Copia de seguridad y restauración de Elastic Search

Volver al Índice de Documentación Pandora FMS

Copia de seguridad y restauración de ElasticSearch (ELK)

La migración de datos de un servidor ElasticSearch mediante Snapshots se realiza con relativa rapidez. En primer lugar, se realiza una copia de seguridad de los datos del servidor y después se guarda en un repositorio para posterior restauración del mismo.

Copia de Seguridad

La máquina donde se realizará el backup la denominaremos como “máquina origen” y la máquina donde se realizará la restauración se denominará “máquina destino”.

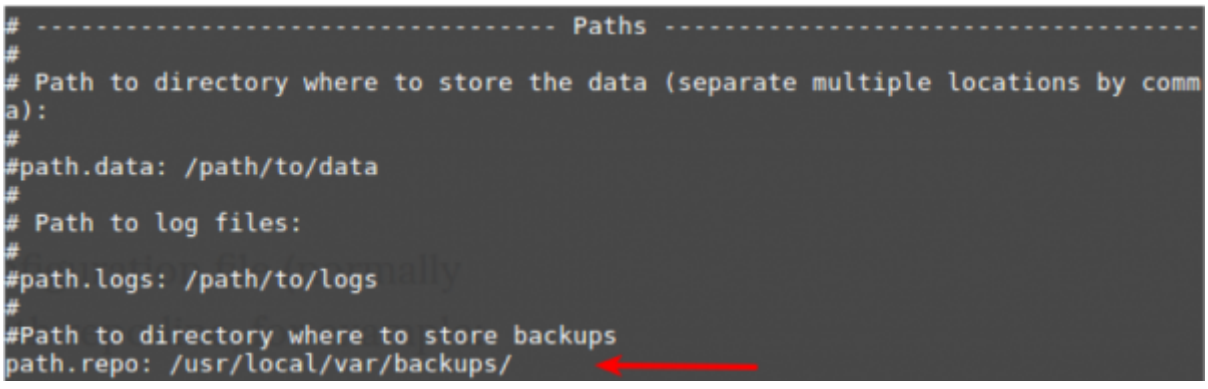
- **En la máquina origen**

1) Modificamos el fichero de configuración de “elasticsearch.yml”:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Y añadimos la siguiente línea:

```
path.repo: /usr/local/var/backups/
```



2) Creamos el directorio añadido anteriormente al fichero de configuración:

```
mkdir -p /usr/local/var/backups/
```

3) Damos permisos de lectura y escritura al directorio y usuario:

```
 chmod 700 /usr/local/var/backups
```

```
chown elasticsearch:elasticsearch /usr/local/var/backups
```

4) Reiniciamos el servicio:

```
/etc/init.d/elasticsearch restart
```

5) Creamos el backup con el siguiente comando:

```
curl -XPUT http://localhost:9200/_snapshot/my_backup -d '{"type": "fs",
"settings": {"compress": "true", "location": "/usr/local/var/backups/"}}}'
```

6) Comprimimos el backup generado anteriormente:

```
cd /usr/local/var/
tar -zcvf elastic_backup.tar.gz backups/
```

7) Desde la máquina destino donde vamos a hacer la restauración, copiamos el backup comprimido de la máquina origen.

- En la máquina destino **scp -P 41122 root@<ipOrigen>:/root/elastic_backup.tar.gz /home/user/backup**

Para utilizar el comando 'scp' se debe tener instalado un servidor ssh en la máquina origen y al menos un cliente ssh en la máquina destino.

Es importante que la versión de ElasticSearch en la máquina importadora sea compatible con la exportación de datos; es decir, en este caso su máquina local debe tener la misma versión o superior. Si no es así, primero debe actualizar ElasticSearch.

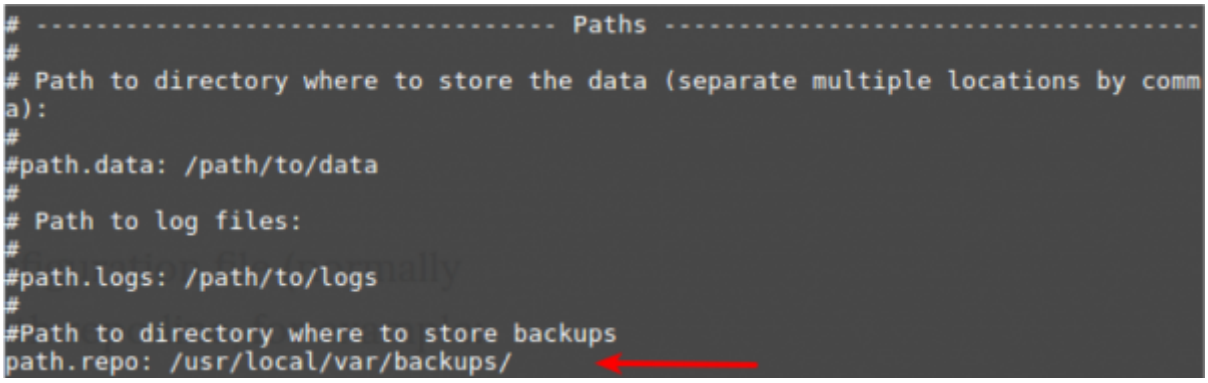
==== Restaurar Copia de Seguridad ==== * En la máquina destino**

1) Modificamos el fichero de configuración de "elasticsearch.yml" de la misma manera que hicimos al crear el backup en la primera máquina:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Y añadimos la siguiente línea:

```
path.repo: /usr/local/var/backups/
```



2) Creamos el directorio añadido anteriormente al fichero de configuración:

```
mkdir -p /usr/local/var/backups/
```

3) Damos permisos de lectura y escritura al directorio:

```
 chmod 700 /usr/local/var/backups
 chown elasticsearch:elasticsearch /usr/local/var/backups
```

4) Reiniciamos el servicio:

```
/etc/init.d/elasticsearch restart
```

5) Descomprimimos el backup que importamos desde la máquina origen:

```
tar -xzvf /home/user/backup/elastic_backup.tar.gz -C /usr/local/var/backups
```

6) Creamos los repositorios donde se localizan las snapshots:

```
curl -X PUT "localhost:9200/_snapshot/my_backup" -H 'Content-Type:
application/json' -d'

{
  "type": "fs",
  "settings": {
    "location": "/usr/local/var/backups"
  }
}
'
```

7) Cerramos los índices:

```
curl -XPOST http://localhost:9200/<nombreIndices>-*/_close
```

El asterisco muestra todos los índices que empiecen por ese nombre.

8) Importamos el backup:

Primero copiamos el backup al repositorio:

```
cp <nombre del snapshot.dat> my_backup_location/
```

Renombramos el fichero sin mayúsculas:

```
mv my_backup_location/<nombre del snapshot.dat> my_backup_location/snap1
```

Finalmente se importa:

```
curl -X POST
"localhost:9200/_snapshot/my_backup/snap1/_restore?wait_for_completion=true"
```

9) Para terminar, reabrimos los índices:

```
curl -XPOST http://localhost:9200/<nombreIndices>-*/_open
```

Volver al Índice de Documentación Pandora FMS