

**ASIR**

PASIR

# MANUAL DE INSTALACIÓN

Pedro Peralta Guerrero  
18 de junio de 2023

# Índice

<b>1. REQUISITOS (INSTALACIÓN NORMAL).</b>	<b>2</b>
1.1. Compatibilidad del sistema operativo y del sistema de archivos. . . . .	2
1.2. Compatibilidad con Java. . . . .	2
1.3. Requisitos de red. . . . .	2
1.4. Ajustes importantes. . . . .	2
<b>2. REQUISITOS (INSTALACIÓN CON DOCKER).</b>	<b>3</b>
2.1. Configuración importante del host. . . . .	3
2.2. Despliegue de los contenedores. . . . .	3
<b>3. Instalación y configuración de logstash</b>	<b>4</b>
<b>4. Instalación de los clientes.</b>	<b>4</b>
4.1. Instalación de Filebeat. . . . .	4
4.2. Fichero filebeat.yml . . . . .	4

## 1. REQUISITOS (INSTALACIÓN NORMAL).

### 1.1. Compatibilidad del sistema operativo y del sistema de archivos.

Se recomienda instalar OpenSearch en Red Hat Enterprise Linux (RHEL) o distribuciones Linux basadas en Debian que utilicen systemd. Evitar utilizar un sistema de archivos de red para el almacenamiento de nodos en un flujo de trabajo de producción. El uso de un sistema de archivos de red para el almacenamiento de nodos puede causar problemas de rendimiento en el clúster debido a factores como las condiciones de la red (como la latencia o el rendimiento limitado) o las velocidades de lectura y escritura. Se debe utilizar unidades de estado sólido (SSD) instaladas en el host para el almacenamiento de nodos siempre que sea posible.

### 1.2. Compatibilidad con Java.

Versión de OpenSearch	Versiones de Java compatibles	Versión Java incluida
1.0 - 1.2.x	11, 15	15.0.1+9
1.3.x	8, 11, 14	8, 11, 14
2.0.0	2.0.0	17.0.2+8

Para utilizar una instalación de Java es necesario establecer la siguiente variable de entorno: **OPENSEARCH\_JAVA\_HOME**

### 1.3. Requisitos de red.

Los siguientes puertos deben estar abiertos para los componentes de OpenSearch.

Número de puerto	Componente OpenSearch
443	Paneles de OpenSearch en AWS OpenSearch Service con cifrado en tránsito (TLS)
5601	Paneles de OpenSearch
9200	OpenSearch REST API
9250	Búsqueda entre clústeres
9250	Búsqueda entre clústeres
9600	Analizador de rendimiento

### 1.4. Ajustes importantes.

Para cargas de trabajo de producción, es necesario aumentar el valor de la propiedad del kernel **vm.max\_map\_count** se trata de una propiedad del kernel utilizada para definir el número máximo de áreas de mapa de memoria que un proceso puede tener. Debe recibir el valor **262144**.

## 2. REQUISITOS (INSTALACIÓN CON DOCKER).

Para empezar necesitaremos descargar e instalar Docker en nuestro sistema, para ello podemos seguir los pasos de la [guía oficial](#).

### 2.1. Configuración importante del host.

Antes de iniciar OpenSearch, se debe revisar algunas configuraciones importantes[1.4] del sistema que pueden afectar el rendimiento de los servicios.

Deshabilitar la paginación de memoria y el rendimiento de intercambio en el host para mejorar el rendimiento: **sudo swapoff -a**.

Aumentar el número de mapas de memoria disponibles para OpenSearch: **vm.max\_map\_count=262144**

### 2.2. Despliegue de los contenedores.

Para desplegar los contenedores se debe descargar el fichero docker-compose.yml alojado en [GitHub](#).

Antes de lanzar estos contenedores con la instrucción docker-compose es muy probable que interese modificarlos para mapear los volúmenes en la ruta más adecuada. También es interesante cambiar el nombre de la red(no es obligatorio pero es recomendable elegir un propio.)

Una vez desplegados los contenedores es importante modificar ciertos parámetros del Dashboard para que este funcione correctamente.

Haciendo uso del editor nano o vi modificaremos el archivo **opensearch\_dashboards.yml**, situado en la ruta donde se encuentre el volumen correspondiente, y establecemos las siguientes variables:

- **opensearchDashboards.autocompleteTimeout=1000000**
- **opensearchDashboards.autocompleteTerminateAfter: 1000000**

Con esto solucionaremos un problema a la hora de intentar utilizar los controles que si no añadimos esto cuando intentemos filtrar nos aparecerá el siguiente error:

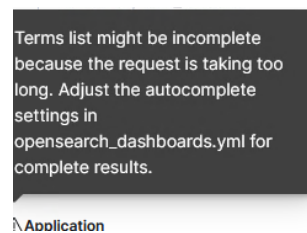


Figura 1: Error dashboard

Una vez desplegado el todos los contenedores haciendo uso de **docker ps** deberíamos ver 4 contenedores:

```
root@opensearch:~# docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
17c94ea24758	opensearchproject/logstash-oss-with-opensearch-output-plugin:8.6.1	"/usr/local/bin/dock..."	3 days ago	Up 3 minutes	0.0.0.0:5044->5044/tcp, :::5044->5044/tcp, 9600/tcp
logstash	opensearchproject/opensearch-dashboards:latest	"/opensearch-dashbo..."	3 days ago	Up 3 minutes	0.0.0.0:5601->5601/tcp, :::5601->5601/tcp
opensearch-dashboards	opensearchproject/opensearch:latest	"/opensearch-docker..."	3 days ago	Up 3 minutes	9200/tcp, 9300/tcp, 9600/tcp, 9650/tcp
18774a523c05	opensearchproject/opensearch:latest	"/opensearch-docker..."	3 days ago	Up 3 minutes	9200/tcp, 9300/tcp, 9600/tcp, 9650/tcp
opensearch-node2	opensearchproject/opensearch:latest	"/opensearch-docker..."	3 days ago	Up 3 minutes	0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp, 0.0.0.0:9600->9600/tcp, :::9600->9600/tcp, 9650/tcp
opensearch-node1	opensearchproject/opensearch:latest	"/opensearch-docker..."	3 days ago	Up 3 minutes	0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp, 0.0.0.0:9600->9600/tcp, :::9600->9600/tcp, 9650/tcp

```
root@opensearch:~#
```

Figura 2: docker ps

Ya podríamos acceder al panel a través de la url: <http://<ip>:5601>

### 3. Instalación y configuración de logstash

Para la instalación de logstash haremos uso de dos ficheros alojados en [GitHub](#), logstash.conf y docker-compose-logstash.yml.

El archivo logstash.conf corresponde a la configuración principal y debe ser alojado en el lugar que el administrador desee pero luego hay que indicar la ruta en el fichero docker-compose-logstash.yml.

También es muy importante modificar el fichero de docker-compose para indicar la red ya que logstash debe estar en la misma que los contenedores de OpenSearch.

### 4. Instalación de los clientes.

Para enviar los logs de los equipos clientes hacia Logstash usaré **Filebeat**, se trata de un agente ligero que nos permite enviar y centralizar logs y archivos.

#### 4.1. Instalación de Filebeat.

1.Descargar e instalar la clave de firma pública.

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

2.Instalar el paquete apt-transport-https antes de continuar(Debian).

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

3.Guardar la definición del repositorio en /etc/apt/sources.list.d/elastic-8.x.list

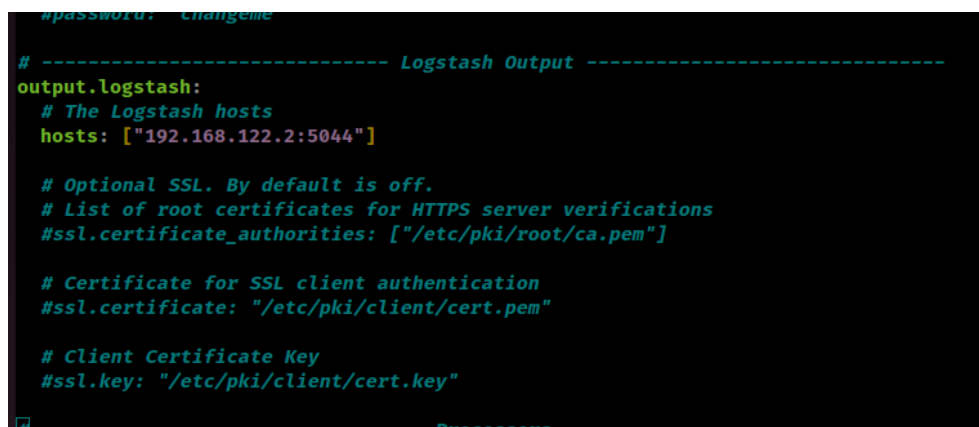
```
1 echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a  
/etc/apt/sources.list.d/elastic-8.x.list
```

4.Ejecutar apt update e instalar.

```
1 apt update && apt install filebeat  
2 systemctl enable filebeat
```

#### 4.2. Fichero filebeat.yml

En este fichero debemos de buscar el apartado **Logstash Output** y definiremos la variable **hosts** con el valor que corresponda, es decir, la dirección ip de la máquina que contiene el plugin Logstash y el puerto que le hayamos establecido.



```
#password: changeme  
  
# ----- Logstash Output -----  
output.logstash:  
  # The Logstash hosts  
  hosts: ["192.168.122.2:5044"]  
  
  # Optional SSL. By default is off.  
  # List of root certificates for HTTPS server verifications  
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]  
  
  # Certificate for SSL client authentication  
  #ssl.certificate: "/etc/pki/client/cert.pem"  
  
  # Client Certificate Key  
  #ssl.key: "/etc/pki/client/cert.key"  
  
# ----- Processors -----
```

Figura 3: filebeat.yml

Además debemos de tener establecido lo siguiente:

```
1 filebeat.config.modules:
2   path: ${path.config}/modules.d/*.yaml
3   reload.enabled: false
4
5 setup.template.settings:
6   index.number_of_shards: 1
7
8 output.logstash:
9   hosts: ["<direccion>:<puerto>"]
10
11 processors:
12   - add_host_metadata:
13     when.not.contains.tags: forwarded
14   - add_cloud_metadata: ~
15   - add_docker_metadata: ~
16   - add_kubernetes_metadata: ~
```

El resto del fichero puede estar comentado.

Para finalizar activaremos el módulo system de Filebeat y indicaremos los logs del sistema que queremos enviar:

```
1 #Activar el modulo system
2 filebeat modules enable system
3 #Comprobar los modulos activados
4 filebeat modules list
```

Ya activado debemos de modificar el fichero correspondiente que se encontrará en **/etc/filebeat/modules.d/system.yml**

```
1 # Module: system Docs: https://www.elastic.co/guide/en/beats/filebeat/master/
   filebeat-module-system.html
2
3 - module: system
4   # Syslog
5   syslog:
6     enabled: true
7     var.paths: ["/var/log/syslog"]
8
9   auth:
10    enabled: true
11    var.paths: ["/var/log/auth.log"]
```