ELK: Beats (Metricbeats)

4.1_metricbeats.pdf

- recogida métricas del OS: RAM, CPU, Disco
- logstash, opcional si se requiere preprocesamiento, si no, directamente a elasticsearch

instalación y configuración

- ```
  curl -L -O
  https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-5.4.2-
  amd64.deb
  sudo dpkg -i metricbeat-5.4.2-amd64.deb
  service metricbeat {start | status | stop}
  ```
- **/etc/metricbeat/metricbeat.yml**, modificar destino en sección **output.eleasticsearch**

modulos

- CPU
- Core
- Filesystem
- Memoria
- Carga
- I/O
- network
- sockets

modulos extra

- monitorización de servicios en concreto
- ...
- apache
- docker
- mysql
- php_fpm
- ...

importar dashboards de ejemplo

Desde el directorio de Metricbeats: `/usr/share/metricbeat/scripts/import_dashboards`

Si Elasticsearch no está en la misma máquina: `/usr/share/metricbeat/scripts/import_dashboards -es http://192.168.1.10:9200`

Si está securizado será necesario los parámetros de autenticación: `-user user_name -pass password`

Muy importante para la creación de dashboards buenos será conocer bien qué representa/significa cada campo. Para ello se puede consultar la documentación oficial en el siguiente enlace:
  ```

https://www.elastic.co/guide/en/beats/metricbeat/current/exported-fields-system.html