Contenidos

[1. Instalar Java y Nginx 1](#_Toc123819679)

[2. Instalar y Configurar Elasticsearch 1](#_Toc123819680)

[3. Instalar Logstash 4](#_Toc123819681)

[4. Instalar y Configurar Kibana 4](#_Toc123819682)

[5. Instalar y Configurar Filebeat 6](#_Toc123819683)

[6. Acceder a la interfaz web de Kibana 7](#_Toc123819684)

[Conclusion 7](#_Toc123819685)

1. Instalar Java y Nginx

1. Actualizar los paquetes del sistema.

$ sudo apt update

1. Instalar paquetes requeridos.

$ sudo apt install wget curl gnupg2 -y

1. Para corer Elasticsearch, se require Java. Instalar Java.

$ sudo apt install openjdk-11-jdk -y

1. Verificar instalación.

$ java -version

1. El dashboard de Kibana usa Nginx como proxy reverso. Instala Nginx webserver.

$ sudo apt install nginx -y

## 2. Instalar y Configurar Elasticsearch

1. Instalar paquetes requeridos.

$ sudo apt install apt-transport-https -y

1. Importar la llave de firma de Elasticsearch PGP.

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

1. Añadir repositorio de Elasticsearch APT.

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

1. Actualizar sistema.

$ sudo apt update

1. Instalar Elasticsearch.

$ sudo apt install elasticsearch -y

1. Editar archivo de configuración de Elasticsearch.

$ sudo nano /etc/elasticsearch/elasticsearch.yml

1. Quitar el comentario “#” de las siguientes líneas.

#network.host: 192.168.0.1

#http.port: 9200

Cambiar valor de network.host a localhost y añadir la siguiente línea en la sección Discovery.

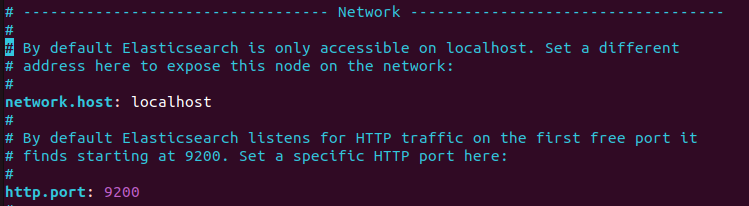
discovery.type: single-node

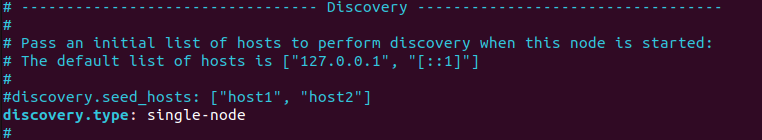
El archivo final debe contener las siguientes líneas:

network.host: localhost

http.port: 9200

discovery.type: single-node





Una cosa opcional que puede hacer mientras configura el archivo de Elasticsearch es que puede cambiar el directorio donde se guardara la base de datos de Elasticsearch.

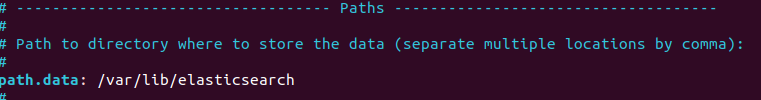
Primero debe cambiar el propietario a elasticsearch del directorio en donde quiere que sea guardado la base de datos de elasticsearch.

$ sudo chown -R elasticsearch:elasticsearch /nuevo/directorio

Luego modificamos el siguiente archivo de elasticsearch.

$ sudo vim /etc/elasticsearch/elasticsearch.yml

Modificamos el valor **/var/lib/elasticsearch** al **/nuevo/directorio**



1. Guardar y cerrar archivo.

Ahora, si siguió el paso opcional, los datos de Elasticsearch serán guardados en el nuevo directorio. Esto es útil para expandir el deposito de datos cuando esta queda corta en nuestro servidor de ELK STACK, otorgando la habilidad de mover la base de datos a otro disco con mayor capacidad de almacenamiento.

Una vez hecho esto, también puede mover el contenido del directorio anterior de la base de datos al nuevo.

sudo mv -vf /var/lib/elasticsearch/\* /nuevo/directorio

1. Recargar el daemon.

$ sudo systemctl daemon-reload

1. Iniciar el servicio de Elasticsearch.

$ sudo systemctl start elasticsearch

1. Habilitar el servicio de Elasticsearch para que inicie al inicio del sistema.

$ sudo systemctl enable elasticsearch

1. Verificar que Elasticsearch esté corriendo y escuchando en el puerto 9200.

$ curl -X GET "localhost:9200"

## 3. Instalar Logstash

1. Instalar Logstash.

$ sudo apt install logstash -y

1. Iniciar el servicio de Logstash.

$ sudo systemctl start logstash

1. Habilitar el servicio de Logstash para que inicie al inicio del sistema.

$ sudo systemctl enable logstash

1. Verificar el estado del servicio de Logstash.

$ sudo systemctl status logstash

## 4. Instalar y configurar Kibana

1. Instalar Kibana.

$ sudo apt install kibana -y

1. Editar el archive de configuración de Kibana.

$ sudo nano /etc/kibana/kibana.yml

1. Quitar el comentario “#” y modificar las siguientes líneas de:

#server.port: 5601

#server.host: "localhost"

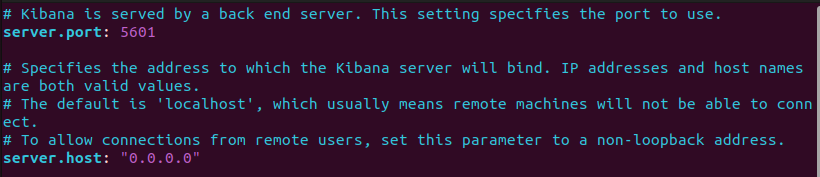
#elasticsearch.hosts: ["http://localhost:9200"]

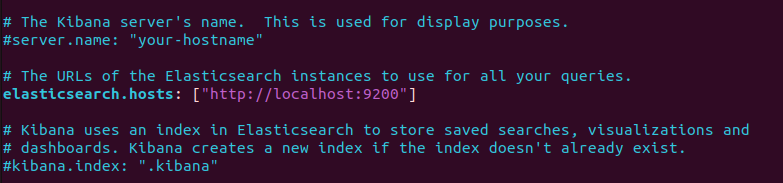
A esto:

server.port: 5601

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://localhost:9200"]





1. Guardar y cerrar el archivo.
2. Iniciar el servicio de Kibana.

$ sudo systemctl start kibana

1. Habilitar el servicio de Kibana para que inicie al inicio de sistema.

$ sudo systemctl enable kibana

1. Habilitar tráfico para el puerto 5601.

$ sudo ufw allow 5601/tcp

## 5. Instalar y Configurar Filebeat

1. Instalar Filebeat.

$ sudo apt install filebeat -y

1. Editar el archive de configuración de Filebeat.

$ sudo nano /etc/filebeat/filebeat.yml

Comentar las siguientes lineas con un “#” al inicio de linea:

#output.elasticsearch:

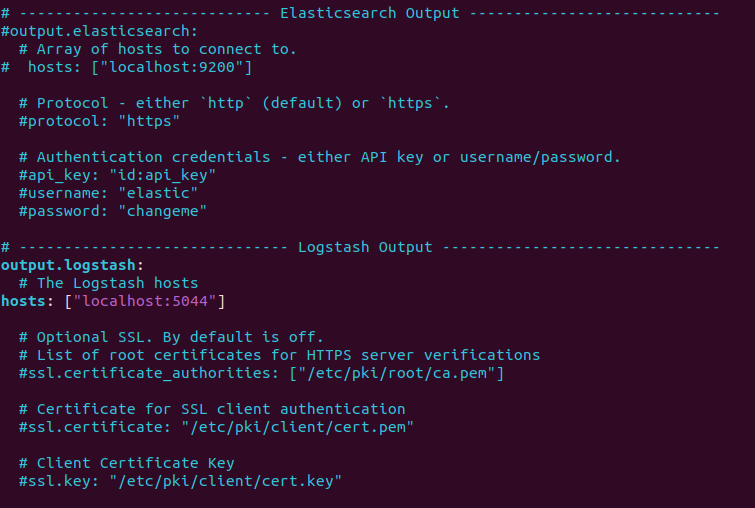
# Array of hosts to connect to.

#hosts: ["localhost:9200"]

Quitar el comentario “#” de Logstash en la sección de output:

output.logstash:

hosts: ["localhost:5044"]



1. Guardar y salir del archivo.
2. Habilitar el sistema de modulos de filebeat.

$ sudo filebeat modules enable system

1. Cargar el index template.

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

1. Iniciar el servicio de Filebeat.

$ sudo systemctl start filebeat

1. Habilitar el servicio de Filebeat para que inicie al inicio de sistema.

$ sudo systemctl enable filebeat

1. Verificar que Filebeat este enviando archivos de log a Logstash para ser procesados.

$ curl -XGET http://localhost:9200/\_cat/indices?v

## 6. Acceder a la interfaz web de Kibana

Abrir un navegador de internet y acceder a la interfaz web de Kibana a través de la siguiente URL http://YourServerIP:5601. Por ejemplo:

http://192.0.2.10:5601

o

http://localhost:5601

## Conclusion

Has instalado exitosamente Elastic Stack en tu servidor. Ya puede acceder al dashboard principal via la interfaz web de Kibana.