INTRODUCCIÓN & INSTALACIÓN KIBANA

KIBANA

Permite visualizar los datos almacenados en Elasticsearch y navegar a través de la Stack de Elastic.

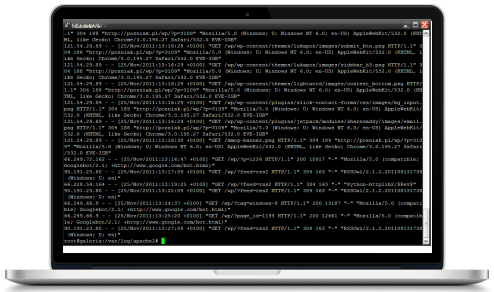
"Una imagen vale más que mil palabras"

1.

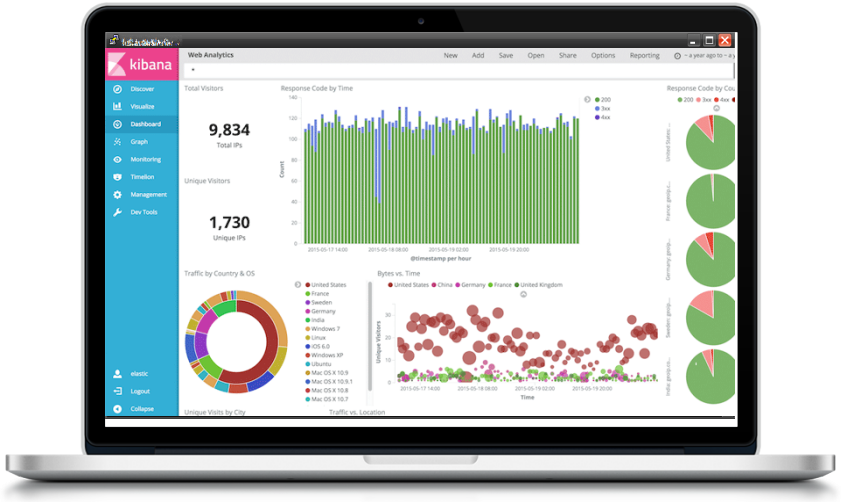
INTRODUCCIÓN

IMPORTANCIA DE LA VISUALIZACIÓN DE DATOS

- ¿Posibilidad de encontrar alguna anomalía?
- Gran cantidad de eventos
- Eventos con múltiples campos
- Distintas fuentes / dispositivos
- …



IMPORTANCIA DE LA VISUALIZACIÓN DE DATOS



CARACTERÍSTICAS DE KIBANA

- Visualizaciones. Histogramas, gráficas en tiempo, tartas y roscos, tablas…
- Datos en tiempo real. Elasticsearch permite que se busque la información segundos después.
- Dashboards. Recoger las visualizaciones en paneles donde tener una vista global de todas.
- Geolocalización. Coordenadas en mapas.
- Extras. *Timeseries*, *Graph*, *Machine Learning*…

2.

INSTALACIÓN

KIBANA

Formatos posibles: *zip*, *tar.gz*, *deb*, *rpm*, *docker*

- Importar Elasticsearch PGP Key

  $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

- Necesario el paquete *apt-transport-https*

  $ sudo apt-get install apt-transport-https

KIBANA

- Almacenar el repositorio en “*/etc/apt/sources.list.d/elastic-5.x.list*” :

  $ echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list

- Instalación:

  $ sudo apt-get update && sudo apt-get install kibana

KIBANA (SysV *init* vs *systemd*)

- Kibana con SysV *init*

  $ sudo update-rc.d kibana defaults 95 10

  $ sudo -i service kibana start/stop

- Kibana con *systemd*

  $ sudo /bin/systemctl daemon-reload

  $ sudo /bin/systemctl enable kibana.service

  $ sudo systemctl start/stop kibana.service

KIBANA (*Paths*)

Las **principales rutas** del servicio Kibana son:

- *home:* /usr/share/kibana
- *bin:* /usr/share/kibana/bin
- *conf:* /etc/kibana
- *data:* /var/lib/kibana
- *optimize:* /usr/share/kibana/optimize
- *logs:* /var/log/kibana
- *plugins:* /usr/share/kibana/plugins

3.

CONFIGURACIÓN

CONFIGURACIÓN: *kibana.yml*

- *server.host.* Dirección donde escuchará kibana. Solo la local, la IP pública o todas las interfaces "*0.0.0.0*".

- *elasticsearch.url.* URL (ip:port) donde está Elasticsearch escuchando.

- *kibana.index*. Kibana usa un índice en Elasticsearch donde guardará búsquedas, visualizaciones y dashboards. Lo crea si éste no existe.

CONFIGURACIÓN: *kibana.yml*

- *pid.file.* Especifica la ruta donde Kibana crea el archivo con el ID del proceso.

- *logging.dest.* Habilita que los logs se almacenen en un fichero.

Nota: ejecución manual -> logs por pantalla siempre que esté comentado el anterior parámetro.

4.

EJECUCIÓN

EJECUCIÓN (*/usr/share/kibana/bin/kibana*)

[info][status][plugin:kibana@5.4.2] Status changed from uninitialized to green…
[info][status][plugin:elasticsearch@5.4.2] Status changed from uninitialized to yellow - Waiting for Elasticsearch
[info][status][plugin:console@5.4.2] Status changed from uninitialized to green…
[info][status][plugin:metrics@5.4.2] Status changed from uninitialized to green…
[info][status][plugin:elasticsearch@5.4.2] Status changed from yellow to green - Kibana index ready
[info][status][plugin:timelion@5.4.2] Status changed from uninitialized to green…
[info][listening] Server running at http://0.0.0.0:5601
[info][status][ui settings] Status changed from uninitialized to green - Ready

URL DE CONEXIÓN A KIBANA

http://172.16.2.21:5601