

3.5 CONFIGURACIÓN BÁSICA INICIAL

Una vez han sido instalados los servicios de **Elasticsearch** y **Kibana**, procederemos a realizar las primeras modificaciones sobre los archivos de configuración de los mismos, realizando algunos cambios como el bloqueo de la memoria para el servicio, deshabilitar la *SWAP* en el sistema operativo y publicar ambos servicios fuera de la interfaz interna de Localhost.

Elasticsearch

Principales rutas de Elasticsearch

```
home:      /usr/share/elasticsearch
bin:       /usr/share/elasticsearch/bin
conf:      /etc/elasticsearch
env:       /etc/default/elasticsearch
data:      /var/lib/elasticsearch
logs:      /var/log/elasticsearch
plugins:   /usr/share/elasticsearch/plugins
```

Configuración de la memoria RAM para el servicio

Será necesario realizar modificaciones en tres archivos:

- En `/etc/elasticsearch/elasticsearch.yml`, descomentar la siguiente línea:

```
bootstrap.memory_lock: true
```

- En `/etc/default/elasticsearch`, descomentar la siguiente línea:

```
MAX_LOCKED_MEMORY=unlimited
```

- En `/etc/security/limits.conf`, añadir:

```
# allow user 'elasticsearch' mlockall
elasticsearch soft memlock unlimited
elasticsearch hard memlock unlimited
```

- En `/usr/lib/systemd/system/elasticsearch.service`, descomentar la siguiente línea:

```
LimitMEMLOCK=infinity
```

Para que el cambio realizado en este último paso tome efecto será necesario reiniciar el demonio:

```
systemctl daemon-reload
```

El último de los cambios a aplicar a la configuración de la memoria es deshabilitar el uso de memoria *SWAP* ya que puede afectar muy negativamente al rendimiento del clúster debido a que es mucho más lenta que la memoria RAM. Para ello será necesario comentar la línea de configuración de la SWAP en el archivo:

```
vi /etc/fstab
```

Configuración del servicio

A continuación se recoge un resumen de los parámetros a configurar en el servicio para que pertenezca el nodo a un clúster compuesto únicamente por él, cambiar el nombre del nodo dentro del servicio y publicarlo fuera de la interfaz interna.

```
cluster.name: elkudemy
node.name: ${HOSTNAME}
bootstrap.memory_lock: true
network.host: ["127.0.0.1", "192.168.1.31"]
```

NOTA: cuidado con el parámetro `network.host` cuya IP deberá ser la de la interfaz donde escuchará el servicio.

Para comprobar el estado del clúster se usará la siguiente consulta de la API desde la terminal, la cual ya se estudiará en módulos posteriores:

```
curl -XGET http://192.168.1.31:9200/_cluster/health?pretty
```

Kibana

Principales rutas de Kibana

```
home:      /usr/share/kibana
bin:       /usr/share/kibana/bin
conf:      /etc/kibana
data:      /var/lib/kibana
optimize:  /usr/share/kibana/optimize
logs:      /var/log/kibana
plugins:   /usr/share/kibana/plugins
```

Configuración de los parámetros de Kibana

A continuación se recoge un resumen de los parámetros a configurar en el servicio de Kibana para que se conecte al nodo de Elasticsearch, publique el servicio a la interfaz externa y escriba sus logs en el correspondiente directorio.

```
server.host: "192.168.1.31"  
elasticsearch.url: "http://192.168.1.31:9200"  
kibana.index: ".kibana"  
logging.dest: /var/log/kibana/kibana.log
```

Nota: Destacar que la ruta del `log` debe existir. En el caso contrario se debe crear dicho directorio con el comando:

```
mkdir /var/log/kibana
```

Y que tengan los permisos necesarios para el usuario kibana:

```
chown -R kibana:kibana /var/log/kibana
```