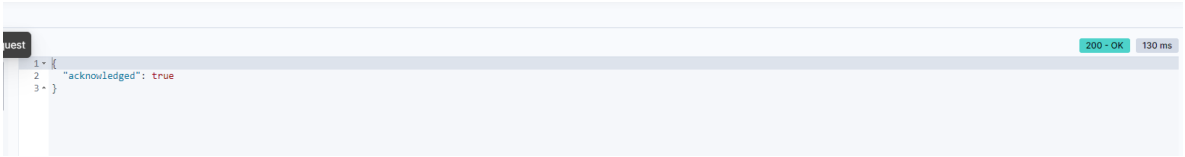
Creación de un índice

https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-create-index.html

Settings Variables Help

```
# 2. Crea un índice con el nombre de log_consultas a partir del siguiente JSON:
POST _index_template/log_consultas
{
  "index_patterns": [
    "log_consultas*"
  ],
  "template": {
    "settings": {
      "number_of_shards": 1
    },
    "mappings": {
      "_source": {
        "enabled": true
      },
      "properties": {
        "@timestamp": {
          "type": "date"
        },
        "estado_consulta": {
          "type": "keyword"
        },
        "servicio": {
          "type": "keyword"
        },
        "administrador": {
          "type": "keyword"
        },
        "consultas_realizadas": {
          "type": "integer"
        }
      }
    }
  }
}
```



https://www.elastic.co/guide/en/elasticsearch/reference/current/docs-bulk.html

```
# 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).
POST /_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":"2010-05-15T09:02:41","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":"2010-05-15T06:44:29","estado_consulta":"consumo","servicio":"modificacion","administrador":"Juan Lara"
  ,"consultas_realizadas":41}
{"index":{"_index":"log_consultas","_id":15}}
{"@timestamp":"2010-05-15T11:16:13","estado_consulta":"informativo","servicio":"modificacion","administrador":"Juan Lara"
  ,"consultas_realizadas":15}
{"index":{"_index":"log_consultas","_id":16}}
{"@timestamp":"2010-05-15T02:46:41","estado_consulta":"consumo","servicio":"consulta","administrador":"Juan Lara"
  ,"consultas_realizadas":26}
{"index":{"_index":"log_consultas","_id":17}}
{"@timestamp":"2010-05-15T08:51:32","estado_consulta":"consumo","servicio":"borrado","administrador":"Juan Lara"
  ,"consultas_realizadas":40}
{"index":{"_index":"log_consultas","_id":18}}
{"@timestamp":"2010-05-15T18:37:49","estado_consulta":"informativo","servicio":"modificacion","administrador":"Juan Carlos"
  ,"consultas_realizadas":8}
{"index":{"_index":"log_consultas","_id":19}}
{"@timestamp":"2010-05-15T22:07:57","estado_consulta":"informativo","servicio":"consulta","administrador":"Juan Lara"
```

Realizar búsquedas sobre el índice

https://www.elastic.co/guide/en/elasticsearch/reference/current/search-your-data.html

```
# 1. Obtener el número de registros con estado_consulta igual a error y consumo.
GET /log_consultas/_search
{
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "estado_consulta": [
              "error",
              "consumo"
            ]
          }
        }
      ]
    }
  },
  "size": 0,
  "track_total_hits": true
}
```


```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 182,
      "relation": "eq"
    },
    "max_score": null,
    "hits": []
  }
}
```

```
# 2. Obtener el número de registros realizados por el administrador Juan Lara.
GET /log_consultas/_search
{
  "query": {
    "bool": {
      "must": [
        {
          "match": {
            "administrador": "Juan Lara"
          }
        }
      ]
    }
  },
  "size": 0,
  "track_total_hits": true
}
```


```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 98,
      "relation": "eq"
    },
    "max_score": null,
    "hits": []
  }
}
```


```
# 3. Obtener el número de registros con estado_consulta igual a informativo y servicio igual a borrado
GET /log_consultas/_search
{
  "query": {
    "bool": {
      "must": {
        "match": {
          "estado_consulta": "informativo"
        }
      },
      "filter": {
        "terms": {
          "servicio": [
            "borrado"
          ]
        }
      }
    }
  },
  "size": 0,
  "track_total_hits": true
}
```

```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 52,
      "relation": "eq"
    },
    "max_score": null,
    "hits": []
  }
}
```


https://opster.com/guides/elasticsearch/data-architecture/elasticsearch-sum-aggregation/

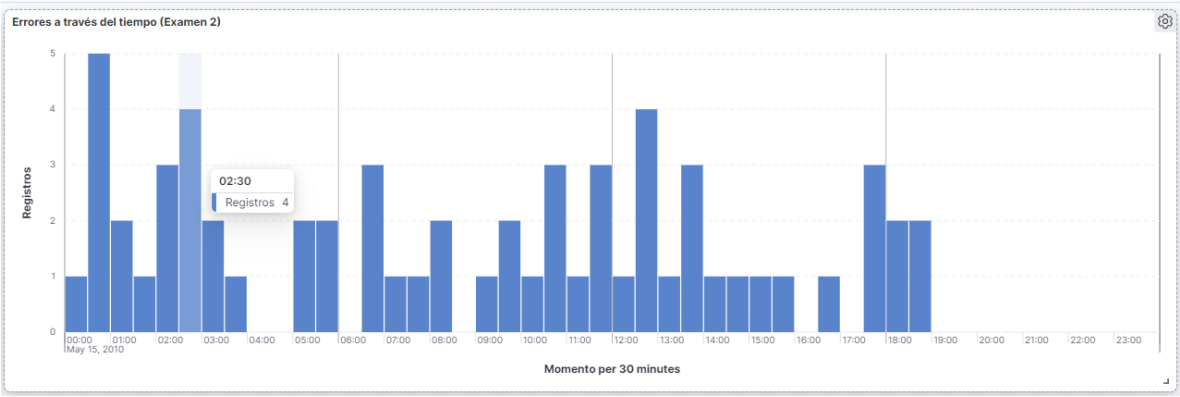
```
# 4. Obtener la suma de los valores en consultas_realizadas con estado_consulta igual a error
GET /log_consultas/_search
{
  "query": {
    "term": {
      "estado_consulta": "error"
    }
  },
  "aggs": {
    "sum_consultas_realizadas": {
      "sum": {
        "field": "consultas_realizadas"
      }
    }
  }
}
```


```
        "servicio": "borrado",
        "administrador": "Carlos Lara",
        "consultas_realizadas": 12
      }
    },
    {
      "_index": "log_consultas",
      "_id": "52",
      "_score": 1.3406837,
      "_source": {
        "@timestamp": "2010-05-15T17:02:14",
        "estado_consulta": "error",
        "servicio": "modificacion",
        "administrador": "Carlos Lara",
        "consultas_realizadas": 28
      }
    }
  ]
},
"aggregations": {
  "sum_consultas_realizadas": {
    "value": 2865
  }
}
}
```

Realizar un tablero para visualizar información de empleados

https://www.elastic.co/guide/en/kibana/current/data-views.html

https://www.elastic.co/guide/en/kibana/current/dashboard.html



Errores/investigación:

- Al principio puse los tipos de datos como text, por lo que posterior tuve que eliminar el índice, cambiarlos a keyword para crear el tablero, y volverlo a crear.
- Derivado de los anterior, al filtrar en el segundo punto, no me reflejaba de manera correcta los datos del administrador Juan Lara.
- No sabía cómo pasar los datos de los índices de kibana al tablero, por lo que investigando, dí con que se tiene que crear una vista para que posterior Lens los pueda tomar.
- Tuve que empaparme e investigar de cuál era la sintaxis para los filtros y agregados.
- Las ligas de lo que leí e investigué se las incluí al inicio en cada sección.