Elasticsearch

Exercício

Quando meu site caiu em 4 de dezembro de 2015 (agrupar status 500 por minuto nos logs do Kafka)

Sundog Education Coralogix PROF. FERNANDO AMARAL

Nossa Solução

```
GET /kafka-logs/_search?size=0&pretty
{
        "query" : {
                "match": {
                        "response": "500"
                }
        },

        "aggs" : {
                "timestamp": {
                        "date_histogram": {
                                "field": "@timestamp",
                                "interval": "minute"
                        }
                }
        }
}
```