10.1 MACHINE LEARNING

La primera funcionalidad que se verá dentro de este módulo de X-pack será **Machine Learning** que nos ayudará a encontrar patrones de comportamiento habituales y una identificación de posibles anomalías dentro de dichos datos.

Descarga de los datos de prueba

Lo primero que se va a necesitar en este laboratorio para mostrar las funcionalidades de Machine Learning serán los datos de prueba, por lo que procedemos a descargarlos y descomprimirlos con los siguientes comandos:

```
mkdir -p Downloads/server_metrics
cd Downloads/server_metrics
wget https://download.elasticsearch.org/demos/machine_learning/gettingstarted/serv
er_metrics.tar.gz
tar -xvf server_metrics.tar.gz
```

Se puede modificar también la configuración de Kibana para que apunte a los tres nodos en vez de solo a uno.

Primer caso de uso

Aprovecharemos la API para la subida del template correspondiente a estos datos

```
curl -X PUT "192.168.1.31:9200/server-metrics" -H 'Content-Type: application/json'
 -d'
{
  "settings": {
    "number_of_shards":1,
    "number_of_replicas":0
  },
  "mappings": {
    "metric": {
      "properties":{
        "@timestamp": {
          "type":"date"
        },
        "accept": {
          "type":"long"
        },
        "deny": {
          "type":"long"
        },
        "host": {
          "type":"keyword"
        },
        "response": {
          "type":"float"
        },
        "service": {
          "type":"keyword"
        },
        "total": {
          "type":"long"
        }
      }
    }
  }
}
'
```

Será necesario modificar el script de subida `upload_server_metrics.sh` ya que no se tiene configurada ningún tipo de autenticación:

```
vi upload_server_metrics.sh
```

y ya si se podrá ejecutar este script que indexará todos los eventos:

```
sh upload_server_metrics.sh
```

Segundo caso de uso

De la misma forma que se realizó antes, lo primero será descargar los archivos que se van a indexar mediante los siguientes comandos:

```
mkdir user-activity
cd user-activity
wget https://download.elasticsearch.org/demos/machine_learning/gettingstarted/user
-activity.json
```

E indexarlo utilizando la API:

```
curl -s -X POST -H "Content-Type: application/json" 192.168.1.31:9200/user-activit
y/_bulk --data-binary "@user-activity.json"
```