



elastic

Agenda

- Download Data
- Install Elasticsearch, Kibana and Logstash
- Introduction Elasticsearch, Kibana and Logstash
- Import Data to Elasticsearch using Logstash
- Create Kibana Dashboard

請別太期待 ...

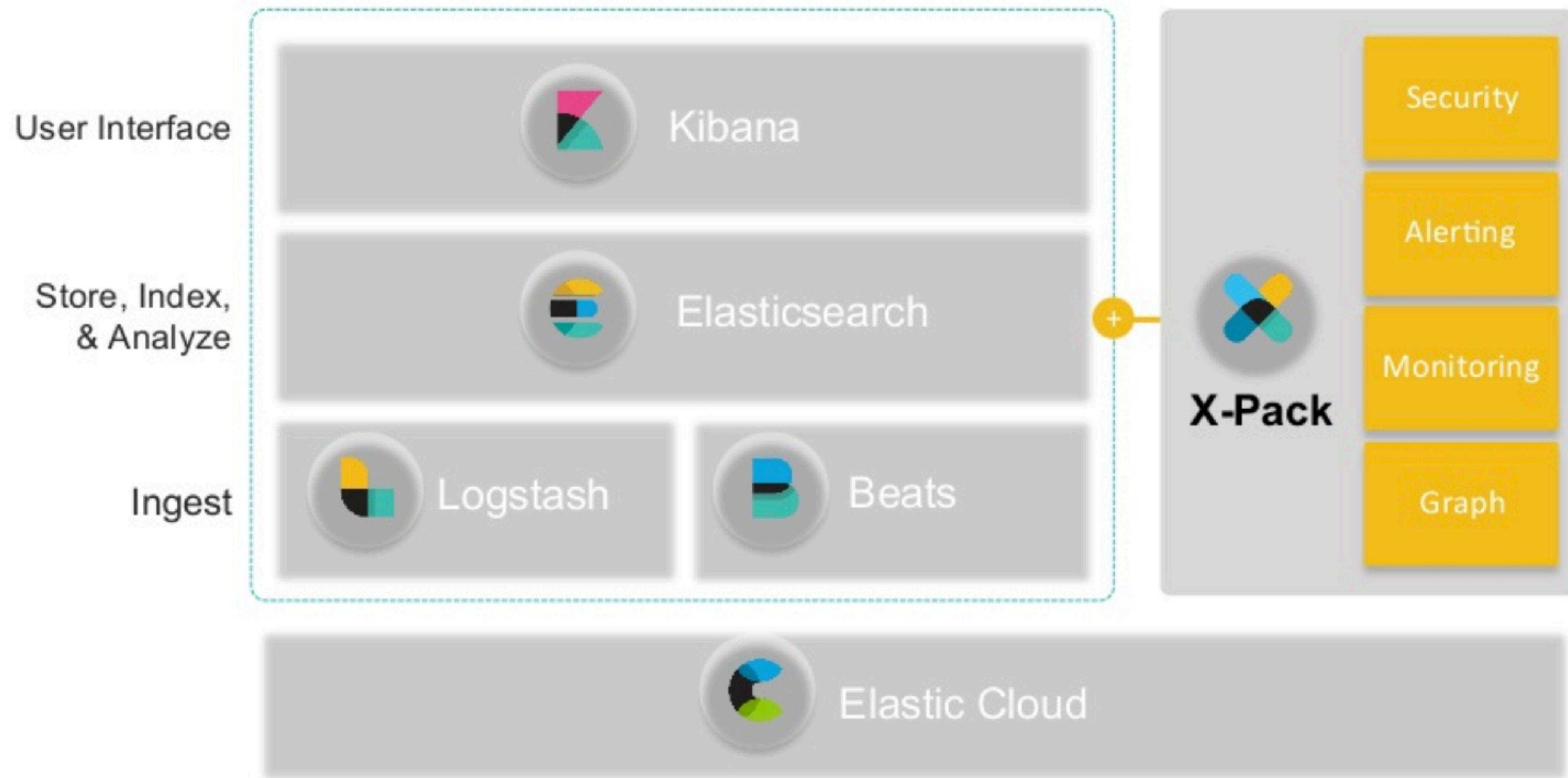


沒什麼能分享給大家

感謝 Square 和 Andy

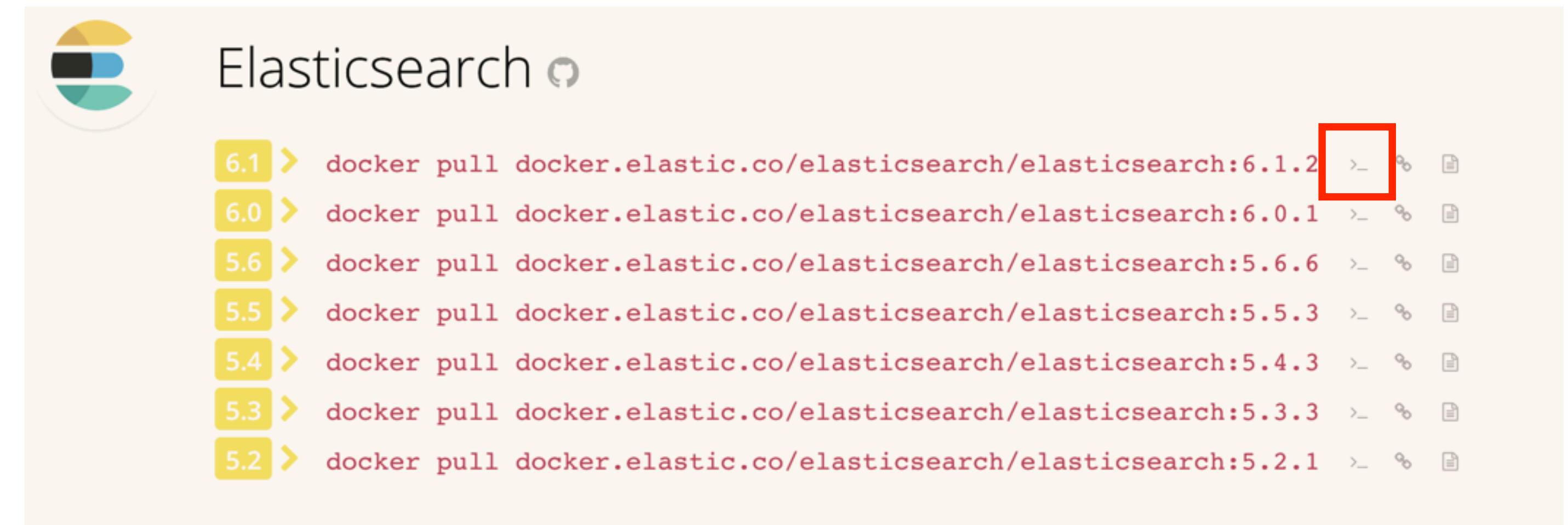


The Elastic Stack



Step1: <https://www.docker.elastic.co/#>

Step2:



Step3: 啟動 Docker

Step4: 執行指令

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



Step1: Mac: https://artifacts.elastic.co/downloads/kibana/kibana-6.1.2-darwin-x86_64.tar.gz

Window: <https://www.elastic.co/guide/en/kibana/current/windows.html>

Step2: 執行

Step3: vim config/kibana.yml

Step4: #server.port:5601

#server.host:“local host”

#server.name:“vickie”

#elasticsearch.url: “http://localhost:9200”

將 # 拿掉，server.name 設定為個人名稱

Step5: 執行指令

./bin/kibana



Step1: <https://www.elastic.co/products/logstash>

Step2: Download

Step3: 安裝 beats

./bin/logstash-plugin install logstash-input-beats

Step4: 執行指令

mkdir conf.d

vim conf.d/test1.conf

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

Version Compatibility with Elasticsearch

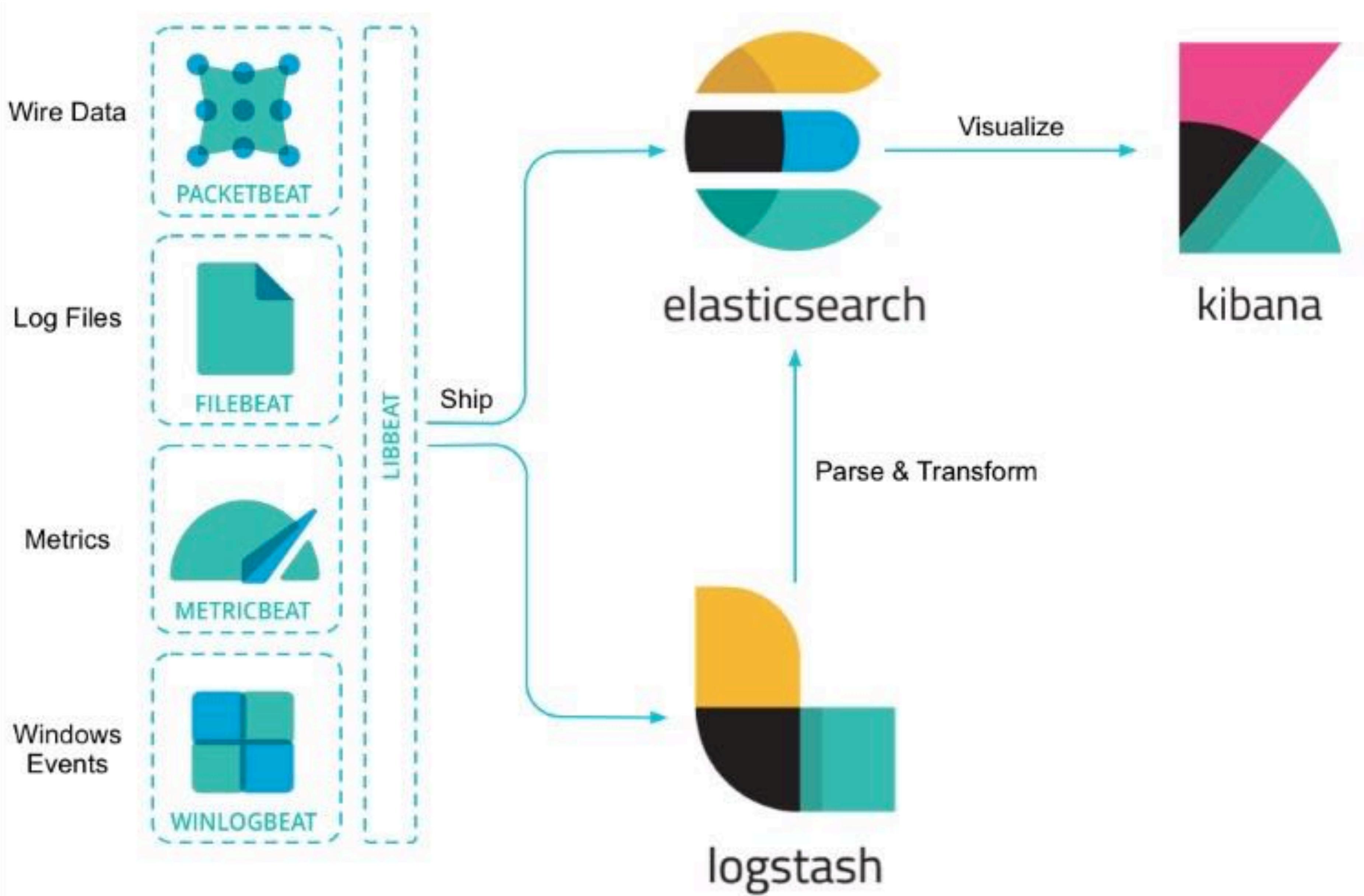
Situation	Example Kibana version	Example ES version	Outcome
Versions are the same.	5.1.2	5.1.2	💚 OK
ES patch number is newer.	5.1.2	5.1.5	⚠️ Logged warning
ES minor number is newer.	5.1.2	5.5.0	⚠️ Logged warning
ES major number is newer.	5.1.2	6.0.0	🚫 Fatal error
ES patch number is older.	5.1.2	5.1.0	⚠️ Logged warning
ES minor number is older.	5.1.2	5.0.0	🚫 Fatal error
ES major number is older.	5.1.2	4.0.0	🚫 Fatal error

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

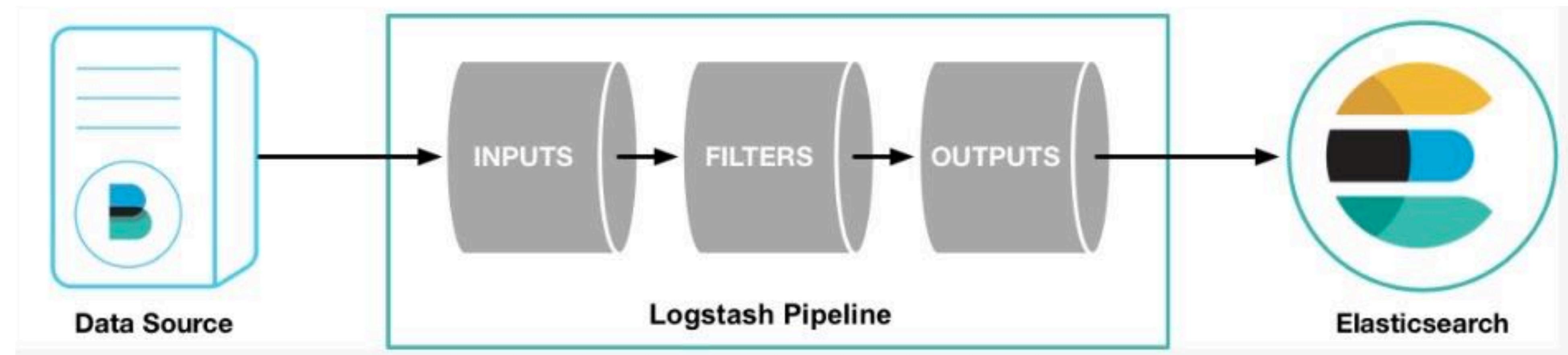
資料做視覺化呈現 (Kibana)。

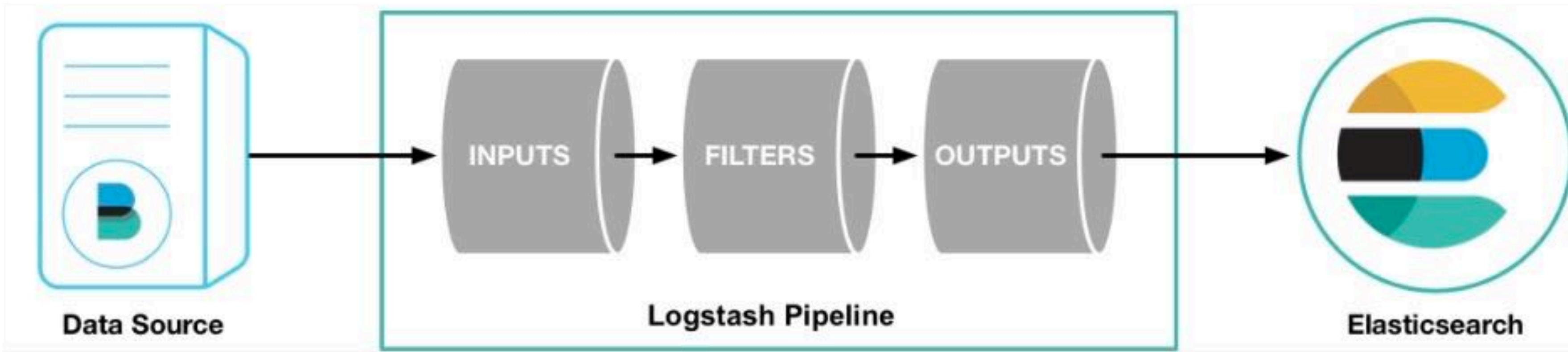


- 
- 提供各式各樣的日誌收集及輸出的 Plugin
 - 可用於串接資料庫或日誌檔案
 - 將資料收集處理後，輸出至 Elasticsearch

- 分散的索引搜尋系統
- 可用於全文檢索
- 提供 REST API 串接
- NoSQL 資料庫的一種，資料以 JSON 進行存取
- 與 MongoDB 一樣都是 Document DB，最大的不同是所有欄位都可以建立索引進行全文搜尋

- 
- 透過網頁介面來呈現資料、製作圖表
 - 透過開發工具對 elasticsearch 執行資料操作
變得更簡單





INPUTS

由各種地方抓取相關的資料，不論是標準輸入
stdin，檔案 (如: csv) 或是監聽一個連線 (如:
kafka) 都可以，並且可以把不同的資料來區隔開
來作為之後用途

```
input {  
    file {  
        path => "/.csv"  
    }  
}
```



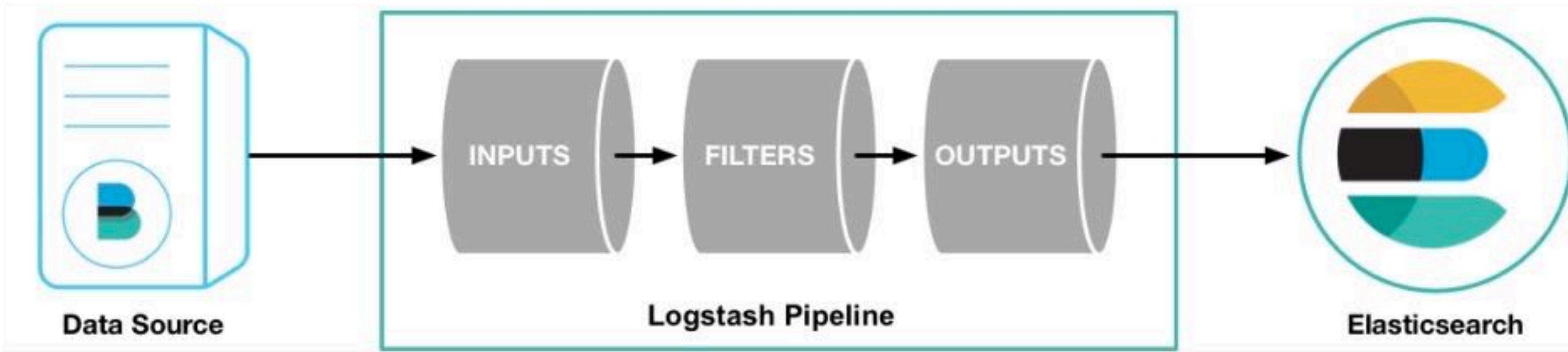
怎麼讓 Logstash 從頭讀文件？

```
input {  
    file {  
        path => "./csv"  
        start_position => "beginning"  
        since_db_path => "/dev/null"  
    }  
}
```



也可以 key-in json 格式文件

```
input {  
    stdin {  
        codec => json  
    }  
}
```



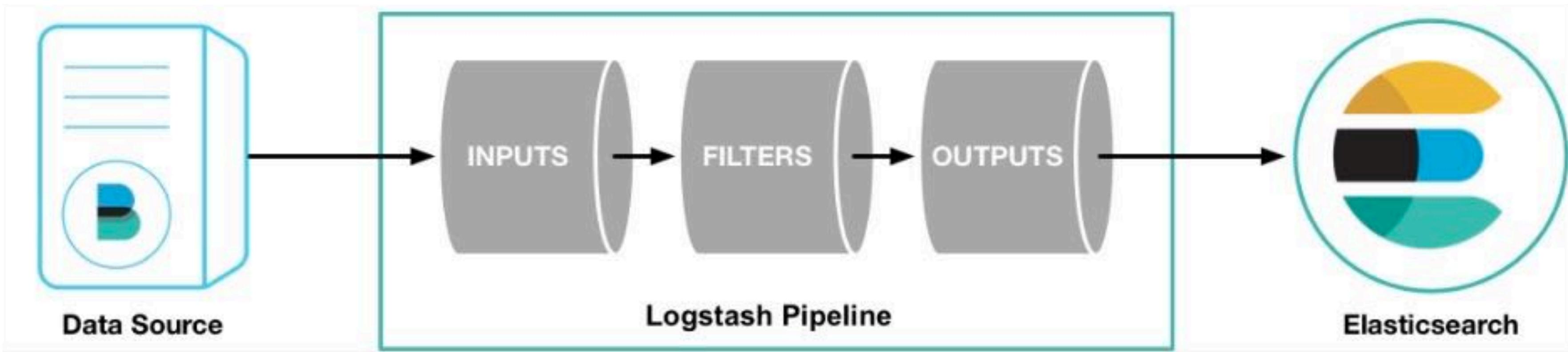
FILTERS

抓取到資料之後，這時候可以選擇使用 grok 去拆解資料，比如說把一串非常長但是沒人看得懂的 log 拆解成各個相對應得資料欄位

```
filter {  
    mutate { #資料型態轉換  
        convert => ["request_time", "float"]  
    }  
}
```



Logstash 在執行 FILTERS 的時候是照順序執行的，有時候依照不同需求會有同樣 Data 需做不同的篩選條件或輸出條件，而在執行多個配置文件可參考<http://www.cnblogs.com/licongyu/p/5442652.html>



OUTPUTS

可以輸出到各種地方，不論是輸出到 `stdout` 印出來，或是直接丟給 Elasticsearch 拿來做分析用甚至可以直接輸出到資料庫

```
output {
```

```
  stdout {
```

```
    codec => rubydebug{ }
```

```
    # codec => json{ }
```

```
}
```

```
}
```



怎麼判斷 Elasticsearch 能不能用？



http://127.0.0.1:9200/

```
{  
  "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"  
}
```

恭喜你！離 Kibana 更近一步了！

http://127.0.0.1:5601/

kibana

-  [Discover](#)
-  [Visualize](#)
-  [Dashboard](#)
-  [Timelion](#)
-  [Dev Tools](#)
-  [Management](#)

 [Collapse](#)

Welcome to Kibana

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

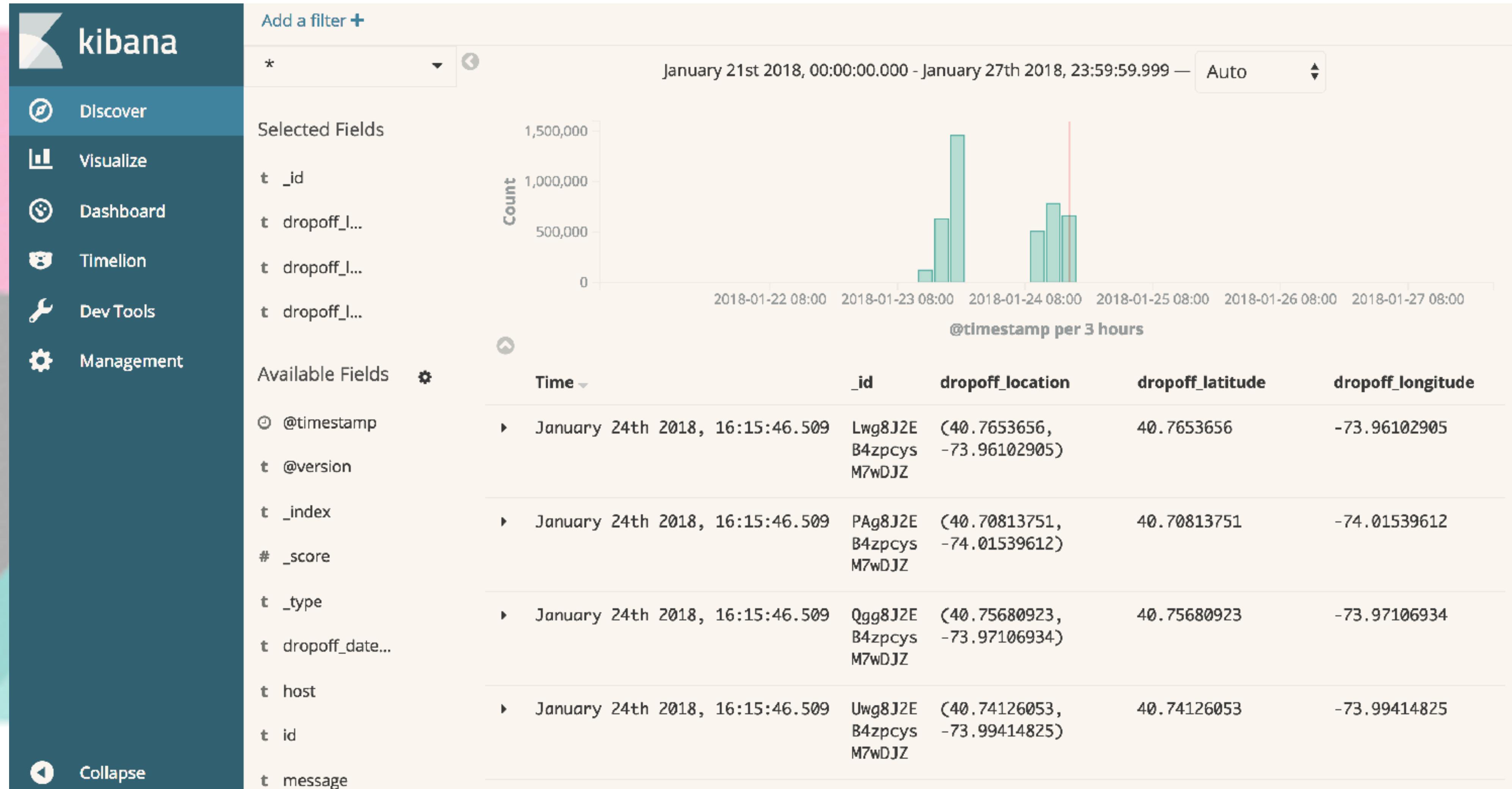
Visualize and Explore Data

-  **Dashboard**
Display and share a collection of visualizations and saved searches.
-  **Discover**
Interactively explore your data by querying and filtering raw documents.
-  **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](#)





kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Status: Red

vickie

Heap Total

71.63 MB

Heap Used

62.25 MB

Load

5.03, 7.30,

7.61

重新投胎！啊不對~重新啟動

Response Time Avg

30527.00 ms

Response Time Max

30527.00 ms

Requests Per Second

0.00

Status Breakdown

ID	Status
plugin:kibana@6.1.2	Ready
plugin:elasticsearch@6.1.2	Request Timeout after 3000ms
plugin:console@6.1.2	Ready

Cat API

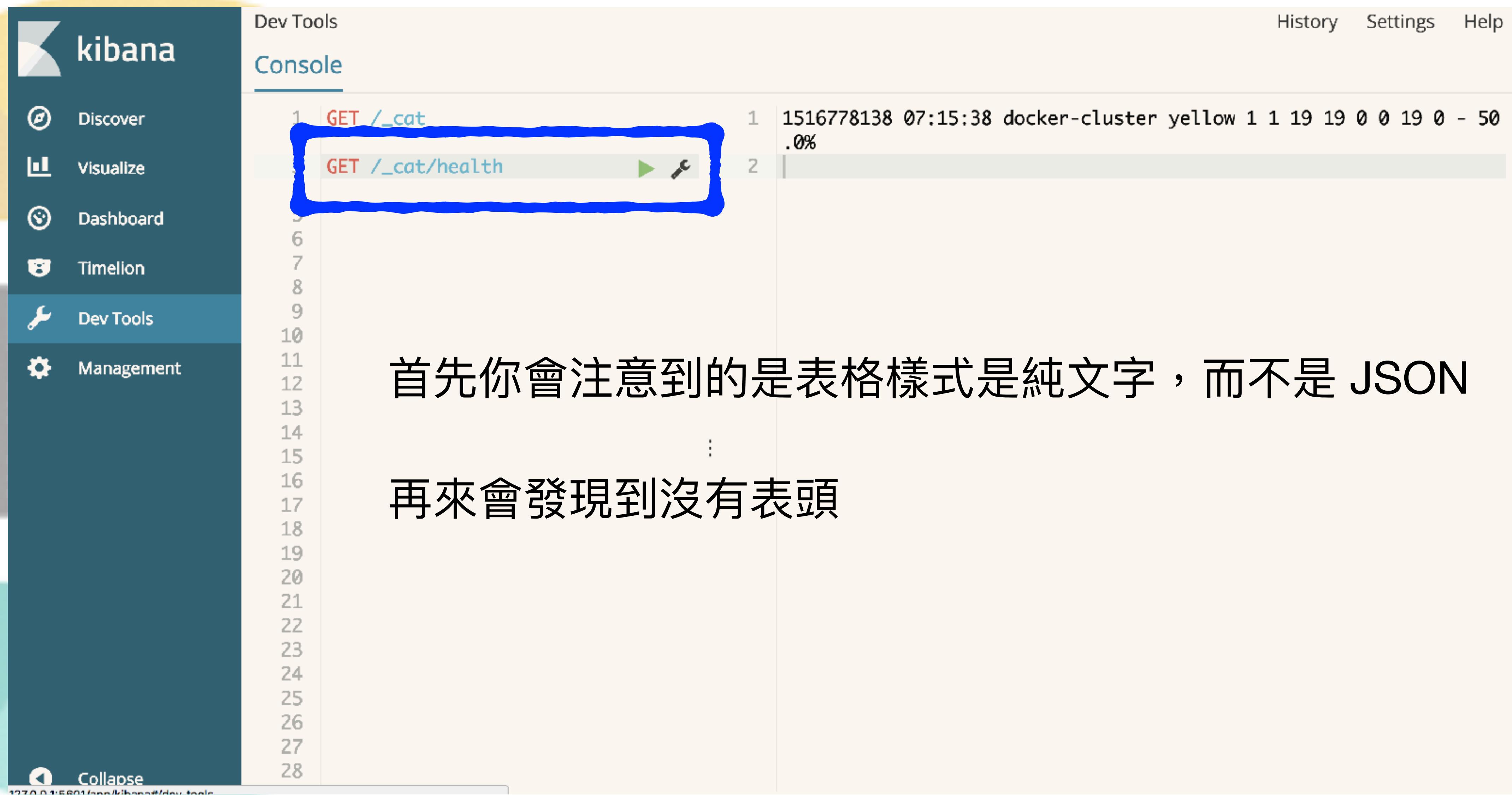
用 Linux 的 cat 命令命名，輸出以表格的形式提供，而不是JSON。當只是想瀏覽一遍集群或者找出內存使用偏高的節點時，對於系統管理員來說這是非常方便的

Dev Tools History Settings Help

Console 通過GET請求發送cat命名可以列出所有可用的API：

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`



The screenshot shows the Kibana Dev Tools Console interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, Dev Tools (which is selected), and Management. The main area is titled "Console" and contains two log entries:

Line	Log Entry
1	1516778138 07:15:38 docker-cluster yellow 1 1 19 19 0 0 19 0 - 50 .0%
2	GET /_cat/health

A blue box highlights the second log entry. The text below the screenshot explains the visual representation of logs in Kibana:

首先你會注意到的是表格樣式是純文字，而不是 JSON

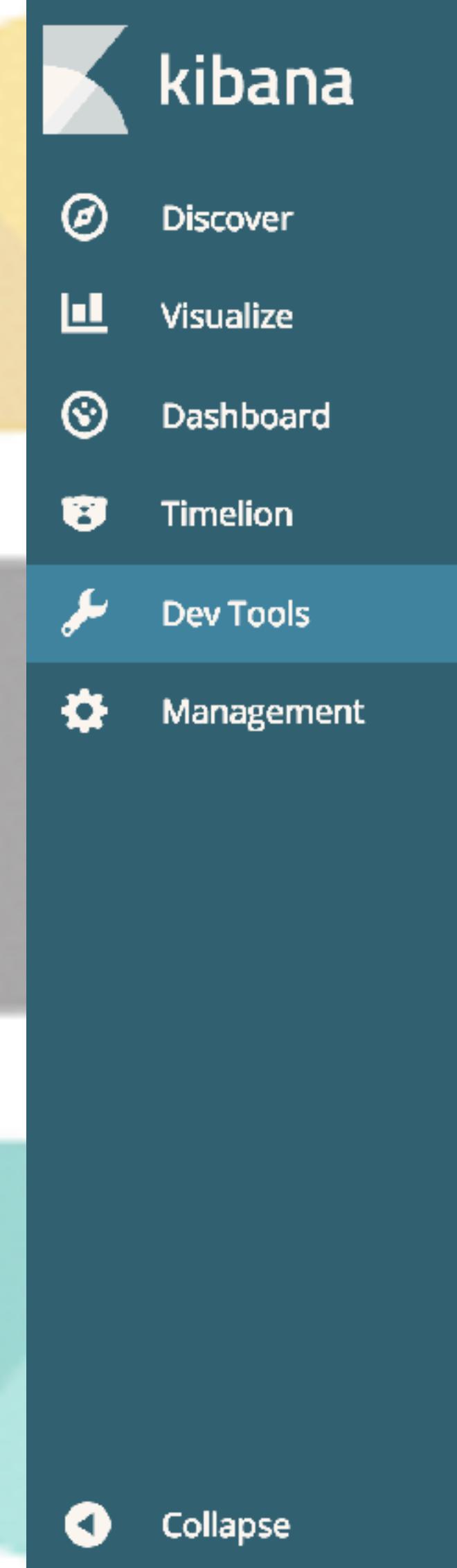
⋮

再來會發現到沒有表頭

要啟用表頭，加上?v 即可

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. A specific request, 'GET /_cat/health?v', is highlighted with a blue box. The response to 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
1516778268	07:17:48	docker-cluster	yellow	1	1	-
19	19	0	0	19	0	50.0%



Dev Tools	看現有的 Logstash 有哪些	History	Settings	Help
Discover				
Visualize				
Dashboard				
Timelion				
Dev Tools				
Management				
	1 GET /_cat	1 health status index	uuid	
	2	pri rep docs.count docs.deleted store.size pri.store.size		
	3 GET /_cat/health	yellow open .monitoring-es-6-2018.01.24 dyCjjss3RyyTlG4oNgfGm		
	4	A 1 1 17992 228 8mb 8mb		
	5 GET /_cat/health?v	yellow open nyc	ZFz1UA13Rzud_PQ3dgIrR	
	6	w 5 1 2122440 0 1.4gb 1.4gb		
	7 GET /_cat/nodes?v	yellow open logstash-2018.01.24	1NQS0eocQuKrr_cBk17e4	
	8	w 5 1 628327 0 157.1mb 157.1mb		
	9 GET /_cat/nodes?help	yellow open logstash-2018.01.23	nY5bDdEJQB2U5a7qAIi29	
	10	A 5 1 752808 0 188.3mb 188.3mb		
	11 GET /_cat/nodes?v&h=ip,port,heapPercent,heapMax	yellow open .kibana	Yuyikeo0Q5SLyp68TUSHH	
	12	A 1 1 4 0 38.6kb 38.6kb		
	13 GET /_cat/indices?v	yellow open .monitoring-es-6-2018.01.22 0tiXa2c3TfWRTjsR2tEEX		
	14	g 1 1 7975 12 3mb 3mb		
	15	yellow open .monitoring-es-6-2018.01.23 arAo5dY1RL2mjNG_ybemq		
	16	g 1 1 26859 182 10.5mb 10.5mb		
	17			
	18			
	19			
	20			
	21			
	22			
	23			
	24			
	25			
	26			
	27			
	28			

檢索 Data

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
23
24
25
26
27
```

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 " " } }] } }

藉由查找出的資訊反檢索 Data

kibana Dev Tools Console

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

2 "took": 8,
3 "timed_out": false,
4 "_shards": {
5 "total": 5,
6 "successful": 5,
7 "skipped": 0,
8 "failed": 0
9 },
10 "hits": {
11 "total": 2122440,
12 "max_score": 1,
13 "hits": [
14 {
15 "_index": "nyc",
16 "_type": "doc",
17 "_id": "8tW6ImEB4zpcysM75k1c",
18 "_score": 1,
19 "_source": {
20 "path": "/Users/vickieliu/Downloads/ny_taxi/train
.csv",
21 "@version": "1",
22 "@timestamp": "2018-01-23T11:15:21.777Z",
23 "vendor_id": "2",
24 "pickup_longitude": "-73.95611572265625",
25 "id": "id3491576",
26 "store_and_fwd_flag": "N",
27 "dropoff_datetime": "2016-01-14 10:10:49",
28 "dropoff_latitude": "40.760963439941406",
29 }
30 }
31 }
32 }

kibana

Dev Tools

Console

尋找特定 Data

Discover

Visualize

Dashboard

Timeline

Dev Tools

Management

Collapse

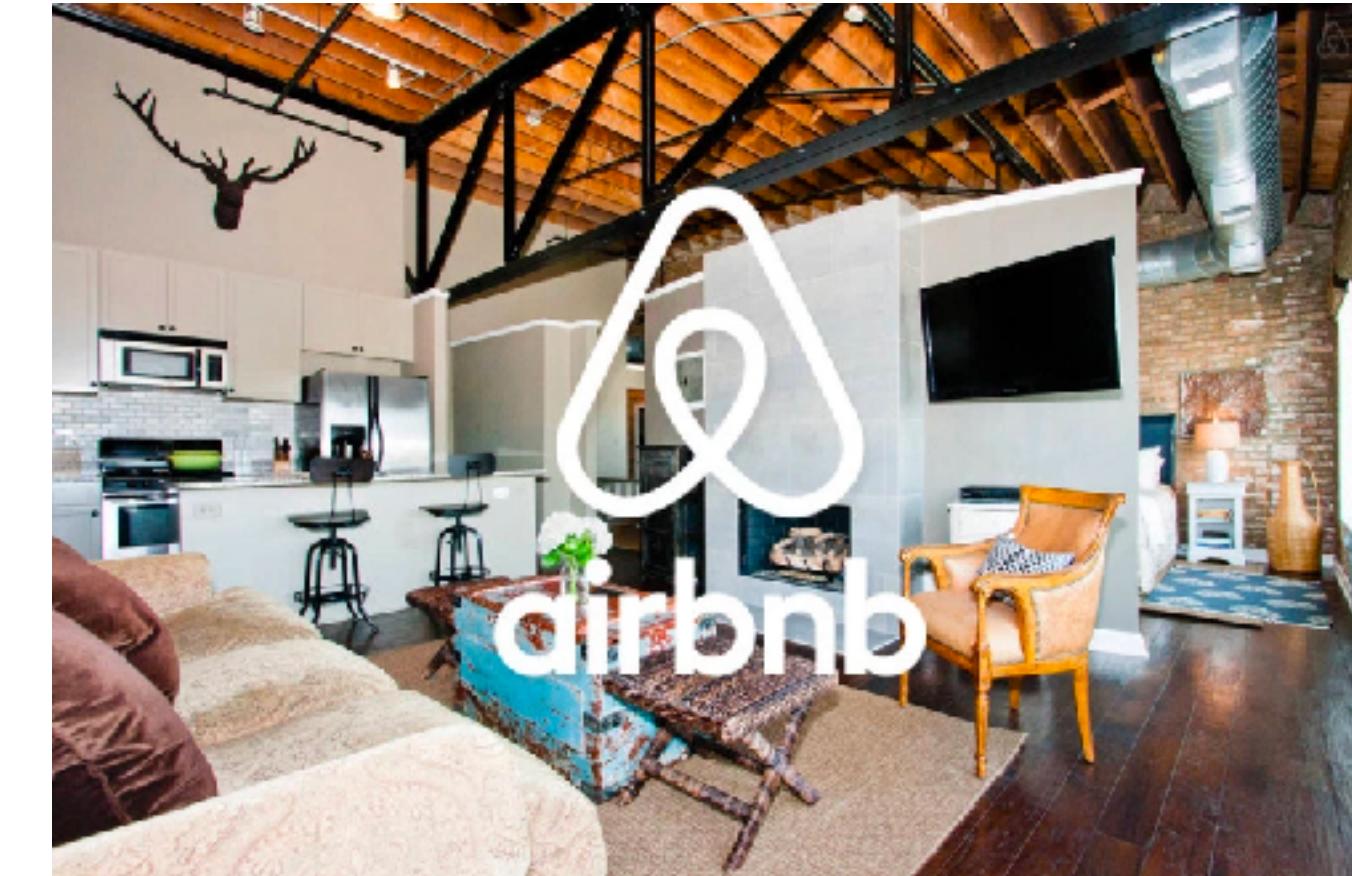
```
15 16 {  
17   "query": {  
18     "match_all": {}  
19   }  
20 }  
21  
22 GET /logstash-2018.01.23/_search  
23 {  
24   "query": {"match":{  
25     "id":"gxn3p5htnn"  
26   }}  
27 }  
28  
29 GET /nyc/_search  
30 {  
31   "query": {  
32     "match_all": {}  
33   }  
34 }  
35  
36 GET /nyc/doc/8tW6ImEB4zpcysM75k1c|  
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 }
```

/train_users.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.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.csv

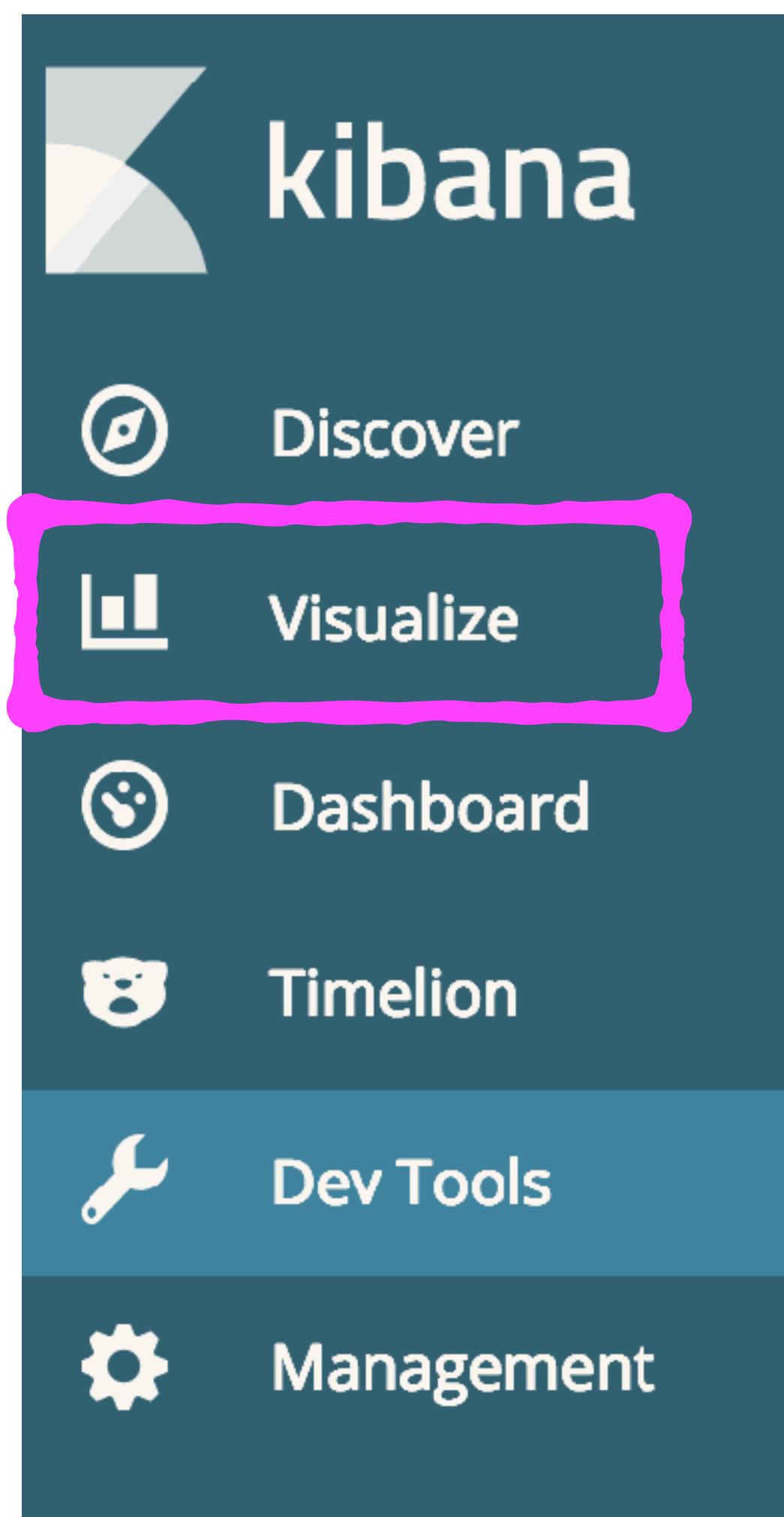
language	affiliate_channel	affiliate_provider	first_affiliate_tracked	signup_app	first_device_type	first_browser	country_destination
en	direct	direct	untracked	Web	Mac Desktop	Chrome	NDF
en	seo	google	untracked	Web	Mac Desktop	Chrome	NDF
en	direct	direct	untracked	Web	Windows Desktop	IE	US
en	direct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

/test1.conf

```
1 input {  
2     file {  
3         path => "/Users/vickieliu/Downloads/train_users.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", "date_first_booking", "gender",  
12         "age", "signup_method", "signup_flow", "language", "affiliate_channel", "affiliate_provider",  
13         "first_affiliate_tracked", "signup_app", "first_device_type", "first_browser", "country_destination"]  
14     }  
15 }  
16 output {  
17     elasticsearch {  
18         hosts => ["localhost:9200"] # "http://localhost:9200"  
19     }  
20     stdout {  
21         codec => rubydebug{ }  
22     }  
23 }
```

Shutdown Logstash

```
liupinrude-MacBook-Pro:logstash-6.1.2 vickieliu$ ps aux | grep logstash
vickieliu      3856  10.0  5.5  6965588 457852  885  S+   2.38+  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     881  882  S+   3:40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$
```



Visualize / New Visualization (unsaved)

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 x

Aggregation

Terms

Field

age.keyword

Order By

metric: Count

Order

Descending ↑ 5 ↓

Custom Label

30
29
28
27
31

A donut chart with five segments. The segments are colored green, blue, purple, pink, and brown. A legend on the right lists the colors with their corresponding values: green (30), blue (29), purple (28), pink (27), and brown (31). The segments correspond to these values in clockwise order starting from the top.

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

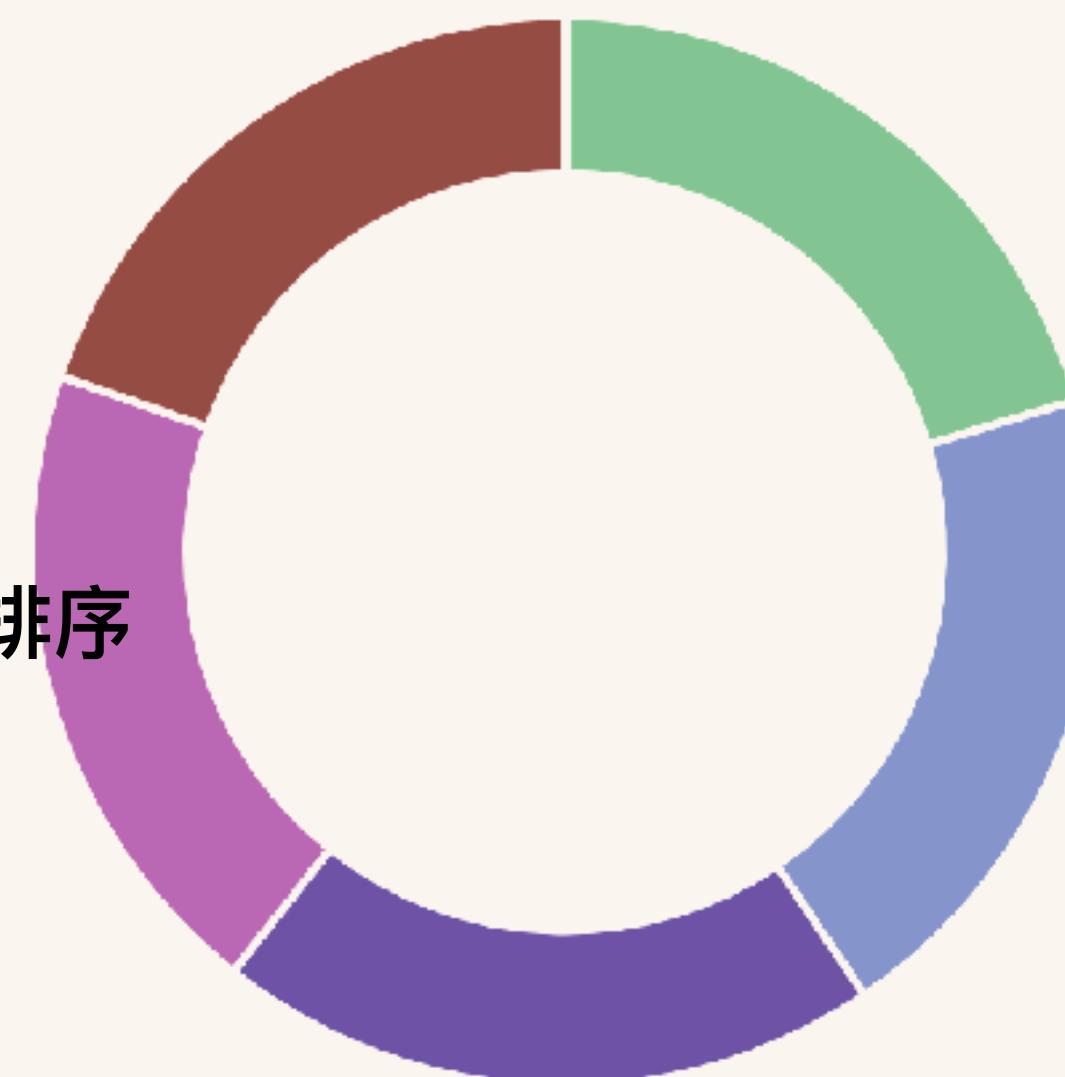


Size



Custom Label

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

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

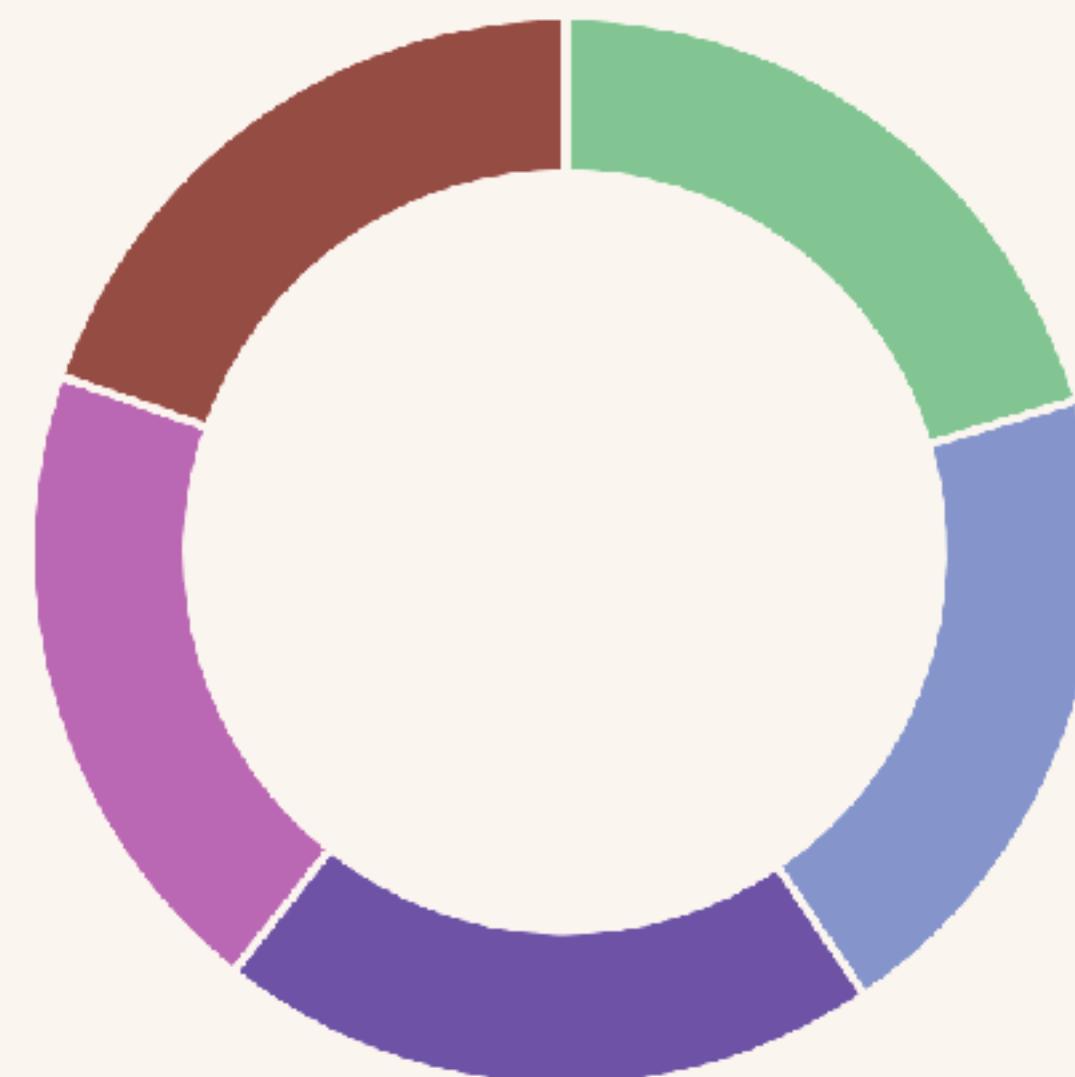
Descending

Size

5

Custom Label

排序是按數量排序



- 30
- 29
- 28
- 27
- 31

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

Buckets

Split Slices



Aggregation

Terms

Field

age.keyword

Order By

metric: Count

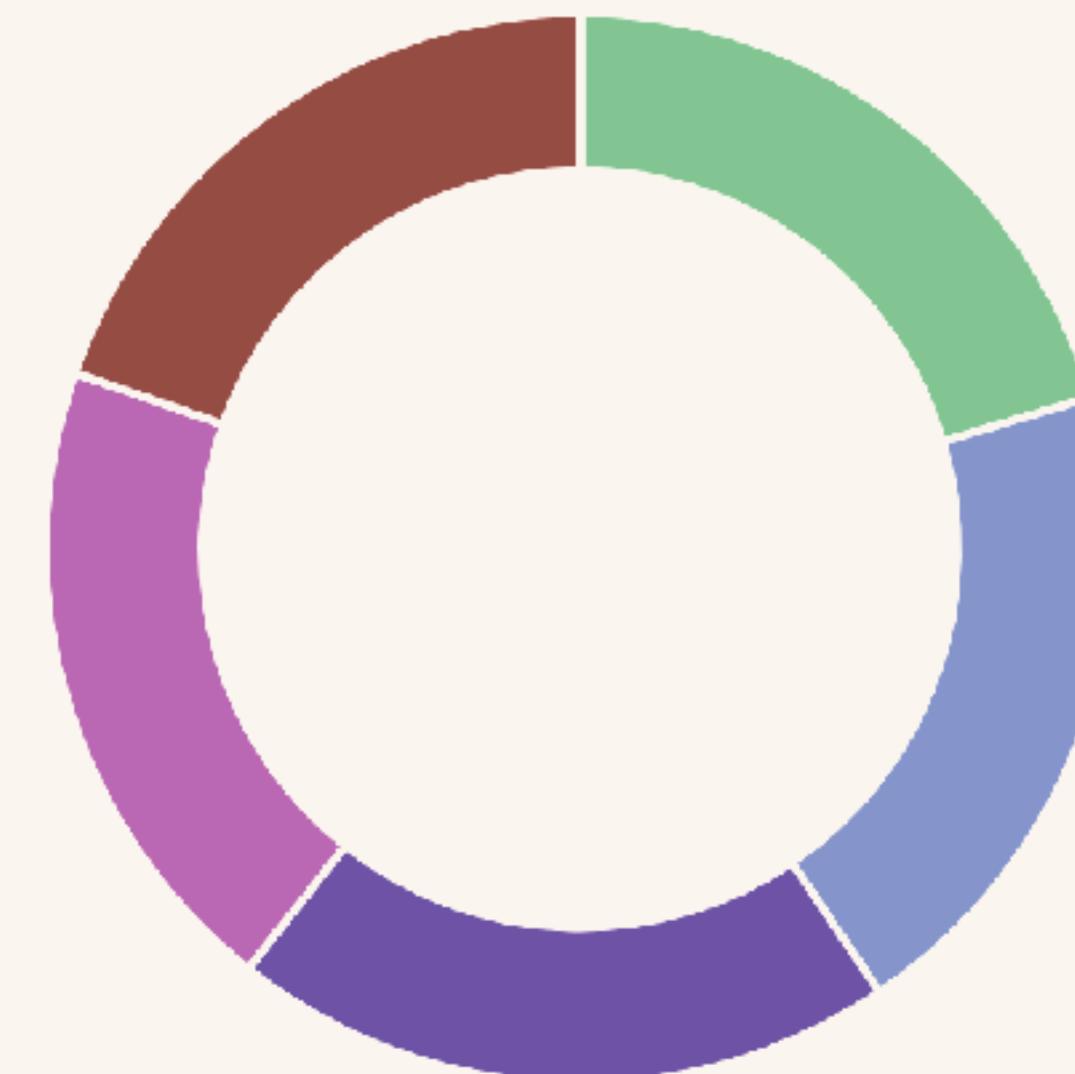
Order

Descending

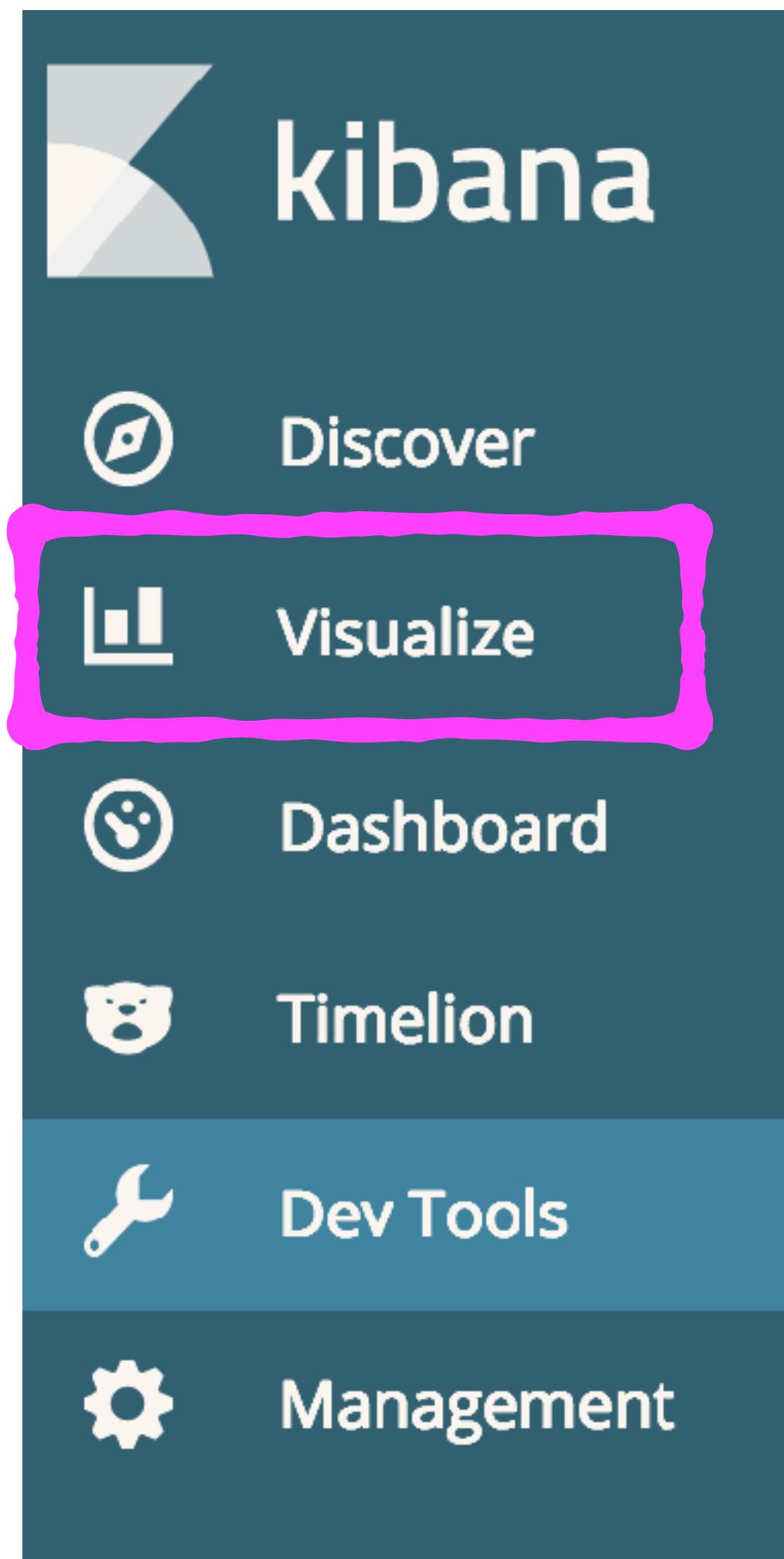
Size

5

Custom Label



保持默認值比較不容易出錯



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

Uses lucene query syntax



Add a filter +

log*

Data Options



Count

Slice Size

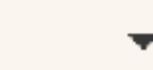
Buckets

Split Slices



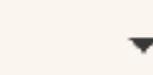
Aggregation

Terms



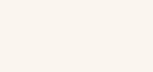
Field

age.keyword



Order By

metric: Count



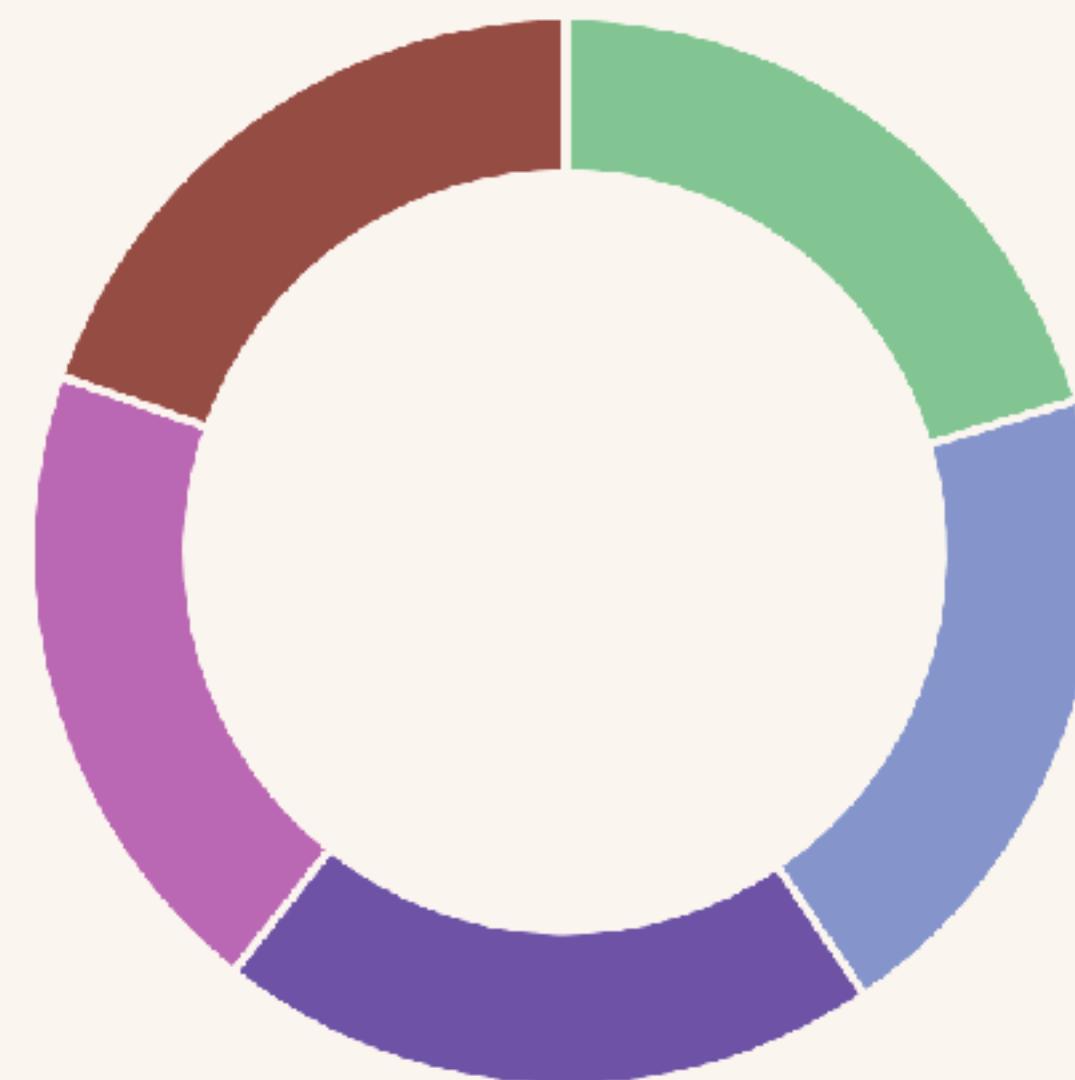
Order

Descending

Size

5

Custom Label



圖形標籤名稱

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

Uses lucene query syntax



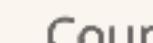
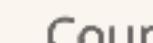
Add a filter +

log*

Data Options



Slice Size



Count

Buckets

Split Slices



Aggregation

Terms



Field

age.keyword



Order By

metric: Count



Order

Descending

Size

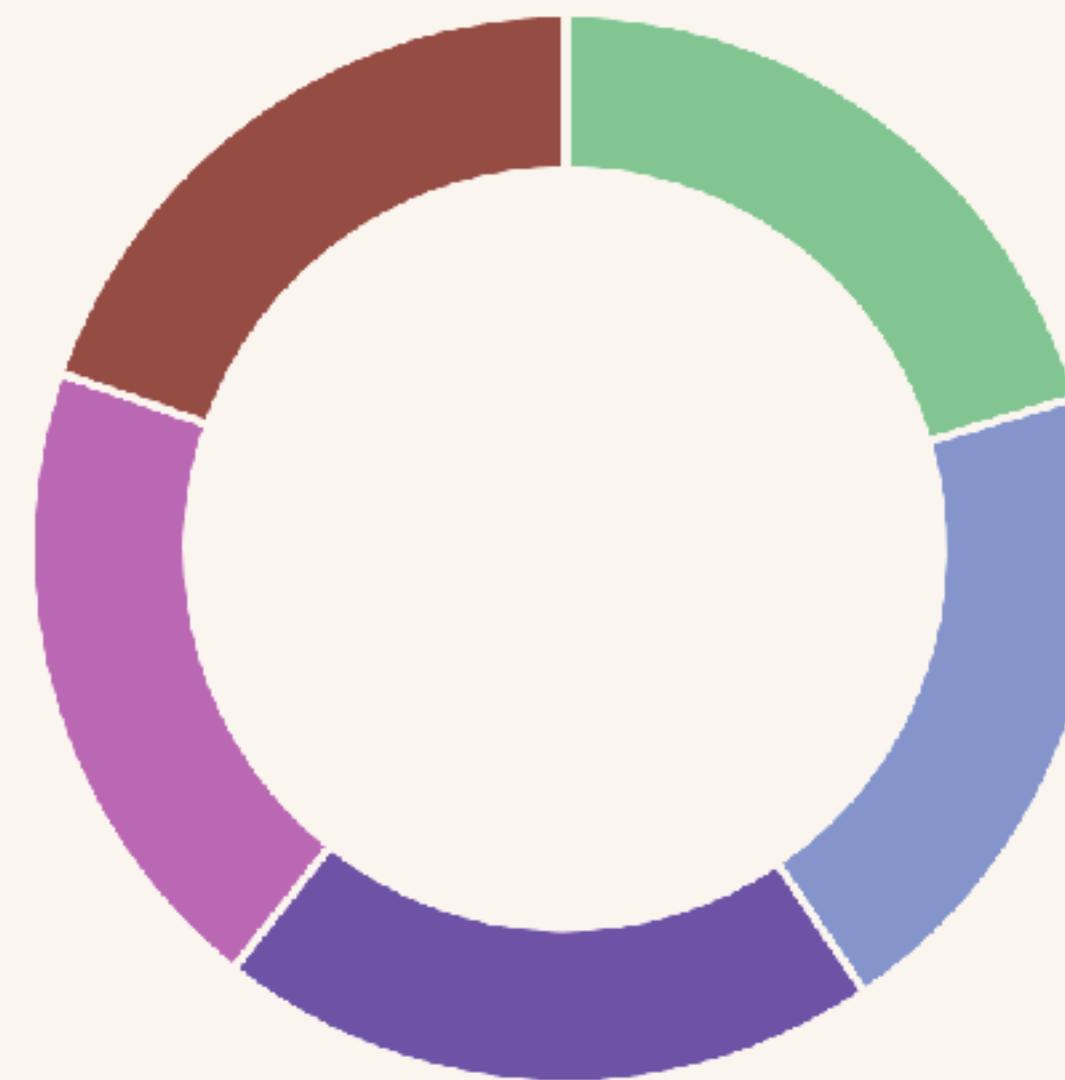


5

Custom Label

如果都設定好，也是自己想要的樣子，即可存檔

- 30
- 29
- 28
- 27
- 31



kibana

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

ELK Stack (Elasticsearch + Logstash + Kibana)

可以幫你解決一些問題如下：

- 太長的 log 却沒有一個方法可以整理跟分析它
- 太多來源的 log，每次查詢一個問題需要打開三四個檔案，但是往往還是不知道原因，得要人工查詢
- 想要透過系統的 log 去做一些商業智慧的分析，但是無從下手

Hands on !

建立一個路徑並將檔案放入

小提醒: 檔名與路徑盡可能都以英文小寫與 _ 符號作為間隔，
在讀取的時候比較不容易出現檔名格式不合的問題

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

-
-
-