ELK DOCUMENTACION

Instalacion elk

Prerequisitos

para instalar java(v-1.8):

Tendremos que instalar una version de java compatible

```
sudo apt-get install openjdk-8-jdk
```

para instalar nginx:

```
sudo apt-get install nginx
```

para descargar elasticsearch:

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.15.0-amd64.deb
```

para descargar kibana:

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-7.15.0-amd64.deb
```

para descargar logstash:

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.15.0-amd64.deb
```

SI queremos cambiar la version de logstash, kibana o elasticsearch, solo tendremos que cambiar los números de versión dentro de wget

```
Para la version 7.15(logstasg):
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.15.0-amd64.deb

Para la version 7.17(logstasg):
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.17.0-amd64.deb

Para la version 8.1.1(logstasg):
wget https://artifacts.elastic.co/downloads/logstash/logstash-8.1.1-amd64.deb
```

Una vez tengamos descargados los paquetes .deb tendremos que desempaquetar/instalar los paquetes

comando dpkg (instalar servicios) :

```
sudo dpkg -i elasticsearch-7.15.0-amd64.deb

sudo dpkg -i kibana-7.15.0-amd64.deb

sudo dpkg -i logstash-7.15.0-amd64.deb
```

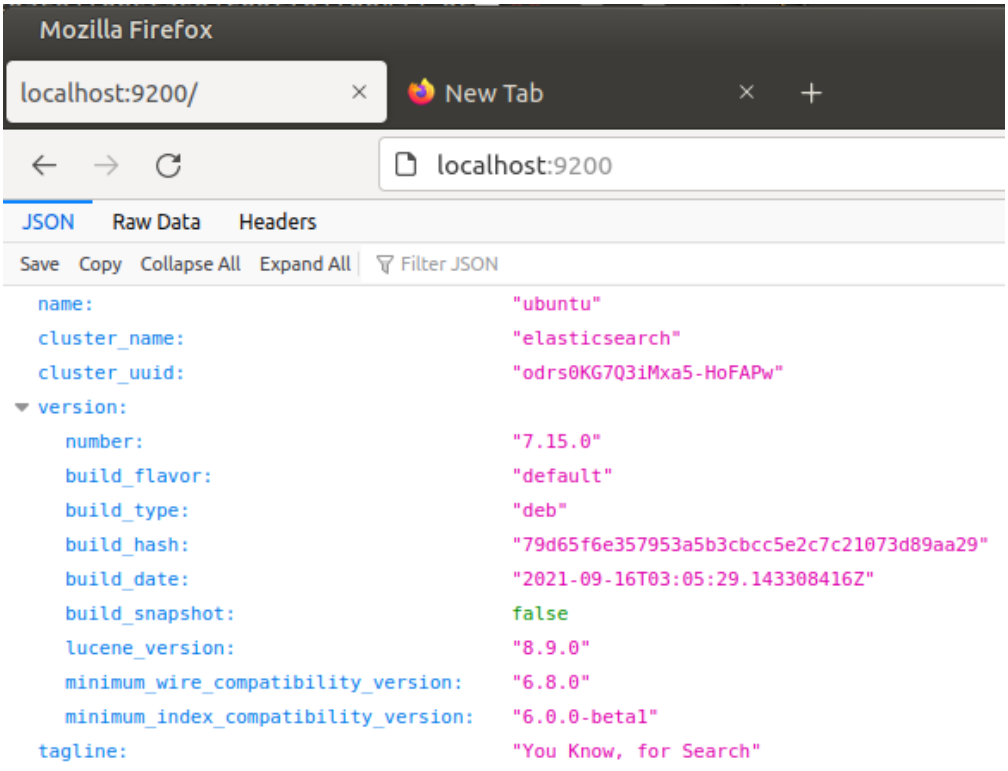
Comprobacion de Servicios

Una vez los tengamos instalados, comprobaremos el funcionamiento:

Elasticsearch

En un navegador se buscaria:

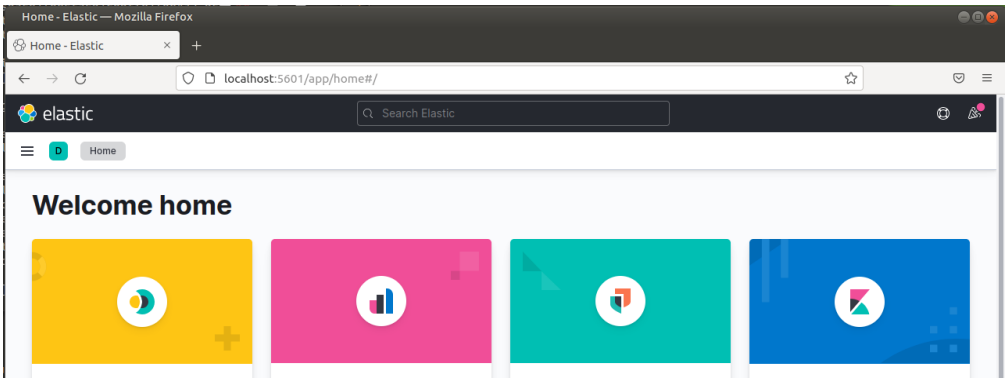
```
localhost:9200
```



Kibana

En un navegador se buscaria:

```
localhost:5601
```



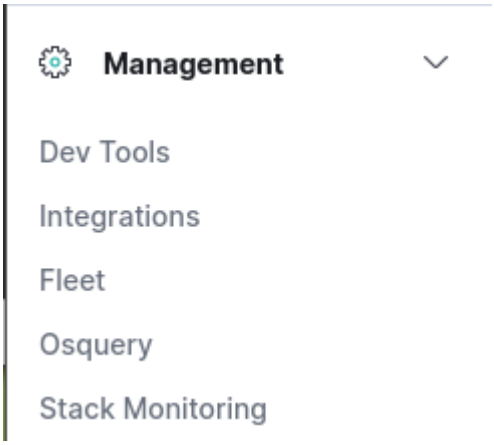
Logstash

En una terminal se ejecutaria:

```
sudo /usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout {} }'
```

Introduccion de Datos

Dentro de dev tools



Tendremos que crear la plantilla de index para el csv

```
POST /clientes/_doc
{
  "mappings": {
    "properties": {
      "usuario": { "type": "text" },
      "servicio": { "type": "text" },
      "permisos": { "type": "text" },
      "equipo": { "type": "text" }
    }
  }
}
```

La cual tendra el que llamarse **nombrefichero.csv**

```
POST /clientes/_doc
{
  "mappings": {
    "properties": {
      "usuario": { "type": "text" },
      "servicio": { "type": "text" },
      "permisos": { "type": "text" },
      "equipo": { "type": "text" }
    }
  }
}
```

una vez creada la platilla para el csv crearemos el **pipeline.conf** para introducir los datos con logstash**y que salga de la lectura del csv automaticamente cuando termine**

esto lo conseguiremos con los valores dentro input y file de:
mode ⇒ read
exit_after_read ⇒ true

```
input {
    file {
        path => "ruta al fichero de csv"
        start_position => beginning
        sincedb_path => "/dev/null"
        mode => read
        exit_after_read => true
        }
    }

filter {

        csv {
                columns => ["columnas creadas en la platilla del index"]
                }

        mutate {
                remove_field => ["columnas a eliminar"]
                }

        }

output {
        stdout { }

        elasticsearch {
                index => "nombre del index creado(clientes en este caso)"
                }
        }
```

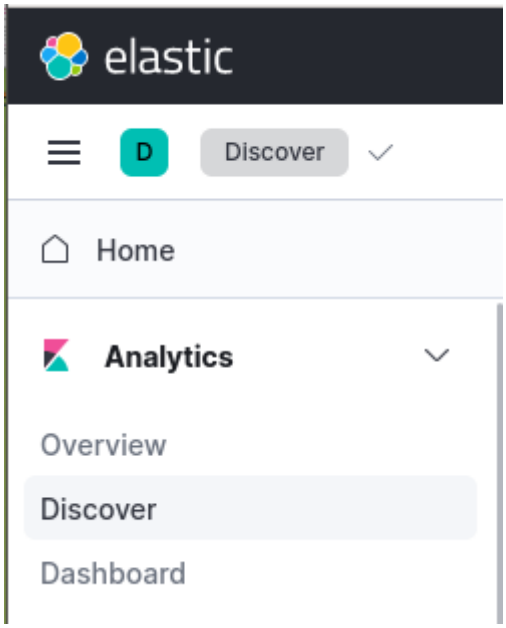
Estrucura del fichero csv:

(Dependiendo de las columnas puestas en nuestro index)

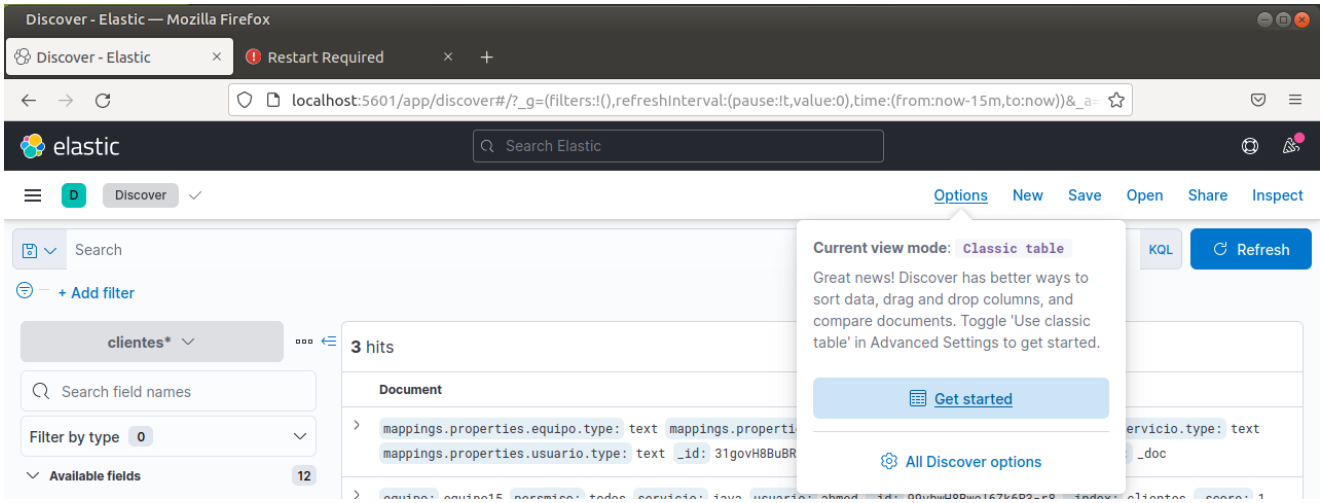
```
valor,valor,valor,valor
valor,valor,valor,valor

....etc....
```

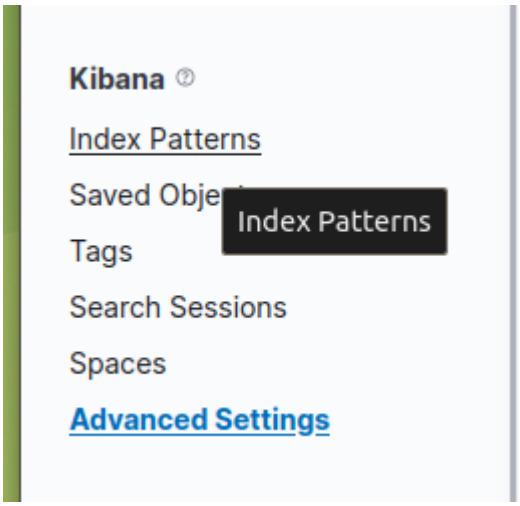
Nos iremos a discover



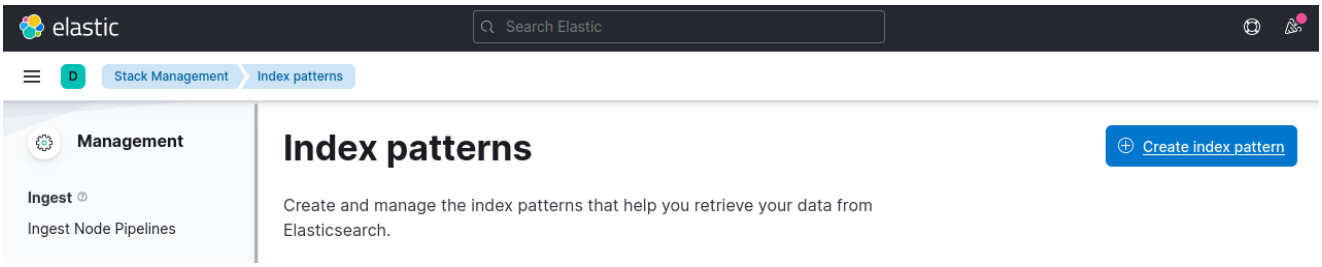
Options ⇒ All discover options



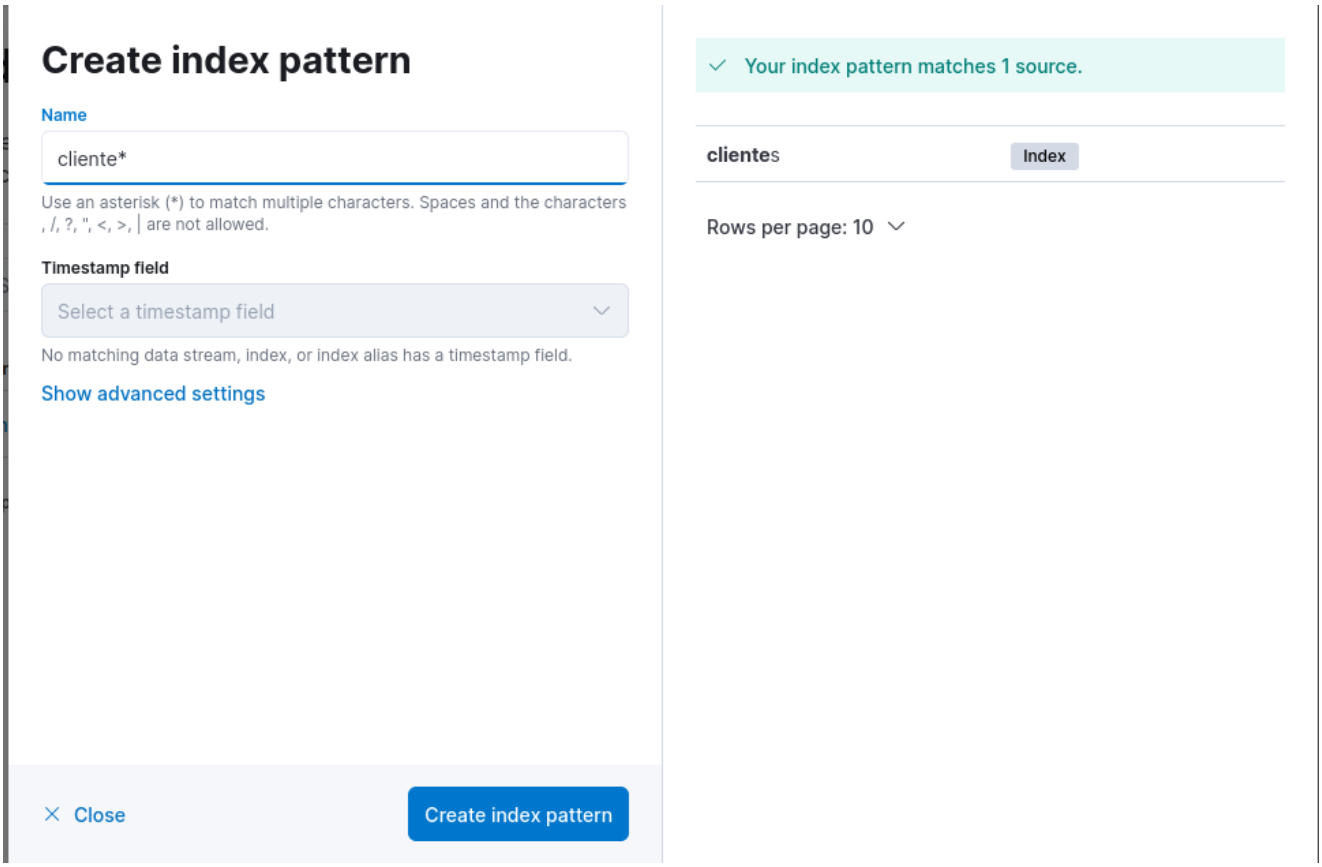
Magement ⇒ Kibana ⇒ Index Patterns



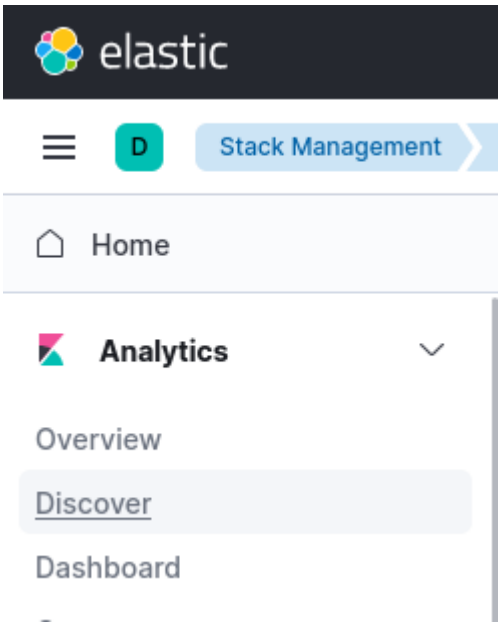
Create index pattern



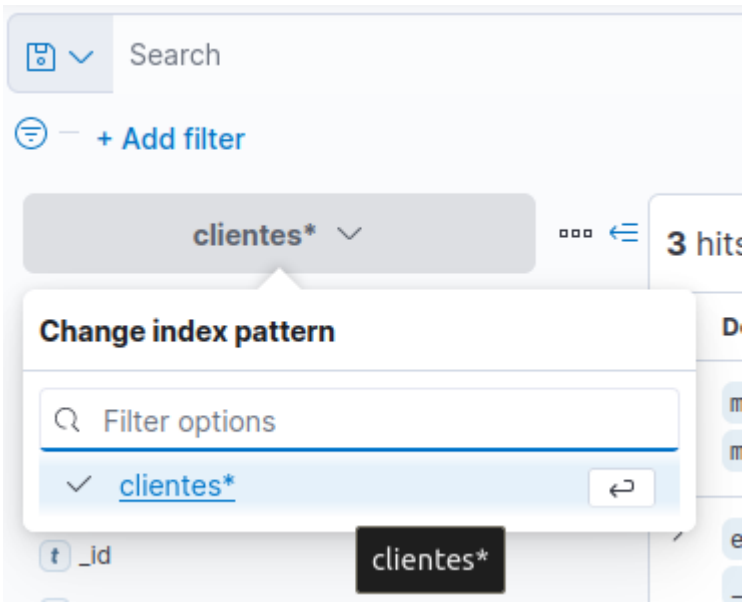
Y Crearemos el index pattern con el nombre que habiamos creado antes



Para ver el indice creado iremos a Analytics ⇒ Discover



Y aqui seleccionar el indice que hemos creado



Para introducir los datos del csv ejecutaremos

```
sudo /usr/share/logstash/bin/logstash -f "ruta fichero pipeline.conf"
```

Y nos saldran los datos introducidos por columnas

3 hits

	Document
›	mappings.properties.equipo.type: text mappings.properties.permisos.type: text mappings.properties.servicio.type: text mappings.properties.usuario.type: text _id: 31govH8BuBRNG_KaxmRa _index: clientes _score: 1 _type: _doc
›	equipo: equipo15 persmiso: todos servicio: java usuario: ahmed _id: 99vhwH8Bwel6Zk6P3-r8 _index: clientes _score: 1 _type: _doc
›	equipo: equipo10 persmiso: todos servicio: php usuario: samuel _id: -NvhwH8Bwel6Zk6P4Oqv _index: clientes _score: 1 _type: _doc