## 5.2 FILEBEAT

En este tema se trabajará con el primero de los Beats. `Filebeat` recoge información y eventos desde archivos y los puede reenviar tanto a Logstash como a Elasticsearch.

En esta práctica utilizaremos un simulador de logs de Apache aleatorio para escribir dichos eventos en un archivo que Filebeat estará monitorizando y enviando dichos eventos en tiempo real a Elasticsearch.

### Fake Apache Log Generator

El proyecto se encuentra publicado en Git. Para su clonado deberemos descargarnos el comando Git y realizar un clonado del repositorio:

```
apt install git
cd /home/elastic/Downloads
git clone https://github.com/kiritbasu/Fake-Apache-Log-Generator.git
```

El proyecto utiliza Python 2.7 por lo que será necesario también instalar el mismo para poder ejecutarlo y el `requirements.txt` del proyecto que acabamos de clonar.

```
sudo apt install python2.7 python-pip
pip install -r requirements.txt
```

Y ya se puede ejecutar el mismo y comenzar a generar logs de prueba:

```
python apache-fake-log-gen.py
python apache-fake-log-gen.py -n 100 -o LOG
cat access_log_*.log
```

### Filebeat

El primer paso será descargar el servicio, instalarlo y configurarlo como servicio del sistema:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a
 /etc/apt/sources.list.d/elastic-6.x.list
sudo apt-get install filebeat
sudo update-rc.d filebeat defaults 95 10
```

A continuación habrá que indicarle al servicio qué es lo que se quiere monitorizar, que deberá apuntar a la ruta donde estemos almacenando los logs que el generador está haciendo y especificar también la IP

donde Elasticsearch está escuchando para enviarle estos eventos. Para ello, se modificará el archivo `/etc/filebeat/filebeat.yml` con los siguientes datos:

```
    enabled: true
    paths:
      - /home/elastic/Downloads/Fake-Apache-Log-Generator/access_log_*.log

    output.elasticsearch:
      hosts: ["192.168.1.31:9200"]
```

Una vez configurado, solo tenemos que arrancar el servicio.

```
service filebeat start
```

Y se puede monitorizar la ejecución del mismo a través de su log:

```
tail -f /var/log/filebeat/filebeat
```

Para generar más logs de prueba solo tendremos que seguir ejecutando el proyecto clonado anteriormente y Filebeat deberá ir recogiéndolos e indexándolos en Elasticsearch:

```
python apache-fake-log-gen.py -n 100 -o LOG
```