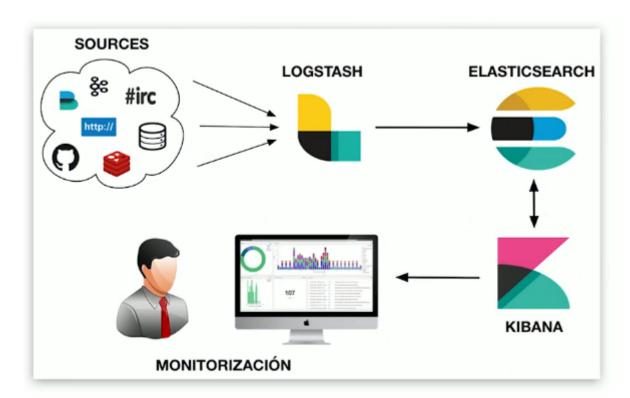
30/10/2025 18:46 1/2 ELK: Logstash

## **ELK: Logstash**



- preprocesamiento (antes de elasticsearch)
- servicio para procesar/transformar información recolectada de diferentes fuentes y enviarla a múltiples tipos de salidas.
- múltiples plugins (de entrada y salida)
  - +200 plugins y posibilidad de desarrollarlos
- permite usar cola de almacenamiento ante errores
  - o kafka, redis como alterntivas más profesionales
- monitorización: visibilidad de recursos de los nodos y estadísticas de servicio
- seguridad: información cifrada en la comunicación con los servicios
- 3 etapas claramente diferenciadas: entrada, filtrado, salida

## entrada

- limpieza de datos
  - o gran cantidad de campos ¿todos necesarios?
  - campos mal formados
- enriquecimiento de datos
  - o añadir información a campos existentes
  - crear campos nuevos
  - o geolocalización
  - o (ejemplo) convertir puertos a protocolos
  - ∘ (ejemplo) IP → latitud, longitud
- ingesta de datos:
  - o formas, tamaños, fuentes variados

## filtrado

- transformaciones al vuelo
- estructura de datos
- trabaja con fingerprints
- reconocmiento de fechas

## salida

- · varias opciones
- ELK: Logstask(instalación y configuración)
- ELK: Logstask(procesamiento)

From:

https://miguelangel.torresegea.es/wiki/ - miguel angel torres egea

Permanent link:

https://miguelangel.torresegea.es/wiki/info:cursos:openwebinars:elk:logstash?rev=1638482522

Last update: 02/12/2021 14:02

