
logstash
elasticsearch
kibana

ELK 主要由三個開源套件所組成，用於

收集日誌資料 (Logstash)、

檢索資料 (Elasticsearch) 並將

資料做視覺化呈現 (Kibana)。

Agenda

- Motivation
- Introduction Elasticsearch, Kibana and Logstash
- Import Data to Elasticsearch using Logstash
- Create Kibana Visualize
- Install Elasticsearch, Kibana and Logstash
- Reference

Motivation

What's the difference

Why use

?

Goal

How to make

Kibana

Elasticsearch Dashboard

Tableau

Data Visualization Tool

The difference between

Elasticsearch (Kibana) 、

MongoDB and Spark (Tableau)

Elasticsearch	Spark	MongoDB
Full Text Retrieval (Score Algorithm)	Parallel Computing (e.g. Real time predict such as linear regression)	Real time data retrieval
透過 Inverted Index (字典) 以及 Hash Function 來快速搜尋相關文字的資料	資料存放在 HDFS 裡，HDFS 以存放大資料為目的故檢索速度相較於一般 RDB or NoSQl 慢	透過 Hash Function 來加速搜尋時間

Inverted Index

- The quick brown fox jumped over the lazy dog
- Quick brown foxes leap over lazy dogs in summer

search quick brown

Term	Doc_1	Doc_2
brown	X	X
quick	X	
Total	2	1

Term	Doc_1	Doc_2
Quick		X
The	X	
brown	X	X
dog	X	
dogs		X
fox	X	
foxes		X
in		X
jumped	X	
lazy	X	X
leap		X
over	X	X
quick	X	
summer		X
the	X	

Introduction Elasticsearch

Elasticsearch

- 建立在全文搜索引擎 Lucene 基礎上
- REST API 串接
- 分散式 (Sharding)
- 查詢統計分析 (Aggregation and Filtering)

Introduction Kibana

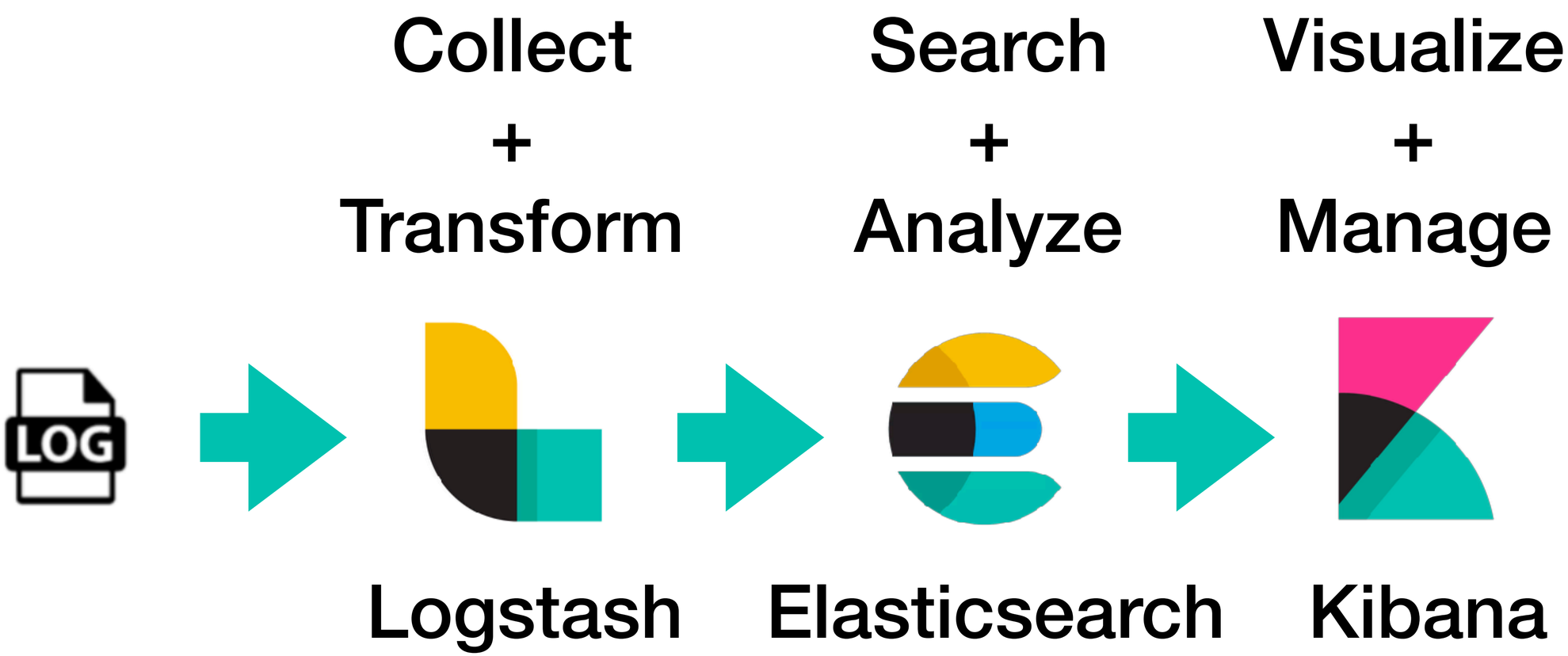
Kibana


kibana
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Discover
Visualize
Dashboard
Timelion
Machine Learning
Graph
Dev Tools
Monitoring
Management
Guest User
Logout
Collapse
Apache - Total Visitors
11,979,137
Apache - Unique Visitors
128,088
Unique Visitors
Apache - Bytes and Count
United States China France Germany India
Count
@timestamp per hour
Apache - Country and Status
United States China France Germany India
200 304 301 404 416 206 412
Apache - Unique Visitors by C...
City
Unique Visitors
Beijing 243,706
Woodbridge 134,791
Seattle 123,545
Seoul 111,663
Mumbai 109,801
Tokyo 106,182
New York 102,947
Apache - Country traffic by hour
United States
China
Germany
India
United Kingdom
Country
Hour of Day
Apache - Top OS
BlackBerry OS
Windows Phone
Windows 7
Windows 10
FreeBSD
Windows Vista
Mac OS X
Windows 8
Other
OpenBSD
Android
Linux
iOS
Fedora
Windows
Ubuntu
Windows 8.1
Windows 2000
Windows XP
Chrome OS
Apache - Visitor Map (geocentroid)
Calgary

Introduction Logstash

Logstash

- Elasticsearch 資料匯入或匯出工具
- 資料格式進行轉換或處理
- AWS SQS、DynamoDB (Amazon NoSQL)、FileSystem、Git、JDBC、Kafka、MongoDB、neo4j、Redis、Solr and Twitter


Collect
+
Transform
Search
+
Analyze
Visualize
+
Manage
LOG
Logstash
Elasticsearch
Kibana

ELK Stack (Elasticsearch + Logstash + Kibana)

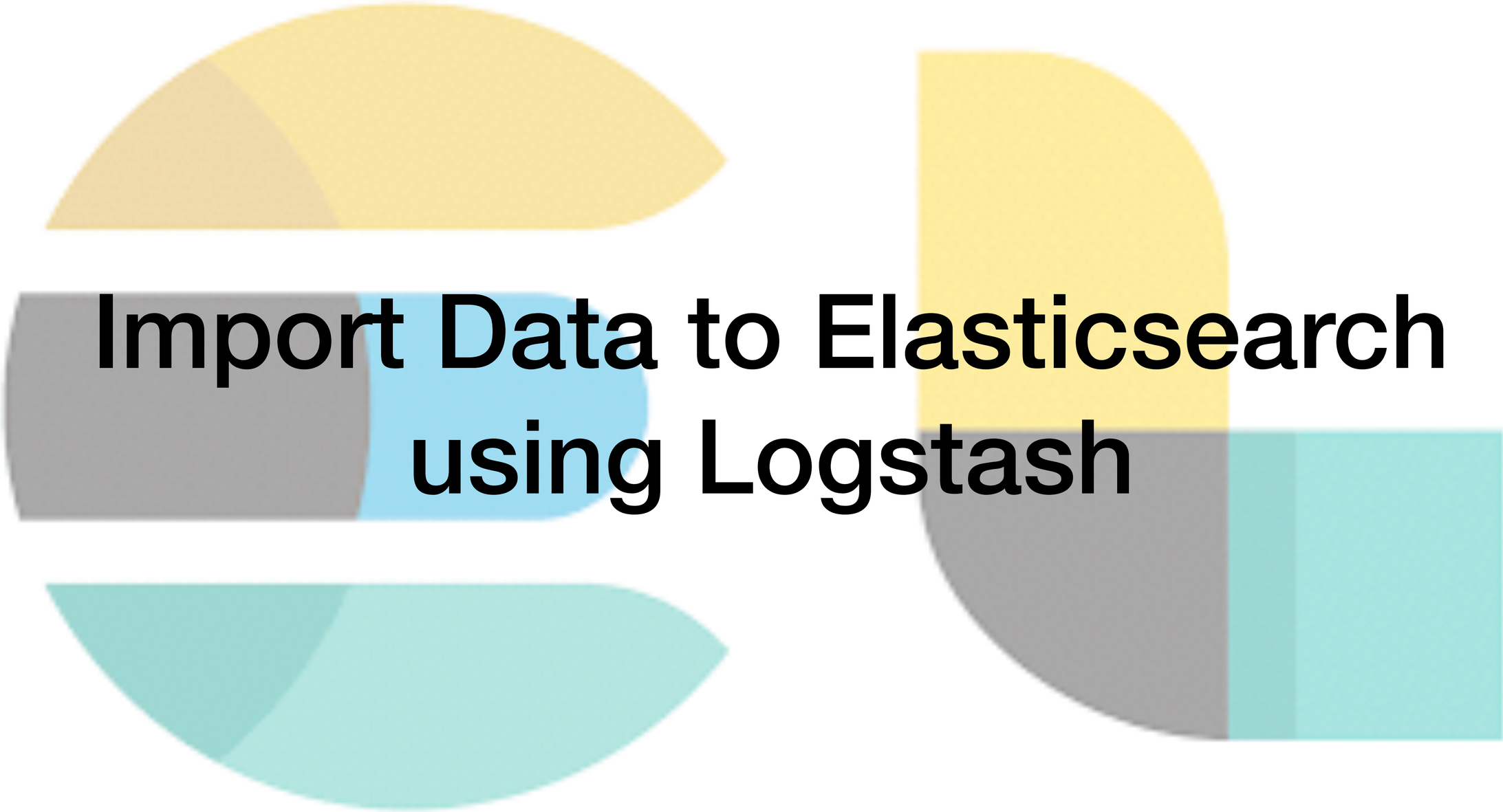
使用場景:

- 業務數據分析
- 錯誤日誌分析
- 數據預警
- 交易資料檢索

ELK Stack (Elasticsearch + Logstash + Kibana)

案例:

- GitHub: 搜索 20TB 的數據，包括 13 億文檔和 1300 億行代碼
- 維基百科: 核心搜索架構
- SoundCloud: 1.8 億用户提供即時而精準的音樂搜索服務
- 百度: 文本數據分析



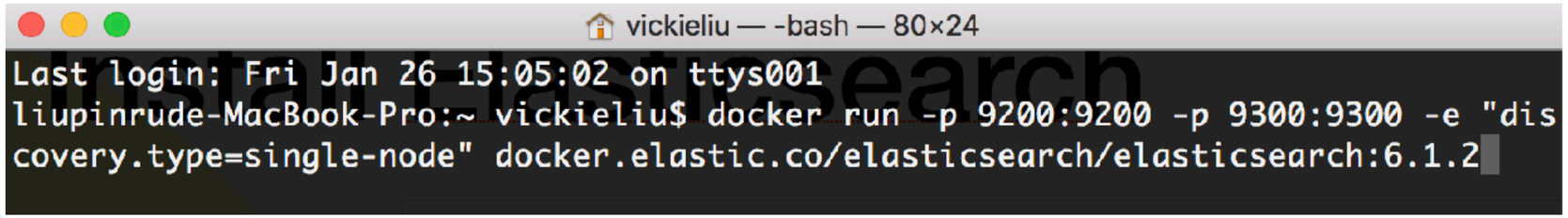
Import Data to Elasticsearch using Logstash

＊需確認 Elasticsearch、Kibana、Logstash 安裝完成

Step1: 啟動 Docker

Step2: 開啟 cmd 後貼上下方指令

```
docker run -p 9200:9200 -p 9300:9300 -e
"discovery.type=single-node" docker.elastic.co/
elasticsearch/elasticsearch:6.1.2
```



Step3: 在瀏覽器開啟

http://127.0.0.1:9200/

看到下方畫面則表示啟動成功，若出現紅色方框的內容則表示在執行步驟中有錯誤需修正


```
{
  "name" : "m8SVP2q",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "1VBLm1iaQLC3frF1hksB0w",
  "version" : {
    "number" : "6.1.2",
    "build_hash" : "5b1fea5",
    "build_date" : "2018-01-10T02:35:59.208Z",
    "build_snapshot" : false,
    "lucene_version" : "7.1.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Step4: 請進入 Logstash 資料夾

可看到路徑底下已存在 config，為了方便辨識

會建議建立一個新資料夾放置需要執行的 conf 檔

mkdir conf.d

```
liupinrude-MacBook-Pro:resources vickieliu$ ls
PyPubSub                kibana-6.1.2            spark
elasticsearch-6.0.0     logstash-6.1.2
kafka                   mongodb
liupinrude-MacBook-Pro:resources vickieliu$ cd logstash-6.1.2/
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$ ls
CONTRIBUTORS                    data
Gemfile                         lib
Gemfile.lock                    logs
LICENSE                         logstash-core
NOTICE.TXT                      logstash-core-plugin-api
bin                             modules
conf.d                          tools
config                          vendor
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$
```

Step5: 建立一個新的 conf 檔

vim conf.d/test1.conf

這裡需要特別注意一件事，若路徑中存在中文名稱可能會導致讀檔失敗，建議在使用 ELK 時，命名路徑與檔名等，盡可能使用小寫英文字母與 _ 進行命名！

test1.conf

```
input {
    file {
        path => "/Users/vickieliu/Downloads/train_users_2.csv"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}
filter {
    csv {
        separator => ","
        columns => ["id", "date_account_created", "timestamp_first_active",
        "date_first_booking", "gender", "age", "signup_method", "signup_flow",
        "language", "affiliate_channel", "affiliate_provider",
        "first_affiliate_tracked", "signup_app", "first_device_type",
        "first_browser", "country_destination"]
  }

}
output {
    elasticsearch {
            hosts => ["localhost:9200"]  #"http://localhost:9200"
    }
    stdout {
        codec => rubydebug{ }
    }
}
```

Input

file
path、start_position、
sincedb_path

kafka
監聽資訊

stdin
自行輸入

test1.conf

```
input {
    file {
        path => "/Users/vickieliu/Downloads/train_users_2.csv"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}
filter {
    csv {
        separator => ","
        columns => ["id", "date_account_created", "timestamp_first_active",
        "date_first_booking", "gender", "age", "signup_method", "signup_flow",
        "language", "affiliate_channel", "affiliate_provider",
        "first_affiliate_tracked", "signup_app", "first_device_type",
        "first_browser", "country_destination"]
  }

}
output {
    elasticsearch {
            hosts => ["localhost:9200"]  #"http://localhost:9200"
    }
    stdout {
        codec => rubydebug{ }
    }
}
```

Filter

csv
separator、columns

grok
定義資料格式

mutate
資料型態轉換

geoip
地理位置

test1.conf

```
input {
    file {
        path => "/Users/vickieliu/Downloads/train_users_2.csv"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}
filter {
    csv {
        separator => ","
        columns => ["id", "date_account_created", "timestamp_first_active",
        "date_first_booking", "gender", "age", "signup_method", "signup_flow",
        "language", "affiliate_channel", "affiliate_provider",
        "first_affiliate_tracked", "signup_app", "first_device_type",
        "first_browser", "country_destination"]
  }

}
output {
    elasticsearch {
            hosts => ["localhost:9200"]  #"http://localhost:9200"
    }
    stdout {
        codec => rubydebug{ }
    }
}
```

Output

elasticsearch
hosts、index

stdout
輸出結果

test1.conf

```
input {
    file {
        path => "/Users/vickieliu/Downloads/train_users_2.csv"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}
filter {
    csv {
        separator => ","
        columns => ["id", "date_account_created", "timestamp_first_active",
        "date_first_booking", "gender", "age", "signup_method", "signup_flow",
        "language", "affiliate_channel", "affiliate_provider",
        "first_affiliate_tracked", "signup_app", "first_device_type",
        "first_browser", "country_destination"]
  }

}
output {
    elasticsearch {
            hosts => ["localhost:9200"]  #"http://localhost:9200"
    }
    stdout {
        codec => rubydebug{ }
    }
}
```

Step6: conf 檔已照需求編輯好後

請確認已啟動 Elasticsearch 和 Kibana

即可在 Logstash 資料夾執行指令

./bin/logstash -f **conf 檔絕對路徑**

ex:

./bin/logstash -f /Users/vickieliu/Developer/resources/logstash-6.1.2/conf.d/test1.conf

Step7: 已經執行一個 conf 檔
想再執行另一個 conf 檔
需將 Logstash Shutdown
確認現在運作中的 Logstash 停止運作

```
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$ ps aux | grep logstash
vickieliu         3856  10.0  5.5  6965588 457852 s003  S+    2:38下午   1:28.47 /usr/bin/java -XX:+UseParNewGC -
XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headle
ss=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -Djruby.jit.threshold=0 -XX:+HeapDumpOnOutOfMemo
ryError -Djava.security.egd=file:/dev/urandom -Xmx1g -Xms1g -Xss2048k -Djffi.boot.library.path=/Users/vickieliu/D
eveloper/resources/logstash-6.1.2/vendor/jruby/lib/jni -Dfile.encoding=UTF-8 -Xbootclasspath/a:/Users/vickieliu/D
eveloper/resources/logstash-6.1.2/vendor/jruby/lib/jruby.jar -classpath : -Djruby.home=/Users/vickieliu/Developer
/resources/logstash-6.1.2/vendor/jruby -Djruby.lib=/Users/vickieliu/Developer/resources/logstash-6.1.2/vendor/jru
by/lib -Djruby.script=jruby -Djruby.shell=/bin/sh org.jruby.Main /Users/vickieliu/Developer/resources/logstash-6.
1.2/lib/bootstrap/environment.rb logstash/runner.rb -f /Users/vickieliu/Developer/resources/logstash-6.1.2/conf.d
/test8.conf
vickieliu         3885   0.0  0.0  4276968    884 s002  S+    2:40下午   0:00.01 grep logstash
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$ kill -9 3856
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$
```

Step8: 請到 Kibana 資料夾執行指令
./bin/kibana

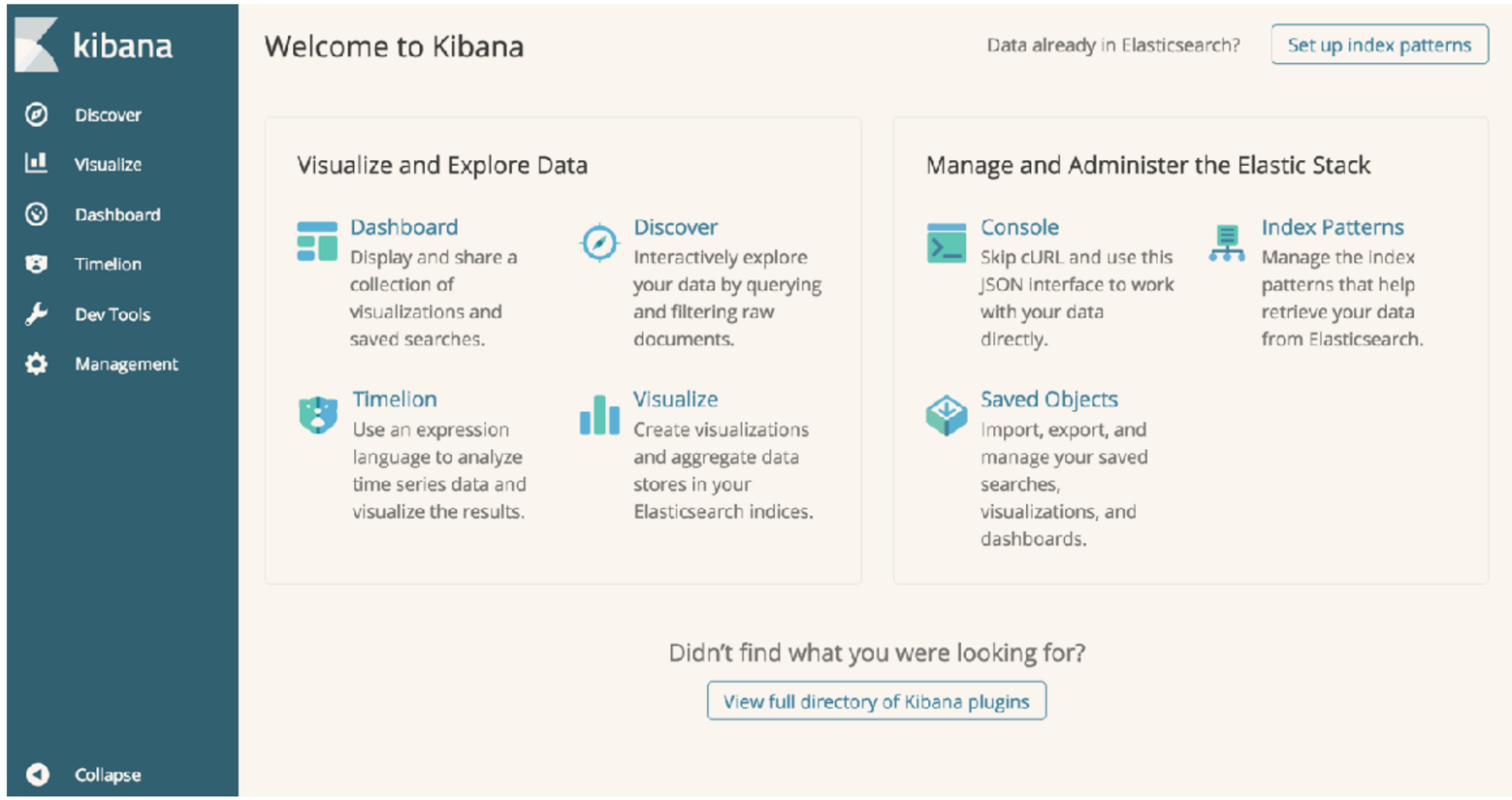
```
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ ls
LICENSE.txt     bin             node            package.json    ui_framework
NOTICE.txt      config          node_modules    plugins         webpackShims
README.txt      data            optimize        src
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ ./bin/kibana
```

```
  log   [08:43:31.159] [info][status][plugin:kibana@6.1.2] Status changed from u
ninitialized to green - Ready
  log   [08:43:31.204] [info][status][plugin:elasticsearch@6.1.2] Status changed
 from uninitialized to yellow - Waiting for Elasticsearch
  log   [08:43:31.235] [info][status][plugin:console@6.1.2] Status changed from
uninitialized to green - Ready
  log   [08:43:31.256] [info][status][plugin:metrics@6.1.2] Status changed from
uninitialized to green - Ready
  log   [08:43:31.564] [info][status][plugin:timelion@6.1.2] Status changed from
 uninitialized to green - Ready
  log   [08:43:31.569] [info][listening] Server running at http://localhost:5601
  log   [08:43:31.579] [info][status][plugin:elasticsearch@6.1.2] Status changed
 from yellow to green - Ready
```

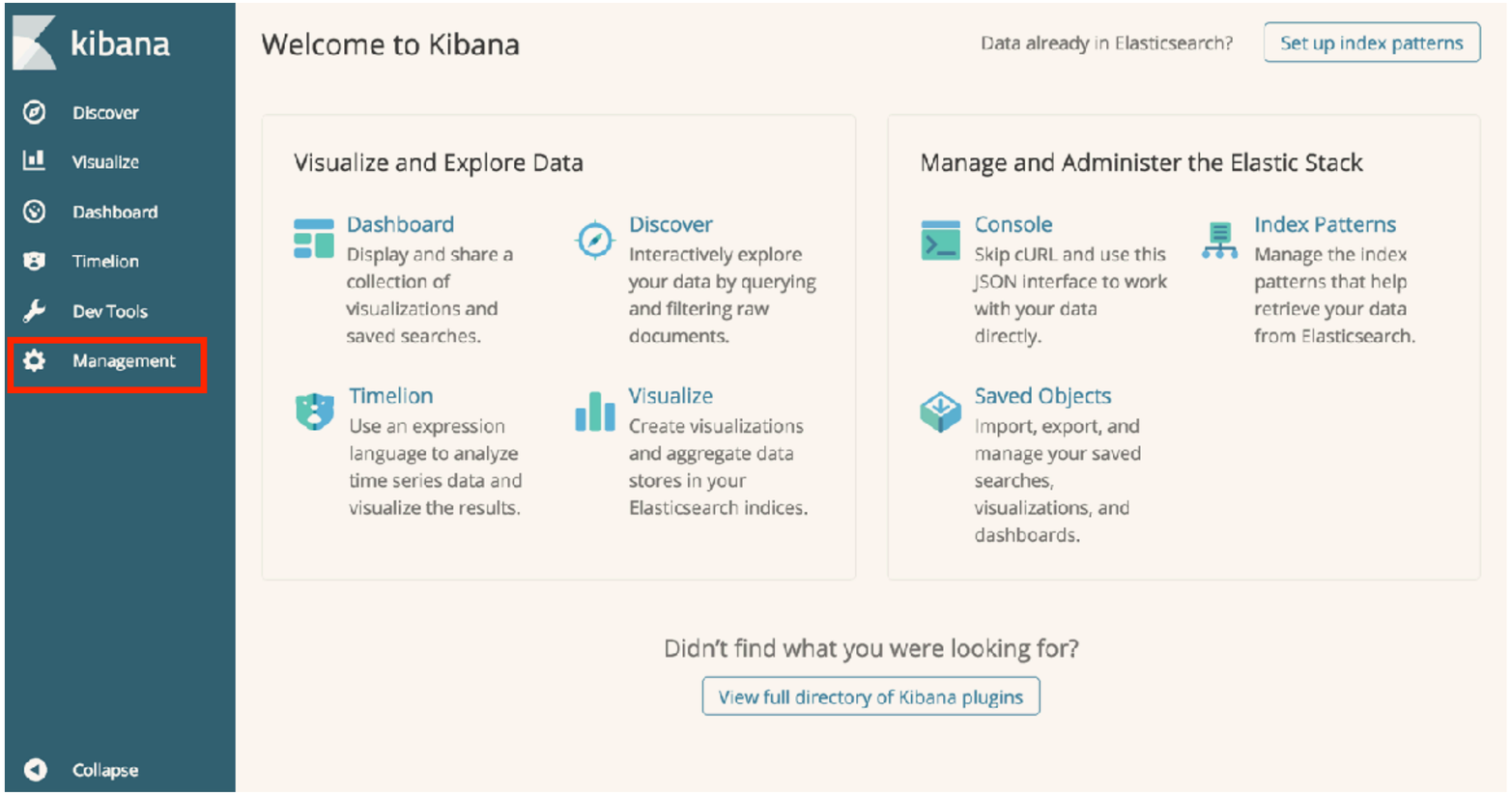
Step9: 在瀏覽器開啟

http://127.0.0.1:5601/

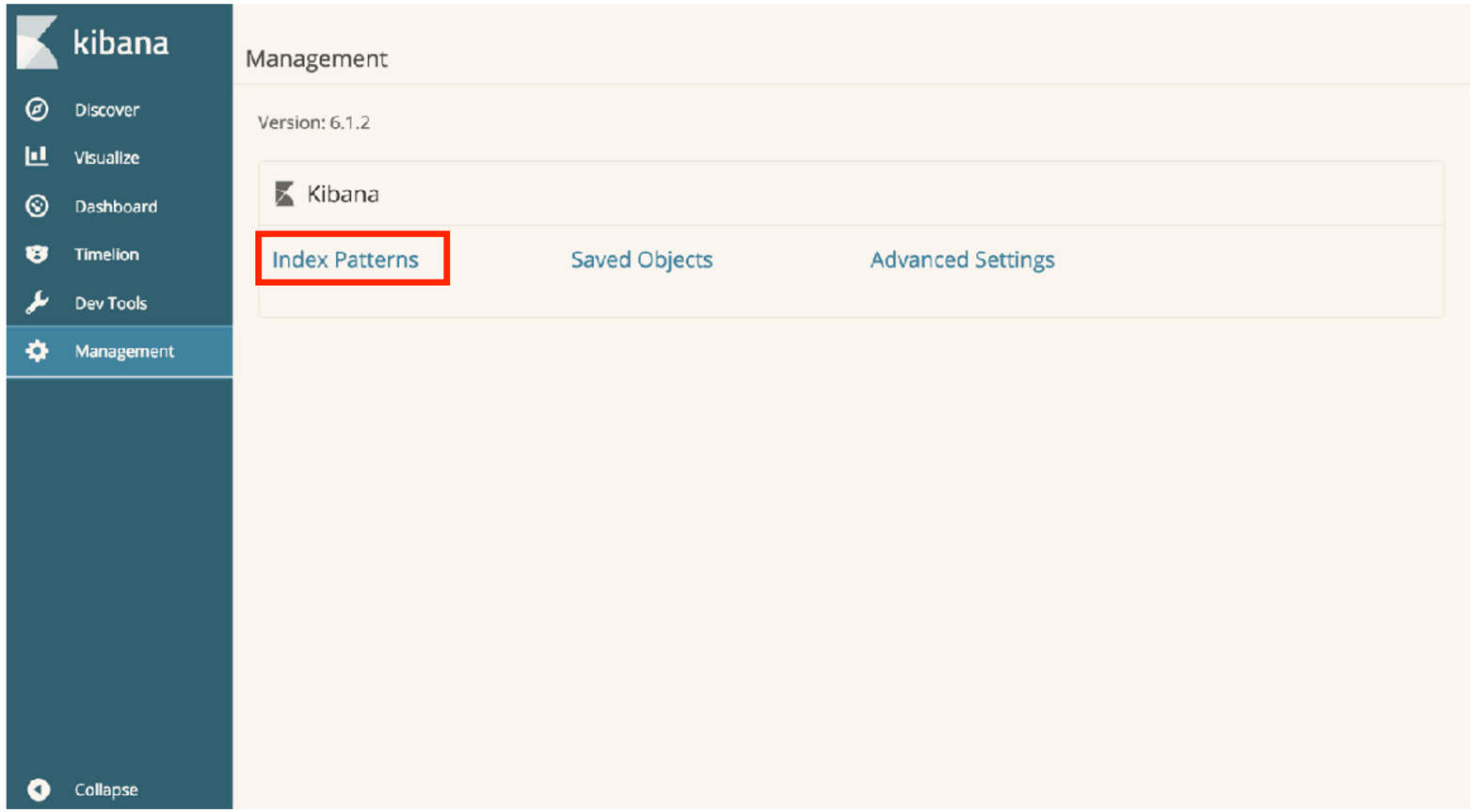
看到下方畫面則表示啟動成功



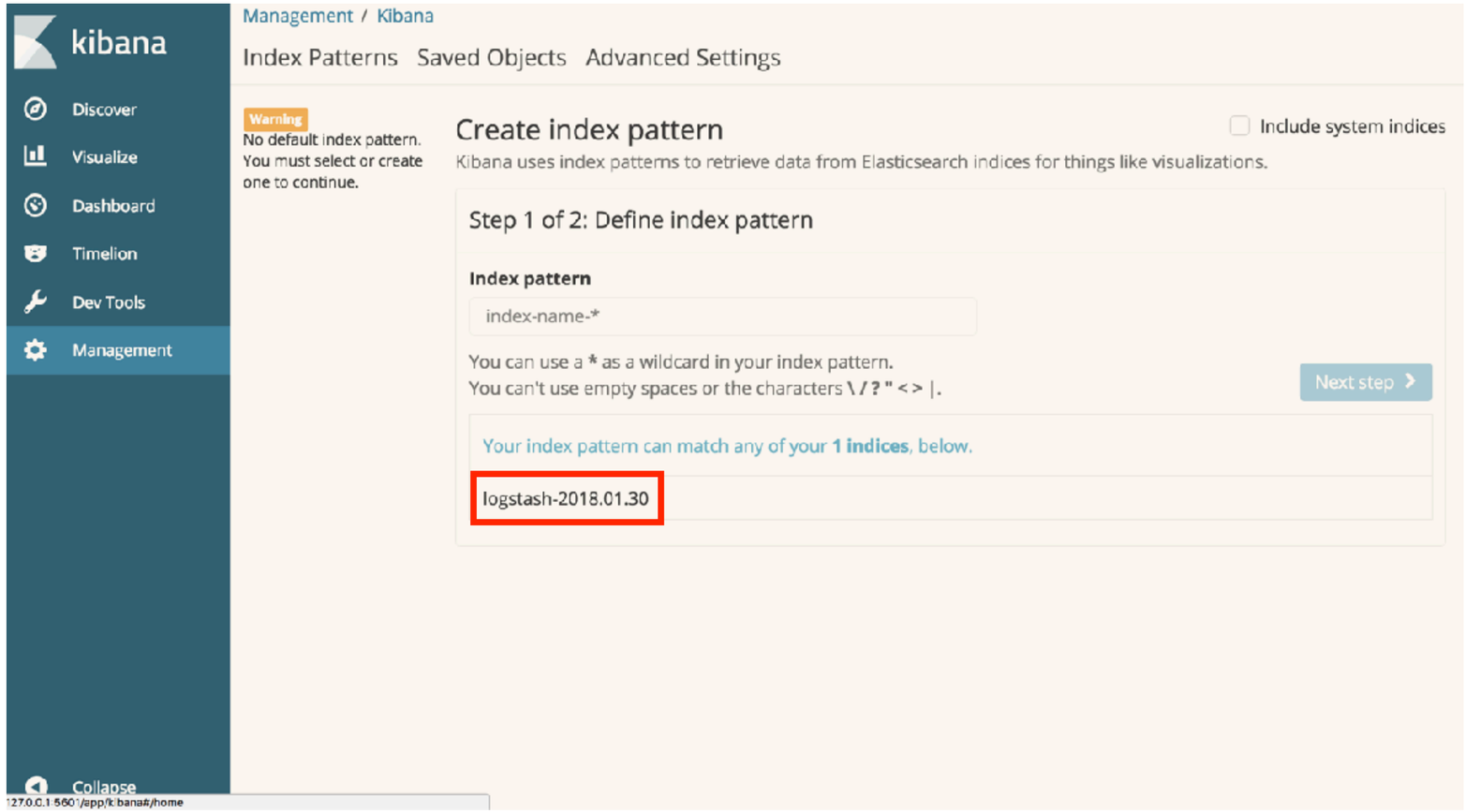
Step10: 點選 Management



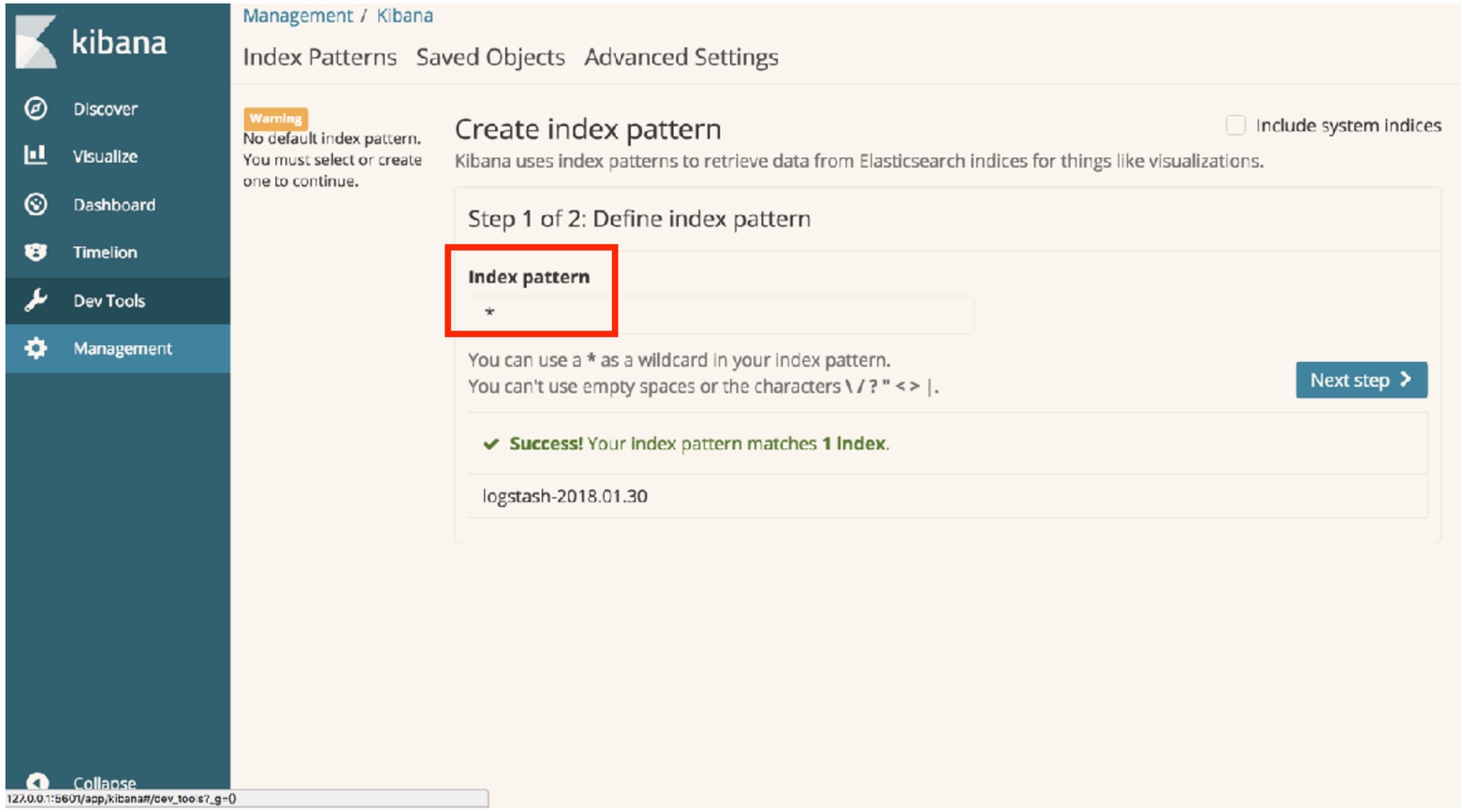
Step11: 點選 Index Patterns



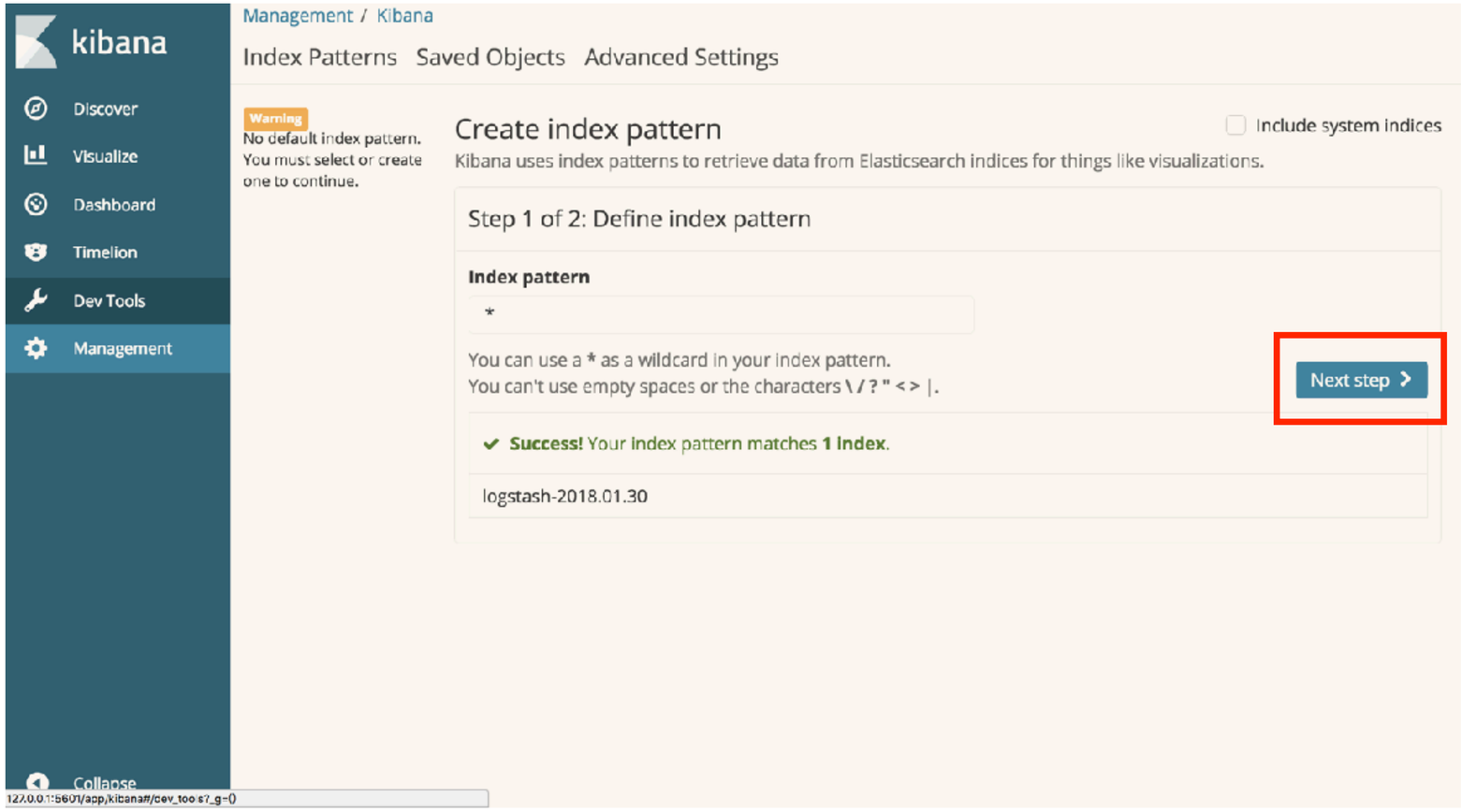
由於在 Logstash 的 test1.conf 檔 output 中未設定 index 所以命名為系統預設 logstash-導入日期



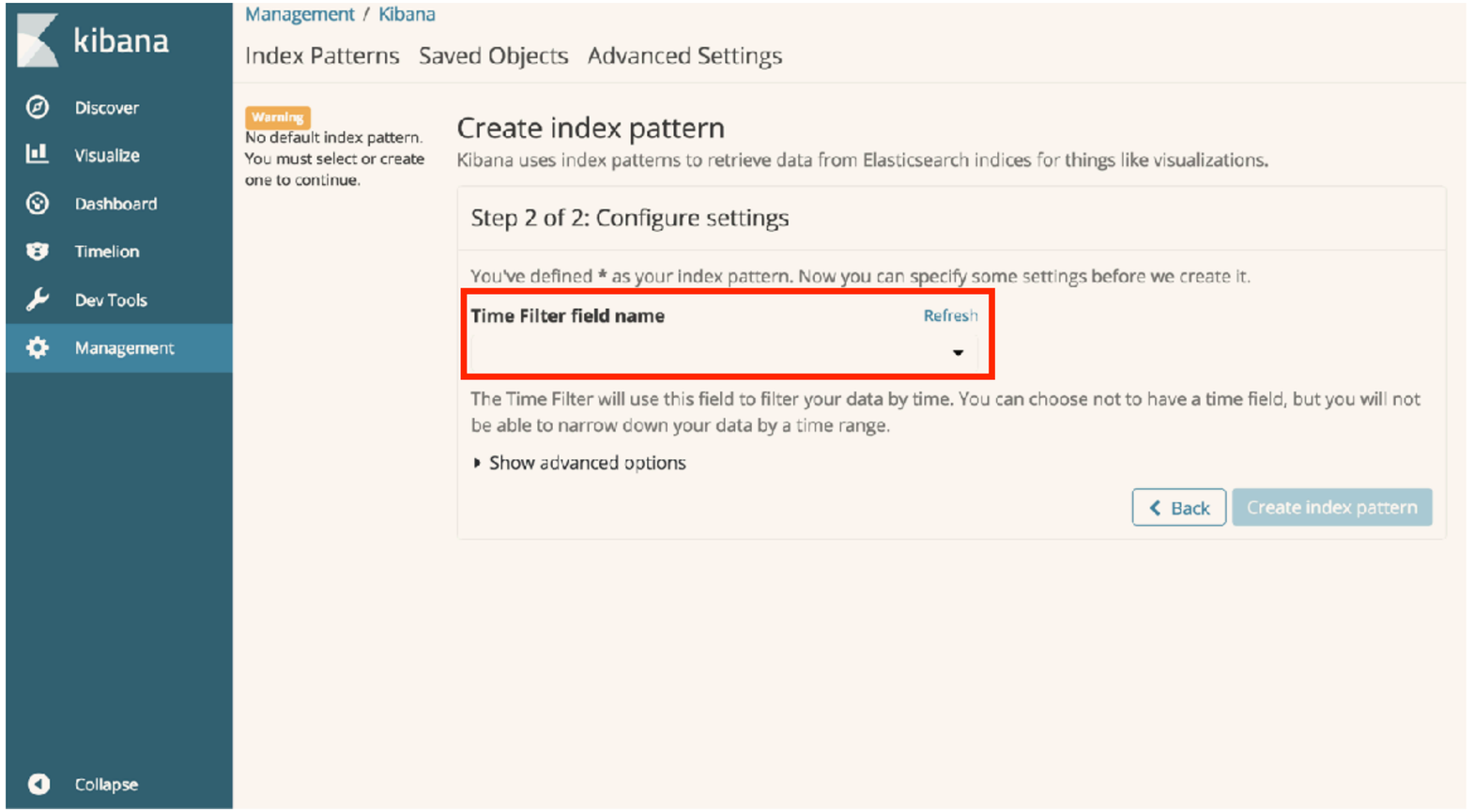
Step12: 在 Index Patterns 中輸入命名名稱
* 等同於選取全部



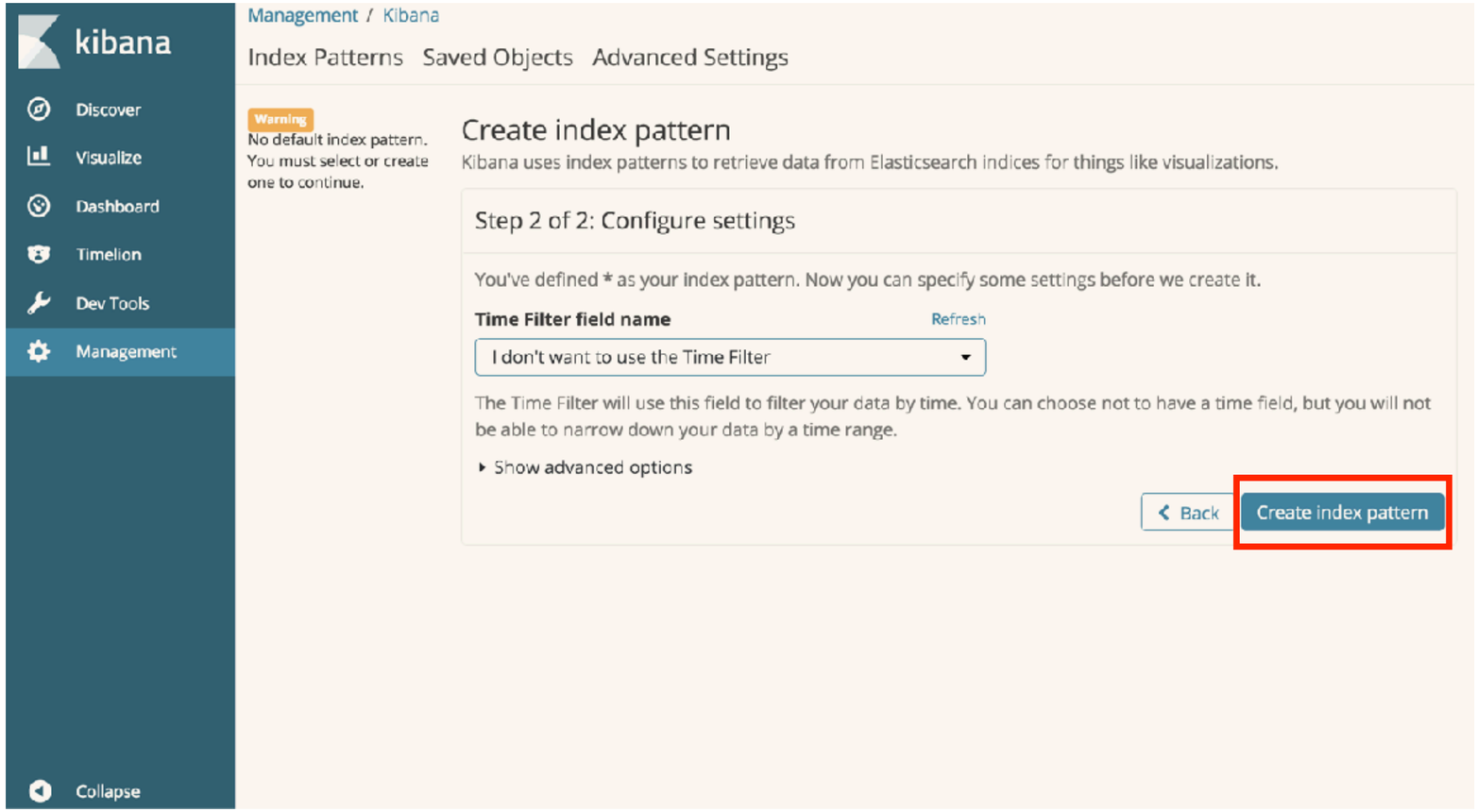
Step13: 出現 “Success! Your index pattern matches 1 index” 等字樣即可按 Next step



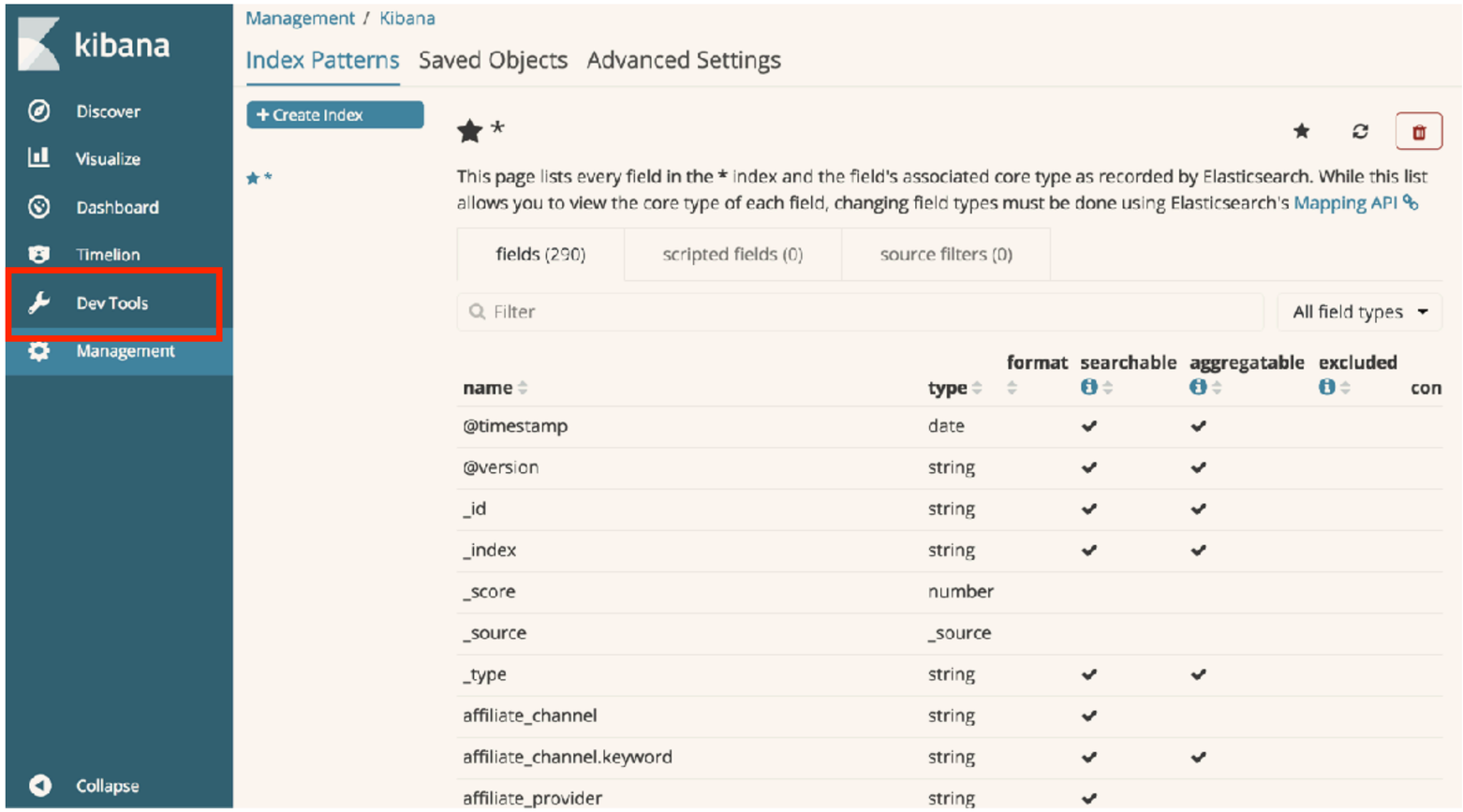
設定配置，Time Filter field name 有下拉式選單可以選取
若未特別設定 @timestamp 則會是導入日期

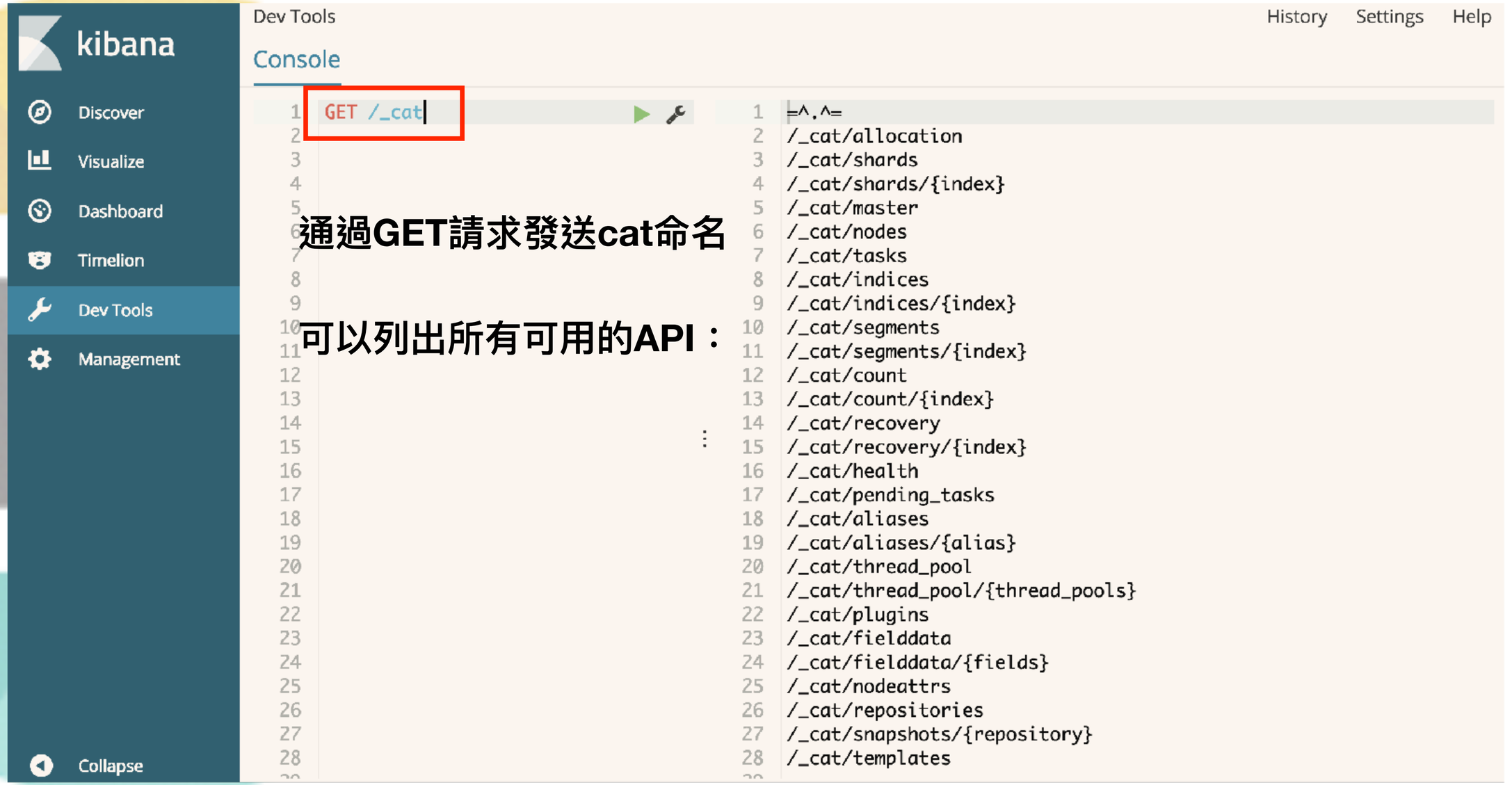


Step14: 由於這組 Data 並未設定 @timestamp
可以選擇 “I don’t want to use the Time Filter”
按下 Create Index pattern



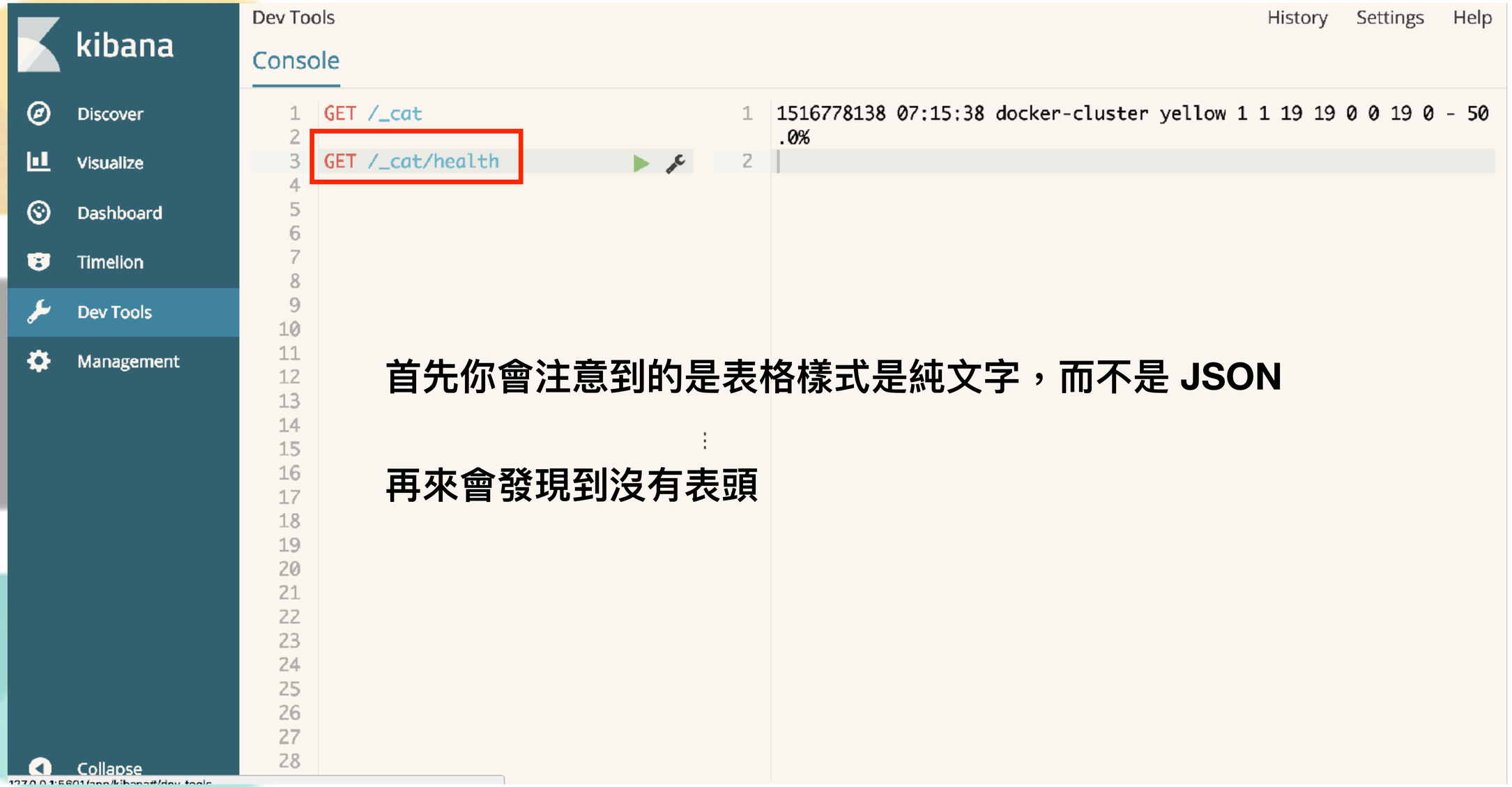
可以看到 Kibana 中已存在剛建立的資料
透過 Discover 索引資料或 Visualize 繪製資料
接下來講一下關於 Dev Tools 中 Cat API 的使用



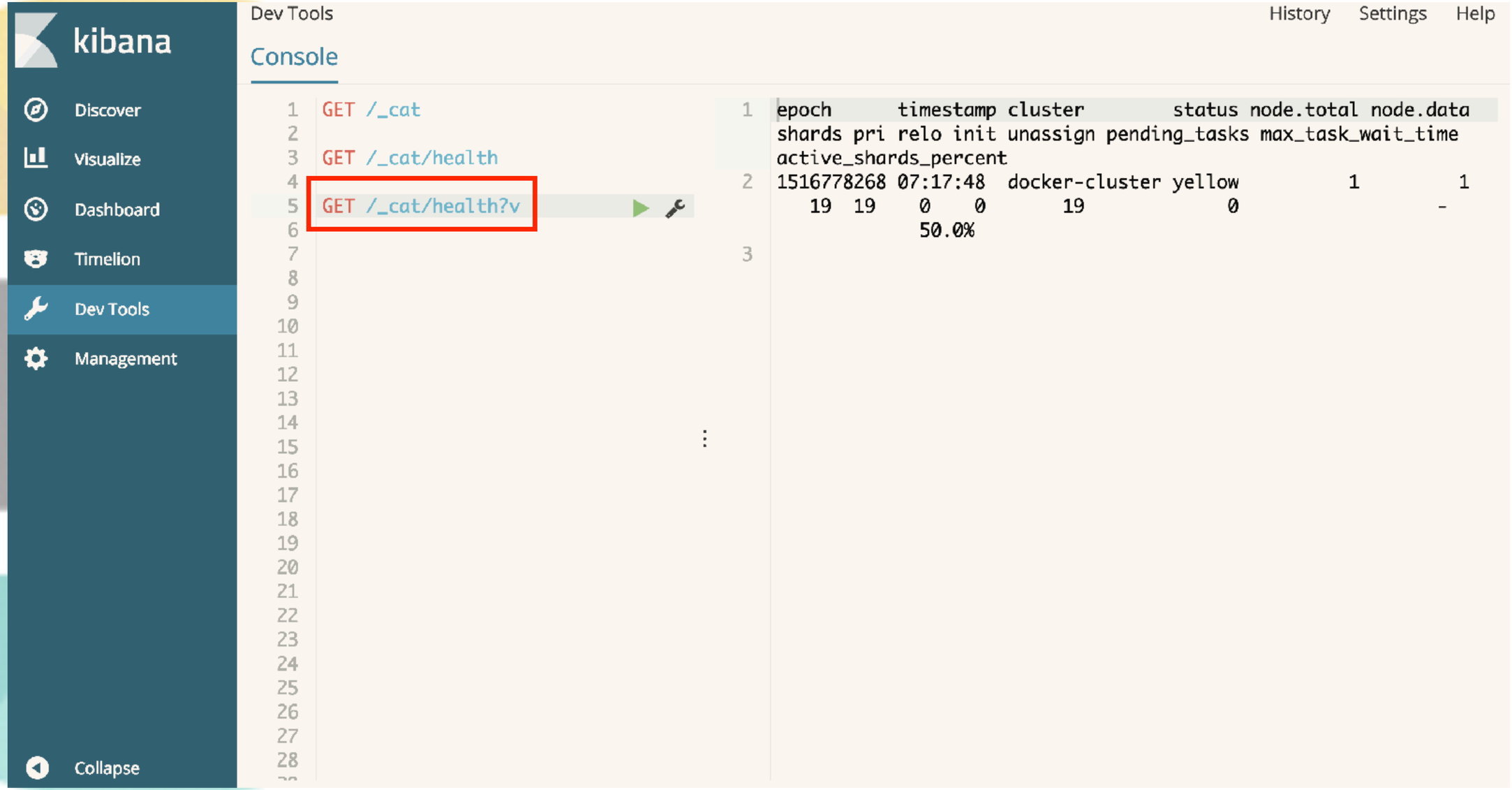


通過GET請求發送cat命名

可以列出所有可用的API：


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
GET /_cat
GET /_cat/health
1516778138 07:15:38 docker-cluster yellow 1 1 19 19 0 0 19 0 - 50.0%
首先你會注意到的是表格樣式是純文字，而不是 JSON
再來會發現到沒有表頭

要啟用表頭，加上 ?v 即可


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
GET /_cat
GET /_cat/health
GET /_cat/health?v
epoch timestamp cluster status node.total node.data shards pri relo init unassign pending_tasks max_task_wait_time active_shards_percent
1516778268 07:17:48 docker-cluster yellow 1 1 19 19 0 0 19 0 - 50.0%


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
看現有的 Logstash 有哪些
GET /_cat
GET /_cat/health
GET /_cat/health?v
GET /_cat/nodes?v
GET /_cat/nodes?help
GET /_cat/nodes?v&h=ip,port,heapPercent,heapMax
GET /_cat/indices?v
health status index uuid pri rep docs.count docs.deleted store.size pri.store.size
yellow open .monitoring-es-6-2018.01.24 dyCjjss3RyyTlG4oNgfGmA 1 1 17992 228 8mb 8mb
yellow open nyc ZFz1UAl3Rzud_PQ3dgIrRw 5 1 2122440 0 1.4gb 1.4gb
yellow open logstash-2018.01.24 lNQS0eocQuKrr_cBk17e4w 5 1 628327 0 157.1mb 157.1mb
yellow open logstash-2018.01.23 nY5bDdEJQB2U5a7qAIi29A 5 1 752808 0 188.3mb 188.3mb
yellow open .kibana Yuyikeo0Q5SLyp68TUShHA 1 1 4 0 38.6kb 38.6kb
yellow open .monitoring-es-6-2018.01.22 0tiXa2c3TfWRTjsR2tEEXg 1 1 7975 12 3mb 3mb
yellow open .monitoring-es-6-2018.01.23 arAo5dYlRL2mjNG_ybemqg 1 1 26859 182 10.5mb 10.5mb


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
GET /_cat
GET /_cat/health
GET /_cat/health?v
GET /_cat/nodes?v
GET /_cat/nodes?help
GET /_cat/nodes?v&h=ip,port,heapPercent,heapMax
GET /_cat/indices?v
GET _search
{
"query": {
"match_all": {}
}
}
{
"took": 23,
"timed_out": false,
"_shards": {
"total": 19,
"successful": 19,
"skipped": 0,
"failed": 0
},
"hits": {
"total": 3556449,
"max_score": 1,
"hits": [
{
"_index": ".kibana",
"_type": "doc",
"_id": "config:6.1.2",
"_score": 1,
"_source": {
"type": "config",
"updated_at": "2018-01-23T06:50:26.338Z",
"config": {
"buildNum": 16363,
"defaultIndex": "afee8430-0009-11e8-a196-cfbf7ba467d8"
}
}
},

檢索 Data

定義檢索 Data 方式


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
GET /_cat
GET /_cat/health
GET /_cat/health?v
GET /_cat/nodes?v
GET /_cat/nodes?help
GET /_cat/nodes?v&h=ip,port,heapPercent,heapMax
GET /_cat/indices?v
GET _search
{
"query": {
"match_all": {}
}
}
GET /logstash-2018.01.23/_search
{
"query": {"match":{
"id":"gxn3p5htnn"
}}
}
{
"took": 53,
"timed_out": false,
"_shards": {
"total": 5,
"successful": 5,
"skipped": 0,
"failed": 0
},
"hits": {
"total": 8,
"max_score": 11.518404,
"hits": [
{
"_index": "logstash-2018.01.23",
"_type": "doc",
"_id": "LdFjImEB4zpcysM7mb92",
"_score": 11.518404,
"_source": {
"path": "/Users/vickieliu/Downloads/train_users_2.csv",
"signup_flow": "0",
"date_account_created": "2010/6/28",
"affiliate_provider": "direct",
"gender": "-unknown-",
"date_first_booking": null,
"@timestamp": "2018-01-23T09:40:04.935Z",
"id": "gxn3p5htnn",

藉由查找出的資訊反檢索 Data

尋找特定 Data


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
16 {
17 "query": {
18 "match_all": {}
19 }
20 }
21
22 GET /logstash-2018.01.23/_search
23 {
24 "query": {"match":{
25 "id":"gxn3p5htnn"
26 }}
27 }
28
29 GET /nyc/_search
30 {
31 "query": {
32 "match_all": {}
33 }
34 }
35
36 GET /nyc/doc/8tW6ImEB4zpcysM75k1c
37
38
39
40
41
42
43
1 {
2 "_index": "nyc",
3 "_type": "doc",
4 "_id": "8tW6ImEB4zpcysM75k1c",
5 "_version": 1,
6 "found": true,
7 "_source": {
8 "path": "/Users/vickieliu/Downloads/ny_taxi/train.csv",
9 "@version": "1",
10 "@timestamp": "2018-01-23T11:15:21.777Z",
11 "vendor_id": "2",
12 "pickup_longitude": "-73.95611572265625",
13 "id": "id3491576",
14 "store_and_fwd_flag": "N",
15 "dropoff_datetime": "2016-01-14 10:10:49",
16 "dropoff_latitude": "40.760963439941406",
17 "host": "liupinrude-MacBook-Pro.local",
18 "passenger_count": "1",
19 "message": "id3491576,2,2016-01-14 09:54:51,2016-01-14 10
:10:49,1,-73.95611572265625,40.767623901367187,-73.970970153808
594,40.760963439941406,N,958",
20 "pickup_datetime": "2016-01-14 09:54:51",
21 "dropoff_longitude": "-73.970970153808594",
22 "pickup_latitude": "40.767623901367187",
23 "trip_duration": "958"
24 }
25 }

Kibana Visualize

＊需確認 Elasticsearch、Kibana、Logstash 安裝完成

Step1: 請到 Kibana 資料夾執行指令
./bin/kibana

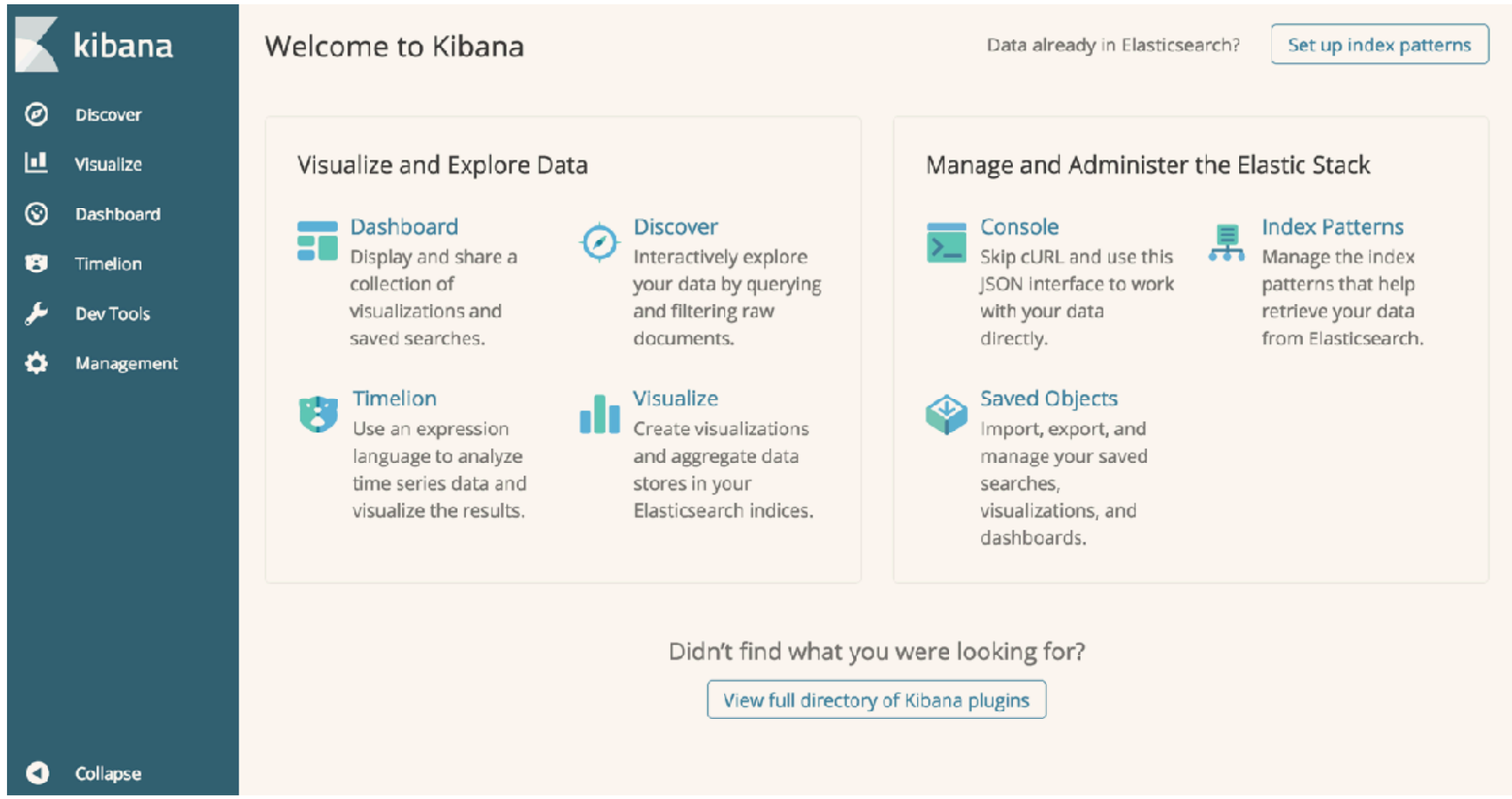
```
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ ls
LICENSE.txt     bin             node            package.json    ui_framework
NOTICE.txt      config          node_modules    plugins         webpackShims
README.txt      data            optimize        src
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ ./bin/kibana
```

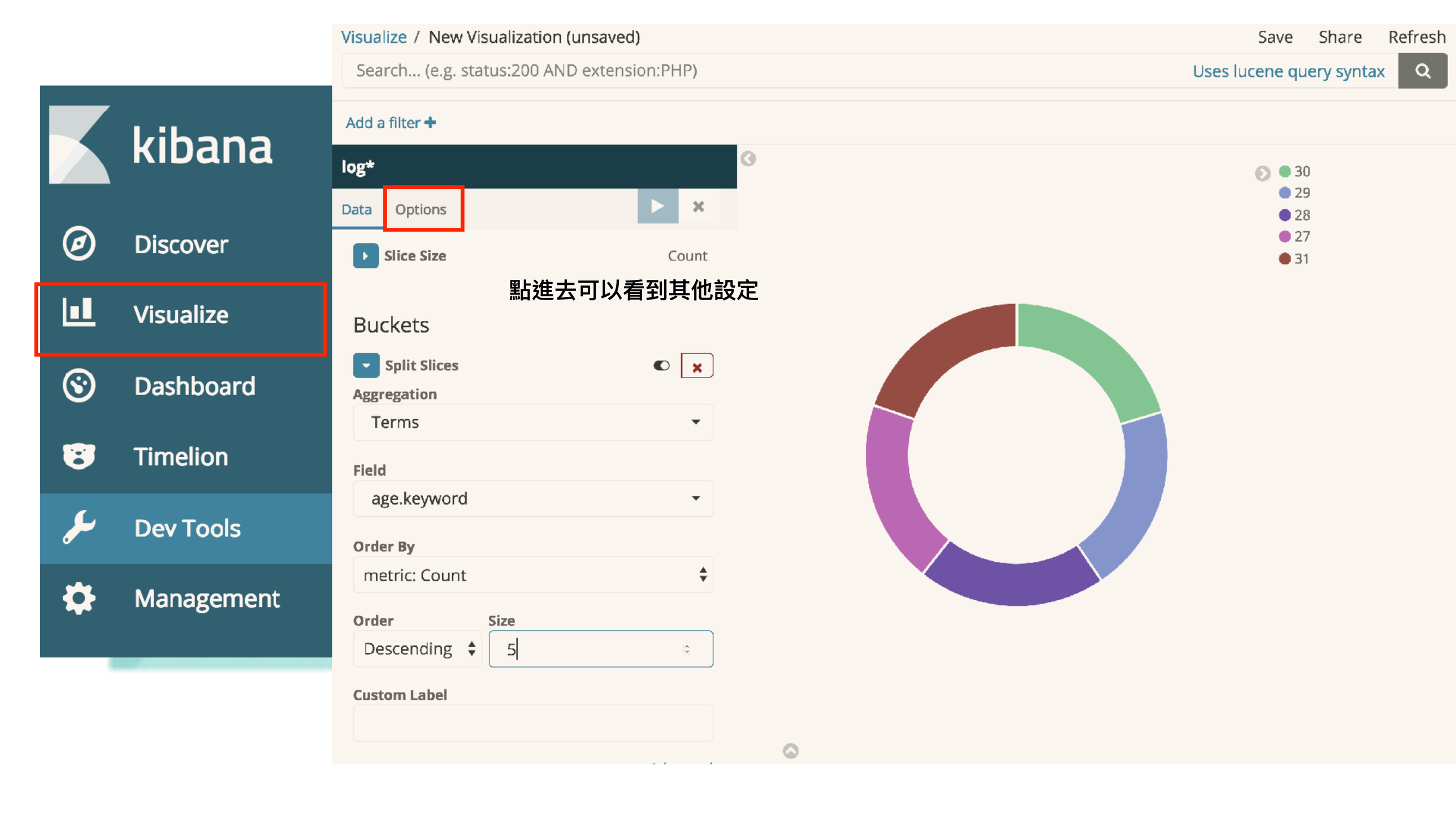
```
  log   [08:43:31.159] [info][status][plugin:kibana@6.1.2] Status changed from u
ninitialized to green - Ready
  log   [08:43:31.204] [info][status][plugin:elasticsearch@6.1.2] Status changed
 from uninitialized to yellow - Waiting for Elasticsearch
  log   [08:43:31.235] [info][status][plugin:console@6.1.2] Status changed from
uninitialized to green - Ready
  log   [08:43:31.256] [info][status][plugin:metrics@6.1.2] Status changed from
uninitialized to green - Ready
  log   [08:43:31.564] [info][status][plugin:timelion@6.1.2] Status changed from
 uninitialized to green - Ready
  log   [08:43:31.569] [info][listening] Server running at http://localhost:5601
  log   [08:43:31.579] [info][status][plugin:elasticsearch@6.1.2] Status changed
 from yellow to green - Ready
```

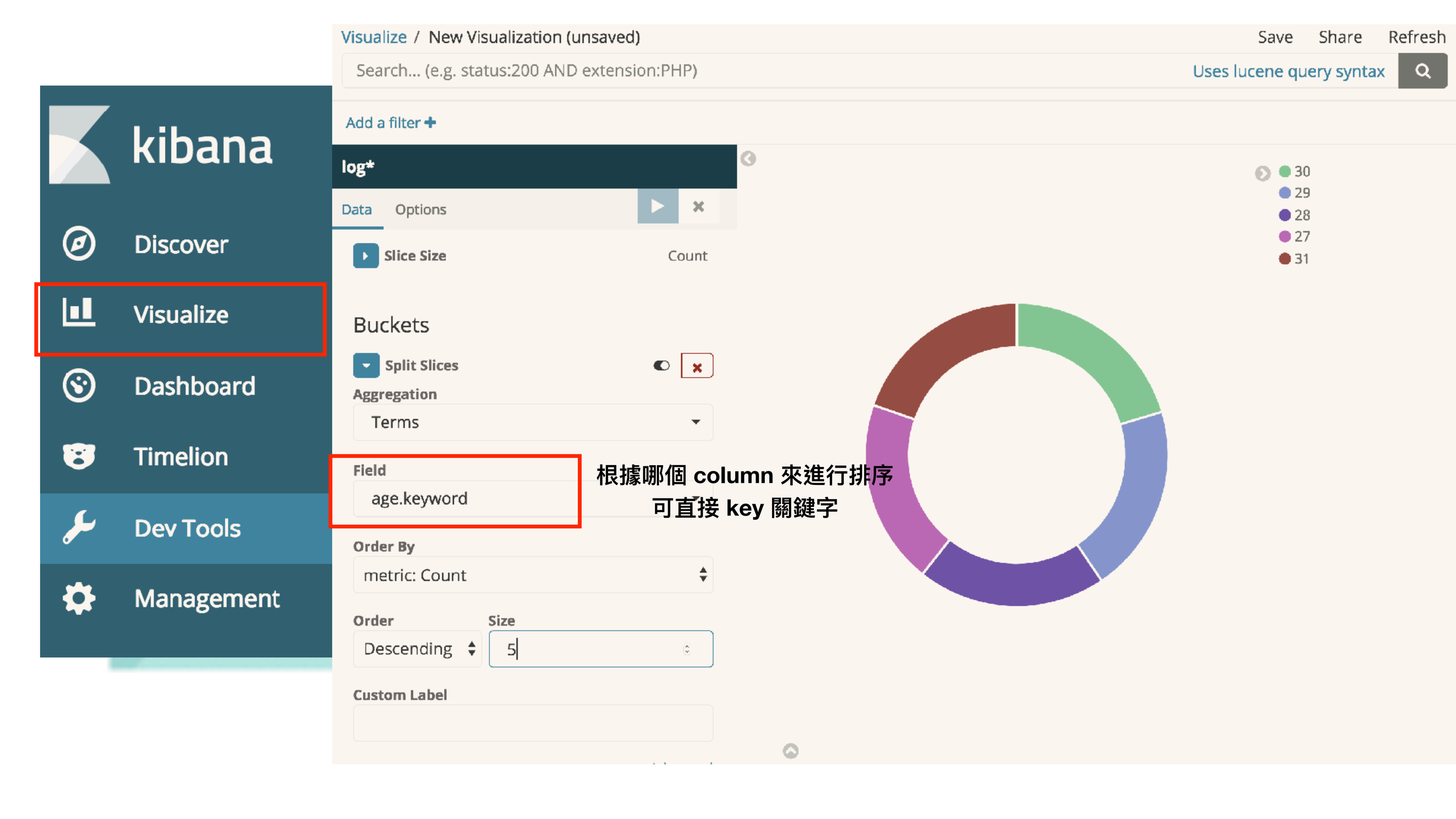
Step2: 在瀏覽器開啟

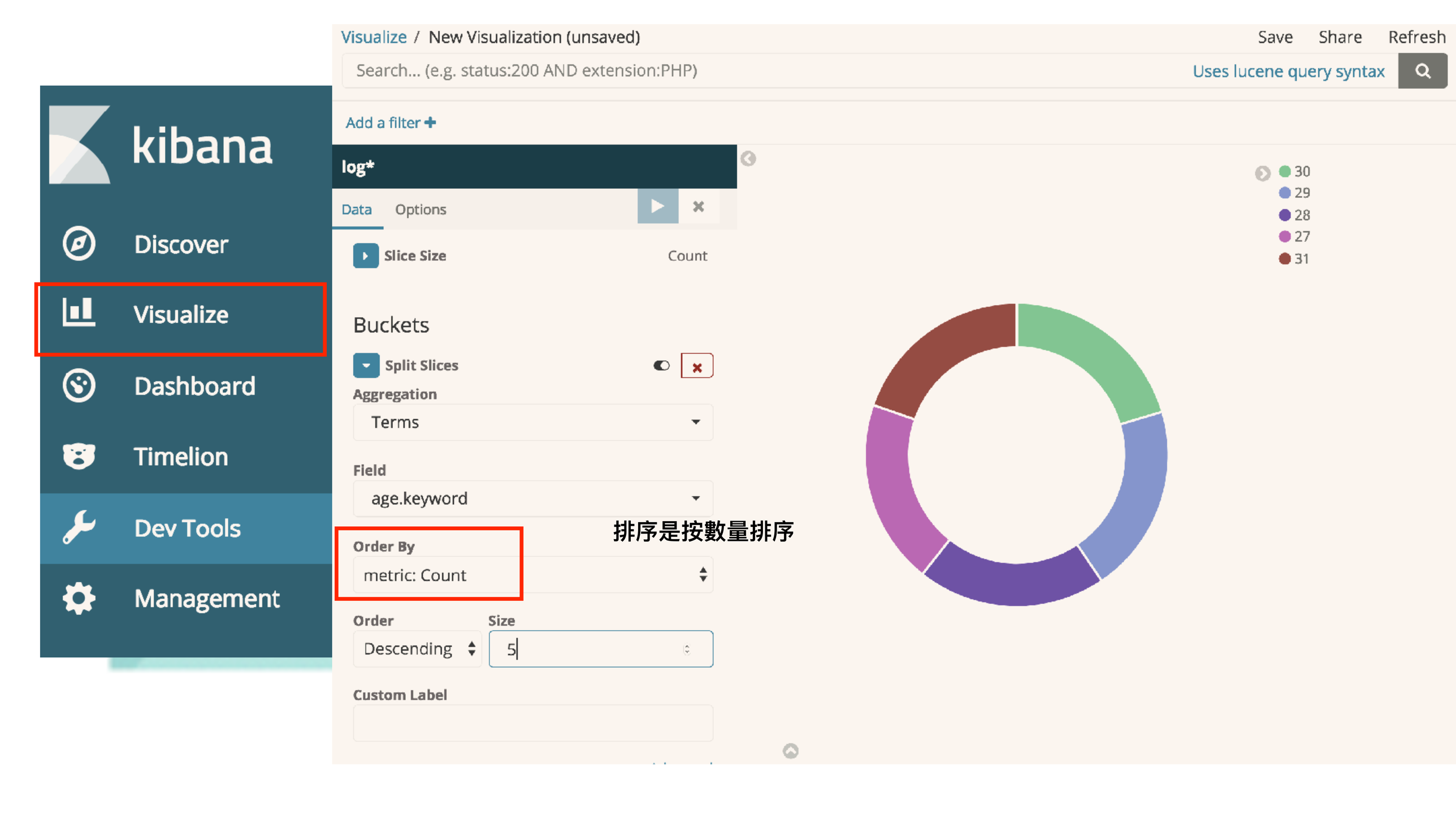
http://127.0.0.1:5601/

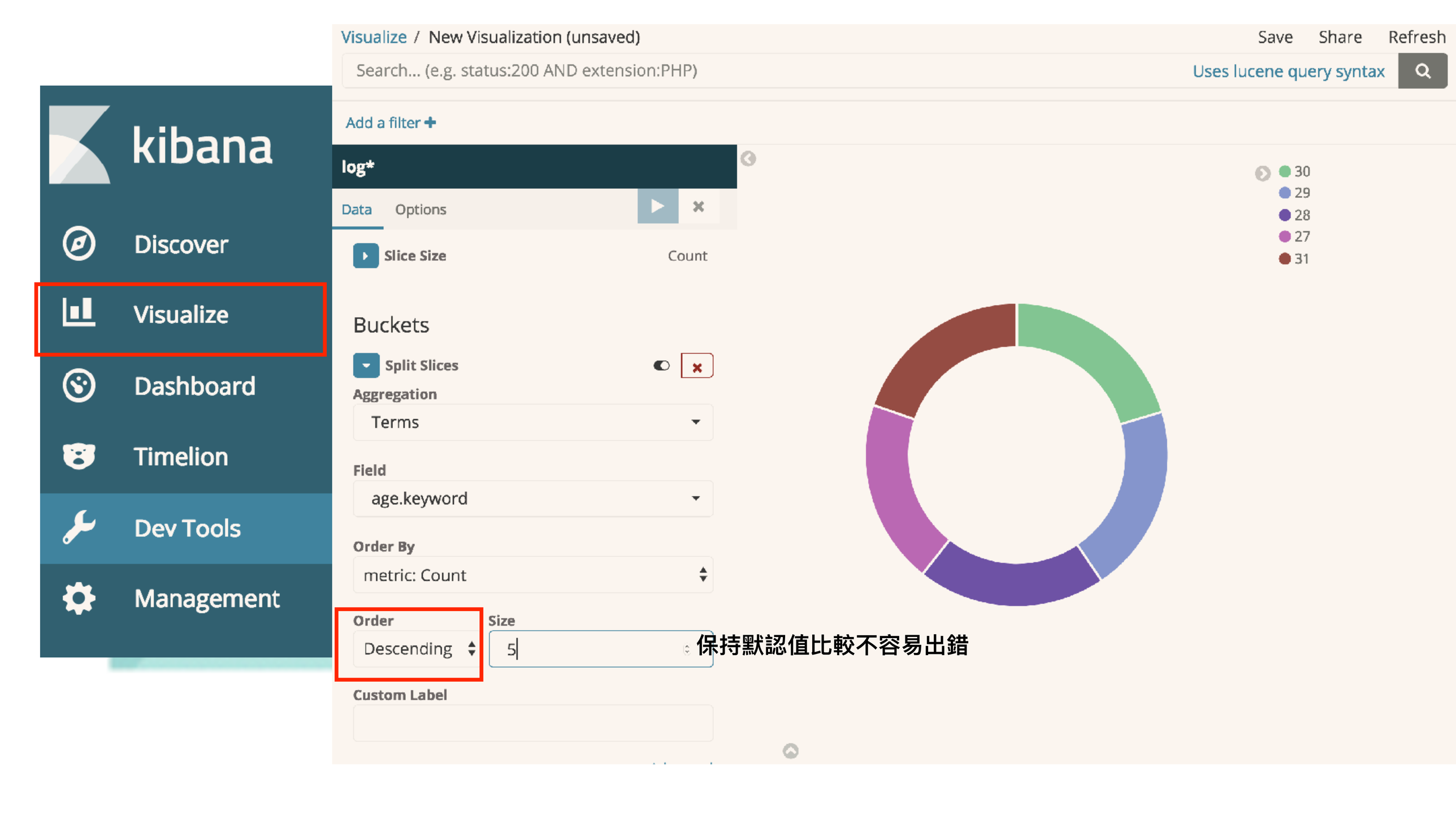
看到下方畫面則表示啟動成功（需先啟動Elasticsearch）

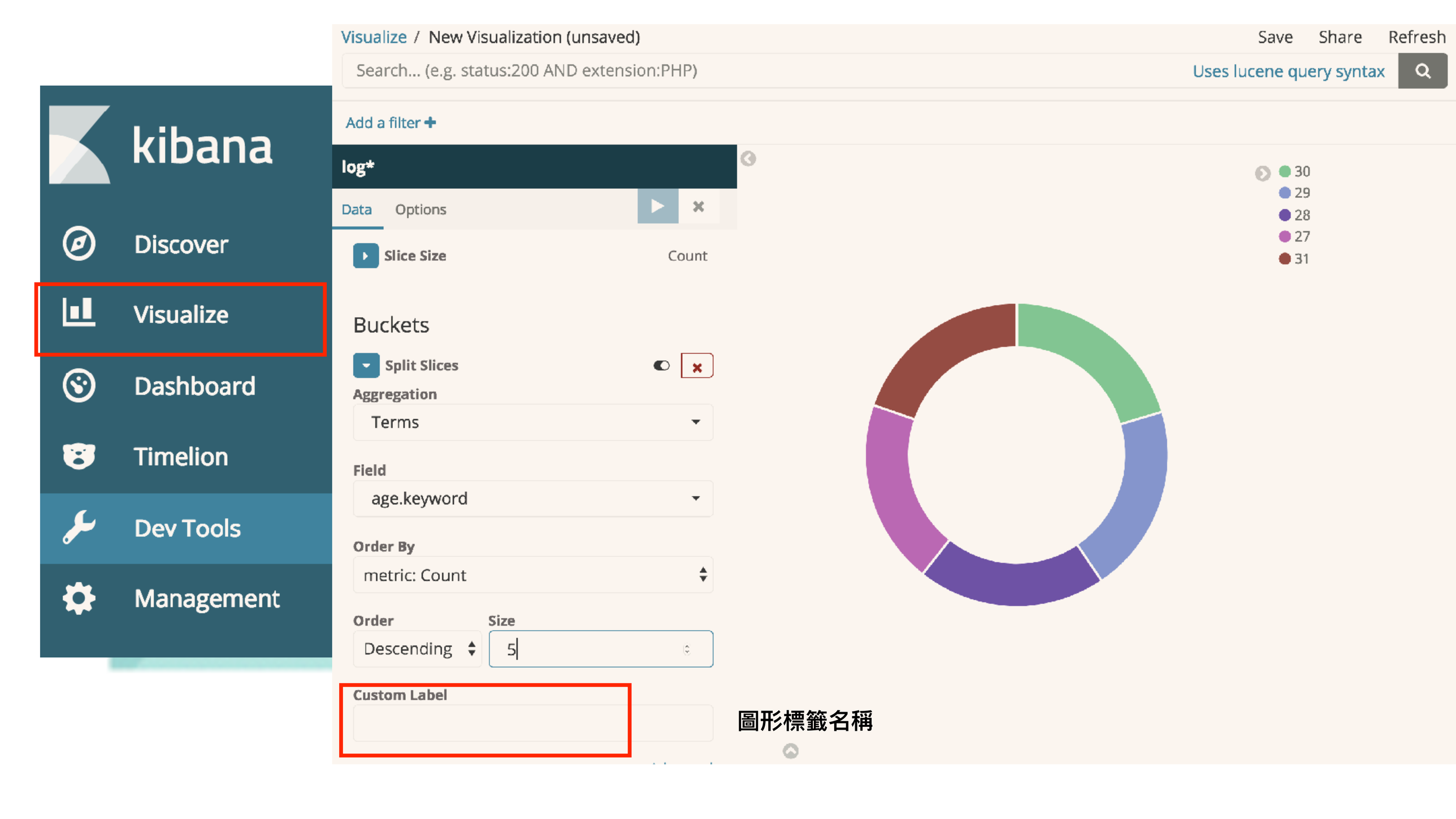



kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
log*
Data
Options
Slice Size
Count
點進去可以看到其他設定
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31


Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
log*
Data
Options
Slice Size
Count
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31
根據哪個 column 來進行排序
可直接 key 關鍵字

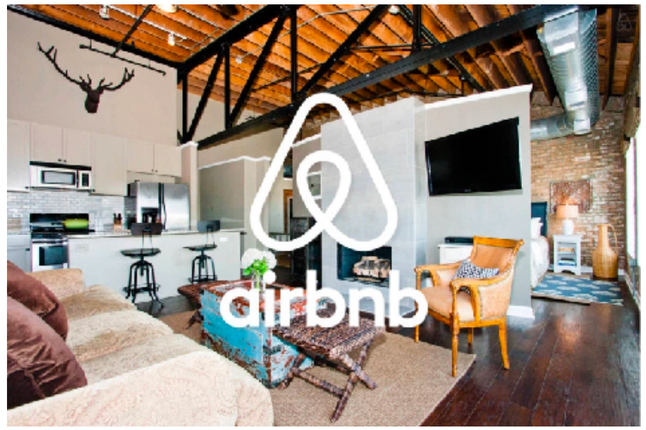

kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
log*
Data
Options
Slice Size
Count
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31
排序是按数量排序


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
log*
Data
Options
Slice Size
Count
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31
保持默認值比較不容易出錯


Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
log*
Data
Options
Slice Size
Count
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31
圖形標籤名稱


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Visualize / New Visualization (unsaved)
Save
Share
Refresh
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
如果都設定好，也是自己想要的樣子，即可存檔
log*
Data
Options
Slice Size
Count
Buckets
Split Slices
Aggregation
Terms
Field
age.keyword
Order By
metric: Count
Order
Descending
Size
5
Custom Label
30
29
28
27
31

/train_users_2.csv



Airbnb New User Bookings

Where will a new guest book their first travel experience?

在這個挑戰中，會得到一個用戶列表以及他們的人口統計信息，網絡會話記錄和一些匯總統計信息。 被要求預測哪個國家是新用戶的第一個預訂目的地。 這個數據集中的所有用戶都來自美國。

目的地國有12種可能的結果：'US', 'FR', 'CA', 'GB', 'ES', 'IT', 'PT', 'NL','DE', 'AU', ‘NDF’ (no destination found), and 'other'.

沒有預定

/train_users_2.csv

id	date_account_create	timestamp_first_activ	date_first_booking	gender	age	signup_method	signup_flow
gxn3p5htnn	2010/6/28	2.01E+13		-unknown-		facebook	0
820tgsjxq7	2011/5/25	2.01E+13		MALE	38	facebook	0
4ft3gnwmtx	2010/9/28	2.01E+13	2010/8/2	FEMALE	56	basic	3
bjjt8pjhuk	2011/12/5	2.01E+13	2012/9/8	FEMALE	42	facebook	0
87mebub9p4	2010/9/14	2.01E+13	2010/2/18	-unknown-	41	basic	0
osr2jwljor	2010/1/1	2.01E+13	2010/1/2	-unknown-		basic	0
lsw9q7uk0j	2010/1/2	2.01E+13	2010/1/5	FEMALE	46	basic	0

/train_users_2.csv

language	affiliate_channel	affiliate_provider	first_affiliate_tracked	signup_app	first_device_type	first_browser	country_destination
en	direct	direct	untracked	Web	Mac Desktop	Chrome	NDF
en	seo	google	untracked	Web	Mac Desktop	Chrome	NDF
en	direct	direct	untracked	Web	Windows Desktop	IE	US
en	direct	direct	untracked	Web	Mac Desktop	Firefox	other
en	direct	direct	untracked	Web	Mac Desktop	Chrome	US
en	other	other	omg	Web	Mac Desktop	Chrome	US
en	other	craigslist	untracked	Web	Mac Desktop	Safari	US

Reference

ELK 介紹
https://oranwind.org/dv-elk-an-zhuang-ji-she-ding-jiao-xue/
讓 Logstash 從頭讀文件
https://elasticsearch.cn/article/11
Logstash Grok
https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html
Kaggle - New York City Taxi Trip Duration
https://www.kaggle.com/c/nyc-taxi-trip-duration
Version Compatibility with Elasticsearch
https://github.com/elastic/kibana
Elasticsearch 簡介
https://www.slideshare.net/rueian3/elasticsearch-45855699
ELK教學
https://blog.johnwu.cc/article/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-red-hat.html
Docker @ Elastic
https://www.docker.elastic.co/#
Visualizing Logs Using ElasticSearch, Logstash and Kibana
https://www.youtube.com/watch?v=Kqs7UcCJquM
利用 Logstash，Elasticsearch 與 Kibana 來分析 log
http://www.evanlin.com/using-logstash-elsticsearch-and-kibana/

Reference

Hands on tutorial to perform Data Exploration using Elastic Search and Kibana (using Python)
https://www.analyticsvidhya.com/blog/2017/05/beginners-guide-to-data-exploration-using-elastic-search-and-kibana/
Elasticsearch 權威指南
https://es.xiaoleilu.com/index.html
Kibana + timelion: time series with the elastic stack
https://www.slideshare.net/swallez/kibana-timelion-time-series-with-the-elastic-stack
Use Logstash to load CSV into Elasticsearch
https://www.youtube.com/watch?v=rKy4sFbIZ3U
Logstash 最佳實踐
https://doc.yonyoucloud.com/doc/logstash-best-practice-cn/index.html
cat API
https://www.elastic.co/guide/cn/elasticsearch/guide/current/_cat_api.html
Elasticsearch 實戰介紹
https://www.slideshare.net/gugod/elasticsearch-19877436

.
.
.