



PRACTICAS ELASTIC SEARCH Y KIBANA

SPS Solutions

Marko Alan Bibiano Cortes
bcortesmarko@gmail.com

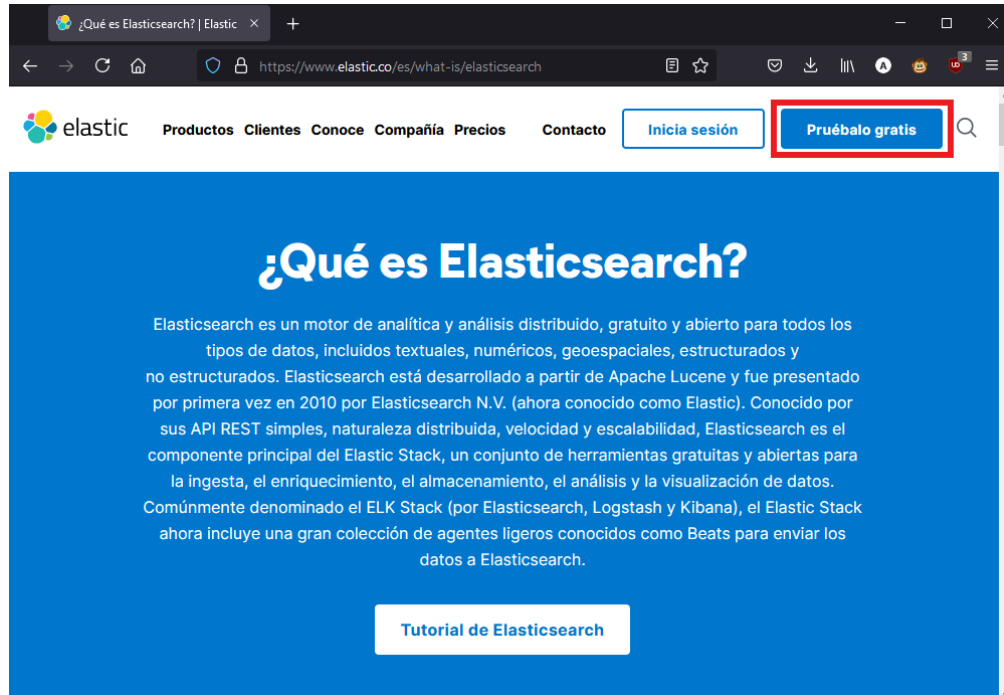
Contenido

Configurar una cuenta en Elastic Search	2
Creación de un Índice	5
Realizar búsquedas sobre el índice	8
Realizar un tablero para visualizar información de empleados	12
Crea un patrón de índice en Kibana	12
Vista de heatmap.....	13
Vista de Barras.....	17
Genera un tablero con las 2 visualizaciones que acabas de crear.	19

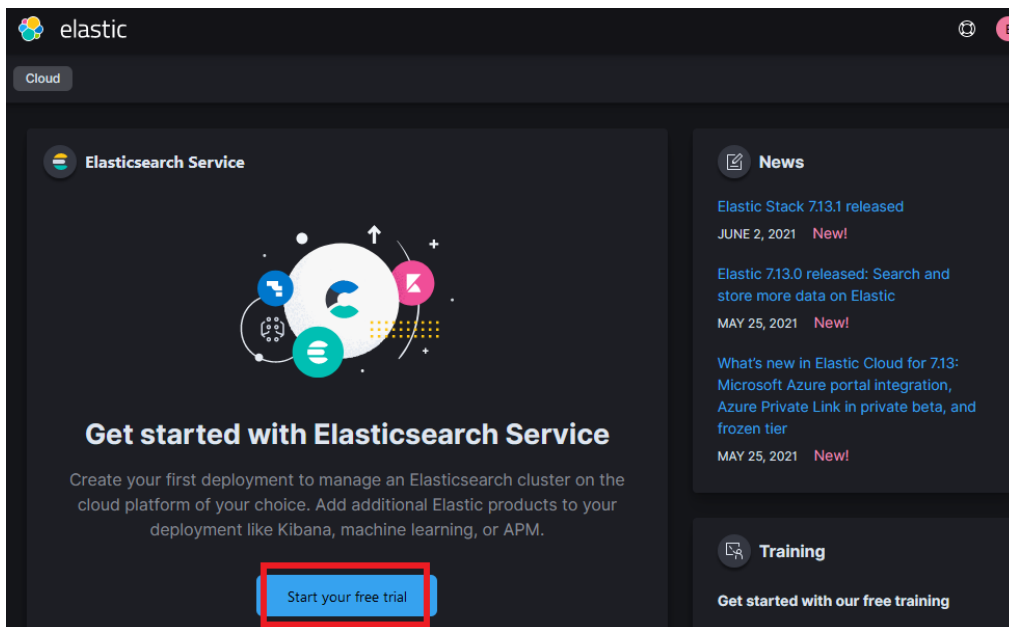
Configurar una cuenta en Elastic Search

1. Abrir la siguiente página y crear una cuenta gratis:

<https://www.elastic.co/es/what-is/elasticsearch>



2. Seleccionamos Elastic Search y Creamos una cuenta gratuita, al terminar nos lleva a la siguiente página, hacemos clic en **Start your free trial**:



3. Colocamos las opciones del deployment
 - Nombre del deployment: sps_practica
 - Plataforma: Amazon Web
 - ServiceRegion: US East (N. Virginia)
 - Elastic Stack version: Mas reciente
 - Optimize your deployment: I/O Optimized


Settings


Choose the cloud provider, region, and Elastic Stack version.


[Collapse](#) ▾

Cloud provider


Pick a cloud and let us handle the rest. No additional accounts required.

Google Cloud

Azure

Amazon Web Services

Region

 N. Virginia (us-east-1) ▾

Hardware profile

I/O Optimized ▾

Version

7.13.2 ▾

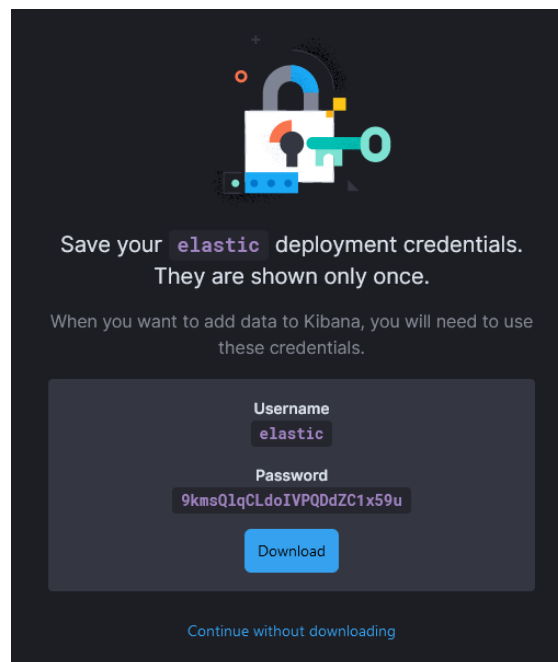
Name your deployment

You can always change this later.

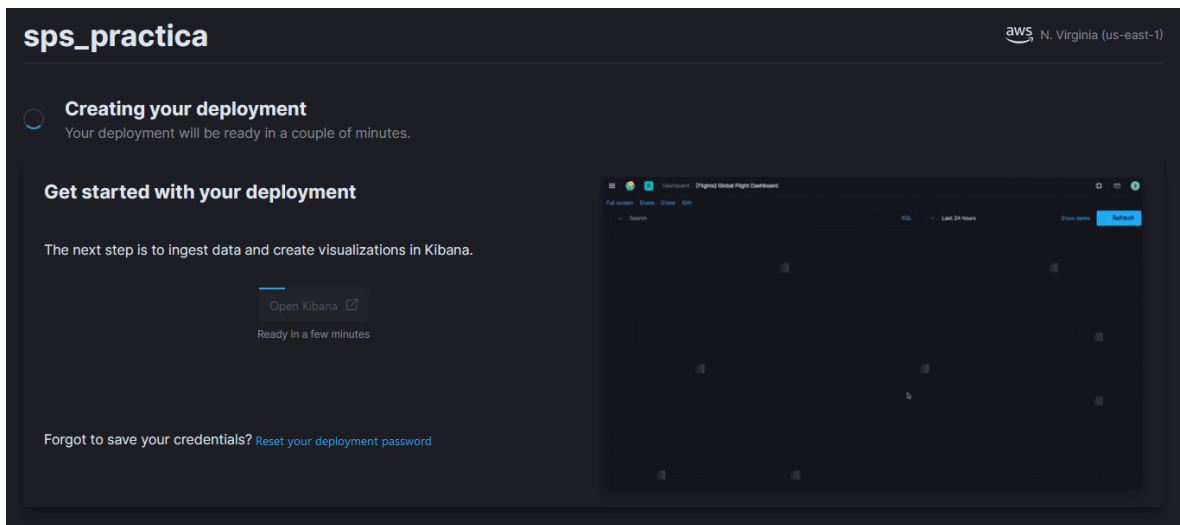
sps_practica

✓ Create deployment

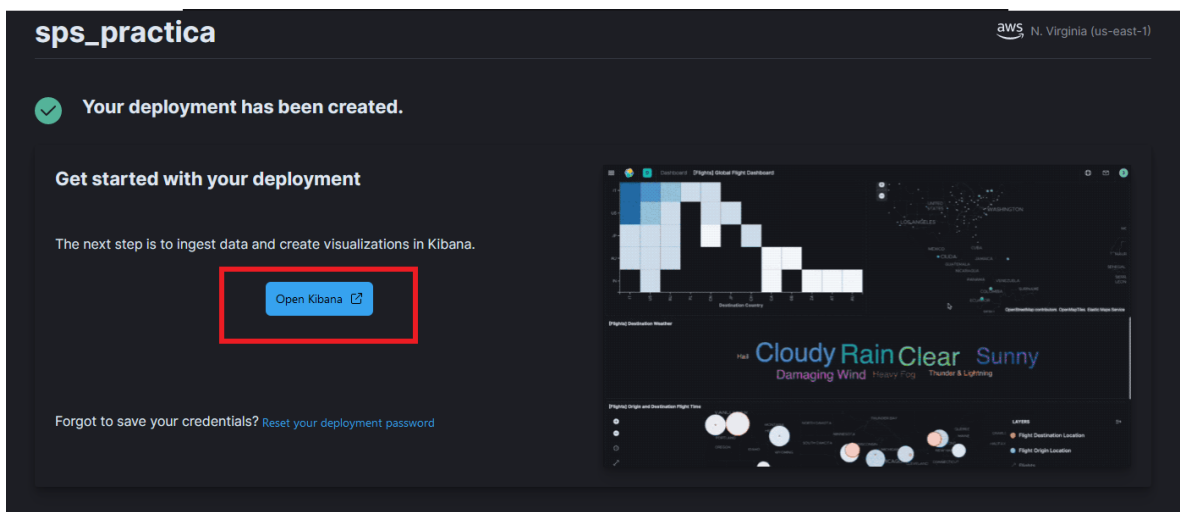
4. Nos muestra las credenciales de nuestro despliegue en Elastic:



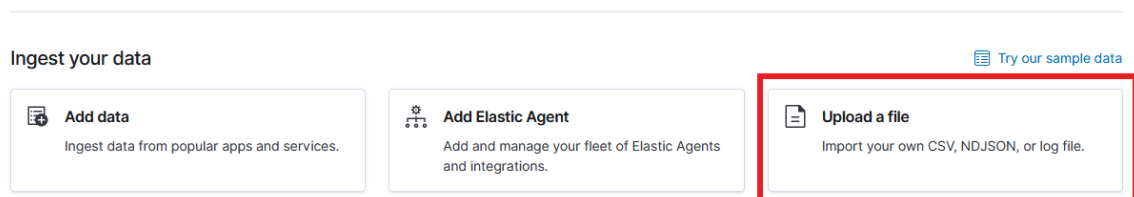
5. Esperamos unos minutos a que se cree la configuración



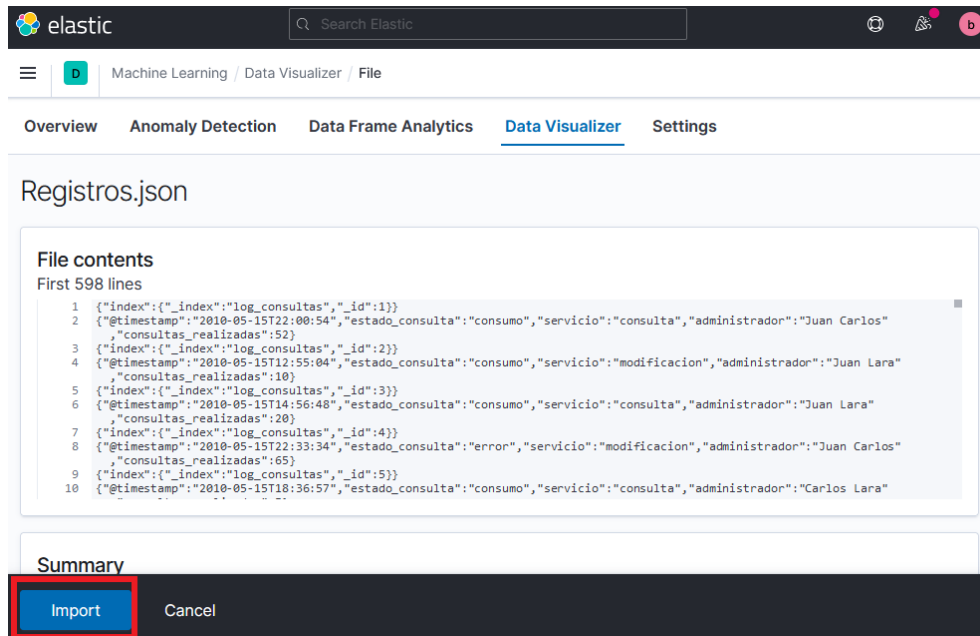
6. Cuando el proceso termine, aparecerá un mensaje diciendo que el despliegue ha sido creado, procedemos a hacer clic en el botón **Open Kibana**:



7. En la página Home de Kibana, Seleccionamos **Upload a file**



8. Cargamos el archivo Registros.json y seleccionamos **Import**

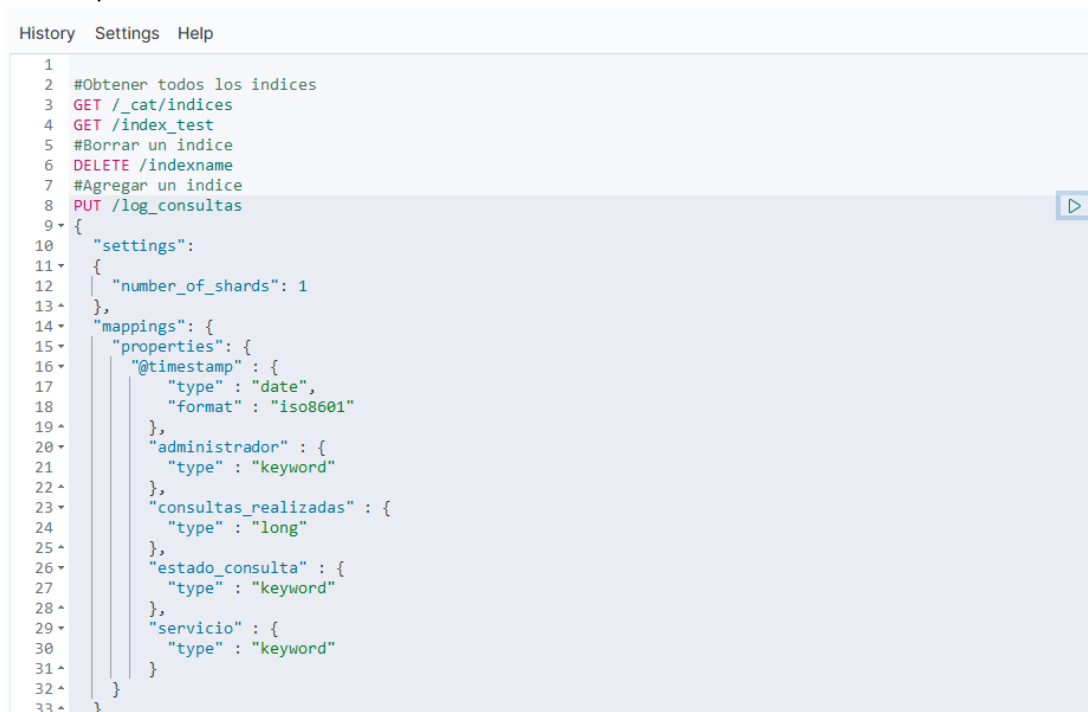


Creación de un Índice

Para realizar estas actividades revise en la documentación oficial de Elastic Search, acerca de como funcionan y se declaran diversos elementos, dejo en el siguiente link la referencia:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

1. La siguiente imagen muestra cuando se cree el índice junto con las propiedades y su mapeado



```

1 {
2   "acknowledged" : true,
3   "shards_acknowledged" : true,
4   "index" : "log_consultas"
5 }
6

```

2. Para crear un template, busque en la documentación oficial:

<https://www.elastic.co/guide/en/elasticsearch/reference/7.13/index-templates.html>

```

PUT /_index_template/template_1
{
  "index_patterns" : ["log_consultas*"],
  "priority" : 1,
  "template": {
    "settings" : {
      "number_of_shards" : 2
    }
  }
}

```

```

1 {
2   "acknowledged" : true
3 }
4

```

3. Con el archivo de Registros.json y usando la API Bulk agregamos los documentos a nuestro índice:

```

Settings Help
#Usar API BULK para meter
POST /log_consultas/_bulk
{"index":{"_index":"log_consultas","_id":1}}
{"@timestamp":"2010-05-15T22:00:54","estado_consulta":"consumo","servicio":"consulta","administrador":"Juan Carlos","consultas_realizadas":52}
{"index":{"_index":"log_consultas","_id":2}}
{"@timestamp":"2010-05-15T12:55:04","estado_consulta":"consumo","servicio":"modificacion","administrador":"Juan Lara","consultas_realizadas":10}
{"index":{"_index":"log_consultas","_id":3}}
{"@timestamp":"2010-05-15T14:56:48","estado_consulta":"consumo","servicio":"consulta","administrador":"Juan Lara","consultas_realizadas":20}
{"index":{"_index":"log_consultas","_id":4}}
{"@timestamp":"2010-05-15T22:33:34","estado_consulta":"error","servicio":"modificacion","administrador":"Juan Carlos","consultas_realizadas":65}
{"index":{"_index":"log_consultas","_id":5}}
{"@timestamp":"2010-05-15T18:36:57","estado_consulta":"consumo","servicio":"consulta","administrador":"Carlos Lara","consultas_realizadas":5}
{"index":{"_index":"log_consultas","_id":6}}
{"@timestamp":"2010-05-15T11:21:05","estado_consulta":"informativo","servicio":"borrado","administrador":"Juan Carlos","consultas_realizadas":50}
{"index":{"_index":"log_consultas","_id":7}}
{"@timestamp":"2010-05-15T18:37:14","estado_consulta":"error","servicio":"modificacion","administrador":"Juan Carlos","consultas_realizadas":32}
{"index":{"_index":"log_consultas","_id":8}}
{"@timestamp":"2010-05-15T02:32:08","estado_consulta":"error","servicio":"modificacion","administrador":"Juan Lara","consultas_realizadas":27}
{"index":{"_index":"log_consultas","_id":9}}
{"@timestamp":"2010-05-15T09:42:41","estado_consulta":"consumo","servicio":"modificacion","administrador":"Juan Lara","consultas_realizadas":23}
{"index":{"_index":"log_consultas","_id":10}}
{"@timestamp":"2010-05-15T00:27:26","estado_consulta":"error","servicio":"consulta","administrador":"Carlos Lara","consultas_realizadas":53}
{"index":{"_index":"log_consultas","_id":11}}
{"@timestamp":"2010-05-15T11:57:20","estado_consulta":"consumo","servicio":"modificacion","administrador":"Juan Lara","consultas_realizadas":3}
{"index":{"_index":"log_consultas","_id":12}}
{"@timestamp":"2010-05-15T12:25:21","estado_consulta":"informativo","servicio":"consulta","administrador":"Juan Lara","consultas_realizadas":39}
{"index":{"_index":"log_consultas","_id":13}}
{"@timestamp":"2010-05-15T23:10:59","estado_consulta":"consumo","servicio":"borrado","administrador":"Juan Carlos","consultas_realizadas":55}
{"index":{"_index":"log_consultas","_id":14}}
{"@timestamp":"2010-05-15T06:44:20","estado_consulta":"consumo","servicio":"modificacion","administrador":"Juan Lara"}

```

4. Resultado de ingresar los datos al índice "log_consultas"

```
1 {
2   "took" : 38,
3   "errors" : false,
4   "items" : [
5     {
6       "index" : {
7         "_index" : "log_consultas",
8         "_type" : "_doc",
9         "_id" : "1",
10        "_version" : 3,
11        "result" : "updated",
12        "_shards" : {
13          "total" : 2,
14          "successful" : 2,
15          "failed" : 0
16        },
17        "_seq_no" : 4,
18        "_primary_term" : 1,
19        "status" : 200
20      }
21    },
22    {
23      "index" : {
24        "_index" : "log_consultas",
25        "_type" : "_doc",
26        "_id" : "2",
27        "_version" : 2,
28        "result" : "updated",
29        "_shards" : {
30          "total" : 2,
31          "successful" : 2,
32          "failed" : 0
33        },
34        "_seq_no" : 5,
35        "_primary_term" : 1,
36        "status" : 200
37      }
38    },
39    {
40      "index" : {
41        "_index" : "log_consultas",
42        "_type" : "_doc",
43        "_id" : "3"
```


Realizar búsquedas sobre el índice

1. Obtener el número de registros con estado_consulta igual a error y consumo

```
62 #Usar API Search
63 #Obtener documentos donde estado_consulta sea "error" o "consumo"
64 GET /log_consultas/_search?size=300
65 {
66   "query": {
67     "terms": {
68       "estado_consulta":
69       [
70         "error",
71         "consumo"
72       ]
73     }
74   }
75 }
```

Resultado de la consulta anterior:

```
1 {
2   "took" : 3,
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" : 1.0,
16    "hits" : [
17      {
18        "_index" : "log_consultas",
19        "_type" : "_doc",
20        "_id" : "1",
21        "_score" : 1.0,
22        "_source" : {
23          "@timestamp" : "2010-05-15T22:00:54",
24          "estado_consulta" : "consumo",
25          "servicio" : "consulta",
26          "administrador" : "Juan Carlos",
27          "consultas_realizadas" : 52
28        }
29      },
30      {
31        "_index" : "log_consultas",
32        "_type" : "_doc",
33        "_id" : "2",
34        "_score" : 1.0,
35        "_source" : {
36          "@timestamp" : "2010-05-15T12:55:04",
37          "estado_consulta" : "consumo",
38          "servicio" : "modificacion",
39          "administrador" : "Juan Lara",
40          "consultas_realizadas" : 10
41        }
42      },
43      {
44        "_index" : "log_consultas",
45        "_type" : "_doc",
```

2. Obtener el número de registros realizados por el administrador Juan Lara

```
#Obtener documentos de Juan Lara
GET /log_consultas/_search?size=300
{
  "query": {
    "term": {
      "administrador": "Juan Lara"
    }
  }
}
```

El resultado es el siguiente:

```
{
  "took" : 4,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 98,
      "relation" : "eq"
    },
    "max_score" : 1.1137259,
    "hits" : [
      {
        "_index" : "log_consultas",
        "_type" : "_doc",
        "_id" : "2",
        "_score" : 1.1137259,
        "_source" : {
          "@timestamp" : "2010-05-15T12:55:04",
          "estado_consulta" : "consumo",
          "servicio" : "modificacion",
          "administrador" : "Juan Lara",
          "consultas_realizadas" : 10
        }
      },
      {
        "_index" : "log_consultas",
        "_type" : "_doc",
        "_id" : "3",
        "_score" : 1.1137259,
        "_source" : {
          "@timestamp" : "2010-05-15T14:56:48",
          "estado_consulta" : "consumo",
          "servicio" : "consulta",
          "administrador" : "Juan Lara",
          "consultas_realizadas" : 20
        }
      },
      {
        "_index" : "log_consultas",
        "_type" : "_doc",

```

3. Obtener el número de registros con estado_consulta igual a informativo y servicio igual a borrado

```
#Obtener documentos con estado_consulta="informativo" y servicio="borrado"
GET /log_consultas/_search?size=300
{
  "query": {
    "bool": {
      "must": [
        {
          "match": {
            "estado_consulta": "informativo"
          }
        },
        {
          "match": {
            "servicio": "borrado"
          }
        }
      ]
    }
  }
}
```

#Obtener la suma de consultas realizadas desde estado consulta "borrado"

Resultados:

```
{
  "took" : 4,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 52,
      "relation" : "eq"
    },
    "max_score" : 1.9729816,
    "hits" : [
      {
        "_index" : "log_consultas",
        "_type" : "_doc",
        "_id" : "6",
        "_score" : 1.9729816,
        "_source" : {
          "@timestamp" : "2010-05-15T11:21:05",
          "estado_consulta" : "informativo",
          "servicio" : "borrado",
          "administrador" : "Juan Carlos",
          "consultas_realizadas" : 50
        }
      },
      {
        "_index" : "log_consultas",
        "_type" : "_doc",
        "_id" : "25",
        "_score" : 1.9729816,
        "_source" : {
          "@timestamp" : "2010-05-15T23:09:17",
          "estado_consulta" : "informativo",
          "servicio" : "borrado",
          "administrador" : "Juan Carlos",
          "consultas_realizadas" : 57
        }
      },
      {
        "_index" : "log_consultas",
        "_type" : "_doc",

```

4. Obtener la suma de los valores en consultas_realizadas con estado_consulta igual a error

#Obtener la suma de consultas realizadas donde estado_consulta="error"

GET /log_consultas/_search?size=0

```
{
  "query": {
    "term": {
      "estado_consulta": "error"
    }
  },
  "aggs": {
    "total_de_consultas_realizadas": {
      "sum": {
        "field": "consultas_realizadas"
      }
    }
  }
}
```

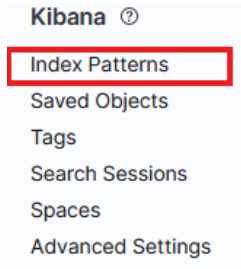
Resultados:

```
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" : 78,
13     "relation" : "eq"
14   },
15     "max_score" : null,
16     "hits" : [ ]
17   },
18 ▾  "aggregations" : {
19 ▾    "total_de_consultas_realizadas" : {
20     "value" : 2865.0
21   }
22   }
23 }
24
```

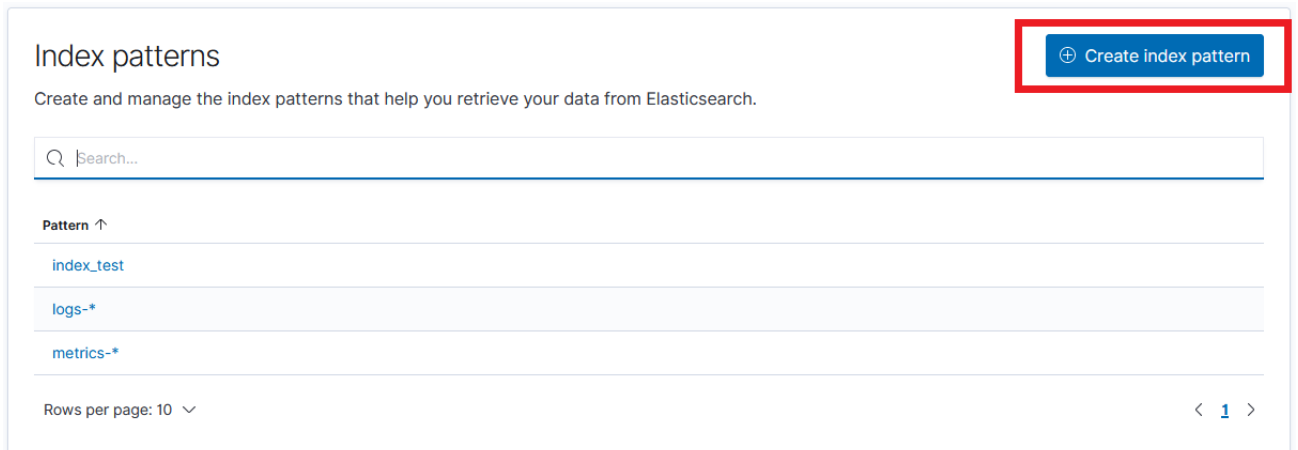
Realizar un tablero para visualizar información de empleados

Crea un patrón de índice en Kibana

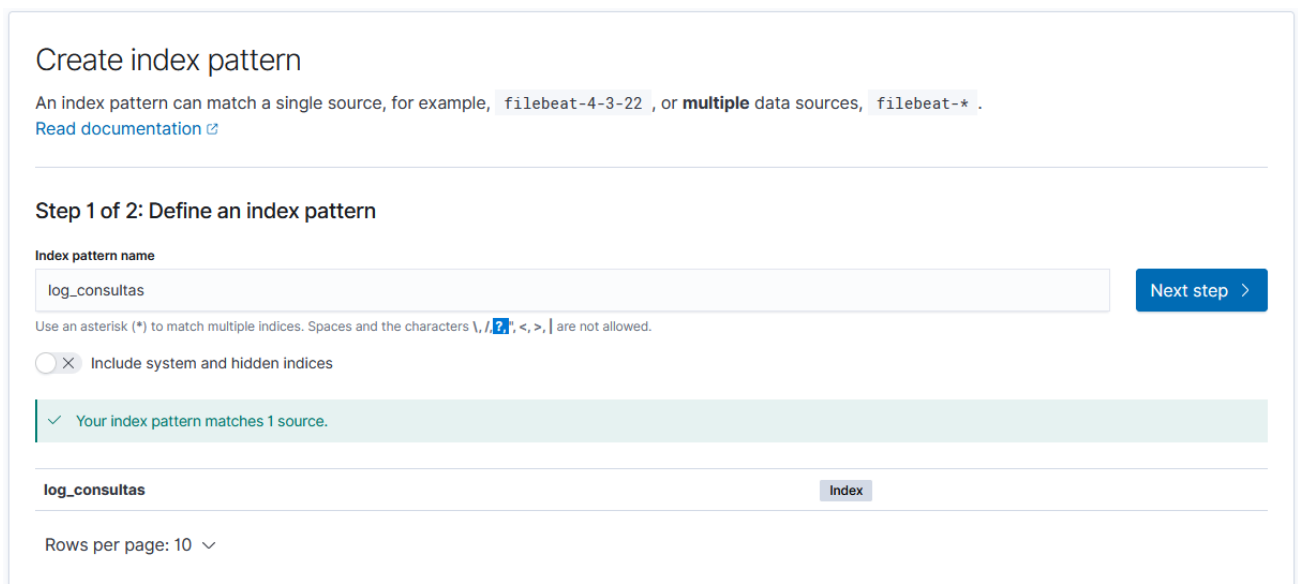
1. Nos dirigimos a **Stack Management**, en las opciones de Kibana seleccionamos la opción **Index Patterns**



2. Seleccionamos **Create Index pattern**



3. Escribimos el patrón de nuestro índice y seleccionamos **Next step**



4. En el campo **Time field** seleccionamos **@timestamp**, para finalizar seleccionamos **Create index pattern**

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 2 of 2: Configure settings

Specify settings for your **log_consultas** index pattern.

Select a primary time field for use with the global time filter.

Time field

Refresh

@timestamp

> Show advanced settings

< Back

Create index pattern

Vista de heatmap

Crear vista heatmap donde mostraras el número de servicios realizados por administrador.

1. Seleccionamos **Visualize Library > Create Visualization**

Building a dashboard? Create content directly from the [Dashboard application](#) using a new integrated workflow.

Visualize Library

+

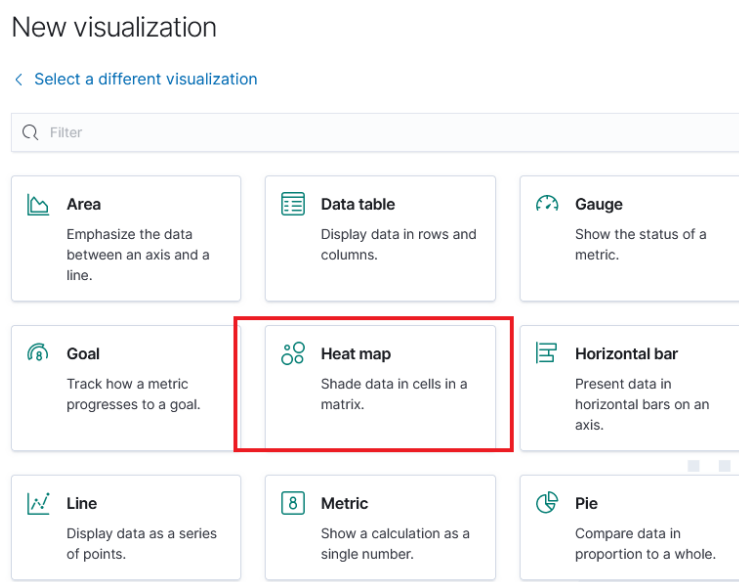
Create visualization

Search...

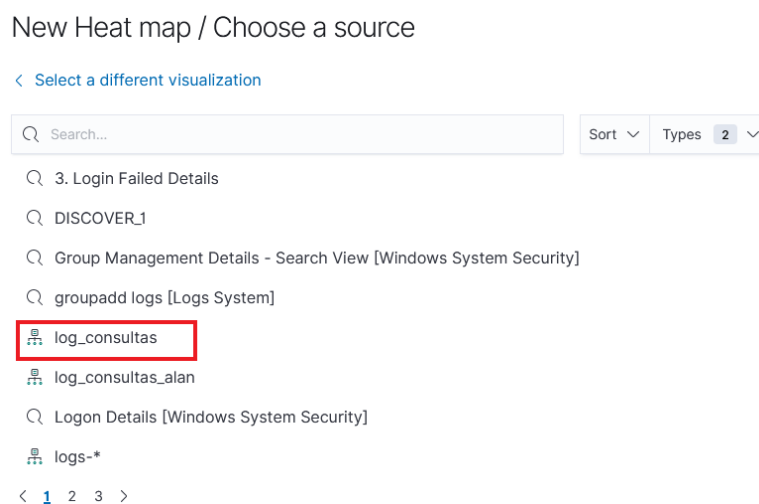
Tags

<input type="checkbox"/>	Title	Type	Description	Tags	Actions
<input type="checkbox"/>	Failed Logons [Windows System Security]	8 Metric			

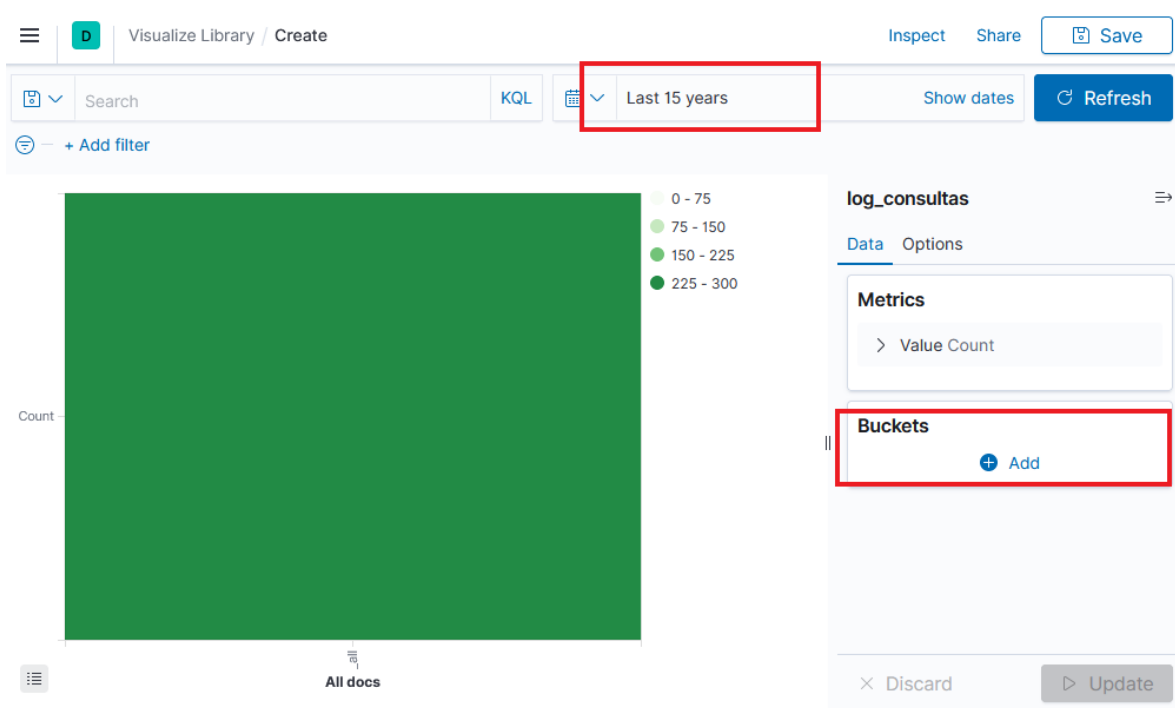
2. Se abre una ventana para escoger el tipo de visualización, seleccionamos **Aggregation based > Heat map**:



3. Seleccionamos **log_consultas**, el Index pattern que creamos:






4. Seleccionamos un rango de 15 años para que muestre todo el contenido del Index, en el apartado **Buckets** seleccionamos **Add** para agregar los valores del eje X y del eje Y.



5. En el eje X colocamos los valores del campo **servicios**

Buckets

▼ X-axis  

Aggregation [Terms help](#) 

Terms ▼



Field

servicio ▼

Order by

Metric: Count ▼

Order **Size**

Descending ▼ 5  

6. En el eje Y colocamos los valores del campo **administradores**

Buckets

> X-axis servicio: Descending

Y-axis

Sub aggregation [Terms help](#)

Terms

Field

administrador

Order by

Metric: Count

Order

Descending

Size

5

7. Seleccionamos la pestaña **Options**, en la sección **Labels** seleccionamos **Show labels**, seleccionamos **Update** para aplicar los cambios

log_consultas

Data **Options**

Number of colors

4

☐ Use custom ranges

Labels

☒ Show labels

☐ Rotate

☐ Overwrite automatic color

Color

BLACK

[Discard](#) [Update](#)

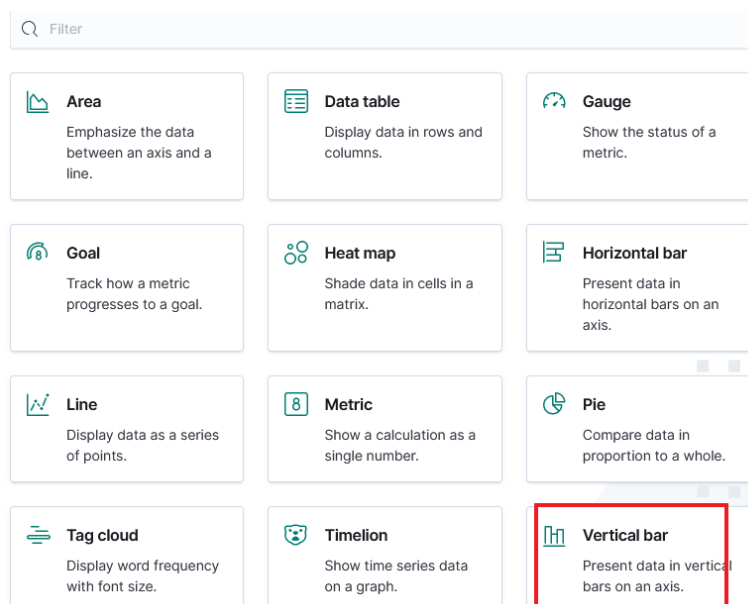
8. El resultado es una visualización como la siguiente:



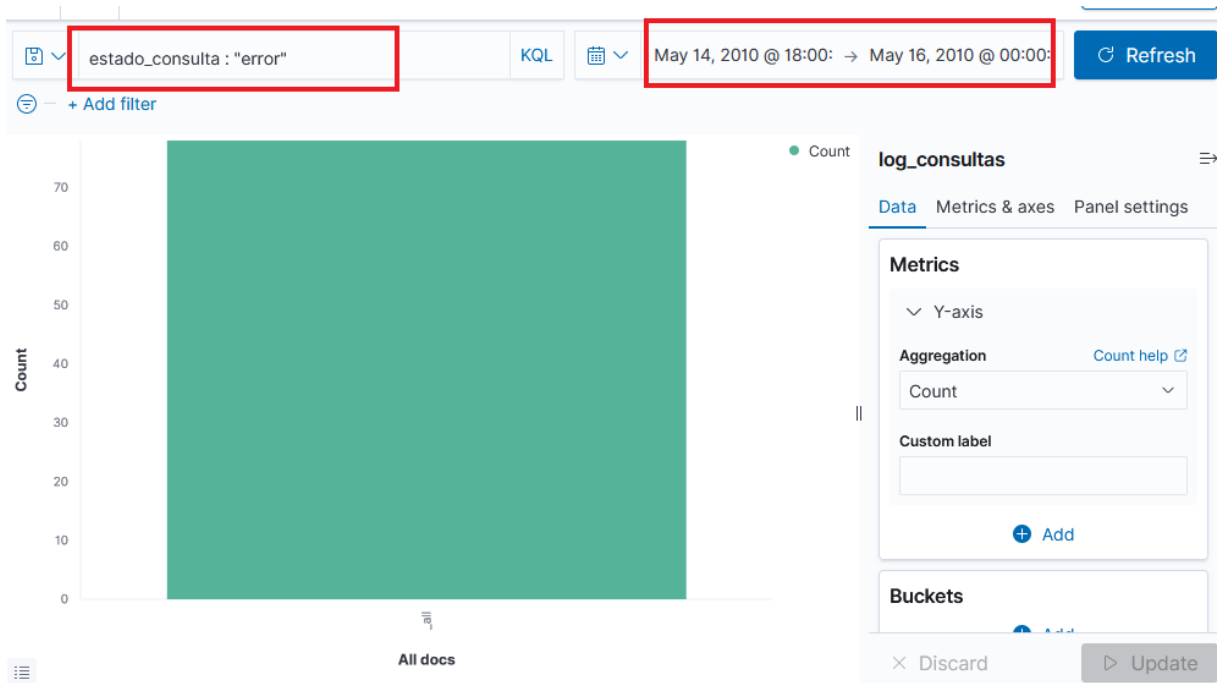
Vista de Barras

Crear una vista de barras donde se grafique el número de registros con estado_consulta igual a error a través del tiempo

1. Repetimos los primeros pasos que en la practica anterior, pero ahora seleccionamos **barra Vertical** al momento de escoger el tipo de visualización y seleccionamos **log_consultas** como fuente:



2. Agregamos un filtro para los estados con error, seleccionamos la fecha de nuestros datos



3. Agregamos un bucket para el eje X, en **Aggregation** seleccionamos **Date Histogram**, en **Field** seleccionamos nuestro campo del tiempo, en **Minimum Interval** escribimos **30m**, hacemos clic en **Update** para aplicar los cambios

Buckets

✓ X-axis



Aggregation

[Date Histogram help](#)

Date Histogram



Field

HH:mm



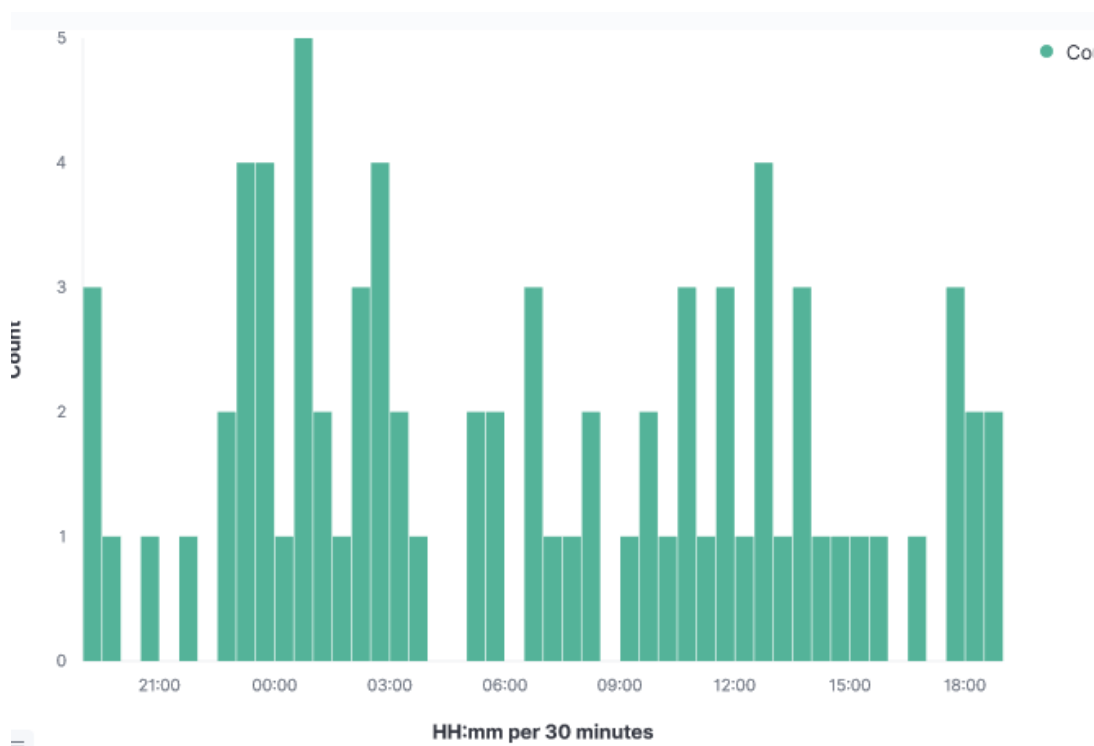
Minimum interval

30m



Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

4. Al finalizar debe de quedar una gráfica como la siguiente



Genera un tablero con las 2 visualizaciones que acabas de crear.

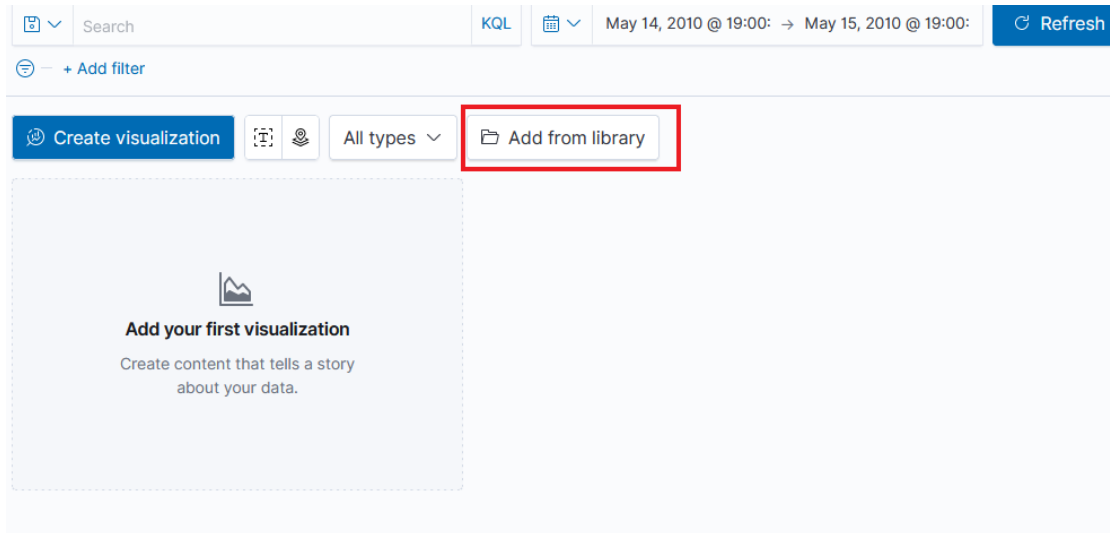
1. Nos dirigimos a las opciones de Dashboards y seleccionamos **Create Dashboard**

Dashboards

[+ Create dashboard](#)

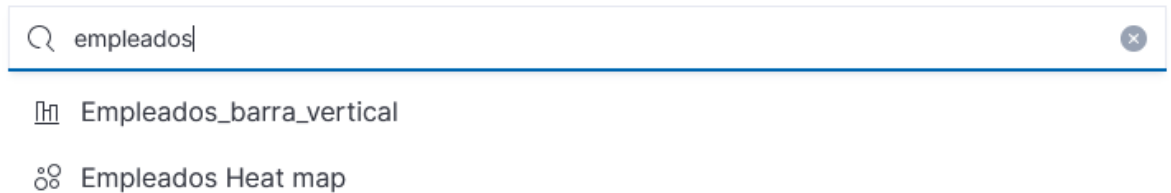
Search...				Tags
<input type="checkbox"/> Title	Description	Tags	Actions	
<input type="checkbox"/> [Elastic Agent] Agent metrics	Elastic Agent metrics dashboard			
<input type="checkbox"/> [Logs System] New users and groups	New users and groups dashboard for the System integration in Logs			
<input type="checkbox"/> [Logs System] SSH login attempts	SSH dashboard for the System integration in Logs			

2. Seleccionamos **Add from library** para agregar las gráficas que creamos

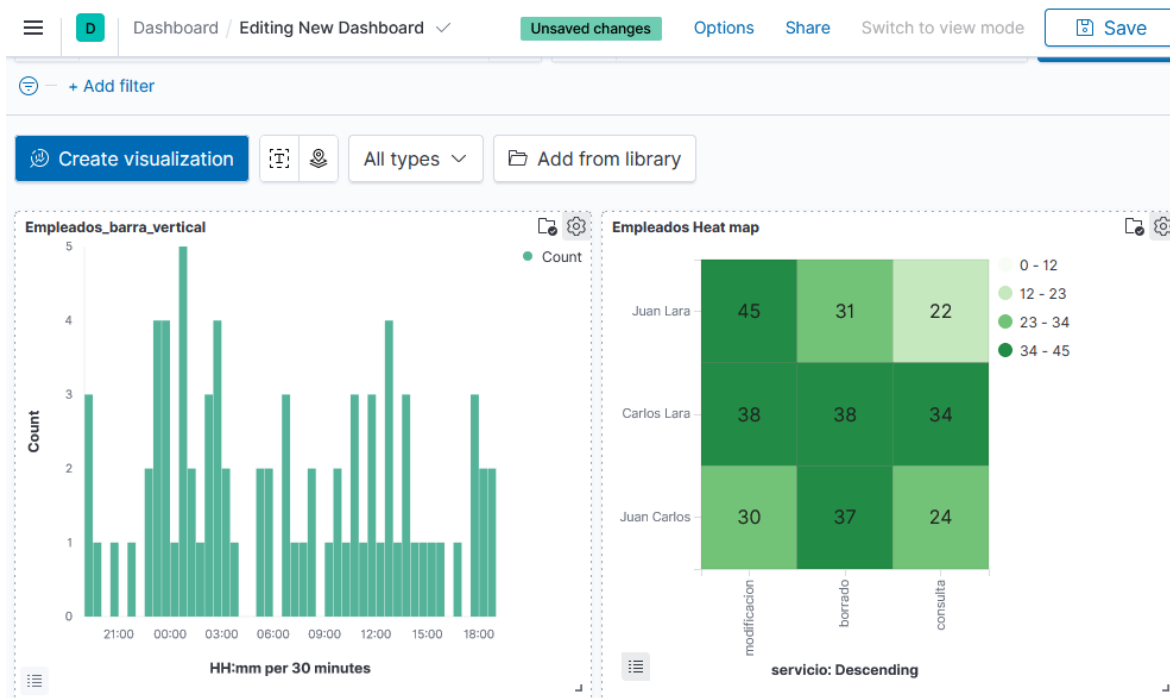


3. Escribimos el nombre en la barra de búsqueda y las agregamos

Add from library



4. Seleccionamos **Save** para guardar el dashboard



5. El resultado final es el siguiente

