ELK: Logstask(instalación y configuración)

3.1_instalacion_y_configuracion.pdf

- arranque de servicio lento
- procesado rápido
- puerto por defecto 9600

instalación

Java 8, el 9 no está soportada (2017)

```
wget -qO - https://artifacts.elastic.co/GPG-KEYelasticsearch | sudo apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a
/etc/apt/sources.list.d/elastic-5.x.list
sudo apt-get update && sudo apt-get install logstash
```

rutas

- **home**: /usr/share/logstash
- **bin**: /usr/share/logstash/bin
- **conf**: /etc/logstash
- **env**: /etc/default/logstash
- **data**: /var/lib/logstash
- **logs**: /var/log/logstash
- **plugins**: /usr/share/logstash/plugins

pipeline

- obligatori entrada y salida, filtrado opcional
- simple:

```
bin/logstash -e 'input { stdin { } } output { stdout {} }'
```

    - -e: permite especificar la configuración en el CLI
    - tiempo y IP se añaden automaticamente