



ELK

Elastic Search, Logstash y Kibana

QUÉ ES ELK

Stack open-source de software libre

- Elastic Search
- Logstash
- Kibana

ETL

- Extract
 - API
 - Beats
 - Web Scraping
- Transform
 - Renombrar campos
 - Transformar una fecha en timestamp
 - Desglosarla en varios campos
- Load
 - Cargar el registro en una Base de Datos

ELK <3 ETL

- [Beats] – Extract
- Logstash – Transform
- Elastic Search – Load
- Kibana – Analyze

ELASTIC SEARCH

- Base de Datos
 - NoSQL
 - Documental (Parecida a MongoDB)
 - Buena para series temporales
- Sharding, réplicas, particiones, RAID
- Buena integración por defecto con Logstash/Kibana

LOGSTASH

- Transformador
- In/Out, pensado para pipelines
 - Datos entran
 - Datos salen procesados
- En Java, pero configurable con fichero legible
- Integración con plugins y ampliable por terceros

KIBANA

- Visualizador de datos
- Cuadros de mandos (Dashboard) personalizables desde 0
- Integración por defecto para
 - Gráficos
 - Mapas (y visualizaciones geográficas)
 - Series temporales (forecasting por ejemplo)

BEATS

- Extractores de info
- Distintos puntos de entrada a la pipeline
- Integraciones out of the box para muchas fuentes de datos
- Altamente configurables

CASOS DE USO COMUNES

- Monitorización y Logs
- Health checks y Observabilidad
 - El sistema está en marcha (uptime)
 - ¿Cuánto está consumiendo de cada recurso? RAM, CPU, Disco duro
- Visualizaciones
 - Geográficas (segmentaciones de clientes)
 - Series temporales (picos de usuarios)
- ETLs y ELTs

BONUS: ELT

- ETL es **E**xtract **T**ransform **L**oad
- ELT es **E**xtract **L**oad **T**ransform
- Diferencias clave:
 - ETL sabes formato de destino, ELT delegas la transformación a más adelante
 - ETL usado en Data Warehouses (estructurado), ELT Data Lakes (al montón)
 - ELT permite poder crear varios ETL y Warehouses, mantienes origen y creas varios destinos