Manual de instalación

En este documento se va a explicar el proceso de instalación del entorno de correlación, el cual se va a desplegar en dos máquinas distintas.
Por un lado tenemos la máquina ELK, en la cual se instalarán los componentes Logstash, Elasticsearch y Kibana. Estos componentes son los encargados de normalizar, enriquecer y almacenar los eventos.
Por otro lado tenemos la máquina ELKorrelator, en la cual se instalará el componente software desarrollado. Será el encargado de correlar los eventos normalizados y enriquecidos a través de consultas a los eventos almacenados en la máquina ELK.



Componentes ELK (192.168.1.123)

ELKorrelator (192.168.1.124)

Instalación de los componentes ELK
En primer lugar vamos a instalar los componentes de la máquina ELK. Se va a comenzar a partir de un Ubuntu Server 16.04 recién instalado.
Lo primero es copiar los ficheros del directorio ficheros_elk a la máquina. En este directorio encontramos una configuración base para Logstash y scripts para generar eventos que prueban el funcionamiento de las reglas de correlación.
Para la correcta instalación se debe utilizar el usuario root.
Si se desean utilizar los scripts de test, se debe tener instalado python2:

```
apt install python-minimal
```

A continuación debemos instalar Java para que puedan funcionar Logstash y Elasticsearch.

```
apt install default-jre
```

Para instalar Elasticsearch ejecutamos:

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.3.deb
dpkg -i elasticsearch-6.2.3.deb
```

Configuramos Elasticsearch para que responda a cualquier IP:

```
vi /etc/elasticsearch/elasticsearch.yml
```

En este caso deseamos que se pueda conectar localhost para que Logstash pueda almacenar datos y la IP de la máquina ELKorrelator(en mi caso 192.168.1.124) para que los Correladores puedan realizar consultas a Elasticsearch. Añado la siguiente línea:

```
network.host: 0.0.0.0
```

Ahora limitamos el acceso con ufw:

```
ufw allow from 192.168.1.124 to any port 9200
ufw enable
```

Si se utilizan conexiones ssh para controlar remotamente el equipo también se debe añadir:

```
ufw allow from any to any port 22
ufw enable
```

Para instalar Logstash ejecutamos:

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-6.2.3.deb
dpkg -i logstash-6.2.3.deb
```

Copiamos la configuración básica, la cual contiene los parseos necesarios para poder probar los scripts de test:

```
cp logstash.conf /etc/logstash/conf.d/
```

Sustituimos la variable "IP_ELKorrelador" por la IP de la máquina ELKorrelador, en este caso:

```
vi /etc/logstash/conf.d/logstash.conf
```

```
:%s/IP_ELKorrelador/192.168.1.124/g
```

Añadimos permisos para que el componente Correlador de ELKorrelator se pueda conectar con el Logstash:
Ahora limitamos el acceso con ufw:

```
ufw allow from 192.168.1.124 to any port 45555
ufw enable
```

Para instalar Kibana ejecutamos:

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-6.2.3-amd64.deb
dpkg -i kibana-6.2.3-amd64.deb
```

Permitir el acceso a Kibana, en primer lugar editamos el fichero de configuración:

```
 vi /etc/kibana/kibana.yml
```

Y añadimos la siguiente línea:

```
server.host: 0.0.0.0
```

También tenemos que abrir el puerto:

```
ufw allow from any to any port 5601
ufw enable
```

Añadimos una línea en el fichero crontab para borrar los ficheros temporales antiguos:

```
vi /etc/crontab
```

```
0 *    * * *   root    find /var/log/elkorrelator/in/ -atime +1 -name "*.log"  -exec rm {} \;
```

Por último reiniciamos los servicios y los activamos para que arranquen automáticamente si se reinicia la máquina:

```
systemctl restart kibana
systemctl restart elasticsearch
systemctl restart logstash
systemctl enable logstash
systemctl enable kibana
systemctl enable elasticsearch
```

Instalación los componentes ELKorrelator

Lo primero es copiar los ficheros del directorio ficheros_ELKorrelador a la máquina. En este directorio encontramos el software desarrollado, un instalador y reglas de correlación de ejemplo. Para la correcta instalación se debe utilizar el usuario root.
En primer lugar se debe tener instalado python2 y requests:

```
apt install python-minimal
apt-get install python-setuptools
sudo easy_install -U requests
```

A continuación debemos instalar Java para que pueda funcionar Logstash(componente detector)

```
apt install default-jre
```

Lo siguiente es instalar "build-essential" para poder compilar el orquestador, escrito en c:

```
apt-get install build-essential
```

Ahora instalamos Logstash, que hará las funciones de detector:

```
 wget https://artifacts.elastic.co/downloads/logstash/logstash-6.2.3.deb
dpkg -i logstash-6.2.3.deb
```

Ejecutamos el instalador, que se encargará de instalar el Orquestador y configurar el detector y los Correladores:

```
/bin/bash instalador.sh
```

Configuramos en el fichero base de los Correladores en que IP se encuentra el Elasticsearch al que tienen que consultar(en este caso 192.168.1.123), la IP en la que se encuentra el Logstash de enriquecimiento de normalización de eventos(en este caso 192.168.1.123) y el Detector(en este caso la misma máquina):

```
vi /usr/share/elkorrelator/bin/correlador.py
:%s/IP_ELASTICSEARCH/192.168.1.123/g
:%s/IP_LOGSTASH/192.168.1.123/g
:%s/IP_DETECTOR/127.0.0.1/g
```

Ahora limitamos el acceso al Detector con ufw:

```
ufw allow from 192.168.1.123 to any port 25555
ufw enable
```

Si se utilizan conexiones ssh para controlar remotamente el equipo también se debe añadir:

```
ufw allow from any to any port 22
ufw enable
```

Por último reiniciamos los servicios y los activamos para que arranquen automáticamente si se reinicia la máquina:

```
systemctl restart orquestador.service
systemctl restart logstash
systemctl enable orquestador.service
systemctl enable logstash
```

Testear instalación

Una vez que están todos los componentes instalados probamos desde la máquina ELK si las reglas de correlación funcionan correctamente:

```
mkdir -p /var/log/centralizador/
```

```
touch /var/log/centralizador/in.log
```

```
systemctl restart logstash
```

```
python test_RULES/R001_fichero.py >> /var/log/centralizador/in.log
python test_RULES/R002_fichero.py >> /var/log/centralizador/in.log
python test_RULES/R003_fichero.py >> /var/log/centralizador/in.log
python test_RULES/R004_fichero.py >> /var/log/centralizador/in.log
```

Ahora vamos a la interfaz de Kibana, accesible en el puerto 5601 de la máquina ELK, en este caso http://192.168.1.123:5601 , y configuramos un “index pattern”:

Ilustración 1: Elegimos logs- como index pattern*

Y elegimos el campo utilizado como “timestamp”:

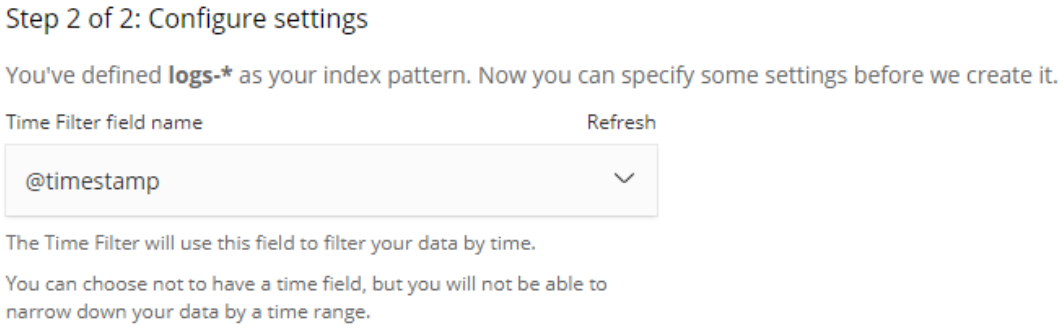

Ilustración 2: Elegimos el campo @timestamp

A continuación importamos las visualizaciones por defecto de ELKorrelaor para Kibana:

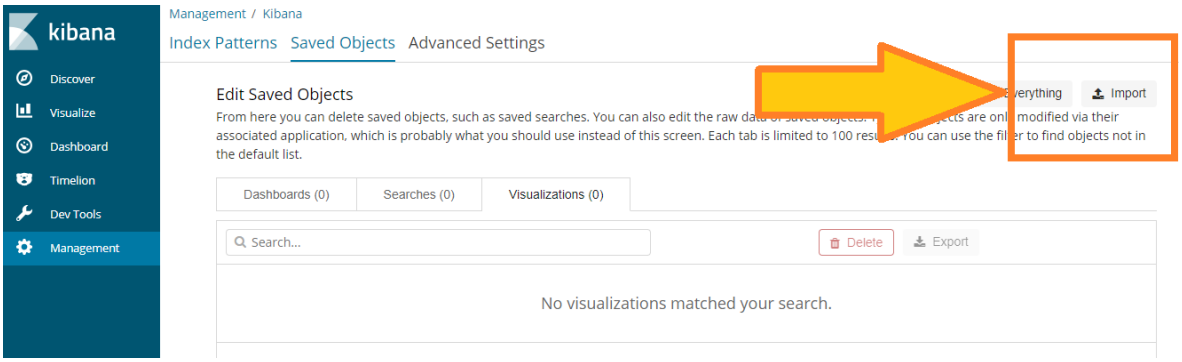

Ilustración 3: Importamos la configuración de Kibana

Por último abrimos el DASHBOARD con nombre "ELKorrelator", en el cual veremos diferentes gráficas generadas a partir de la información de las alertas de correlación:

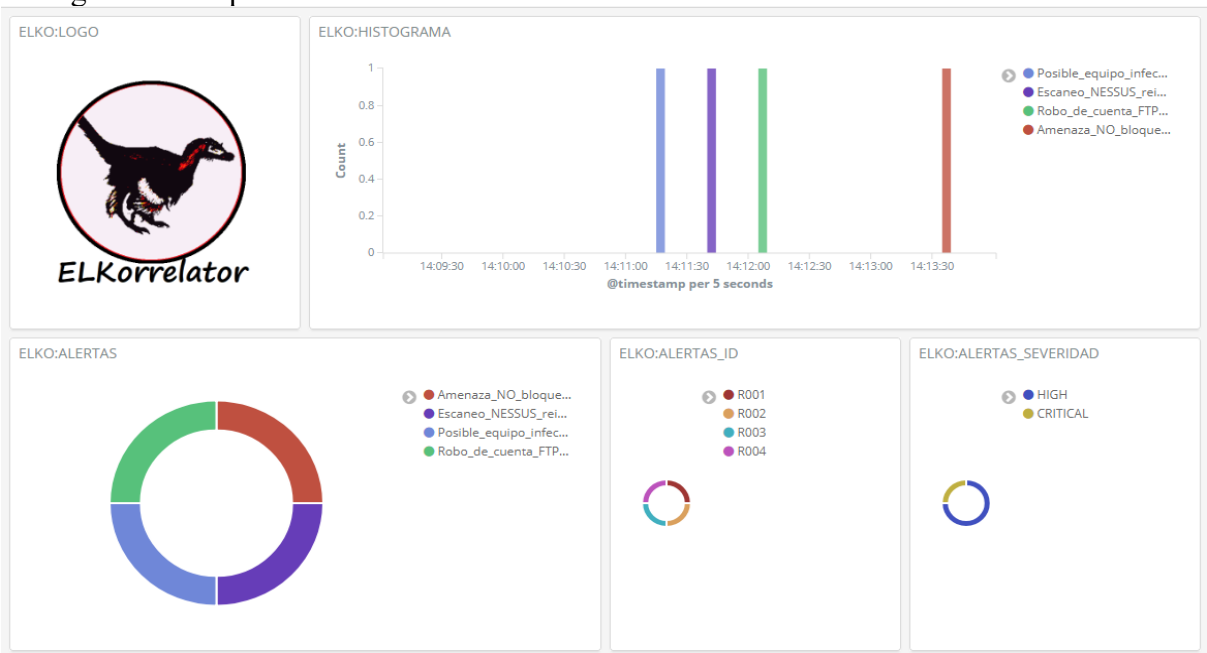

Ilustración 4: Dashboard con la información de las alertas de correlación