Instalando ElasticSearch + Kibana en local con Docker

Introducción

Al final con la aparecion de Laravel Herd y por las cosas que hago, preferia desmantelar en mis proyectos que no necesitan **Laravel sail** por ser modernos y actualizados. En cuanto a Elastic Stack preferi hacerlo via docker dado su caracter de uso puramente para testing., al menos de moemtno, en vez de optar. por una instalación local 100%.

Asi que te dejo como lo hice en mi mac silicon.

Instalación

Elastic search single node

Oficial

Crear un red para elastic

```
❯ docker network create elastic
```

Bajarse la imagen

```
❯ docker pull docker.elastic.co/elasticsearch/elasticsearch:8.11.2
8.11.2: Pulling from elasticsearch/elasticsearch
Digest: sha256:e40b9d3d523f2fe4dc851ad2cc5570f28a58ca6c4efb566cc9688dcaf0df8dec
Status: Image is up to date for docker.elastic.co/elasticsearch/elasticsearch:8.11.2
docker.elastic.co/elasticsearch/elasticsearch:8.11.2
```

Verificar la imagen

Se requiere tener instalado en tu entorno Cosign si quieres verificar la imagen.

- Primero bajarse la firma de la imagen

```
❯ wget https://artifacts.elastic.co/cosign.pub
--2023-12-10 09:17:56--  https://artifacts.elastic.co/cosign.pub
Resolviendo artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130
Conectando con artifacts.elastic.co (artifacts.elastic.co)[34.120.127.130]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 178 [application/x-mspublisher]
Grabando a: «cosign.pub»

cosign.pub
100%[=======================================================================================
=================================================>]     178  --.-KB/s    en 0s

2023-12-10 09:17:57 (28,3 MB/s) - «cosign.pub» guardado [178/178]
```

- Después verificarla

```
❯ cosign verify --key cosign.pub docker.elastic.co/elasticsearch/elasticsearch:8.11.2

Verification for docker.elastic.co/elasticsearch/elasticsearch:8.11.2 --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - Existence of the claims in the transparency log was verified offline
  - The signatures were verified against the specified public key
```

Instalar elasticsearch container

Esta es una variante del manual. El motivo es claro. Es crear dos volumenes:

- Uno con el directorio donde se guardan los indices.
- Otro donde se guarda la configuración.

> Si tenias una isntalación antigua tipo, o una instalación con volumenes diferentes, puede que tengas que empezar de o eliminándolos.

```
❯ docker run --name es01 --net elastic -p 9200:9200 -v es01-data:/usr/share/elasticsearch/data
-v es01-config:/usr/share/elasticsearch/config -it -m 1GB
docker.elastic.co/elasticsearch/elasticsearch:8.11.2
...
 Elasticsearch security features have been automatically configured!
 Authentication is enabled and cluster connections are encrypted.

  Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):
  w78bj=MMasWeb6S1mnZR

  HTTP CA certificate SHA-256 fingerprint:
  464224b5bc542f16b37d86d9038633bfe0a9a01acaab7fe7fe78ff6e838f60dc

  Configure Kibana to use this cluster:
• Run Kibana and click the configuration link in the terminal when Kibana starts.
• Copy the following enrollment token and paste it into Kibana in your browser (valid for the
next 30 minutes):

eyJ2ZXIiOiI4LjExLjIiLCJhZHIiOlsiMTcyLjI3LjAuMjo5MjAwIl0sImZnciI6IjQ2NDIyNGI1YmM1NDJmMTZiMzdkOD
ZkOTAzODYzM2JmZTBhOWEwMWFjYWFiN2ZlN2ZlNzhmZjZlODM4ZjYwZGMiLCJrZXkiOiIxaXpkVW93QjJlZDFvZmRMRTBC
UTo2ZWVtYmJLZ1FkT1U4N1YyN0pkQnpBIn0=

 Configure other nodes to join this cluster:
• Copy the following enrollment token and start new Elasticsearch nodes with
`bin/elasticsearch --enrollment-token <token>` (valid for the next 30 minutes):

eyJ2ZXIiOiI4LjExLjIiLCJhZHIiOlsiMTcyLjI3LjAuMjo5MjAwIl0sImZnciI6IjQ2NDIyNGI1YmM1NDJmMTZiMzdkOD
ZkOTAzODYzM2JmZTBhOWEwMWFjYWFiN2ZlN2ZlNzhmZjZlODM4ZjYwZGMiLCJrZXkiOiIyQ3pkVW93QjJlZDFvZmRMRTBC
Zzp4ZlNfc3R5QlRtYVFzUVZBbFBGcE13In0=

  If you're running in Docker, copy the enrollment token and run:
  `docker run -e "ENROLLMENT_TOKEN=<token>"
docker.elastic.co/elasticsearch/elasticsearch:8.11.2`
```

Instalar kibana

Bajar la imagen

```
docker run --name kib01 --net elastic -p 5601:5601 -v kib01-config:/usr/share/kibana/config
docker.elastic.co/kibana/kibana:8.11.2
...

[2023-12-10T08:37:49.859+00:00][INFO ][root] Holding setup until preboot stage is completed.



i Kibana has not been configured.

Go to http://0.0.0.0:5601/?code=812523 to get started.
```

Acudiremos al navegador con la url mostrada, y alli usaremos el **enrollment token** para terminar la configuración.

Con eso ya tendremos configurado Kibana + Elasticsearch en docker.

Preparar las cosas para userse en nuestr app

Necesitamos el certificado de elastic

```
❯ export ELASTIC_PASSWORD="w78bj=MMasWeb6S1mnZR"
❯ docker cp es01:/usr/share/elasticsearch/config/certs/http_ca.crt
~/Sites/certificates/http_ca_local.crt
Successfully copied 3.58kB to /Users/abkrim/Sites/certificates/http_ca_local.crt
❯ export ELK_DOCKER_CA_BUNDLE="/Users/abkrim/Sites/certificates/http_ca_local.crt"
```

Yo lo hago así, guardar en una carpeta especial el certificado, porque uso un único docker para cada servicio del stack de Elasticsearch, para todos mis proyectos de desarrollo.

Prueba de concpeto

Una vez arriba ambos containers puedo probar elastic en el shell, y auq e asi sabre si luego la configuración de mis app de Laravel pasaran con lso datos que tengo.

> Uso dos variables de shell, evidentemente

```
❯ curl --cacert $ELK_DOCKER_CA_BUNDLE -u elastic:$ELASTIC_PASSWORD https://localhost:9200


{
  "name" : "9618d13f0939",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "-wSu0Nm-QviovkB3rW6f5w",
  "version" : {
    "number" : "8.11.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "76013fa76dcbf144c886990c6290715f5dc2ae20",
    "build_date" : "2023-12-05T10:03:47.729926671Z",
    "build_snapshot" : false,
    "lucene_version" : "9.8.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Con eso ya tengo verificación de os datos que necesita mi app para funcionar en local con mis dockers del stack de elasticsearch.

Upgrade

En caso de trabajar sin `docker compose` Ver Arranque, Actualización, y cosas de Elastic con Docker

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #3
Created 2023-12-10 09:08:51 UTC by Abkrim
Updated 2024-12-22 07:09:04 UTC by Abkrim