**INSTALACION**

Se va a realizar la instalación en servidor dedicado, con tres servidores por cada parte del ELK Stack, tres de elasticsearch, tres de logstash y uno de kibana para balancear la carga, todos ellos serán en sistema operativo RHEL 8 y tendrán 4 CPUs y 8 GB de RAM.

## ELASTICSEARCH

### Instalación Elasticsearch

Lo primero que se hará será importar la clave GPG de Elasticsearch todos los servidores donde se vaya a montar el Elasticsearch (en este caso son tres). Se hará lanzando el siguiente comando:

rpm-import https://artifacts.elastic.co/GPG-KEY-elasticsearch

En segundo lugar, se creará el repositorio en la ruta: ***/etc/yum.repos.d/elastic.repo***

En el repositorio se indicará lo siguiente:

Texto

Descripción generada automáticamente

Ilustración 2 : Repositorio Elasticsearch

Ahora hay que configurar el fichero ***/etc/hosts*** donde se pondrá la IP y el hostname de las máquinas que van a pertenecer a nuestro elastic. Esto se tendrá que hacer en todos los servidores que vayan a pertenecer a elastic siendo el fichero igual en todos.

Antes de finalizar la instalación de Elasticsearch será necesario instalar Java JDK con el siguiente comando ***yum install java-openjdk -y.*** Esto se tendrá que hacer en los tres servidores de este Elasticsearch y en los otros tres servidores donde se instale el logstash.

Por último, se ejecutará ***yum install elasticsearch -y*** en los tres servidores. Una vez hecho con el comando ***yum list elasticsearch*** se podrán ver los paquetes instalados junto a la versión.

### Configuración Elasticsearch

Para configurar los servidores de Elasticsearch se hará en la ruta ***/etc/elasticsearch/elasticsearch.yml.***

En este fichero se buscará “xpack.security.enabled” y se debe poner en false en cada uno de los servidores hasta que se configure la seguridad de kibana, momento en el que este campo será cambiado a true.



Ilustración 3 : Configuración Elasticsearch 1

El servidor emvelksearchtest01 quedará así:

Texto

Descripción generada automáticamente

Ilustración 4 : Configuración Elasticsearch 2

Se repetirá el mismo proceso en los demás servidores de Elasticsearch indicando el network.host y el node.name correspondiente.

### Iniciar el servicio

Estos comandos se tendrán que ejecutar en los tres servidores:

1. systemctl daemon-reload

2. systemctl enable elasticsearch.service

3. systemctl start elasticsearch.service

4. netstat -putona |grep 9200

Este último comando dará una salida como la siguiente:

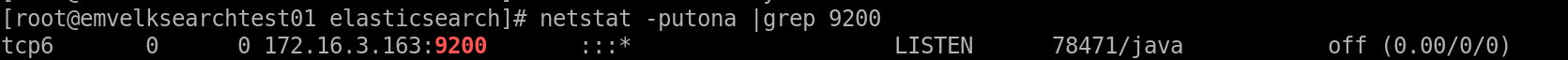


Ilustración 5 : Puertos Elasticsearch

Una vez hecho esto se probarán estas ejecuciones en el servidor correspondiente para saber que todo va correctamente:

curl http://emvelksearchtest01:9200

curl http://emvelksearchtest02:9200

curl http://emvelksearchtest03:9200

## LOGSTASH

### Instalacion Logstash

Lo primero que se hará será importar la clave GPG de Elasticsearch. Para ello se ejecutará el siguiente comando de nuevo:

***rpm-import https://artifacts.elastic.co/GPG-KEY-elasticsearch***

Ahora hay que configurar el fichero ***/etc/hosts*** donde hay que poner la IP y el hostname de las máquinas que van a pertenecer a este elastic. Esto se tendrá que hacer en cada los servidores que vaya a pertenecer a elastic siendo el fichero igual en todos.

Igual que se hizo en los servidores de Elasticsearch, deberá crearse el repositorio en la ruta: ***/etc/yum.repos.d/logstash.repo*** donde hay que poner:

Texto

Descripción generada automáticamente

Ilustración 6 : Repositorio Logstash

A continuación, se debe instalar ***yum install java-openjdk -y*** en los servidores de logstash y después se ejecutará ***yum install logstash -y.***

Una vez hecho esto, con el comando ***yum list logstash*** se pueden ver los paquetes instalados junto a la versión.

Imagen que contiene Texto

Descripción generada automáticamente

Ilustración 7 : Instalación Logstash

### Configuración Logstash

Primero se creará una copia de seguridad del fichero de configuración en los servidores de logstash de la siguiente forma:

***cp -p /etc/logstash/logstash-sample.conf /etc/logstash/conf.d/logstash.conf***

Y ahora en el fichero ***conf.d/logstash.conf*** se incluye:

Texto

Descripción generada automáticamente

Ilustración 8 : Configuración Logstash

### Iniciar servicio

Estos comandos se tendrán que ejecutar en los servidores de logstash:

1. systemctl daemon-reload

2. systemctl start logstash

3. systemctl enable logstash

4. systemctl status logstash

Deberá dar una salida como:

Texto

Descripción generada automáticamente

Ilustración 9 : Estado Logstash

## KIBANA

### Instalación Kibana

Lo primero que se hará será importar la clave GPG de Elasticsearch como en los servidores anteriores. Se lanzará el siguiente comando:

***rpm-import*** [***https://artifacts.elastic.co/GPG-KEY-elasticsearch***](https://artifacts.elastic.co/GPG-KEY-elasticsearch)

Se continua igual que en los servidores de Elasticsearch y Logstash configurando el fichero ***/etc/hosts*** donde se añadirá la ip y el hostname de todas las máquinas que van a pertenecer a este Elastic.

Después habrá también que crear el repositorio en la ruta: ***/etc/yum.repos.d/******kibana.repo***que será como los anteriores:

Texto

Descripción generada automáticamente

Ilustración 10 : Repositorio Kibana

La diferencia es que en estos servidores de Kibana no será necesario el paquete **yum install java-openjdk** .

Directamente se ejecutará **yum install kibana -y** en los tres servidores. Una vez hecho con el comando **yum list kibana** se podrán ver los paquetes instalados junto a la versión.

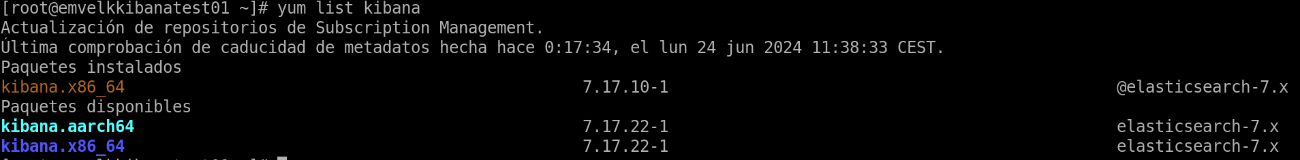


Ilustración 11 : Instalación Kibana

### Configuración Kibana

Para la configuración se buscará el fichero de configuración que está en ***/etc/kibana/kibana.yml***

Y la configuración quedará de esta forma:

Texto

Descripción generada automáticamente con confianza media

Ilustración 12 : Configuración Kibana

### Iniciar servicio

Estos comandos se tendrán que ejecutar en el servidor de Kibana:

1. systemctl daemon-reload

2. systemctl enable kibana

3. systemctl start kibana

## CONFIGURACIÓN INTERFAZ

Lo primero que se debe hacer es generar un CA en el servidor emvelksearchtest01.

Para ello se ejecuta en ese mismo servidor:

***/usr/share/elasticsearch/bin/elasticsearch-certutil ca***

Esta ejecución solicitará insertar una contraseña.

Después de esto, es ese mismo servidor se ejecutará:

**/usr/share/elasticsearch/bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12**

Cuando muestre “Enter password for CA (elastic-stack-ca.p12)” se deberá insertar la contraseña que se puso en el paso anterior.

Por último, pide una segunda contraseña que se debe facilitar.

Después hay que copiar el fichero donde se ha guardado la CA a la ruta ***/etc/elasticsearch*** con el siguiente comando:

**cp -p /usr/share/elasticsearch/elastic-certificates.p12 /etc/elasticsearch**

Una vez hecho esto se tiene que dar permisos al fichero:

**chmod 660 /etc/elasticsearch/elastic-certificates.p12**

Con el permiso 660 se logra que el usuario propietario pueda leer y escribir, pero no ejecutar (primer 6), los miembros del grupo propietario pueden leer y escribir, pero no ejecutar (segundo 6) y otros usuarios no tienen ningún permiso sobre el archivo (el último 0).

También se debe indicar que el propietario del fichero es elasticserch:

**chown root:elasticsearch /etc/elasticsearch/elastic-certificates.p12**

Con esto se señala que “root” es el propietario y “elasticsearch” es el grupo propietario del archivo.

En el fichero de configuración situado en la ruta ***/etc/elasticsearch/ elasticsearch.yml*** de los tres servidores de Elasticsearch se deben añadir las siguientes líneas:

xpack.security.enabled: true

xpack.security.transport.ssl.enabled: true

xpack.security.transport.ssl.verification\_mode: certificate

xpack.security.transport.ssl.keystore.path: elastic-certificates.p12

xpack.security.transport.ssl.truststore.path: elastic-certificates.p12

Texto

Descripción generada automáticamente

Ilustración 13 : Configuración Elasticsearch 3

Para que todo funcione correctamente habrá que copiar el certificado y el keystore a los otros 2 servidores de Elasticsearch con esa misma configuración, se hará con un scp:

**scp/etc/elasticsearch/elasticsearch.keystore emvelksearchtest02:/etc/elasticsearch/**

**scp /etc/elasticsearch/elastic-certificates.p12 emvelksearchtest02:/etc/elasticsearch/**

Lo mismo se haría con emvelksearchtest03.

Al reiniciar los servidores de Elasticsearch podría dar fallo el SSL para evitarlo se ejecutará lo siguiente:

**/usr/share/elasticsearch/bin/elasticsearch-keystore add xpack.security.transport.ssl.keystore.secure\_password**

**/usr/share/elasticsearch/bin/elasticsearch-keystore add xpack.security.transport.ssl.truststore.secure\_password**

Después de esto se reinicia el servidor de Kibana:

systemctl restart kibana

systemctl restart elasticsearch.service

Ahora en el servidor emvelksearchtest01 se debe poner la contraseña de inicio de sesión con:

**/usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive**

Para terminar, en el servidor de Kibana para establecer la contraseña puesta se añadirá en el fichero de configuración en la ruta ***/etc/kibana/kibana.yml***:

elasticsearch.username: "user"

elasticsearch.password: "password"

Finalmente, ya hay acceso a la interfaz de Kibana:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 14 : Página inicio de sesión Kibana

Tras meter las credenciales previamente añadidas se podrá ver la página principal de Kibana.

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

Ilustración 15 : Página principal Kibana

## ELASTIC MAPS

Elastic Maps es una herramienta integrada en Kibana que analiza datos geoespaciales. Permite visualizar múltiples índices como capas únicas en una sola vista para analizar los datos. En este caso se utiliza para visualizar los datos de inicio de sesión en el correo electrónico según la zona geográfica en la Comunidad de Madrid [9].

Para poder utilizar esta herramienta es necesario crear un índice en Elasticsearch que contenga datos geoespaciales.

Texto

Descripción generada automáticamente

Ilustración 16 : Creación índice punto geométrico

Este índice “índice\_maps” se crea de tipo “geo\_point” para poder almacenar datos con latitud y longitud de la siguiente manera:

Texto

Descripción generada automáticamente

Ilustración 17 : Añadir datos en índice

Se introduce con un POST en el índice “índice\_maps” creado anteriormente, el campo “location” con una latitud y longitud y se asocia a un nombre.

Los datos geográficos necesitan principalmente la latitud y longitud, pero cada punto puede contener métricas, marca de tiempo…

Elasticsearch permite todo tipo de datos de ubicación, desde puntos geográficos hasta formas geométricas como polígonos, en este caso se verá el uso de ambos.

Para crear un índice en el que insertar posteriormente formas geométricas tiene que ser de esta forma:

Texto

Descripción generada automáticamente

Ilustración 18 : Creación índice forma geométrica

Para un índice con puntos geográficos se utiliza “geo\_point”, sin embargo, para las formas geométricas se utiliza “geo\_shape”.

En el caso de este índice “polígono\_cmadrid” necesitará que se ingeste un campo que espera texto como “zone” y un campo que espera coordenadas para crear polígonos como es “geometry”.

Además, existe un servicio de mapa de Elastic en el que vienen mapas base provistos con formas de vectores detalladas. También se verá esto más adelante en el punto 4.4 y se explicará la diferencia entre utilizar esto o hacerlo en forma de polígonos.