5.5 Winlogbeats & Auditbeats

Este tema trabaja con los dos *Beats* que no son multiplataforma y están orientados a la auditoría de lo que ocurre en los sistemas operativos Windows y Unix.

Auditbeat

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 update && sudo apt-get install auditbeat
sudo update-rc.d auditbeat defaults 95 10
```

Una vez descargado, para configurarlo serán necesarias las mismas modificaciones que es han realizado en el servicio de Metricbeats modificando el archivo de configuración del servicio `/etc/auditbeat/auditbeat.yml` :

```
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["192.168.1.31:9200"]

setup.kibana:
  # Kibana Host
  host: "192.168.1.31:5601"
```

Para arrancar el servicio y monitorizar su ejecución se pueden utilizar los siguinetes comandos:

```
service auditbeat start
tail -f /var/log/auditbeat/auditbeat
```

Como ya se ha añadido en el archivo de configuración la ruta a Kibana, se puede realizar el importado automático de visualizaciones y dashboards a la misma. Para ello deberemos irnos al *home* de Auditbeat y ejecutar los siguientes comandos para la subida de los mismos:

```
cd /usr/share/auditbeat
mv kibana bin
./bin/auditbeat setup --dashboards -c /etc/auditbeat/auditbeat.yml
```

Se crea un archivo dentro de `/bin` que es uno de los directorios que se monitoriza por defecto que simplemente realice la ejecución de un `ifconfig` :

```
sudo vim /bin/net.sh

#!/bin/sh
# Shows ip address of eth3
/sbin/ifconfig
```

Y una vez creado, con el servicio de Auditbeat funcionando, se le pondrán los permisos necesarios y se ejecutará:

```
sudo chmod 755 /bin/net.sh
net.sh
```

Posteriormente podremos crear reglas que monitoricen la ejecución de distintos comandos:

```
audit rules:
    -w /usr/bin/who -p x -k my_execs
    -w /usr/bin/whatis -p x -k my_execs
```

Winlogbeat

En el caso de Winlogbeat todo se realiza de forma más gráfica, realizando la descarga de la última versión estable desde la página oficial. Únicamente habrá que modificar el archivo `winlogbeat.yml` como se viene haciendo con el resto de Beats. Posteriormente, ejecutamos Winlogbeat y deberemos empezar a recibir los EventCodes de Windows.