**Instalar la solución de almacenamiento de logs ELK**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Requisitos previos**](#_g59i8ewd3ed3) **2**

[**2.1 Instalación de Java**](#_quz27hoxzkz4) **2**

[**2.2 Instalación de Nginx**](#_uxkninnv14ib) **2**

[**3. Instalar y configurar Elasticsearch**](#_6qvhshx9u3wi) **3**

[**4. Instalar y configurar Kibana**](#_jh7v2ee838y6) **4**

[**5. Instalar y configurar Logstash**](#_1wjnsa1ctytc) **6**

[**6. Instalar y configurar Filebeat**](#_4jf479qvhcji) **7**

[**7. Explorar los paneles de Kibana**](#_votoi5uq2mpn) **10**

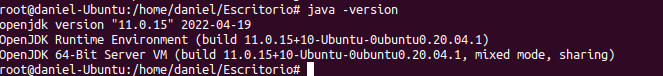
# **2. Requisitos previos**

## **2.1 Instalación de Java**

La opción más sencilla para instalar Java es utilizar la versión que forma parte del paquete de Ubuntu. Por defecto, Ubuntu 20.04 incluye Open JDK 11, que es una variante de código

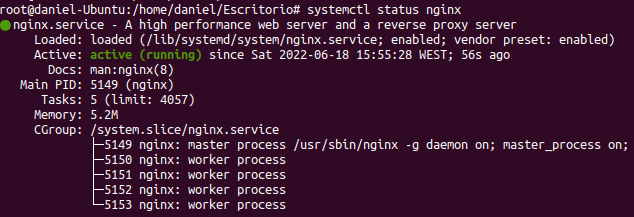
abierto de JRE y JDK.

Para instalar esta versión, primero actualice el índice de paquetes y una vez hecho comprobamos la versión

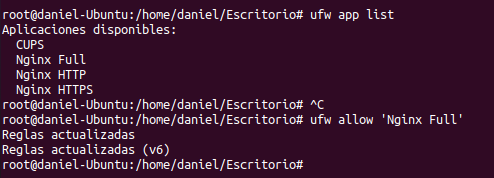


## **2.2 Instalación de Nginx**

Instalamos nginx, seguidamente ajustaremos el firewall ufw para permitir el acceso al servicio. Vemos que aplicaciones podemos abrir con el siguiente comando



Es recomendable que activemos el perfil más restrictivo, pero en nuestro caso permitiremos todo el tráfico.



# **3. Instalar y configurar Elasticsearch**

Para comenzar, utilizaremos cURL, la herramienta de línea de comandos para transferir datos con URL, para importar la clave GPG pública de Elasticsearch a APT.

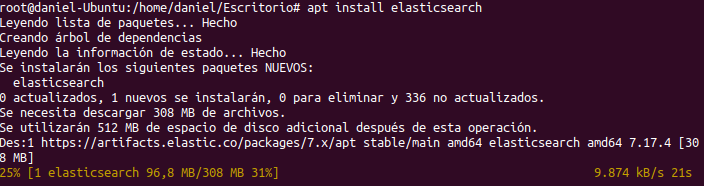
Analizaremos el resultado del comando cURL al programa apt-key, que añade la clave GPG pública a APT.

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

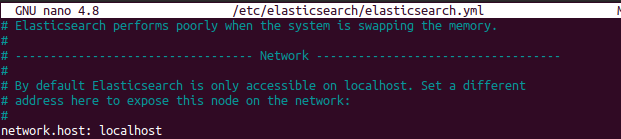
A continuación, agregaremos la lista de fuentes de Elastic al directorio sources.list.d, donde APT buscará nuevas fuentes:

echo “deb https://artifacts.elastic.co/packages/7.x/apt stable main” | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

Ahora podemos instalar elasticsearch

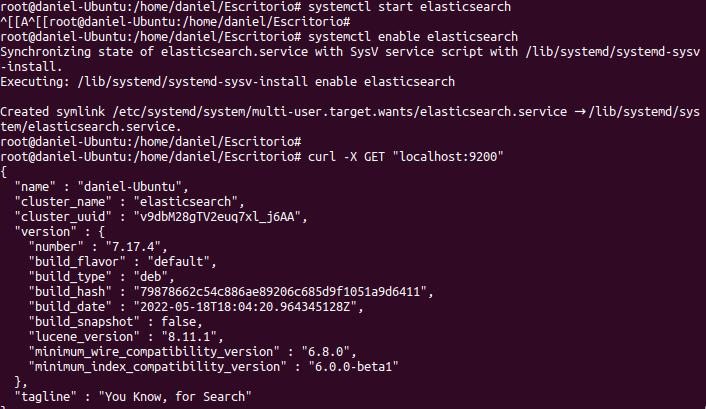


Ahora, Elasticsearch está instalado y listo para usarse. Utilizaremos un editor de texto para editar el archivo de configuración principal de Elasticsearch, elasticsearch.yml.



Iniciamos el servicio de Elasticsearch. Cuando termina, ejecutamos el siguiente comando para permitir que Elasticsearch se cargue cada vez que el servidor se inicia

Podemos comprobar que está funcionando con el siguiente comando:



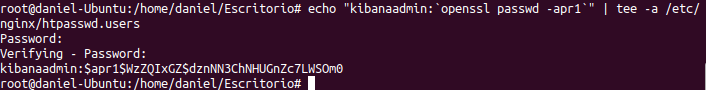
# **4. Instalar y configurar Kibana**

De acuerdo con la documentación oficial, tendremos que instalar Kibana solo después de instalar Elasticsearch. La instalación en este orden garantiza que los componentes de los que depende cada producto estén correctamente implementados.

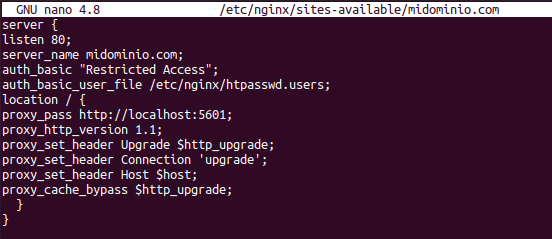
Debido a que ya agregamos la fuente de paquetes de Elastic en el paso anterior, podemos instalar los componentes restantes de Elastic Stack usando apt.

Debido a que Kibana está configurado para escuchar solo en localhost, debemos configurar un proxy inverso para permitir el acceso externo a este. Utilizaremos Nginx para este propósito.

Con el siguiente comando se crearán el usuario y la contraseña administrativa de Kibana, y se almacenarán en el archivo htpasswd.users. Configuraremos Nginx para que requiera este nombre de usuario y contraseña, y lea este archivo de manera momentánea:

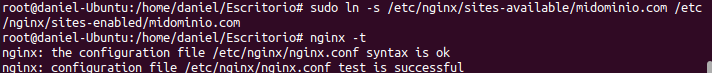


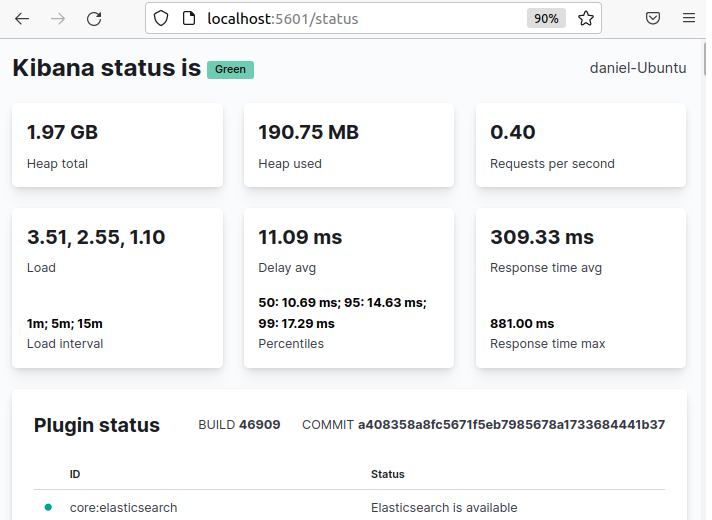
A continuación, creamos un archivo de bloque en Nginx. Añadimos el siguiente bloque de código al archivo, y nos aseguramos de actualizar midominio.com para que coincida con la FQDN o la dirección IP pública de su servidor.



A continuación, habilitamos la nueva configuración creando un enlace simbólico al directorio sites-enabled y comprobamos que no hay errores de sintaxis en la configuración

Con esto, el acceso a Kibana será posible a través de su FQDN o de la dirección IP pública del servidor de Elastic Stack. Podemos comprobar la página de estado del servidor de Kibana visitando la siguiente dirección e ingresando sus credenciales de inicio de sesión cuando se soliciten:



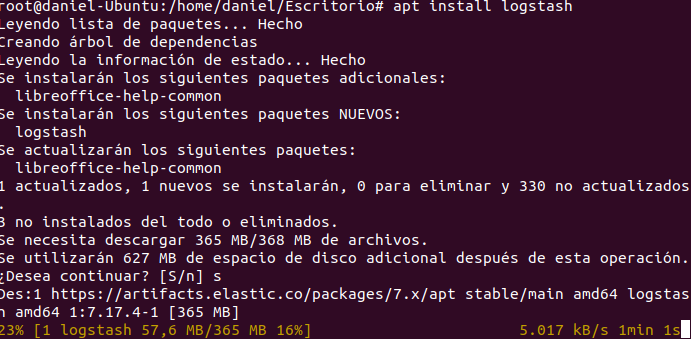


usuario: kibanaadmin password: password

# **5. Instalar y configurar Logstash**

Aunque es posible que Beats envíe datos de manera directa a la base de datos de Elasticsearch, es recomendable usar Logstash para procesar los datos.

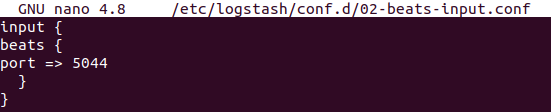
Esto permitirá, de forma más flexible, recopilar datos de diferentes fuentes, transformarlos en un formato común y exportarlos a otra base de datos. Instalamos Logstash con este comando:



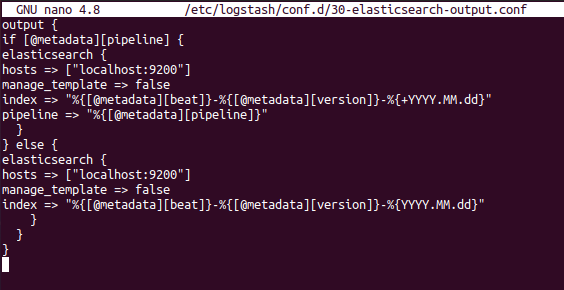
Los archivos de configuración de Logstash residen en el directorio /etc/logstash/conf.d. Para obtener más información sobre la sintaxis de configuración, podemos consultar la referencia de configuración que proporciona Elastic.

Un proceso de Logstash tiene dos elementos necesarios, input y output, y un elemento opcional, filter. Los complementos de entrada consumen datos de una fuente, los complementos del filtro procesan los datos, y los complementos de salida escriben los datos en un destino

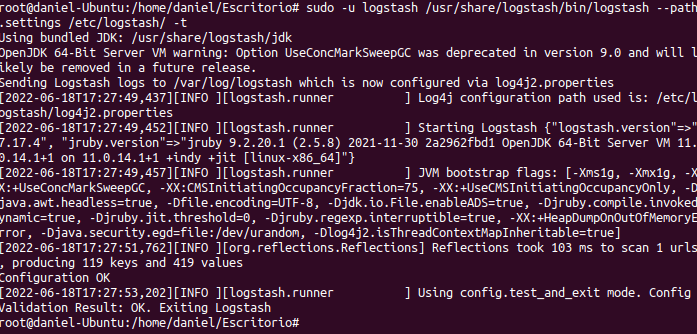
Crearemos un archivo de configuración llamado 02-beats-input.conf en el que establecerá su entrada de Filebeat: Introducimos las siguientes líneas y grabamos



También creamos un archivo de configuración llamado 30-elasticsearch-output.conf:



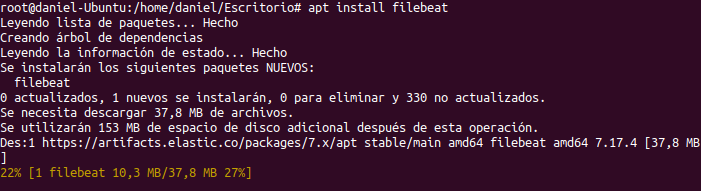
Ahora probamos la configuración de Logstash con el siguiente comando:



# **6. Instalar y configurar Filebeat**

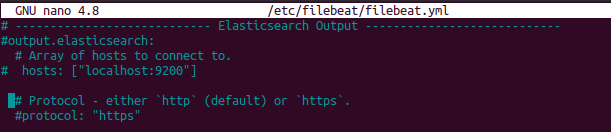
La pila de Elastic utiliza varios transportadores de datos ligeros llamados Beats para recopilar datos de varias fuentes y transportarlos a Logstash o Elasticsearch

Instalamos Filebeat usando apt, a continuación, configuraremos Filebeat para que se conecte a Logstash. Aquí, modificaremos el archivo de configuración de ejemplo que viene con Filebeat.

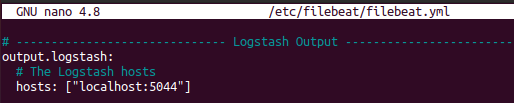


A continuación, configuraremos Filebeat para que se conecte a Logstash. Aquí, modificaremos el archivo de configuración de ejemplo que viene con Filebeat. Usaremos Logstash para aplicar procesamiento adicional a los datos recopilados por Filebeat.

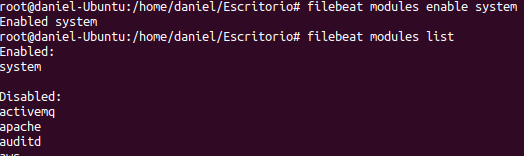
Filebeat no tendrá que enviar datos de manera directa a Elasticsearch, por lo que desactivaremos esa salida. Para hacerlo, buscamos la sección output.elasticsearch y comentamos las siguientes líneas.



A continuación, configuramos la sección output.logstash. Eliminamos el comentario de las líneas output.logstash: y hosts: [”localhost:5044”]

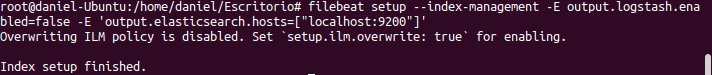


En este tutorial usaremos el módulo de sistema, que recopila y analiza registros creados por el servicio de registro del sistema de distribuciones comunes de Linux. Lo habilitamos

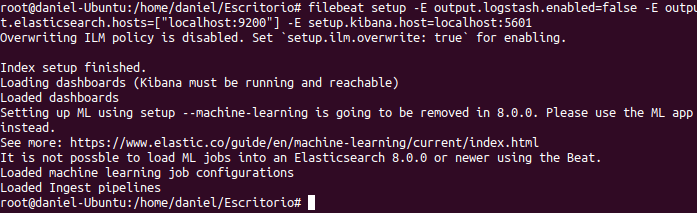


Por defecto, Filebeat está configurado para usar rutas predeterminadas para los registros syslog y de autorización. En el caso de este tutorial, no necesitamos aplicar cambios en la configuración. A continuación, debemos configurar los procesos de ingesta de Filebeat, que analizan los datos de registro antes de enviarlos a través de Logstash a Elasticsearch.

A continuación, cargamos la plantilla de índice en Elasticsearch. Un índice de Elasticsearch es un conjunto de documentos que tienen características similares. Los índices se identifican con un nombre, que se utiliza para referirse al índice cuando se realizan varias operaciones dentro de este. La plantilla de índice se aplicará de forma automática al crear un nuevo índice. Para cargar la plantilla, utilice el siguiente comando:



Al cargar los paneles, Filebeat se conecta a Elasticsearch para verificar la información de la versión. Para cargar paneles cuando se habilite Logstash, tendremos que desactivar el resultado de Logstash y habilitar el de Elasticsearch:

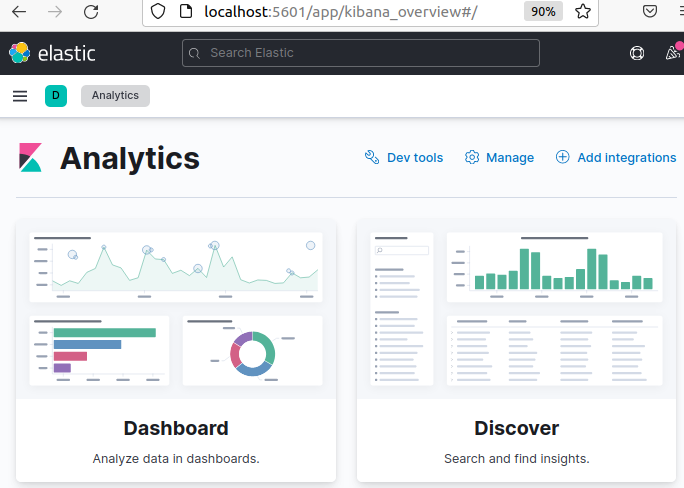


Ahora podemos iniciar y habilitar Filebeat. Si configuramos la pila de Elastic de manera correcta, Filebeat iniciará el envío de sus registros syslog y de autorización a Logstash, que a su vez cargará esos datos en Elasticsearch. Para verificar que Elasticsearch realmente reciba estos datos, podemos consultar el índice de Filebeat con este comando:



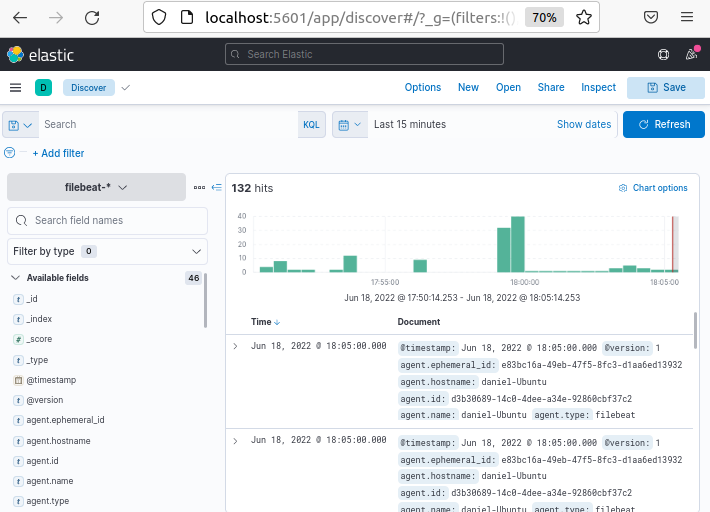
# **7. Explorar los paneles de Kibana**

Una vez que hayamos iniciado sesión, deberíamos recibir la página de inicio de Kibana:



Hacemos clic en el enlace Descubrir de la barra de navegación a la izquierda. En la página Discover, seleccionamos el patrón de índice predeterminado de filebeat-\* para ver datos de Filebeat.

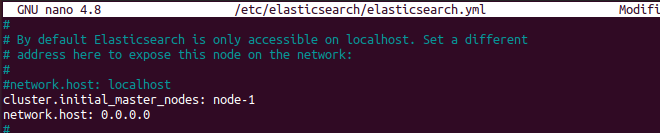
- Visualizaremos un histograma con eventos de registro y algunos mensajes de registro a continuación:



Si queremos conectar una máquina Windows a nuestro sistema para que envíe los datos de los registros.

Tendremos que cambiar la configuración del fichero elasticsearch.yml y decirle que escuche

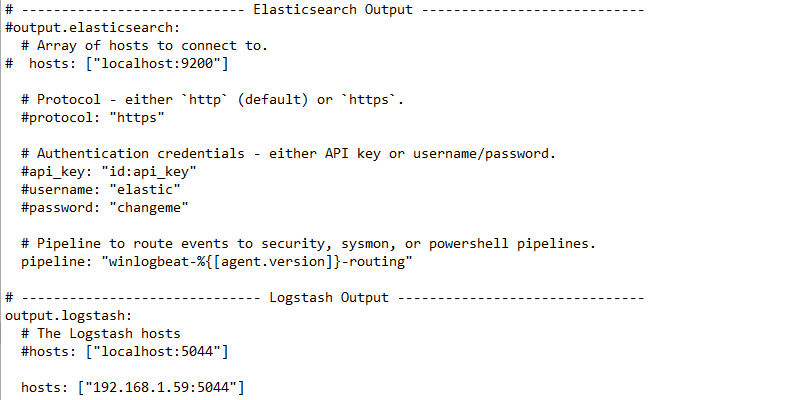
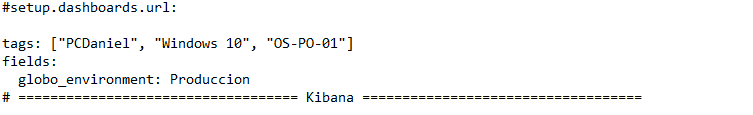
en todas las direcciones de red:

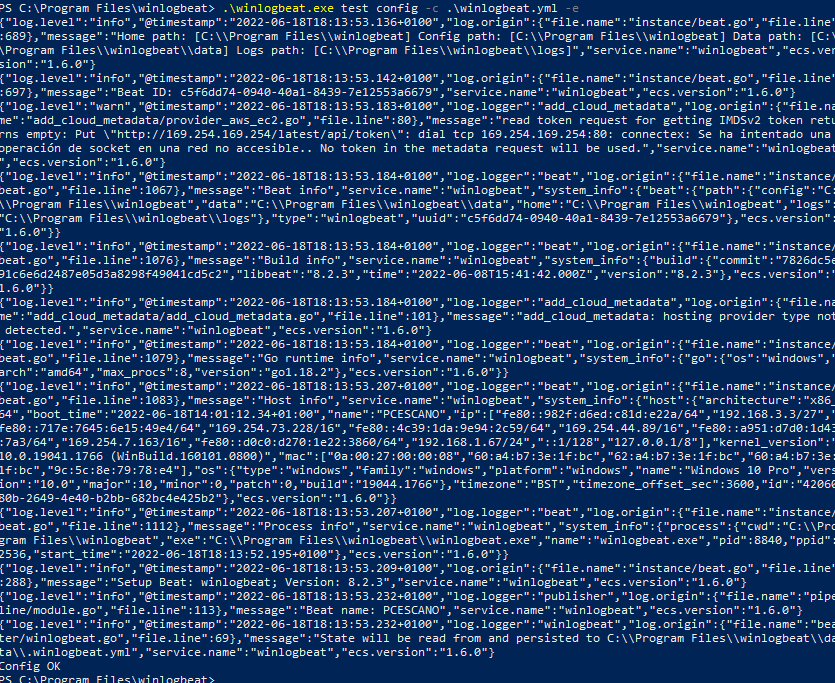


Seguidamente descargamos winlogbeat en la máquina de Windows.

Copiamos el contenido del zip en C:\archivos de programa\winlogbeat

Editamos el fichero winlogbeat.yml y configuramos la conexión con logstash





Bien, ahora desde Kibana crearemos el patrón para este índice, abrimos Kibana, «Management» >» Index Patterns» > «Create Index Pattern», indicamos como patrón ‘winlogbeat-\*’ y seguimos el asistente:



Para ver los datos que hemos ido obteniendo, vamos a «Discover», seleccionamos el patrón recién creado de Winlogbeat, si todo ha ido como debe, nuestros equipos Windows le estarán mandando los eventos a Logstash y éste a Elasticsearch, tendremos almacenados los registros de todos los eventos que hemos redirigido.

