



Instalación y Configuración ELK + Snort

Seguridad en Redes

Docente: Ing. Gonzalo Vilanova

Alumna: Flavia De Rosa

Legajo: 158.739-0

Comisión: K4571

| | |
|-------------------------------|-----------|
| Requisitos Previos | 3 |
| ELK | 3 |
| Descarga | 3 |
| Instalación | 7 |
| Copia de seguridad (opcional) | 8 |
| Configuración | 8 |
| Metricbeat(opcional). | 13 |
| Filebeat (opcional) | 18 |
| Snort | 22 |
| Descarga | 22 |
| Instalación | 22 |
| Creación de reglas - Prueba | 26 |
| Inicio de servicio Snort | 26 |

Requisitos Previos

- Maquina virtual con SO WIN o LINUX
- jdk java (version compatible)
- RAM de 2GB aprox

Instalación - java jdk

Desde terminal ejecutamos el comando para la instalación de java

```
lubuntu@lubuntu:~$ sudo apt install openjdk-8-jdk
```

Verificamos la versión

```
lubuntu@lubuntu:~$ java -version
openjdk version "1.8.0_275"
OpenJDK Runtime Environment (build 1.8.0_275-8u275-b01-0ubuntu1~18.04-b01)
OpenJDK 64-Bit Server VM (build 25.275-b01, mixed mode)
```

ELK

Descarga

Hay 2 opciones

1. Agregando los repositorios y realizando la descarga por terminal

<https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html>

Ejecutando desde terminal con permisos de administrador (sudo su)

APT



To add the Beats repository for APT:

1. Download and install the Public Signing Key:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key
```

2. You may need to install the `apt-transport-https` package on Debian before proceeding:

```
sudo apt-get install apt-transport-https
```

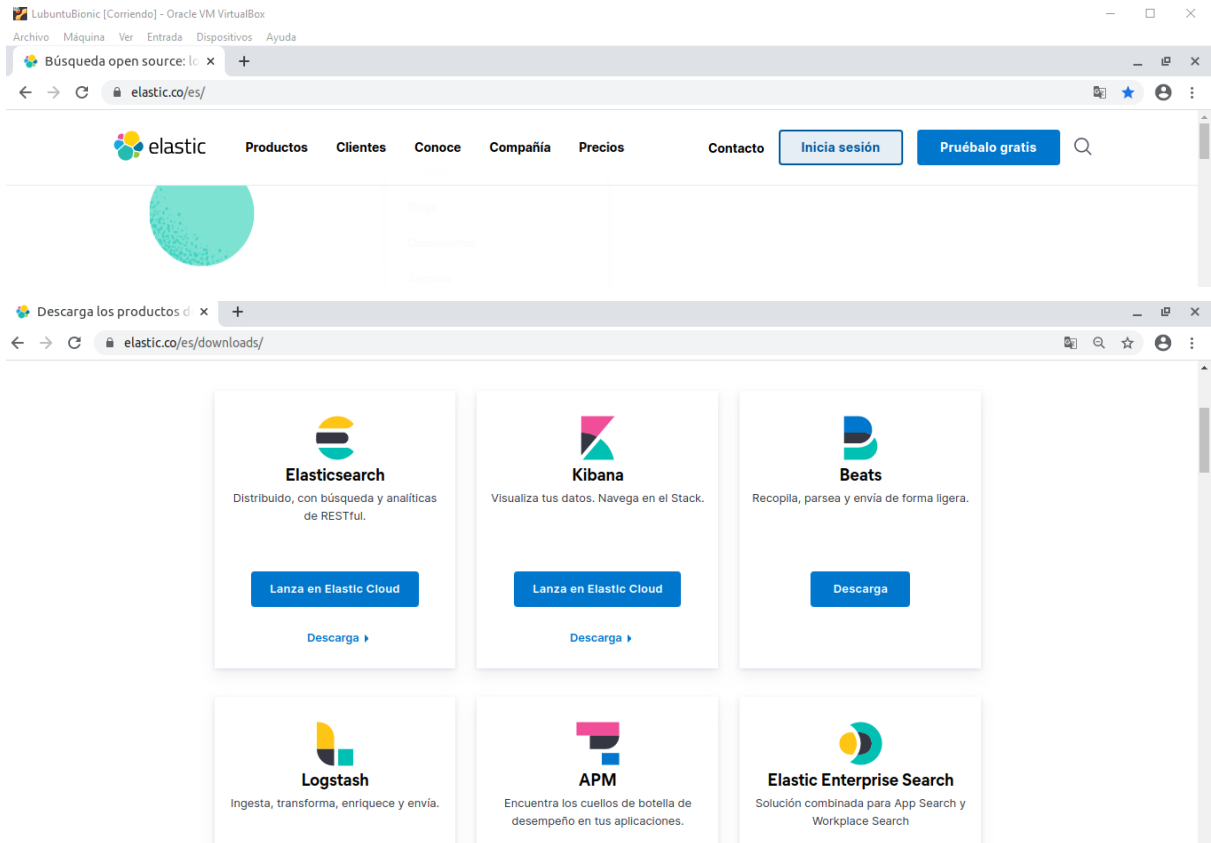
3. Save the repository definition to `/etc/apt/sources.list.d/elastic-7.x.list`:

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo
```

La ventaja de esta forma es que se puede actualizar la versión sin tener que descargar y descomprimir. Incluso si deseo agregar otro servicio de los disponibles lo puedo hacer con install, dado que ya está linkeado el link de los repositorios.

```
apt install kibana metricbeat openjdk-11-jre-headless logstash filebeat
```

2. Desde la página de elastic.co, elegimos la opción “Pruébalo gratis”



Descargamos los paquetes de:

1. Elasticsearch
2. Kibana
3. Logstash

1. Elastic Search.

Presionamos Descargar y elegimos la versión que corresponda nuestro sistema operativo (en nuestro caso LINUX_X86_64)

Download Elasticsearch

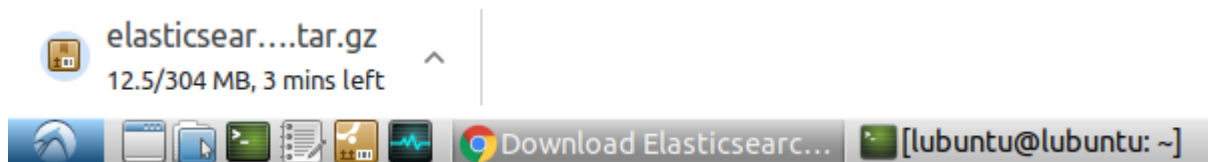
Want it hosted? Deploy on Elastic Cloud. [Get Started »](#)

Version: 7.10.0
Release date: November 11, 2020
License: [Elastic License](#)

Downloads:

| | |
|--------------------------------------|---------------------------------------|
| WINDOWS sha asc | MACOS sha asc |
| LINUX X86_64 sha asc | LINUX AARCH64 sha asc |
| DEB X86_64 sha asc | DEB AARCH64 sha asc |
| RPM X86_64 sha asc | RPM AARCH64 sha asc |
| MSI (BETA) sha asc | |

Comienza la descarga



Mientras se realiza la descarga se puede descargar Kibana.

Una vez descargado, hay que descomprimirlo para poder instalarlo.

```
lubuntu@lubuntu:~/Downloads$ tar -xzf elasticsearch-7.10.0-linux-x86_64.tar.gz
```

2. Kibana

Presionamos Descargar y elegimos la versión que corresponda nuestro sistema operativo (en nuestro caso LINUX_X86_64)

Download Kibana

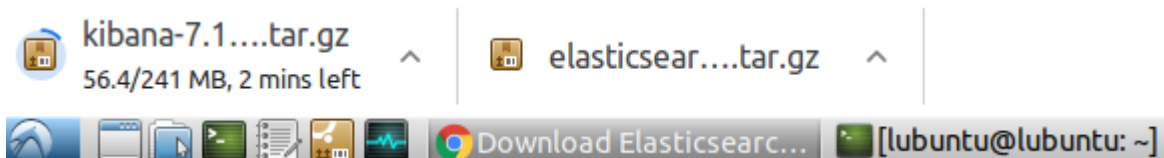
Want it hosted? Deploy on Elastic Cloud. [Get Started »](#)

Version: 7.10.0
Release date: November 11, 2020
License: [Elastic License](#)

Downloads:

| | |
|--------------------------------------|---------------------------------------|
| WINDOWS sha asc | MAC sha asc |
| LINUX 64-BIT sha asc | RPM 64-BIT sha asc |
| DEB 64-BIT sha asc | LINUX AARCH64 sha asc |

Comienza la Descarga



Mientras se realiza la descarga se puede descargar Logstash.

Una vez descargado, hay que descomprimirlo para poder instalarlo.

```
lubuntu@lubuntu:~/Downloads$ tar -xzvf kibana-7.10.0-linux-x86_64.tar.gz
```

3. Logstash.

Presionamos Descargar y elegimos la versión que corresponda nuestro sistema operativo (en nuestro caso LINUX_X86_64)

Download Logstash

Want to upgrade? We'll give you a hand. [Migration Guide »](#)

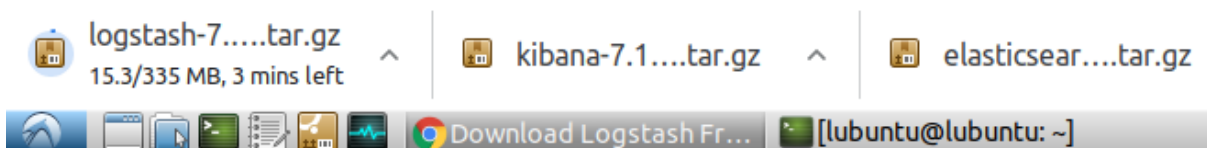
Version: 7.10.0

Release date: November 11, 2020

License: [Elastic License](#)

Downloads:

| | | | |
|------------------------------|---|-------------------------------|---|
| LINUX X86_64 | sha asc | LINUX AARCH64 | sha asc |
| MACOS | sha asc | WINDOWS | sha asc |
| DEB X86_64 | sha asc | DEB AARCH64 | sha asc |
| RPM X86_64 | sha asc | RPM AARCH64 | sha asc |



Una vez descargado, hay que descomprimirlo para poder instalarlo.

```
lubuntu@lubuntu:~/Downloads$ tar -xzvf logstash-7.10.0-linux-x86_64.tar.gz
```

Creamos un directorio tpSeguridadEnRedes y movemos los archivos descomprimidos de elasticsearch, kibana y logstash.

```
lubuntu@lubuntu:~/tpSeguridadEnRedes$ ls
elasticsearch-7.10.0  kibana-7.10.0-linux-x86_64  logstash-7.10.0
lubuntu@lubuntu:~/tpSeguridadEnRedes$
```

Instalación

1. Elasticsearch.

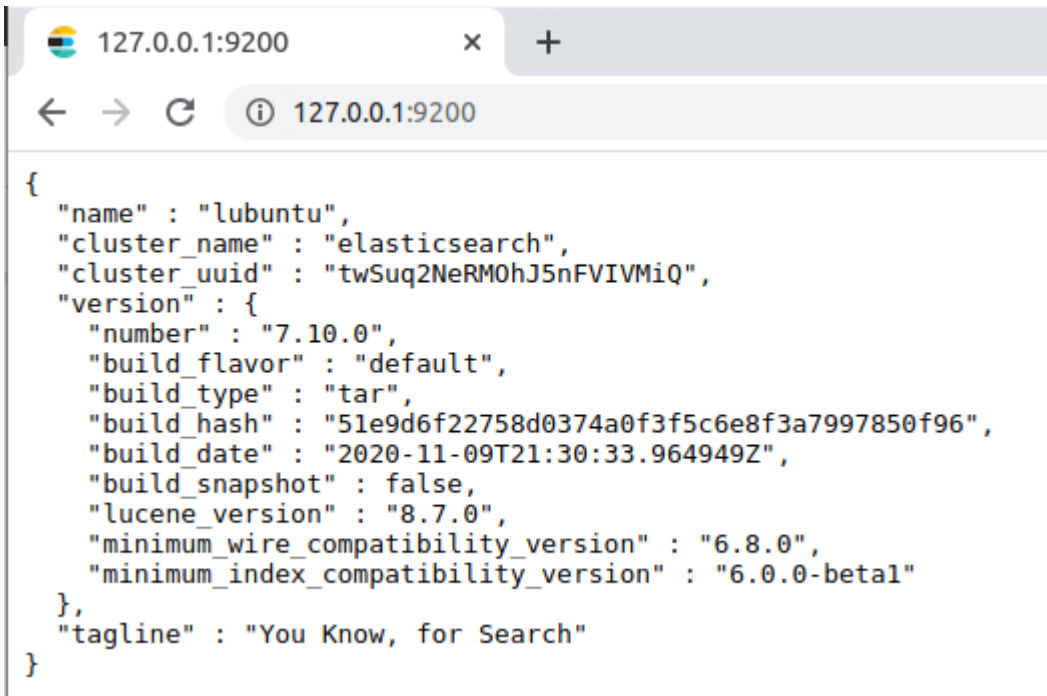
Abro una terminal y ubico la carpeta ../bin de los archivos descomprimidos de elasticsearch.

```
lubuntu@lubuntu:~/tpSeguridadEnRedes/elasticsearch-7.10.0/bin$
```

Ejecuto el archivo con el mismo nombre, con ./elasticsearch

```
lubuntu@lubuntu:~/tpSeguridadEnRedes/elasticsearch-7.10.0/bin$ ls
elasticsearch                  elasticsearch-saml-metadata
elasticsearch-certgen         elasticsearch-setup-passwords
elasticsearch-certutil        elasticsearch-shard
elasticsearch-cli             elasticsearch-sql-cli
elasticsearch-croneval        elasticsearch-sql-cli-7.10.0.jar
elasticsearch-env            elasticsearch-syskeygen
elasticsearch-env-from-file   elasticsearch-users
elasticsearch-keystore        x-pack-env
elasticsearch-migrate         x-pack-security-env
elasticsearch-node            x-pack-watcher-env
elasticsearch-plugin
lubuntu@lubuntu:~/tpSeguridadEnRedes/elasticsearch-7.10.0/bin$ ./elasticsearch
```

Una vez instalado, abro un navegador y accedo por localhost a 127.0.0.1:9200, donde 9200 es el puerto de escucha de elasticsearch y verifico que se encuentre a la escucha.



```
{
  "name" : "lubuntu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "twSuq2NeRM0hJ5nFVIVMiQ",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",
    "build_date" : "2020-11-09T21:30:33.964949Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Dejamos elasticsearch corriendo y hacemos lo mismo con kibana.

2. Kibana

Abro otra terminal y ubico la carpeta ../bin de los archivos descomprimidos de kibana

```
lubuntu@lubuntu:~/tpSeguridadEnRedes/kibana-7.10.0-linux-x86_64/bin$
```

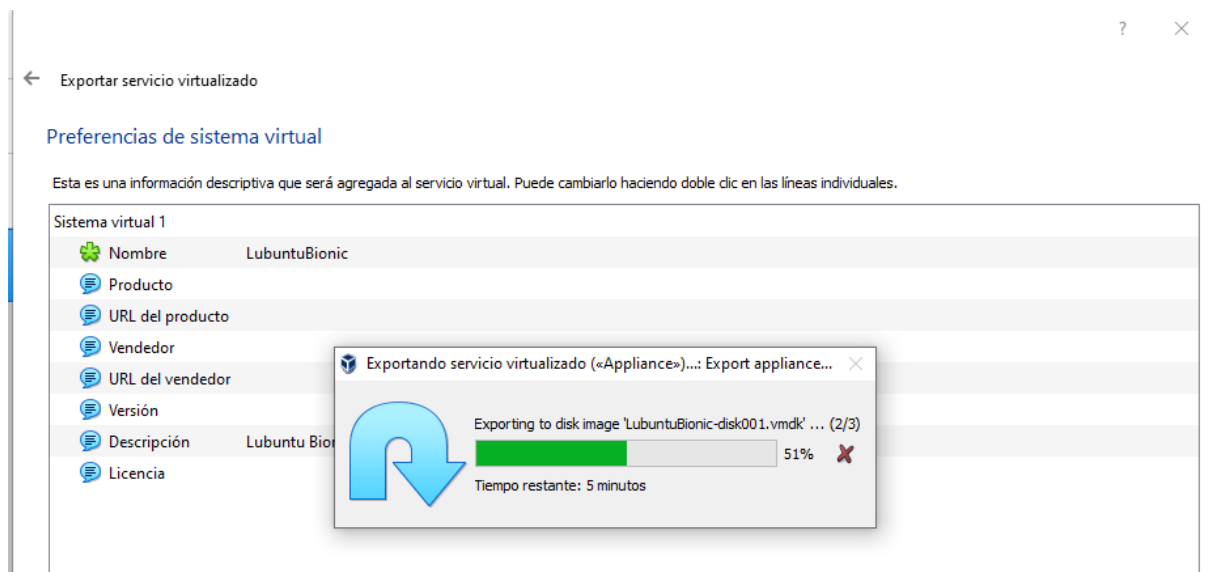
Ejecuto el archivo con el mismo nombre, con ./kibana

```
] Starting monitoring stats collection
log [14:23:38.868] [info][listening] Server running at http://localhost:5601
log [14:23:41.037] [info][server][Kibana][http] http server running at http://localhost:5601
```

Copia de seguridad (opcional)

Una vez realizada la instalación y antes de la configuración de los servicios, es recomendable que se realice una copia de seguridad, a través de la clonación de la vm actual.

Desde el menú de Virtualbox, Archivo > Exportar, seguir los pasos del asistente



Configuración

1. Elasticsearch

Abrimos el archivo de configuración de elasticsearch

```
root@lubuntu:/home/lubuntu# nano /etc/elasticsearch/elasticsearch.yml
```

Verificamos que los path sean los correctos.

Algunos cambios realizados

```
# ----- Network -----
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: 0.0.0.0
#
# Set a custom port for HTTP:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
```


- network.host: 0.0.0.0, para que el servidor de kibana escuche cualquier ip.
- http.port : 9200, es el puerto por defecto

```
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[:,1]"]
#
discovery.seed_hosts: 0.0.0.0
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
cluster.initial_master_nodes: ${HOSTNAME}
#
# For more information, consult the discovery and cluster formation module documentation.
#
```

- discovery.seed_host: 0.0.0.0 para evitar restricciones
- cluster.initial_master_nodes: \${HOSTNAME}, exige que sea un nombre como en node.name

Ejecutamos para que levante el servicio y cree los links.

```
root@lubuntu:/home/lubuntu# systemctl daemon-reload && systemctl enable elasticsearch.service
```

```
root@lubuntu:/home/lubuntu# systemctl daemon-reload && systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
root@lubuntu:/home/lubuntu#
```

Iniciamos servicio Elasticsearch

```
root@lubuntu:/home/lubuntu# systemctl start elasticsearch
```

systemctl start elasticsearch

Verificamos si la API Rest funciona correctamente o si aparece algún error con los logs.

systemctl status elasticsearch

```
root@lubuntu:/home/lubuntu# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-11-13 17:00:59 CET; 2min 2s ago
     Docs: https://www.elastic.co
   Main PID: 1069 (java)
    Tasks: 47 (limit: 2756)
   CGroup: /system.slice/elasticsearch.service
           └─1069 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -Xmx1g -Xms1g -XX:+UseG1GC -XX:-OmitStackTraceInFastThrow -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
           └─1254 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 13 17:00:33 lubuntu systemd[1]: Starting Elasticsearch...
Nov 13 17:00:59 lubuntu systemd[1]: Started Elasticsearch.
lines 1-12/12 (END)
```

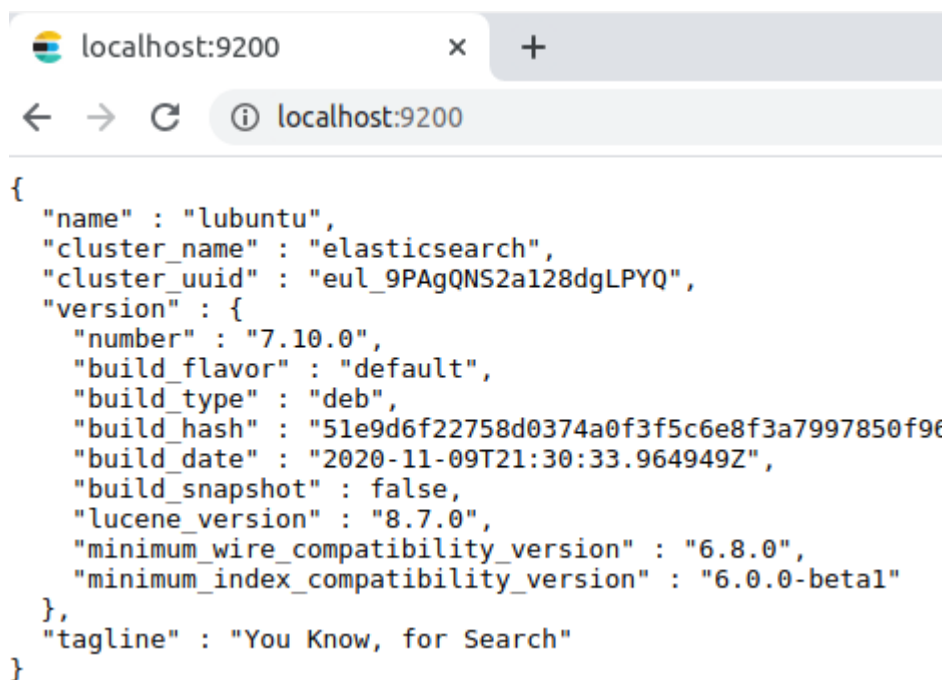
Prueba desde la vm

```

root@lubuntu:/home/lubuntu# curl -X GET "localhost:9200"
{
  "name" : "lubuntu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "eul_9PAgQNS2a128dgLPYQ",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",
    "build_date" : "2020-11-09T21:30:33.964949Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@lubuntu:/home/lubuntu#

```

Prueba desde el navegador



```

{
  "name" : "lubuntu",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "eul_9PAgQNS2a128dgLPYQ",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",
    "build_date" : "2020-11-09T21:30:33.964949Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

```

Se pueden ver los logs que genera elasticsearch en

```

root@lubuntu:/home/lubuntu# ls -ltr /var/log/elasticsearch
total 128
-rw-r--r-- 1 elasticsearch elasticsearch 2016 Nov 13 17:00 gc.log.00
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_deprecation.log
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_audit.json
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_deprecation.json
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_index_indexing_slowlog.log
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_index_search_slowlog.log
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_index_search_slowlog.json
-rw-r--r-- 1 elasticsearch elasticsearch 0 Nov 13 17:00 elasticsearch_index_indexing_slowlog.json
-rw-r--r-- 1 elasticsearch elasticsearch 34469 Nov 13 17:01 elasticsearch_server.json
-rw-r--r-- 1 elasticsearch elasticsearch 16541 Nov 13 17:01 elasticsearch.log
-rw-r--r-- 1 elasticsearch elasticsearch 62306 Nov 13 17:14 gc.log
root@lubuntu:/home/lubuntu#

```

2. Kibana

Abrimos el archivo de configuración de kibana

```
root@lubuntu:/home/lubuntu# nano /etc/kibana/kibana.yml
```

server.port : 5601, es el puerto por defecto de kibana

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601
```

elasticsearch.hosts: queda con la opción por defecto dado que están instalados en la misma pc.

```
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]
```

logging.dest: se define una ruta para que guarde los logs en un archivo dentro de kibana.

```
# Enables you to specify a file where Kibana stores log output.
logging.dest: /var/log/kibana/kibana.log
```

Ejecutamos para que levante el servicio y cree los links

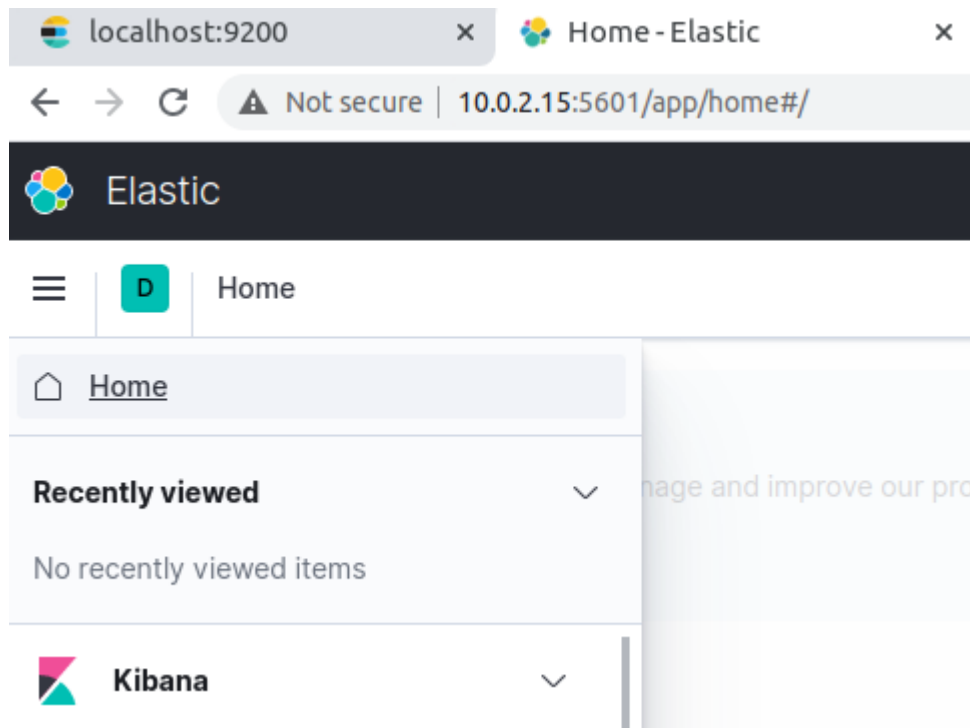
systemctl daemon-reload && systemctl enable kibana

Iniciamos servicio kibana

```
root@lubuntu:/home/lubuntu# systemctl start kibana
root@lubuntu:/home/lubuntu# systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-11-13 17:37:17 CET; 7s ago
     Main PID: 1749 (node)
       Tasks: 11 (limit: 2756)
      CGroup: /system.slice/kibana.service
              └─1749 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/node

Nov 13 17:37:17 lubuntu systemd[1]: Started Kibana.
lines 1-9/9 (END)
```

Desde el navegador, cargo la ip de la pc ubuntu y el puerto de kibana



Cuando iniciamos por primera vez a Kibana entrando con la ip de nuestra pc: el puerto de kibana, podemos habilitar opciones de seguridad que provee elasticsearch, las cuales vienen deshabilitadas por defecto.

Enable Elasticsearch security features X-Pack



When you use the basic and trial licenses, the Elasticsearch security features are disabled by default. To enable them:

1. Stop Kibana. The method for starting and stopping Kibana varies depending on how you installed it. For example, if you installed Kibana from an archive distribution (.tar.gz or .zip), stop it by entering `Ctrl-C` on the command line. See [Starting and stopping Kibana](#).
2. Stop Elasticsearch. For example, if you installed Elasticsearch from an archive distribution, enter `Ctrl-C` on the command line. See [Stopping Elasticsearch](#).
3. Add the `xpack.security.enabled` setting to the `ES_PATH_CONF/elasticsearch.yml` file.



The `ES_PATH_CONF` environment variable contains the path for the Elasticsearch configuration files. If you installed Elasticsearch using archive distributions (zip or tar.gz), it defaults to `ES_HOME/config`. If you used package distributions (Debian or RPM), it defaults to `/etc/elasticsearch`. For more information, see [Configuring Elasticsearch](#).

For example, add the following setting:

```
xpack.security.enabled: true
```

Estas opciones son configurables siempre y cuando no se tenga la version basica o de prueba de elasticsearch.

Metricbeat(opcional).

Permite recopilar métricas del sistema que vienen configuradas por defecto.

En nuestro caso está instalado en la misma pc donde esta elasticsearch y kibana (por eso queda localhost por defecto), pero si las métricas deben ser reportadas a otra pc, en el campo "host" se debe indicar la ip de la pc donde esta kibana y elasticsearch

```
setup.kibana:
# Kibana Host
# Scheme and port can be left out and will be set to the default $
# In case you specify and additional path, the scheme is required$
# IPv6 addresses should always be defined as: https://[2001:db8::$
host: "localhost:5601"
```

Las salidas pueden ser hacia elasticsearch o hacia logstash.

```
# ----- Elasticsearch Output ----
output.elasticsearch:
# Array of hosts to connect to.
hosts: ["localhost:9200"]
# Protocol - either `http` (default) or `https`.
#protocol: "https"
```

Ejecutamos

systemctl daemon-reload && systemctl enable metricbeat e iniciamos el servicio.

systemctl start metricbeat

systemctl status metricbeat

```
root@ubuntu:/home/ubuntu# systemctl status metricbeat
● metricbeat.service - Metricbeat is a lightweight shipper for metri
   Loaded: loaded (/lib/systemd/system/metricbeat.service; enabled;
   Active: active (running) since Fri 2020-11-13 18:02:37 CET; 6s ago
     Docs: https://www.elastic.co/products/beats/metricbeat
   Main PID: 2278 (metricbeat)
     Tasks: 8 (limit: 2756)
    CGroup: /system.slice/metricbeat.service
            └─2278 /usr/share/metricbeat/bin/metricbeat --environment

Nov 13 18:02:39 ubuntu metricbeat[2278]: 2020-11-13T18:02:39.607+01
Nov 13 18:02:39 ubuntu metricbeat[2278]: 2020-11-13T18:02:39.607+01
Nov 13 18:02:39 ubuntu metricbeat[2278]: 2020-11-13T18:02:39.608+01
Nov 13 18:02:39 ubuntu metricbeat[2278]: 2020-11-13T18:02:39.608+01
Nov 13 18:02:39 ubuntu metricbeat[2278]: 2020-11-13T18:02:39.610+01
Nov 13 18:02:40 ubuntu metricbeat[2278]: 2020-11-13T18:02:40.104+01
Nov 13 18:02:40 ubuntu metricbeat[2278]: 2020-11-13T18:02:40.584+01
Nov 13 18:02:40 ubuntu metricbeat[2278]: 2020-11-13T18:02:40.584+01
Nov 13 18:02:41 ubuntu metricbeat[2278]: 2020-11-13T18:02:41.384+01
Nov 13 18:02:41 ubuntu metricbeat[2278]: 2020-11-13T18:02:41.387+01
lines 1-19/19 (END)
```

Desde el dashboard de kibana, elijo del panel izquierdo

Discover> Crear índice (dado que vamos a crear datos propios y no vamos a usar los de ejemplo que provee kibana)

El patrón para el índice es metricbeat-* con @timestamp

Update your Elasticsearch indices individually or in bulk. [Learn more.](#)

☐ Include rollup indices ☐ Include hidden indices

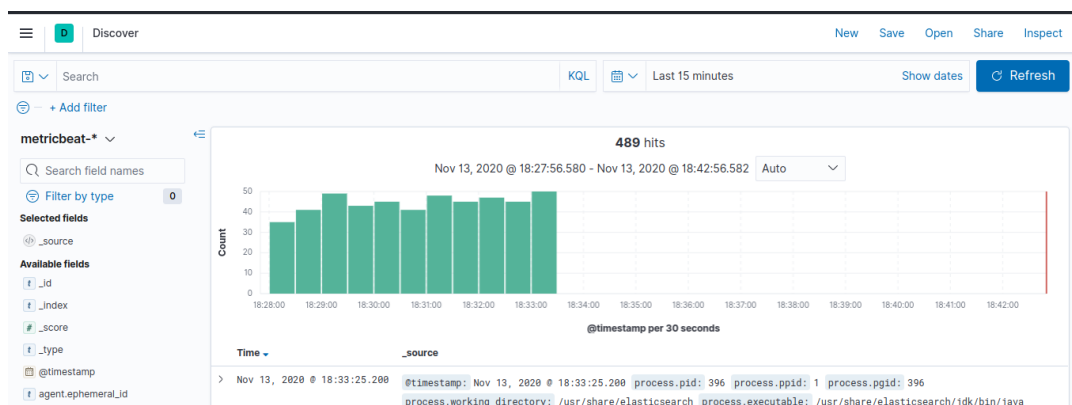
Search

Lifecycle status Lifecycle phase Reload indices

| Name | Health | Status | Primaries | Replicas | Docs count | Storage size | Data stream |
|-------------------------------------|--------|--------|-----------|----------|------------|--------------|-------------|
| metricbeat-7.10.0-2020.11.13-000001 | yellow | open | 1 | 1 | 1775 | 1mb | |

Rows per page: 10

Se recibieron 1775 líneas de logs(por ahora) con ese índice que creamos, con un espacio ocupado de 1mb.

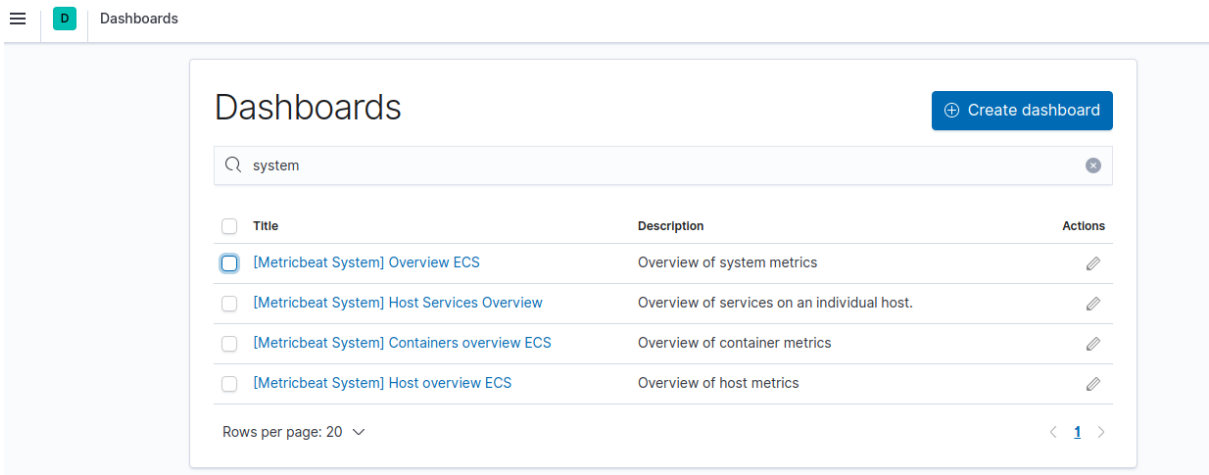
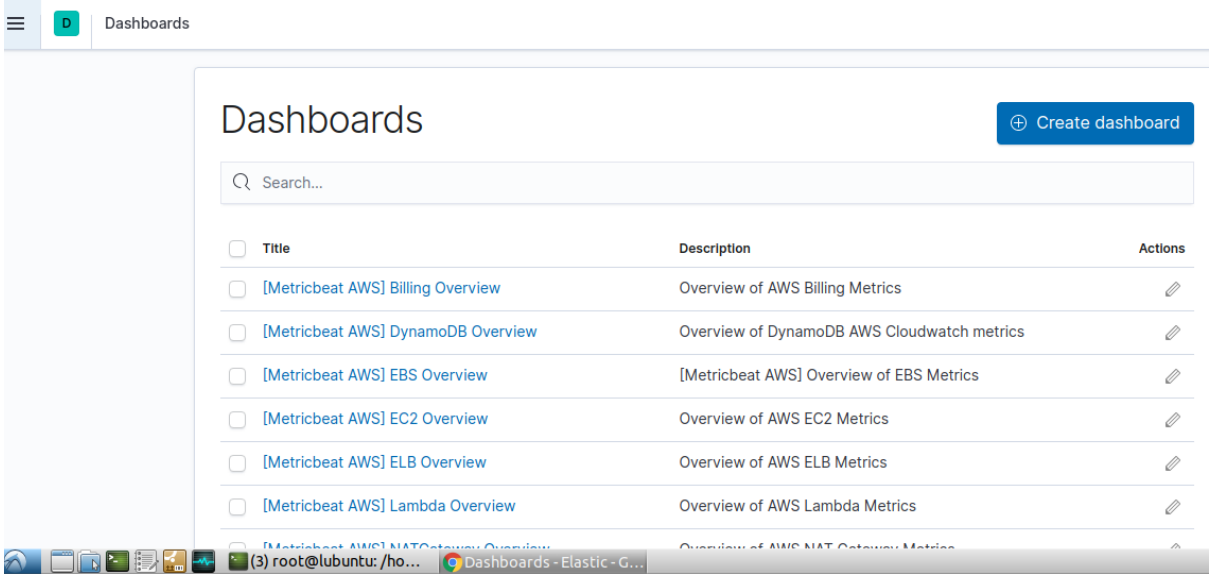


Creamos un dashboard para visualizar las capturas de los datos indexados.

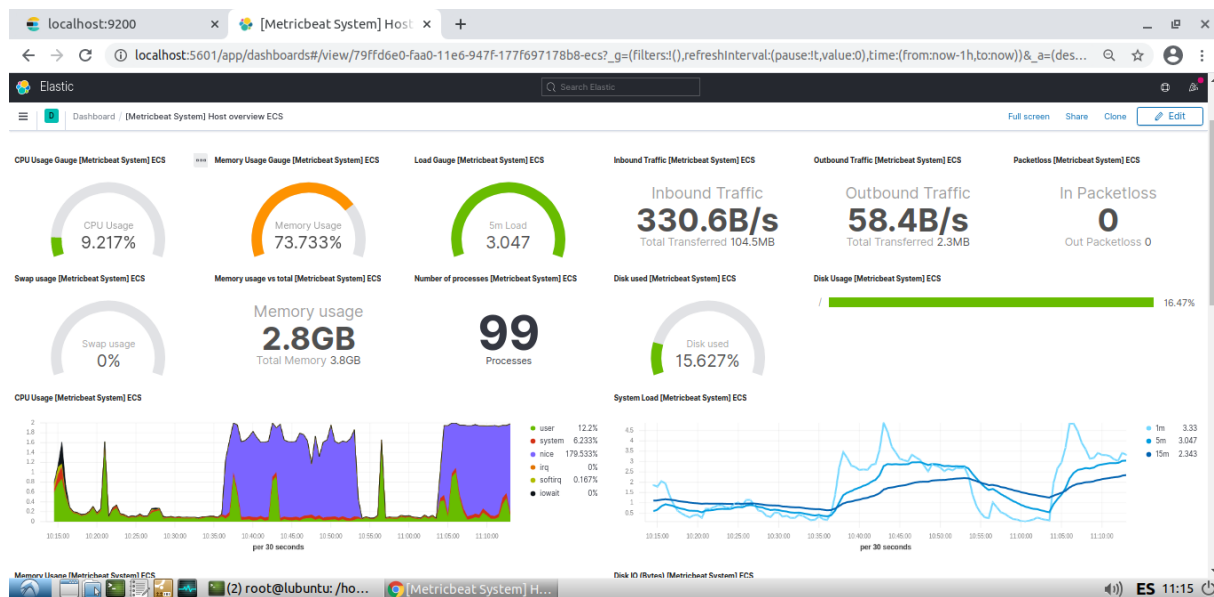
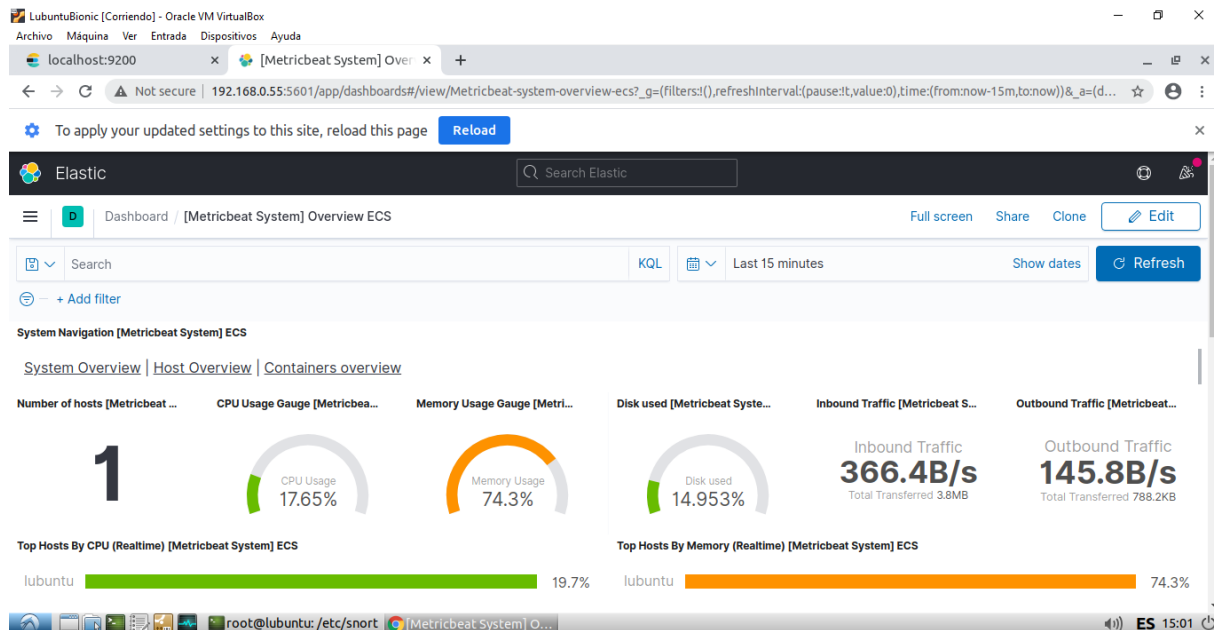
Realizamos un setup a metricbeat para que se puedan traer datos para generar un dashboard a kibana.

```
root@lubuntu:/home/lubuntu# systemctl stop metricbeat
root@lubuntu:/home/lubuntu# metricbeat setup -e
```

Luego de realizar el setup de metricbeat por terminal, vamos a la web y creamos un dashboard, eligiendo alguno de los que aparecen en la lista



El resultado corresponde a la información de un nodo



3. Logstash

Archivo de configuración (/etc/logstash/logstash.yml)

```
# ----- Data path -----  
#  
# Which directory should be used by logstash and its plugins  
# for any persistent needs. Defaults to LOGSTASH_HOME/data  
#  
path.data: /var/lib/logstash  
#  
# ----- Pipeline Settings -----  
#
```



```
#
pipeline.ordered: auto
#
# ----- Pipeline Configuration Settings -----
#
# Where to fetch the pipeline configuration for the main pipeline
#
path.config: /etc/logstash
#
# Pipeline configuration string for the main pipeline
#
# config.string:
#
# At startup, test if the configuration is valid and exit (dry run)
#
config.test_and_exit: true
#
```

```
# log.level: info
path.logs: /var/log/logstash
#
# ----- Other Settings ---
```

```
# ----- HTTP API Settings -----
# Define settings related to the HTTP API here.
#
# The HTTP API is enabled by default. It can be disabled, but features that rely
# on it will not work as intended.
http.enabled: true
#
```

Necesita de una máquina virtual de java

Una vez verificada la versión de java (**java --version**), se pasa a configurar logstash

systemctl daemon-reload && systemctl enable logstash

Se ejecuta el comando desde terminal para establecer un filtro que capture la entrada y salida sea por consola pero con formato json, en logs de Logstash.

```
root@lubuntu:/home/lubuntu# /usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }'
```

/usr/share/logstash/bin/logstash -e "input { stdin { } } output { stdout { } }"

```
root@lubuntu:/home/lubuntu# /usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }' --path.settings=/etc/logstash
```

Este comando me permite saber en la línea del .yml donde esta el error. Si el comando anterior funciona, no es necesario ejecutar este último.

/usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }' --path.settings=/etc/logstash

```
root@lubuntu: /home/lubuntu
File Edit Tabs Help
root@lubuntu:/home/lubuntu# systemctl start elasticsearch
root@lubuntu:/home/lubuntu# systemctl start kibana
root@lubuntu:/home/lubuntu# /usr/share/logstash/bin/logstash 'input { stdin { }
} output { stdout { } }'
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in ve
rsion 9.0 and will likely be removed in a future release.
```

```
[INFO ] 2020-11-19 22:19:50.849 [Agent thread] agent - Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipeline
s=>[]}
[INFO ] 2020-11-19 22:19:51.496 [Api Webserver] agent - Successfully started Logstash API endpoint {:port=>9600}
hola
{
  "message" => "hola",
  "@timestamp" => 2020-11-19T21:19:59.296Z,
  "host" => "lubuntu",
  "@version" => "1"
}
```

Esto indica que Logstash está configurado correctamente.

systemctl start logstash

Filebeat (opcional)

Debido a que se presentaron varios problemas al probar logstash con snort, se decide instalar otro de los servicios de elastic.co, para probar los eventos desde la misma pila de servicios y después incorporar el IDS Snort.

```
setup.kibana:
# Kibana Host
# Scheme and port can be left out and will be set to the default (http and 5601)
# In case you specify an additional path, the scheme is required: http://localhost:5601/path
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
host: "localhost:5601"
```

El output puede ser a elasticsearch o a logstash, en principio lo probamos desde elastic

```
# ----- Elasticsearch Output -----
output.elasticsearch:
# Array of hosts to connect to.
hosts: ["localhost:9200"]

# Protocol - either `http` (default) or `https`.
#protocol: "https"

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
#username: "elastic"
#password: "changeme"

# ----- Logstash Output -----
#output.logstash:
# The Logstash hosts
#hosts: ["localhost:5044"]
```

Se testea la configuración de filebeat

```
root@lubuntu:/home/lubuntu# filebeat test config -e
```

```
2020-11-24T11:20:54.008-0300 INFO eslegclient/connection.go:99 elasticsearch url: http://localhost:9200
2020-11-24T11:20:54.009-0300 INFO [publisher] pipeline/module.go:113 Beat name: lubuntu
Config OK
```

Se cargan los dashboard de filebeat (deben estar los servicios de elasticsearch y kibana funcionando)

```
root@lubuntu:/home/lubuntu# filebeat setup -e
```

```
2020-11-24T11:28:34.040-0300 INFO [esclientleg] eslegclient/connection.go:314 Attempting to
7.10.0
2020-11-24T11:28:34.040-0300 INFO cfgfile/reload.go:262 Loading of config files completed.
Loaded Ingest pipelines
```

```
root@lubuntu:/home/lubuntu# filebeat setup --dashboards
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

Copiamos archivos de log (probamos con uno de snort) para configurar los pipelines de logstash y la ingesta de filebeat.

Generamos el servicio filebeat

```
root@lubuntu:/home/lubuntu# systemctl daemon-reload && systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
root@lubuntu:/home/lubuntu#
```

Los servicios funcionan y se ven los nuevos dashboard de filebeat desde kibana.

```
# Change to true to enable this input configuration.
enabled: true
```

Se reconfigura la salida de filebeat para que sea con Logstash en lugar de elasticsearch.

```
# ----- Logstash Output -----
output.logstash:
# The Logstash hosts
hosts: ["localhost:5044"]
```

Se agrega el path donde esta el archivo de log de ingesta

```
# Paths that should be crawled and fetched. Glob based paths.
paths:
# - /var/log/*.log
#- c:\programdata\elasticsearch\logs\*
- /home/lubuntu/alert.log
```

Creación de pipeline (fichero de ingesta)

```
root@lubuntu: /home/lubuntu
File Edit Tabs Help
GNU nano 2.9.3 /etc/logstash/conf.d/ag2.conf

input {
  beat {
    port => "5044"
  }
}

filter {
  grok {
    match => {"message" => "%{COMBINEDAPACHELOG}"}
  }
  geoip {
    source => "clientip"
  }
}

output {
  elasticsearch {
    hosts => [ "localhost:9200", "192.168.0.55:9200" ]
    #manage_template => false
    #index => "logstash-%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
}
```

Se prueba configuración

```
/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/ag2.conf --config.test_and_exit
```

```
/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/snort-03.conf
--config.test_and_exit
```

```
Configuration OK
[INFO ] 2020-11-24 12:23:17.865 [LogStash::Runner] runner - Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logs
tash
root@lubuntu:/home/lubuntu#
```

Se recarga la configuración

```
/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/ag2.conf
--config.reload.automatic
```

```
/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/snort-03.conf
--config.reload.automatic
```

Se habilita el módulo system y logstash de filebeat.

```
root@lubuntu:/home/lubuntu# sudo filebeat modules enable system
Enabled system
root@lubuntu:/home/lubuntu# sudo filebeat modules enable logstash
Enabled logstash
root@lubuntu:/home/lubuntu# filebeat modules list
Enabled:
logstash
system
```

Se prueba configuración de filebeat con Logstash

```
filebeat -c filebeat.yml test output
```

```

root@lubuntu:/home/lubuntu# filebeat -c filebeat.yml test output
logstash: localhost:5044...
connection...
  parse host... OK
  dns lookup... OK
  addresses: 127.0.0.1
  dial up... ERROR dial tcp 127.0.0.1:5044: connect: connection refused
root@lubuntu:/home/lubuntu#

```

Verifico puertos de escucha

```

root@lubuntu:/home/lubuntu# netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53          0.0.0.0:*                LISTEN      281/systemd-resolve
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      372/sshd
tcp        0      0 0.0.0.0:5601           0.0.0.0:*                LISTEN      9682/node
tcp6       0      0 :::9200                 :::*                    LISTEN      9470/java
tcp6       0      0 :::9300                 :::*                    LISTEN      9470/java
tcp6       0      0 :::22                   :::*                    LISTEN      372/sshd
root@lubuntu:/home/lubuntu# nano /etc/logstash/logstash.yml

```

Snort

Antes de instalar Snort, me aseguro la interfaz y la IP que corresponde a la pc a la que le quiero configurar el IDS.

Verificamos con ifconfig la ip y la interfaz de la máquina linux y el gateway de la pc anfitriona, para configurarlo mientras se descargo la versión de Snort.

```
root@lubuntu:/home/lubuntu# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.55  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 2800:2121:5400:43b:ea57:4b5c:85b3:79ff  prefixlen 128  scopeid 0x0
```

Descarga

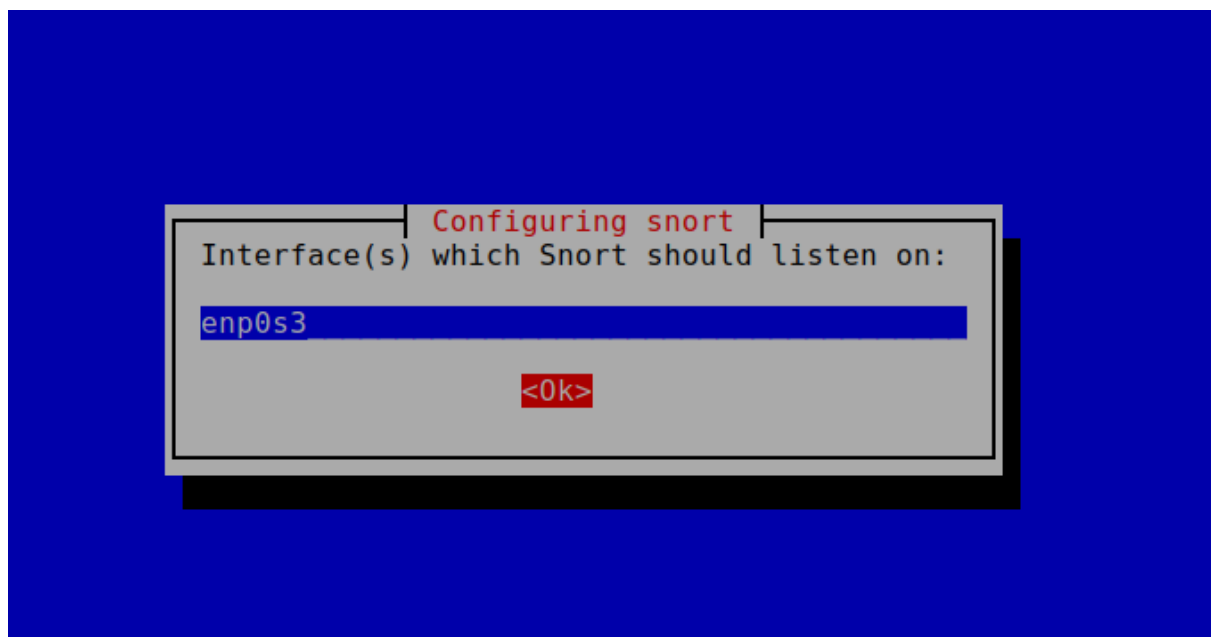
Desde una terminal y con permisos de administrador ejecuto **apt install snort**.

También se puede descargar de la página snort.org, los archivos comprimidos.

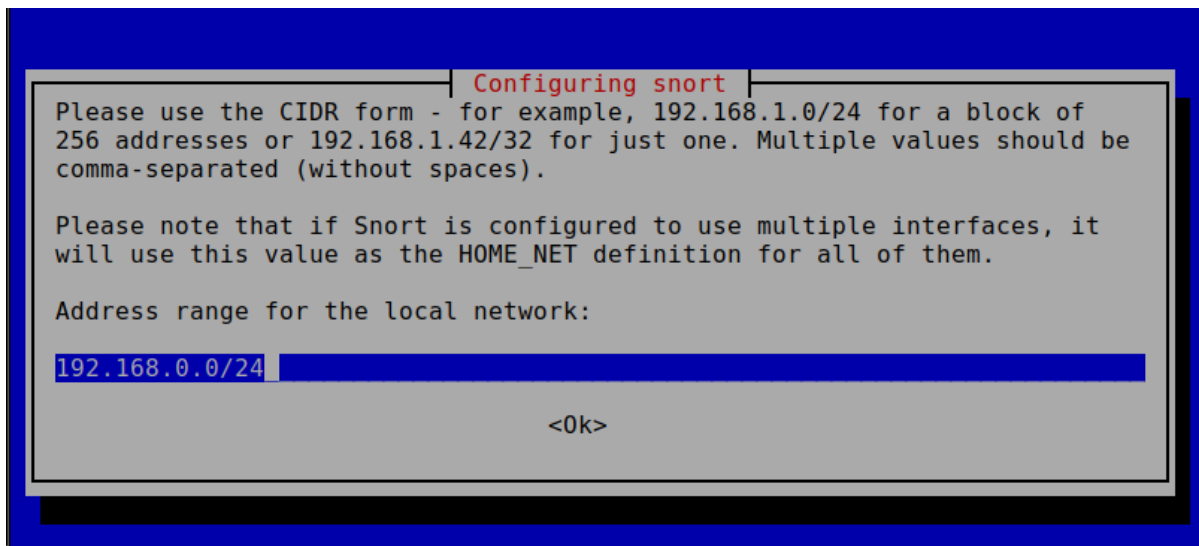
Instalación

Seguimos los pasos del asistente de instalación

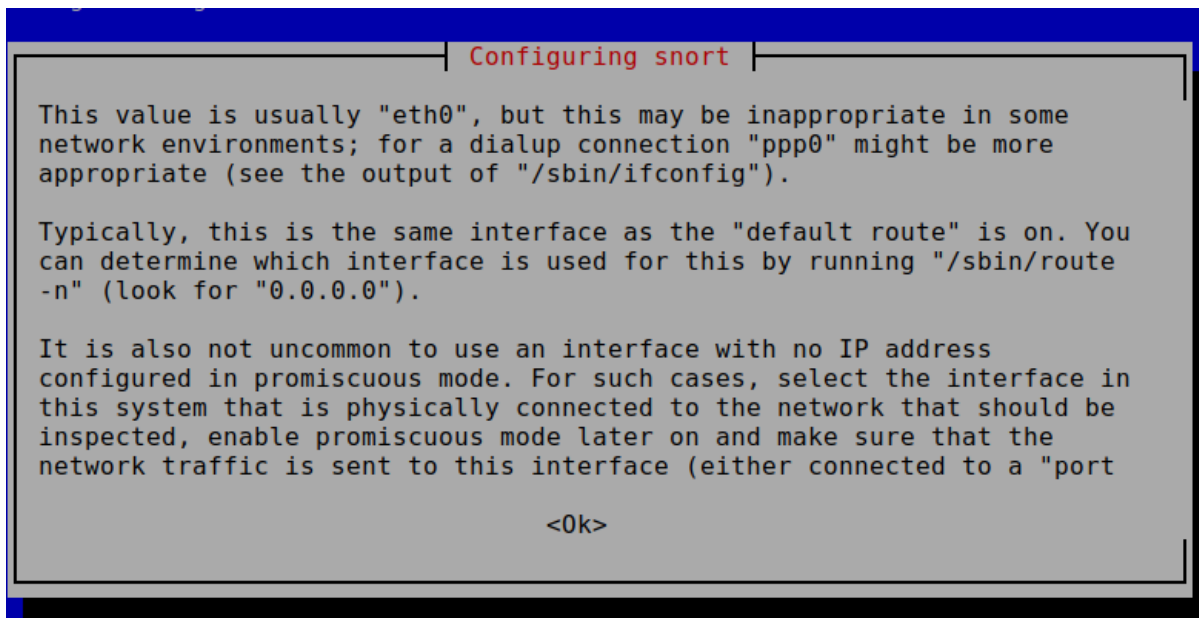
1. Escribir el nombre de la interfaz a la que corresponde la ip de la pc Linux



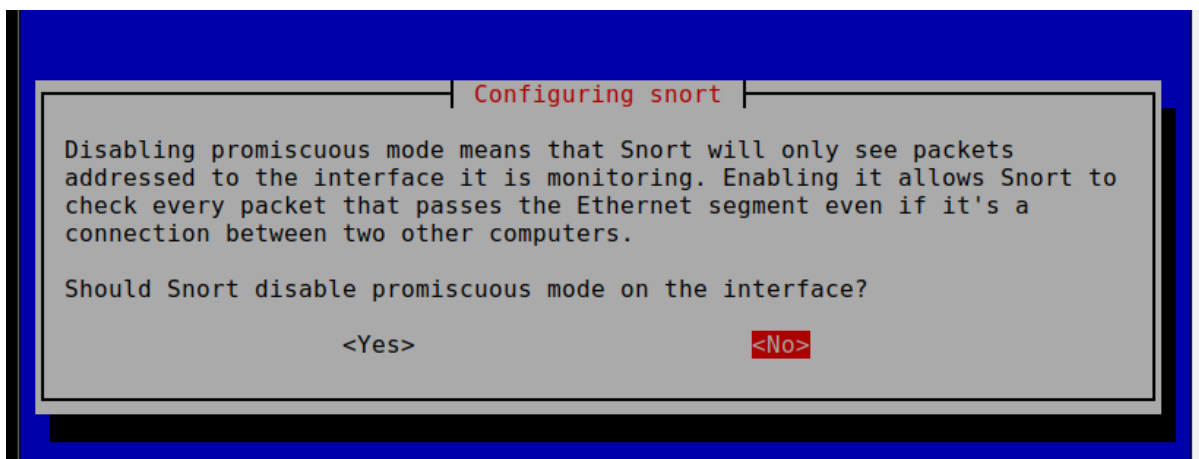
2. Escribir el rango de ips para las redes que analizara Snort,



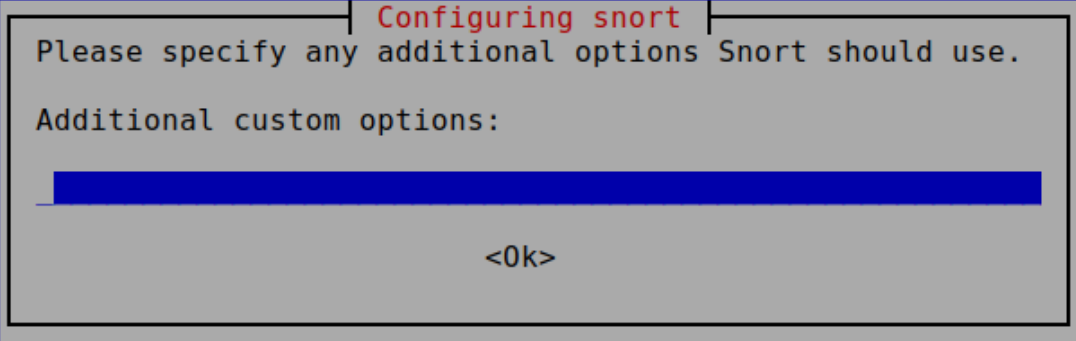
3. Este paso es solo informativo, se presiona Ok.



4. Se deja activado el modo promiscuo de Snort



5. No se agrega ninguna opción adicional



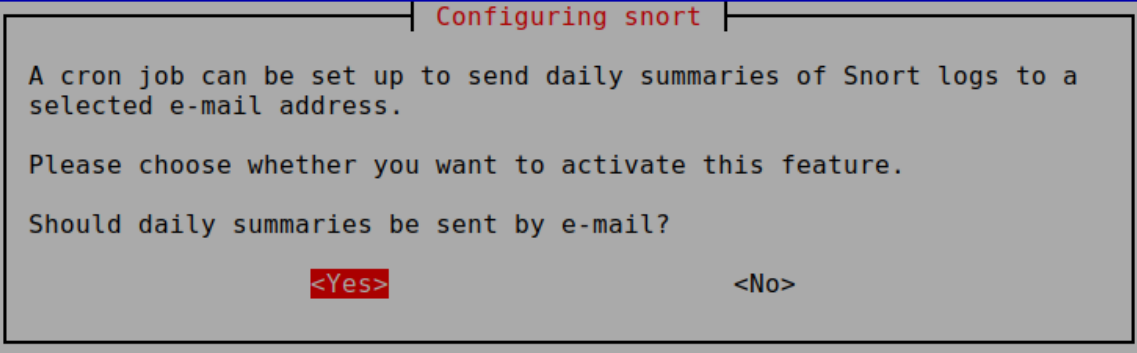
Configuring snort

Please specify any additional options Snort should use.

Additional custom options:

<Ok>

6. Se acepta recibir notificaciones por mail



Configuring snort

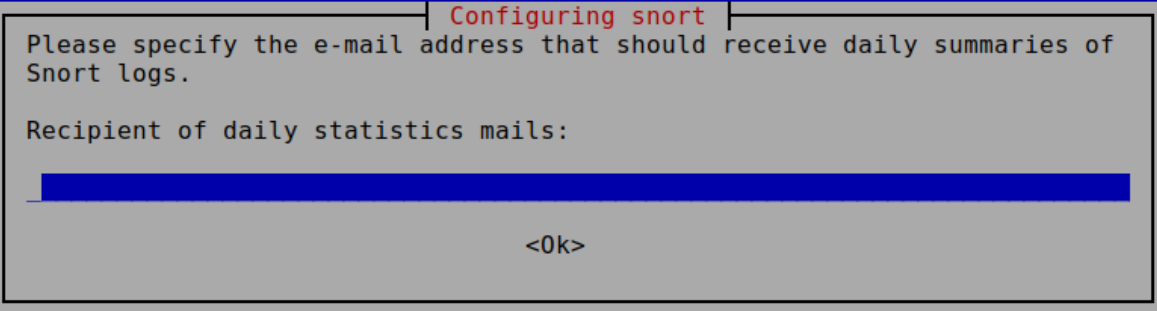
A cron job can be set up to send daily summaries of Snort logs to a selected e-mail address.

Please choose whether you want to activate this feature.

Should daily summaries be sent by e-mail?

<Yes> **<No>**

7. Se especifica la dirección de correo



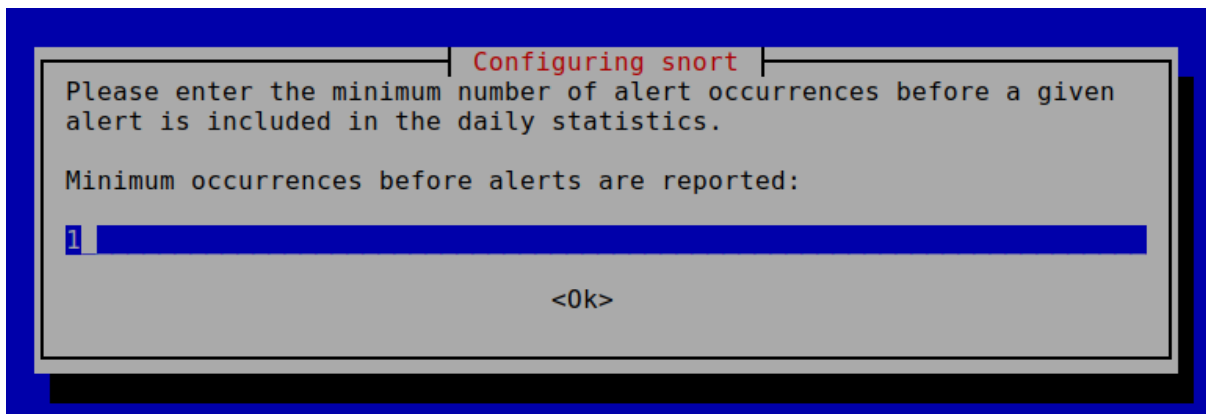
Configuring snort

Please specify the e-mail address that should receive daily summaries of Snort logs.

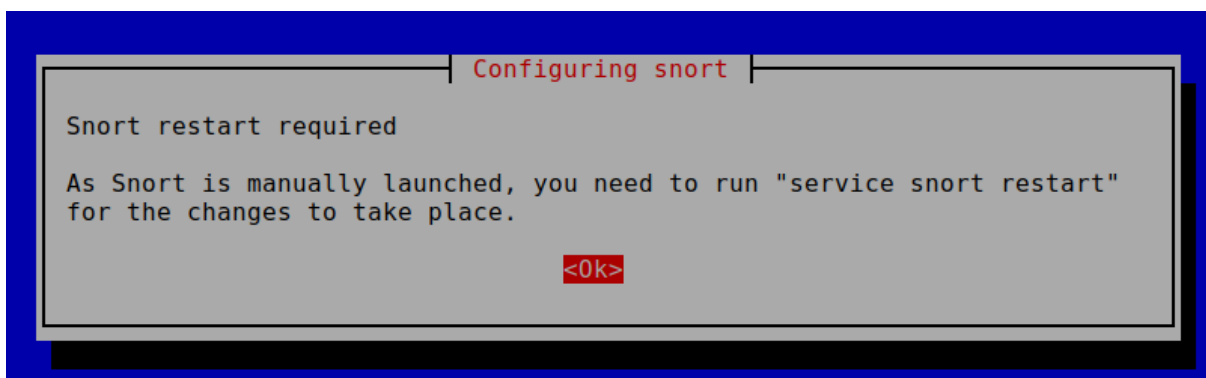
Recipient of daily statistics mails:

<Ok>

8. Las alertas se configuran para que aparezcan a la primera ocurrencia.



9. Como se configura el reinicio manual, deberá hacerse después del asistente



Una vez finalizada la instalación, se accede a /etc/snort/snort.conf y se agregan los datos de configuración para los logs

```
# config logdir:
config logdir: /etc/snort/log/
output alert_fast: alert.log
output unified2: filename snort.log,limit 64
config set_gid: 504
config set_uid: 504
config snaplen: 1500
```

Desde la terminal, se reinicia Snort.

```
root@lubuntu:/home/lubuntu# /etc/init.d/snort restart
root@lubuntu:/home/lubuntu# dpkg-reconfigure snort
[ ok ] Stopping snort (via systemctl): snort.service.
root@lubuntu:/home/lubuntu# /etc/init.d/snort restart
[ ok ] Restarting snort (via systemctl): snort.service.
root@lubuntu:/home/lubuntu#
```

Creación de reglas - Prueba

Para la creación de reglas, se accede al archivo de reglas locales de snort

```
root@lubuntu:/home/lubuntu# nano /etc/snort/rules/local.rules
```

Se crea una regla para el protocolo ICMP, con un mensaje desde cualquier puerto.

```
GNU nano 2.9.3 /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp 192.168.0.1/24 any -> any any (msg:"Alguien esta haciendo ping";sid:19910316;rev:1;)
```

Se accede al archivo de configuración de Snort, para modificar algunos parámetros y verificar la regla creada

```
root@lubuntu:/home/lubuntu# nano /etc/snort/snort.conf
```

Se modifica la ipvar HOME_NET para que apunte a la ip del gateway y el ipvar EXTERNAL_NET con la ip de la pc anfitriona con windows.

```
GNU nano 2.9.3 /etc/snort/snort.conf Modified
# Step #1: Set the network variables.  For more information, see README.variables
#####
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.0.1/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET 192.168.0.117
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Inicio de servicio Snort

Desde una terminal con permisos de administrador.

```
cd /etc/snort/
```

```
snort -A console -c /etc/snort/snort.conf -i enp0s3
```

```

--== Initialization Complete ==--

o"~
'~~~
-*)> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT DETECTION ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Commencing packet processing (pid=1174)

```

Se abre una terminal en la pc anfitriona y se ejecuta un ping para ver si Snort lo detecta por la regla creada en el archivo.

```

root@lubuntu:/home/lubuntu# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.55 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 2800:2121:5400:43b:ea57:4b5c:85b3:79ff prefixlen 128 scopeid 0x0

```

```

C:\Windows\system32>ping 192.168.0.55

Haciendo ping a 192.168.0.55 con 32 bytes de datos:
Respuesta desde 192.168.0.55: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.55: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.55: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.55: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.55:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

```

Desde la pc Linux vemos la captura por consola de los paquetes enviados, con los parámetros y el mensaje que agregamos en la regla.

```
Preprocessor Object: SI-PF version 1.0 - Build 1
Commencing packet processing (pid=1307)
11/14-00:14:32.459589  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:32.459589  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:32.459589  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:32.459604  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.55 -> 192.168.0.117
11/14-00:14:33.470233  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:33.470233  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:33.470233  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:33.470255  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.55 -> 192.168.0.117
11/14-00:14:34.474145  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:34.474145  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:34.474145  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:34.474179  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.55 -> 192.168.0.117
11/14-00:14:35.480369  [**] [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:35.480369  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:35.480369  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.117 -> 192.168.0.55
11/14-00:14:35.480401  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Priority: 0] {ICMP} 192.168.0.55 -> 192.168.0.117
```

Links útiles

<https://www.elastic.co/es/downloads/elasticsearch>

https://www.java.com/es/download/help/linux_x64_install.html

<http://yanez.pro/blog/servidores/comprimir-y-descomprimir-gz-tar-gz-y-zip-por-linea-de-comandos/>

<https://ubunlog.com/instala-java-8-9-y-10-en-ubuntu-18-04-y-derivados/>

<https://www.youtube.com/watch?v=8ycqfPtGUB0>

<https://logz.io/blog/configure-yaml-files-elk-stack/>

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-18-04-es>

<https://puerto53.com/linux/centralizacion-de-logs-con-logstash-filebeat-y-elasticseark/>

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-es>

<https://www.youtube.com/watch?v=7i9VRJoeoOg>

<https://www.youtube.com/watch?v=5L6LOhG20V0&t=22s>

<https://es.linux-console.net/?p=921>

https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html#_apt

<https://www.solvetic.com/tutoriales/article/5739-comandos-para-configurar-y-sincronizar-hora-fecha-y-zona-horaria-en-ubuntu-1804/>

<https://discuss.elastic.co/t/failed-to-connect-to-backoff-async-tcp-localhost-5044-dial-tcp-127-0-0-1-connect-connection-refused/213713/5>