# TAREA 07

# SIEM ELK

## INCIDENTES DE CIBERSEGURIDAD

**ALBA MOREJÓN GARCÍA**

**2024/2025**

**Ciberseguridad en Entornos de las Tecnologías de la Información**

**La Monitorización Multipunto en el SIEM**

**En la Unidad 7 hemos estudiado cómo instalar y configurar un SIEM ELK completo, situándolo en la misma red que los diferentes agentes IDS que detectarán las intrusiones y enviarán la información de registros de SNORT a través de Filebeat.**

**La estructura creada en la Tarea 6, es la presente en cualquier entorno productivo en la que suele haber una sonda Snort en cada una de las máquinas perimetrales, comprometidas, vulnerables, etc., cuya información de logging se ha de redirigir hacia una única máquina en la que estará instalado el SIEM (Elastic Stack).**

**Pues bien, continuando con el trabajo iniciado en la Tarea 6 asociada a la Unidad 6, en esta tarea abordaremos la lectura y tratamiento del log que centraliza la información de todas las sondas Snort, filtrando su contenido, almacenándolo en la base de datos y preparando un conjunto de visualizaciones que recogeremos en un Tablero de Monitorización Multipunto.**

**Apartado 1: Instalación y configuración de Elasticsearch.**

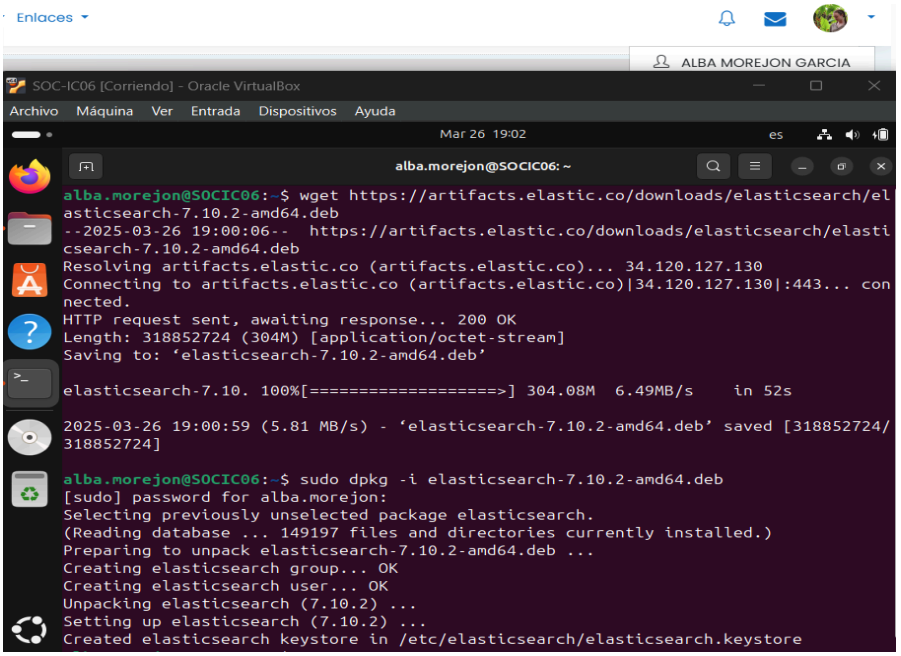
**a) Detallar la configuración a efectuar en Elasticsearch.**

**b) Prueba de funcionamiento de Elasticsearch.**

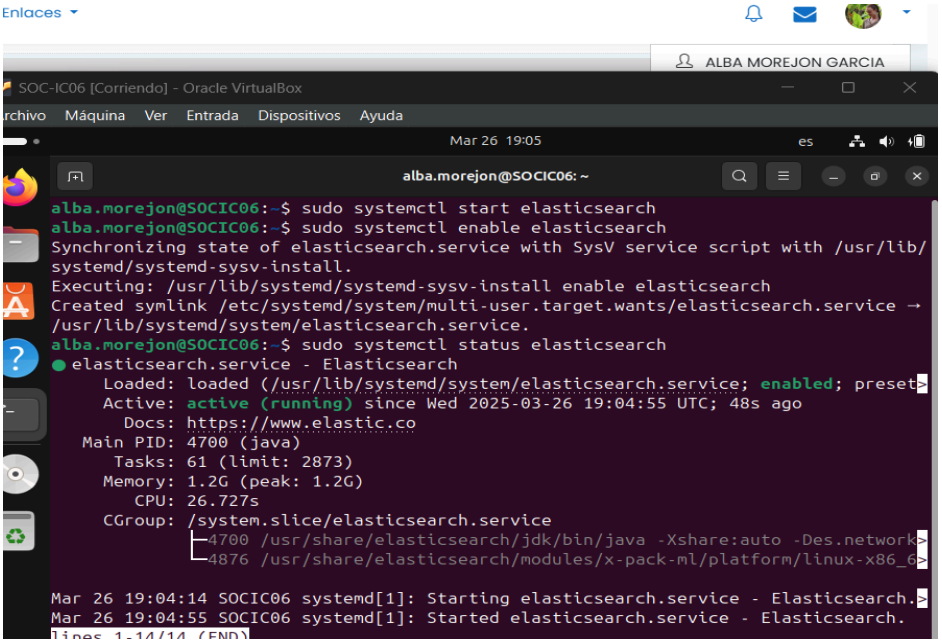
Descargamos e instalamos Elasticsearch con los siguientes comandos:

wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.10.2-amd64.deb

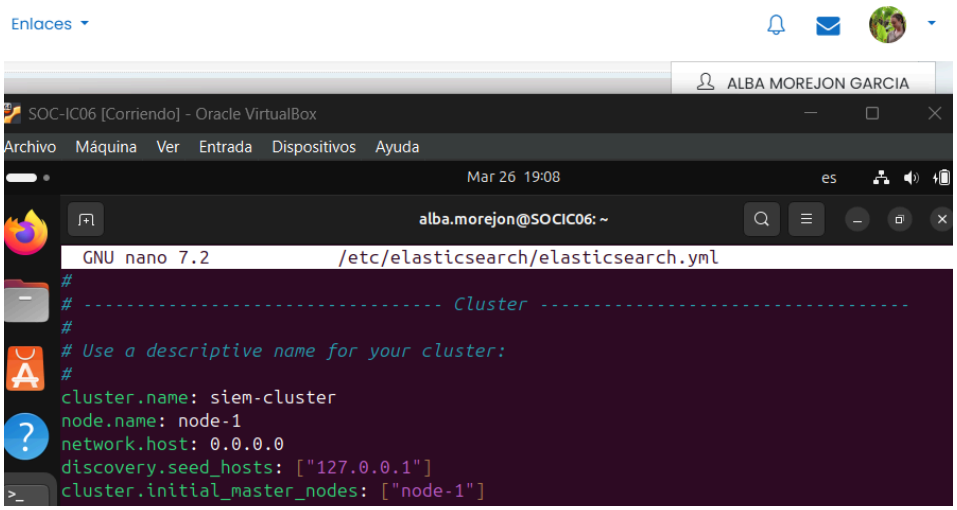
sudo dpkg -i elasticsearch-7.10.2-amd64.deb



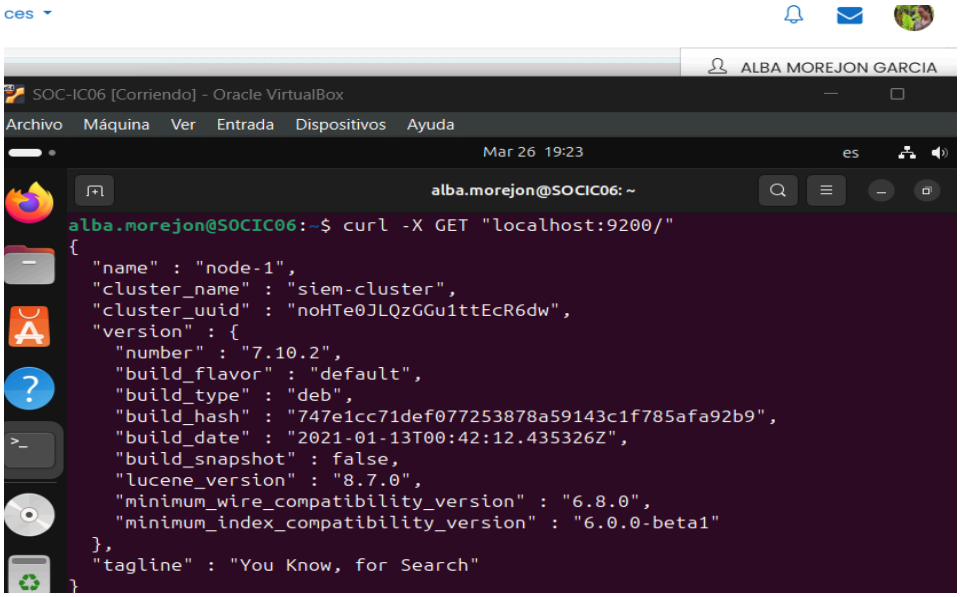

Iniciamos el servicio y comprobamos su estado



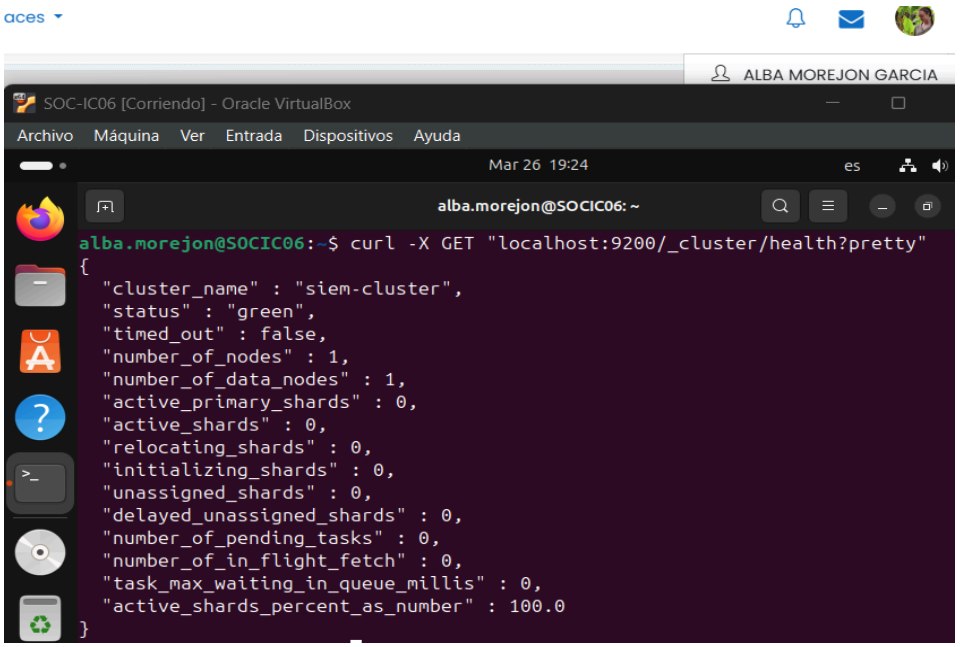

Añadimos la siguiente configuración en el fichero elasticsearch.yml para que pueda iniciar y funcionar correctamente: asignamos un nombre al cluster y al nodo, le indicamos las interfaces de red disponibles, le indicamos la dirección y el nodo principal desde el que se actuará.



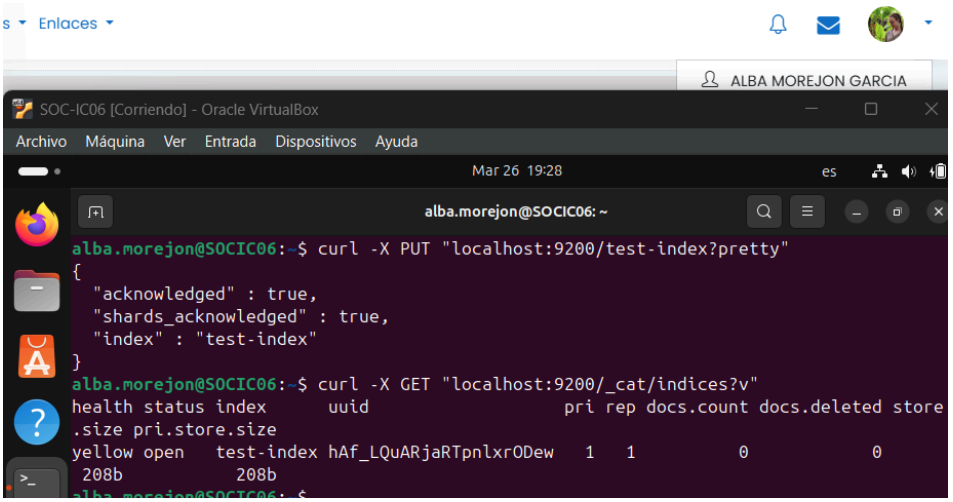

Comprobamos que esté bien configurado:
Se realiza una solicitud al servidor para obtener información básica sobre el nodo (nombre del nodo y el cluster, versión elasticsearch y otras configuraciones)




Se realiza una solicitud para tener información sobre el estado del cluster, el número de nodos, número de shards…

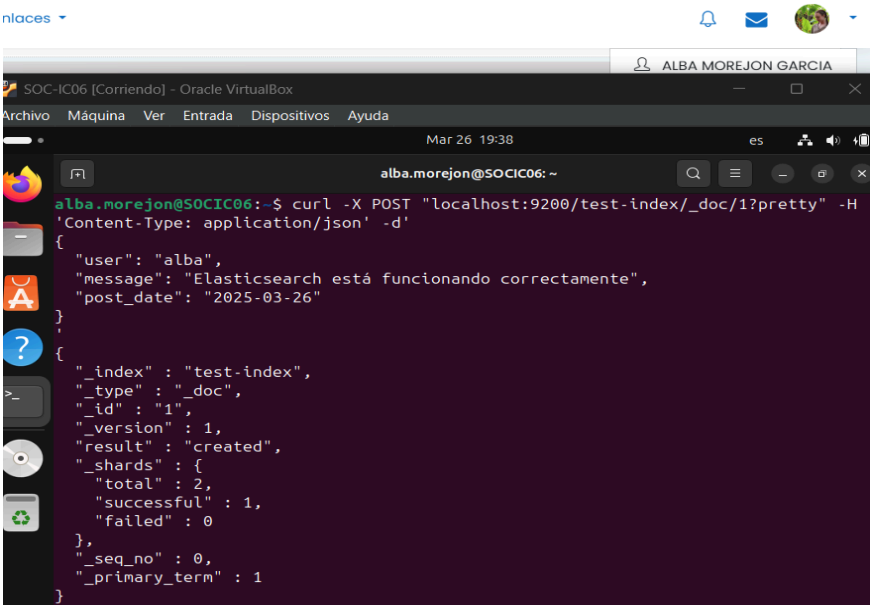



Creamos un índice (test.index) y vemos que se haya configurado correctamente. Listamos todos los índices existentes dentro del clúster, mostrando el estado, el nombre el UUID…

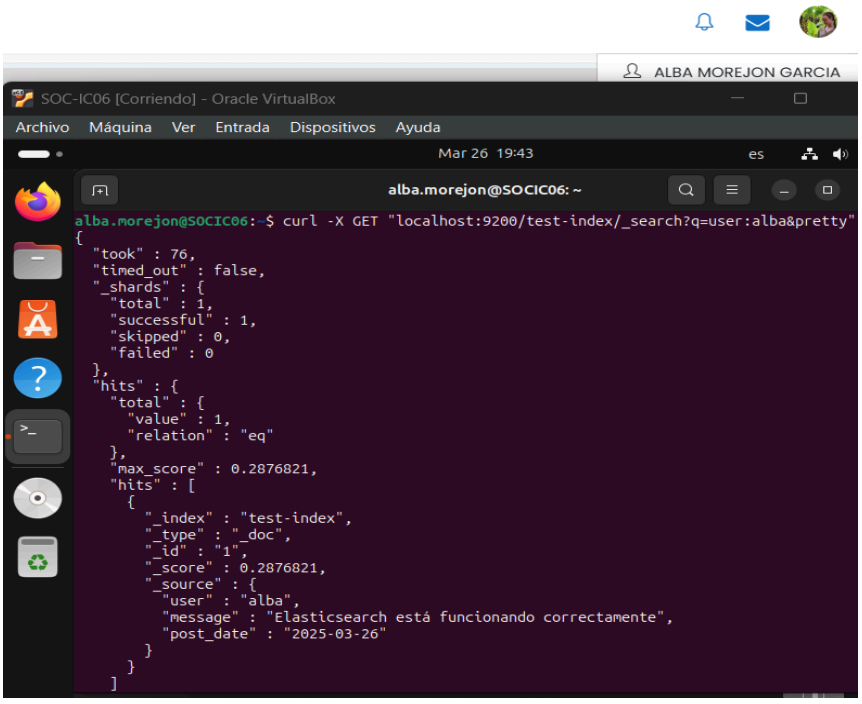



Pruebas:

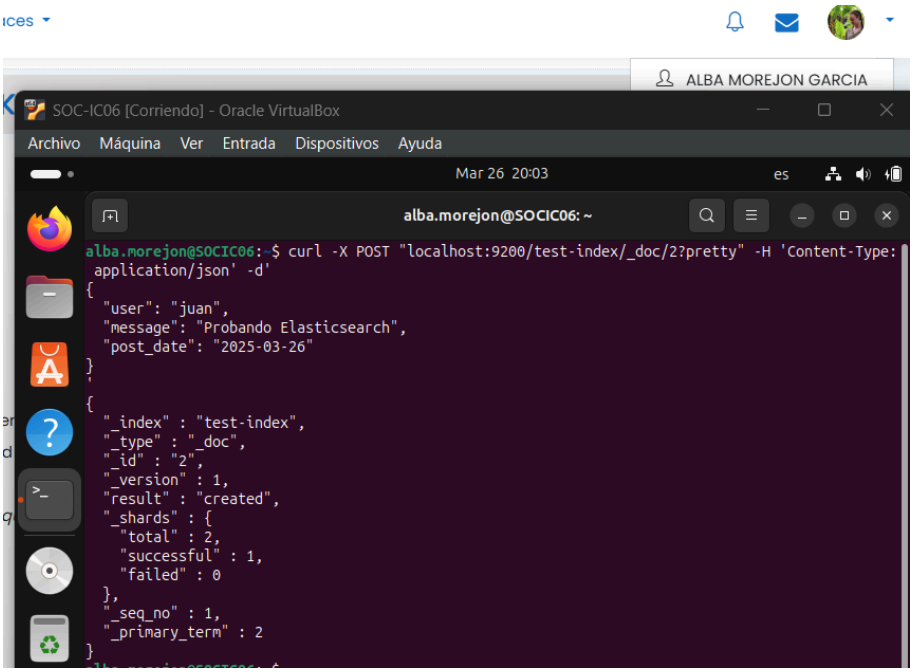
Creamos un documento en el índice creado anteriormente, test-index (con los datos del inicio del código)



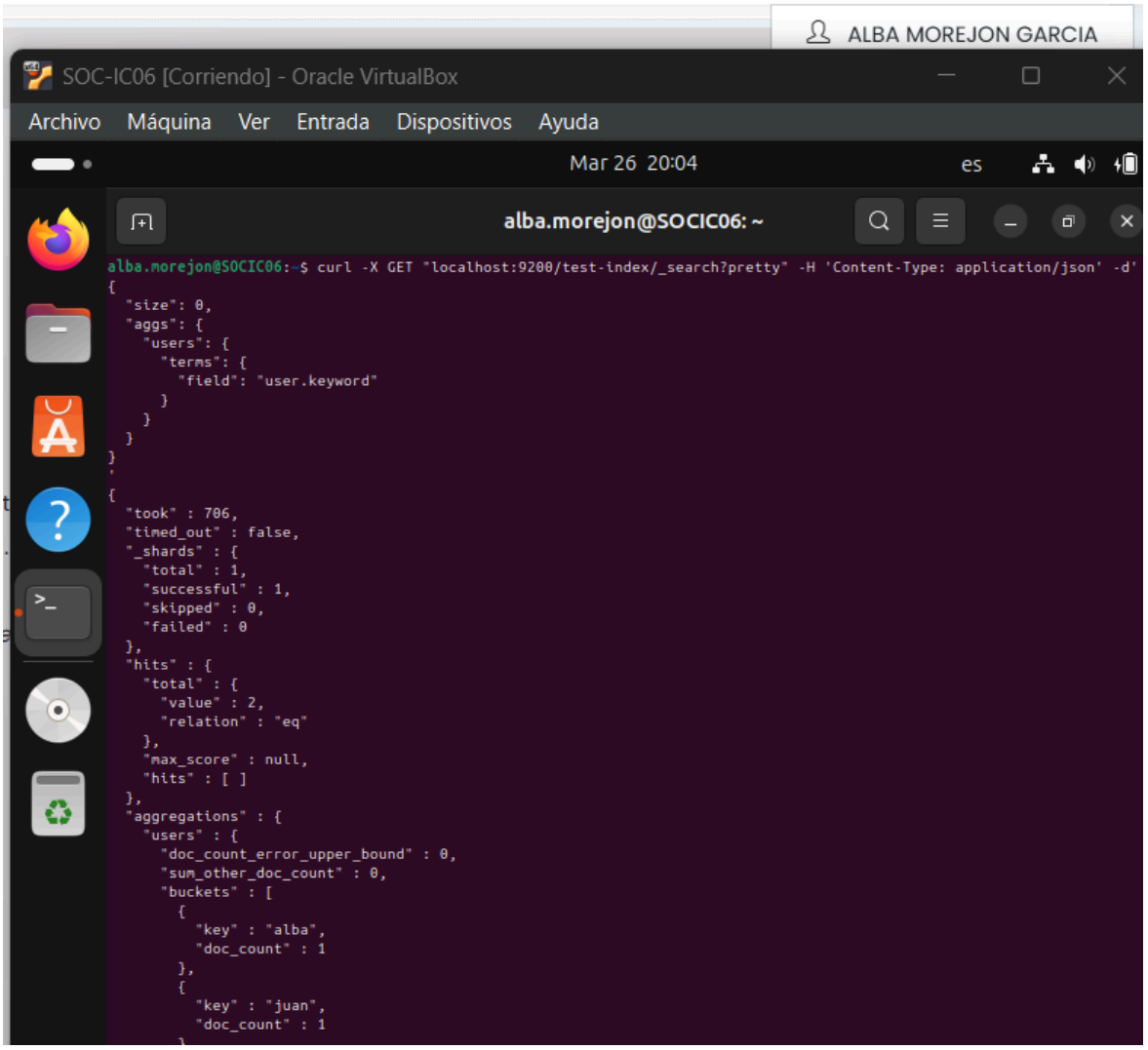

Realizamos una búsqueda en el índice buscando el documento anterior



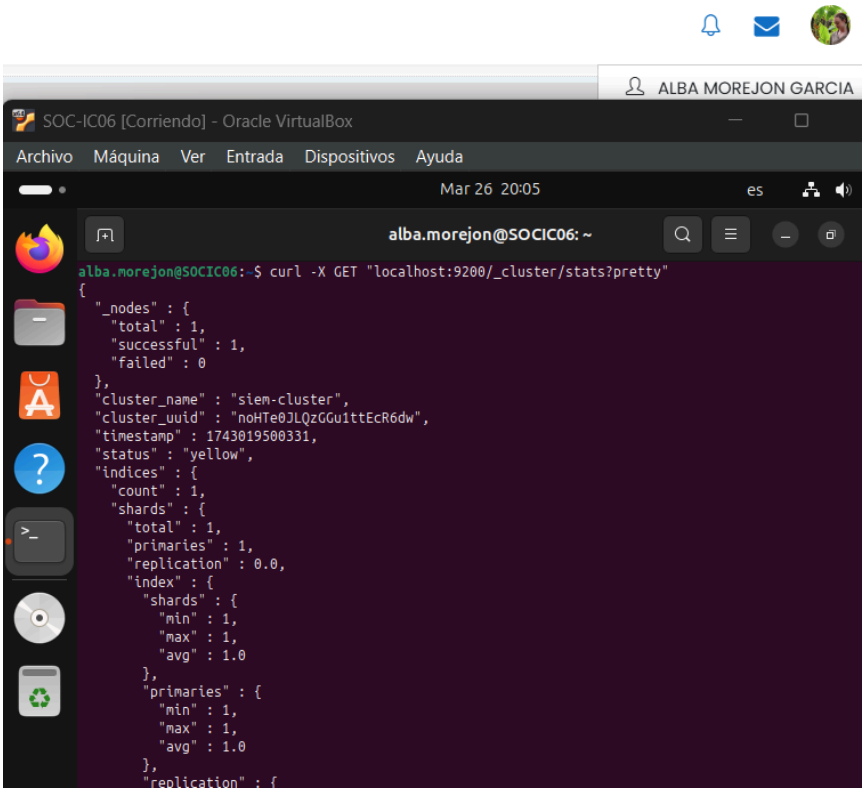

Agregamos otro documento en el mismo índice:




Utilizamos el siguiente comando para contar cuantos documentos existen de cada usuario




Obtenemos información y verificamos de nuevo que el clúster esté funcionando correctamente

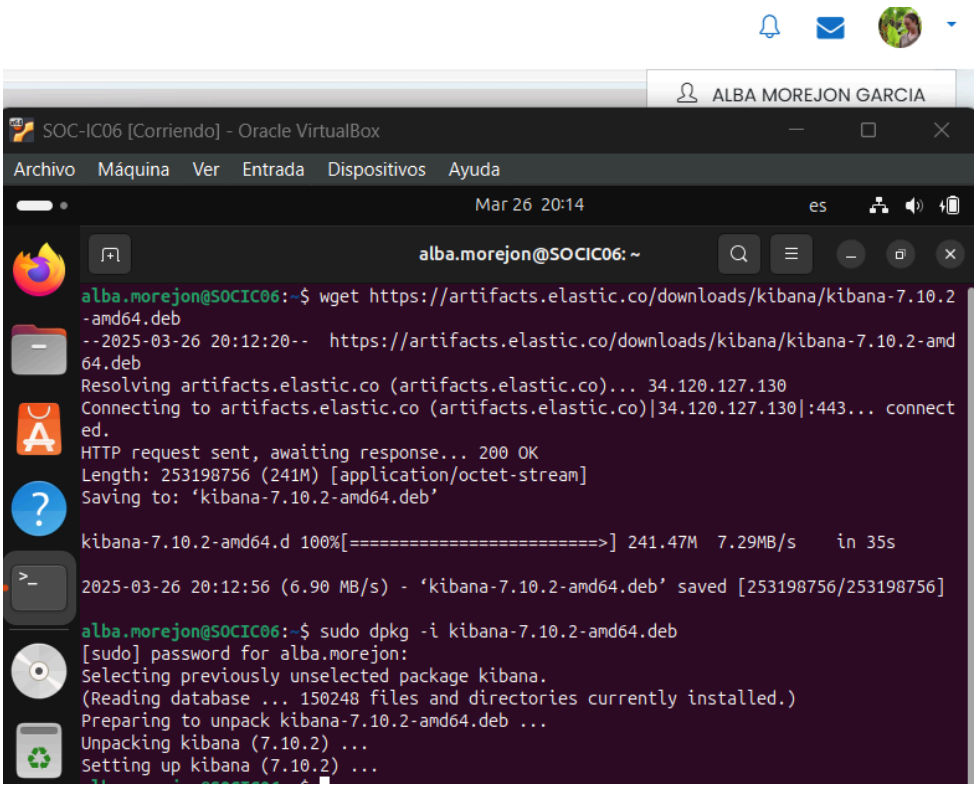



**Apartado 2: Instalación y configuración de Kibana.**

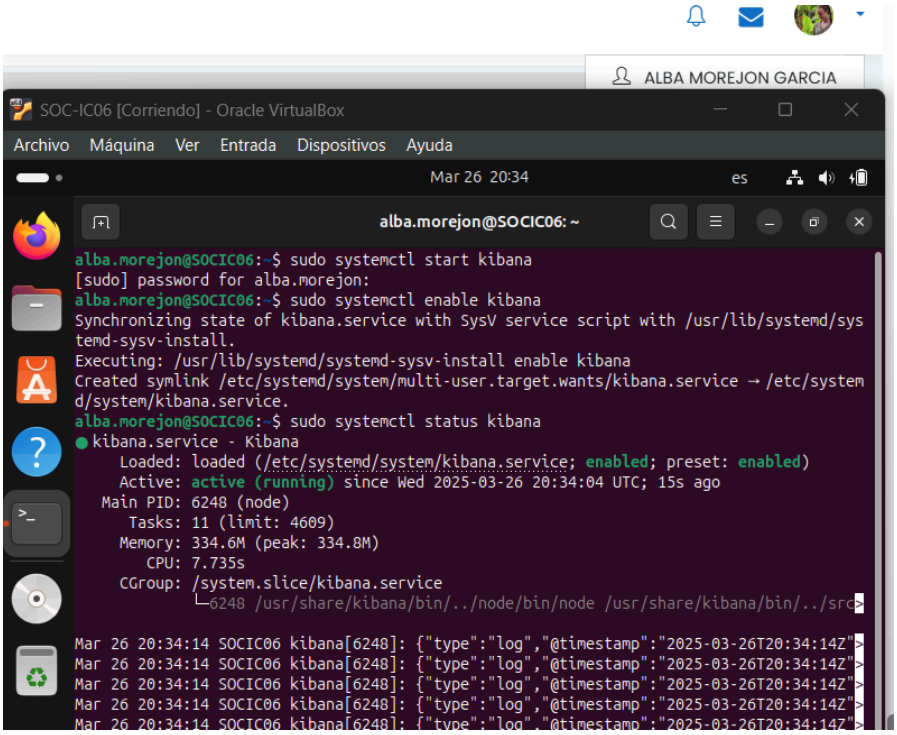
**a) Detallar la configuración a efectuar en Kibana.**

**b) Prueba de acceso al menú principal de Kibana.**

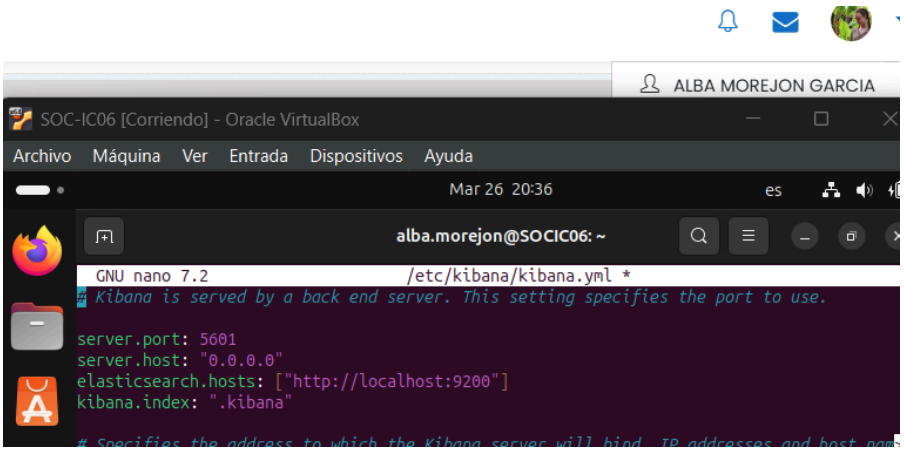
Descargamos e instalamos Kibana




Iniciamos el servicio y comprobamos el estado

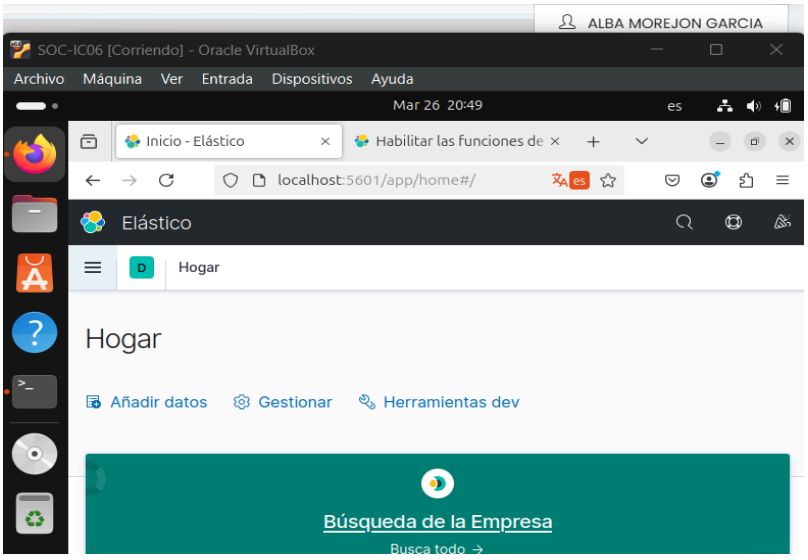


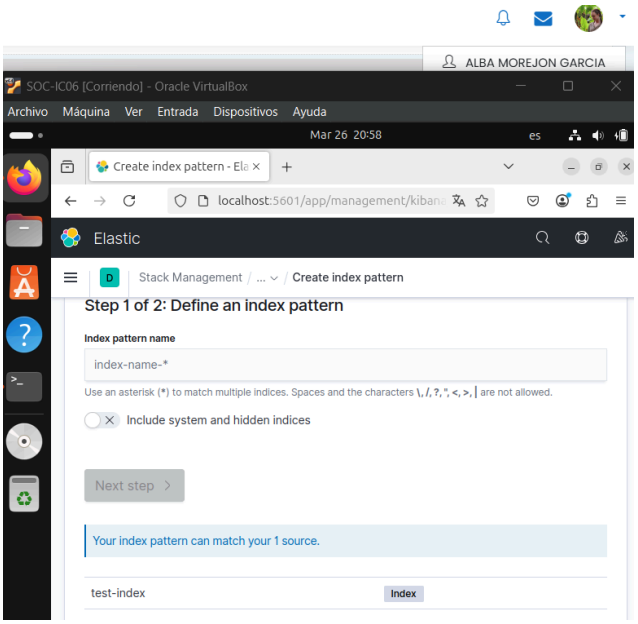

Editamos el archivo de configuración kibana.yml, añadimos el puerto en el que la herramienta está escuchando, configuramos todas las interfaces de red que escuchará, especificamos la dirección Elasticsearch al que se conectará y define el nombre del índice en Elasticsearch donde Kibana almacenará sus datos.

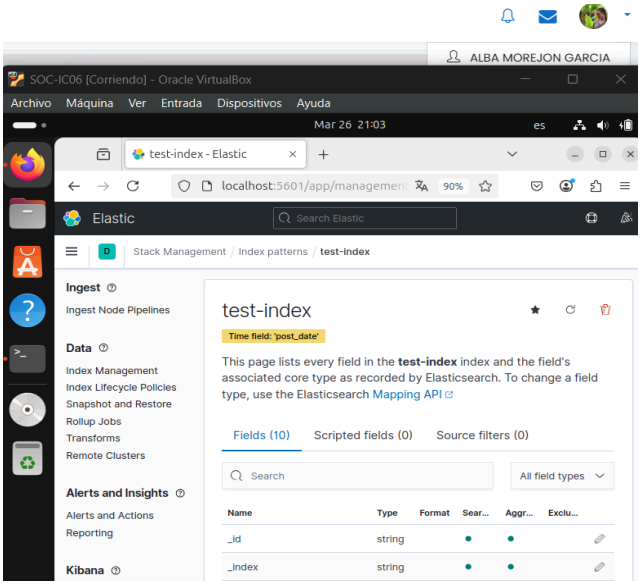



Comprobamos que funcione correctamente navegando en la web: http://localhost:5601

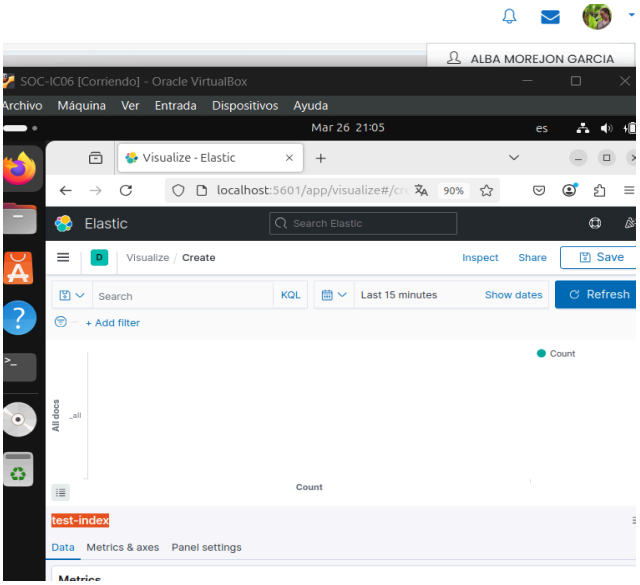
- Cargamos la página
- Creamos el patrón de índice para poder gestionarlo (elegimos el índice creado con elasticsearch)

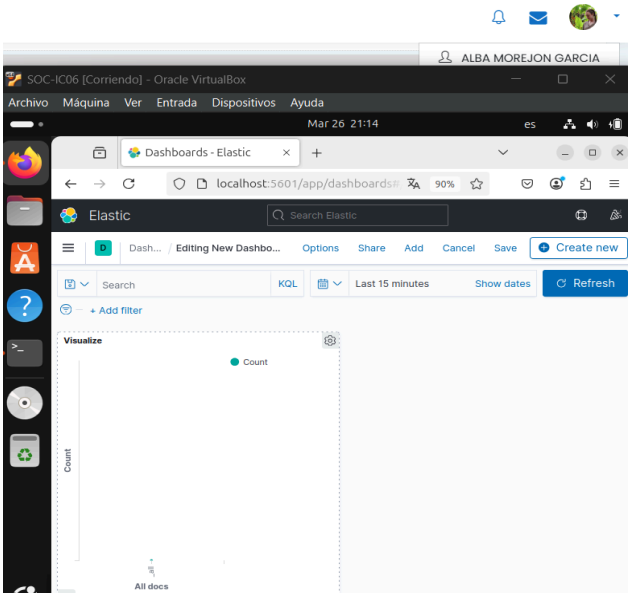





- En la sección visualize, creamos una nueva visualización con los datos del índice text-index
- Creamos un Dashboard



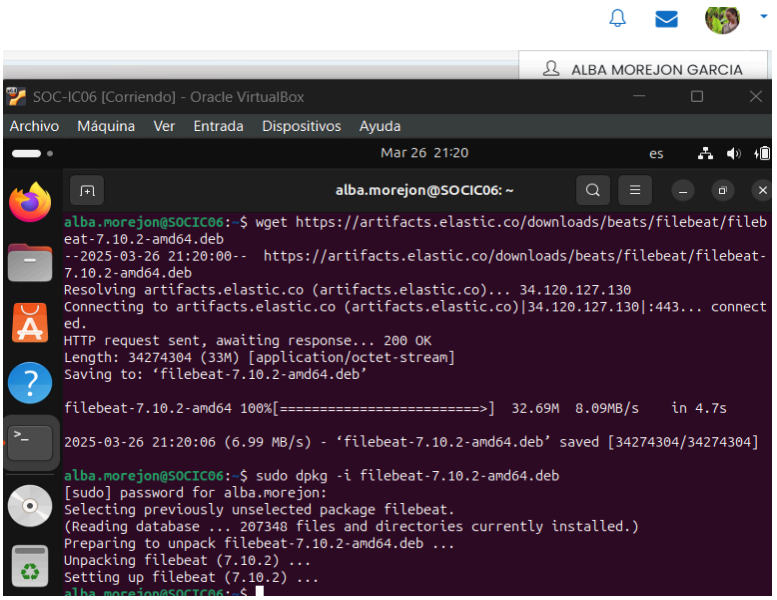




**Apartado 3: Instalación y configuración de Filebeat.**

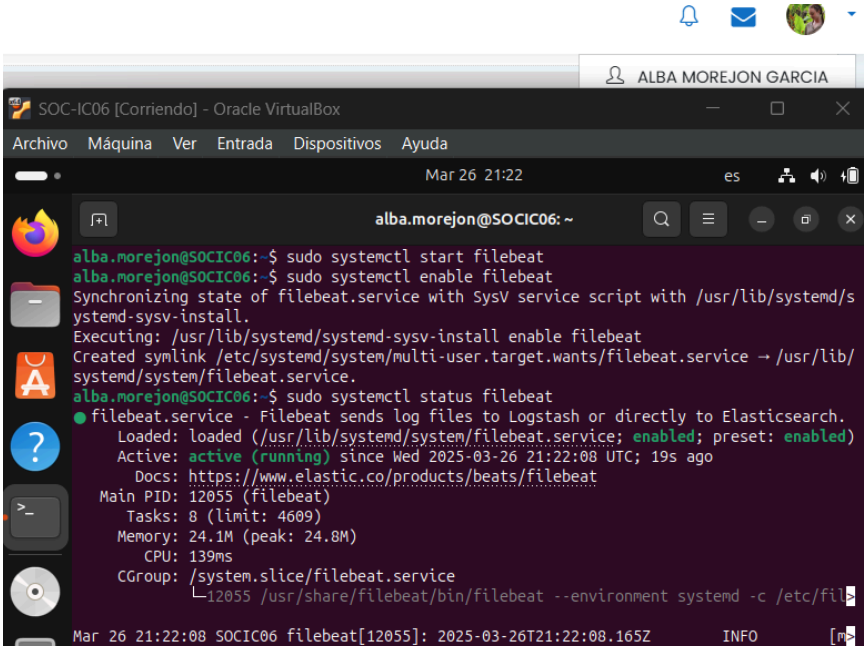
**a) Detallar la configuración a efectuar en el agente IDS para enviar los registros de Snort a Logstash.**

**b) Mostrar una prueba de funcionamiento de Filebeat mostrando los registros por consola.**

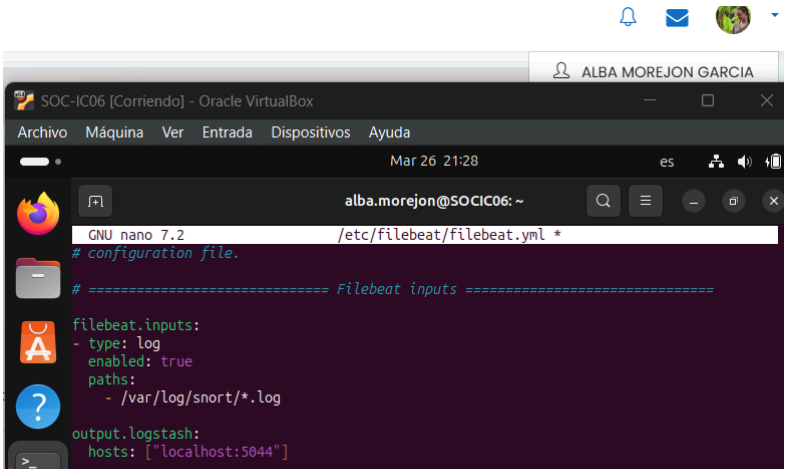
Descargamos e instalamos Filebeat



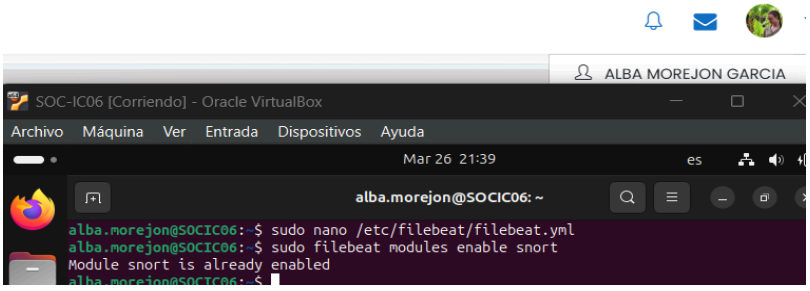
Iniciamos el servicio



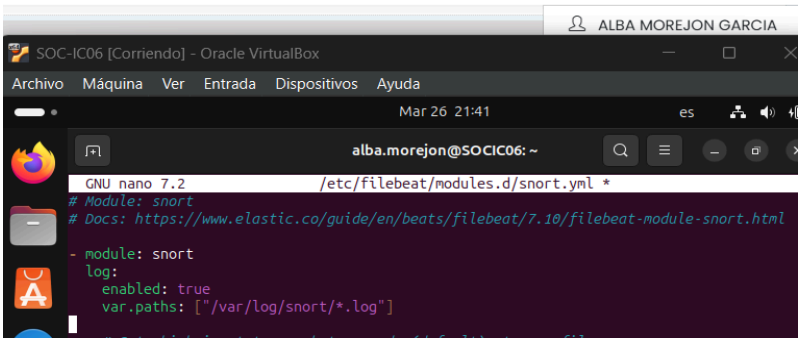

Configuramos Filebeat para que pueda leer los registros de Snort (habilitamos la entrada de logs, con la ruta de archivos que debe leer) y enviarlos Logstash (especificando la dirección del servidor al que el servicio mandará los registros, utilizaremos esta misma máquina en el puerto 5044).



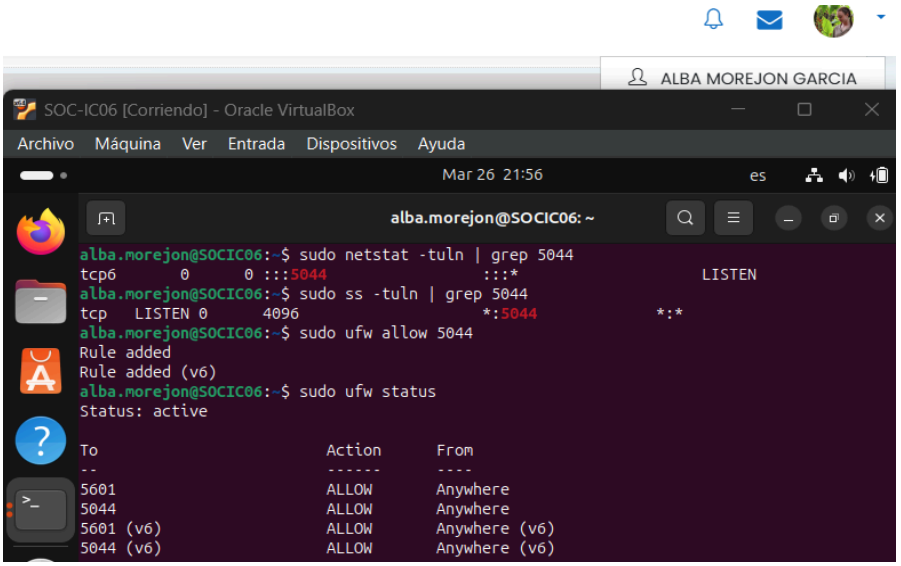

Habilitamos el módulo de Filebeat para Snort



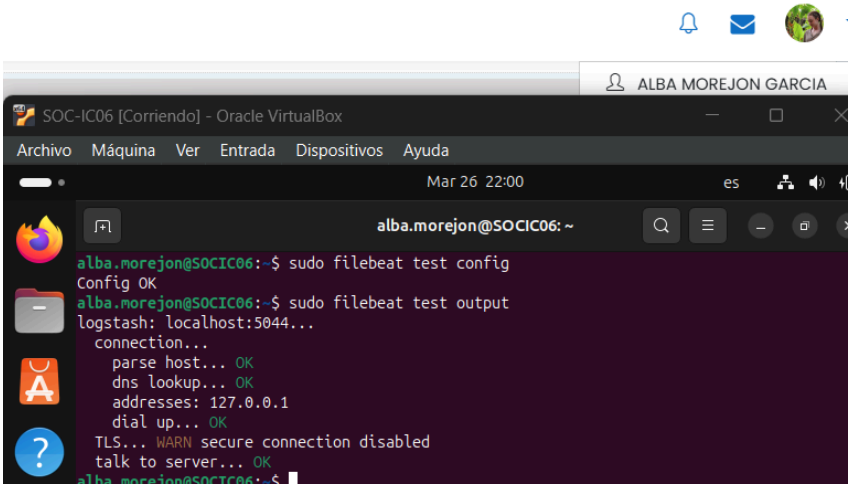

Configuramos el módulo de Snort en el archivo snort.yml



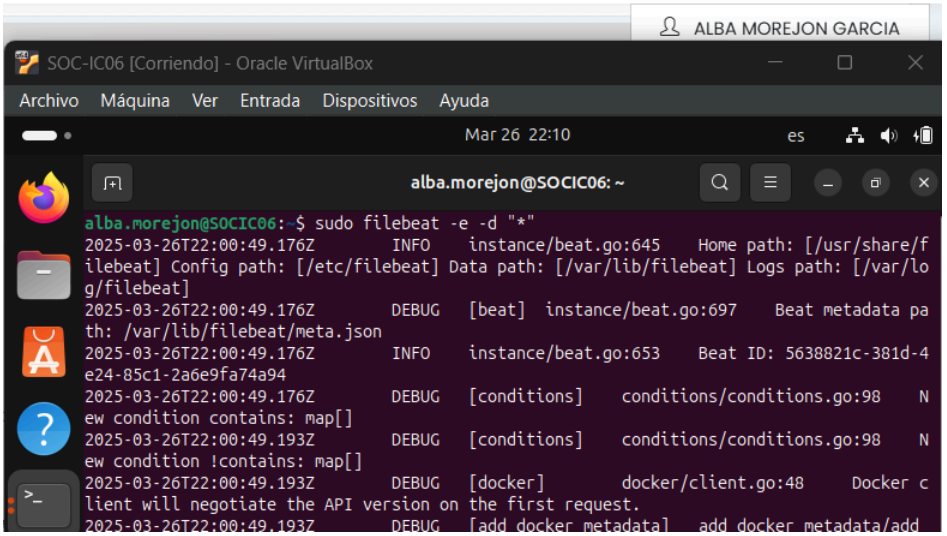

Verificamos que los puertos estén abiertos




Hacemos una prueba de verificar la configuración y probamos la salida de Logstash




Ejecutamos Filebeat en modo depuración para ver los registros

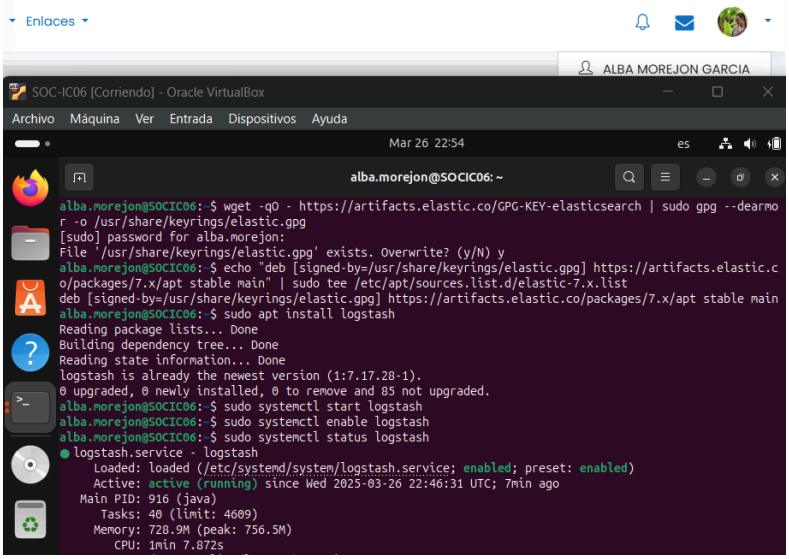



**Apartado 4: Instalación y configuración de Logstash.**

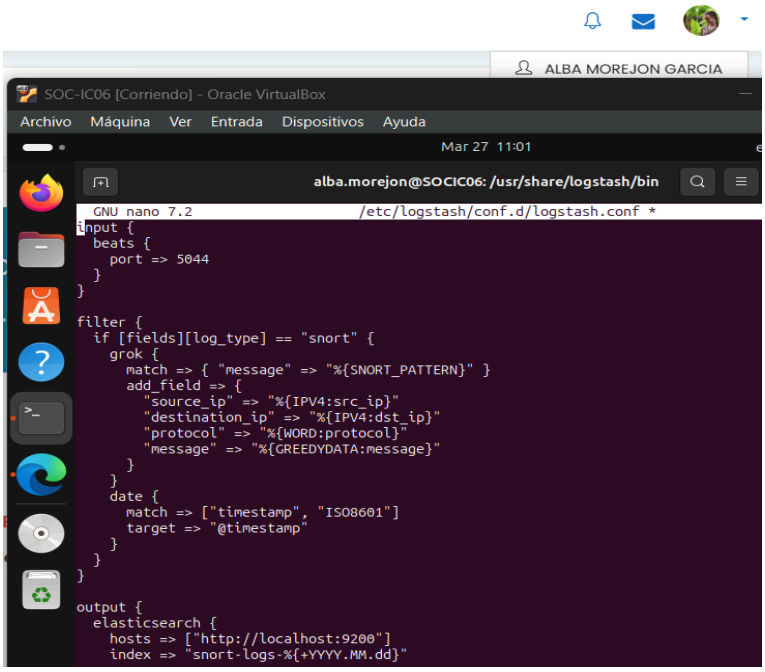
**a) Detallar la configuración a efectuar en Logstash para recibir los logs de Filebeat y reenviarlos a Elasticsearch.**

**b) Mostrar una prueba de funcionamiento en la que se puede visualizar la información del índice de logstash en Kibana.**

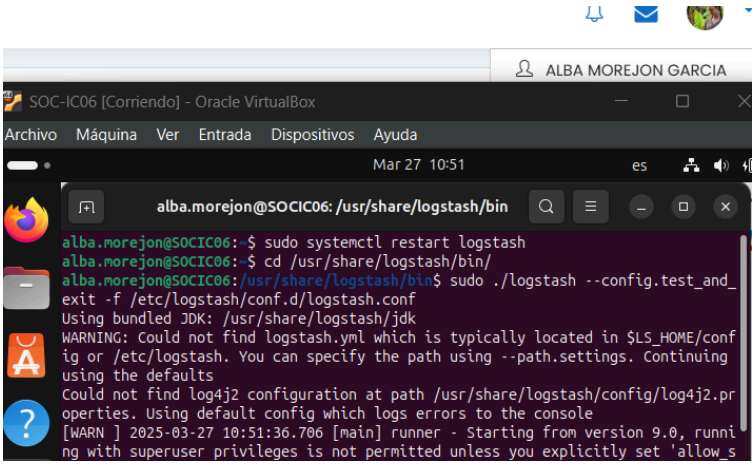
Agregamos la clave de Elasticshared y el repositorio de Logstash. Instalamos Logstash, iniciamos y habilitamos el servicio Logstash comprobando que su estado correcto



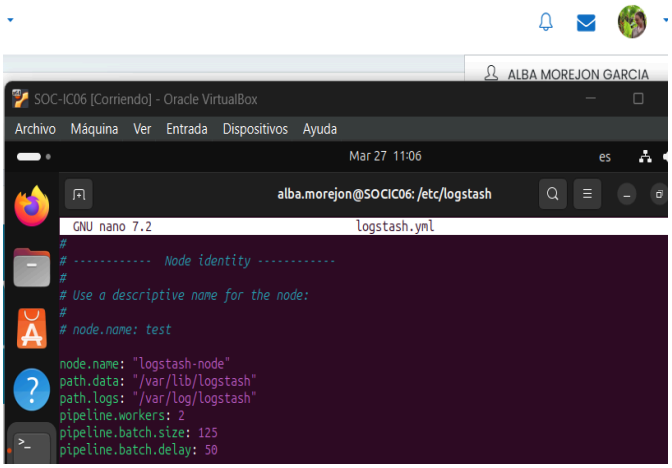

Añadimos la configuración para Filebeat

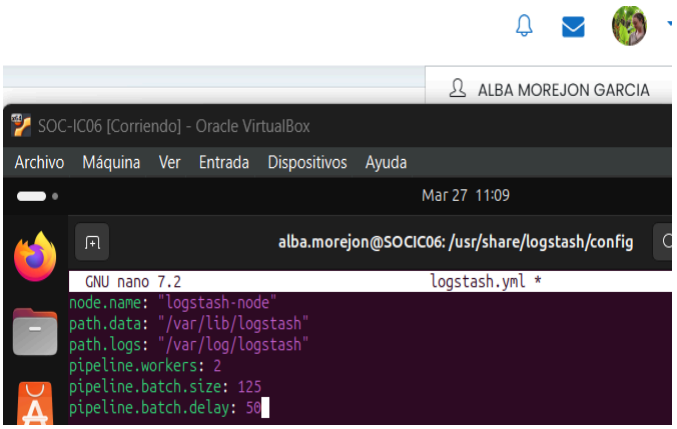



Verificamos que la configuración no tenga errores

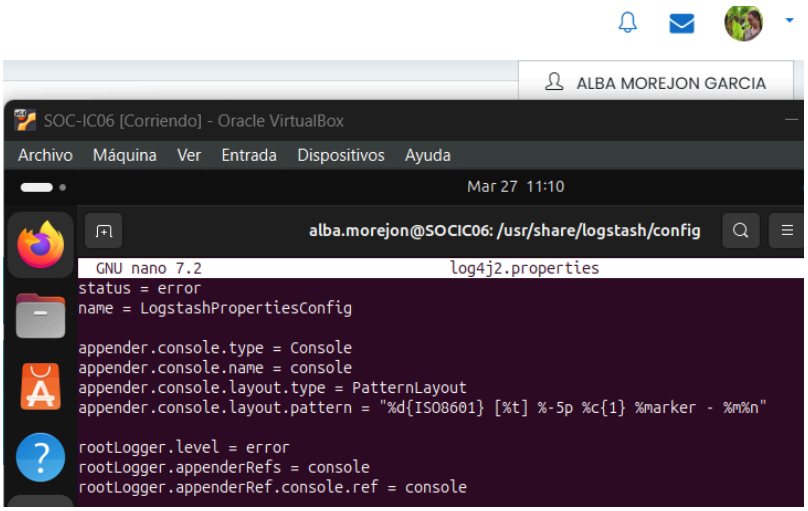



Le añadimos la siguiente información a los ficheros logstash.yml

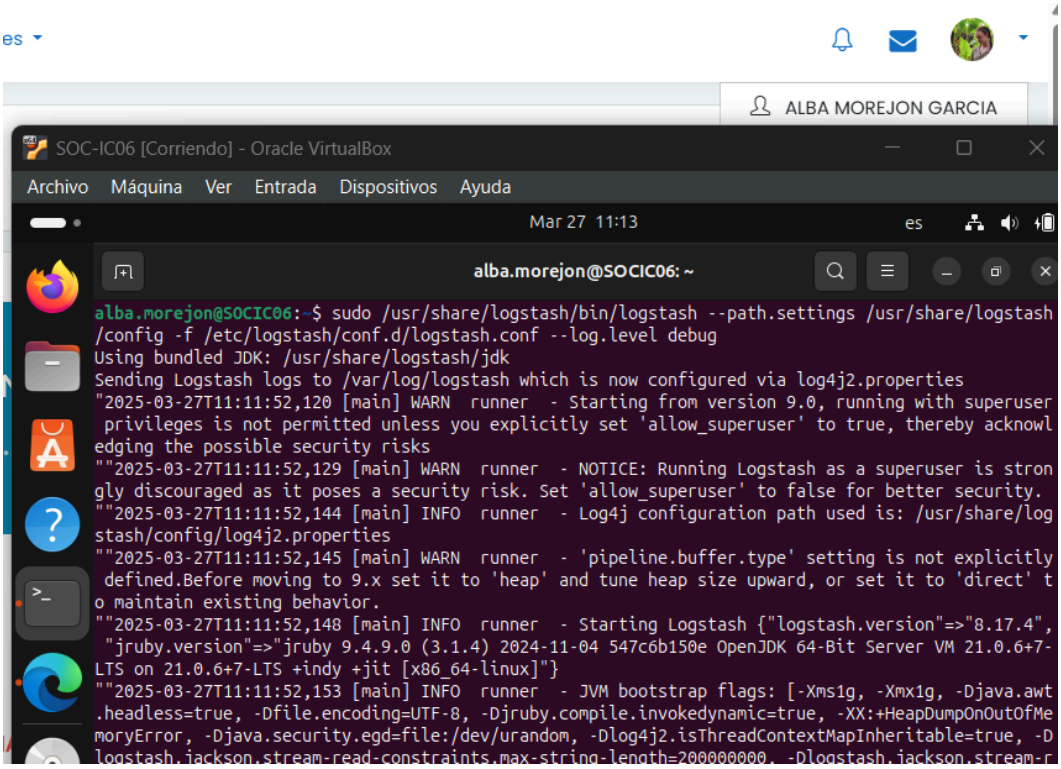


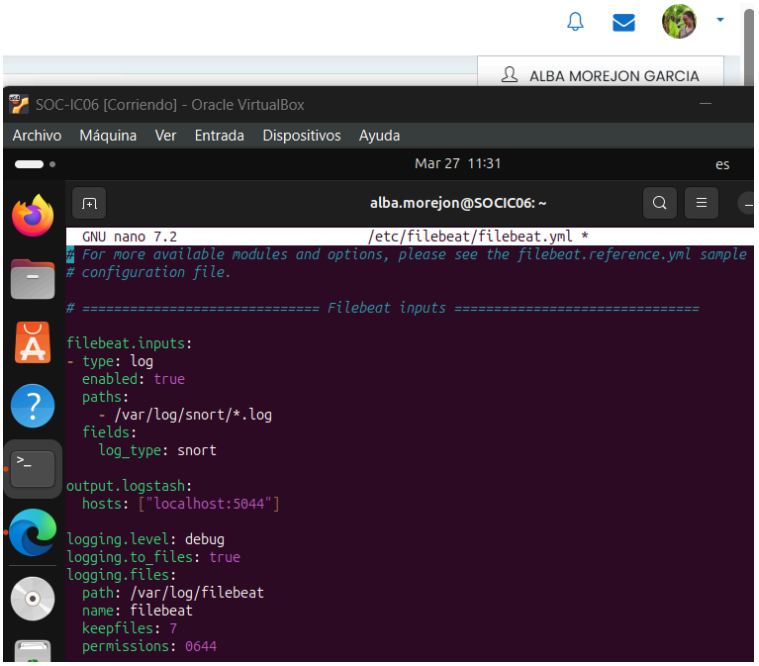

Creamos el fichero log4j2.properties y añadimos lo siguiente

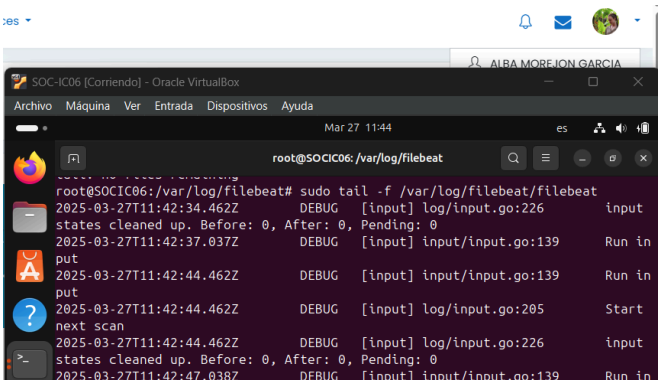



Ejecutamos logs en modo depuración para ver los registros de consola




Editamos el archivo filebeat.yml y vemos los logs



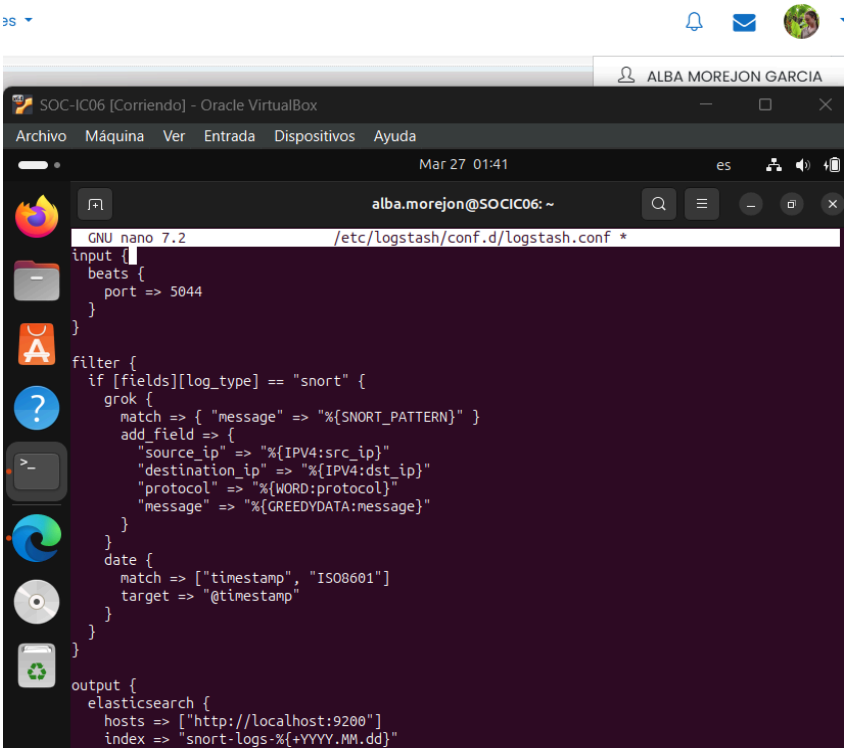




**Apartado 5: Creación de un filtro en Logstash.**

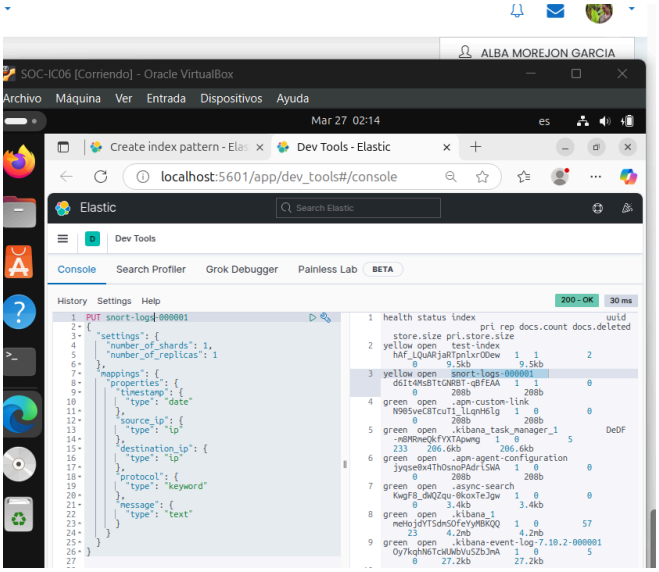
**a) Detallar la configuración a efectuar en Logstash para crear un Pipeline que filtre la información creando campos para los diferentes valores del mensaje de log creado en Snort.**

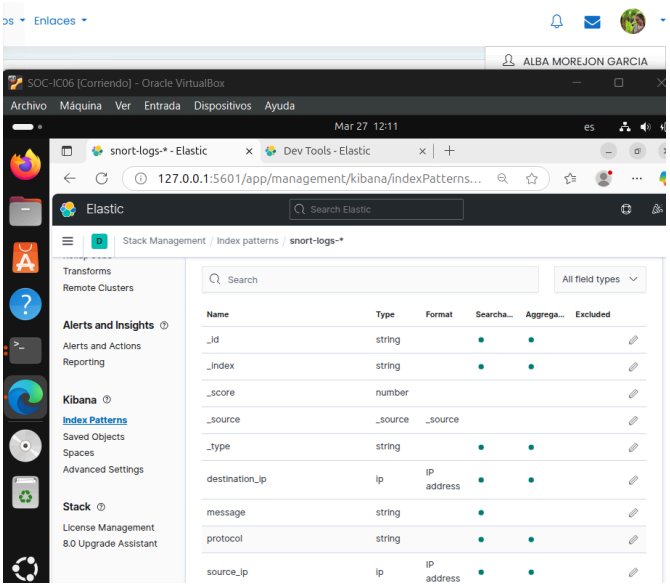
**b) Mostrar el índice que se crea con la información de sus diferentes campos.**

Configuramos el fichero logstash.conf



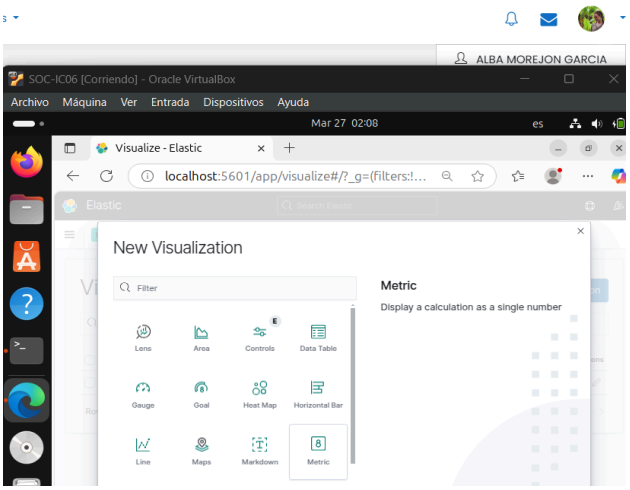
Creamos el índice snort-logs de forma manual



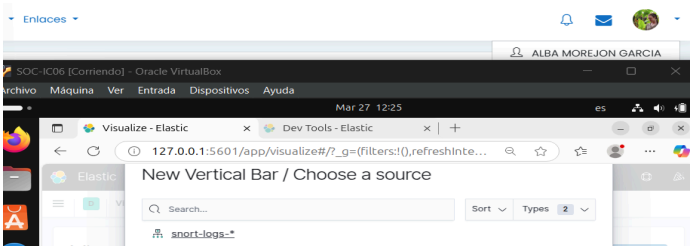




**Apartado 6: Tablero de Monitorización Multipunto.**
**a) Detallar la creación de dos contadores, uno para todos los PINGs desde la red interna y otro para los de la red externa.**
**b) Detallar la creación de dos histogramas, uno para los intentos de inicio de sesión por SSH y otro para los accesos a PHPMyadmin.**
**c) Detallar la creación de un nuevo tablero (dashboard) en Kibana que contenga los contadores y los histogramas creados anteriormente.**

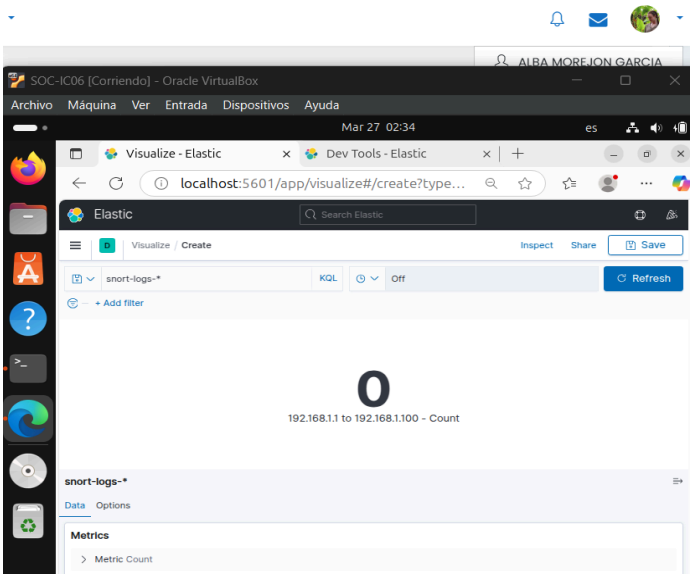
Seleccionando en el menú lateral el apartado Visualize (dentro de Kibana). y pulsamos en “Create visualization”. Nos da la opción de nos da la opción de seleccionar Metric y procedemos a crear dos visualizaciones para establecer red donde van a actuar.

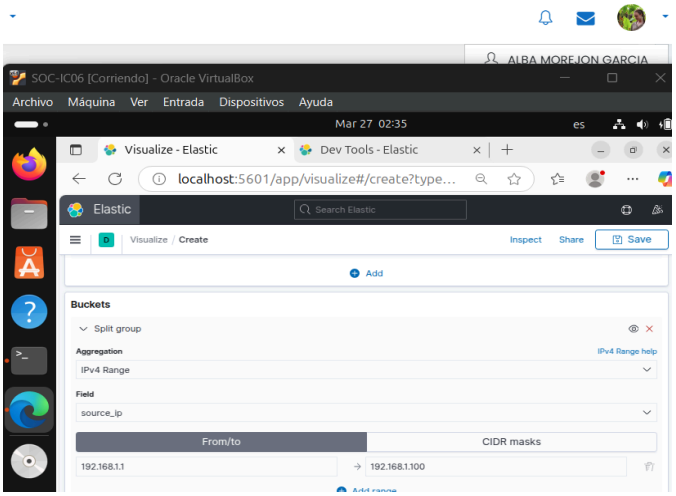



Elegimos el índice que creamos



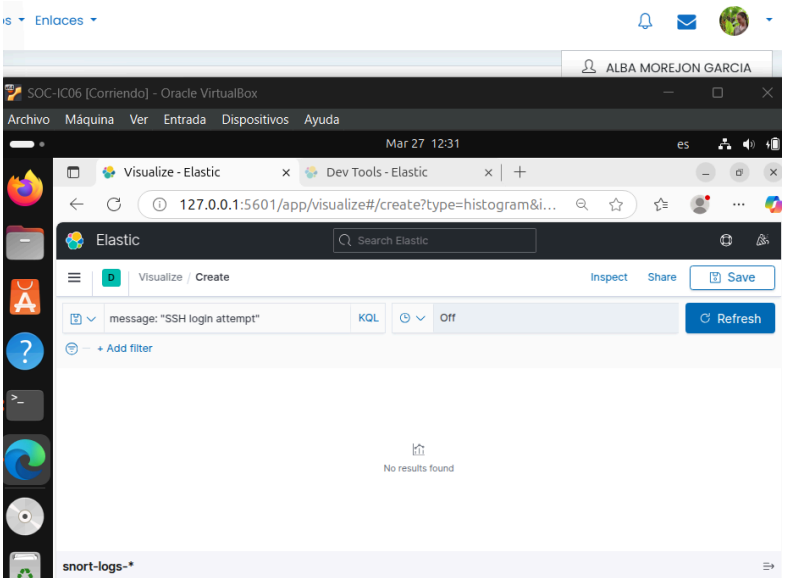

Establecemos los valores de Count y le damos el rango de IPs donde actuará

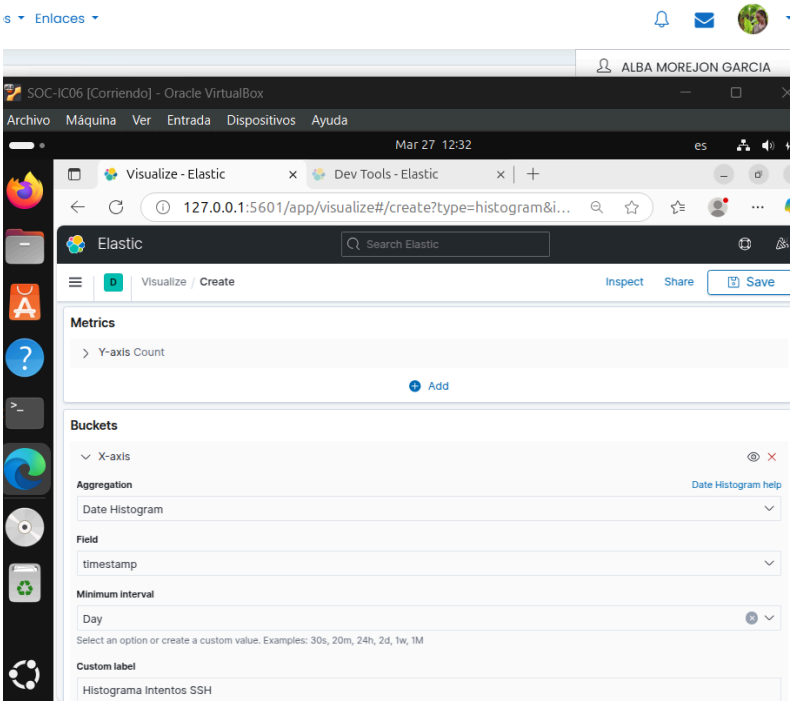


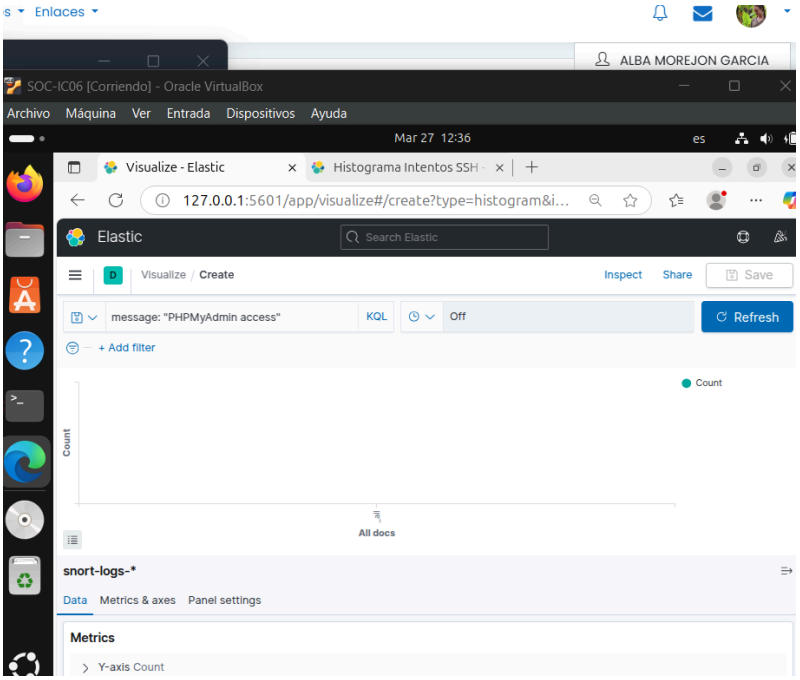




Haremos lo mismo pero cambiando el rango para la red externa

A continuación crearemos otras visualizaciones de tipo Histograma para los inicios de sesión con SSH y PHPMyadmin dando los siguientes valores


Enlaces
ALBA MOREJON GARCIA
SOC-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Mar 27 12:31
es
Visualize - Elastic
Dev Tools - Elastic
127.0.0.1:5601/app/visualize#/create?type=histogram&i...
Elastic
Search Elastic
Visualize / Create
Inspect
Share
Save
message: "SSH login attempt"
KQL
Off
Refresh
+ Add filter
No results found
snort-logs-*


Enlaces
ALBA MOREJON GARCIA
SOC-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Mar 27 12:32
es
Visualize - Elastic
Dev Tools - Elastic
127.0.0.1:5601/app/visualize#/create?type=histogram&i...
Elastic
Search Elastic
Visualize / Create
Inspect
Share
Save
Metrics
Y-axis Count
Add
Buckets
X-axis
Aggregation
Date Histogram help
Date Histogram
Field
timestamp
Minimum interval
Day
Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M
Custom label
Histograma Intentos SSH


Enlaces
ALBA MOREJON GARCIA
SOC-IC06 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Mar 27 12:36
es
Visualize - Elastic
Histograma Intentos SSH
127.0.0.1:5601/app/visualize#/create?type=histogram&i...
Elastic
Search Elastic
Visualize / Create
Inspect
Share
Save
message: "PHPMyAdmin access"
KQL
Off
Refresh
+ Add filter
Count
Count
All docs
snort-logs-*
Data
Metrics & axes
Panel settings
Metrics
Y-axis Count

Creamos un nuevo Dashboard, seleccionando en el menú lateral “Dashboard” y haciendo click sobre”Create Dashboard” y añadimos las vistas creadas anteriormente