



Practica de Elastic 2021

Services & processes solutions de CV

---

## Contenido

1.1	Introducción .....	1
1.2	Practica.....	1
1.2.1	Aprovisionamiento de ELK.....	1
1.2.2	Creación de un índice -- Tiempo 2 horas.....	4
1.2.3	Realizar búsquedas sobre el índice -- Tiempo 2 horas .....	7
1.2.4	Realizar un tablero para visualizar información de empleados .....	10

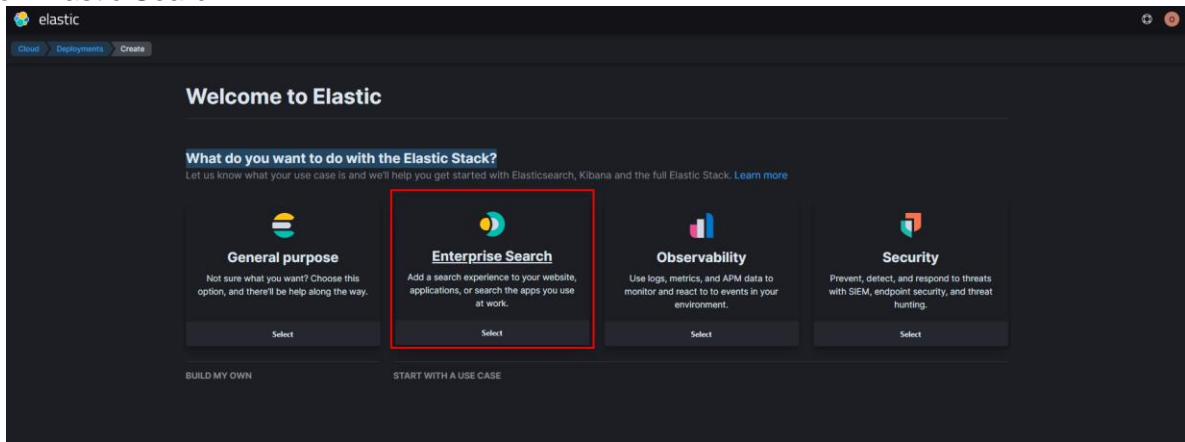
## 1.1 Introducción

Esta práctica tiene como objetivo identificar las habilidades de autoaprendizaje y resolución de problemas, a través de la exploración de una tecnología relativamente nueva llamada “**Elasticsearch**”.

## 1.2 Practica

### 1.2.1 Aprovisionamiento de ELK

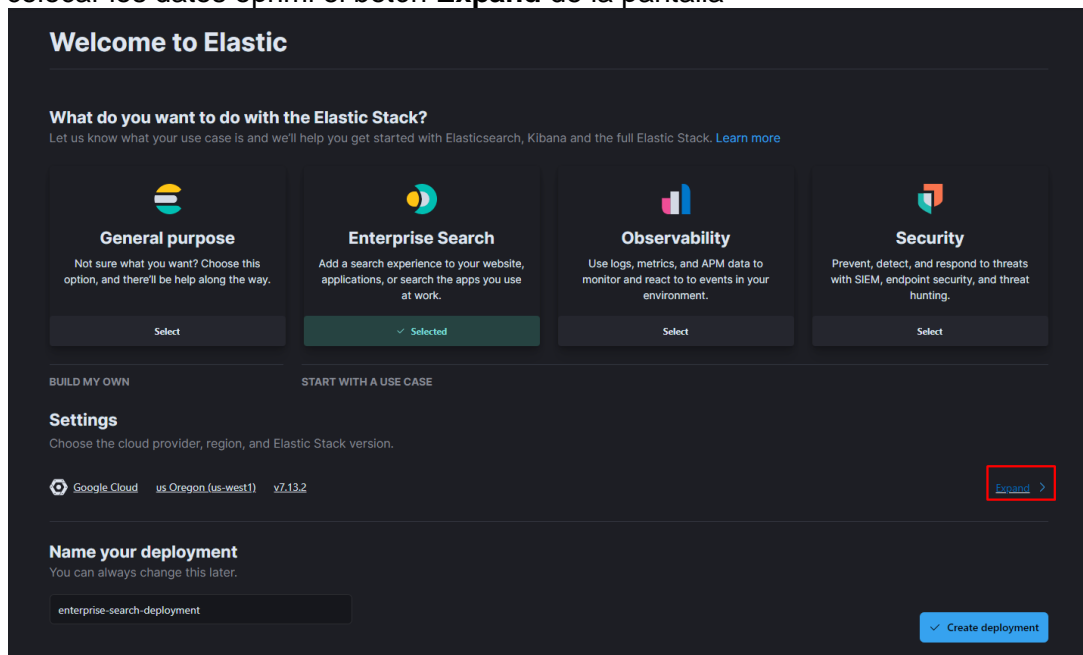
Lo primero hice es crear una cuenta en Elastic como versión de prueba, después elegí que es lo que quiero hacer con Elastic Search



Después coloco los datos propuestos en el documento **Práctica de Elastic 2021.pdf**, los cuales son:

- Nombre del deployment: sps\_practica
- Plataforma: Amazon Web Service
- Region: US East (N. Virginia)
- Elastic Stack version: Mas reciente
- Optimize your deployment: I/O Optimized

Para poder colocar los datos oprimi el botón **Expand** de la pantalla



Una vez colocados los datos queda de la siguiente manera, en mi caso no encontré esta opción **Optimize your deployment: I/O Optimized**, seleccione el boton **Create deployment**.

The screenshot shows the 'Settings' page in the Elastic Cloud console. Under the 'Cloud provider' section, 'Amazon Web Services' is selected. The 'Region' is set to 'us N. Virginia (us-east-1)' and the 'Version' is '7.13.2'. In the 'Name your deployment' section, the name 'sps\_practica' is entered. A red box highlights the 'Create deployment' button.

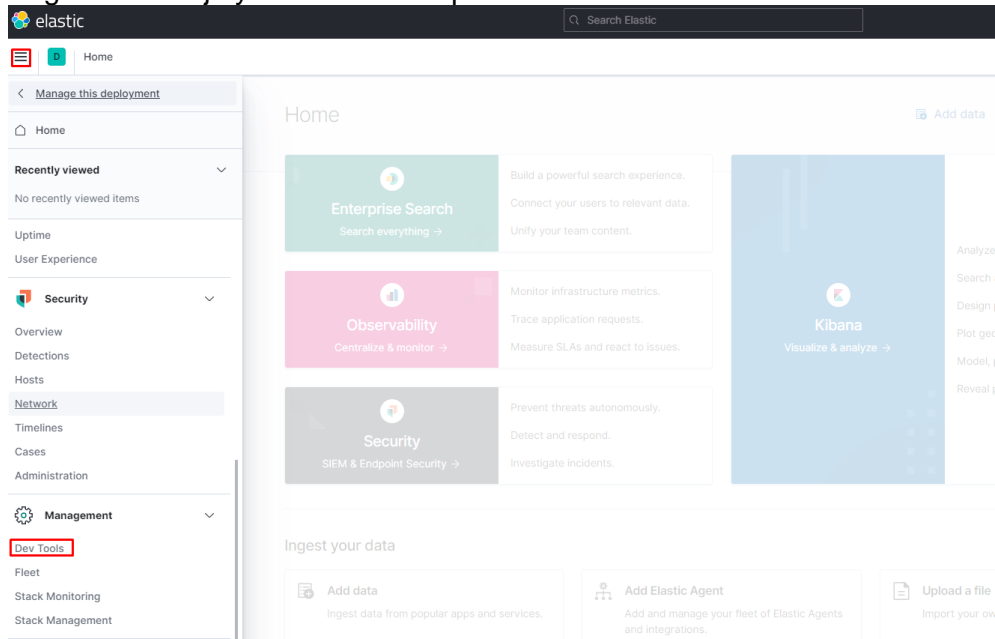
Esto tardara un poco para crear el despliegue. Descargue las credenciales para su almacenamiento.

The screenshot shows a modal dialog box titled 'Save your elastic deployment credentials. They are shown only once.' It displays the 'Username' as 'elastic' and the 'Password' as 'Elastic-Cloud-User:AWS-Access-Key-ID:Secret-Key'. A red box highlights the 'Download' button. There is also a 'Continue without downloading' link at the bottom.

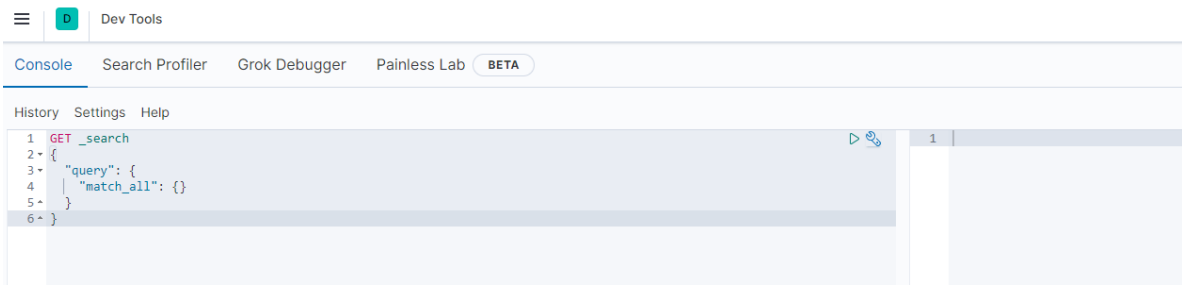
Una vez que termina esto seleccione la opción **Open Kibana**.

The screenshot shows the 'Deployments' page in the Elastic Cloud console. The deployment 'sps\_practica' is listed with a status of 'Healthy'. A red box highlights the 'Open Kibana' button. The page also includes a 'Get started with your deployment' section with a link to 'Open Enterprise Search'.

Me abrió la siguiente pantalla en la cual seleccione el menú icono de las 3 líneas en la parte superior izquierda y me dirigi hasta abajo y seleccione la opción de **Dev Tools**.



En la pantalla visualice lo siguiente



Dado que es una herramienta que nunca he utilizado me puse a investigar en la documentación para saber cómo realizar:

- Creación de un índice
- Borrar un índice, ya que me equivoqué y lo hice mal.
- Insertar datos a un índice

El siguiente link es la documentación o los pasos a seguir para crear, borrar, insertar datos en un index <https://www.elastic.co/guide/en/elasticsearch/reference/current/indices.html>  
Encontre algo, decía que Elasticsearch tiene una terminología que hace referencia a una base de datos.

MySQL (RDBMS) Terminology	ElasticSearch Terminology
Database	Index
Table	Type
Row	Document

A como lo entendí es que para base de datos el termino base de datos es lo mismo que index en ElasticSearch, tabla es un type y Row es un Document, por lo que entiendo un registro en ElasticSearch es un document.

Por lo que entiendo ElasticSearch funciona como una base de datos documental.

## 1.2.2 Creación de un índice -- Tiempo 2 horas

### 1.2.2.1 Selecciona tu consola de Dev Tools para realizar la siguiente actividad

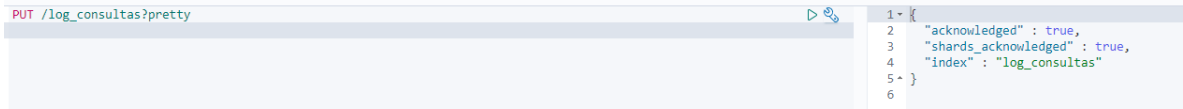
Hice la creación del índice con el nombre de **log\_consultas**

PUT /log\_consultas?pretty

**PUT** significa que se va a crear un índice.

**Log\_consultas** será el nombre del índice

**Pretty** es para que en la respuesta nos la regrese entendible o en un formato bonito.



```
PUT /log_consultas?pretty
{
  "acknowledged": true,
  "shards_acknowledged": true,
  "index": "log_consultas"
}
```

### 1.2.2.2 Selecciona tu consola de Dev Tools para realizar la siguiente actividad

Para realizar la inserción de los datos lo realice con la siguiente instrucción

POST /log\_consultas/\_doc?pretty

```
{
  "@timestamp": "2010-05-15T22:00:54",
  "estado_consulta": "consumo",
  "servicio": "consulta",
  "administrador": "Juan Carlos",
  "consultas_realizadas": 52
}
```

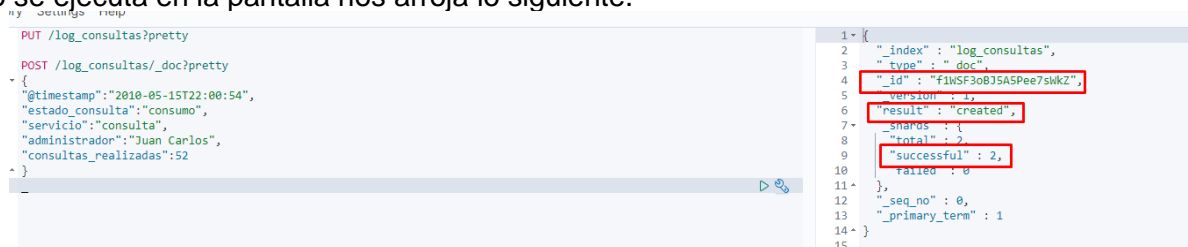
**POST** es para enviar la información que se requiere

**Log\_consultas** será el nombre del índice

**\_doc** es para indicar que insertaremos un documento

**Pretty** es para que en la respuesta nos la regrese entendible o en un formato bonito.

Cuando se ejecuta en la pantalla nos arroja lo siguiente.



```
POST /log_consultas/_doc?pretty
{
  "@timestamp": "2010-05-15T22:00:54",
  "estado_consulta": "consumo",
  "servicio": "consulta",
  "administrador": "Juan Carlos",
  "consultas_realizadas": 52
}
{
  "_index": "log_consultas",
  "_type": "doc",
  "_id": "f1wSF3oBJSASPe7smkZ",
  "_version": 1,
  "result": "created",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 0,
  "_primary_term": 1
}
```

La creación del documento fue exitosa.

Después se obtiene el mapping que se realizo con el documento que se creo con el siguiente comando.

GET log\_consultas

**GET** nos devolverá la información sobre el índice.

**Log\_consultas** será el nombre del índice

Esto es lo que arroja el **GET**

```
{
  "log_consultas" : {
    "aliases" : { },
    "mappings" : {
      "properties" : {
        "@timestamp" : {
          "type" : "date"
        },
        "administrador" : {
          "type" : "text",
          "fields" : {
            "keyword" : {

```

```

        "type" : "keyword",
        "ignore_above" : 256
      }
    },
    "consultas_realizadas" : {
      "type" : "long"
    },
    "estado_consulta" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "servicio" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    }
  },
  "settings" : {
    "index" : {
      "routing" : {
        "allocation" : {
          "include" : {
            "_tier_preference" : "data_content"
          }
        }
      }
    },
    "number_of_shards" : "1",
    "provided_name" : "log_consultas",
    "creation_date" : "1623892766275",
    "number_of_replicas" : "1",
    "uuid" : "koOO0s3VRNa0_1LUU2HNvw",
    "version" : {
      "created" : "7130299"
    }
  }
}

```

Este GET entre tantas cosas nos arroja el tipo de dato que tiene cada atributo del documento

**1.2.2.3      Obtén el mapping del índice anterior y genera un template a partir de este índice haciendo uso del API de plantillas (TEMPLATE). El patrón para el índice debe ser: “log\_consultas\*”. Verifica los tipos de datos hagan sentido con la información almacenada**

Este paso no lo pude hacer

**1.2.2.4      Una vez definido tu template cargaras una serie de documentos en tu índice utilizando el archivo que se encuentra en el escritorio: log\_consultas.json . Para esto utiliza el API (BULK)**

Se cargaron uno por uno los registros que estaban en el JSON haciendo un total de 299 con la siguiente instrucción.

**PUT** significa que se va a crear un índice.

**Log\_consultas** será el nombre del índice

**\_doc** es para indicar que insertaremos un documento

**299** en este caso es el index del ultimo registro que se inserto

**Pretty** es para que en la respuesta nos la regrese entendible o en un formato bonito.

PUT /log\_consultas/\_doc/299?pretty

```
{
  "@timestamp": "2010-05-15T18:36:26",
  "estado_consulta": "informativo",
  "servicio": "borrado",
  "administrador": "Juan Carlos",
  "consultas_realizadas": 74
}
```



## 1.2.3 Realizar búsquedas sobre el índice -- Tiempo 2 horas

### 1.2.3.1 Obtener el número de registros con estado consulta igual a error y consumo.

Con la ayuda de la siguiente consulta nos trajo los registros con **estado\_consulta** igual a error y consume GET /log\_consultas/\_search?pretty=true&q=estado\_consulta:error||consumo  
Habiendo un total de 182 registros

```
1 {
2   "took" : 1,
3   "timed_out" : false,
4   "_shards" : {
5     "total" : 1,
6     "successful" : 1,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : {
12      "value" : 182,
13      "relation" : "eq"
14    },
15    "max_score" : 1.3406837,
16    "hits" : [
17      {
18        "_index" : "log_consultas",
19        "_type" : "_doc",
20        "_id" : "8",
21        "_score" : 1.3406837,
22        "_source" : {
23          "@timestamp" : "2010-05-15T02:32:08",
24          "estado_consulta" : "error",
25          "servicio" : "modificacion",
26          "administrador" : "Juan Lara",
27          "consultas_realizadas" : 27
28        }
29      },
30    ]
31  }
```

### 1.2.3.2 Obtener el número de registros realizados por el administrador Juan Lara.

Con la ayuda de la siguiente consulta nos trajo los registros por el **administrador** Juan Lara.  
GET /log\_consultas/\_search?pretty=true&q=administrador:"Juan Lara"  
Habiendo un total de 98 registros.



```
1 {
2   "took" : 2,
3   "timed_out" : false,
4   "_shards" : {
5     "total" : 1,
6     "successful" : 1,
7     "skipped" : 0,
8     "failed" : 0
9   },
10  "hits" : {
11    "total" : {
12      "value" : 98,
13      "relation" : "eq"
14    },
15    "max_score" : 0.8232369,
16    "hits" : [
17      {
18        "_index" : "log_consultas",
19        "_type" : "_doc",
20        "_id" : "8",
21        "_score" : 0.8232369,
22        "_source" : {
23          "@timestamp" : "2010-05-15T02:32:08".
```

### 1.2.3.3 Obtener la suma de los valores en consultas realizadas con estado consulta igual a error

Con la ayuda de la siguiente consulta nos trajo la suma de los valores en **consultas\_realizadas** con **estado\_consulta** igual a error.

POST /log\_consultas/\_search?pretty

```
{
  "query": {
    "constant_score": {
      "filter": {
        "match": { "estado_consulta": "error" }
      }
    }
  },
  "aggs": {
    "consultas_realizadas": { "sum": { "field": "consultas_realizadas" } }
  }
}
```

Haciendo una sumatoria de 2865.

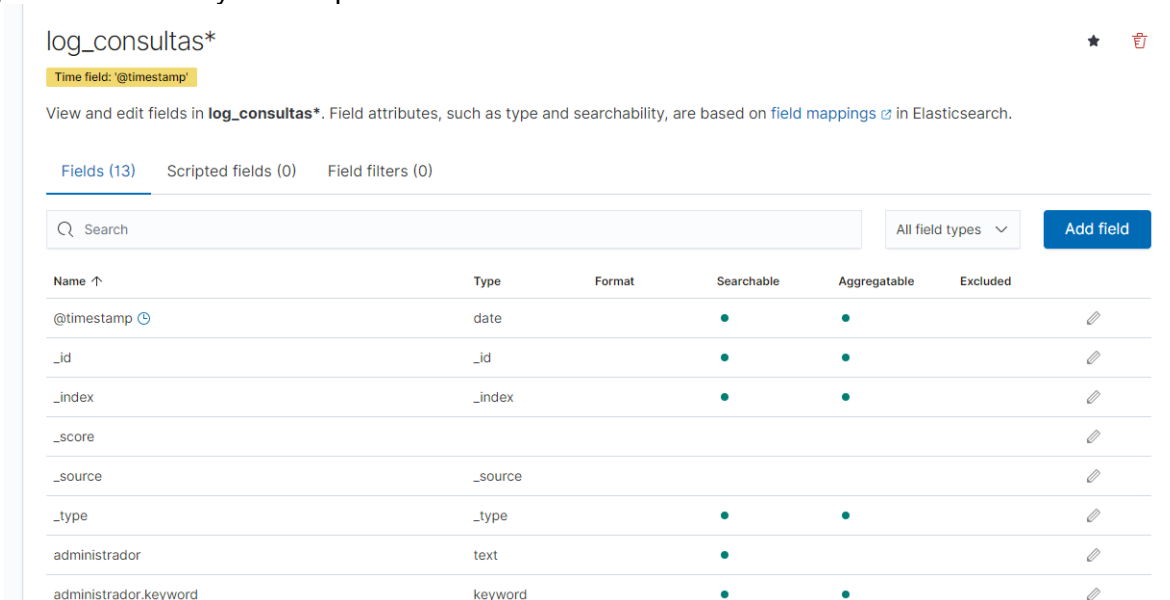
```
POST /log_consultas/_search?pretty
{
  "query": {
    "constant_score": {
      "filter": {
        "match": { "estado_consulta": "error" }
      }
    }
  },
  "aggs": {
    "consultas_realizadas": { "sum": { "field": "consultas_realizadas" } }
  }
}
```

```
124   "_id" : "48",
125   "_score" : 1.0,
126   "_source" : {
127     "@timestamp" : "2010-05-15T23:55:45",
128     "estado_consulta" : "error",
129     "servicio" : "borrado",
130     "administrador" : "Carlos Lara",
131     "consultas_realizadas" : 12
132   },
133 },
134 {
135   "_index" : "log_consultas",
136   "_type" : "_doc",
137   "_id" : "52",
138   "_score" : 1.0,
139   "_source" : {
140     "@timestamp" : "2010-05-15T17:02:14",
141     "estado_consulta" : "error",
142     "servicio" : "modificacion",
143     "administrador" : "Carlos Lara",
144     "consultas_realizadas" : 28
145   },
146 },
147 }
148 },
149 "aggregations" : {
150   "consultas_realizadas" : {
151     "value" : 2865.0
152   },
153 },
154 }
155 }
```

## 1.2.4 Realizar un tablero para visualizar información de empleados

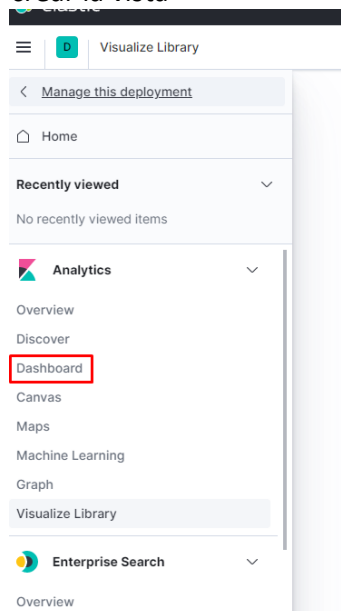
Crea un patrón de índice en **Kibana**, dirígete a la opción de **Management** y selecciona la opción **Kibana > Index Patterns** y selecciona el índice que creaste en los pasos anteriores **log\_consultas** tomando como **Time Filter** el campo de **@timestamp**.

Me dirigi a la ruta indica y cree el patron de índice.



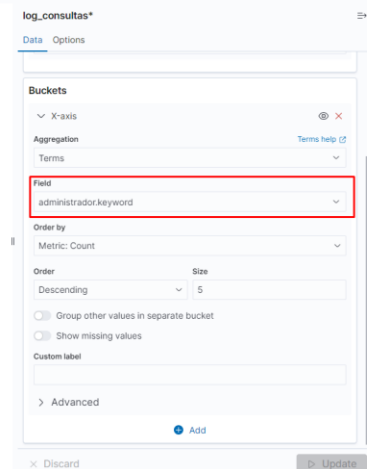
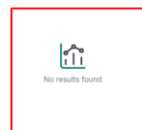
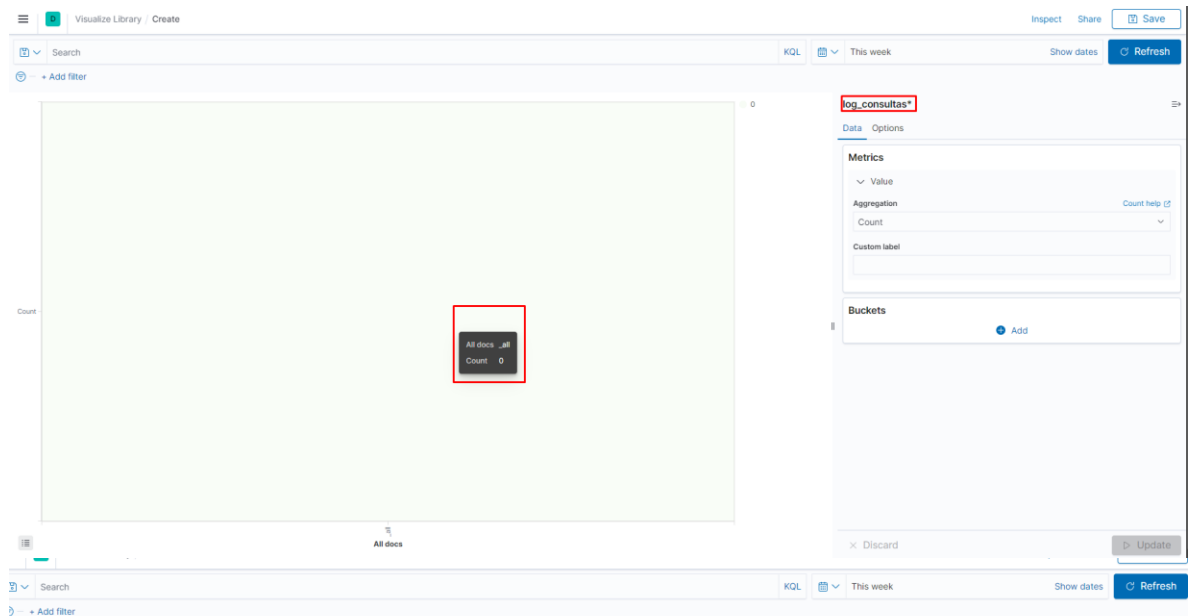
### 1.2.4.1 Vista de heat map, donde mostraras el número de servicios realizados por administrador

Me dirigi al menú de Analytics para poder crear la vista



Presione el botón de **Create new dashboard**.

No pude crear las vistas solicitadas ya que siempre intentaba agregar los parámetros de búsqueda y aparecía que no había documentos creados



Igual en el dashboard no me arrojaba datos

