

ELK筆記

1. 安裝ElasticSearch、Logstash、Kibana

2. 在ElasticSearch匯入及查詢 Sample Data

3. Kibana 視覺化呈現(一) 垂直柱狀圖、折線圖及區域圖

4. Kibana 視覺化呈現(二)圓餅圖、度量圖及標籤雲

5. Kibana 視覺化呈現(三)資料表、計量圖

6. ELK 搜尋語法

7. Timelion

8. 地圖教學

- <https://www.elastic.co/blog/custom-region-maps-in-kibana-6-0>
- <https://www.elastic.co/blog/custom-basemaps-for-region-and-coordinate-maps-in-kibana>

▲ 上面的地圖要先建板:

<https://www.notion.so/ElasticSearch-d55a70759c394beabaed9dbc03445a33>

PUT /whiskey_kibana_final_latlon_1

```
{
  "mappings": {
    "properties": {
      "location": {
        "type": "geo_point"
      }
    }
  }
}
```

▲ 經緯度格式有3種

<https://www.elastic.co/guide/cn/elasticsearch/guide/current/lat-lon-formats.html>

1. <https://www.youtube.com/watch?v=-lSaOx6u9rs>
2. https://www.tutorialspoint.com/kibana/kibana_working_with_coordinate_map.htm
3. <https://www.notion.so/ElasticSearch-d55a70759c394beabaed9dbc03445a33>

9. 創建儀錶板

10. 多圖教學(影片)

11. 定期清掉舊資料

- 從vm <https://blog.johnwu.cc/article/elk-purge-elasticsearch-index.html>
- 從python

```
from elasticsearch import Elasticsearch
es.indices.delete(index='elk_test', ignore=[400, 404])
es = Elasticsearch("http://IP:9200/")
```