



SPLUNK Y ELASTICSEARCH

Laboratorio 2 Ejercicio SIEM



5 DE DICIEMBRE DE 2024

UAH

Enrique García Cuadrado Carlos Garrido Junco

Contenido

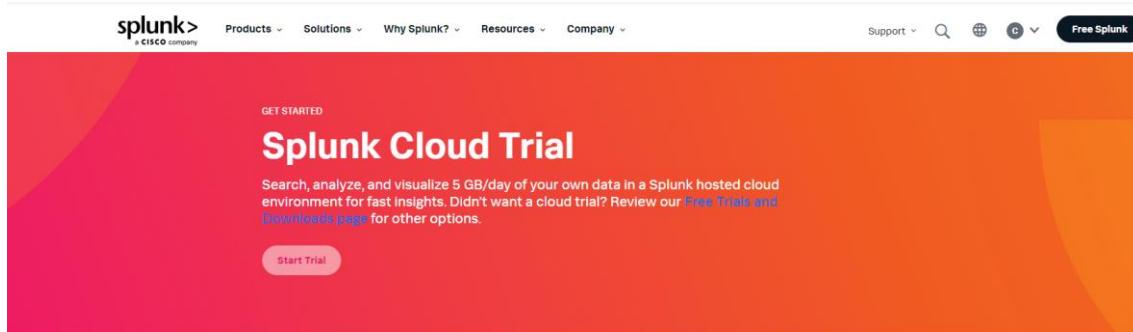
Ejercicio 1: Ejercicio 1: Configuración de entorno con SIEM.....	2
Instalación Splunk	2
Gestionar los inicios de sesión de dos sistemas operativos diferentes.....	6
Encuentra la cantidad de eventos de inicio de sesión exitosos y fallidos por usuario.....	24
Crea una visualización de barras que muestre la cantidad de eventos de inicio de sesión exitosos y fallidos.....	27
Ejercicio 2: Instalación de Elasticsearch	29
Instalación de elasticsearch	29
Visualizar distintos valores en Kibana.....	34
Mejorando la seguridad en elasticsearch.....	41

Ejercicio 1: Ejercicio 1: Configuración de entorno con SIEM

Instalación Splunk

Hemos escogido el sistema operativo ZorinOS, donde haremos la instalación del Splunk, y otra máquina con sistema operativo Ubuntu que mandará logs en la que se instaló el Snort. Se utilizará la instalación de la práctica anterior. El objetivo de esta parte es hacer la instalación en otro sistema operativo al que hicimos la práctica uno. También explicaremos cómo hacer la instalación mediante Docker, ya que en Docker Hub hay una imagen de Splunk, lo cual facilita la instalación. Además instalaremos un splunk forwarder en un sistema Windows ya que Windows lo utilizan el 90 por ciento de los usuarios.

Lo primero es acceder a la página web y registrarnos. Una vez que nos hayamos registrado, nos mandará un correo para validar la sesión. Al validarla, nos saldrá el siguiente mensaje.



Thank you for registering, your free trial is on its way!

You will receive an email within 15 minutes. Check your spam folder if it doesn't arrive.

If you still need help, please reach out to Splunk support.

Ilustración 1 validación de cuenta

Tenemos que descargar la versión splunk Enterprise, elegimos la versión Linux .deb.

Splunk Enterprise 9.3.2

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

The screenshot shows the download section of the Splunk website for version 9.3.2. It's set to the Linux 64-bit category. Three package formats are listed: .rpm (947.5 MB), .tgz (947.75 MB), and .deb (716.43 MB). Each has a "Download Now" button and a "Copy wget link" button. A tooltip indicates that the link has been copied to the clipboard.

Ilustración 2Splunk enterprise

Seleccionamos el enterprise, elegimos Linux mod deb para que se nos descargue el paquete a instalar nos dará un wget con el enlace a descargar:

```
carlos@carlos-VirtualBox:~/Desktop$ wget -O splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb "https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb"
--2024-12-05 13:39:23-- https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 52.84.66.28, 52.84.66.10, 52.84.66.41, ...
```

Ilustración 3wget splunk

Ejecutamos el siguiente comando para instalar el paquete descargado

```
Dpkg -i <paquete descargado>
```

```
carlos@carlos-VirtualBox:~/Desktop$ dpkg -i splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
```

Ilustración 4dpkg -i splunk

Para hacer las instalaciones hemos cambiado a modo root escribiendo sudo su
Una vez instalado accedemos al directorio donde se encuentra el binario, el cual es /opt/splunk/bin y damos permisos de ejecución al fichero splunk de la siguiente forma:

```
root@carlos-VirtualBox:/opt/splunk/bin# chmod +x splunk
```

Ilustración 5chmod +x splunk

Y ahora podemos ejecutar el binario de la siguiente forma:

```
root@carlos-VirtualBox:/opt/splunk/bin# ./splunk -enable boot-start
```

Ilustración 6 ejecutar splunk

Nos sale un texto en el cual nos pide aceptar las condiciones.

```
"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all associated Splunk technology and all Intellectual Property Rights created or acquired: (a) prior to the date of the Statement of Work that includes such C&I Services Materials, or (b) after the date of such Statement of Work but independently of the C&I Services provided under such Statement of Work.
```

```
"Statement of Work" means the statements of work and/or any and all applicable Orders, that describe the specific services to be performed by Splunk, including any materials and deliverables to be delivered by Splunk.
```

```
Do you agree with this license? [y/n]: y
```

Ilustración 7 Aceptar condiciones

Además de solicitarnos nombre de usuario y password.

Volvemos a ejecutar y nos sale que el script se ha inicializado.

```
root@carlos-VirtualBox:/opt/splunk/bin# ./splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@carlos-VirtualBox:/opt/splunk/bin#
```

Ilustración 8 Ejecución ./splunk

Probamos que se ejecuta correctamente utilizando ./splunk start



```
carlos@CarlosKike:~$ cd /opt/splunk/bin/
carlos@CarlosKike:/opt/splunk/bin$ ./splunk start

Warning: cannot create "/opt/splunk/var/log/splunk"
Warning: cannot create "/opt/splunk/var/log/introspection"
Warning: cannot create "/opt/splunk/var/log/watchdog"

Warning: cannot create "/opt/splunk/var/log/client_events"
Pid file "/opt/splunk/var/run/splunk/splunkd.pid" unreadable.: Permission denied
Error opening username mapping file: /opt/splunk/etc/users/users.ini err: Cannot open file=/opt/splunk/etc/users/users.ini for parsing: Permission denied
Cannot initialize: /opt/splunk/etc/apps/launcher/metadata/local.meta: Permission denied
Cannot initialize: /opt/splunk/etc/apps/splunk_assist/metadata/local.meta: Permission denied
```

Ilustración 9splunk start

Una vez arrancada nos podremos meter en el login que está en la ruta

```
127.0.0.1:8000
```

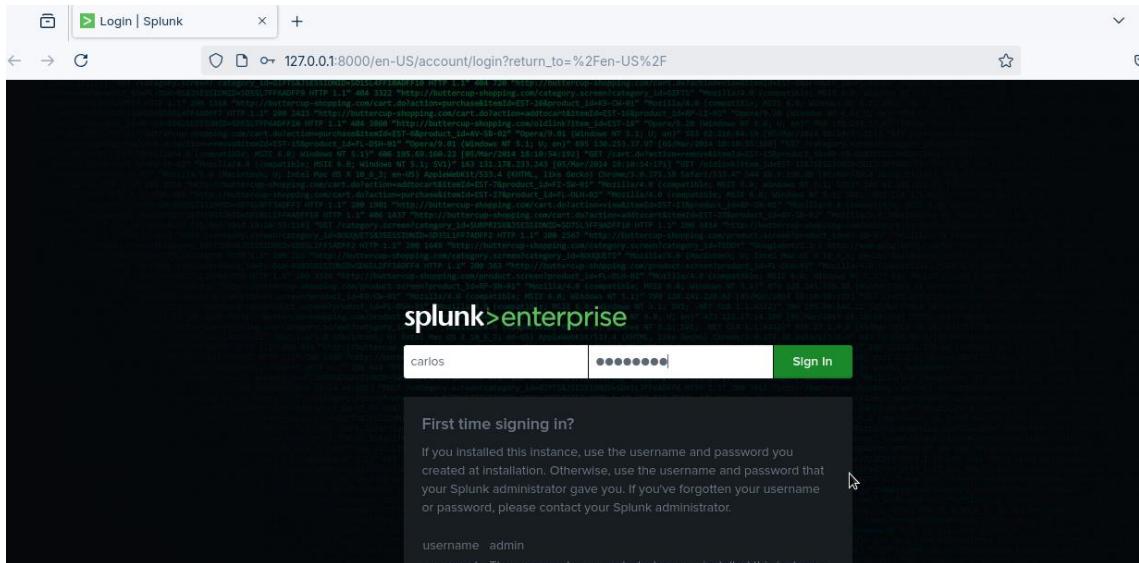


Ilustración 10 Login Splunk

Tenemos que introducir el usuario y la contraseña que se nos solicitó durante el paso de habilitación.

Tambien se puede ejecutar con Docker, basta con bajar la imagen de Docker hub splunk/splunk con el siguiente comando:

Docker pull splunk/splunk

Y ejecutamos el siguiente comando para ejecutar el contenedor:

```
sudo docker run -d -e "SPLUNK_START_ARGS=--accept-license" -e
"SPLUNK_PASSWORD=changeme" -e "SPLUNK_USER=root" -p "8000:8000"
splunk/splunk
```

Para ver su correcto funcionamiento hacemos un wget

```
→ ~ wget http://localhost:8000
--2024-12-04 17:25:49-- http://localhost:8000/
Resolviendo localhost (localhost)... 127.0.0.1
Conectando con localhost (localhost)[127.0.0.1]:8000... conectado.
Petición HTTP enviada, esperando respuesta... 303 See Other
Ubicación: http://localhost:8000/en-US/ [siguiente]
--2024-12-04 17:25:49-- http://localhost:8000/en-US/
Reutilizando la conexión con localhost:8000.
Petición HTTP enviada, esperando respuesta... 303 See Other
Ubicación: http://localhost:8000/en-US/account/login?return_to=%2Fen-US%2F [siguiente]
--2024-12-04 17:25:49-- http://localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
Reutilizando la conexión con localhost:8000.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 13515 (13K) [text/html]
Guardando como: 'index.html'

Index.html          100%[=====] 13,20K  ----KB/s   en 0s
2024-12-04 17:25:49 (337 MB/s) - 'index.html' guardado [13515/13515]
```

Ilustración 11wget localhost

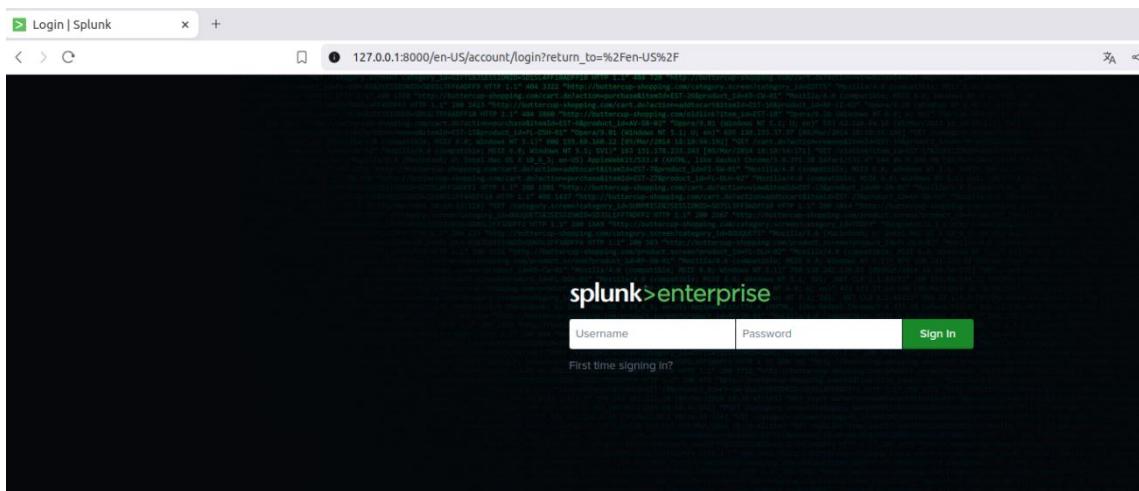


Ilustración 12 Login splunk

Si queremos parar el contenedor podemos hacer:

```
docker stop "idcontenedor"
```

Si queremos levantar lo ejecutamos:

```
docker start "idcontenedor"
```

Gestionar los inicios de sesión de dos sistemas operativos diferentes.

El contenedor lo ejecutamos con la máquina en la que tenemos Ubuntu.

Continuaremos con la instalación que teníamos hecho en nuestra máquina virtual con zorin el escenario por el momento es el siguiente:

Portatil con Ubuntu que tiene instalado el snort de la práctica anterior en el cual manda las alertas al SIEM que está ejecutándose en una máquina virtual en otro dispositivo y un equipo con Windows que también manda alertas al SIEM el esquema es el siguiente:

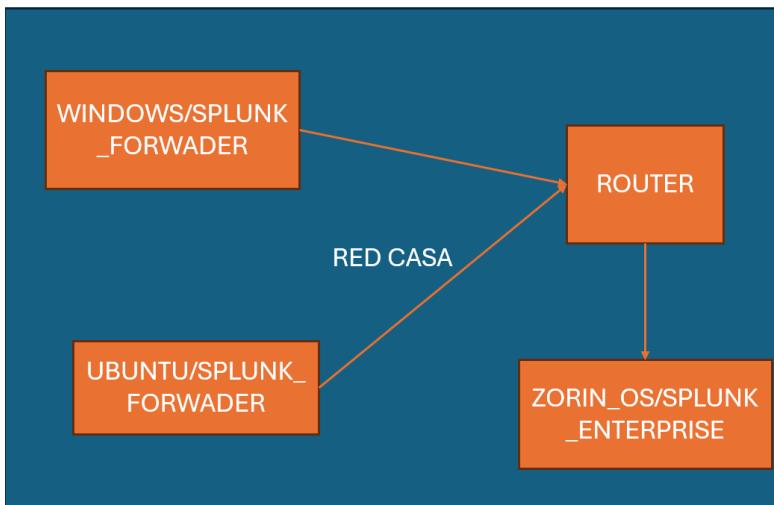


Ilustración 13 Configuración

Lo primero que hacemos es habilitar las conexiones ssh desde nuestro portátil ejecutando los siguientes comandos para poder hacer inicios de sesión a través de ssh desde otro equipo.

Sudo apt install openssh-server

```
→ 'Grimorios git:(main)' sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass ufw
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 751 kB de archivos.
Se utilizarán 6.046 kB de espacio de disco adicional después de esta operación.
'Desea continuar? [S/n] s'
```

Ilustración 14 instalar openssh

Una vez ejecutado comprobamos el status ejecutando el siguiente comando:

Sudo Systemctl status ssh

```

Procesando despachadores para bien ssh (2.10.2-1) ...
→ Grimorios git:(main) sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Sat 2024-12-07 18:02:44 CET; 9s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 7749 (sshd)
     Tasks: 1 (limit: 9006)
   Memory: 1.7M
      CPU: 17ms
     CGroup: /system.slice/ssh.service
             └─7749 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

dic 07 18:02:44 carlos-HP-Laptop-15s-fq2xxx systemd[1]: Starting OpenBSD Secure Shell server...
dic 07 18:02:44 carlos-HP-Laptop-15s-fq2xxx sshd[7749]: Server listening on 0.0.0.0...
dic 07 18:02:44 carlos-HP-Laptop-15s-fq2xxx sshd[7749]: Server listening on ::...
dic 07 18:02:44 carlos-HP-Laptop-15s-fq2xxx systemd[1]: Started OpenBSD Secure Shell server.

[lines 1-16/16 (END)]

```

Ilustración 15 Sudo Systemctl status ssh

Probamos la ejecución desde otra máquina

```

C:\Users\carlos>ssh carlos@192.168.1.45
The authenticity of host '192.168.1.45 (192.168.1.45)' can't be established.
ED25519 key fingerprint is SHA256:[REDACTED]
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.45' (ED25519) to the list of known hosts.
carlos@192.168.1.45's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 3 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

31 actualizaciones de seguridad adicionales se pueden aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

Last login: Tue Nov  5 00:35:18 2024
→ ~ ls
Ciberseguridad  index.html.1  prueba.txt-01.cap  snap
Descargas        kali-linux-2022_v2.ova  prueba.txt-01.csv  Videos
Documentos       Música            prueba.txt-01.kismet.csv 'VirtualBox VMs'
eclipse-workspace 'New Graph (1).mtgl'  prueba.txt-01.kismet.netxml volatility3
edroom_ej1_project 'New Graph (2).mtgl'  prueba.txt-01.log.csv wget-log
Escritorio       OneDrive         Pública           workspace

```

Ilustración 16 conexión ssh

Y vemos que se nos conecta correctamente.

Y a continuación descargamos el splunk universal forwarder:

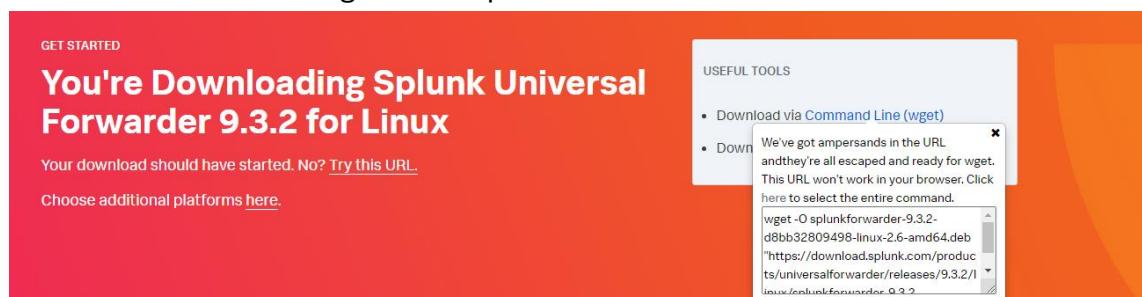
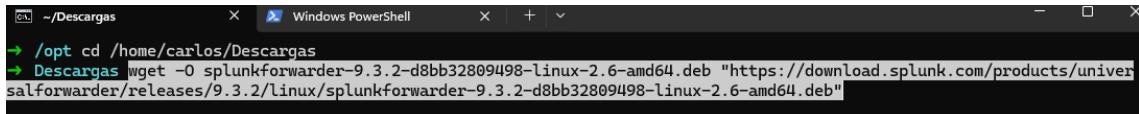


Ilustración 17 splunk universal forwarder

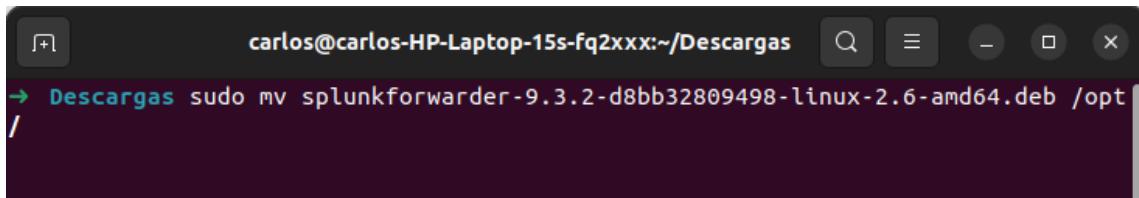
Y lo descargamos:



```
~\Descargas          x  Windows PowerShell  x  +  v
→ /opt cd /home/carlos/Descargas
→ Descargas wget -O splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb "https://download.splunk.com/products/univer
salforwarder/releases/9.3.2/linux/splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb"
```

Ilustración 18 descarga splunkforwader

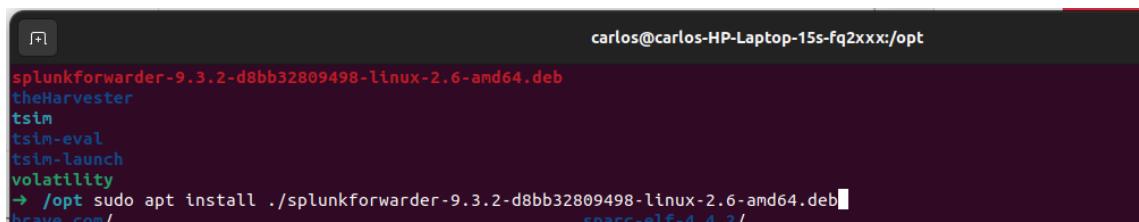
Movemos el archivo ejecutable a la carpeta opt que es donde se guardan los binarios que descarga el usuario.



```
carlos@carlos-HP-Laptop-15s-fq2xxx:~/Descargas
→ Descargas sudo mv splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb /opt
```

Ilustración 19 sudo mv splunkforwader /opt

Y ahora instalamos el splunkforwarder.

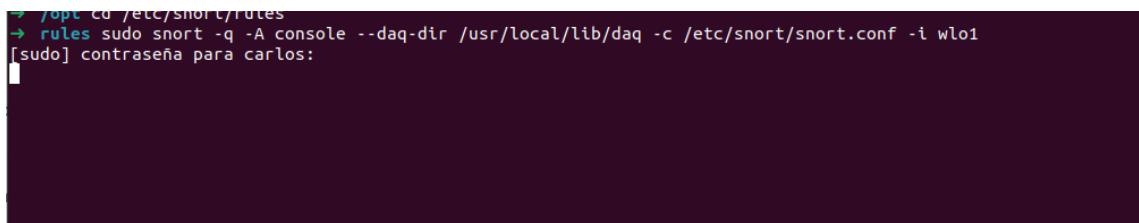


```
carlos@carlos-HP-Laptop-15s-fq2xxx:/opt
splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb
theHarvester
tsim
tsim-eval
tsim-launch
volatility
→ /opt sudo apt install ./splunkforwarder-9.3.2-d8bb32809498-linux-2.6-amd64.deb
```

Ilustración 20 sudo apt install ./splunkfowarder

Para ejecutar le snort ejecutamos el siguiente comando:

```
sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1
```



```
→ /opt cd /etc/snort/rules
→ rules sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1
[sudo] contraseña para carlos:
```

Ilustración 21 Ejecutar snort

Paramos la ejecución y e introducimos una nueva regla para poder encontrar si están haciendo un acceso no autorizado desde ssh

```

carlos@carlos-HP-Laptop-15s-fq2xxx:/opt
x carlos@carlos-HP-Laptop-15s-fq2xx
→ rules sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1
[sudo] contraseña para carlos:
z
[1] + 11832 suspended sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf
→ rules vim local.rules
[2] + 11985 suspended vim local.rules
→ rules sudo vim local.rules

```

Ilustración 22 sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1

La regla es la siguiente:

```
alert tcp any any -> any 22 (msg:"Intento de conexión ssh" ; sid :100017;rev:1;)
```

```

carlos@carlos-HP-Laptop-15s-fq2xxx:/opt
x carlos@carlos-HP-Laptop-15s-fq2xx
#REGLAS por búsqueda por contenido
alert tcp any any -> any any ( msg:"busqueda de contenido malicioso"; content:"GET"; http_method; content:"hacking"; ht
#DDOS ATTACK DETECTION
alert tcp any any -> any any (flags: S; msg:"Possible SYN Dos"; flow: stateless; threshold: type both, track by_dst, co
alert tcp any any -> any any (flags: A; msg:"Possible ACK Dos"; flow: stateless; threshold: type both, track by_dst, co
alert tcp any any -> any any (flags: R; msg:"Possible RST Dos"; flow: stateless; threshold: type both, track by_dst, co
alert tcp any any -> any any (flags: F; msg:"Possible FIN Dos"; flow: stateless; threshold: type both, track by_dst, co
alert udp any any -> any any (msg:"Possible UDP Dos"; flow: stateless; threshold: type both, track by_dst, count 1000,
alert icmp any any -> any any (msg:"Possible ICMP Dos"; threshold: type both, track by_dst, count 250, seconds 3; sid:1
#DDOS ATTACK DETECTION
alert tcp any any -> any any (flags: S; msg:"Possible SYN DDoS"; flow: stateless; threshold: type both, track by_dst, c
alert tcp any any -> any any (flags: A; msg:"Possible ACK DDoS"; flow: stateless; threshold: type both, track by_dst, c
alert tcp any any -> any any (flags: R; msg:"Possible RST DDoS"; flow: stateless; threshold: type both, track by_dst, c
alert tcp any any -> any any (flags: F; msg:"Possible FIN DDoS"; flow: stateless; threshold: type both, track by_dst, c
alert udp any any -> any any (msg:"Possible UDP DDoS"; flow: stateless; threshold: type both, track by_dst, count 10000
alert icmp any any -> any any (msg:"Possible ICMP DDoS"; threshold: type both, track by_dst, count 100000, seconds 10;
#PING OF DEATH DETECTION
alert icmp any any -> any any (msg:"Possible Ping of Death"; dsiz: > 10010; sid:555555;rev:1;)
#regla para detectar inicio de sesión ssh
alert tcp any any -> any 22 (msg:"Intento de conexión ssh" ; sid :100017;rev:1;)
~
```

Ilustración 23 reglas de snort

Volvemos a ejecutar el snort y hacemos una conexión ssh desde el otro equipo

```

sudo snort -q -A console --daq-dir /usr/local/
carlos@carlos-HP-Laptop-15s-fq2xxx:/opt
x carlos@carlos-HP-Laptop-15s-fq2xx
→ rules sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1

```

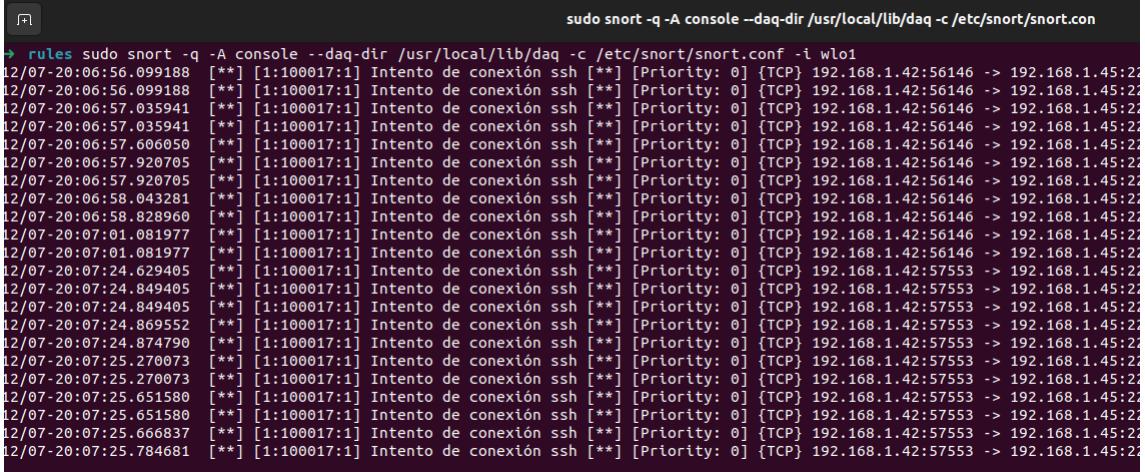
Ilustración 24 ejecutar snort

Hacemos la conexión ssh como se muestra en la imagen:

```
PS C:\Users\carlos> ssh carlos@192.168.1.45
carlos@192.168.1.45's password: |
```

Ilustración 25 conexión ssh

En la siguiente captura se comprueba que correctamente se ha detectado la conexión ssh :

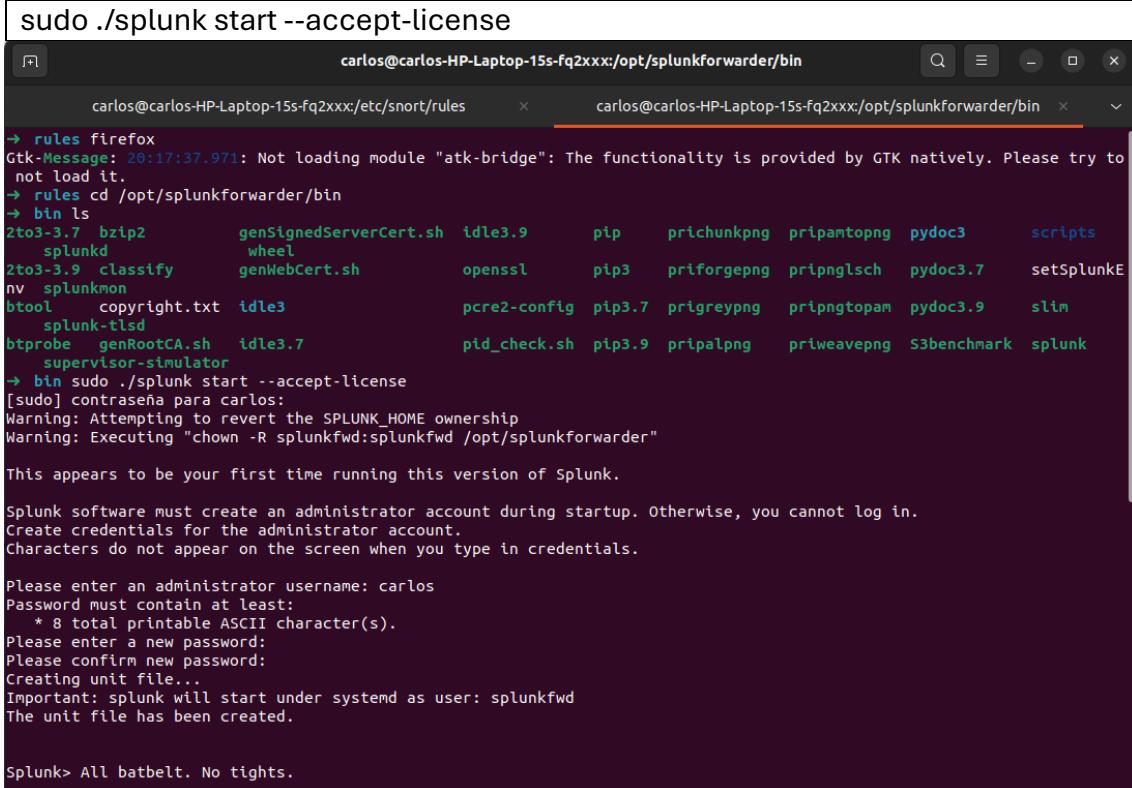


```
sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1
→ rules sudo snort -q -A console --daq-dir /usr/local/lib/daq -c /etc/snort/snort.conf -i wlo1
12/07-20:06:56.099188 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:56.099188 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:57.035941 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:57.035941 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:57.066050 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:57.920705 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:57.920705 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:58.043281 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:06:58.828960 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:07:01.081977 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:07:01.081977 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:56146 -> 192.168.1.45:22
12/07-20:07:24.629405 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:24.849405 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:24.849405 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:24.869552 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:24.874790 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.270073 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.270073 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.651580 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.651580 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.666837 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
12/07-20:07:25.784681 [**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] {TCP} 192.168.1.42:57553 -> 192.168.1.45:22
```

Ilustración 26 snort detecta de ssh

Ahora que ya está recogiendo correctamente los logs tenemos que configurar el splunk forwarder para que le pase los logs al indexer splunk.

Ejecutamos el siguiente comando:



```
sudo ./splunk start --accept-license
carlos@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/bin
carlos@carlos-HP-Laptop-15s-fq2xxx:/etc/snort/rules      carlos@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/bin
→ rules firefox
Gtk-Message: 20:17:37.971: Not loading module "atk-bridge": The functionality is provided by GTK natively. Please try to
not load it.
→ rules cd /opt/splunkforwarder/bin
→ bin ls
2to3-3.7 bzip2      genSignedServerCert.sh  idle3.9      pip      prichunkpng  pri pamtopng  pydoc3      scripts
splunkd          wheel
2to3-3.9 classify  genWebCert.sh    openssl      pip3      priforgepng  pri pnglsch  pydoc3.7    setSplunkE
nv splunkmon
btool          copyright.txt  idle3          pcre2-config  pip3.7   prigreypng  pri pngtopam  pydoc3.9    slim
splunk-tlsd
btprobe        genRootCA.sh  idle3.7       pid_check.sh  pip3.9   pri palpng   pri weavepng  S3benchmark  splunk
supervisor-simulator
→ bin sudo ./splunk start --accept-license
[sudo] contraseña para carlos:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: carlos
Password must contain at least:
     * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.

Splunk> All batbelt. No tights.
```

Ilustración 27 Ejecución splunk forwarder

Ahora tenemos que agregar la información servidor donde se renvía los logs del snort.

```
Sudo ./splunk add forward-server 192.168.1.43
```

Pero antes tenemos que habilitar el plugin del snort dentro de la máquina de zorinOS

The screenshot shows the Splunk Apps Browser interface. At the top, there is a search bar with 'snort' typed into it. Below the search bar, there are three filter buttons: 'Best Match', 'Newest', and 'Popular'. A message indicates '2 Apps' found. The first result is 'Snort 3 JSON Alerts', which has a green 'Install' button. A brief description states: 'This repository is a Technology Add-On for Splunk that allows you to ingest IDS alerts into Splunk from Snort 3 in json format. This plugin normalizes these alerts conform to the "Intrusion Detection" model in the Splunk Common Information Model (CIM), and can be accessed within any app or dashboard that reports Intrusion Detection events.' The second result is 'Snort Alert for Splunk', also with a green 'Install' button. Its description says: 'This app provides field extractions for Snort alert logs (fast and full) as well as dashboards, saved searches, reports, event types, tags and event search interfaces. While this app is not formally supported, the developer can be reached at gransen@splunk.com OR in splunk-usergroups slack, @Guillaume Pierre Fransen. Responses are made on a best ... More'.

Ilustración 28 Apps splunk

Introducimos el usuario y contraseña que nos creamos para página web oficial de splunk y lo descargamos:

The screenshot shows a mobile application window titled 'Complete'. It displays a message: 'Snort Alert for Splunk was successfully installed.' Below this message are two buttons: 'Open the App' and 'Go Home'. In the bottom right corner, there is a large green 'Done' button.

Ilustración 29 Instalación correcta del snort

Y ahora desde la aplicación podremos ver los eventos de snort:

The screenshot shows the 'Snort Event Summary' page in Splunk. At the top, there are tabs for 'Search', 'Snort Event Search', 'Snort Event Summary' (which is selected), 'Snort World Map', and 'Reports'. On the right, there are buttons for 'Edit', 'Export', and '...'. The main area is divided into four quadrants: 'Events and Sources' (Events: 0, Sources: 0), 'Top Source Countries' (No results found), 'Top 10 Classifications' (No results found), and 'Snort Event Types' (No results found). The entire interface has a dark theme.

Ilustración 30 Logs de snort

Continuamos entonces con la configuración del snort universal forwader.

Para que pueda recibir nuestro splunk los datos tenemos que habilitar un puerto por el cual escuche que en nuestro caso será el 9997

The screenshot shows the 'Add new' configuration page for receiving data. The title is 'Forwarding and receiving > Receive data > Add new'. The section is titled 'Configure receiving' with the sub-instruction 'Set up this Splunk instance to receive data from forwarder(s.)'. A field 'Listen on this port *' contains the value '9997'. Below it is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom are 'Cancel' and 'Save' buttons.

Ilustración 31 habilitar puerto por defecto de entrada 9997

Ahora ejecutamos el forwader server y lo añadimos:

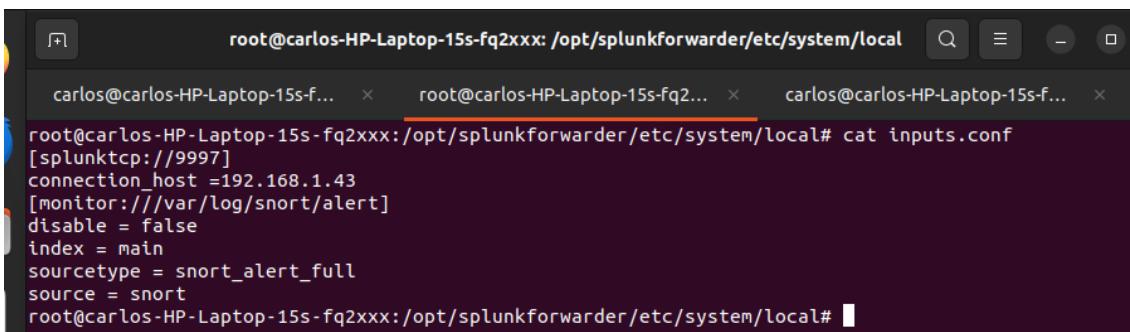
```
sudo ./splunk enable boot-start
```

```
sudo ./splunk add forward-server 192.168.1.43:9997
```

```
→ bin sudo ./splunk add forward-server 192.168.1.43
[sudo] contraseña para carlos:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: carlos
Password:
192.168.1.43 specified in incorrect format. Please specify in <host>:<port> form
→ bin sudo ./splunk add forward-server 192.168.1.43:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.1.43:9997.
→ bin
```

Ilustración 32 sudo ./splunk add forward-server 192.168.1.43:9997

Ahora continuamos y configuraremos el archivo inputs.conf en el caso de no estar creado lo creamos:



```
root@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/etc/system/local# cat inputs.conf
[splunktcp://9997]
connection_host =192.168.1.43
[monitor:///var/log/snort/alert]
disable = false
index = main
sourcetype = snort_alert_full
source = snort
root@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/etc/system/local#
```

Ilustración 33 cat inputs.conf

Para el renvió de nuestro agente a nuestro index añadimos el siguiente monitor.

```
root@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/snort/
```

Ilustración 34añadir monitor

Después de añadir nuestro monitor hacemos un restart del splunk

```
./Splunk restart
Password:
Cannot create another input with the name "/var/log/snort/alert", one already exists.
root@carlos-HP-Laptop-15s-fq2xxx:/opt/splunkforwarder/bin# ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...
```

Ilustración 35 Splunk restart

Y podemos comprobar que los logs han llegado correctamente al splunk

The screenshot shows a Splunk search interface. The search bar at the top contains the query "host='carlos-HP-Laptop-15s-fq2xxx'". Below the search bar, it says "47 events (12/10/24 6:00:00.000 AM to 12/11/24 6:09:10.000 AM) No Event Sampling". The "Events (47)" tab is selected. The results table has columns for "Time" and "Event". The events listed are all related to SSH connection attempts from the host "carlos-HP-Laptop-15s-fq2xxx" to various IP addresses (192.168.1.45, 192.168.1.42, 192.168.1.45:22). The events show timestamps from 12/11/24 6:06:43 to 12/11/24 6:06:43.129423. The "Event" column contains log entries like "[**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] (TCP) 192.168.1.42:52676 -> 192.168.1.45:22" and "[**] [1:100017:1] Intento de conexión ssh [**] [Priority: 0] (TCP) 192.168.1.42:52676 -> 192.168.1.45:22". The source field consistently shows "/var/log/snort/snort.alertfast". The sourcetype is "fast-too_small".

Ilustración 36 Intentos de conexión ssh

Como podemos ver la cantidad de eventos de sesión de inicio ssh gracias a la combinación del snort con el splunk

Ahora lo hacemos para Windows para Windows tenemos que descargar el splunk universal Forwarder para Windows

Splunk Universal Forwarder 9.4.0

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

The screenshot shows the download page for the Splunk Universal Forwarder Windows version 9.4.0. It offers two options: "Windows 10" (32-bit) and "Windows 10, 11 Windows Server 2019, 2022" (64-bit). Both packages are in ".msi" format. The "Windows 10" package is 64.99 MB and the "Windows 10, 11" package is 176.63 MB. Each package has a "Download Now" button and a "Copy wget link" button. There is also a "More" dropdown menu.

Ilustración 37 Splunk Universal Forwarder Windows

Cuando se descargue el instalador nos pedirá proporcionarle la ip destino y el puerto y un usuario y contraseña.

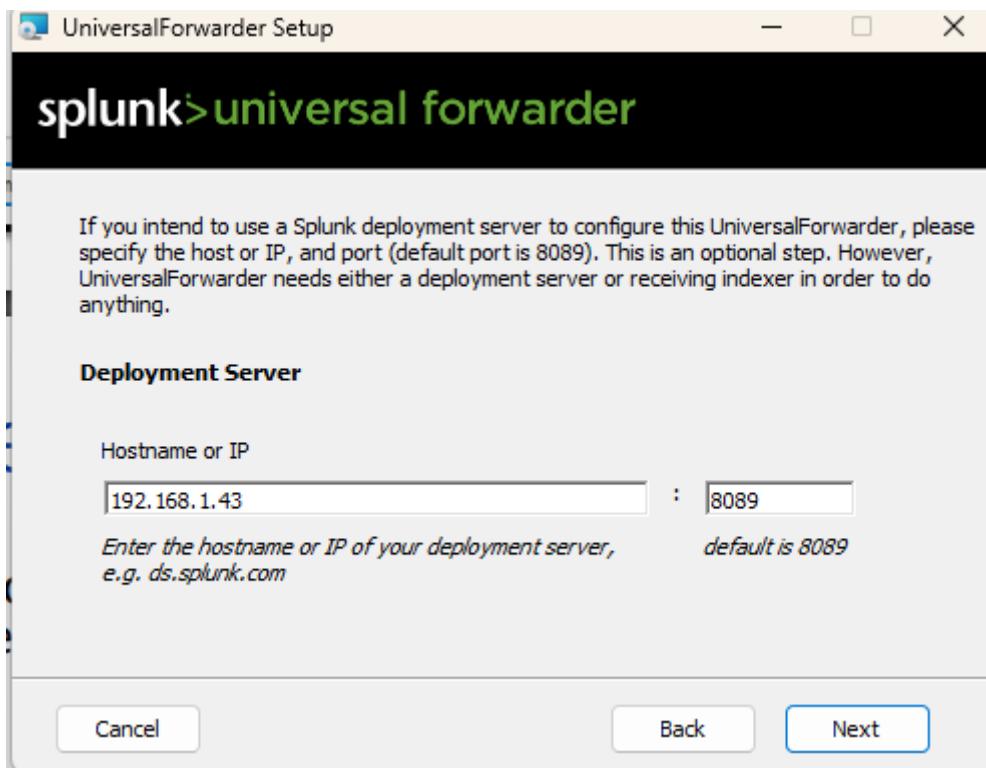


Ilustración 38Instalación splunk forwader en Windows



Ilustración 39Introducir Ip destino más puerto

Ahora nos dirigimos a la siguiente ruta:

C:\Program Files\SplunkUniversalForwarder\etc\system\local

En la cual comprobamos si la ip es la correcta del servidor, en el caso de que cambiase debido a que estamos usando DHCP la podemos cambiar en el archivo output.conf.

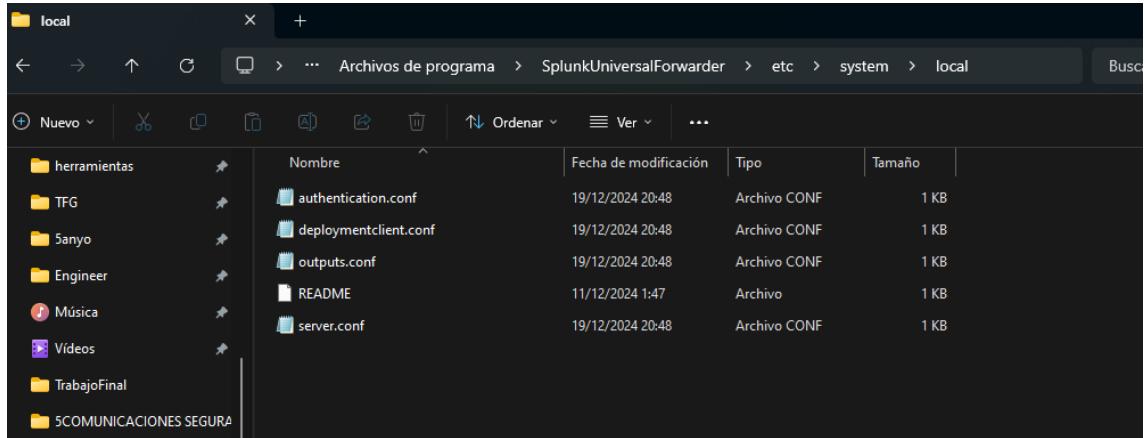


Ilustración 40 archivos de configuración splunk forwarder

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.1.43:9997

[tcpout-server://192.168.1.43:9997]
```

Ilustración 41 Archivo de configuración de salida

Ahora nos toca añadir el plugin en la siguiente ruta extraemos el zip en la siguiente ruta:

“C:\Program Files\SplunkUniversalForwarder\etc\apps”.

Para eso nos lo descargamos de la página web oficial

The screenshot shows the Splunkbase website with the URL splunkbase.splunk.com/app/742. The page title is "Splunk Add-on for Microsoft Windows". It includes a "Find an app" search bar, a "Submit an App" button, and navigation links for "Main Page", "Collections", and "Apps". A note at the top states: "*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on for Windows 5.0.0 introduced breaking changes. If you are upgrading from a version of the Splunk Add-on for Windows that is earlier than 5.0.0, you must follow the...". Below this is a "Download" button with the Splunk logo.

Ilustración 42 plugin para windows

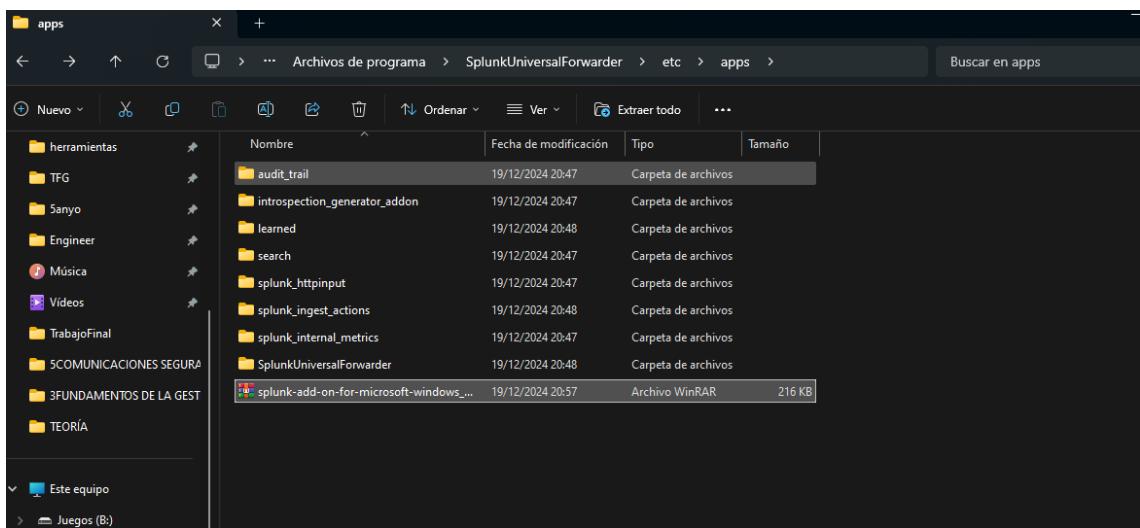


Ilustración 43/etc/apps winrar

Y lo extraemos tiene que extraerse tanto la carpeta Splunk_Ta_windows y el msi:

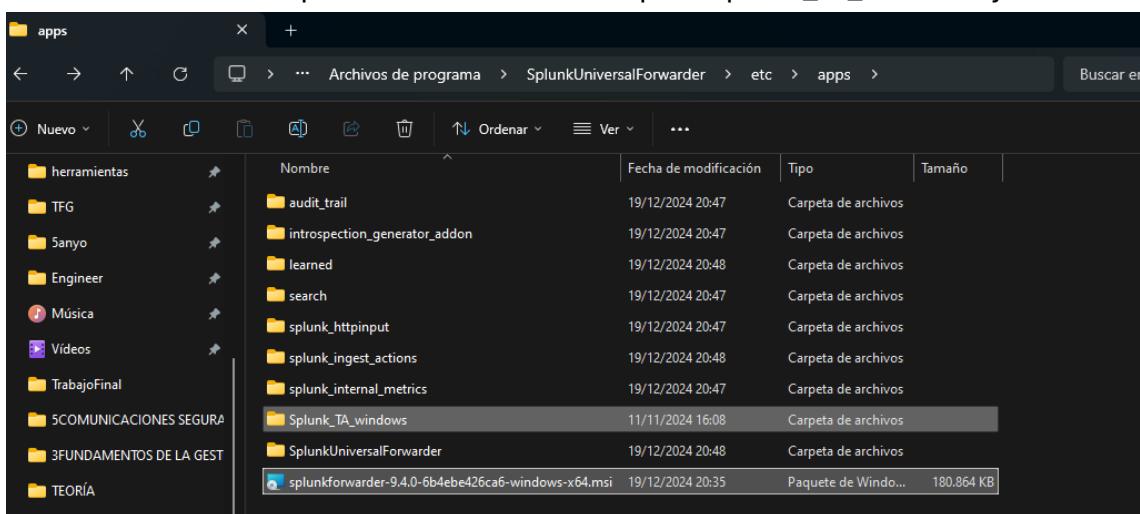


Ilustración 44 /etc/apps

Ahora creamos un directorio llamado local/default en el cual vamos a copiar el input.conf que viene en la carpeta que anteriormente hemos extraído:

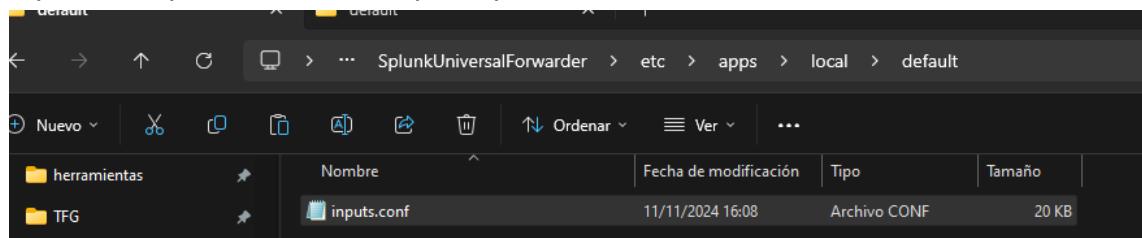


Ilustración 45 ruta

Y cambiamos los siguientes valores:

```
[WinEventLog://Application]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
[WinEventLog://Security]
disabled = 0
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
blacklist1 = EventCode="4662" Message="Object
Type:(?!\\s*groupPolicyContainer)"
blacklist2 = EventCode="566" Message="Object
Type:(?!\\s*groupPolicyContainer)"
renderXml=false
[WinEventLog://System]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
```

Quedaría como en la siguiente imagen:

```
1 ##  
2 ## SPDX-FileCopyrightText: 2024 Splunk, Inc.  
3 ## SPDX-License-Identifier: LicenseRef-Splunk-8  
4 ## DO NOT EDIT THIS FILE!  
5 ## Please make all changes to files in $SPLUNK_  
6 ## To make changes, copy the section/stanza you  
7 ## into ../local and edit there.  
8 ##  
9  
10  
11  
12 ##### OS Logs #####  
13 [WinEventLog://Application]  
14 disabled = 0  
15 start_from = oldest  
16 current_only = 0  
17 checkpointInterval = 5  
18 renderXml=false  
19  
20 [WinEventLog://Security]  
21 disabled = 0  
22 start_from = oldest  
23 current_only = 0  
24 evt_resolve_ad_obj = 1  
25 checkpointInterval = 5  
26 blacklist1 = EventCode="4662" Message="Object 1  
27 blacklist2 = EventCode="566" Message="Object Tj  
28 renderXml=false  
29  
30 [WinEventLog://System]  
31 disabled = 0  
32 start_from = oldest  
33 current_only = 0  
34 checkpointInterval = 5  
35 renderXml=false  
36
```

Ilustración 46 inputs.conf

****Nos hemos percatado que en la guía de la práctica está puesto que dicho fichero debe de estar dentro de la ruta ./apps/local/default y estando ahí no funciona tiene que estar en el directorio ./etc/system/local junto al archivo de output.conf que configuramos previamente.

Ahora vamos a servicios de Windows y reinstalamos el servicio del splunkforwader para que pueda actualizarse:

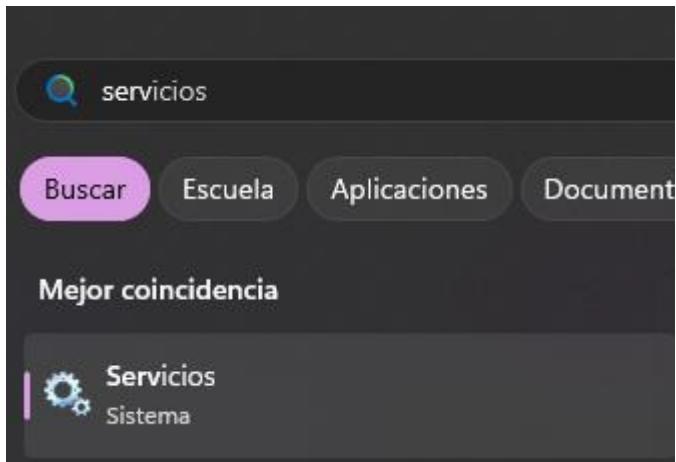


Ilustración 47 Servicios

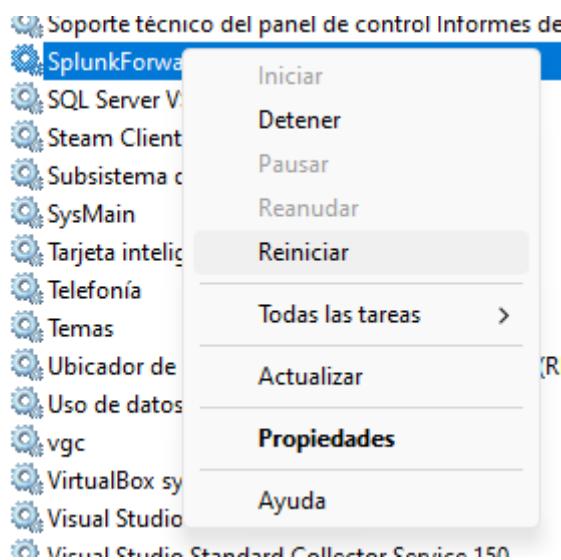


Ilustración 48 Restart Splunkforwader

Para enviar los logs deshabilitamos el windows firewall en un entorno profesional habría que configurarlo correctamente:

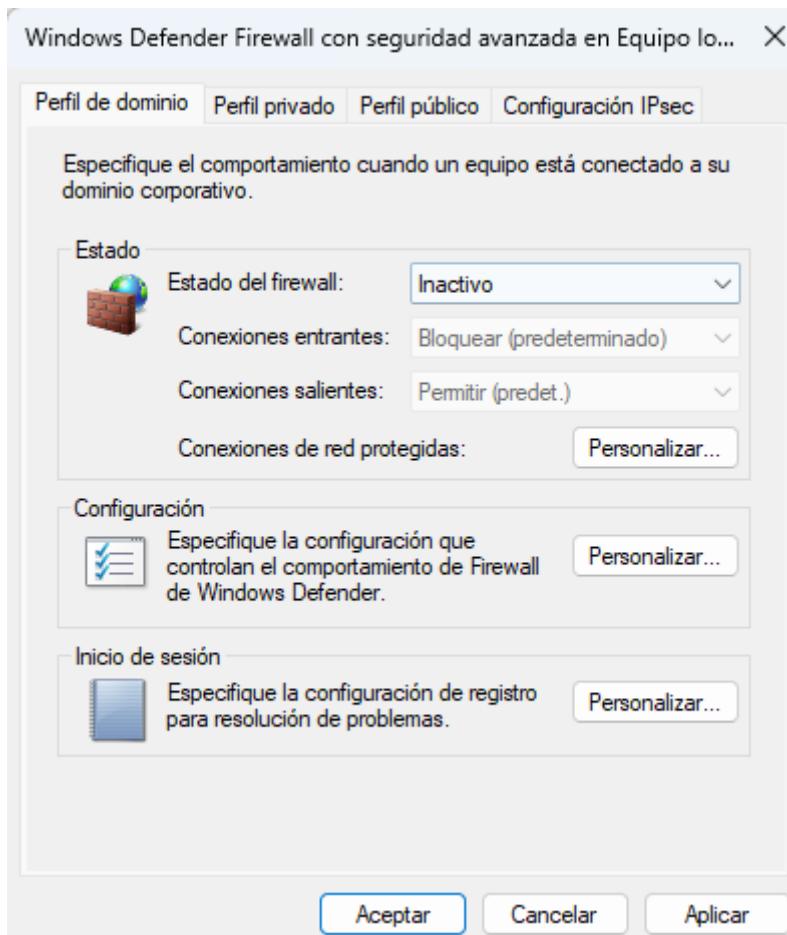


Ilustración 49 firewall Windows

Los log de evento de inicio de sesión estan en el registro de seguridad (Security Event Log)

Para comprobar que se está ejecutando correctamente podemos ver el status como se muestra en la imagen:

```
C:\Program Files\SplunkUniversalForwarder\bin>splunk.exe status
splunkForwarder: Running (pid 42828)

C:\Program Files\SplunkUniversalForwarder\bin>
```

Ilustración 50 Comprobar status SplunkUniversalForwarder

El comando para hacer las pruebas de sesión es el siguiente:

```
runas /user:UsuarioDestino cmd
```

Podemos ver que los logs han sido registrados correctamente en el enterprise

The screenshot shows the Splunk Data Summary interface. On the left, there's a table titled 'Hosts (4)' with columns 'Host', 'Count', and 'Last Update'. The host 'DESKTOP-EIEVS9V' is highlighted with a red box and has a count of 92,075. A tooltip for 'Table Views' appears over the table, explaining how to prepare data without using SPL. The bottom right corner of the screen shows the Windows system tray with the Splunk icon and the text '22:15 19/12/2024'.

Ilustración 51 Dispositivo en Windows

Buscamos con el siguiente EventCode como viene en la captura siguiente 4624

The screenshot shows the Splunk New Search interface. The search query is 'host="DESKTOP-EIEVS9V" EventCode=4624'. The results table shows one event with the following details:

	Time	Event
>	12/19/24 4:12:39.000 PM	12/19/2024 10:12:39 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-EIEVS9V SourceName=Microsoft Windows security auditing. Type=Información RecordNumber=1085490 Keywords=Auditoría correcta TaskCategory=Logon OpCode=Información Message=Se inició sesión correctamente en una cuenta. Firmante: Id. de seguridad: NT AUTHORITY\SYSTEM Nombre de cuenta: DESKTOP-EIEVS9V\$ Dominio de cuenta: WORKGROUP Id. de inicio de sesión: 0x3E7 Información de inicio de sesión: Tipo de inicio de sesión: 5 Modo de administrador restringido: - Credential Guard remota: - Cuenta virtual: No Token elevado: Sí

Ilustración 52 Inicios de sesión

Y esto son los inicios de sesión como se puede comprobar en la siguiente imagen

List	Format	20 Per Page
i	Time	Event
		Nombre de cuenta: SYSTEM Dominio de cuenta: NT AUTHORITY Id. de inicio de sesión: 0x3E7 Inicio de sesión vinculado: 0x0 Nombre de cuenta de red: - Dominio de cuenta de red: - GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}
		Información de proceso: Id. de proceso: 0x5b4 Nombre de proceso: C:\Windows\System32\services.exe
		Información de red: Nombre de estación de trabajo: - Dirección de red de origen: - Puerto de origen: -
		Información de autenticación detallada: Proceso de inicio de sesión: Advapi Paquete de autenticación: Negotiate Servicios transitados: - Nombre de paquete (solo NTLM): - Longitud de clave: 0
		Este evento se genera cuando se crea una sesión de inicio. Lo genera el equipo al que se tuvo acceso. Los campos de firmante indican la cuenta del sistema local que solicitó el inicio de sesión. Suele ser un servicio como el servicio de servidor o un proceso local como Winlogon.exe o Services.exe. El campo Tipo de inicio de sesión indica la clase de inicio de sesión que se realizó. Los tipos más comunes son 2 (interactivo) y 3 (red). Los campos Nuevo inicio de sesión indican la cuenta para la que se creó el nuevo inicio de sesión, es decir, aquella en la que se inició la sesión. Los campos de red indican dónde se originó una solicitud de inicio de sesión remota. Nombre de estación de trabajo no está siempre disponible y se puede dejar en blanco en algunos casos. El campo de nivel de suplantación indica en qué medida un proceso en la sesión de inicio de sesión puede suplantarla. Los campos de información de autenticación proporcionan información detallada sobre esta solicitud de inicio de sesión específica. - GUID de inicio de sesión es un identificador único que se puede usar para correlacionar este evento con un evento KDC. - Servicios transitados indica los servicios intermedios que participaron en esta solicitud de inicio de sesión. - Nombre de paquete indica el subprotocolo que se usó entre los protocolos NTLM. - Longitud de clave indica la longitud de la clave de sesión generada. Será 0 si no se solicitó una clave de sesión.
		Collapse Host = DESKTOP-EIEVS9V : source = WinEventLog:Security : sourceType = WinEventLog:Security

Ilustración 53 Inicio Correcto

Los inicios correctos van determinados con el código 4624 y los inválidos o fallidos 4625.

Encuentra la cantidad de eventos de inicio de sesión exitosos y fallidos por usuario.

Para el tema de diferenciar los eventos de inicio de sesión exitosos vs los fallidos, tenemos que habilitar los logs de ssh para que se guarden en el var/log/auth.log

Para ello, tenemos que ir al archivo de configuración ssh y poner LogLever VERBOSE y una vez que se ha hecho como se ve en las imágenes se registra tanto las conexiones fallidas como las conexiones exitosas, este archivo de log es el que vamos a enviar a través de del Splunk Forwarder al ZorinOS que está escuchando , para luego mostrarlo.

```

vim /etc/ssh/sshd_config
carlos@CarlosKike:/opt/splunkforwarder/bin
vim /etc/ssh/sshd_config
carlos@CarlosKike:/opt/splunkforwarder/bin

```

```

# CheckHostIP yes
# ConnectTimeout 0
# StrictHostKeyChecking ask
IdentityFile ~/.ssh/id_rsa
IdentityFile ~/.ssh/id_dsa
IdentityFile ~/.ssh/id_ecdsa
IdentityFile ~/.ssh/id_ed25519
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACS hmac-md5,hmac-sha1,umac-64@openssh.com
EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostkey no
# RSAAuthentication ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
UserKnownHostsFile ~/.ssh/known_hosts.d/nk
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
LogLevel VERBOSE

```

Ilustración 54 LogLevel VERBOSE

```

vim /etc/ssh/sshd_config
carlos@CarlosKike:/var/log
carlos@CarlosKike:/opt/splunkforwarder/bin
carlos@CarlosKike:/var/log

```

```

sudo snort -q -A console -daq-dir /usr/local/lib/daq </etc/snort/snort...
log vim /etc/ssh/sshd_config
log sudo vim /etc/ssh/sshd_config
[sudo] contraseña para carlos:
log sudo systemctl restart sshd

```

Ilustración 55 sshd_config y restaurar servicio ssh

```

tail -f auth.log
carlos@CarlosKike:/opt/splunkforwarder/bin
tail -f auth.log
carlos@CarlosKike:/var/log

```

```

log tail -f auth.log
log vim /etc/ssh/sshd_config
log sudo vim /etc/ssh/sshd_config
[sudo] contraseña para carlos:
log sudo systemctl restart sshd

```

Ilustración 56 tail -f auth.log

Se lo añadimos al forwarder-splunk

```

carlos@CarlosKike:/opt/splunkforwarder/bin
carlos@CarlosKike:/opt/splunkforwarder/bin
carlos@CarlosKike:/var/log

```

```

sudo snort -q -A console -daq-di...
log vim /etc/ssh/sshd_config
log sudo vim /etc/ssh/sshd_config
[sudo] contraseña para carlos:

```

Ilustración 57 /opt/splunkforwader

```

carlos@CarlosKike:/opt/splunkforwarder/bin
carlos@CarlosKike:/opt/splunkforwarder/bin
carlos@CarlosKike:/var/log

```

```

sudo snort -q -A console -daq-dir /usr/local/lib/daq -c /etc/snort/snort...
log vim /etc/ssh/sshd_config
log sudo vim /etc/ssh/sshd_config
[sudo] contraseña para carlos:

```

Ilustración 58 splunk restart

En el splunk ahora se puede ver la cantidad de inicios fallidos y correctos:

The screenshot shows a Splunk search interface with the following details:

- Time Range:** Format Timeline ▾ (Zoom Out) + Zoom to Selection X Deselect
- Fields:** List ▾ All Fields
- Selected Fields:** host, source, source_type
- Interesting Fields:** date, hour, minute, month, year, zone, index, timeout, pid, process, user, server, timeoffset, timestamp.
- Event Log:**

Time	Event
Dec 11 12:44:33 6:44:33.000 AM	Failed password for carlos from 192.168.1.42 port 53118 ssh2 host=carlos-HP-Laptop-15s-fq2xxx sshd[16557] source=[var/log/auth.log] source_type=syslog
Dec 11 12:44:32 6:44:32.000 AM	Dec 11 12:44:32 carlos-HP-Laptop-15s-fq2xxx sshd[2957] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53118 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:44:32 6:44:32.000 AM	Dec 11 12:44:32 carlos-HP-Laptop-15s-fq2xxx sshd[16557] pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.42 user=carlos host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:44:31 6:44:31.000 AM	Dec 11 12:44:31 carlos-HP-Laptop-15s-fq2xxx sshd[2957] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53118 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:44:30 6:44:30.000 AM	Dec 11 12:44:30 carlos-HP-Laptop-15s-fq2xxx sshd[2957] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53118 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:42:27 6:42:27.000 AM	Dec 11 12:42:27 carlos-HP-Laptop-15s-fq2xxx sshd[2957] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53112 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:42:27 6:42:27.000 AM	Dec 11 12:42:27 carlos-HP-Laptop-15s-fq2xxx sshd[16557] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53112 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:42:27 6:42:27.000 AM	Dec 11 12:42:27 carlos-HP-Laptop-15s-fq2xxx sshd[16557] pam_unix(sshd:session): session opened for user carlos(uid=1000) by (uid=9) host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:42:23 6:42:23.000 AM	Dec 11 12:42:23 carlos-HP-Laptop-15s-fq2xxx sshd[16557] Accepted password for carlos from 192.168.1.42 port 53112 ssh2 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog
Dec 11 12:42:23 6:42:23.000 AM	Dec 11 12:42:23 carlos-HP-Laptop-15s-fq2xxx sshd[16557] [1:100017:1] Intento de conexión ssh (TCP) 192.168.1.42:53112 -> 192.168.1.45:22 host=carlos-HP-Laptop-15s-fq2xxx source=[var/log/auth.log] source_type=syslog

Ilustración 59 Logs del ubuntu

Con los de Windows es todavía mucho más sencillo solo hay que filtra por los event code anterior mencionados.

The screenshot shows a Splunk search interface with the following details:

- Search:** host="DESKTOP-EIEVS9V" EventCode=4624
- Results:** ✓ 379 events (12/18/24 4:00:00.000 PM to 12/19/24 4:29:01.000 PM) No Event Sampling ▾
- Event Types:** Event / 2701, Daterme, Statistics, Visualization

Ilustración 60 Intentos correctos

The screenshot shows a Splunk search interface with the following details:

- Search:** host="DESKTOP-EIEVS9V" EventCode=4625
- Results:** ✓ 9 events (12/18/24 4:00:00.000 PM to 12/19/24 4:29:36.000 PM) No Event Sampling ▾
- Event Types:** Events (9), Patterns, Statistics, Visualization

Ilustración 61 Intentos Fallidos

Crea una visualización de barras que muestre la cantidad de eventos de inicio de sesión exitosos y fallidos

Para poder crear la visualización lo primero que tenemos que hacer es buscar nuestra query en search y ver que los datos son encontrados:

The screenshot shows the Splunk search interface with the following details:

Search Bar: Accepted

Results Summary: ✓ 3 events (12/10/24 8:00:00.000 AM to 12/11/24 8:16:46.000 AM) No Event Sampling ▾

Event List:

Time	Event
12/11/24 6:42:27.000 AM	Dec 11 12:42:27 carlos-HP-Laptop-15s-fq2xxx sshd[16450]: Accepted password for carlos from 192.168.1.42 port 53112 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog
12/11/24 6:14:55.000 AM	Dec 11 12:14:55 carlos-HP-Laptop-15s-fq2xxx sshd[6659]: Accepted password for carlos from 192.168.1.42 port 52735 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog
12/11/24 6:05:53.000 AM	Dec 11 12:05:53 carlos-HP-Laptop-15s-fq2xxx sshd[5954]: Accepted password for carlos from 192.168.1.42 port 52676 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog

Ilustración 62 Peticiones Aceptadas

The screenshot shows the Splunk search interface with the following details:

Search Bar: Failed

Results Summary: ✓ 3 events (12/10/24 8:00:00.000 AM to 12/11/24 8:19:28.000 AM) No Event Sampling ▾

Event List:

Time	Event
12/11/24 6:44:33.000 AM	Dec 11 12:44:33 carlos-HP-Laptop-15s-fq2xxx sshd[16557]: Failed password for carlos from 192.168.1.42 port 53118 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog
12/11/24 6:15:13.000 AM	Dec 11 12:15:13 carlos-HP-Laptop-15s-fq2xxx sshd[6718]: Failed password for carlos from 192.168.1.42 port 52737 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog
12/11/24 6:15:04.000 AM	Dec 11 12:15:04 carlos-HP-Laptop-15s-fq2xxx sshd[6718]: Failed password for carlos from 192.168.1.42 port 52737 ssh2 host = carlos-HP-Laptop-15s-fq2xxx source = /var/log/auth.log sourcetype = syslog

Ilustración 63 Peticiones Fallidas

Luego creamos una dashboard

The screenshot shows the Splunk dashboard creation interface with the following details:

Header: splunk>enterprise Apps ▾

Top Bar: Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Dashboard List: Dashboards

Bottom Buttons: Create New Dashboard

Ilustración 64 Dashboards

En nuestro caso la hemos llamado logsshevent y añadimos dos paneles para los cuales vamos a poner nuestras consultas:

The screenshot shows the Grafana interface with the 'Add Panel' dialog open. On the left, a sidebar lists various chart types under 'New (15)': Events, Statistics Table, Line Chart, Area Chart, Column Chart (which is selected and highlighted in blue), Bar Chart, Pie Chart, Scatter Chart, Bubble Chart, Single Value, Radial Gauge, Filler Gauge, Marker Gauge, Cluster Map, and Choropleth Map. Below this is a link to 'New from Report (7)'. On the right, the 'New Column Chart' configuration panel is shown. It includes a 'Time Range' section with 'Use time picker' and 'Last 24 hours' dropdowns, a 'Content Title' field containing 'optional', a 'Search String' field containing 'Failed', and a 'Run Search' button.

Ilustración 65 New Column Chart

Hacemos lo mismo para las peticiones aceptadas, pero poniendo en la consulta “Accepted”. La dashboard nos debería salir de la siguiente forma indicando los intentos de conexión fallidos y aceptados en función del tiempo.

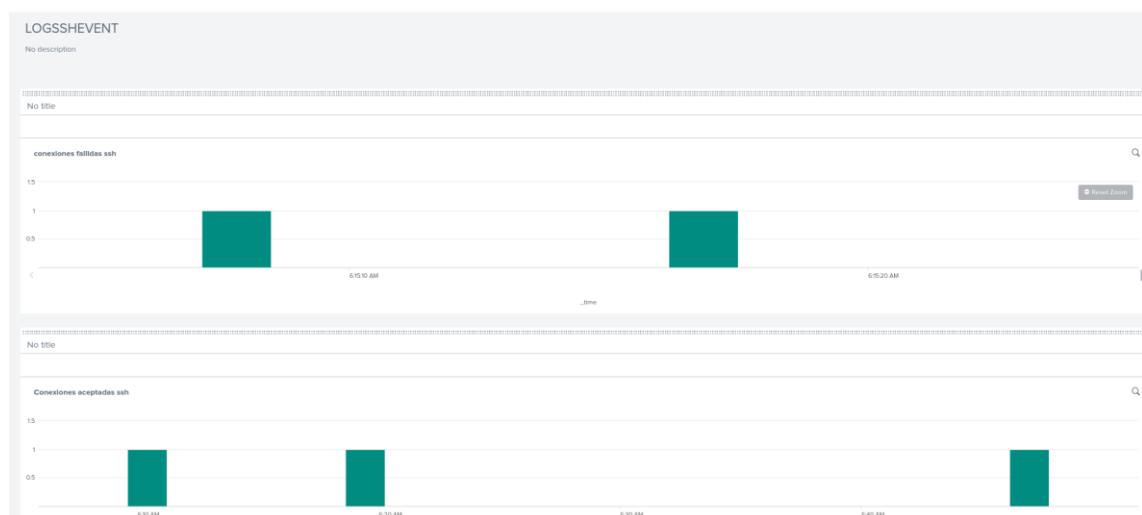


Ilustración 66 Dashboard conexiones fallidas y aceptadas

Para ver los logs de Windows sería aplicar lo mismo pero filtrando por los Eventcode 4624 y 4625.

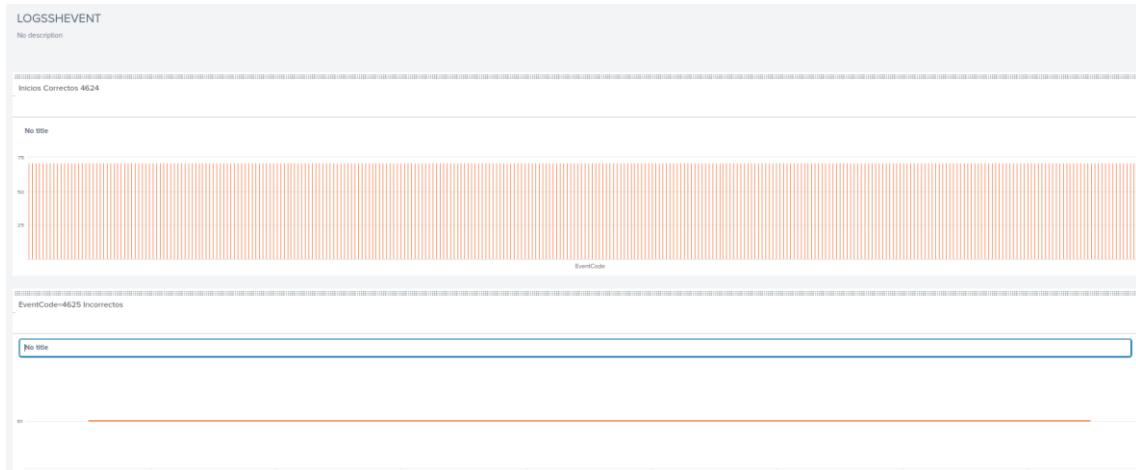


Ilustración 67 Dashboard conexiones aceptadas y fallidas

Ejercicio 2: Instalación de Elasticsearch

Instalación de elasticsearch

El primer paso ha sido instalar openssh-server. Esto asegura que el sistema pueda aceptar conexiones SSH permitiendo a los administradores acceder al terminal del servidor desde cualquier ubicación con las credenciales adecuadas.

```
vboxuser@carlosyenrique:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server
  ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 163 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,747 kB of additional disk space will
be used.
Do you want to continue? [Y/n] y
```

Ilustración 68 Instalación de openssh-server

Después hemos modificado el usuario para añadirlo a la lista de sudoers y darle privilegios de administrador. Al hacerlo nos aseguramos de que este usuario pueda ejecutar comandos con permisos elevados, necesarios para tareas de configuración y mantenimiento del sistema.

```
vboxuser@carlosyenrique:~$ sudo usermod -aG sudo vboxuser
```

Ilustración 69 Actualización de privilegios del usuario

Hemos instalado curl que es lo que nos dejará hacer llamadas a la API de Elasticsearch y será lo que usemos para probar y gestionar las distintas operaciones ofrecidas por Elasticsearch, como la creación de índices, la consulta de documentos o la configuración del clúster, siendo así una forma rápida de verificar que el servicio funciona correctamente.

```
vboxuser@carlosyenrique:~$ sudo apt install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcurl3t64-gnutls libcurl4t64
The following NEW packages will be installed:
  curl
```

Ilustración 70 Instalación de curl

El siguiente paso ha sido aumentar la memoria virtual disponible para asignarla a la máquina virtual de java (JVM), que es el motor subyacente utilizado por Elasticsearch. Este ajuste es para garantizar que el servicio pueda manejar cargas de trabajo más pesadas y ser más eficiente.

```
vboxuser@carlosyenrique:~$ sudo sysctl -w vm.max_map_count=2
62144
vm.max_map_count = 262144
vboxuser@carlosyenrique:~$
```

Ilustración 71 ajuste del sistema

Ahora es el momento de instalar Java. Esto garantiza que el entorno tenga la capacidad de ejecutar la JVM, que es necesaria para que Elasticsearch y sus servicios funcionen correctamente.

```
vboxuser@carlosyenrique:~$ sudo apt install openjdk-8-jdk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

Ilustración 72 Instalación de java

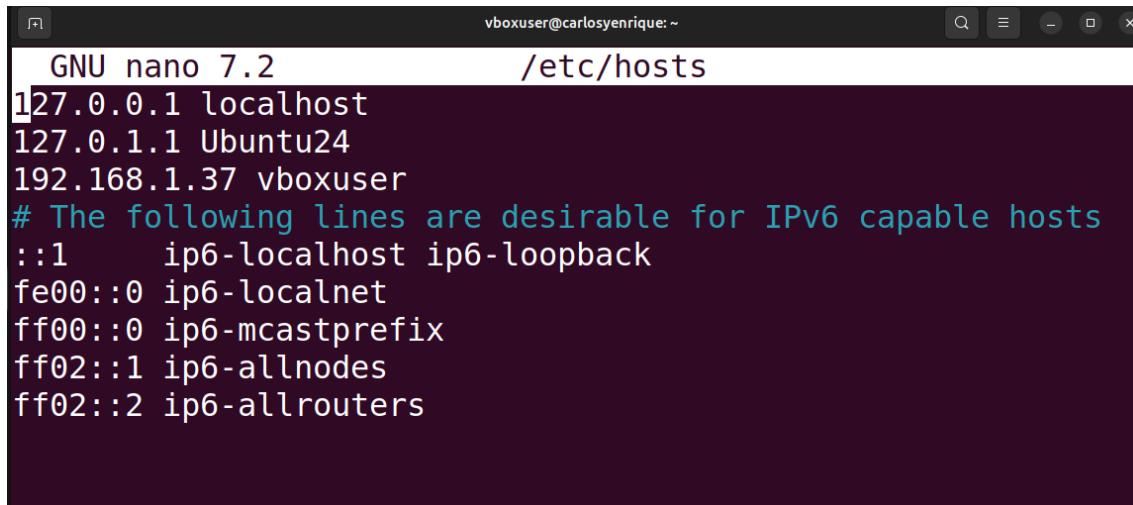
Después de instalar Java, hemos comprobado su versión con el comando:

```
vboxuser@carlosyenrique:~$ java -version
openjdk version "1.8.0_432"
OpenJDK Runtime Environment (build 1.8.0_432-8u432-ga~us1-0u
buntu2~24.04-ga)
OpenJDK 64-Bit Server VM (build 25.432-bga, mixed mode)
```

Ilustración 73 Comprobación de la versión de java

A continuación, hemos editado el archivo /etc/hosts para añadir la dirección IP local, y que los servicios puedan resolver correctamente el nombre del host. Este archivo actúa como un mapa entre nombres de host y direcciones IP permitiendo que los servicios se comuniquen dentro del sistema.

Al realizar este ajuste, nos aseguramos que no habrá problemas de conectividad ni de resolución de nombres durante la ejecución de Elasticsearch.



```
GNU nano 7.2          /etc/hosts
127.0.0.1 localhost
127.0.1.1 Ubuntu24
192.168.1.37 vboxuser
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Ilustración 74 Archivo /etc/hosts/

El siguiente paso ha sido descargar desde la página oficial de Elastic las cuatro aplicaciones que utilizaremos en este proyecto: Elasticsearch, Kibana, Logstash y Filebeat. Cada una de estas herramientas sirve para algo específico dentro del ecosistema. En este caso son las que nos dejarán gestionar, procesar, visualizar y analizar datos.

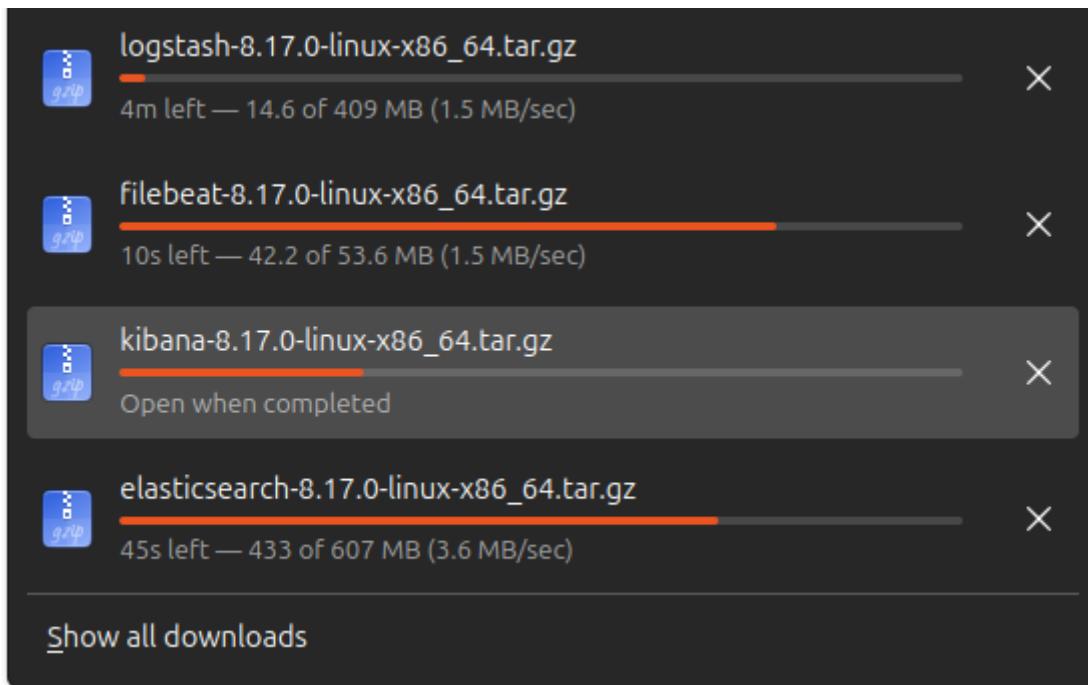


Ilustración 75 Descargas activas

Ahora iniciamos Elasticsearch utilizando el comando ./ que ejecuta directamente el binario desde el directorio de instalación.

```
vboxuser@carlosyenrique:~/Downloads$ ./elasticsearch-8.17.0/bin/elasticsearch
CompileCommand: dontinline java/lang/invoke/MethodHandle.set
AsTypeCache bool dontinline = true
CompileCommand: dontinline java/lang/invoke/MethodHandle.ast
ypeUncached bool dontinline = true
[2024-12-14T18:18:43,887][INFO ][o.e.n.j.JdkVectorLibrary ]
[carlosyenrique] vec_caps=0
[2024-12-14T18:18:43,898][INFO ][o.e.n.NativeAccess      ]
[carlosyenrique] Using native vector library; to disable sta
rt with -Dorg.elasticsearch.nativeaccess.enableVectorLibrary
```

Ilustración 76 Inicialización de elasticsearch

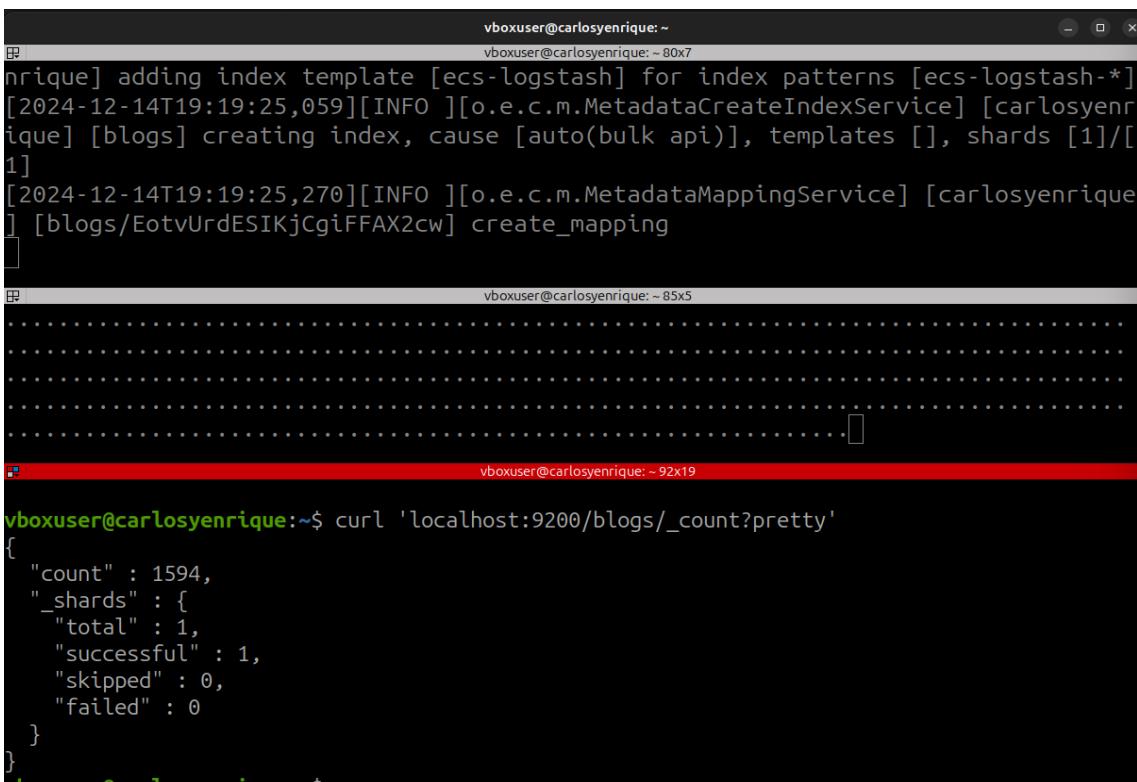
Una vez que elasticsearch está en funcionamiento vamos a iniciar logstash utilizando el archivo de configuración específico para la práctica. Este archivo ha sido lo hemos modificado para nuestro usuario en concreto vboxuser.

El archivo de configuración incluye detalles como la ruta de entrada de los logs, el formato de los datos y la conexión a elasticsearch.

```
vboxuser@carlosyenrique:~$ sudo ./logstash-8.17.0/bin/logstash -f blogs_csv.conf
Using bundled JDK: /home/vboxuser/logstash-8.17.0/jdk
Sending Logstash logs to /home/vboxuser/logstash-8.17.0/logs which is now configured via log4j2.properties
```

Ilustración 77 Inicialización de logstash

Una vez que estos dos servicios están corriendo comprobamos que la conexión entre ellos es buena usando el comando curl que realiza una solicitud HTTP directamente al servicio de elasticsearch para comprobar que está recibiendo datos desde logstash y que todo está funcionando bien.



The screenshot shows a terminal window with two tabs. The top tab has the title 'vboxuser@carlosyenrique: ~' and contains log output from logstash. It shows index creation for 'blogs' and mapping creation for 'blogs/_count'. The bottom tab has the title 'vboxuser@carlosyenrique: ~ 85x5' and contains the command 'curl 'localhost:9200/blogs/_count?pretty''. The response is a JSON object with 'count': 1594 and '_shards': { 'total': 1, 'successful': 1, 'skipped': 0, 'failed': 0 }.

```
vboxuser@carlosyenrique:~$ sudo ./logstash-8.17.0/bin/logstash -f blogs_csv.conf
Using bundled JDK: /home/vboxuser/logstash-8.17.0/jdk
Sending Logstash logs to /home/vboxuser/logstash-8.17.0/logs which is now configured via log4j2.properties

[2024-12-14T19:19:25,059][INFO ][o.e.c.m.MetadataCreateIndexService] [carlosyenrique] [blogs] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]
[2024-12-14T19:19:25,270][INFO ][o.e.c.m.MetadataMappingService] [carlosyenrique] [blogs/EotvUrdESIKjCgiFFAX2cw] create_mapping
[2024-12-14T19:19:25,270][INFO ][o.e.c.m.MetadataMappingService] [carlosyenrique] [blogs/EotvUrdESIKjCgiFFAX2cw] create_mapping

vboxuser@carlosyenrique:~$ curl 'localhost:9200/blogs/_count?pretty'
{
  "count" : 1594,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  }
}
```

Ilustración 78 Petición curl de comprobación

Ahora usaremos filebeats para capturar registros hacia elastic.

Lo primero ha sido cambiar el archivo de configuración filebeats.yml y poner nuestro usuario. Lo iniciamos indicando el archivo de configuración y hacemos un curl count para ver si le llegan los logs a elastic.

El resultado muestra que más de un millón de logs han sido capturados y enviados, lo que nos confirma que filebeat está funcionando bien y que elasticsearch está recibiendo los datos.

```
vboxuser@carlosyenrique:~/filebeat-8.17.0-linux-x86_64$ curl 'localhost:9200/_count?pretty'
{
  "count" : 1753070,
  "_shards" : {
    "total" : 4,
    "successful" : 4,
    "skipped" : 0,
    "failed" : 0
  }
}
```

Ilustración 79 Petición curl de verificación

Visualizar distintos valores en Kibana

El siguiente paso ha sido iniciar Kibana, la herramienta de visualización de datos y administración. Esta herramienta nos permite interactuar con los datos almacenados en elasticsearch para poder crear visualizaciones e incluirlas en dashboards.

También nos permite gestionar configuraciones avanzadas mediante la interfaz gráfica.

```
vboxuser@carlosyenrique: ~ 86x14
is now available: Task Manager is healthy
[2024-12-14T20:09:47.096+00:00][INFO ][status] Kibana is now available
[2024-12-14T20:09:47.175+00:00][INFO ][plugins.elasticAssistant.service] Updating data streams - .kibana-elastic-ai-assistant-attack-discovery-*
[2024-12-14T20:09:47.179+00:00][INFO ][plugins.fleet] Fleet Usage: {"agents_enabled":true,"agents":{},"total_enrolled":0,"healthy":0,"unhealthy":0,"offline":0,"inactive":0,"unenrolled":0,"total_all_statuses":0,"updating":0}, "fleet_server":{},"total_all_statuses":0,"total_enrolled":0,"healthy":0,"unhealthy":0,"offline":0,"updating":0,"inactive":0,"unenrolled":0,"num_host_urls":0}, "license_issued_to": "elasticsearch"
[2024-12-14T20:09:48.103+00:00][INFO ][plugins.reporting.store] Linking ILM policy to reporting data stream: .kibana-reporting, component template: kibana-reporting@custom
[2024-12-14T20:09:48.215+00:00][WARN ][plugins.alerting.usage] Error executing alerting telemetry task: getTotalAlertsCountAggregations - {}
```

Ilustración 80 Inicialización de kibana

Una vez iniciado Kibana accedemos a su interfaz a través del navegador utilizando la dirección del servidor y el puerto predeterminado 5601.

The screenshot shows the Elasticsearch Index Management interface. On the left, there's a sidebar with navigation links like Management, Ingest, Data, Index Management, Alerts and Insights, and Kibana. The main area is titled "Index Management" and has tabs for Indices, Data Streams, Index Templates, Component Templates, and Enrich Policies. Under the Indices tab, there's a search bar, filters for Lifecycle status and phase, and buttons for Reload indices and Create index. A table lists four indices: "blogs" (yellow, open, 1 primary, 1 replica, 1,594 documents, 10mb storage), "logs_server1" (yellow, open, 1 primary, 1 replica, 582,063 documents, 206.26mb storage), "logs_server2" (yellow, open, 1 primary, 1 replica, 584,599 documents, 208.23mb storage), and "logs_server3" (yellow, open, 1 primary, 1 replica, 584,814 documents, 207.45mb storage). Below the table, it says "Rows per page: 10".

Ilustración 81 Vista del index management

Ahora vamos a crear una nueva visualización con data view eligiendo un patrón para que recoja los logs. Creamos uno tanto para los logs del blog como para los de los servidores.

The screenshot shows the Elasticsearch Data Views interface. The left sidebar includes Management, Ingest, Data, Index Management, Alerts and Insights, and Kibana. The main area is titled "Vista 1 Carlos y Enrique" and has buttons for Delete, Set as default, and Edit. It shows an index pattern of "logs*" and a time field of "@timestamp". Below this, there are tabs for Fields (56), Scripted fields (0), Field filters (0), and Relationships (0). A table lists fields with columns for Name, Type, Format, Searchability, Aggregability, and Excluded. Fields listed include @timestamp (date), _id (_id), _ignored (_ignored), _index (_index), _score, _source, agent.ephemeral_id (text), agent.ephemeral_id.keyword (keyword), agent.id (text), and agent.id.keyword (keyword). At the bottom, it says "Rows per page: 10".

Ilustración 82 Vista del dataview

The screenshot shows the Elasticsearch Stack Management Data Views interface. On the left, there's a sidebar with various navigation links like Data, Index Management, Data Set Quality, Rollup Jobs, Transforms, Remote Clusters, Migrate, Alerts and Insights, Kibana, Data Views, and Stack. The main area is titled 'Vista 2 Carlos y Enrique logs server'. It shows an index pattern of 'logs_*' and a time field of '@timestamp'. Below this, there's a table for 'Fields (58)' with columns for Name, Type, Format, Searchable, Aggregatable, and Excluded. Fields listed include @timestamp, _id, _ignored, _index, _score, _source, agent ephemeral_id, agent ephemeral_id keyword, agent id, and agent id keyword. At the bottom right of the table, there are pagination controls (1, 2, 3, 4, 5, 6, >).

Ilustración 83 Vista de dataview

Ahora creamos las visualizaciones

Evolución de logs por tiempo: Gráfico de líneas para analizar la cantidad de logs generados a lo largo del tiempo usando el campo @timestamp.

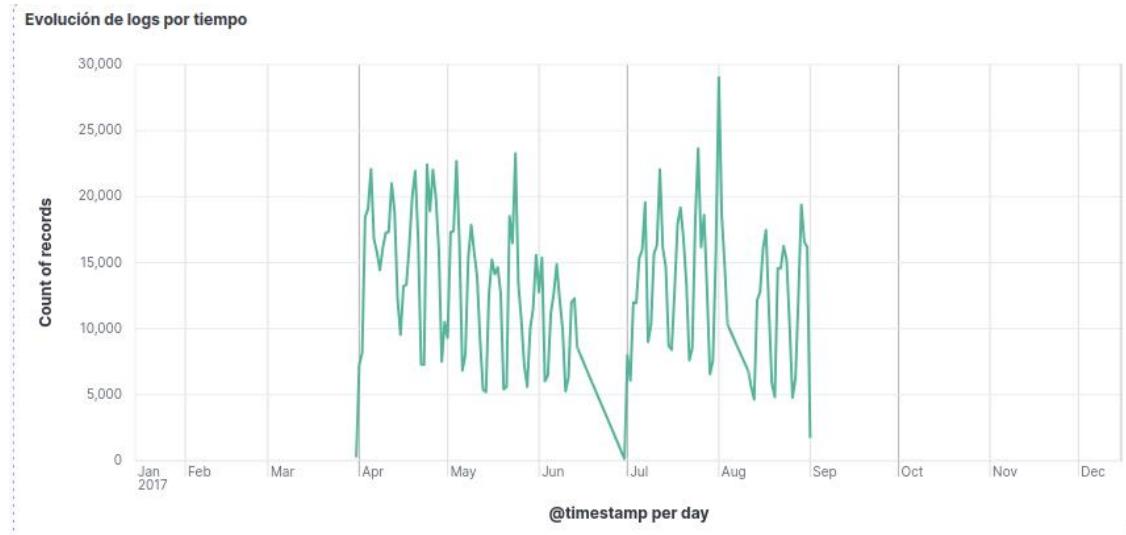


Ilustración 84 Evolución de logs por tiempo

Distribución de logs por nivel: Gráfico de barras para entender la severidad de los logs usando el campo level.keyword

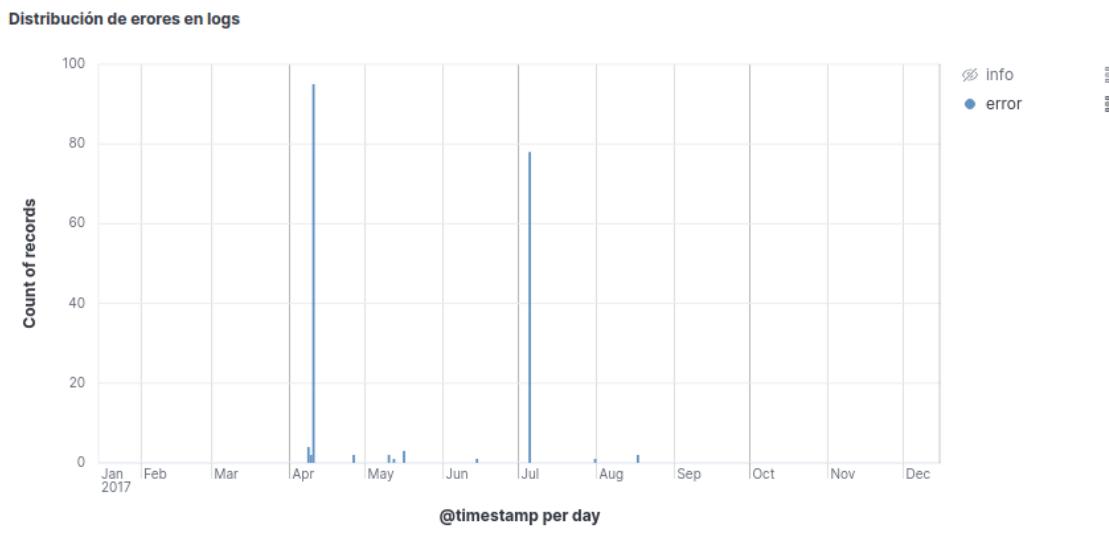


Ilustración 85 Distribución de logs por nivel

Distribución de logs por host: Gráfico circular para identificar qué host genera más logs con el campo host.keyword

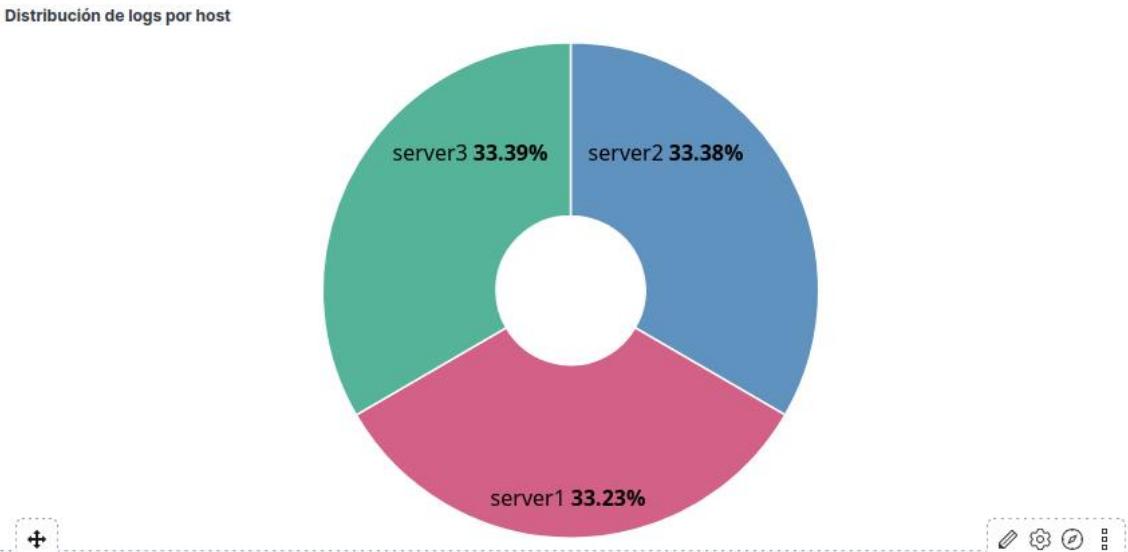


Ilustración 86 Distribución de logs por host

Tiempo de ejecución promedio: Métrica para calcular el tiempo promedio de ejecución de las solicitudes con el campo runtime_ms

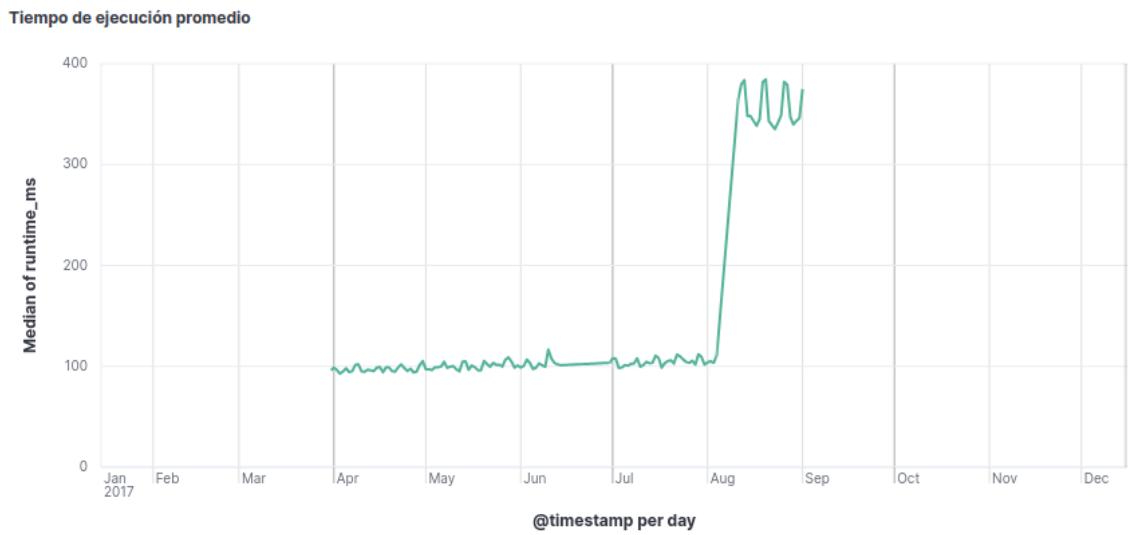


Ilustración 87 Tiempo de ejecución promedio

Tamaño de respuesta por host: Gráfico de barras para ver el tamaño promedio de las respuestas por host con el campo response_size y el campo host.keyword

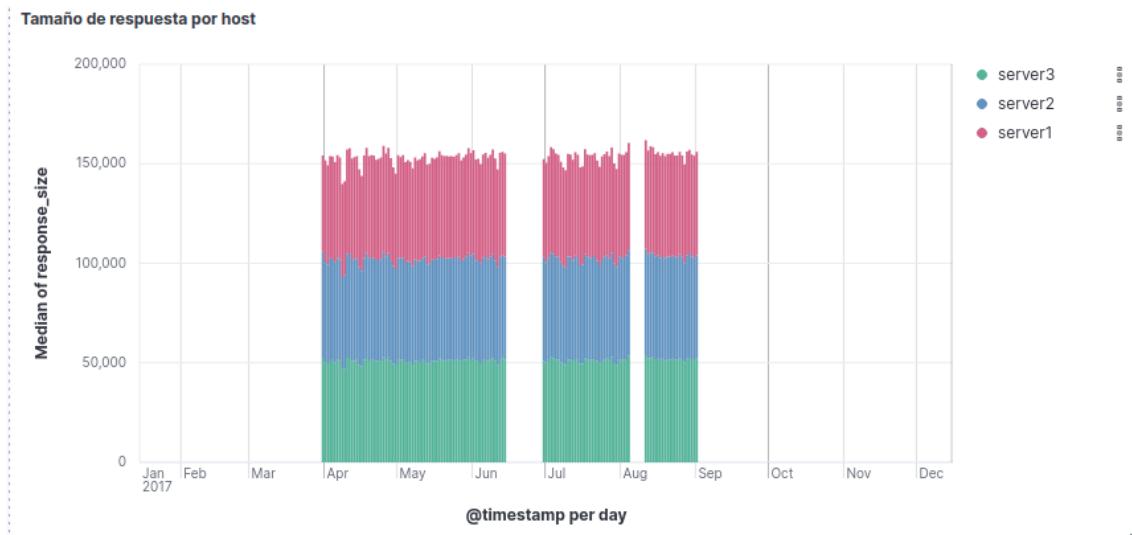


Ilustración 88 Tamaño de respuesta por host

Distribución de métodos HTTP: Gráfico circular para analizar qué métodos HTTP (GET, POST, etc.) se usan más con el campo method.keyword

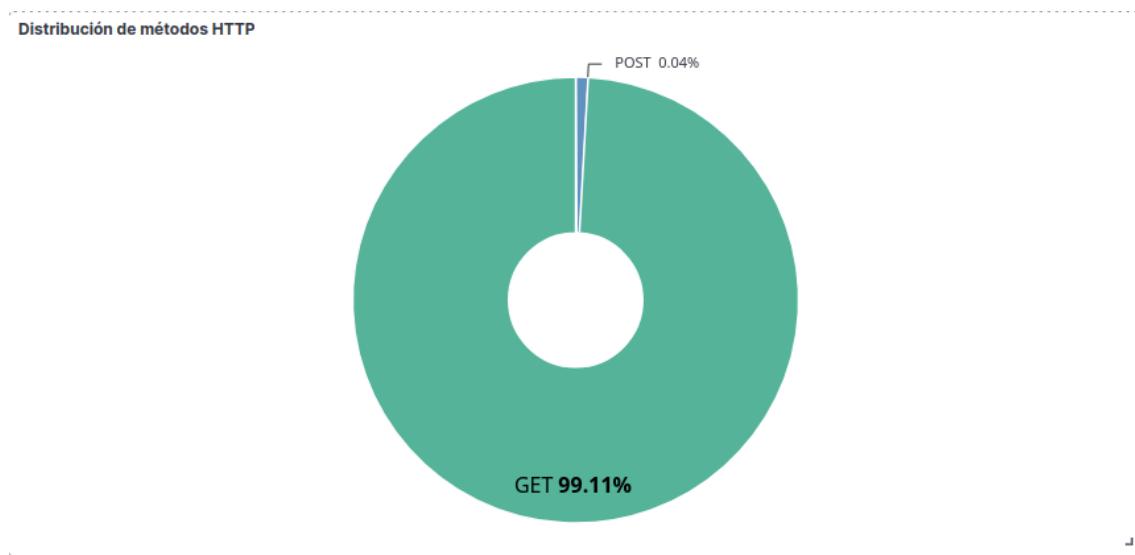


Ilustración 89 Distribución de métodos HTTP

Distribución de logs por ciudades: Este treemap muestra la distribución porcentual de logs por ciudades. Cada rectángulo representa una ciudad indicando la cantidad de logs registrados según el campo city

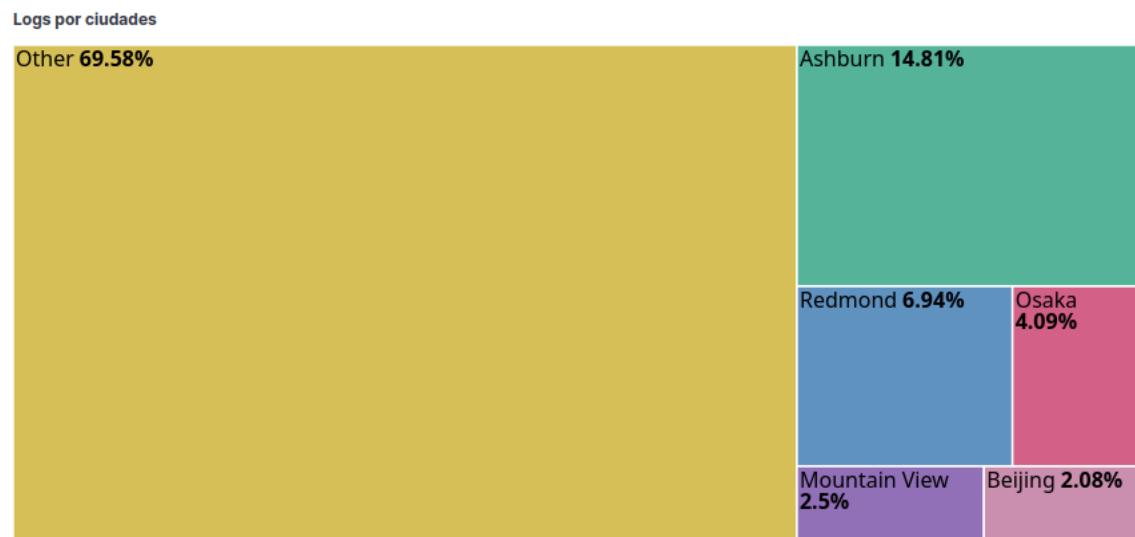


Ilustración 90 Distribución de logs por ciudades:

Distribución de los logs por continente y ciudades:

Gráfico de barras combinado que distribuye los logs por ciudades y a su vez por continentes usando el campo geoip.continent_code

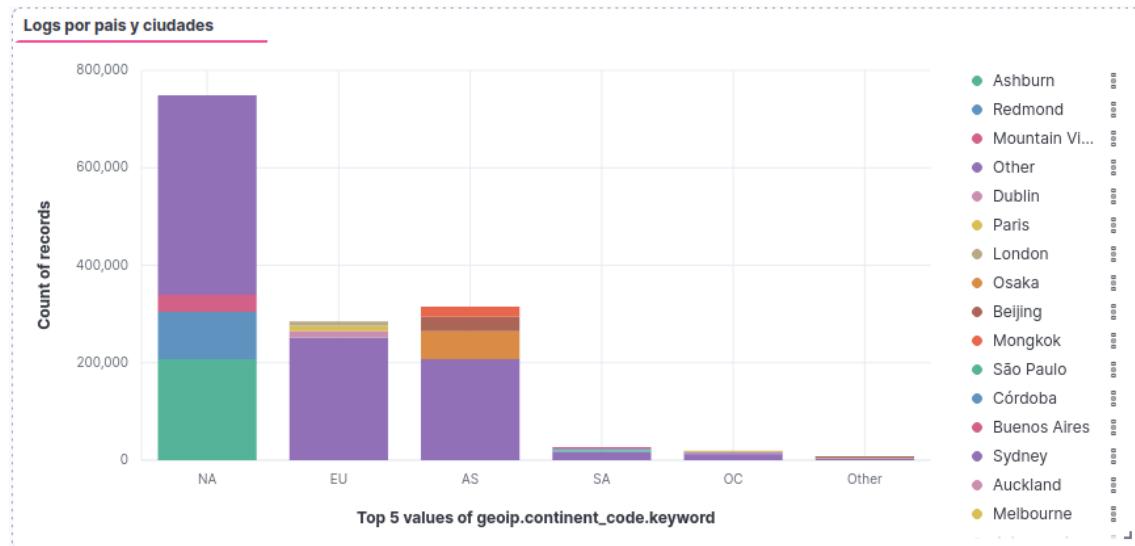


Ilustración 91 Gráfica de Distribución de los logs por continente y ciudades

El dashboard de kibana donde visualizar todos los datos quedaría así, agrupando todas las gráficas en un mismo sitio.

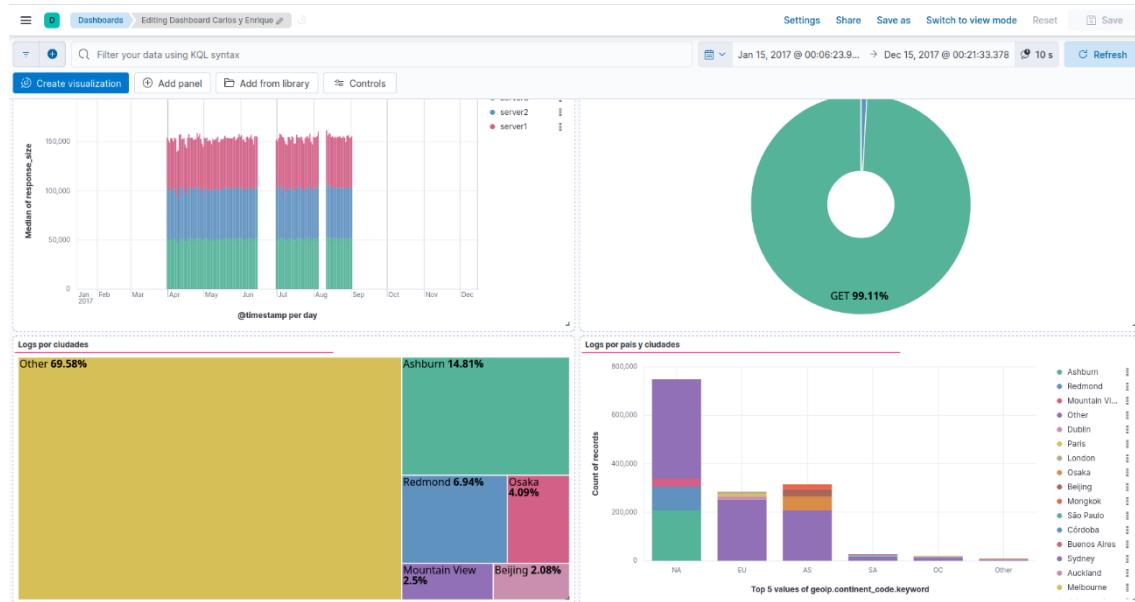


Ilustración 92 Dashboard de Kibana

Mejorando la seguridad en elasticsearch

Como parte extra de la práctica hemos querido darle un poco más de seguridad al entorno por lo que lo primero que hemos hecho es abrir la consola de dev tools.

Con el comando GET / podemos ver la información básica del clúster donde se encuentra la versión de la instancia de elasticsearch, el nombre del nodo y el nombre del clúster.

The screenshot shows the Elasticsearch Dev Tools Console interface. The top navigation bar includes 'Dev Tools' and 'Console'. The 'Console' tab is selected. The left panel is the 'Shell' tab, containing a code editor with the following content:

```
1 # Welcome to the Dev Tools Console!
2 #
3 # You can use Console to explore the Elasticsearch API.
4 # See the Elasticsearch API reference to learn more:
5 # https://www.elastic.co/guide/en/elasticsearch/reference/current/rest-apis.html
6 #
7 # Here are a few examples to get you started.
8
9 # Create an index
10 PUT /my-index
11
12
13 # Add a document to my-index
14 POST /my-index/_doc
15 {
16   "id": "park_rocky-mountain",
17   "title": "Rocky Mountain",
18   "description": "Bisected north to south by the
Continental Divide, this portion of the Rockies
has ecosystems varying from over 150 riparian
lakes to montane and subalpine forests to
treeless alpine tundra."
19 }
20
21
22 # Perform a search in my-index
23 GET /
```

The right panel displays the response to the GET request:

```
1 {
2   "name": "carlosyenrique",
3   "cluster_name": "elasticsearch",
4   "cluster_uuid": "zuABC0-NTWCNvx2zocFp6g",
5   "version": {
6     "number": "8.17.0",
7     "build_flavor": "default",
8     "build_type": "tar",
9     "build_hash":
10       "2b6a7fed44faa321997703718f07ee0420804b41",
11     "build_date": "2024-12-11T12:08:05.663969764Z",
12     "build_snapshot": false,
13     "lucene_version": "9.12.0",
14     "minimum_wire_compatibility_version": "7.17.0",
15     "minimum_index_compatibility_version": "7.0.0"
16   },
17   "tagline": "You Know, for Search"
```

At the bottom, the status bar shows '200 - OK' and '17 ms'.

Ilustración 93 Petición GET para verificar el contenido

Con este comando podemos ver la información de los índices:

The screenshot shows the Elasticsearch Dev Tools Console interface. The top navigation bar includes 'Dev Tools' and 'Console'. The 'Console' tab is selected. The left panel is the 'Shell' tab, containing a code editor with the following content:

```
1 GET /_cat/indices
```

The right panel displays the response to the GET request:

```
1 green open .internal.alerts-transform.health.alerts-default-000001
2 green open .internal.alerts-observability.logs.alerts-default-000001
3 green open .internal.alerts-observability.uptime.alerts-default-000001
4 yellow open logs._server2
```

Ilustración 94 Petición GET para verificar el contenido

Ahora vamos a cambiar el archivo de configuración `elasticsearch.yml` y añadir un nombre de clúster. Esto ayuda a identificar el clúster en entornos donde haya muchas instancias de elasticsearch (antes esta línea estaba comentada).

```

vboxuser@carlosyenrique:~/elasticsearch-8.17.0/config 86x16
GNU nano 7.2                                     elasticsearch.yml *
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: elastic_cluster
#
# ----- Node -----
#

```

Ilustración 95 Archivo de configuración de elasticsearch

Después hemos iniciado kibana con el parámetro -E node.name=node1, lo que nos permite asignar un nombre específico al nodo en ejecución y comprobamos con el GET que se ha hecho el cambio de forma correcta.

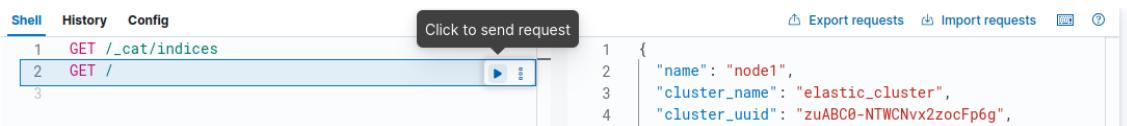


Ilustración 96 Petición GET para ver el cambio

El siguiente paso consiste en modificar el tamaño del heap de memoria asignado a la JVM utilizada por elasticsearch para mejorar el rendimiento. Este ajuste se hace editando estas dos líneas en el archivo jvm.options que antes estaban comentadas.

```

vboxuser@carlosyenrique:~/elasticsearch-8.17.0/config 86x16
GNU nano 7.2                                     jvm.options *
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## which should be named with .options suffix, and the min and
## max should be set to the same value. For example, to set the
## heap to 4 GB, create a new file in the jvm.options.d
## directory containing these lines:
##
-Xms4g
-Xmx4g
##
```

Ilustración 97 jvm.options

Para habilitar características avanzadas de seguridad como el cifrado de las comunicaciones TLS, la gestión avanzada de usuarios y roles o el control de acceso basado en IP es necesario registrarse y activar la prueba gratuita de 30 días

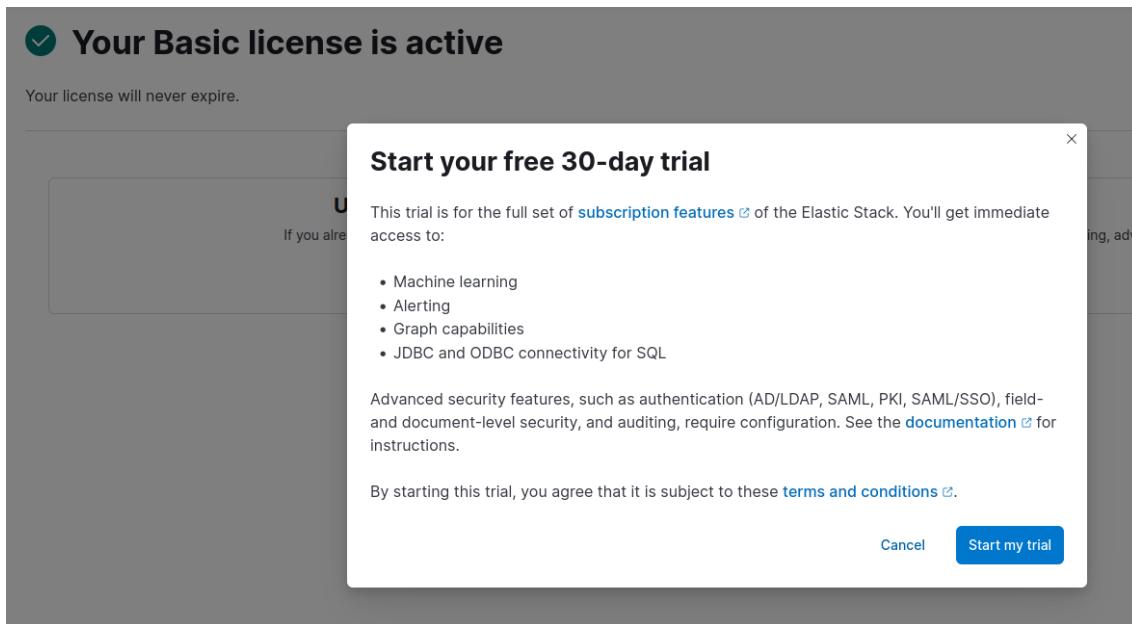


Ilustración 98 Mensaje de licencia activada

✓ Your Trial license is active

Your license will expire on January 14, 2025 1:29 AM GMT

Ilustración 99 Mensaje de licencia activada

Ahora de nuevo en el archivo de configuración cambiamos estos parámetros a true para activar las opciones de seguridad avanzadas y reiniciamos los servicios.

Esto activa la autenticación, la autorización y el cifrado en las comunicaciones entre clientes y nodos.

```
vboxuser@carlosyenrique: ~/elasticsearch-8.17.0/config$ nano elasticsearch.yml
GNU nano 7.2
elasticsearch.yml *
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 14-12-2024 18:18:36
#
# -----
#
# Enable security features
xpack.security.enabled: true
xpack.security.enrollment.enabled: true
```

Ilustración 100 Petición curl de comprobación

De esta forma al hacer ahora una petición nos va a saltar este error ya que necesitaremos una contraseña para autenticar la petición.

```
vboxuser@carlosyenrique:~/elasticsearch-8.17.0/config$ curl 'localhost:9200/*/nodes?pretty'
{
  "error" : {
    "root_cause" : [
      {
        "type" : "security_exception",
        "reason" : "missing authentication credentials for REST request [/*/nodes?pretty]",
        "header" : {
          "WWW-Authenticate" : [
            "Basic realm=\"security\"", "charset=UTF-8",
            "ApiKey"
          ]
        }
      }
    ]
  }
}
```

Ilustración 101 Petición curl de comprobación

Esta contraseña la generamos con el siguiente comando:

```
vboxuser@carlosyenrique:~$ ./elasticsearch-8.17.0/bin/elasticsearch-reset-password -u elastic
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y

Password for the [elastic] user successfully reset.
New value: dTyqe-z_gp_hDYva=1wn
```

Ilustración 102 Comando para generar la contraseña

Ahora al hacer el curl nos pide la contraseña y nos devuelve el resultado

```
vboxuser@carlosyenrique:~$ curl -u elastic --anyauth 'localhost:9200/_cat/nodes?pretty'
Enter host password for user 'elastic':
127.0.0.1 8 97 3 0.27 0.44 0.45 cdfhilmrstw * node1
```

Ilustración 103 Petición curl para comprobación

En este punto tenemos que indicarle a kibana que también requerirá autenticación para conectarse con elastisearch por lo que en su archivo de configuración añadimos el usuario y la contraseña y reiniciamos los servicios.

```
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the
# index at startup. Your Kibana users still need to authenticate with Elasticsearch,
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "dTyqe-z_gp_hDYva=1wn"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
```

Ilustración 104 Archivo de configuración de elasticsearch

Además, como estamos en la última versión podemos hacer esto de forma más eficiente generando un token en elasticsearch:

```
vboxuser@carlosyenrique:~/elasticsearch-8.17.0$ ./bin/elasticsearch-service-tokens create elastic/kibana kibana-token  
SERVICE_TOKEN elastic/kibana/kibana-token = AAEAAWVsYXN0aW Mva2liYW5hL2tpYmFuYS10b2tlbjoxQTVjQkZCRFFwVzQ1bFRITWhvUDZn
```

Ilustración 105 Generación del token en elasticsearch

Y añadiéndolo al keystore de kibana:

```
vboxuser@carlosyenrique:~/kibana-8.17.0$ sudo chown -R vboxuser:vboxuser /home/vboxuser/kibana-8.17.0/config  
vboxuser@carlosyenrique:~/kibana-8.17.0$ ./bin/kibana-keystore create  
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider  
Created Kibana keystore in /home/vboxuser/kibana-8.17.0/config/kibana.keystore  
vboxuser@carlosyenrique:~/kibana-8.17.0$ ./bin/kibana-keystore add elasticsearch.serviceAccountToken  
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider  
Enter value for elasticsearch.serviceAccountToken: ****  
*****
```

Ilustración 106 Se añade el token al keystore de kibana

Ahora, al iniciar Kibana nos aparece una pantalla para hacer login en elasticsearch. Esto añade una capa de autenticación que protege el acceso al sistema.

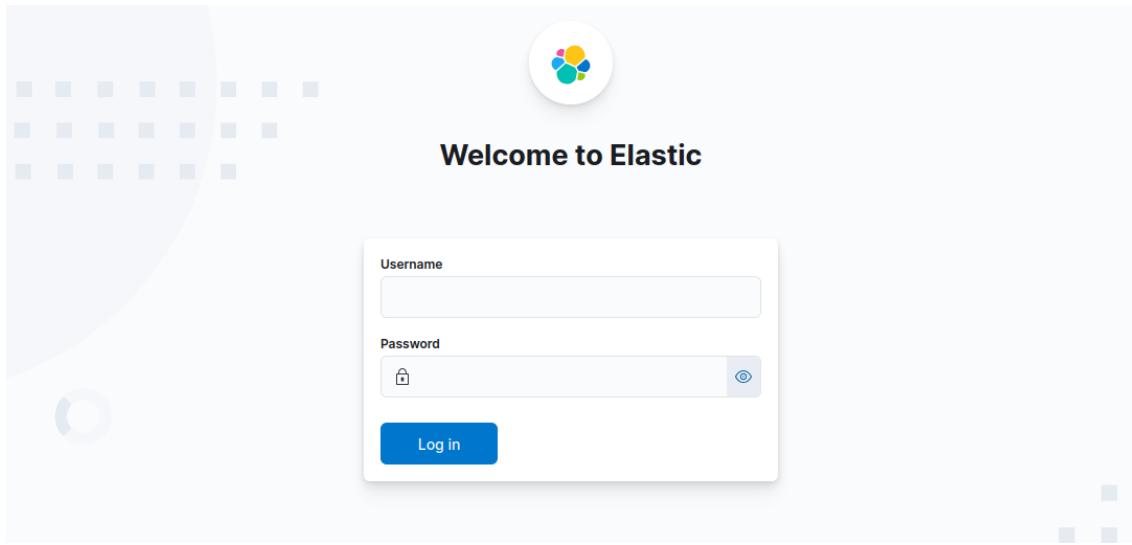


Ilustración 107 Autenticación de elasticsearch

Al implementar estas medidas de seguridad hemos reforzado la protección del entorno asegurando que elasticsearch no esté expuesto a accesos no autorizados y así mantener la integridad y la confidencialidad de la información.