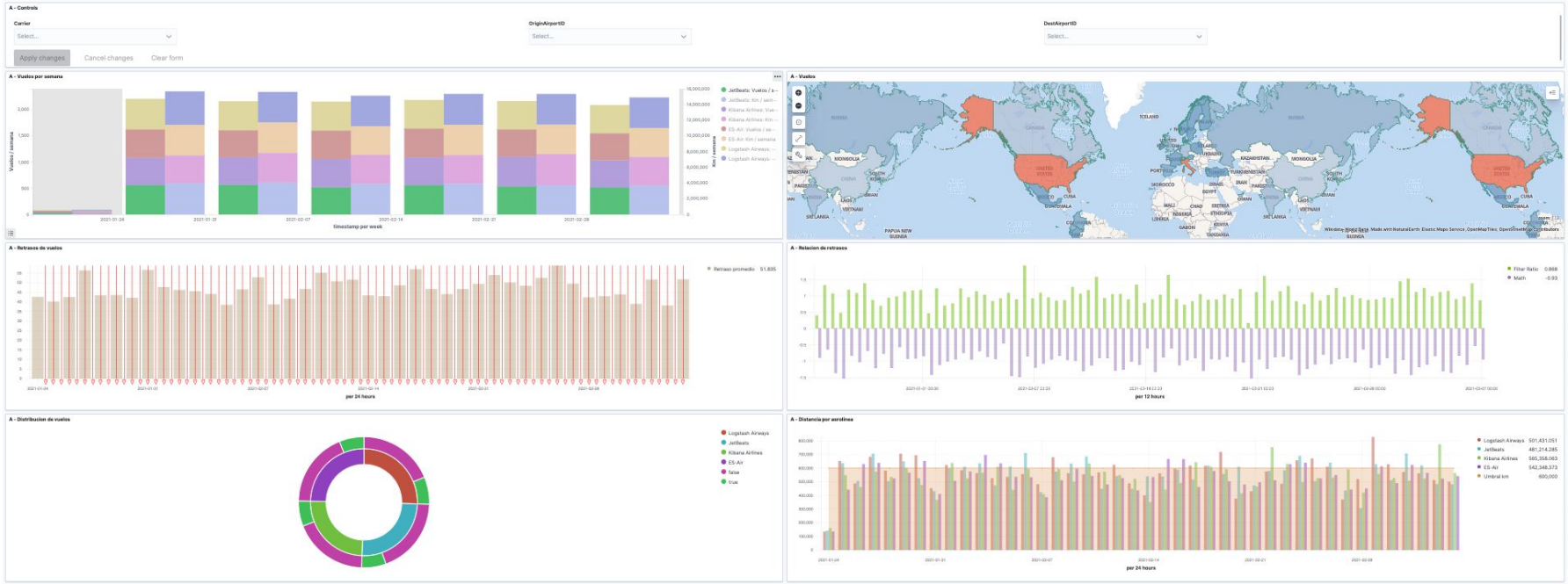
- Kibana ofrece una gran variedad de herramientas de visualización de datos, incluyendo
  - Lens, una herramienta de "arrastrar y colocar" fácil de usar es un buen lugar para comenzar
  - Un juego de visualizaciones más avanzadas que incluye tablas, diagramas de pie, histogramas de tiempo, histogramas, 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

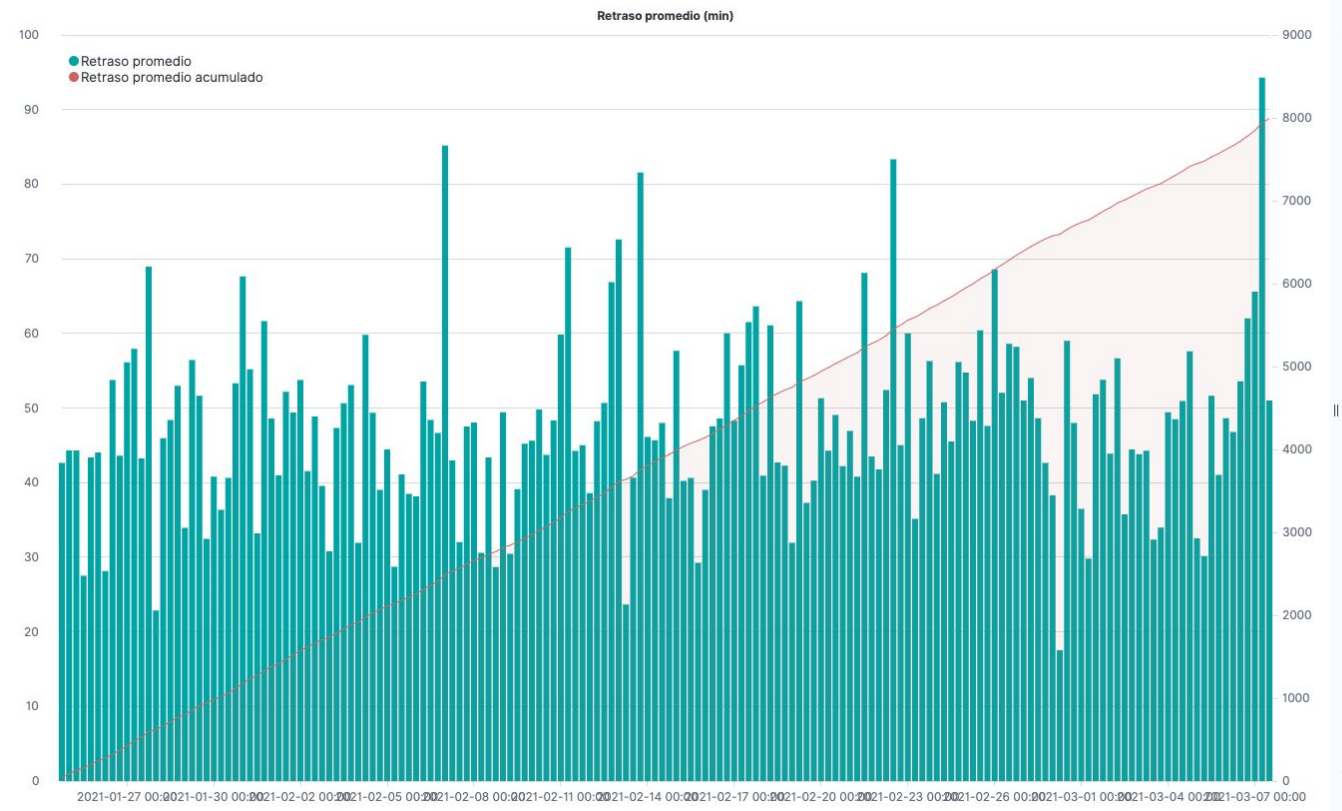
- La mejor manera de comenzar con visualización en Kibana es resolviendo problemas
- Encuentra
  - La distribución de vuelos de cada aerolínea
  - La fracción de retrasos de cada aerolínea
  - Los vuelos semanales de todas las aerolíneas
  - Los vuelos semanales de cada aerolínea
  - Las distancia en 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
  - Continua 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)
    .cusum().yaxis(2).label('Retraso promedio acumulado')
    .title('Retraso promedio (min)')
```

Discard Update

elastic

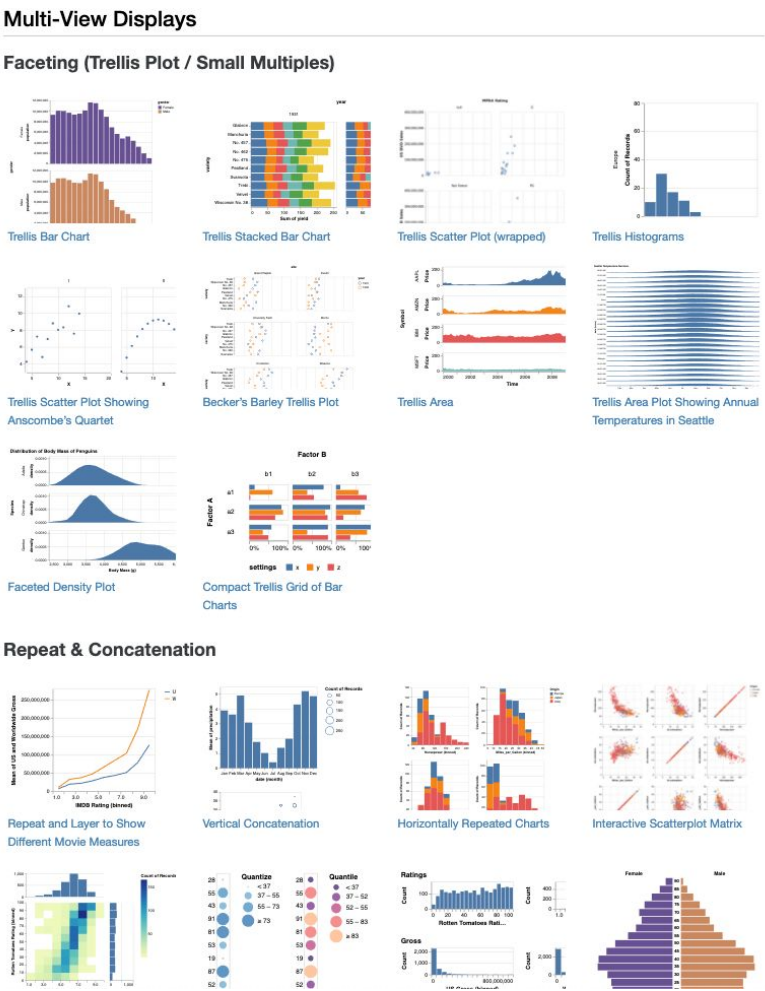
Infografías con Canvas

- 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

elastic

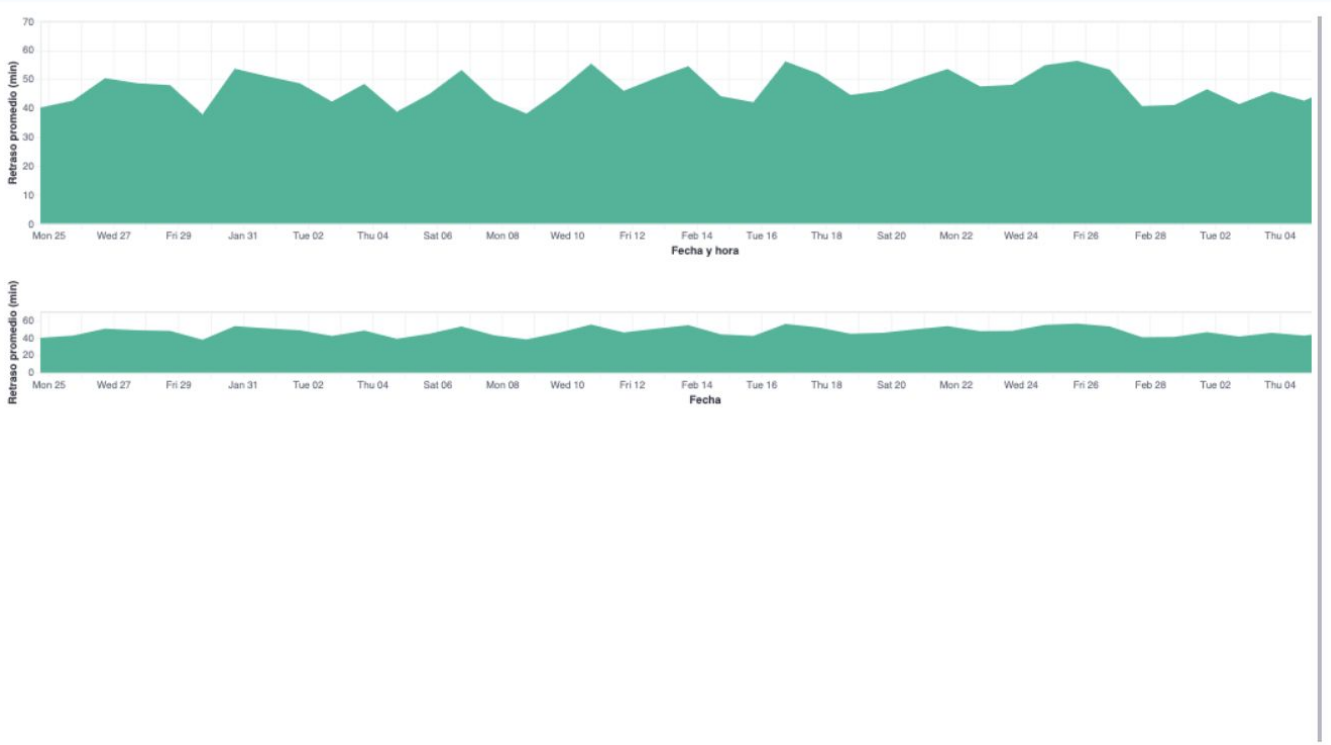
Visualización con Vega-Lite

- 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



elastic

Ejemplo: Gráfica interactiva con Kibana y Vega-Lite



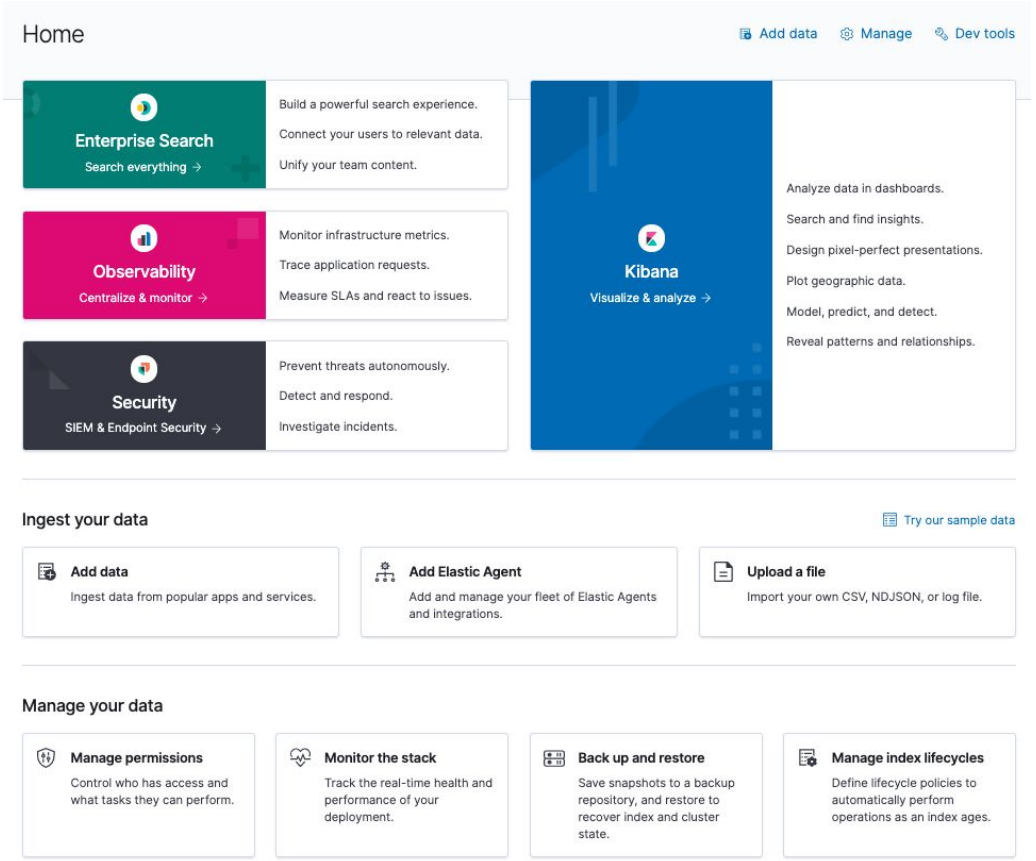

```
{
  "$schema": "https://vega.github.io/schema/vega-lite/v4.json",
  "data": {
    "name": "data1",
    "url": {
      "index": "kibana_sample_data_flights",
      "body": {
        "size": 0,
        "aggs": {
          "por_dia": {
            "date_histogram": {
              "field": "timestamp",
              "interval": "day"
            },
            "aggs": {
              "retraso_promedio": {
                "avg": {
                  "field": "FlightDelayMin"
                }
              }
            }
          }
        }
      }
    },
    "format": {
      "property": "aggregations.por_dia.buckets"
    }
  },

  "vconcat": [{
    "width": 480,
    "mark": "area",
    "encoding": {
      "x": {
        "field": "key",
        "type": "temporal",
        "scale": {"domain": {"selection": "brush"}},
        "axis": {"title": "Fecha y hora"}
      },
      "y": {"field": "retraso_promedio.value", "type": "quantitative",
        "axis": {"title": "Retraso promedio (min)"}}
    }
```


elastic

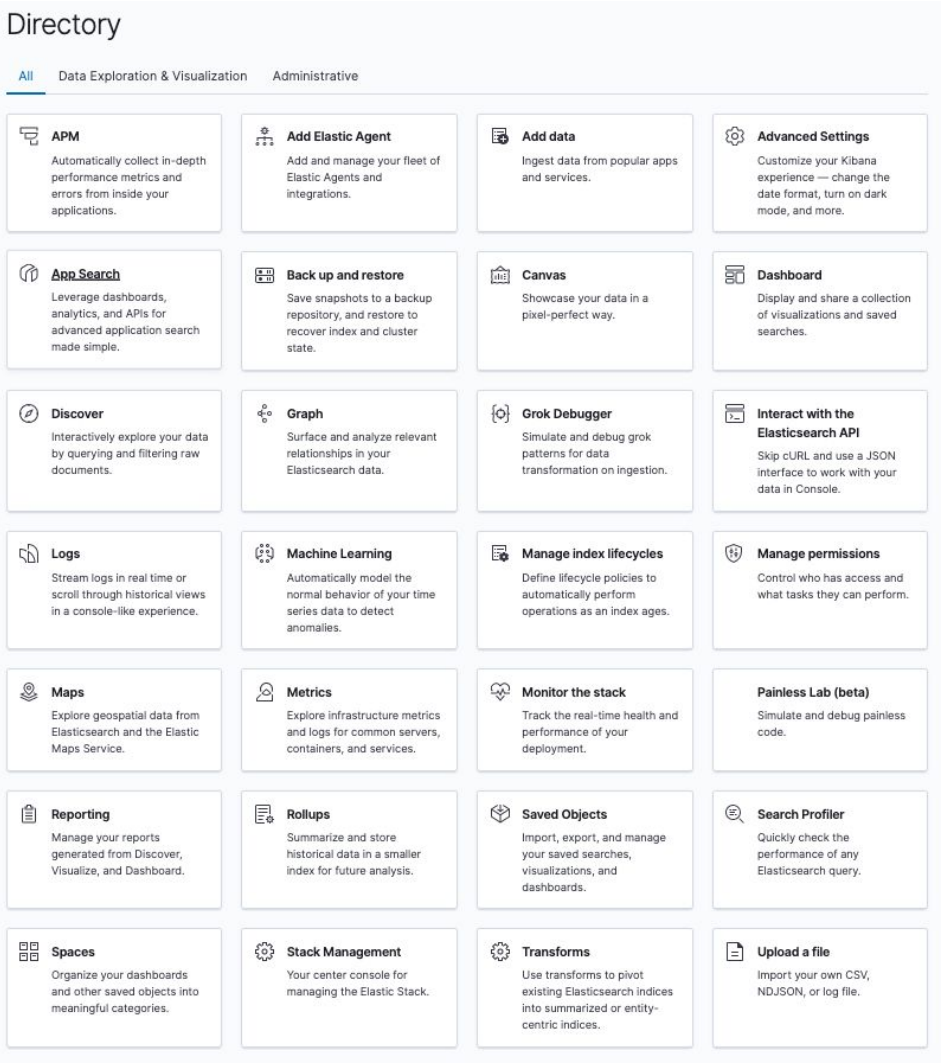
Otras apps de Kibana

Casos de uso de Kibana

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



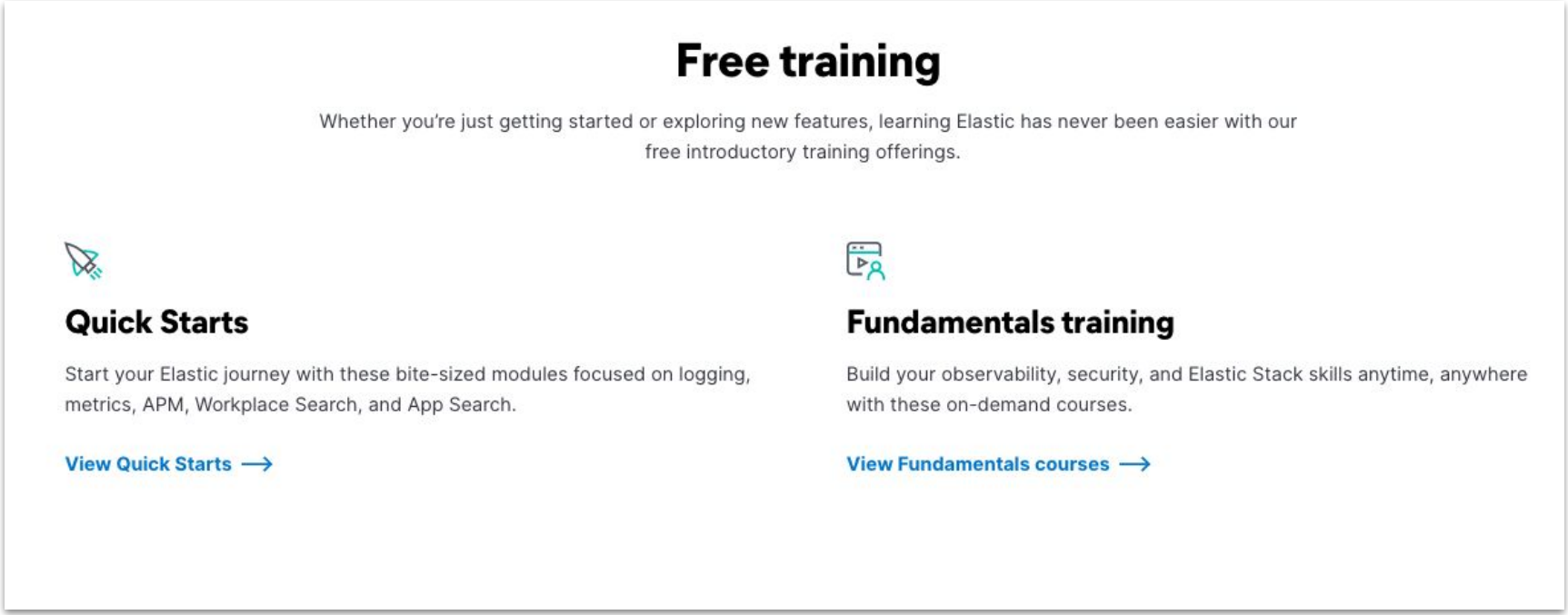
Directorio de apps



elastic

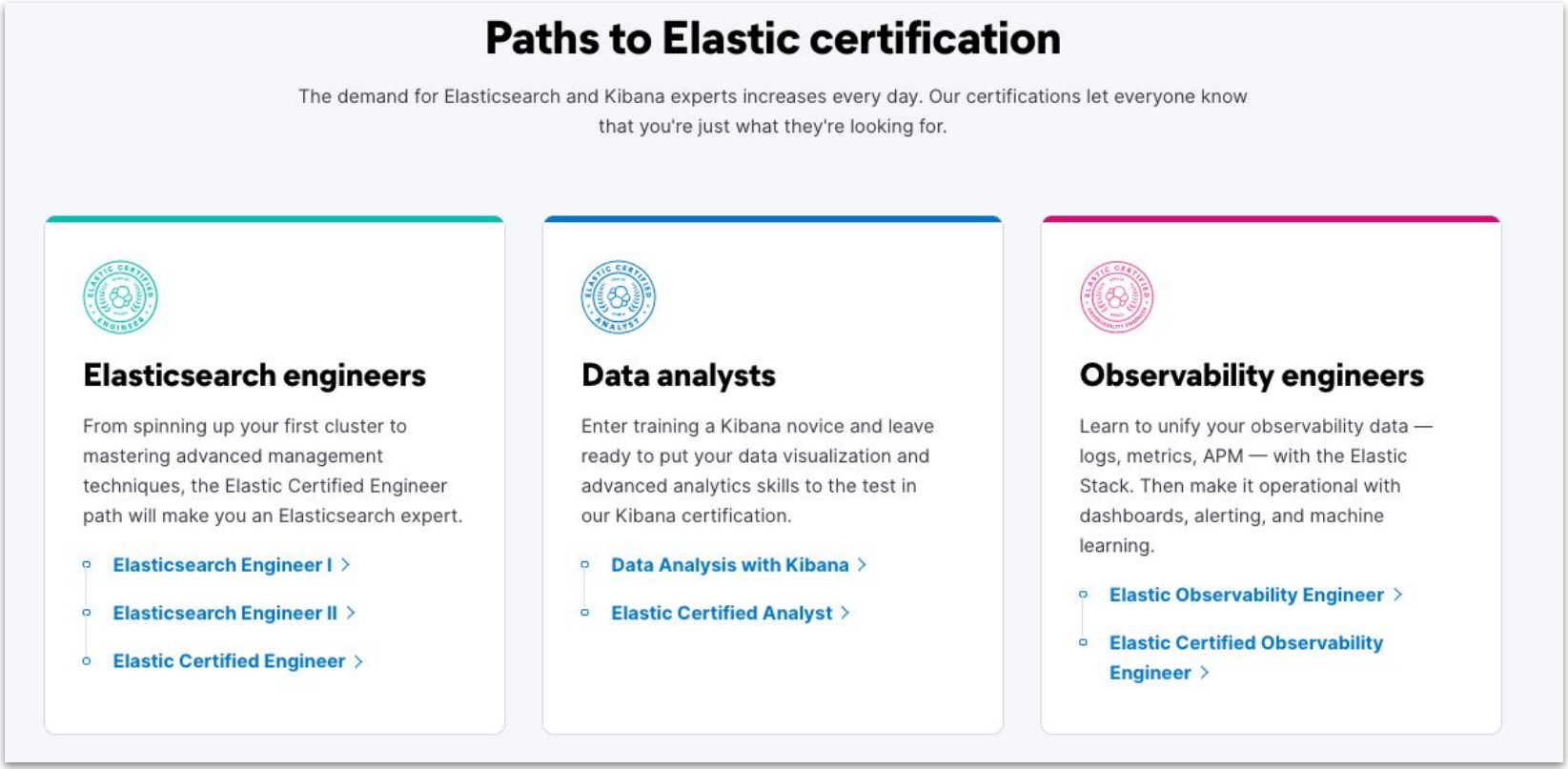
Sigue aprendiendo

Cursos gratuitos



elastic

Planes de estudio de certificación



elastic

Especializaciones

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

elastic

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/