**Arkime**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Instalación y configuración**](#_g59i8ewd3ed3) **2**

[**3. Actividades**](#_6t9gvk46aslx) **7**

# **2. Instalación y configuración**

1. Actualizar el sistema (Ubuntu 20.04.3 LTS) e instalar algunos paquetes necesarios

sudo apt-get update

sudo apt-get upgrade

2. Arkime usa el motor de búsqueda ElasticSearch. Antes de instalarlo debemos agregarlo al repositorio

APT: wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch -- no-check-certificate | apt-key add -

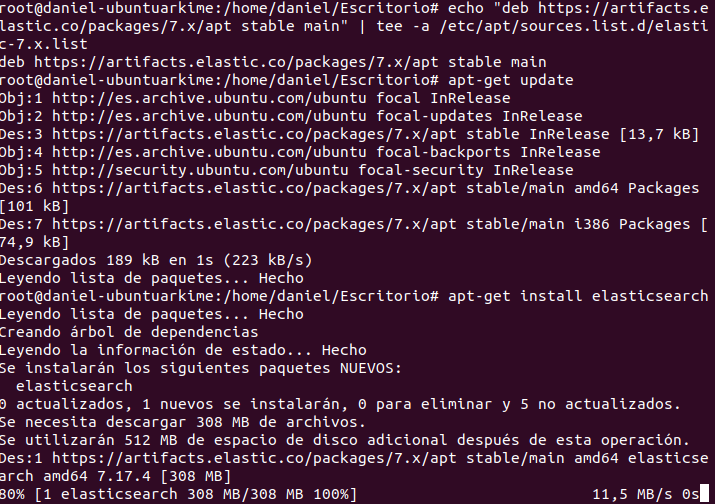
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | tee -a

/etc/apt/sources.list.d/elastic-7.x.list

Instalamos el paquete:

apt-get update

apt-get install elaticsearch



3. Editar el archivo de configuración de ElasticSearch para indicarle que la máquina virtual de Java que usa tendrá disponible hasta 1 GB de la memoria RAM:

Indicar los parámetros:

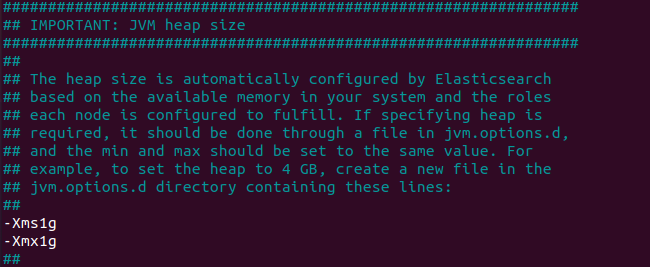
-Xms1g

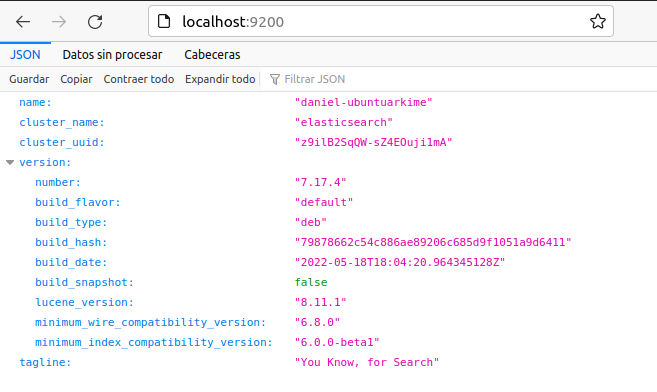
-Xmx1g

4. Configurar en el arranque el servicio elasticsearch y comprobar su estado:

systemctl enable [–now] elasticsearch

systemctl status elasticsearch



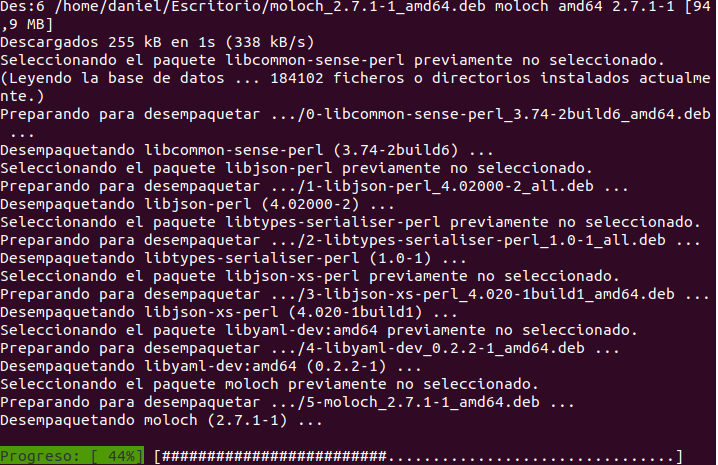


5. Descargar Arkime e instalar el paquete:

wget https://s3.amazonaws.com/files.molo.ch/builds/ubuntu-20.04/moloch\_2.7.1- 1\_amd64.deb

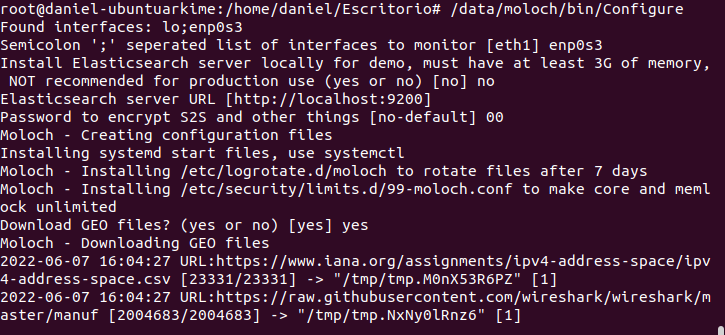
apt install ./moloch\_2.7.1-1\_amd64.deb





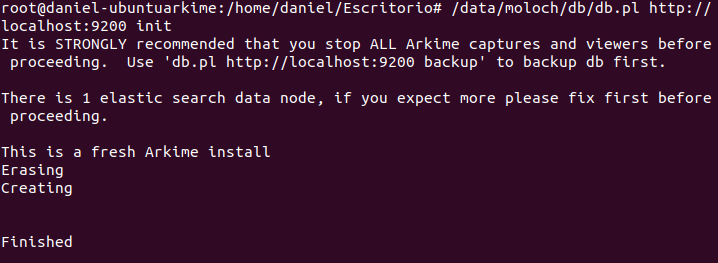
6. Para configurar Arkime debemos ejecutar el asistente solo la primera vez:

/data/moloch/bin/Configure



7. Seguidamente inicializaremos los datos de la BBDD de ElasticSearch:3

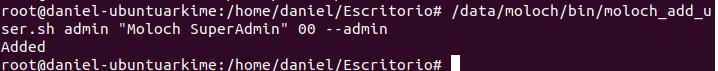
/data/moloch/db/db.pl http://localhost:9200 init



8. Crearemos una cuenta de usuario de tipo administrador para poder acceder a la web de Arkime.

Deberemos indicar la contraseña que tendrá el usuario admin:

/data/moloch/bin/moloch\_add\_user.sh admin "Moloch SuperAdmin" mipassword –admin



9. Seguidamente debemos iniciar los otros dos componentes de Arkime:

systemctl enable --now molochcapture

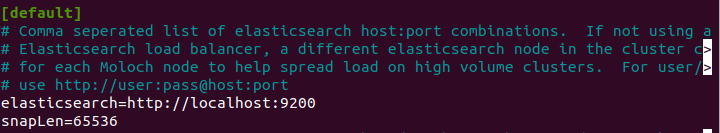
systemctl enable --now molochviewer

10. Luego editaremos el fichero de configuración .ini de Arkime para que el tamaño máximo de los paquetes capturados sea de 65536 Bytes (máximo de IPv4). Para ello modificamos el archivo

/data/moloch/etc/config.ini y añadimos la opción

[default]

snapLen=65536

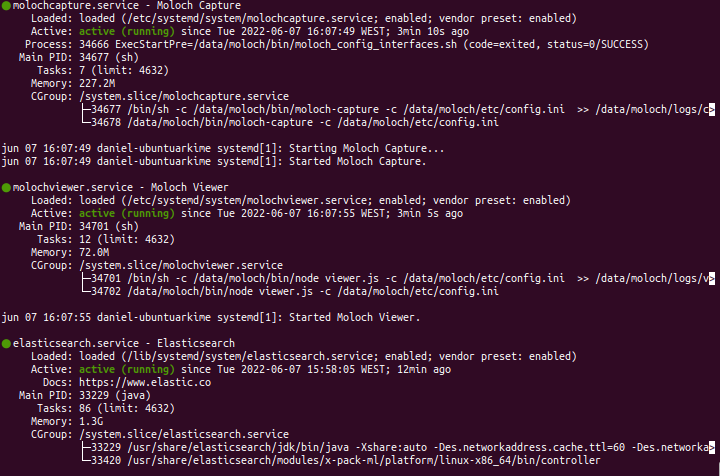


11. Podemos consultar el estado del servidor Arkime consultando el log:

tail -f /data/moloch/logs/viewer.log

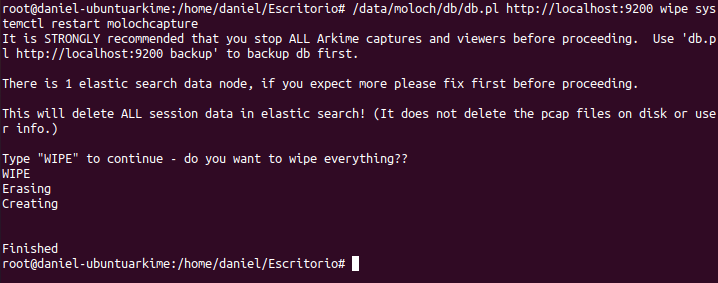
Además podemos hacerlo mediante:

systemctl status molochcapture molochviewer elasticsearch



12. El último paso será borrar los posibles datos que contuviera la BBDD de Arkime:

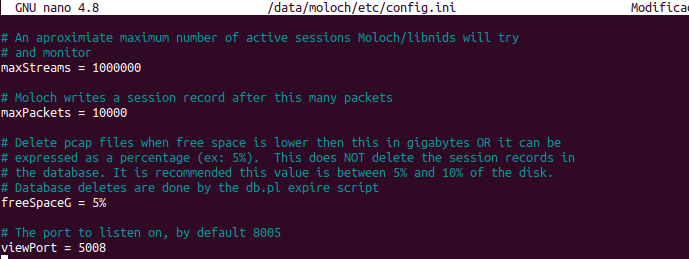
/data/moloch/db/db.pl http://localhost:9200 wipe systemctl restart molochcapture



# **3. Actividades**

1 - Configurar Arkime para que escuche por el puerto 5008 en lugar del puerto 8005 (archivo config.ini).

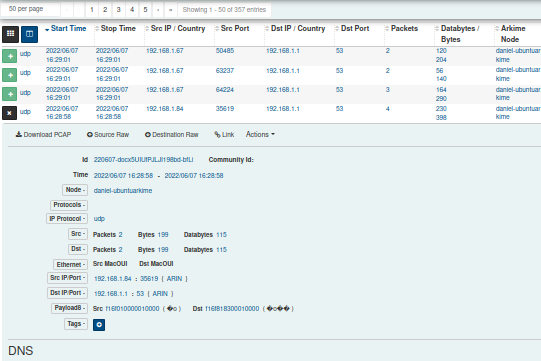
Insertar capturas de pantalla de los pasos más relevantes; así como de la visita final al panel de control web de Arkime.



2.- Capturar con Arkime el tráfico de red del equipo Linux. Se deberá generar como mínimo el siguiente tráfico de red desde el equipo Linux:

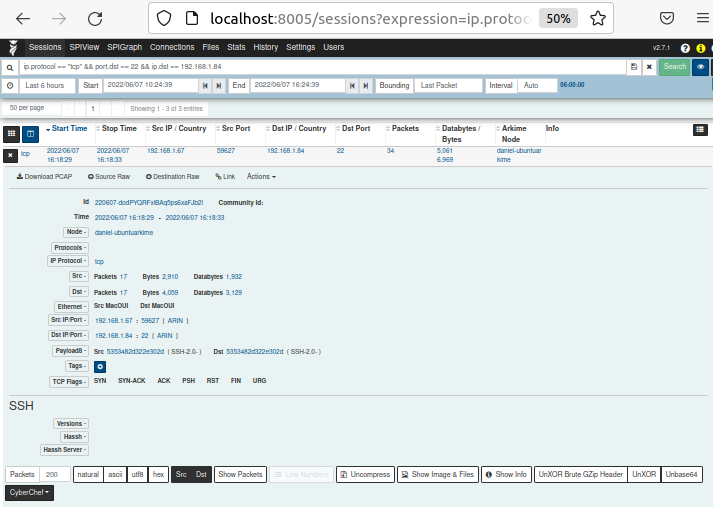
- Visitar algunas webs (HTTPs y HTTP) – curl

host.dns == EXISTS!



-Instalar un servidor SSH en el equipo Linux y conectar con él desde otro equipo – putty

ip.protocol == "tcp" && port.dst == 22 && ip.dst == Iplinux



3.- Generar con Arkime una gráfica de tipo tabla (SPIGraph) que muestre dos columnas (fields):

Las direcciones IP de destino (campo Dst IP) y el Hostname de los servidores web visitados (campo host.http).

Muestra 0 paquetes de 815.

