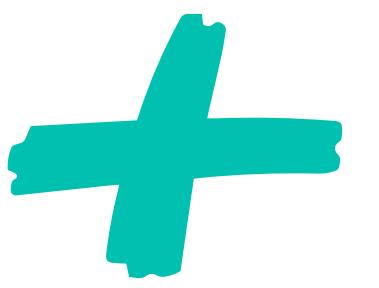
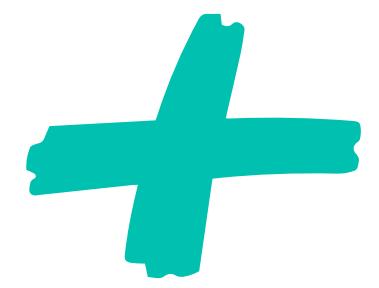
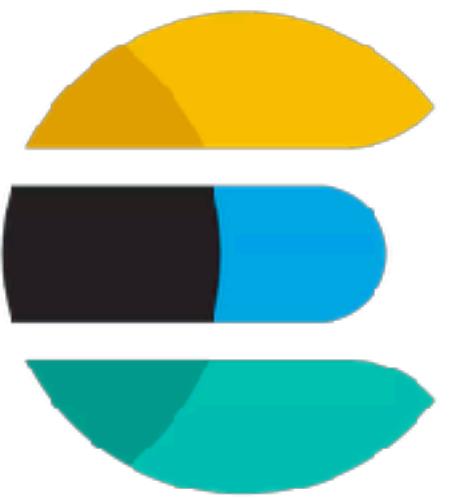




logstash



elasticsearch



kibana

ELK 主要由三個開源套件所組成，用於

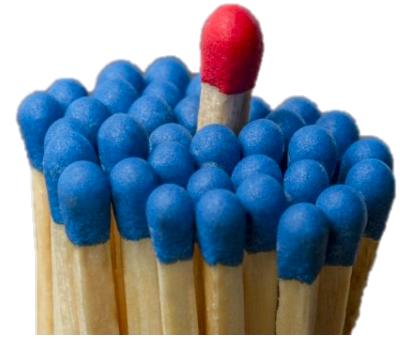
收集日誌資料 (Logstash)、

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



What's the difference

Why use
?

Motivation



How to make



Goal

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 以存放大量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

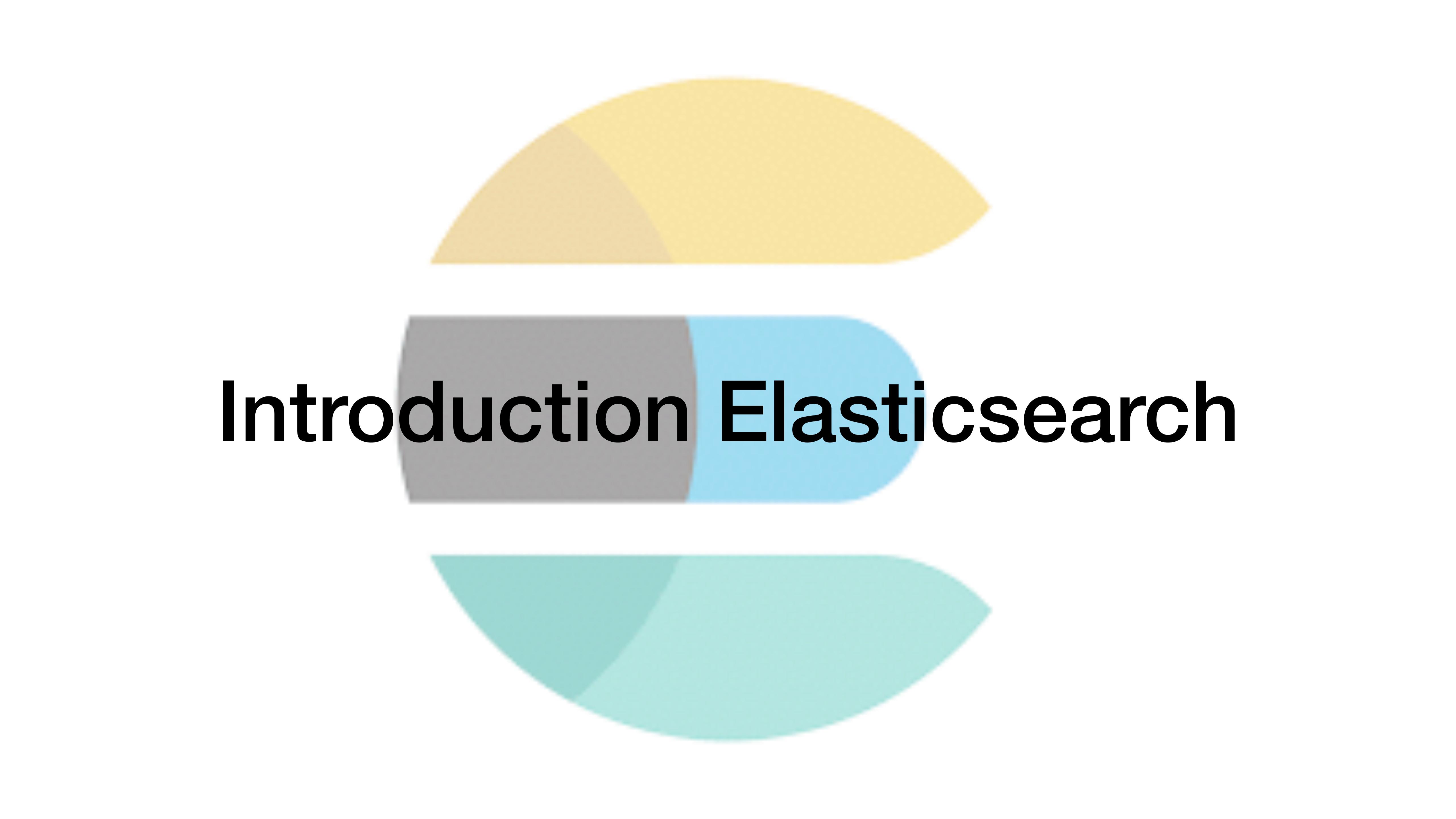
Inverted Index

- 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





Introduction Logstash

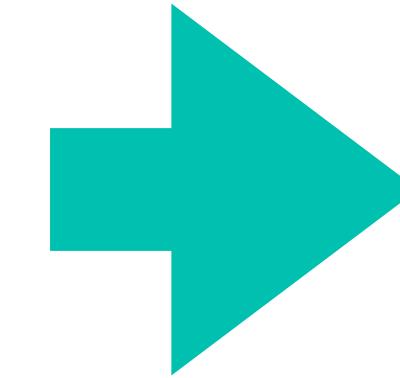
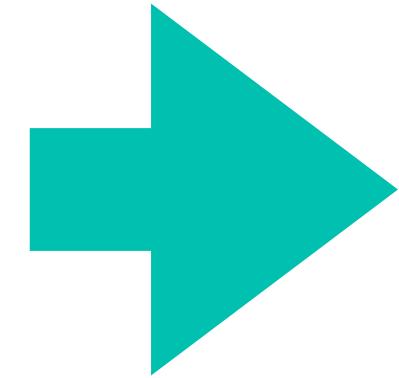
Logstash

- 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

+

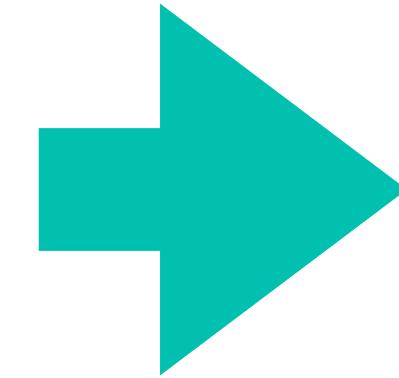
Transform



Search

+

Analyze



Visualize

+

Manage



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: 搜尋 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 億用戶提供即時而精準的音樂搜索服務
- 百度: 文本數據分析



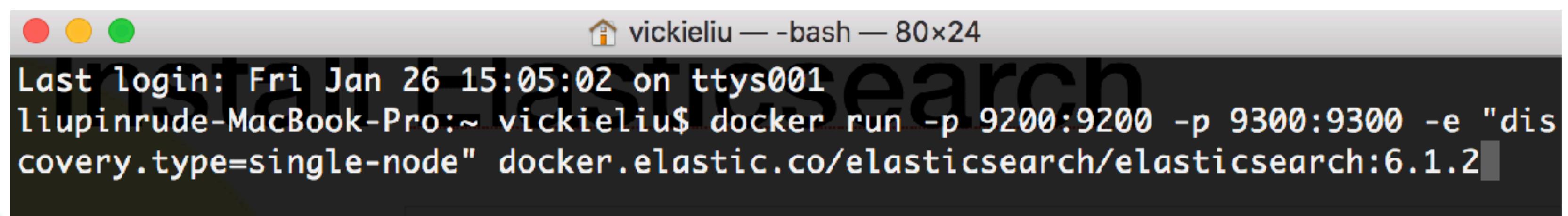
Import Data to Elasticsearch using Logstash

* 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
```



```
vickieliu — bash — 80x24  
Last login: Fri Jan 26 15:05:02 on ttys001  
liupinrude-MacBook-Pro:~ vickieliu$ 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
Gemfile
Gemfile.lock
LICENSE
NOTICE.TXT
bin
conf.d
config
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
1 input {
2     file {
3         path => "/Users/vickieliu/Downloads/train_users_2.csv"
4         start_position => "beginning"
5         sincedb_path => "/dev/null"
6     }
7 }
8 filter {
9     csv {
10        separator => ","
11        columns => ["id", "date_account_created", "timestamp_first_active",
12                      "date_first_booking", "gender", "age", "signup_method", "signup_flow",
13                      "language", "affiliate_channel", "affiliate_provider",
14                      "first_affiliate_tracked", "signup_app", "first_device_type",
15                      "first_browser", "country_destination"]
16    }
17 }
18 output {
19     elasticsearch {
20         hosts => ["localhost:9200"] ##"http://localhost:9200"
21     }
22     stdout {
23         codec => rubydebug{ }
24     }
25 }
```

Input

file

path、start_position、
since_db_path

kafka

監聽資訊

stdin

自行輸入

```
test1.conf
1 input {
2   file {
3     path => "/Users/vickieliu/Downloads/train_users_2.csv"
4     start_position => "beginning"
5     since_db_path => "/dev/null"
6   }
7 }
8 filter {
9   csv {
10     separator => ","
11     columns => ["id", "date_account_created", "timestamp_first_active",
12       "date_first_booking", "gender", "age", "signup_method", "signup_flow",
13       "language", "affiliate_channel", "affiliate_provider",
14       "first_affiliate_tracked", "signup_app", "first_device_type",
15       "first_browser", "country_destination"]
16   }
17 }
18 output {
19   elasticsearch {
20     hosts => ["localhost:9200"] #"http://localhost:9200"
21   }
22 }
```

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
1 input {
2   file {
3     path => "/Users/vickieliu/Downloads/train_users_2.csv"
4     start_position => "beginning"
5     sincedb_path => "/dev/null"
6   }
7 }
8 filter {
9   csv {
10     separator => ","
11     columns => ["id", "date_account_created", "timestamp_first_active",
12       "date_first_booking", "gender", "age", "signup_method", "signup_flow",
13       "language", "affiliate_channel", "affiliate_provider",
14       "first_affiliate_tracked", "signup_app", "first_device_type",
15       "first_browser", "country_destination"]
16   }
17 }
18 output {
19   elasticsearch {
20     hosts => ["localhost:9200"] #"http://localhost:9200"
21   }
22 }
```

Output

elasticsearch
hosts、index

stdout
輸出結果

```
test1.conf
1 input {
2   file {
3     path => "/Users/vickieliu/Downloads/train_users_2.csv"
4     start_position => "beginning"
5     sincedb_path => "/dev/null"
6   }
7 }
8 filter {
9   csv {
10     separator => ","
11     columns => ["id", "date_account_created", "timestamp_first_active",
12       "date_first_booking", "gender", "age", "signup_method", "signup_flow",
13       "language", "affiliate_channel", "affiliate_provider",
14       "first_affiliate_tracked", "signup_app", "first_device_type",
15       "first_browser", "country_destination"]
16   }
17 }
18 output {
19   elasticsearch {
20     hosts => ["localhost:9200"] #"http://localhost:9200"
21   }
22 }
```



**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.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -Djruby.jit.threshold=0 -XX:+HeapDumpOnOutOfMemoryError -Djava.security.egd=file:/dev/urandom -Xmx1g -Xms1g -Xss2048k -Djffi.boot.library.path=/Users/vickieliu/Developer/resources/logstash-6.1.2/vendor/jruby/lib/jni -Dfile.encoding=UTF-8 -Xbootclasspath/a:/Users/vickieliu/Developer/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/jruby/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

The screenshot shows the Kibana interface. On the left is a dark sidebar with the Kibana logo and links to Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. Below this is a 'Collapse' button. The main area has a light background. At the top center is the text 'Welcome to Kibana'. In the top right corner are two buttons: 'Data already in Elasticsearch?' and 'Set up index patterns'. The central part of the screen is divided into three sections: 'Visualize and Explore Data' (containing Dashboard, Timelion, Discover, and Visualize), 'Manage and Administer the Elastic Stack' (containing Console, Index Patterns, and Saved Objects), and a search bar at the bottom with the placeholder 'Didn't find what you were looking for?' and a 'View full directory of Kibana plugins' button.

Welcome to Kibana

Data already in Elasticsearch? Set up index patterns

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Collapse

Visualize and Explore Data

Discover

Interactively explore your data by querying and filtering raw documents.

Dashboard

Display and share a collection of visualizations and saved searches.

Timelion

Use an expression language to analyze time series data and visualize the results.

Visualize

Create visualizations and aggregate data stores in your Elasticsearch indices.

Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Index Patterns

Manage the index patterns that help retrieve your data from Elasticsearch.

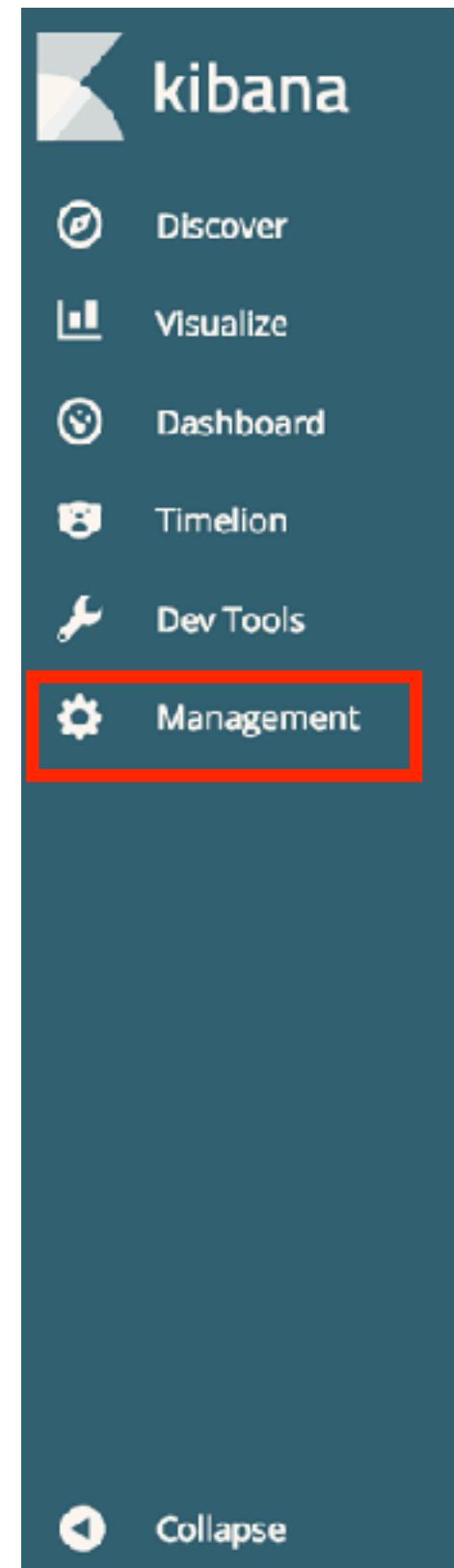
Saved Objects

Import, export, and manage your saved searches, visualizations, and dashboards.

Didn't find what you were looking for?

View full directory of Kibana plugins

Step10: 點選 Management



The screenshot shows the Kibana interface. On the left, a dark sidebar lists several options: Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The 'Management' option is highlighted with a red rectangular box. The main content area is titled 'Welcome to Kibana'. It features two main sections: 'Visualize and Explore Data' and 'Manage and Administer the Elastic Stack'. The 'Discover' section under 'Visualize and Explore Data' includes a description of what it does and a link to 'Discover'. The 'Timelion' section also provides a description and a link. The 'Management' section includes 'Console', 'Index Patterns', and 'Saved Objects', each with a brief description and a link. At the bottom, there's a search bar placeholder and a link to 'View full directory of Kibana plugins'.

Welcome to Kibana

Data already in Elasticsearch? [Set up index patterns](#)

Visualize and Explore Data

Discover
Display and share a collection of visualizations and saved searches.

Timelion
Use an expression language to analyze time series data and visualize the results.

Discover
Interactively explore your data by querying and filtering raw documents.

Visualize
Create visualizations and aggregate data stores in your Elasticsearch indices.

Manage and Administer the Elastic Stack

Console
Skip cURL and use this JSON interface to work with your data directly.

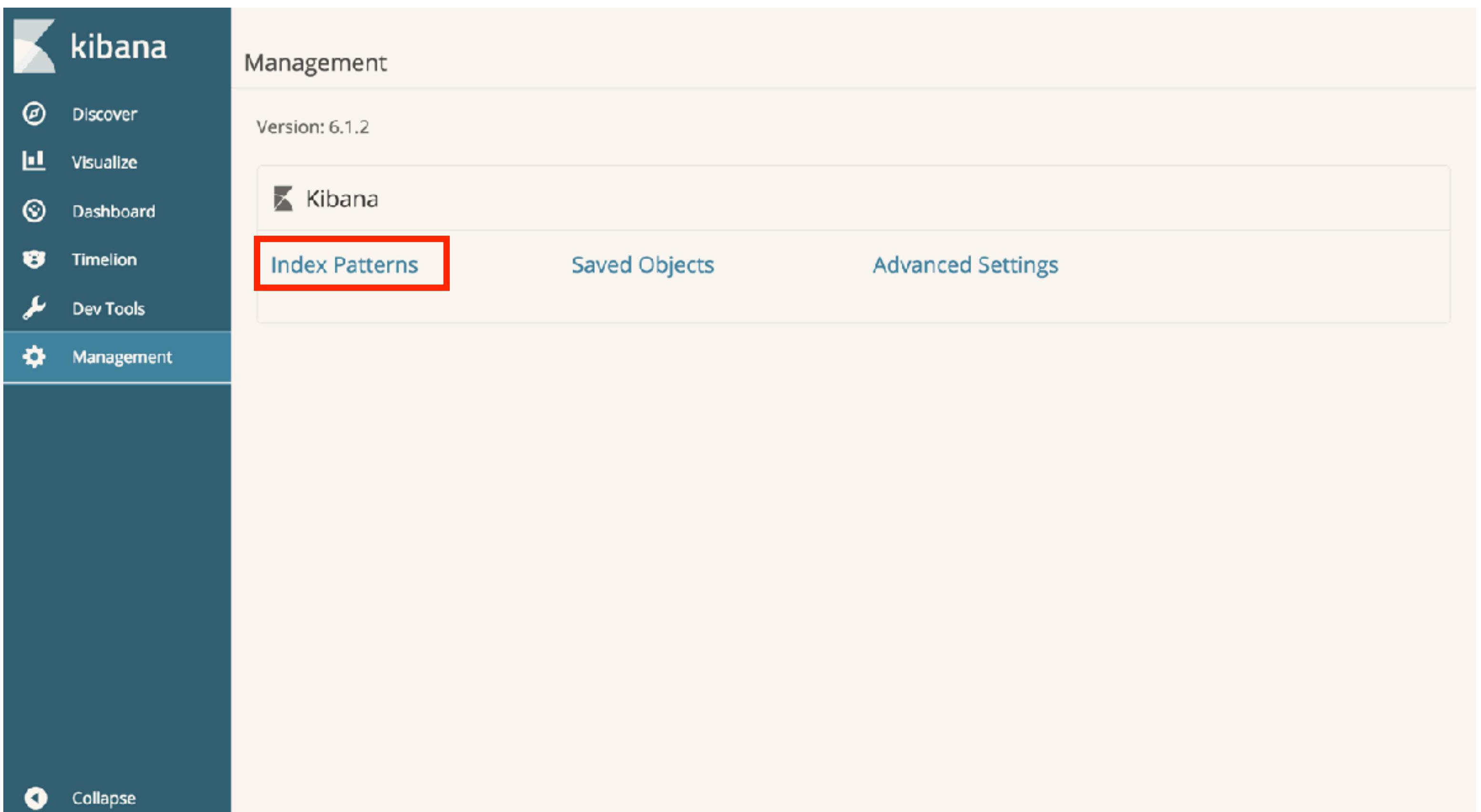
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.

Saved Objects
Import, export, and manage your saved searches, visualizations, and dashboards.

Didn't find what you were looking for?

[View full directory of Kibana plugins](#)

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

The screenshot shows the Kibana Management interface with the 'Management / Kibana' header. On the left, a sidebar includes 'Discover', 'Visualize', 'Dashboard', 'Timelion', 'Dev Tools', and 'Management' (which is selected). A warning message states: 'Warning: No default index pattern. You must select or create one to continue.' Below this, the 'Create index pattern' section is displayed. It contains a 'Step 1 of 2: Define index pattern' heading, an 'Index pattern' input field containing 'index-name-*', and a note: 'You can use a * as a wildcard in your index pattern. You can't use empty spaces or the characters \ / ? " < > |.' A red box highlights the index pattern 'logstash-2018.01.30'. A 'Next step >' button is visible on the right. The bottom of the screen shows the URL '127.0.0.1:5601/app/kibana#/home'.

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

The screenshot shows the Kibana Management interface. On the left, there is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The Management icon is highlighted. The main area has a header 'Management / Kibana' with tabs for Index Patterns, Saved Objects, and Advanced Settings. A warning message states: 'Warning: No default index pattern. You must select or create one to continue.' Below this, a section titled 'Create index pattern' says 'Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.' It contains a form for 'Step 1 of 2: Define index pattern' with a red box around the 'Index pattern' input field, which contains the character '*'. Below the input field, instructions say: 'You can use a * as a wildcard in your index pattern. You can't use empty spaces or the characters \ / ? " < > | .' To the right of the input field is a 'Next step >' button. At the bottom of the form, a success message says: '✓ Success! Your index pattern matches 1 Index.' followed by the text 'logstash-2018.01.30'. The URL at the bottom of the browser window is '127.0.0.1:5601/app/kibana#/dev_tools/_g-0'.

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

The screenshot shows the Kibana Management interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The Management icon is highlighted. The main area has a header "Management / Kibana" with tabs for Index Patterns, Saved Objects, and Advanced Settings. A warning message says "No default index pattern. You must select or create one to continue." Below it, a section titled "Create index pattern" with the sub-instruction "Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations." contains a form for defining an index pattern. The input field contains the wildcard character "*". To the right of the input field is a note: "You can use a * as a wildcard in your index pattern. You can't use empty spaces or the characters \ / ? " < > | .". At the bottom of this section, a green success message reads "✓ Success! Your index pattern matches 1 Index." followed by the index name "logstash-2018.01.30". A blue "Next step" button is located on the far right, with a red box drawn around it to indicate it should be clicked.

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

The screenshot shows the Kibana Management interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The Management option is selected. The main area is titled 'Management / Kibana' and shows 'Index Patterns' (highlighted in blue), 'Saved Objects', and 'Advanced Settings'. A warning message states: 'Warning: No default index pattern. You must select or create one to continue.' Below this, the title 'Create index pattern' is followed by the sub-instruction 'Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.' The current step is 'Step 2 of 2: Configure settings'. It says, 'You've defined * as your index pattern. Now you can specify some settings before we create it.' A red box highlights the 'Time Filter field name' dropdown menu, which contains a single option: '@timestamp'. To the right of the dropdown are 'Refresh' and a dropdown arrow. Below the dropdown, a note says: 'The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.' There is also a 'Show advanced options' link. At the bottom right are 'Back' and 'Create index pattern' buttons.

**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**

The screenshot shows the Kibana Management interface. On the left, there's a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools, and Management. The Management icon is highlighted with a blue background. At the top right, there are links for Index Patterns, Saved Objects, and Advanced Settings. A warning message in an orange box states: "Warning: No default index pattern. You must select or create one to continue." Below this, the main area is titled "Create index pattern" with the sub-instruction "Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations." A section titled "Step 2 of 2: Configure settings" contains the text "You've defined * as your index pattern. Now you can specify some settings before we create it." Under "Time Filter field name", a dropdown menu is set to "I don't want to use the Time Filter". A note below explains: "The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range." There are "Show advanced options" and "Back" buttons at the bottom.

Management / Kibana

Index Patterns Saved Objects Advanced Settings

Warning
No default index pattern.
You must select or create
one to continue.

Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Step 2 of 2: Configure settings

You've defined * as your index pattern. Now you can specify some settings before we create it.

Time Filter field name [Refresh](#)

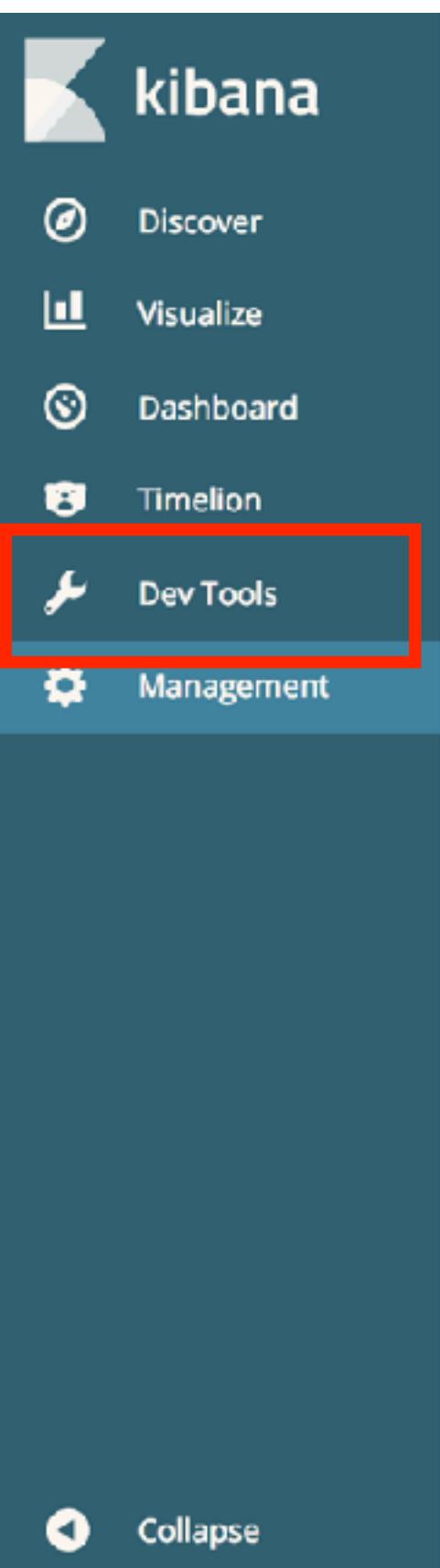
I don't want to use the Time Filter

The Time Filter will use this field to filter your data by time. You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

▶ Show advanced options

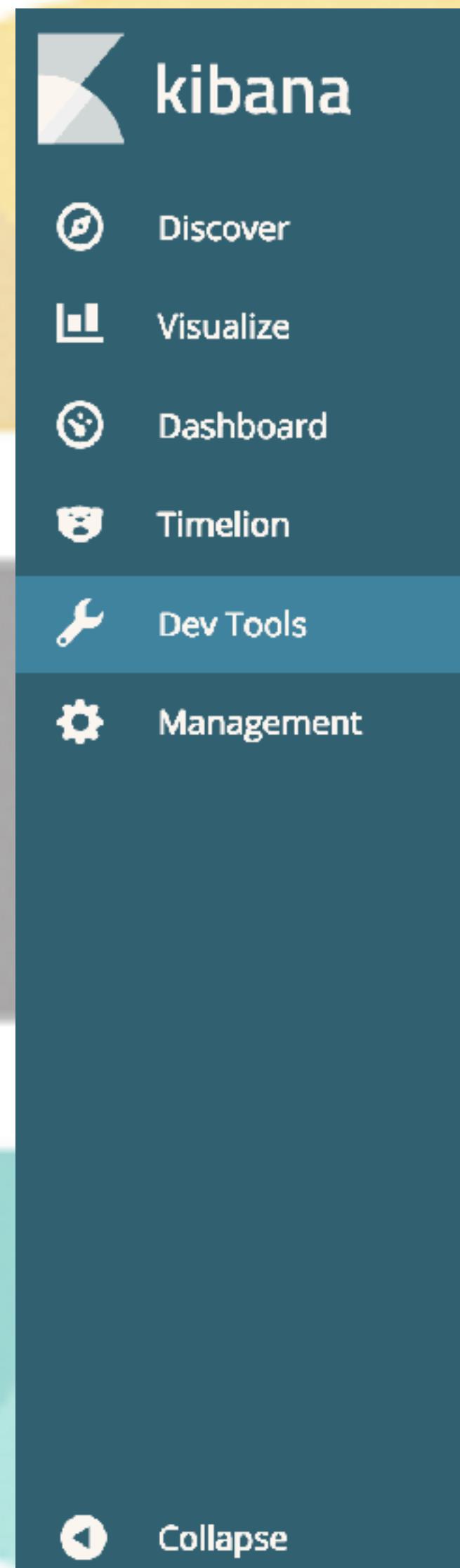
Back [Create index pattern](#)

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



The screenshot shows the Kibana Management interface. On the left, there is a sidebar with the following options: Discover, Visualize, Dashboard, Timeline, Dev Tools (which is highlighted with a red box), and Management. Below the sidebar, there is a "Collapse" button. The main area is titled "Management / Kibana" and contains tabs for Index Patterns, Saved Objects, and Advanced Settings. A prominent "Index Patterns" tab is selected. Below the tabs, there is a section with two stars and a note: "This page lists every field in the * index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API %". There are three buttons: "fields (290)", "scripted fields (0)", and "source filters (0)". Below these buttons is a "Filter" input field and a "All field types" dropdown. The main content area displays a table of field mappings:

name	format	searchable	aggregatable	excluded	type	con
@timestamp		✓	✓		date	
@version		✓	✓		string	
_id		✓	✓		string	
_index		✓	✓		string	
_score					number	
_source					_source	
_type		✓	✓		string	
affiliate_channel		✓			string	
affiliate_channel.keyword		✓	✓		string	
affiliate_provider		✓			string	



Dev Tools

History Settings Help

Console

1 GET /_cat|



1 |=^.=
2 /_cat/allocation
3 /_cat/shards
4 /_cat/shards/{index}
5 /_cat/master
6 /_cat/nodes
7 /_cat/tasks
8 /_cat/indices
9 /_cat/indices/{index}
10 /_cat/segments
11 /_cat/segments/{index}
12 /_cat/count
13 /_cat/count/{index}
14 /_cat/recovery
15 /_cat/recovery/{index}
16 /_cat/health
17 /_cat/pending_tasks
18 /_cat/aliases
19 /_cat/aliases/{alias}
20 /_cat/thread_pool
21 /_cat/thread_pool/{thread_pools}
22 /_cat/plugins
23 /_cat/fielddata
24 /_cat/fielddata/{fields}
25 /_cat/nodeattrs
26 /_cat/repositories
27 /_cat/snapshots/{repository}
28 /_cat/templates

通過GET請求發送cat命名

可以列出所有可用的API：



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

```
1 GET /_cat
2
3 GET /_cat/health
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
```

要啟用表頭，加上?v 即可

The screenshot shows the Kibana interface with the 'Dev Tools' tab selected in the sidebar. The main area is the 'Console' tab, displaying a list of API requests. The request at index 5, 'GET /_cat/health?v', is highlighted with a red box. The response for this request is shown in a table:

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

Dev Tools

Console 看現有的 Logstash 有哪些

Discover Visualize Dashboard Timelion Dev Tools Management

Collapse

```
1 GET /_cat
2
3 GET /_cat/health
4
5 GET /_cat/health?v
6
7 GET /_cat/nodes?v
8
9 GET /_cat/nodes?help
10
11 GET /_cat/nodes?v&h=ip,port
,heapPercent,heapMax
12
13 GET /_cat/indices?v
14
15
16
17
18
19
20
21
22
23
24
25
26
27
```

▶ 🔍 :

	1	health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size	
1	yellow	open	.	monitoring-es-6-2018.01.24	dyCjjss3RyyTlG4oNgfGm	A	1	1	17992	228	8mb	8mb
2	yellow	open	nyc		ZFz1UA13Rzud_PQ3dgIrR	w	5	1	2122440	0	1.4gb	1.4gb
3	yellow	open	logstash-2018.01.24		1NQS0eocQuKrr_cBk17e4	w	5	1	628327	0	157.1mb	157.1mb
4	yellow	open	logstash-2018.01.23		nY5bDdEJQB2U5a7qAIi29	A	5	1	752808	0	188.3mb	188.3mb
5	yellow	open	.kibana		Yuyikeo0Q5SLyp68TUSHH	A	1	1	4	0	38.6kb	38.6kb
6	yellow	open	.monitoring-es-6-2018.01.22		0tiXa2c3TfWRTjsR2tEEX	g	1	1	7975	12	3mb	3mb
7	yellow	open	.monitoring-es-6-2018.01.23		arAo5dY1RL2mjNG_ybemq	g	1	1	26859	182	10.5mb	10.5mb
8						9						

kibana

Dev Tools

Console

檢索 Data

History Settings Help

Discover Visualize Dashboard Timelion Dev Tools Management Collapse

```
1 GET /_cat
2
3 GET /_cat/health
4
5 GET /_cat/health?v
6
7 GET /_cat/nodes?v
8
9 GET /_cat/nodes?help
10
11 GET /_cat/nodes?v&h=ip,port
     ,heapPercent,heapMax
12
13 GET /_cat/indices?v
14
15 GET _search
16 {
17   "query": {
18     "match_all": {}
19   }
20 }
```

▶ 🔧 :

```
1 {
2   "took": 23,
3   "timed_out": false,
4   "_shards": {
5     "total": 19,
6     "successful": 19,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": 3556449,
12    "max_score": 1,
13    "hits": [
14      {
15        "_index": ".kibana",
16        "_type": "doc",
17        "_id": "config:6.1.2",
18        "_score": 1,
19        "_source": {
20          "type": "config",
21          "updated_at": "2018-01-23T06:50:26.338Z",
22          "config": {
23            "buildNum": 16363,
24            "defaultIndex": "afee8430-0009-11e8-a196-cfbf7ba4
25          }
26        }
27      },
28    ]
29  }
30 }
```

定義檢索 Data 方式

Dev Tools History Settings Help

Console

```
1 GET /_cat
2
3 GET /_cat/health
4
5 GET /_cat/health?v
6
7 GET /_cat/nodes?v
8
9 GET /_cat/nodes?help
10
11 GET /_cat/nodes?v&h=ip,port
     ,heapPercent,heapMax
12
13 GET /_cat/indices?v
14
15 GET _search
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 }
```

1 {
2 "took": 53,
3 "timed_out": false,
4 "_shards": {
5 "total": 5,
6 "successful": 5,
7 "skipped": 0,
8 "failed": 0
9 },
10 "hits": {
11 "total": 8,
12 "max_score": 11.518404,
13 "hits": [
14 {
15 "_index": "logstash-2018.01.23",
16 "_type": "doc",
17 "_id": "LdFjImEB4zpcysM7mb92",
18 "_score": 11.518404,
19 "_source": {
20 "path": "/Users/vickieliu/Downloads/train_users_2
.csv",
21 "signup_flow": "0",
22 "date_account_created": "2010/6/28",
23 "affiliate_provider": "direct",
24 "gender": "-unknown-",
25 "date_first_booking": null,
26 "@timestamp": "2018-01-23T09:40:04.935Z",
27 "id": "gxn3p5htnn",
28 }
29 }
30 }
31 }
32 }

kibana

Dev Tools

Console

藉由查找出的資訊反檢索 Data

History Settings Help

```
8   "took": 8,
9   "timed_out": false,
10  "_shards": {
11    "total": 5,
12    "successful": 5,
13    "skipped": 0,
14    "failed": 0
15  },
16  "hits": {
17    "total": 2122440,
18    "max_score": 1,
19    "hits": [
20      {
21        "_index": "nyc",
22        "_type": "doc",
23        "_id": "8tW6ImEB4zpcysM75k1c",
24        "_score": 1
25      }
26    ]
27  }
28
29 GET /logstash-2018.01.23/_search
30 {
31   "query": {
32     "match_all": {}
33   }
34 }
```

Discover Visualize Dashboard Timelion Dev Tools Management

Collapse

▶ 🔒

8
9 GET /_cat/nodes?help
10
11 GET /_cat/nodes?v&h=ip, port
 , heapPercent, heapMax
12
13 GET /_cat/indices?v
14
15 GET _search
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 }

kibana

Dev Tools

Console

尋找特定 Data

```
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  
20    :10:49,1,-73.95611572265625,40.767623901367187,-73.970970153808  
21    594,40.760963439941406,N,958",  
22    "pickup_datetime": "2016-01-14 09:54:51",  
23    "dropoff_longitude": "-73.970970153808594",  
24    "pickup_latitude": "40.767623901367187",  
25    "trip_duration": "958"  
26  }  
27 }  
28 }
```



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
```

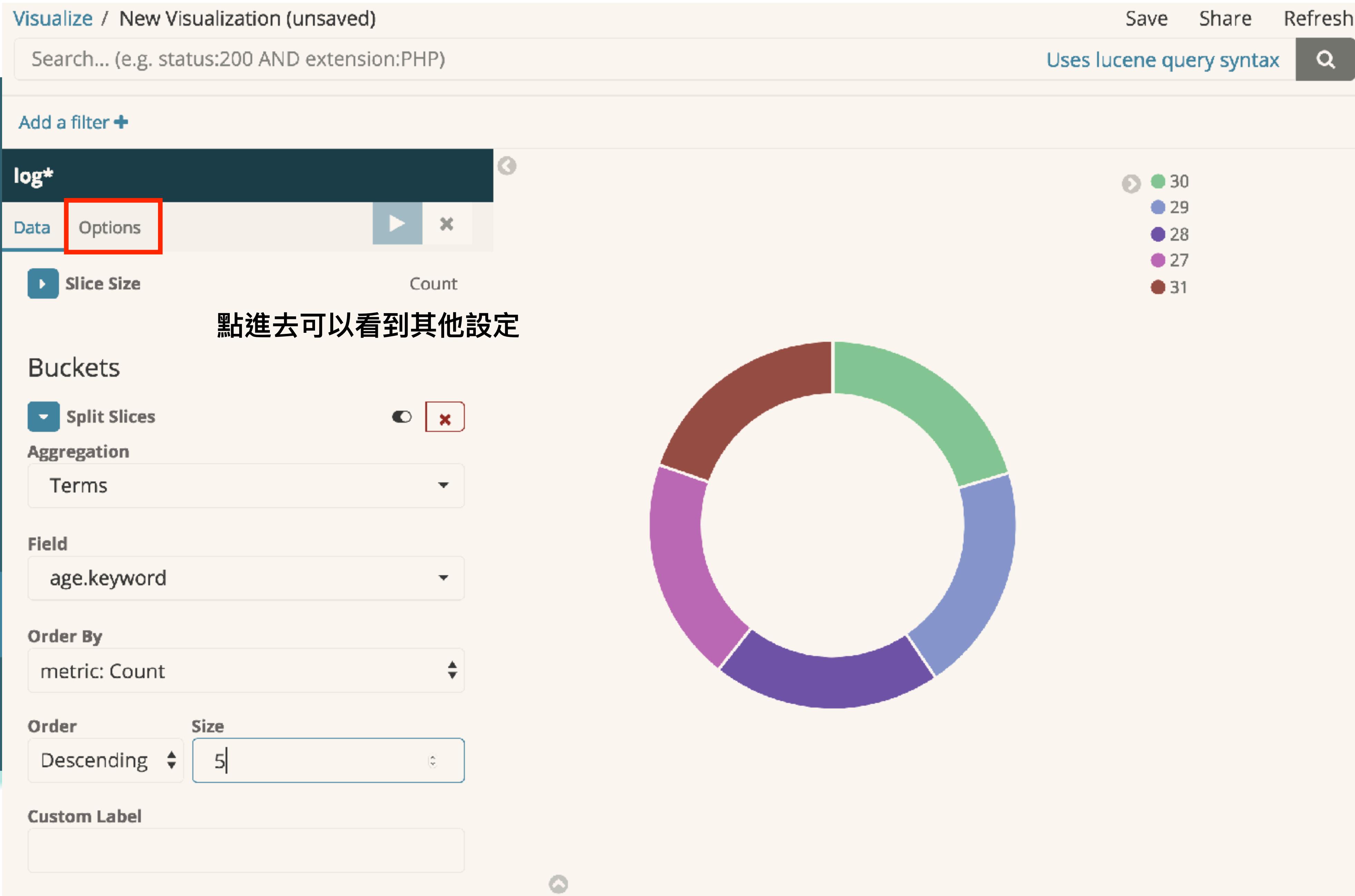
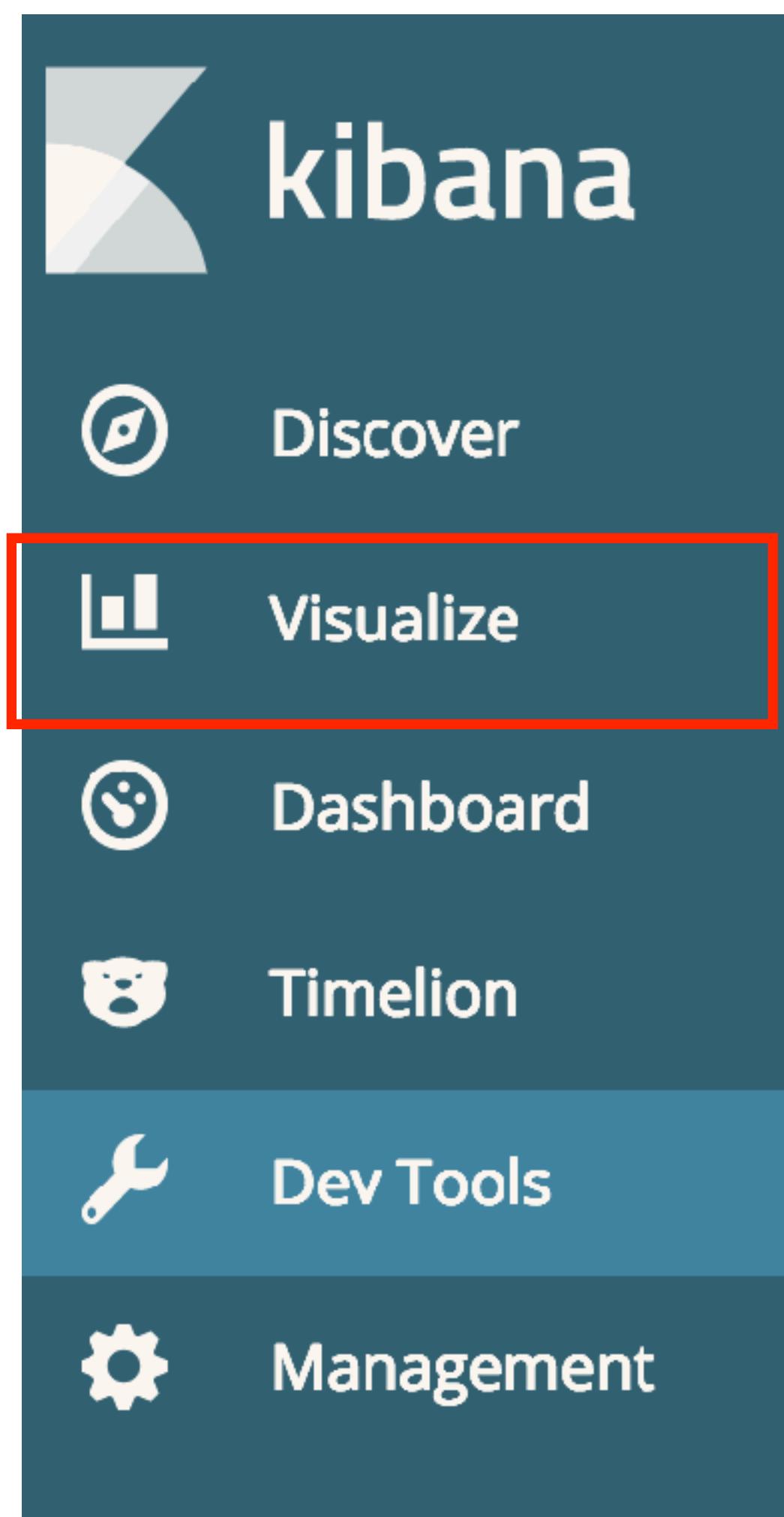
```
log  [08:43:31.159] [info][status][plugin:kibana@6.1.2] Status changed from u
ninitialized to green - Ready
log  [08:43:31.204] [info][status][plugin:elasticsearch@6.1.2] Status changed
from uninitialized to yellow - Waiting for Elasticsearch
log  [08:43:31.235] [info][status][plugin:console@6.1.2] 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）

The screenshot shows the Kibana interface. On the left is a sidebar with the Kibana logo and links to Discover, Visualize, Dashboard, Timelion, Dev Tools, Management, and a Collapse button. The main area has a header "Welcome to Kibana" and a "Data already in Elasticsearch?" link. It features two main sections: "Visualize and Explore Data" and "Manage and Administer the Elastic Stack". The "Visualize and Explore Data" section includes "Dashboard" (display and share a collection of visualizations and saved searches), "Timelion" (use an expression language to analyze time series data and visualize the results), and "Discover" (interactively explore your data by querying and filtering raw documents). The "Manage and Administer the Elastic Stack" section includes "Console" (skip cURL and use this JSON interface to work with your data directly), "Index Patterns" (manage the index patterns that help retrieve your data from Elasticsearch), and "Saved Objects" (import, export, and manage your saved searches, visualizations, and dashboards). At the bottom, there's a search bar placeholder "Didn't find what you were looking for?", a "View full directory of Kibana plugins" button, and a "Set up index patterns" button.



Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

log*

Data Options



Count

Slice Size



Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Buckets

Split Slices



Aggregation

Terms

Field

age.keyword

Order By

metric: Count

Order

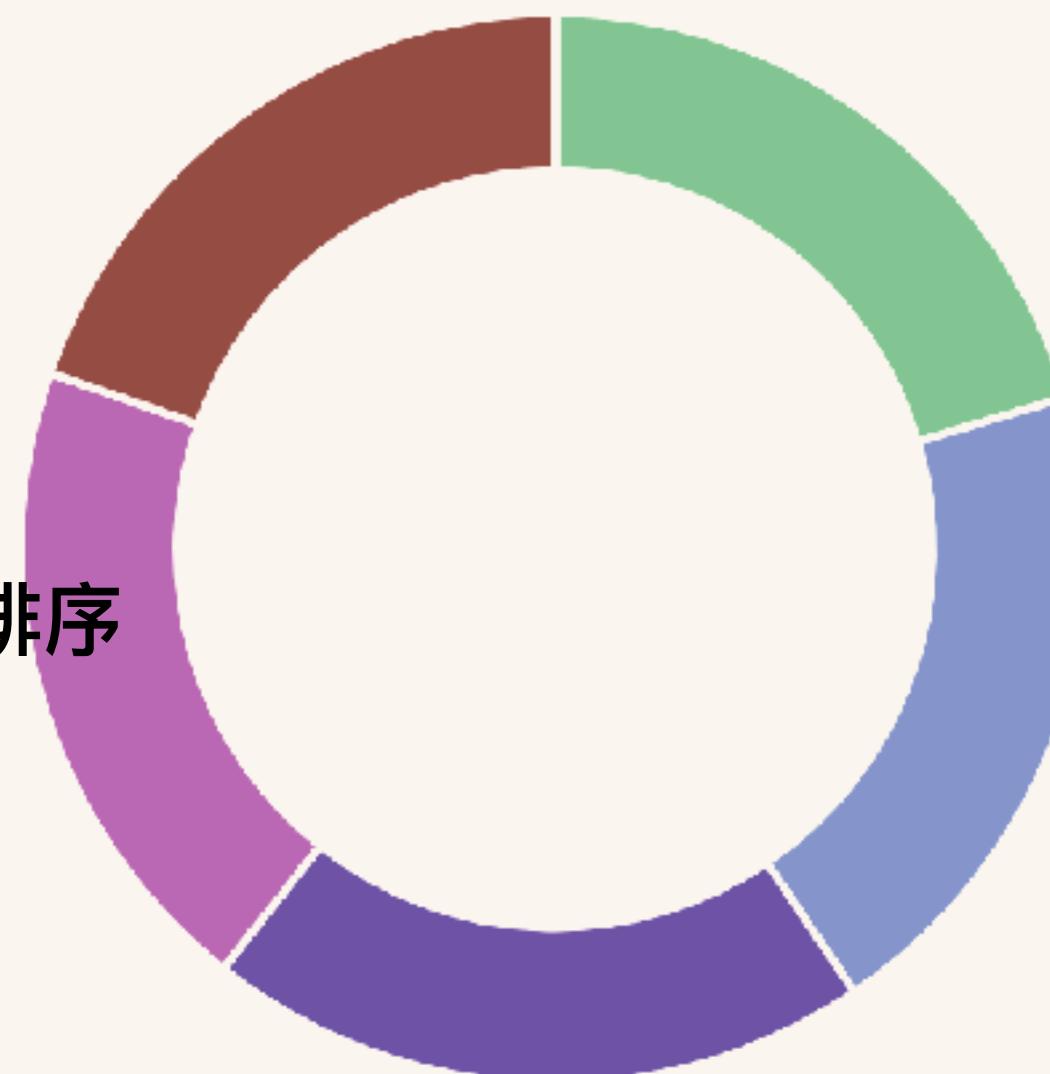
Descending

Size

5

Custom Label

根據哪個 column 來進行排序
可直接 key 關鍵字



- 30
- 29
- 28
- 27
- 31

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax



Add a filter +

log*

Data Options



Count

Slice Size

Buckets

Split Slices



Aggregation

Terms



Field

age.keyword



Order By

metric: Count



Order

Descending



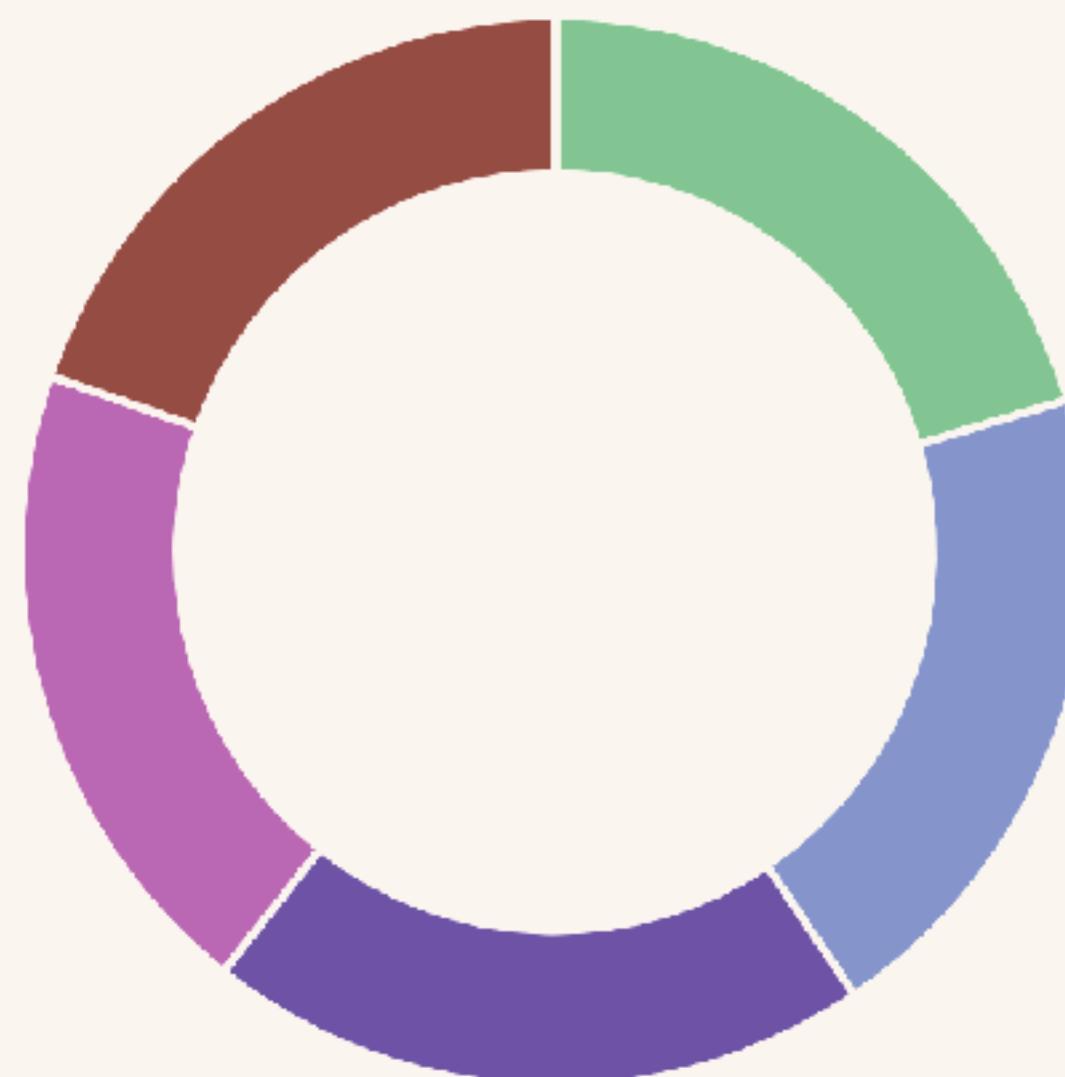
Size



5

Custom Label

排序是按數量排序



kibana

- Discover**
- Visualize**
- Dashboard**
- Timelion**
- Dev Tools**
- Management**

Search... (e.g. status:200 AND extension:PHP)

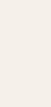
Uses lucene query syntax



Add a filter +

log*

Data Options



Count

Slice Size

- 30
- 29
- 28
- 27
- 31



kibana



Discover



Visualize



Dashboard



Timelion



Dev Tools



Management

Buckets

Split Slices



Aggregation

Terms



Field

age.keyword



Order By

metric: Count



Order

Descending

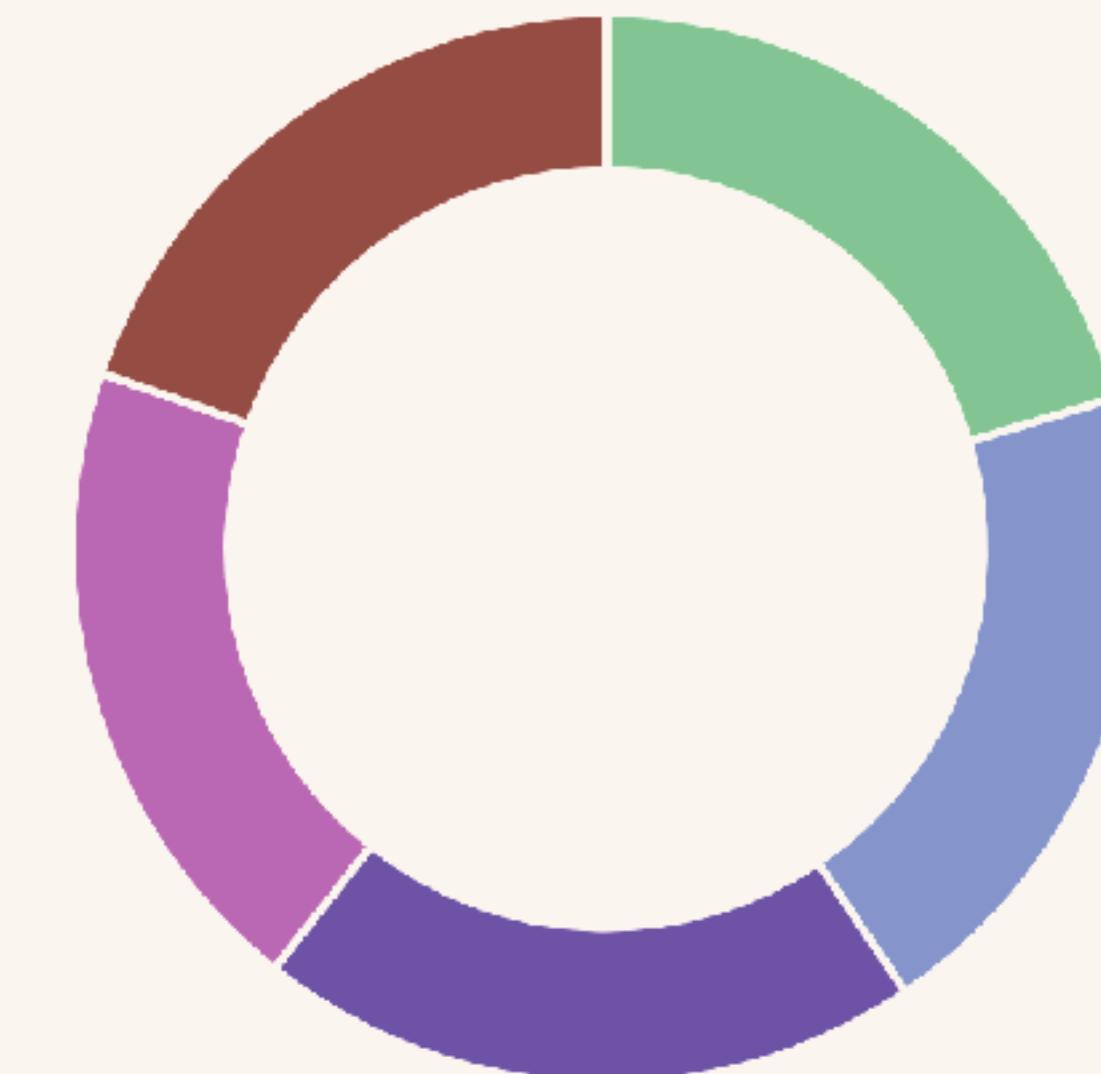
Size



5

保持默認值比較不容易出錯

Custom Label



Search... (e.g. status:200 AND extension:PHP)

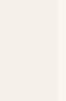
Uses lucene query syntax



Add a filter +

log*

Data Options



Slice Size

Count

- 30
- 29
- 28
- 27
- 31

Buckets

Split Slices



Aggregation

Terms



Field

age.keyword



Order By

metric: Count



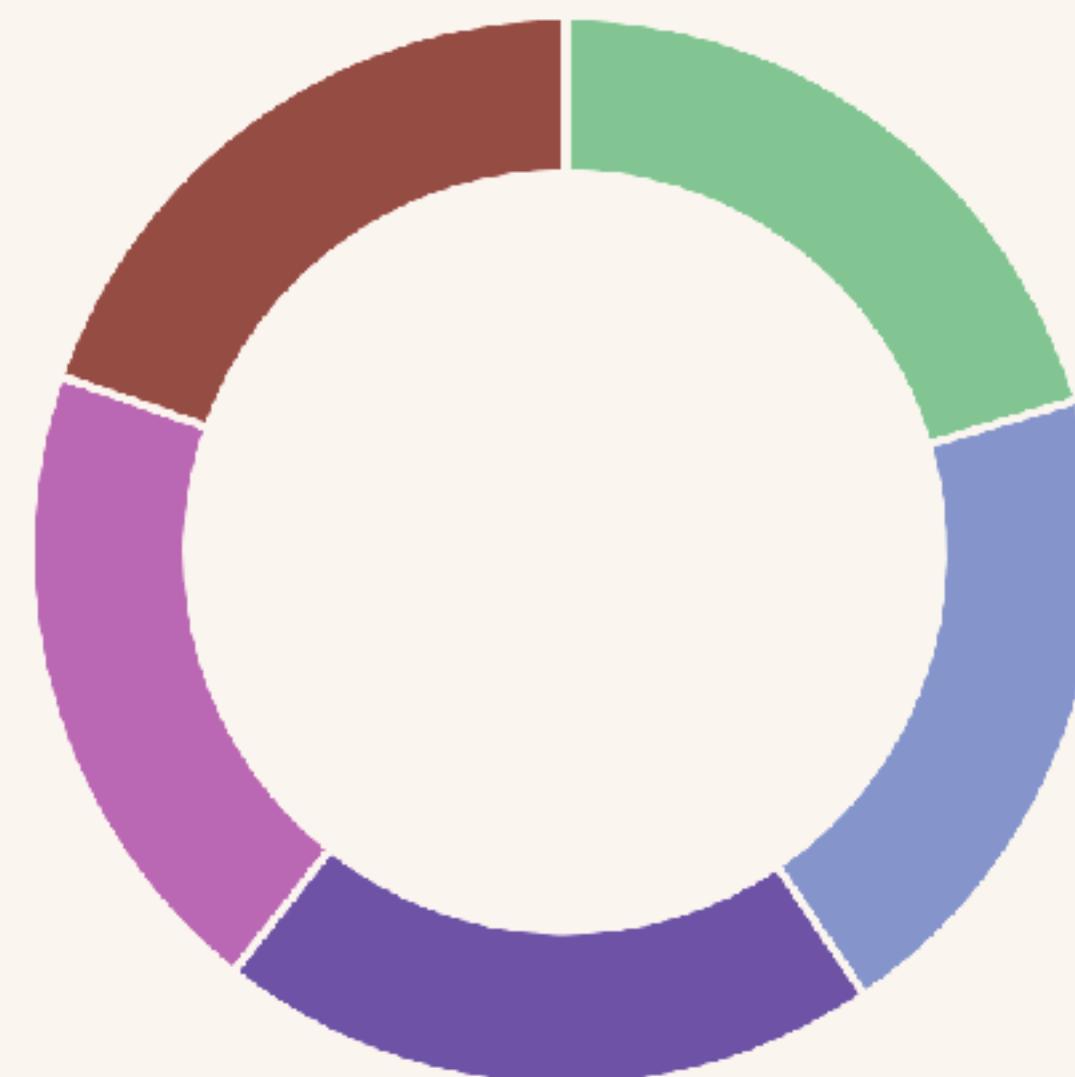
Order

Descending

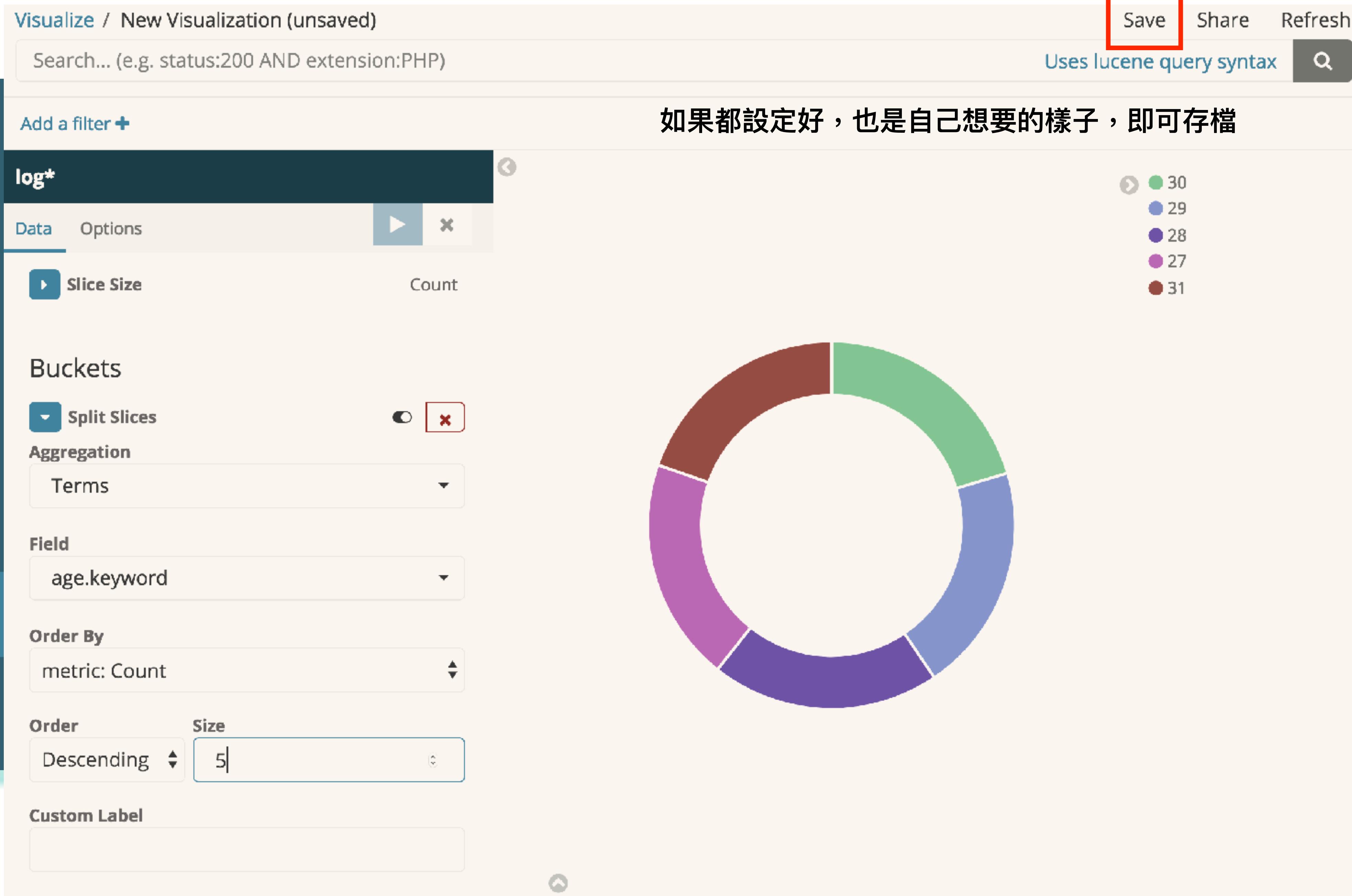
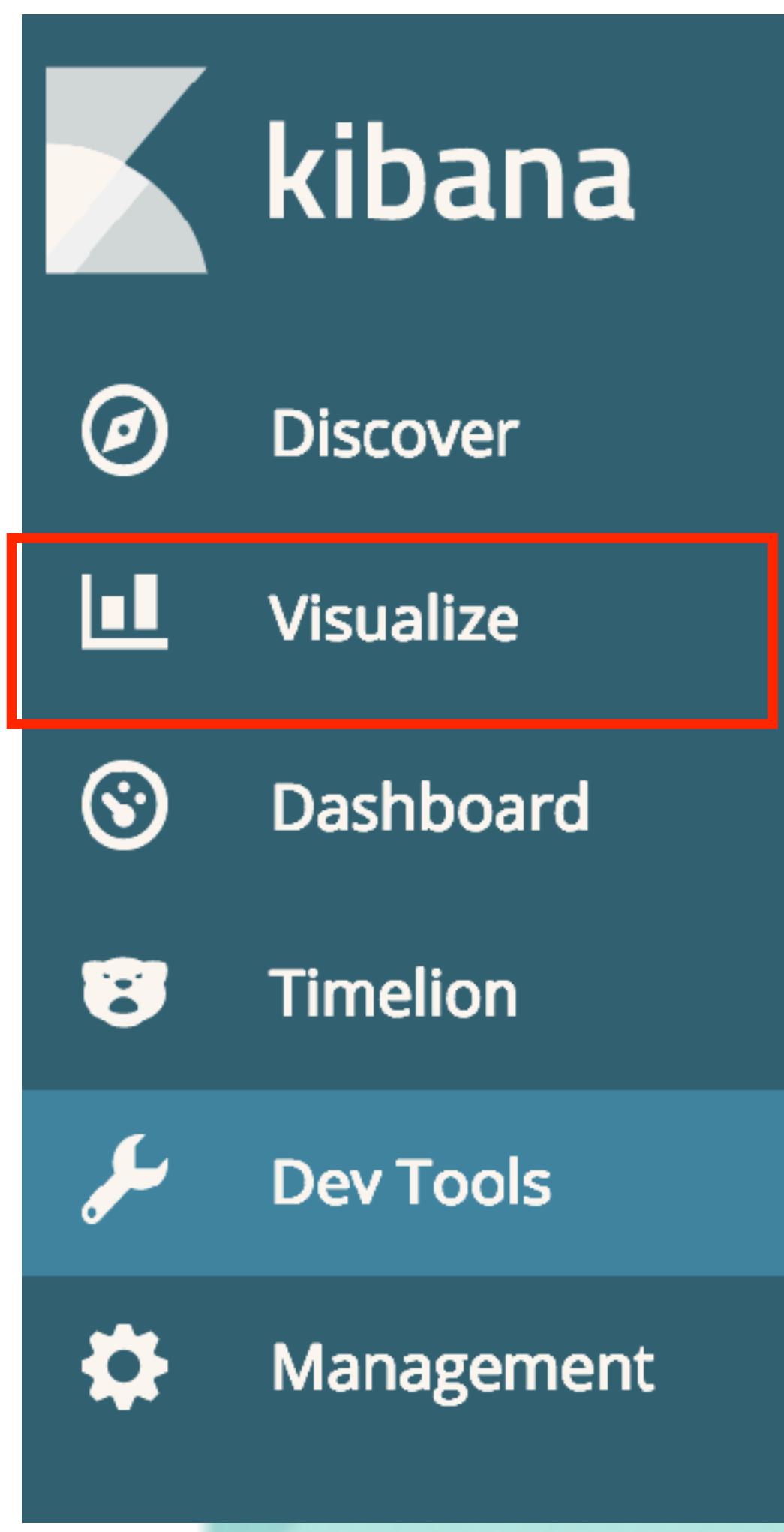
Size



Custom Label



圖形標籤名稱



/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_acco unt_create	timestamp _first_activ	date_first_b ooking	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-elasticsearch-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>

-
-
-