



Incidentes de Ciberseguridad

PRÁCTICA UD2 ELK
10/05/2024

1.- Introducción a ELK	3
2.- Requisitos previos.....	3
3.- instalación y configuración de Elasticsearch	3
4.- Instalación de Kibana	9
5.- Instalación y configuración Logstash.....	12
6.- Instalación y configuración Filebeat	15
7.- Instalación y configuración Nginx	18
8.- Verificación de la instalación	22

1.- Introducción a ELK

ELK es un conjunto de herramientas de código abierto utilizado para la recopilación, almacenamiento, análisis y visualización de datos. Este conjunto está compuesto por Elasticsearch, una potente base de datos de búsqueda y análisis distribuido; Logstash, un motor de procesamiento de datos que permite la ingesta, transformación y enriquecimiento de datos de múltiples fuentes; y Kibana, una interfaz de usuario web diseñada para la visualización y exploración de datos, facilitando la creación de dashboards e informes interactivos. Juntas, estas herramientas proporcionan una solución completa para la monitorización y análisis de logs, permitiendo a las organizaciones obtener información valiosa de sus datos de forma eficiente y escalable.

2.- Requisitos previos

Un [ubuntu-22.04.3-desktop-amd64.iso](#) con Ubuntu 22.04, con 4GB de RAM, 2 CPU y 25gb disco configuradas con un usuario sudo no root. Estos son los requisitos mínimos para Elasticsearch.

OpenJDK 11 instalado.

Nginx instalado en el servidor, que configuraremos más adelante como Proxy Inverso.

También será necesario un dominio o subdominio para configurar el acceso a Kibana.

3.- instalación y configuración de Elasticsearch

Elasticsearch es un motor de búsqueda y análisis distribuido de código abierto desarrollado por Elastic. Es parte integral del ELK stack (Elasticsearch, Logstash, y Kibana) y se utiliza para indexar, buscar y analizar grandes volúmenes de datos en tiempo real. Aquí tienes una descripción detallada de sus características principales:

Motor de Búsqueda: Elasticsearch está diseñado para ser extremadamente rápido en la búsqueda de texto completo. Utiliza una estructura de índice invertido para indexar y almacenar los datos, lo

que permite realizar búsquedas complejas en grandes volúmenes de información de manera eficiente.

Distribuido y Escalable: Elasticsearch está diseñado para ser altamente distribuido y escalable. Puede dividir los datos en múltiples nodos y distribuirlos en un clúster para mejorar la disponibilidad y el rendimiento. Esto permite escalar horizontalmente el sistema para manejar grandes volúmenes de datos y cargas de trabajo.

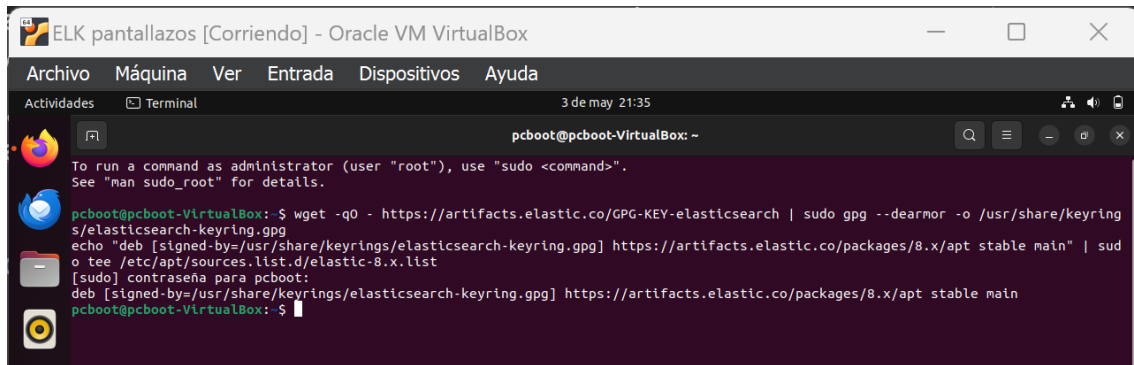
API RESTful: Elasticsearch proporciona una API RESTful que permite interactuar con el sistema a través de solicitudes HTTP. Esto facilita la integración con aplicaciones y servicios externos, así como la automatización de tareas de administración y gestión.

Análisis de Texto Completo: Elasticsearch ofrece capacidades avanzadas de análisis de texto completo, incluyendo tokenización, filtrado, stemming y relevancia de búsqueda. Esto permite realizar búsquedas sofisticadas que tienen en cuenta la semántica y el contexto del texto.

Funcionalidades de Agregación: Además de la búsqueda de texto completo, Elasticsearch también permite realizar agregaciones sobre los datos indexados. Esto incluye operaciones de agregación como sumas, promedios, máximos, mínimos, y más, que pueden utilizarse para generar informes y análisis de datos.

Integración con Kibana y Logstash: Elasticsearch se integra estrechamente con Kibana y Logstash para formar el ELK stack. Kibana se utiliza para la visualización y el análisis de datos, mientras que Logstash se utiliza para la ingestión de datos desde diversas fuentes.

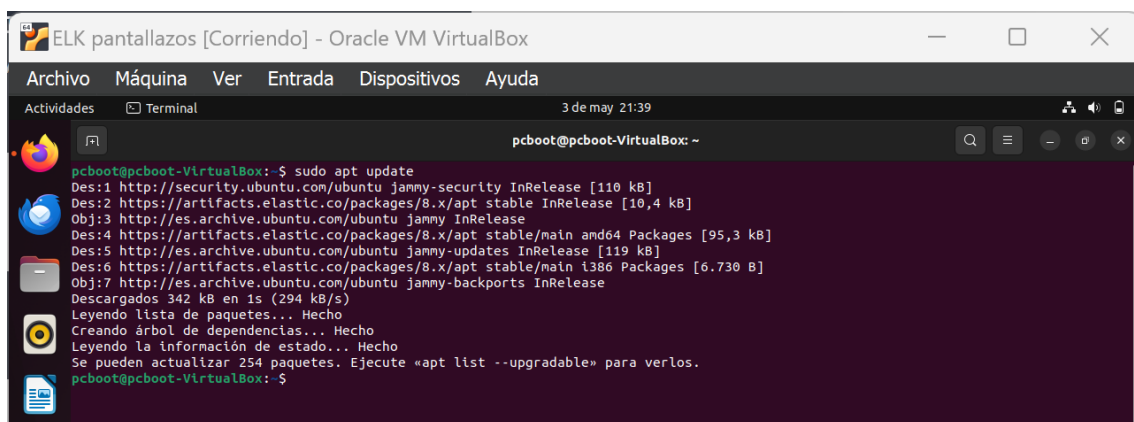
En resumen, Elasticsearch es una potente plataforma de búsqueda y análisis de datos que proporciona capacidades avanzadas para indexar, buscar y analizar grandes volúmenes de información en tiempo real. Su diseño distribuido y escalable, junto con su API RESTful y sus capacidades de análisis de texto completo, lo convierten en una opción popular para una amplia gama de casos de uso, desde búsqueda en sitios web hasta análisis de registros de aplicaciones.



```
pcboot@pcboot-VirtualBox: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
pcboot@pcboot-VirtualBox:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyring  
s/elasticsearch-keyring.gpg  
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sud  
o tee /etc/apt/sources.list.d/elastic-8.x.list  
[sudo] contraseña para pcboot:  
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main  
pcboot@pcboot-VirtualBox:~$
```

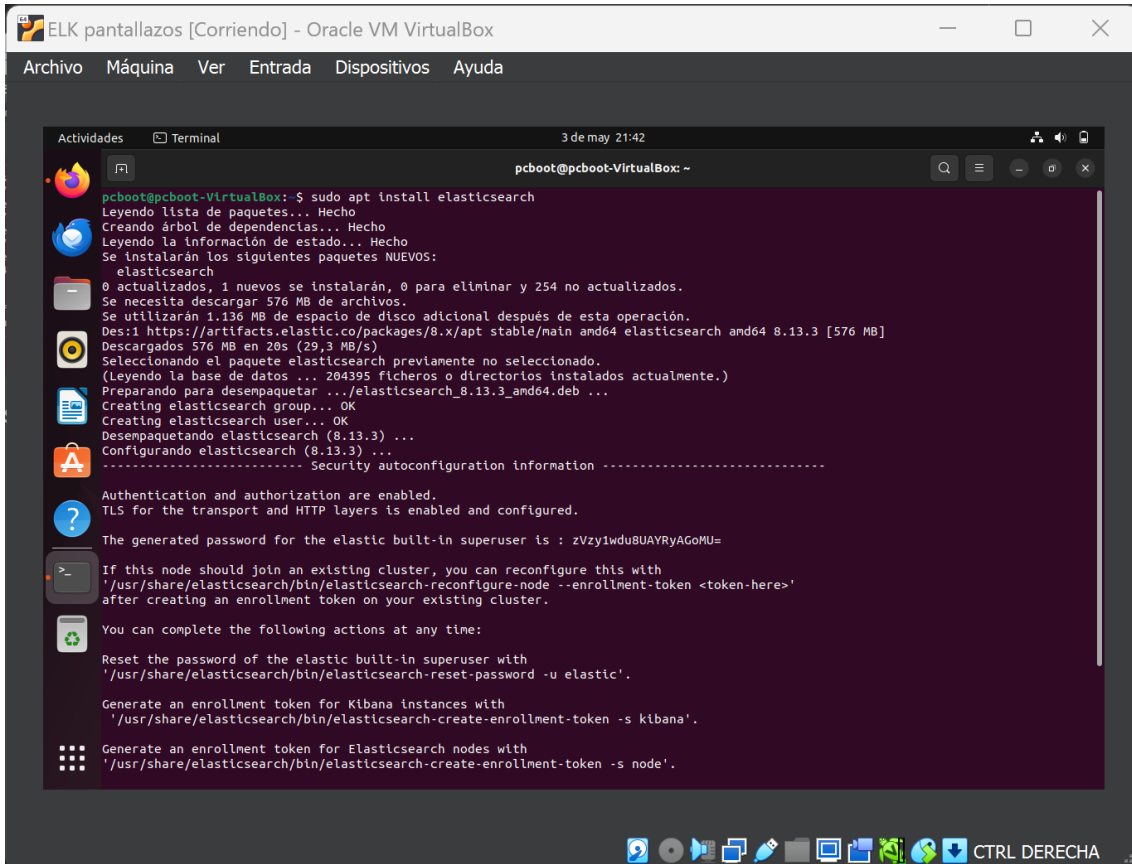
En esta pantalla, se procede a añadir los componentes de ElasticSearch no se encuentran en los repositorios de Ubuntu, pero se puede instalar por APT añadiendo los repositorios a ejecutar los siguientes comandos:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch |  
sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-  
keyring.gpg  
  
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-  
keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable  
main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```



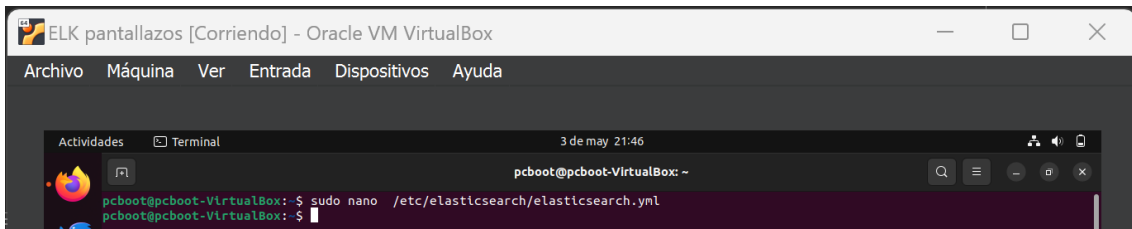
```
pcboot@pcboot-VirtualBox:~$ sudo apt update  
Des:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Des:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10,4 kB]  
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy InRelease  
Des:4 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [95,3 kB]  
Des:5 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]  
Des:6 https://artifacts.elastic.co/packages/8.x/apt stable/main i386 Packages [6.730 B]  
Obj:7 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Descargados 342 kB en 1s (294 kB/s)  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se pueden actualizar 254 paquetes. Ejecute «apt list --upgradable» para verlos.  
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede actualizar los repositorios con el comando `sudo apt update` y pulsamos la tecla Enter para ejecutar el comando.



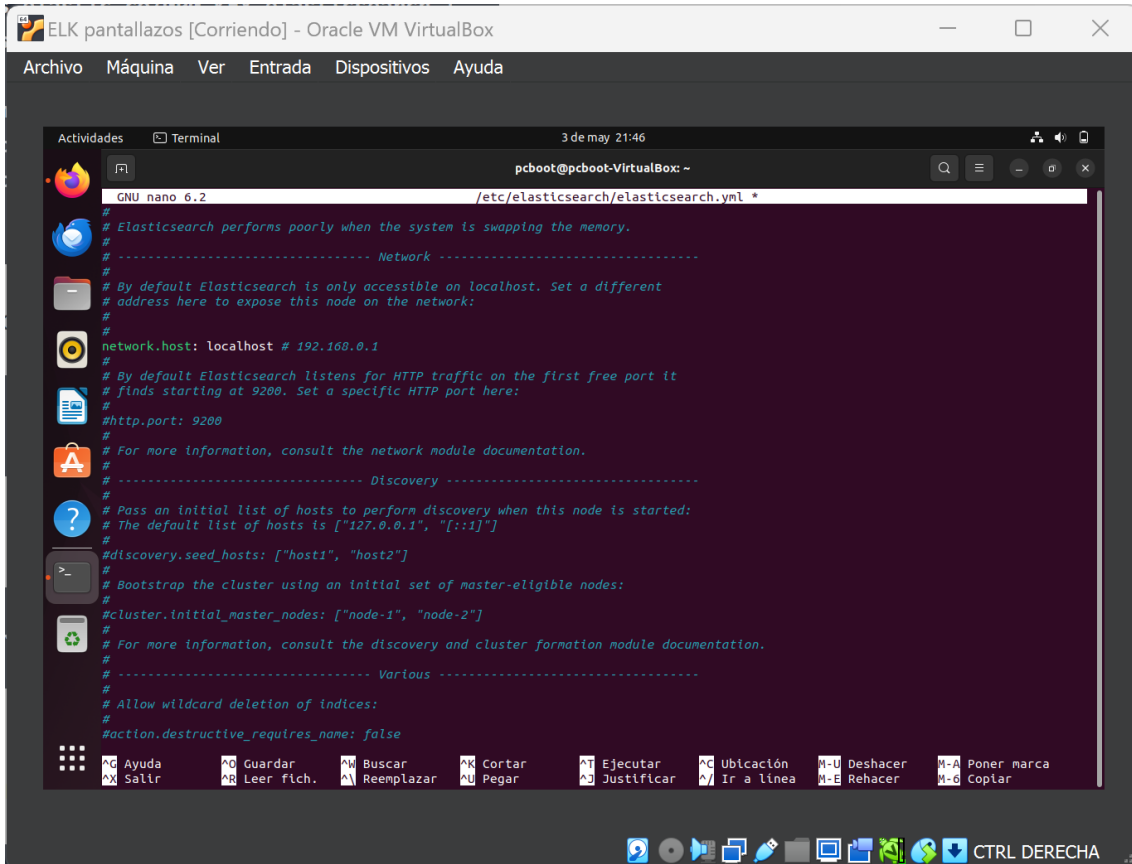
```
pcboot@pcboot-VirtualBox: ~  
$ sudo apt install elasticsearch  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  elasticsearch  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 254 no actualizados.  
Se necesita descargar 576 MB de archivos.  
Se utilizarán 1.136 MB de espacio de disco adicional después de esta operación.  
Des:1 https://artifacts.elastic.co/packages/8.x/apt/stable/main amd64 elasticsearch amd64 8.13.3 [576 MB]  
Descargados 576 MB en 20s (29,3 MB/s)  
Seleccionando el paquete elasticsearch previamente no seleccionado.  
(Leyendo la base de datos ... 204395 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../elasticsearch_8.13.3_amd64.deb ...  
Creating elasticsearch group... OK  
Creating elasticsearch user... OK  
Desempaquetando elasticsearch (8.13.3) ...  
Configurando elasticsearch (8.13.3) ...  
----- Security autoconfiguration information -----  
  
Authentication and authorization are enabled.  
TLS for the transport and HTTP layers is enabled and configured.  
  
The generated password for the elastic built-in superuser is : zVzyIwdu8UAYRyAGoMu=  
  
If this node should join an existing cluster, you can reconfigure this with  
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'  
after creating an enrollment token on your existing cluster.  
  
You can complete the following actions at any time:  
  
Reset the password of the elastic built-in superuser with  
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.  
  
Generate an enrollment token for Kibana instances with  
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.  
  
Generate an enrollment token for Elasticsearch nodes with  
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.
```

En esta pantalla, se procede a instalar elasticsearch con el comando `sudo apt install elasticsearch` y pulsamos la tecla Enter para ejecutar el comando.



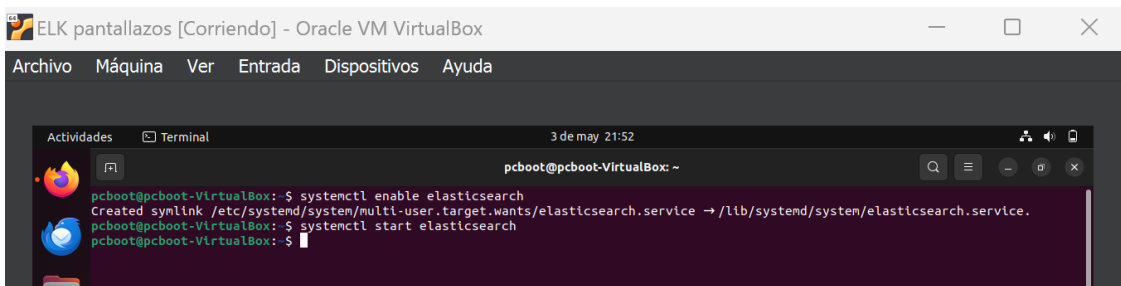
```
pcboot@pcboot-VirtualBox: ~  
$ sudo nano /etc/elasticsearch/elasticsearch.yml  
pcboot@pcboot-VirtualBox: $
```

En esta pantalla, se procede a editar el archivo `elasticsearch.yml` con el comando `sudo nano /etc/elasticsearch/elasticsearch.yml` y pulsamos la tecla Enter para ejecutar el comando.



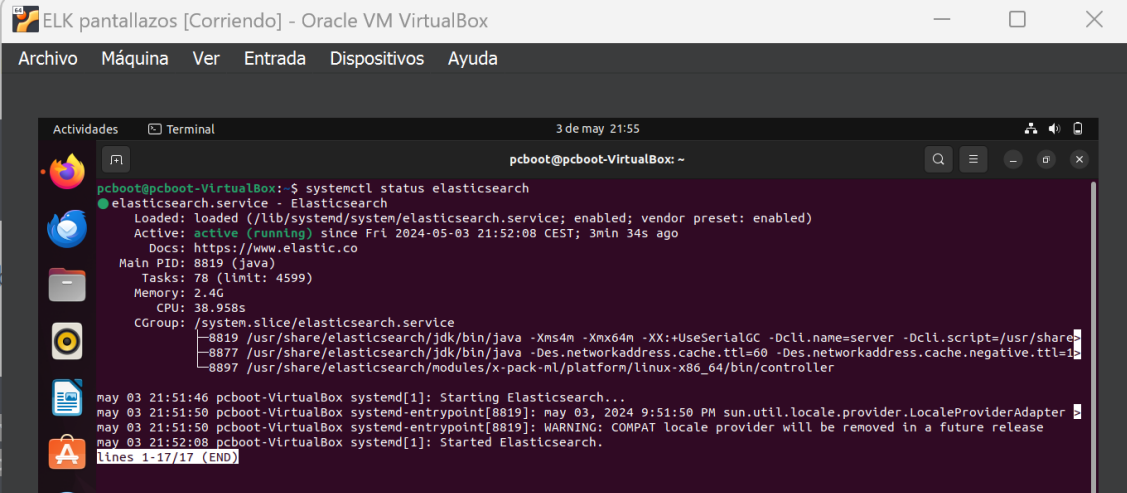
```
pcboot@pcboot-VirtualBox: ~  
GNU nano 6.2 /etc/elasticsearch/elasticsearch.yml *  
#  
# Elasticsearch performs poorly when the system is swapping the memory.  
# ----- Network -----  
# By default Elasticsearch is only accessible on localhost. Set a different  
# address here to expose this node on the network:  
#  
network.host: localhost # 192.168.0.1  
#  
# By default Elasticsearch listens for HTTP traffic on the first free port it  
# finds starting at 9200. Set a specific HTTP port here:  
#http.port: 9200  
# For more information, consult the network module documentation.  
# ----- Discovery -----  
# Pass an initial list of hosts to perform discovery when this node is started:  
# The default list of hosts is ["127.0.0.1", "[:1]"]  
#  
#discovery.seed_hosts: ["host1", "host2"]  
# Bootstrap the cluster using an initial set of master-eligible nodes:  
#cluster.initial_master_nodes: ["node-1", "node-2"]  
# For more information, consult the discovery and cluster formation module documentation.  
# ----- Various -----  
# Allow wildcard deletion of indices:  
#action.destructive_requires_name: false  
#-----  
# Ayuda      # Guardar  # Buscar    # Cortar    # Ejecutar  # Ubicación  # Deshacer  # Poner marca  
# Salir      # Leer fich. # Reemplazar # Pegar      # Justificar # Ir a línea  # Rehacer   # Copiar
```

En esta pantalla, se procede a modificar la línea `#network.host` : `192.168.0.1` por la líneas siguientes `network.host : localhost # 192.168.0.1` y pulsamos la teclas `CTRL+O` para guardar los datos y pulsamos la tecla `CTRL+X` para salir del nano.



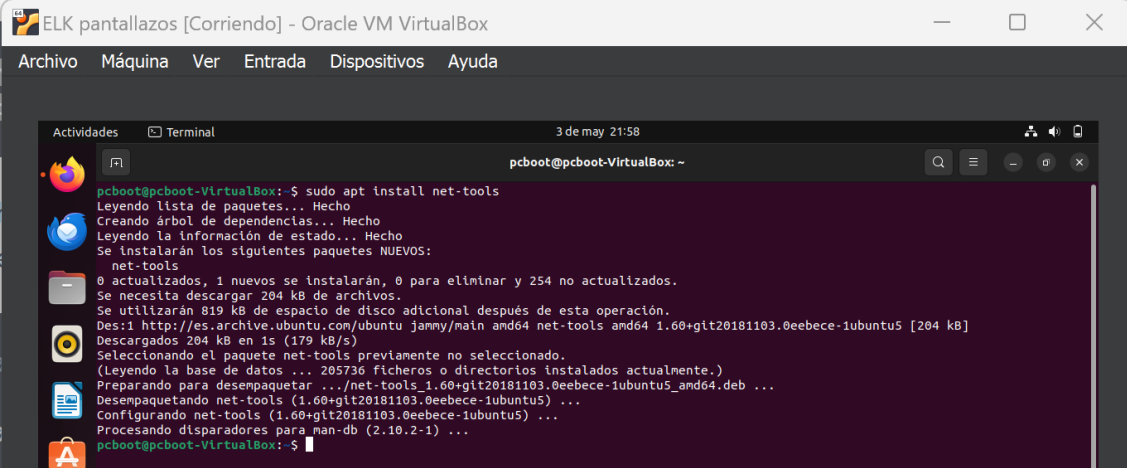
```
pcboot@pcboot-VirtualBox: ~  
pcboot@pcboot-VirtualBox:~$ systemctl enable elasticsearch  
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.  
pcboot@pcboot-VirtualBox:~$ systemctl start elasticsearch  
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede habilitar y arrancar el servicio de ElasticSearch con los comandos siguientes `systemctl enable elasticsearch` y `systemctl start elasticsearch`.



```
pcboot@pcboot-VirtualBox: ~  
$ systemctl status elasticsearch  
● elasticsearch.service - Elasticsearch  
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2024-05-03 21:52:08 CEST; 3min 34s ago  
     Docs: https://www.elastic.co  
   Main PID: 8819 (java)  
    Tasks: 78 (limit: 4599)  
   Memory: 2.4G  
      CPU: 38.958s  
   CGroup: /system.slice/elasticsearch.service  
           └─8819 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/...  
           └─8877 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=1...  
           └─8897 /usr/share/elasticsearch/modules/x-pack-nl/platform/linux-x86_64/bin/controller  
  
may 03 21:51:46 pcboot-VirtualBox systemd[1]: Starting Elasticsearch...  
may 03 21:51:50 pcboot-VirtualBox systemd-entrypoint[8819]: may 03, 2024 9:51:50 PM sun.util.locale.provider.LocaleProviderAdapter  
may 03 21:51:50 pcboot-VirtualBox systemd-entrypoint[8819]: WARNING: COMPAT locale provider will be removed in a future release  
may 03 21:52:08 pcboot-VirtualBox systemd[1]: Started Elasticsearch.  
lines 1-17/17 (END)
```

En esta pantalla, se procede a verificar si está el servicio Elasticsearch con el comando `systemctl status elasticsearch` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox: ~  
$ sudo apt install net-tools  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
 net-tools  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 254 no actualizados.  
Se necesitan descargar 204 kB de archivos.  
Se utilizarán 819 kB de espacio de disco adicional después de esta operación.  
Des: http://es.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ubuntu5 [204 kB]  
Descargados 204 kB en 1s (179 kB/s)  
Seleccionando el paquete net-tools previamente no seleccionado.  
(Leyendo la base de datos ... 205736 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...  
Desempaquetando net-tools (1.60+git20181103.0eebece-1ubuntu5) ...  
Configurando net-tools (1.60+git20181103.0eebece-1ubuntu5) ...  
Procesando disparadores para man-db (2.10.2-1) ...  
pcboot@pcboot-VirtualBox: ~
```

En esta pantalla, se procede a instalar net-tools con el comando `sudo apt install net-tools` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox: ~  
$ netstat -tulnp | grep 9300  
(No todos los procesos pueden ser identificados, no hay información de propiedad del proceso  
no se mostrarán, necesita ser superusuario para verlos todos.)  
tcp6      0      0 0.0.0.0:9300          :::*        ESCUCHAR  -  
pcboot@pcboot-VirtualBox: ~
```

En esta pantalla, se procede a ejecutar el comando `netstat -tulnp | grep 9300` para verificar que Elasticsearch está utilizando el puerto 9300.

4.- Instalación de Kibana

Kibana es una plataforma de visualización y análisis de datos de código abierto desarrollada por Elastic. Se utiliza comúnmente junto con Elasticsearch y Logstash (a veces conocido como ELK stack) para formar un conjunto completo de herramientas para la gestión de datos y la visualización de datos en tiempo real. Aquí tienes una descripción más detallada de sus características principales:

Visualización de Datos: Kibana proporciona una amplia gama de opciones para visualizar datos, incluyendo gráficos de barras, gráficos circulares, mapas geográficos, tablas, histogramas y más. Estas visualizaciones pueden personalizarse y configurarse para adaptarse a las necesidades específicas de análisis de datos de cada usuario.

Panel de Control: Permite a los usuarios crear paneles de control personalizados que contienen múltiples visualizaciones de datos para obtener una vista general completa de los datos. Estos paneles pueden organizarse y diseñarse según las preferencias del usuario.

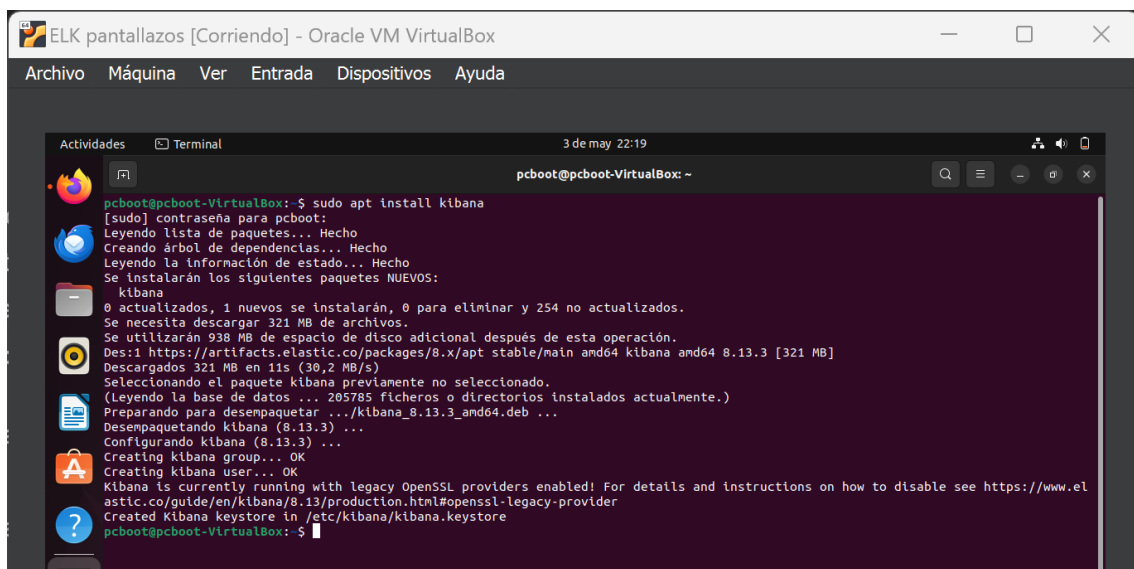
Exploración de Datos: Kibana ofrece capacidades de exploración de datos que permiten a los usuarios investigar y analizar conjuntos de datos de manera interactiva. Puedes filtrar, buscar y perforar en los datos para descubrir patrones, tendencias y anomalías.

Integración con Elasticsearch: Kibana está estrechamente integrado con Elasticsearch, que es un motor de búsqueda y análisis distribuido. Esto permite a los usuarios realizar búsquedas y consultas complejas en grandes volúmenes de datos de manera eficiente.

Seguridad y Acceso Controlado: Ofrece características de seguridad robustas que permiten controlar el acceso a los datos y las funcionalidades de Kibana. Esto incluye autenticación de usuarios, autorización basada en roles y auditoría de actividades.

Escalabilidad: Kibana está diseñado para ser altamente escalable, lo que significa que puede manejar grandes volúmenes de datos y escalar horizontalmente para satisfacer las demandas de aplicaciones empresariales a gran escala.

En resumen, Kibana es una herramienta poderosa para la visualización y el análisis de datos que proporciona a los usuarios las herramientas necesarias para explorar, comprender y tomar decisiones basadas en datos de manera efectiva.

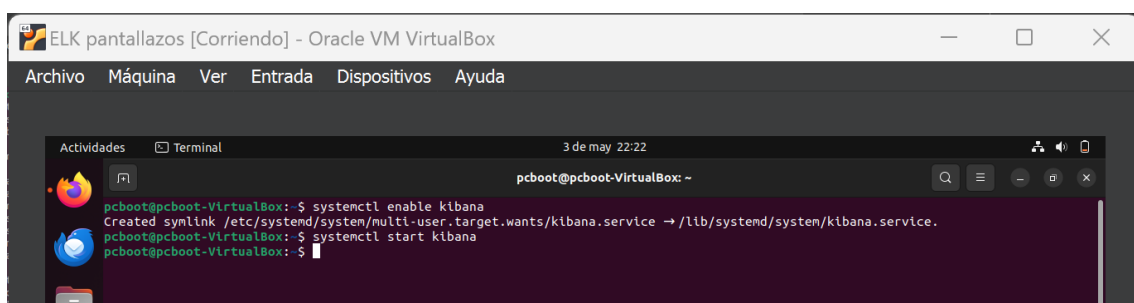


```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal
3 de may 22:19
pcboot@pcboot-VirtualBox: ~

pcboot@pcboot-VirtualBox:~$ sudo apt install kibana
[sudo] contraseña para pcboot:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  kibana
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 254 no actualizados.
Se necesita descargar 321 MB de archivos.
Se utilizarán 938 MB de espacio de disco adicional después de esta operación.
Des:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.13.3 [321 MB]
Descargados 321 MB en 11s (30,2 MB/s)
Seleccionando el paquete kibana previamente no seleccionado.
(Leyendo la base de datos ... 205785 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../kibana_8.13.3_amd64.deb ...
Desempaquetando kibana (8.13.3) ...
Configurando kibana (8.13.3) ...
Creating kibana group... OK
Creating kibana user... OK
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/8.13/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla se instala kibana con el comando `sudo apt install kibana` y pulsamos la tecla Enter para ejecutar el comando.

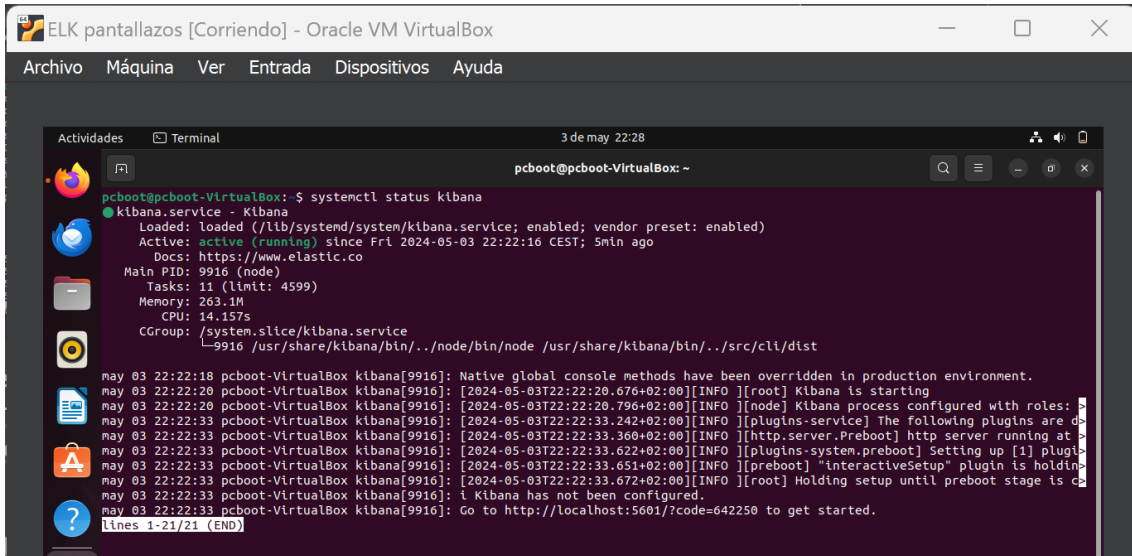


```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal
3 de may 22:22
pcboot@pcboot-VirtualBox: ~

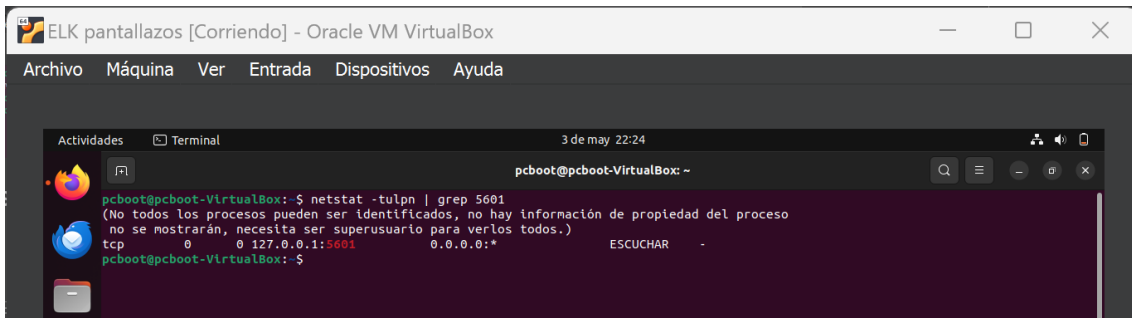
pcboot@pcboot-VirtualBox:~$ systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.
pcboot@pcboot-VirtualBox:~$ systemctl start kibana
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede a habilitar y arrancar servicio kibana con el comando `systemctl enable kibana` y `systemctl start kibana`.



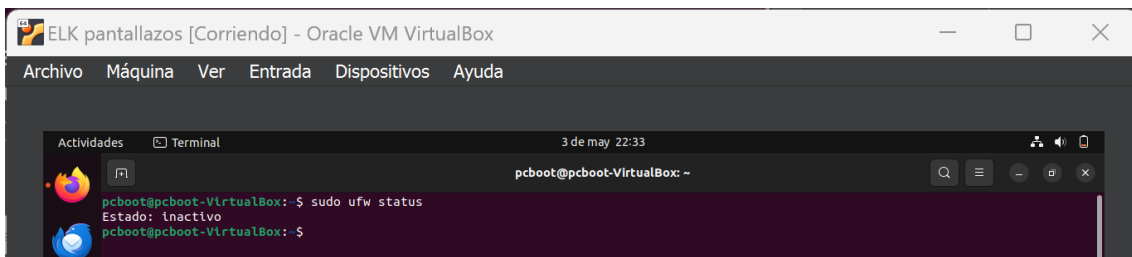
```
pcboot@pcboot-VirtualBox: ~  
$ systemctl status kibana  
kibana.service - Kibana  
Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)  
Active: active (running) since Fri 2024-05-03 22:22:16 CEST; 5min ago  
Docs: https://www.elastic.co  
Main PID: 9916 (node)  
Tasks: 11 (limit: 4599)  
Memory: 263.1M  
CPU: 14.157s  
CGroup: /system.slice/kibana.service  
          └─9916 /usr/share/kibana/bin/./node/bin/node /usr/share/kibana/bin/./src/cli/dist  
  
may 03 22:22:18 pcboot-VirtualBox kibana[9916]: Native global console methods have been overridden in production environment.  
may 03 22:22:20 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:20.676+02:00][INFO ][root] Kibana is starting  
may 03 22:22:20 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:20.796+02:00][INFO ][node] Kibana process configured with roles: d  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:33.242+02:00][INFO ][plugins-service] The following plugins are d  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:33.360+02:00][INFO ][http.server.Preboot] http server running at  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:33.622+02:00][INFO ][plugins-system.preboot] Setting up [1] plugi  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:33.651+02:00][INFO ][preboot] "interactiveSetup" plugin is holdi  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: [2024-05-03T22:22:33.672+02:00][INFO ][root] Holding setup until preboot stage is c  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: i Kibana has not been configured.  
may 03 22:22:33 pcboot-VirtualBox kibana[9916]: Go to http://localhost:5601/?code=642250 to get started.  
lines 1-21/21 (END)
```

En esta pantalla, se procede a verificar si está el servicio kibana esta activado con el comando `systemctl status kibana` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox: ~  
$ netstat -tulnp | grep 5601  
(No todos los procesos pueden ser identificados, no hay información de propiedad del proceso  
no se mostrarán, necesita ser superusuario para verlos todos.)  
tcp      0      0 0.0.0.0:5601 0.0.0.0:*          ESCUCHAR  -  
pcboot@pcboot-VirtualBox: ~$
```

En esta pantalla, se procede a ejecutar el comando `netstat -tulnp | grep 5601` para verificar que kibana está utilizando el puerto 5601.



```
pcboot@pcboot-VirtualBox: ~  
$ sudo ufw status  
Estado: inactivo  
pcboot@pcboot-VirtualBox: ~$
```

En este caso el firewall esta inactivo y no tenemos que hacer nada, pero si el firewall este activo tenemos que configurarlo para permitir el tráfico en el puerto 5601, que es el puerto por defecto de Kibana:

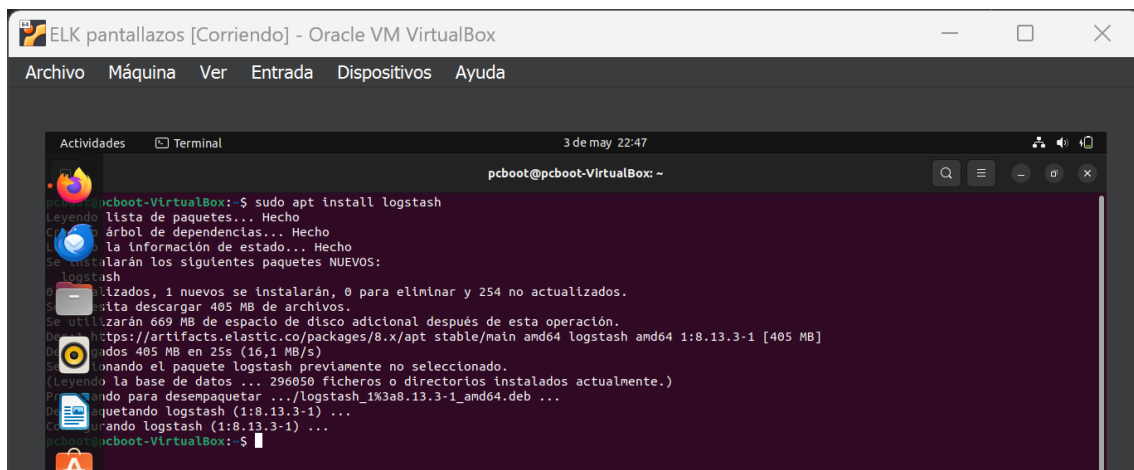
Para permitir el tráfico en el puerto 5601 tenemos que ejecutar el siguiente comando `sudo ufw allow 5601/tcp` esto permitirá el tráfico TCP en el puerto 5601.

Para verificar la regla agregada usaremos el comando `sudo ufw status` esto te mostrará la lista actualizada de reglas del firewall, donde deberías ver la regla que acabas de agregar para el puerto 5601.

Para activar el firewall (si aún no está activado) usaremos el comando `sudo ufw enable` esto activará el firewall y aplicará las reglas que has configurado.

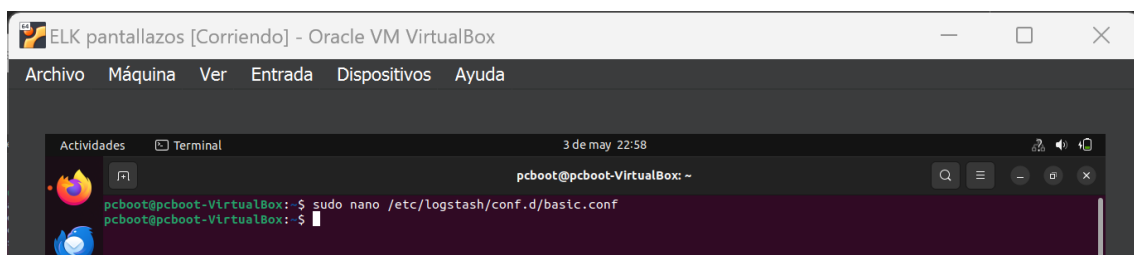
Con estos pasos, deberías haber configurado correctamente el firewall en Ubuntu para permitir el tráfico en el puerto 5601, lo que permitirá a los usuarios acceder a Kibana desde sus navegadores web. Recuerda que estos pasos asumen que estás utilizando `ufw`, que es la herramienta de firewall predeterminada en Ubuntu. Si estás utilizando otra herramienta de firewall, los pasos pueden variar.

5.- Instalación y configuración Logstash



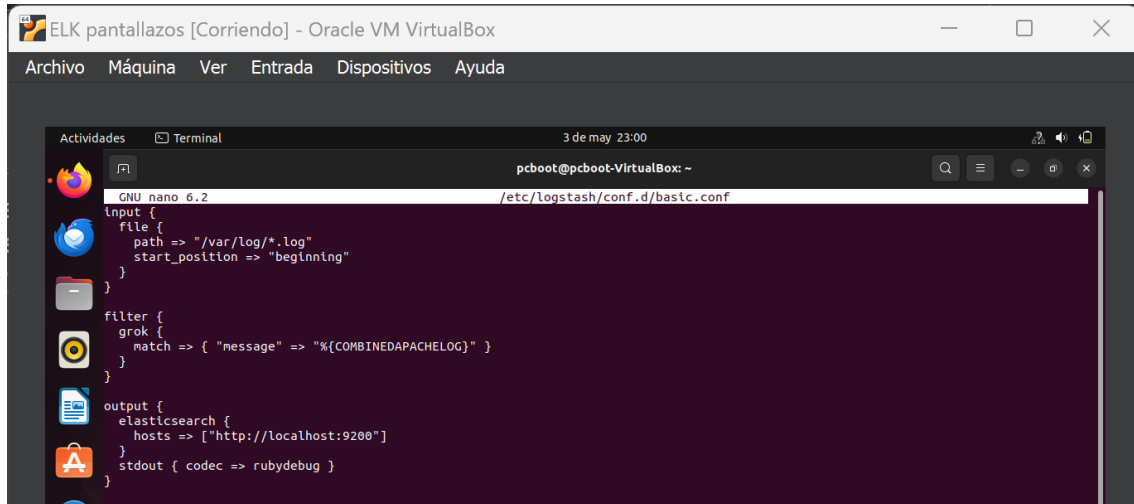
```
pcboot@pcboot-VirtualBox: ~  
$ sudo apt install logstash  
Leyendo lista de paquetes... Hecho  
Construyendo árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  logstash  
Paquetes a instalar: 1 nuevos se instalarán, 0 para eliminar y 254 no actualizados.  
Se utilizarán 669 MB de espacio de disco adicional después de esta operación.  
Se descargará:  
  https://artifacts.elastic.co/packages/8.x/apt/stable/main/amd64/logstash_1:8.13.3-1 [405 MB]  
Se descargarán 405 MB en 25s (16,1 MB/s)  
Construyendo el paquete logstash previamente no seleccionado.  
Leyendo la base de datos ... 296050 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../logstash_1%3a8.13.3-1_amd64.deb ...  
Desempaquetando logstash (1:8.13.3-1) ...  
Construyendo logstash (1:8.13.3-1) ...  
pcboot@pcboot-VirtualBox: ~$
```

En esta pantalla, se procede a instalar el programa logstash con el comando `sudo apt install logstash` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox: ~$ sudo nano /etc/logstash/conf.d/basic.conf  
pcboot@pcboot-VirtualBox: ~$
```

En esta pantalla, se procede a editar el fichero basic.conf con el comando `sudo nano /etc/logstash/conf.d/basic.conf` y pulsamos la tecla Enter para ejecutar el comando.



En esta pantalla, se procede a escribir el código siguiente:

```
input {
  file {
    path => "/var/log/*.log"
    start_position => "beginning"
  }
}

filter {
  grok {
    match      =>      {      "message"      =>
"%{COMBINEDAPACHELOG}" }
  }
}

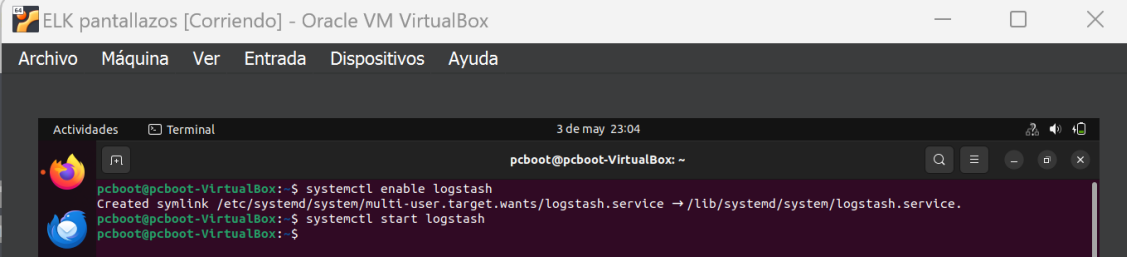
output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
  }
}
```

```
}

stdout { codec => rubydebug }

}
```

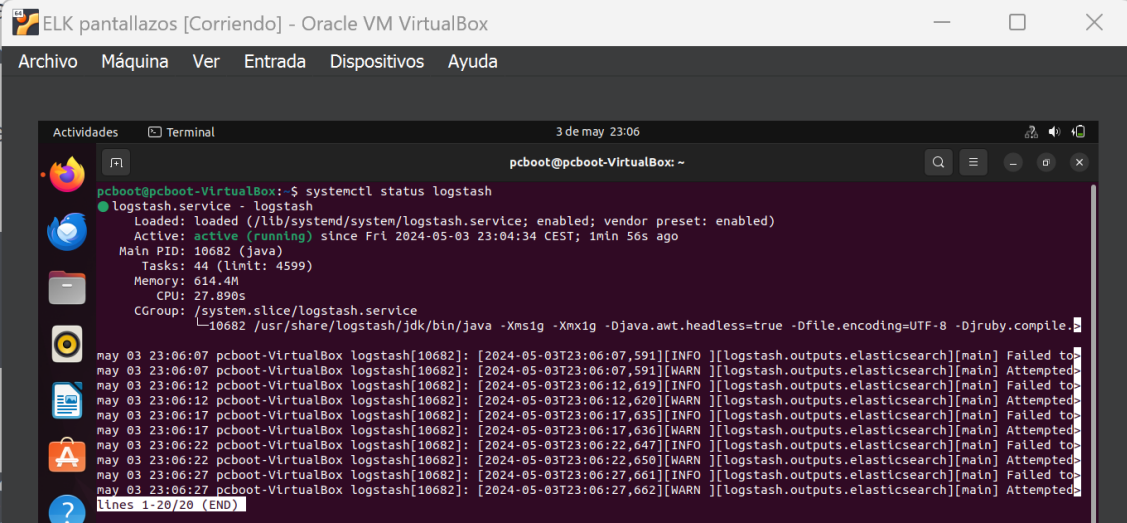
Se procede a guardar el fichero con las teclas CTRL+O para guardar los datos y CTRL+X para salir del editor nano.



```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal
3 de may 23:04
pcboot@pcboot-VirtualBox: ~
pcboot@pcboot-VirtualBox:~$ systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
pcboot@pcboot-VirtualBox:~$ systemctl start logstash
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede a habilitar y arrancar servicio logstash con el comando `systemctl enable logstash` y `systemctl start logstash`.



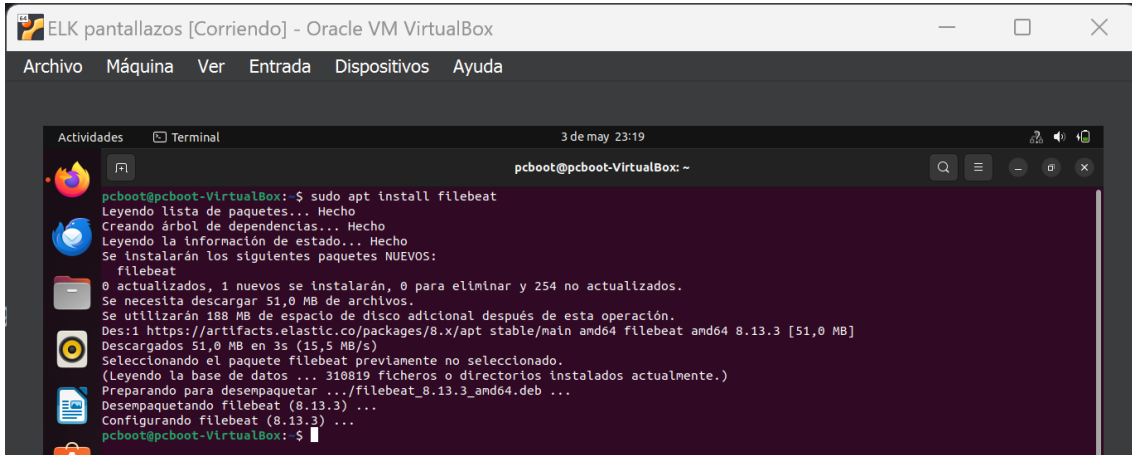
```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Actividades  Terminal
3 de may 23:06
pcboot@pcboot-VirtualBox: ~
pcboot@pcboot-VirtualBox:~$ systemctl status logstash
logstash.service - logstash
Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2024-05-03 23:04:34 CEST; 1min 56s ago
Main PID: 10682 (java)
Tasks: 44 (Limit: 4599)
Memory: 614.4M
CPU: 27.890s
CGroup: /system.slice/logstash.service
└─10682 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile...

may 03 23:06:07 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:07.591][INFO ][logstash.outputs.elasticsearch][main] Failed to
may 03 23:06:07 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:07.591][WARN ][logstash.outputs.elasticsearch][main] Attempted
may 03 23:06:12 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:12.619][INFO ][logstash.outputs.elasticsearch][main] Failed to
may 03 23:06:12 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:12.620][WARN ][logstash.outputs.elasticsearch][main] Attempted
may 03 23:06:17 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:17.635][INFO ][logstash.outputs.elasticsearch][main] Failed to
may 03 23:06:17 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:17.636][WARN ][logstash.outputs.elasticsearch][main] Attempted
may 03 23:06:22 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:22.647][INFO ][logstash.outputs.elasticsearch][main] Failed to
may 03 23:06:22 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:22.650][WARN ][logstash.outputs.elasticsearch][main] Attempted
may 03 23:06:27 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:27.661][INFO ][logstash.outputs.elasticsearch][main] Failed to
may 03 23:06:27 pcboot-VirtualBox logstash[10682]: [2024-05-03T23:06:27.662][WARN ][logstash.outputs.elasticsearch][main] Attempted
lines 1-20/20 (END)
```

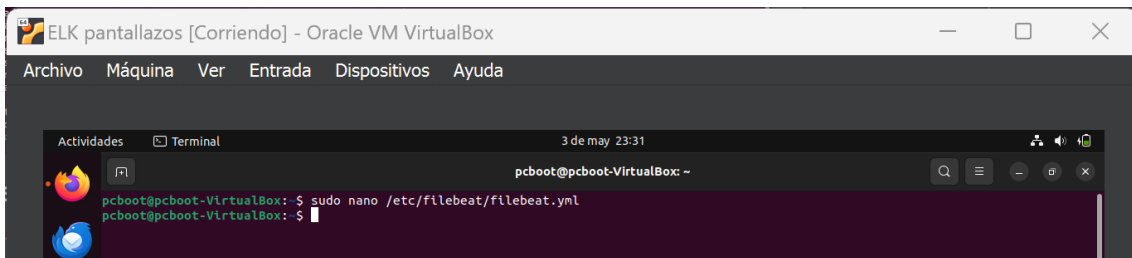
En esta pantalla, se procede a verificar si el servicio esta activo con el comando `systemctl status logstash` y pulsamos la tecla Enter para ejecutar el comando.

6.- Instalación y configuración Filebeat




```
pcboot@pcboot-VirtualBox: ~  
$ sudo apt install filebeat  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes NUEVOS:  
  filebeat  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 254 no actualizados.  
Se necesita descargar 51,0 MB de archivos.  
Se utilizarán 188 MB de espacio de disco adicional después de esta operación.  
Des:1 https://artifacts.elastic.co/packages/8.x/apt/stable/main/amd64/filebeat amd64 8.13.3 [51,0 MB]  
Descargados 51,0 MB en 3s (15,5 MB/s)  
Seleccionando el paquete filebeat previamente no seleccionado.  
(Leyendo la base de datos ... 310819 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../filebeat_8.13.3_amd64.deb ...  
Desempaquetando filebeat (8.13.3) ...  
Configurando filebeat (8.13.3) ...  
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede a instalar filebeat con el comando `sudo apt install filebeat` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox:~$ sudo nano /etc/filebeat/filebeat.yml  
pcboot@pcboot-VirtualBox:~$
```

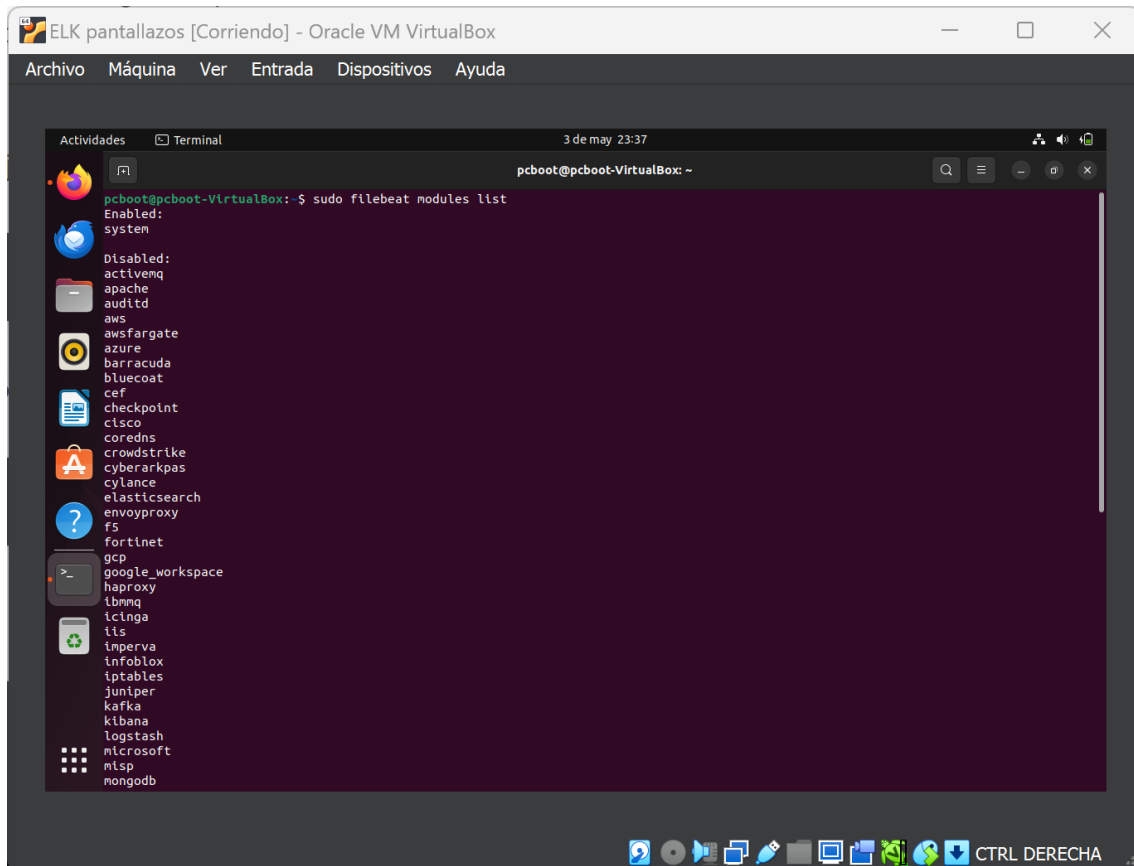
En esta pantalla, se procede a editar el fichero `filebeat.yml` con el comando `sudo nano /etc/filebeat/filebeat.yml` y pulsamos la tecla Enter para ejecutar el comando.



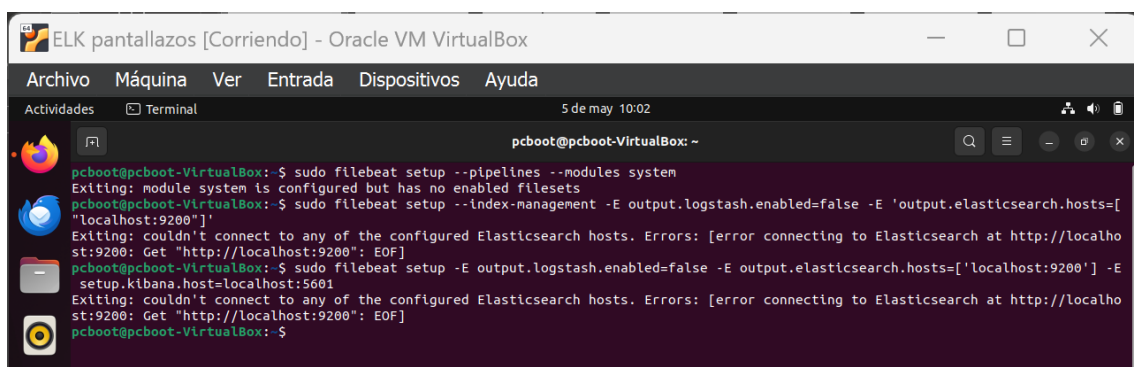
The screenshot shows a terminal window titled "ELK pantallazos [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The terminal interface shows the prompt "pcboot@pcboot-VirtualBox: ~" and the command "sudo filebeat modules enable system" being executed. The output is "Enabled system". The terminal window also displays the date and time "3 de may 23:34" and various system icons.

```
pcboot@pcboot-VirtualBox: ~  
pcboot@pcboot-VirtualBox:~$ sudo filebeat modules enable system  
Enabled system  
pcboot@pcboot-VirtualBox:~$
```

Página 16 de 24



En esta pantalla, se procede realizar un listado de los modulos de filebeat con el comando `sudo filebeat modules list` y pulsamos la tecla Enter para ejecutar el comando.



En esta pantalla, se procede cargar la canalización de ingesta para el módulo del sistema con el comando siguiente:

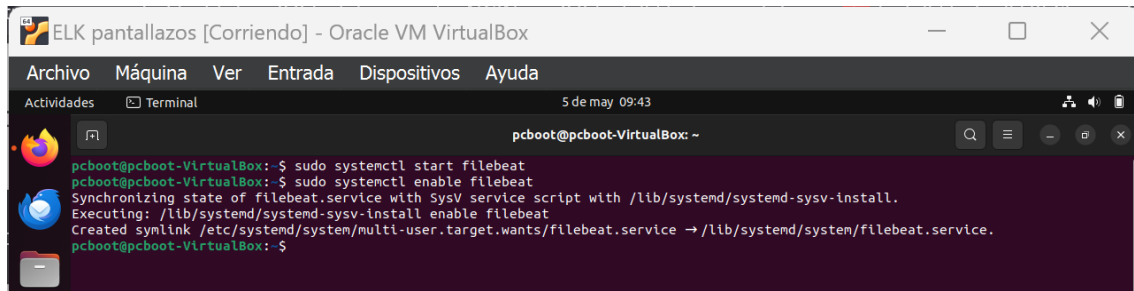
`sudo filebeat setup --pipeline --module system` y pulsamos la tecla Enter para ejecutar el comando.

Se procede, a cargar la plantilla con el comando siguiente:

```
sudo filebeat setup --index-management -E
output.logstash.enabled=false -E
'output.elasticsearch.hosts=['localhost:9200']'
```

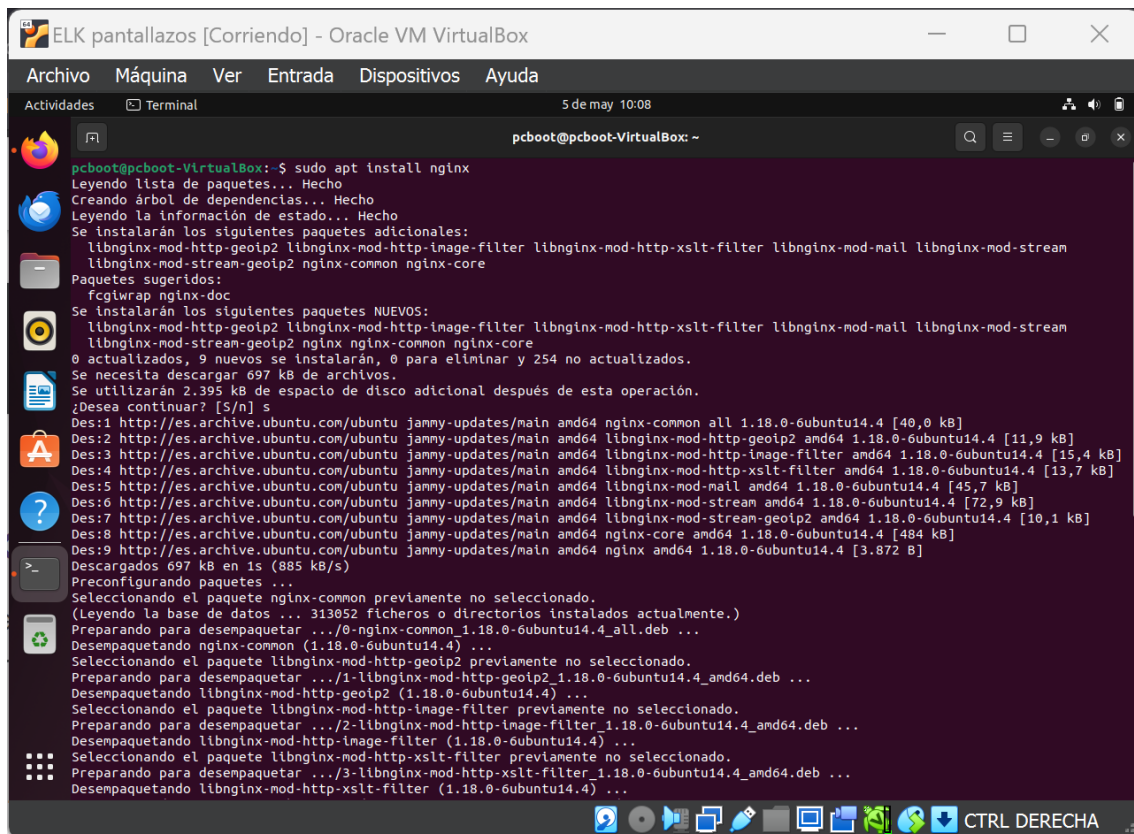
Se procede, a cargar los paneles de kibana prediseñados y visualizar los datos de filebeat con el comando siguiente:

```
sudo filebeat setup -E output.logstash.enabled=false -E
output.elasticsearch.hosts=['localhost:9200'] -E
setup.kibana.host=localhost:5601
```

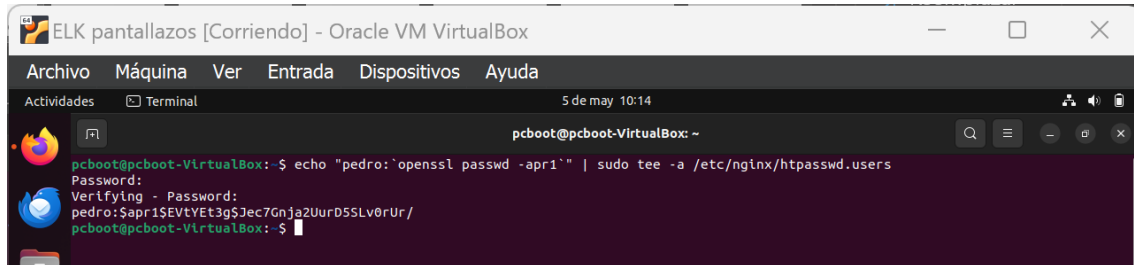


En esta pantalla, se procede iniciar el servicio filebeat con el comando sudo systemctl start filebeat y habilitar filebeat con el comando sudo systemctl enable filebeat.

7.- Instalación y configuración Nginx



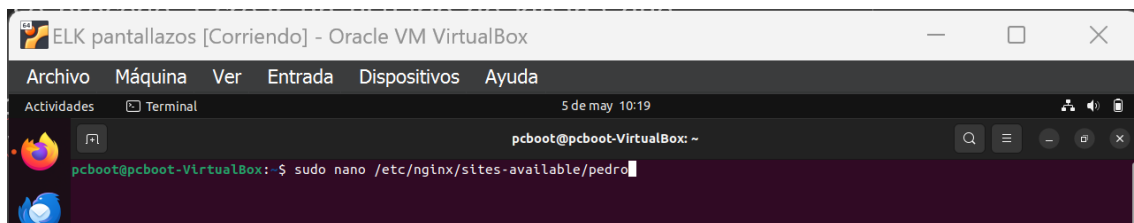
En esta pantalla, se procede a instalar el programa Nginx con el comando `sudo apt install nginx` y pulsamos la tecla Enter para ejecutar el comando.



```
pcboot@pcboot-VirtualBox: ~  
$ sudo apt install nginx  
[...]  
pcboot@pcboot-VirtualBox: ~  
$ echo "pedro:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users  
Password:  
Verifying - Password:  
pedro:$apr1$EVtYEt3g$Jec7GnJa2UurD5SLv0rUr/  
pcboot@pcboot-VirtualBox: ~
```

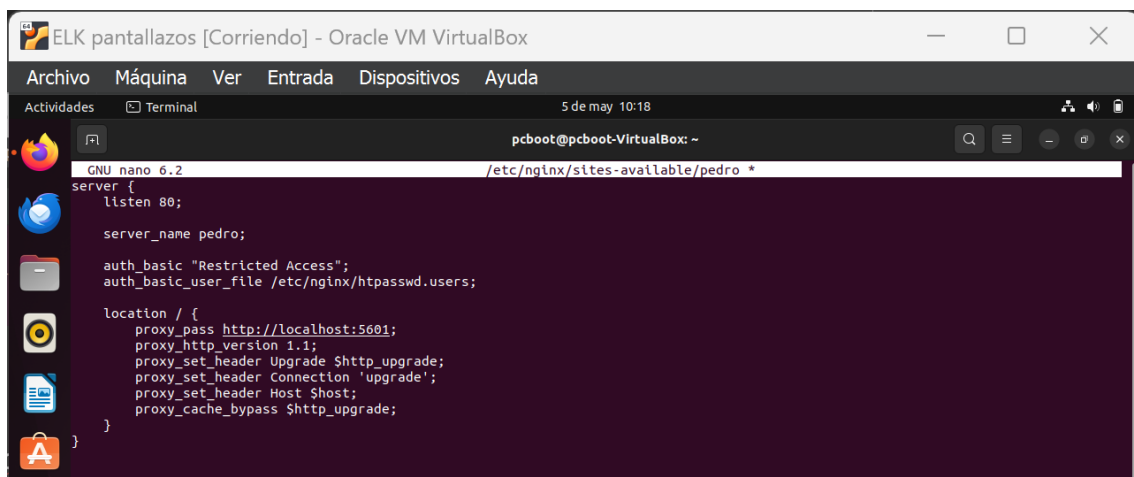
En esta pantalla, se procede a crear un usuario de kibana que utilizará para acceder a la interfaz web con el comando siguiente:

```
echo "pedro:`openssl passwd -apr1`" | sudo tee -a  
/etc/nginx/htpasswd.users
```



```
pcboot@pcboot-VirtualBox: ~  
$ sudo nano /etc/nginx/sites-available/pedro
```

En esta pantalla, se procede a crear un nombre de dominio con el comando `sudo nano /etc/nginx/sites-available/pedro` y pulsamos la tecla Enter para ejecutar el comando.

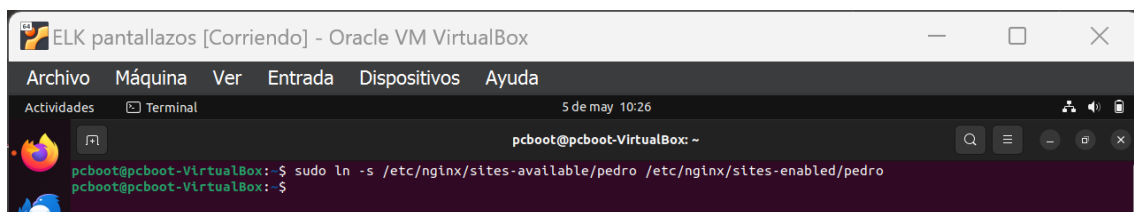


```
GNU nano 6.2 /etc/nginx/sites-available/pedro *  
server {  
    listen 80;  
  
    server_name pedro;  
  
    auth_basic "Restricted Access";  
    auth_basic_user_file /etc/nginx/htpasswd.users;  
  
    location / {  
        proxy_pass http://localhost:5601;  
        proxy_http_version 1.1;  
        proxy_set_header Upgrade $http_upgrade;  
        proxy_set_header Connection 'upgrade';  
        proxy_set_header Host $host;  
        proxy_cache_bypass $http_upgrade;  
    }  
}
```

En esta pantalla, se procede a escribir en el fichero este contenido:

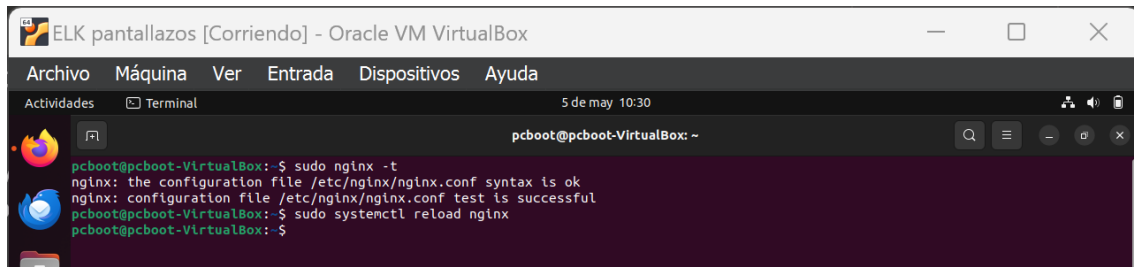
```
server {  
    listen 80;  
  
    server_name pedro;  
  
    auth_basic "Restricted Access";  
    auth_basic_user_file /etc/nginx/htpasswd.users;  
  
    location / {  
        proxy_pass http://localhost:5601;  
        proxy_http_version 1.1;  
        proxy_set_header Upgrade $http_upgrade;  
        proxy_set_header Connection 'upgrade';  
        proxy_set_header Host $host;  
        proxy_cache_bypass $http_upgrade;  
    }  
}
```

Se procede, a guardar el fichero con las tecla CTRL+O para guardar y CTRL+X para salir del nano.



En esta pantalla, se procede habilitar el nuevo fichero de configuración con el comando siguiente:

```
sudo ln -s /etc/nginx/sites-available/pedro /etc/nginx/sites-enabled/pedro
```

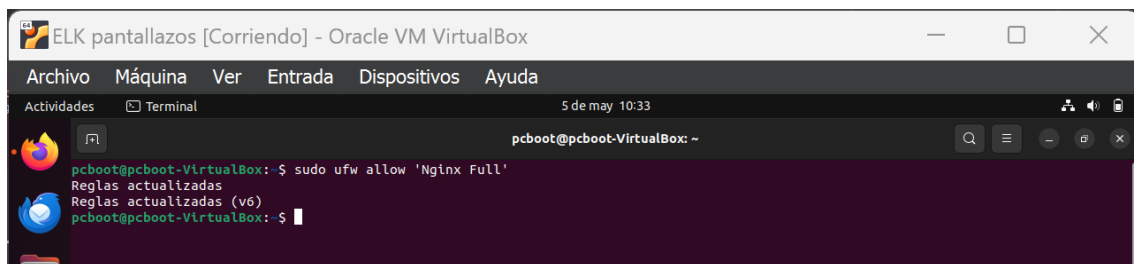


```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
5 de may 10:30
pcboot@pcboot-VirtualBox: ~
pcboot@pcboot-VirtualBox:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
pcboot@pcboot-VirtualBox:~$ sudo systemctl reload nginx
pcboot@pcboot-VirtualBox:~$
```

En esta pantalla, se procede a probar el fichero de configuración y a cargar Nginx con los comandos siguientes:

`sudo nginx -t`

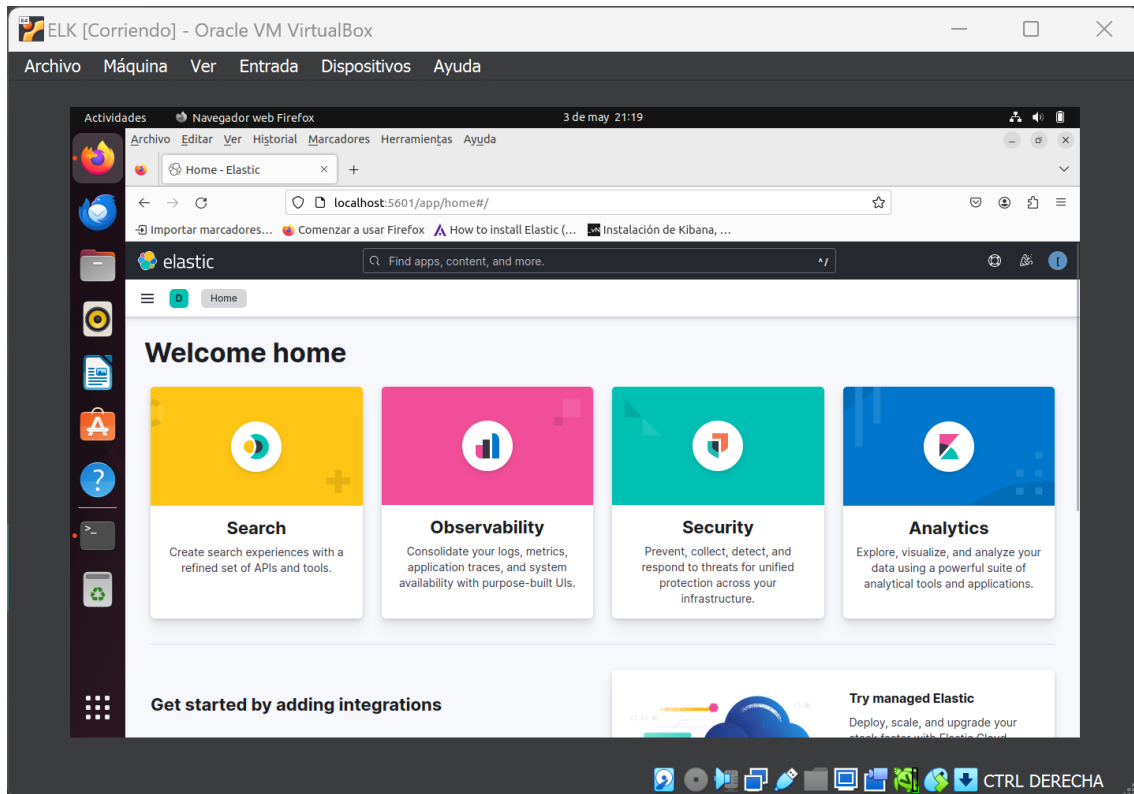
`sudo systemctl reload nginx`



```
ELK pantallazos [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
5 de may 10:33
pcboot@pcboot-VirtualBox: ~
pcboot@pcboot-VirtualBox:~$ sudo ufw allow 'Nginx Full'
Reglas actualizadas
Reglas actualizadas (v6)
pcboot@pcboot-VirtualBox:~$
```

Si tiene un firewall UFW activo, deberá permitir conexiones a Nginx. Puede hacer esto con el comando `ufw allow 'Nginx Full'` pero no es mi caso porque no tengo el firewall UFW activo.

8.- Verificación de la instalación



En esta pantalla se procede, a verificar que todos está instalado correctamente accediendo a kibana desde explorador con url <http://localhost:5601>.

Índice Alfabético

A

Access.....	20
actividades	9
API	4
APT	5
automatización	4
autorización	9

C

canalización.....	17
capacidades.....	4, 9
características	3, 9
comandos.....	5, 7, 21
comentario.....	16
compuesto	3
configuración	2, 3, 12, 15, 18, 20, 21
configurarlo.....	11
conjunto	3, 9
Connection	20
CPU.....	3
creación.....	3
CTRL	7, 14, 16, 20

D

decisiones	10
descripción	3, 9
disponibilidad.....	4

E

editor	14, 16
Elastic	3, 9
Elasticsearch.....	2, 3, 4, 9
ELK.....	2, 3, 4, 9
enriquecimiento.....	3
Enter.....	5, 6, 8, 10, 11, 12, 13, 14, 15, 16, 17, 19
escala	10
específicas	9
exploración	3, 9

F

Filebeat	2, 15
----------------	-------

Full	21
Funcionalidades	4

G

geográficos.....	9
gráficos.....	9

H

herramientas.....	3, 9, 10
Host.....	20
hosts.....	13, 16, 18
HTTP	4

I

información.....	3, 4
informes.....	3, 4
ingesta.....	3, 17
ingestión	4
instalación.....	2, 3, 22
integración	4
interfaz	3, 19
Introducción.....	2, 3
iso 3	

K

KEY	5
Kibana	2, 3, 4, 9, 10, 11, 12

L

lista.....	12
Logstash	2, 3, 4, 9, 12

M

módulo.....	16, 17
monitorización	3
motor	3, 9
múltiples	3, 4, 9

N

necesarias	10
necesidades.....	9
Nginx	2, 3, 18, 19, 21

O

opción	4
opciones.....	9
OpenJDK.....	3
operaciones.....	4
organizaciones	3

P

paneles.....	9, 18
pantalla ...	5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22
patrones.....	9
plantilla	17
poderosa	10
preferencias	9
procesamiento	3
Proxy	3
Puedes.....	9

R

RAM	3
recopilación.....	3
regla	12
reglas.....	12
relevancia.....	4
rendimiento	4
repositorios	5
Requisitos.....	2, 3
RESTful	4
Restricted	20

robustas	9
roles	9

S

Seguridad	9
semántica	4
servicios	4
solicitudes	4
solución.....	3
status	8, 11, 12, 14

T

TCP	12
tecla	5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20
teclas.....	7, 14
tendencias.....	9
tokenización.....	4
tráfico.....	11, 12
transformación	3

U

Ubuntu	3, 5, 12
UFW	21
Upgrade	20
usuario	3, 9, 19
usuarios.....	9, 10, 12

V

valiosa	3
Verificación	2, 22
vista.....	9
visualización	3, 4, 9, 10
visualizaciones	9
volúmenes.....	3, 4, 9, 10