

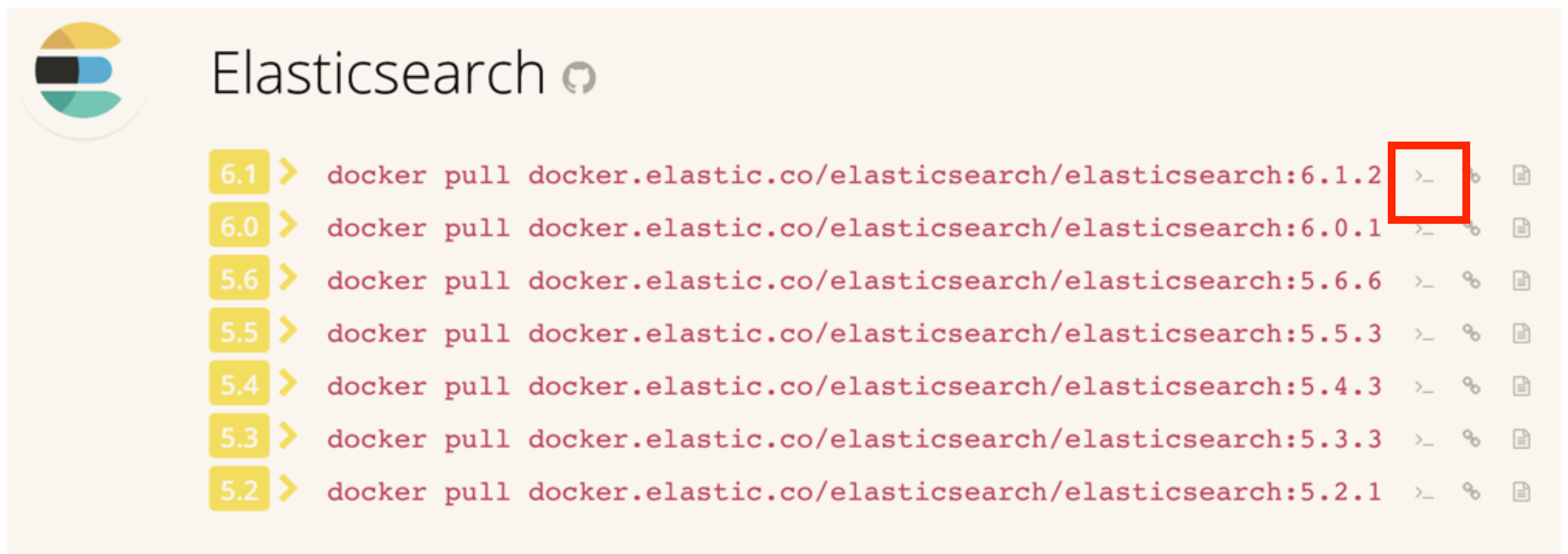


Install Elasticsearch

Step1: 在瀏覽器中開啟

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

Step2: 進入網址後點選紅色方框（複製指令）



Elasticsearch

Version	Command	Copy	Share	Download
6.1	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:6.1.2</code>	>_ (highlighted)	>_	Download
6.0	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:6.0.1</code>	>_	>_	Download
5.6	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:5.6.6</code>	>_	>_	Download
5.5	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:5.5.3</code>	>_	>_	Download
5.4	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:5.4.3</code>	>_	>_	Download
5.3	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:5.3.3</code>	>_	>_	Download
5.2	<code>docker pull docker.elastic.co/elasticsearch/elasticsearch:5.2.1</code>	>_	>_	Download

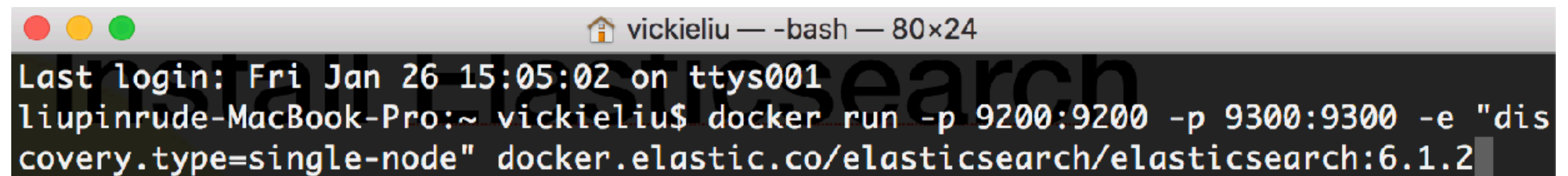
Step3: 啟動 Docker

(若未安裝 Docker 請參考 <https://github.com/b96705008/DTAG-sharing/blob/master/2017.08.25-Docker/Introduce%20Docker.pdf>)



**Step4: 開啟 cmd 後貼上剛剛 Step2 複製的指令
下載完成後若要啟動 Elasticsearch 請在
cmd 執行下方指令**

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

A screenshot of a macOS terminal window. The title bar shows a home icon, the username 'vickieliu', and the shell '-bash' with a window size of '80x24'. The terminal content shows a login message: 'Last login: Fri Jan 26 15:05:02 on ttys001'. Below that, the prompt 'liupinrude-MacBook-Pro:~ vickieliu\$' is followed by the command 'docker run -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" docker.elastic.co/elasticsearch/elasticsearch:6.1.2'. The command is partially highlighted with a light blue background.

```
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
```

**Step4: 開啟 cmd 後貼上剛剛 Step2 複製的指令
下載完成後若要啟動 Elasticsearch 請在
cmd 執行下方指令**

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



But ...

**實際使用過會發現下次再開啟 Elasticsearch 的時候
上次導入的資料都不見了**

**如果希望留住之前使用的資料，需建立一個 volume，就像是
開一個虛擬的硬碟空間，將那個 volume 連結 (mount) 到
Elasticsearch 的 container，之後整個 Docker 重啟時，只
要指定原先使用的 volume 就能連到上次存的資料**

如果希望留住之前使用的資料，請將 Step 4 改為
(紅色部分為新增部分)

Step 4: 若要啟動 Elasticsearch 請在 cmd 執行下方指令
docker volume create elasticsearch-vol

```
docker run --name elasticsearch6.1 -v elasticsearch-vol:/usr/share/elasticsearch/data  
-p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" docker.elastic.co/  
elasticsearch/elasticsearch:6.1.2
```

下次開啟時，請在 cmd 執行下方指令即可使用上次的資料

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

Step5: 在瀏覽器開啟

<http://127.0.0.1:9200/>

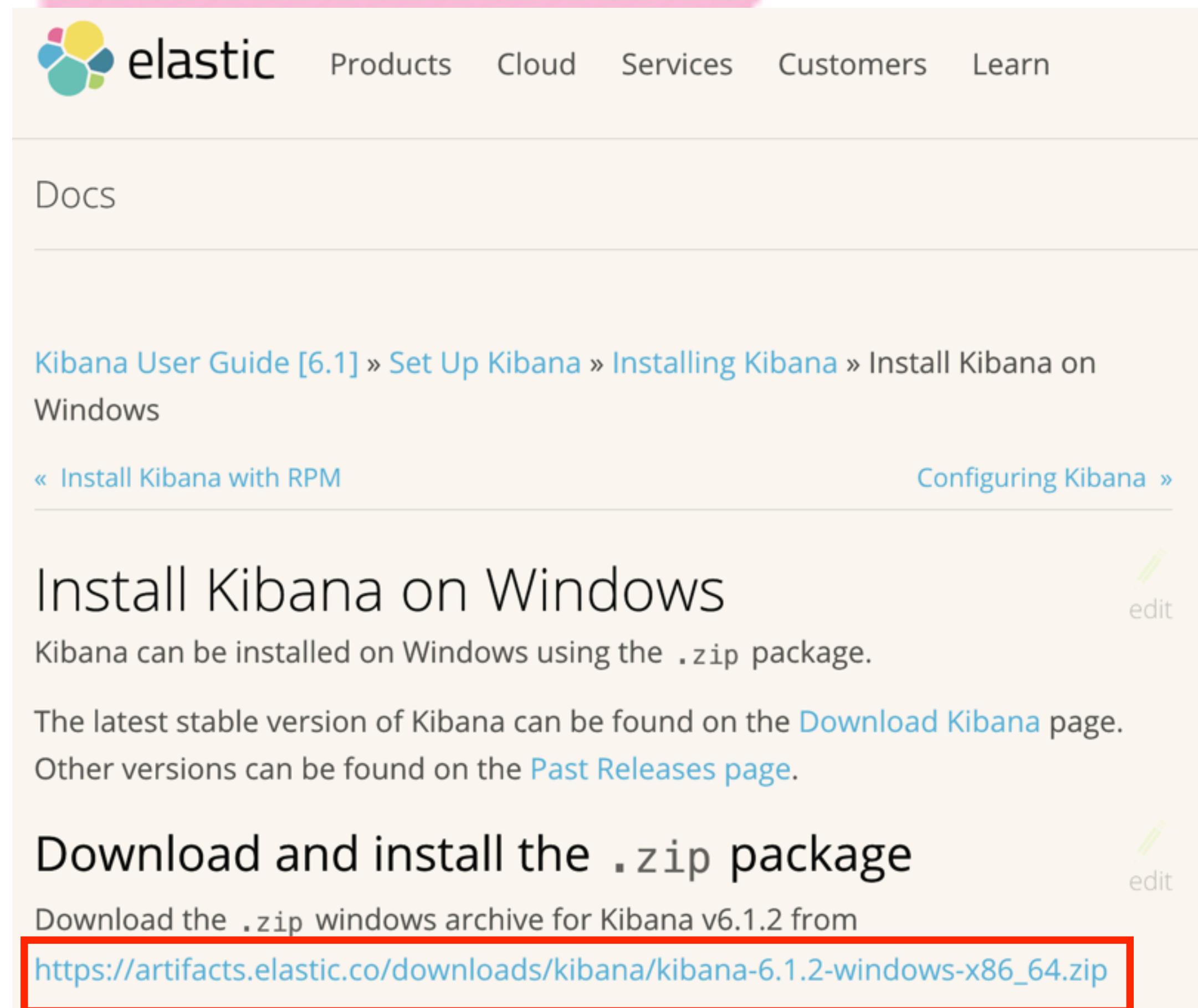
看到下方畫面則表示啟動成功，若出現紅色方框的內容則表示在執行步驟中有錯誤需修正



```
{
  "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"
}
```




Install Kibana



The screenshot shows the Elastic Kibana User Guide page for Windows installation. The page has a pink header bar with the Elastic logo and navigation links: Products, Cloud, Services, Customers, and Learn. Below the header, the breadcrumb trail is: Docs » Kibana User Guide [6.1] » Set Up Kibana » Installing Kibana » Install Kibana on Windows. The main content area is titled 'Install Kibana on Windows' and includes the text: 'Kibana can be installed on Windows using the .zip package. The latest stable version of Kibana can be found on the Download Kibana page. Other versions can be found on the Past Releases page.' Below this, there is a section titled 'Download and install the .zip package' with the instruction: 'Download the .zip windows archive for Kibana v6.1.2 from' followed by a URL: https://artifacts.elastic.co/downloads/kibana/kibana-6.1.2-windows-x86_64.zip. The URL is highlighted with a red rectangular box.

elastic Products Cloud Services Customers Learn

Docs

Kibana User Guide [6.1] » Set Up Kibana » Installing Kibana » Install Kibana on Windows

« Install Kibana with RPM Configuring Kibana »

Install Kibana on Windows

Kibana can be installed on Windows using the .zip package.

The latest stable version of Kibana can be found on the [Download Kibana](#) page. Other versions can be found on the [Past Releases](#) page.

Download and install the .zip package

Download the .zip windows archive for Kibana v6.1.2 from

https://artifacts.elastic.co/downloads/kibana/kibana-6.1.2-windows-x86_64.zip

Step1: 在瀏覽器中開啟

Mac 使用者請開啟: https://artifacts.elastic.co/downloads/kibana/kibana-6.1.2-darwin-x86_64.tar.gz

下載完成後請執行

Window 使用者請開啟: <https://www.elastic.co/guide/en/kibana/current/windows.html>

**並點選紅色方框內的 zip 檔進行下載
完成後請執行**

Step2: 下載完成後請進入 Kibana 資料夾

路徑下 config 中有 kibana.yml 內容需要修改

vim config/kibana.yml

```
liupinrude-MacBook-Pro:resources vickieliu$ ls
PyPubSub          kibana-6.1.2
elasticsearch-6.0.0  logstash-6.1.2
kafka              mongodb
liupinrude-MacBook-Pro:resources vickieliu$ pwd
/Users/vickieliu/Developer/resources
liupinrude-MacBook-Pro:resources vickieliu$
```

```
liupinrude-MacBook-Pro:resources vickieliu$ cd kibana-6.1.2/
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$
```

```
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ cd config/
liupinrude-MacBook-Pro:config vickieliu$ ls
kibana.yml
liupinrude-MacBook-Pro:config vickieliu$
```


Step3: 找到檔案中下面這四行並將 # 拿掉

其中 server.name 請設定為個人名稱，其餘毋須更動


#server.port:5601

#server.host:"local host"

#server.name:"vickie"

#elasticsearch.url: "http://localhost:9200"

修改後如下:



```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601
# Specifies the address to which the Kibana server will bind. IP addresses and host
# names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able
# to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"
# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# This only affects the URLs generated by Kibana, your proxy is expected to remove the
# basePath value before forwarding requests to Kibana. This setting cannot end in a slash.
server.basePath: ""
# The maximum payload size in bytes for incoming server requests.
server.maxPayloadBytes: 1048576
# The Kibana server's name. This is used for display purposes.
server.name: "vickie"
# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://localhost:9200"
```


Step4: 存檔後即可啟動 Kibana

這時請回到 Step2 的 Kibana 資料夾執行指令

`./bin/kibana`

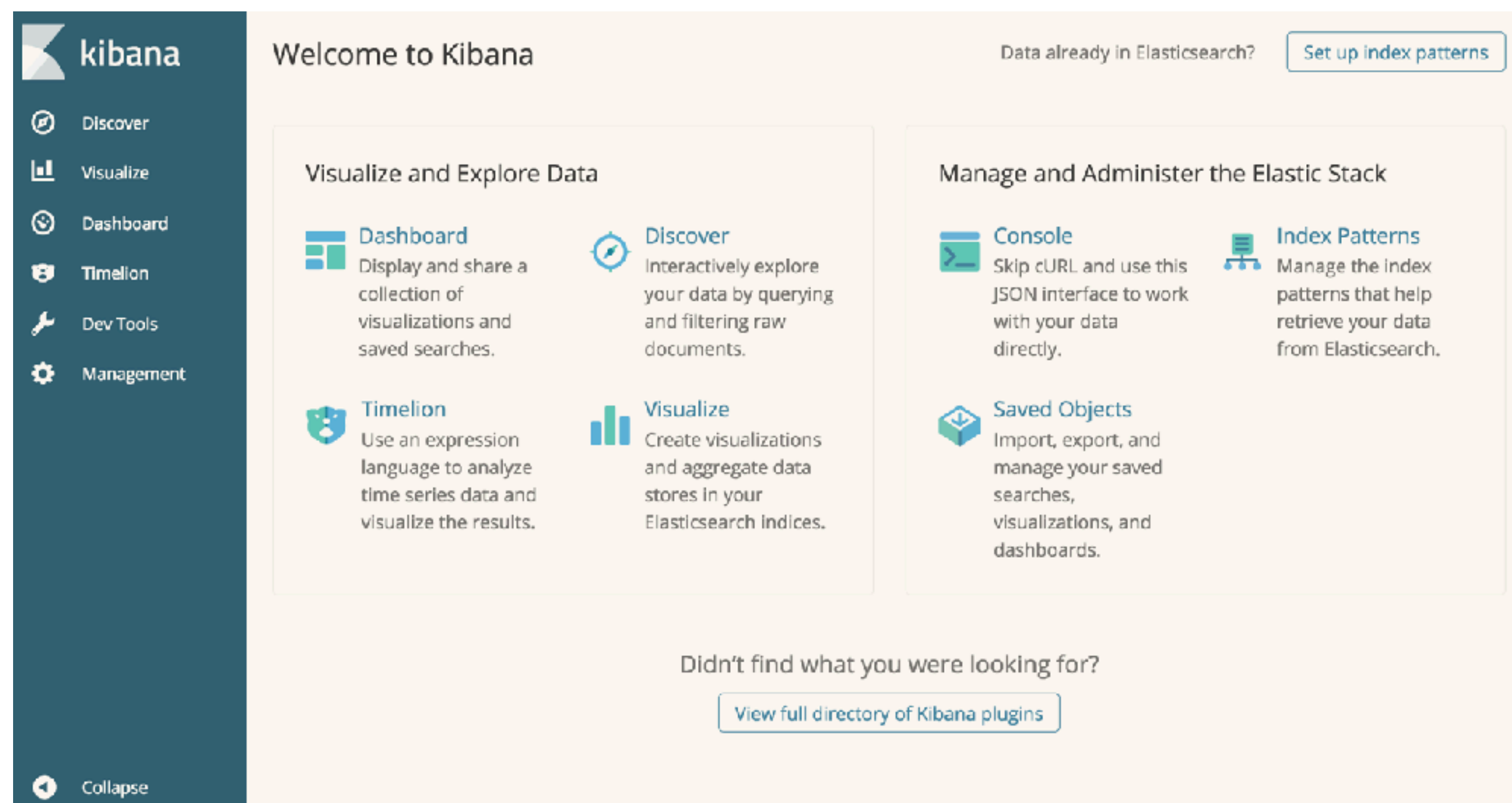
```
liupinrude-MacBook-Pro:kibana-6.1.2 vickieliu$ ls
LICENSE.txt      bin              node             package.json     ui_framework
NOTICE.txt       config          node_modules     plugins          webpackShims
README.txt       data            optimize         src
liupinrude-MacBook-Pro:kibana-6.1.2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

Step5: 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）



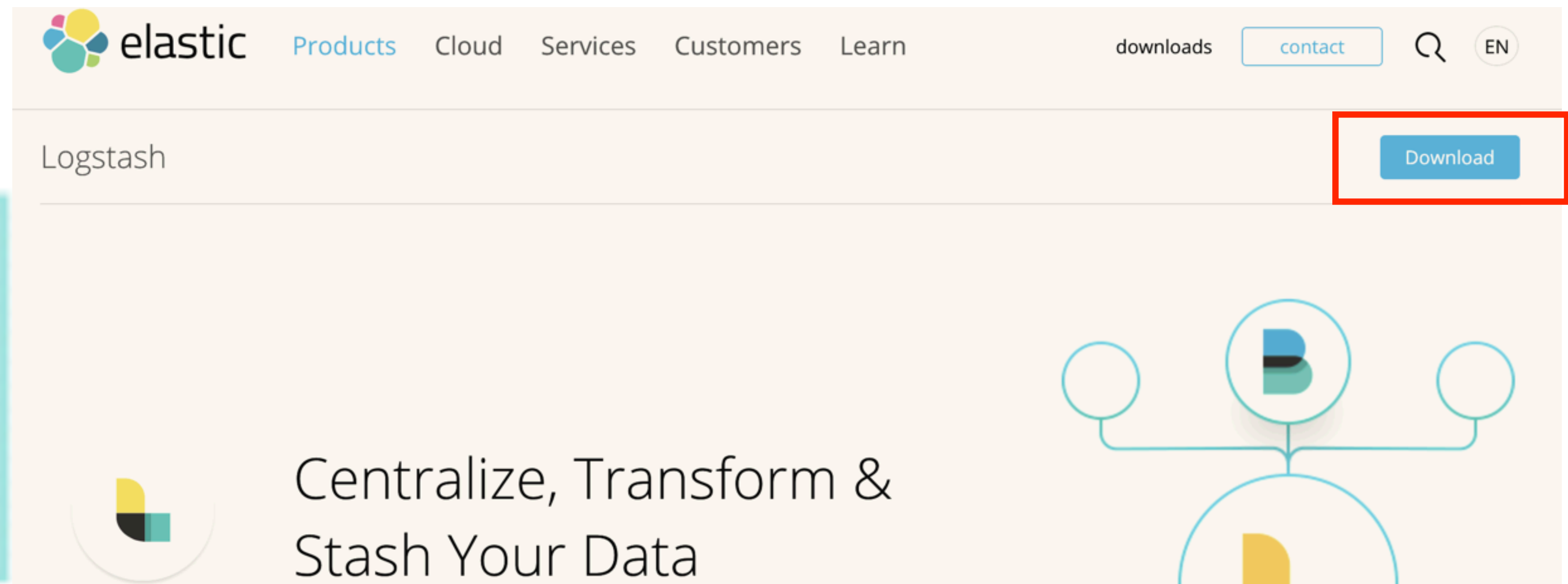


Install Logstash

Step1: 在瀏覽器中開啟

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

點選紅色方框進行下載



Step2: 擇一進行下載並執行（個人是選擇 zip 進行下載）

Downloads

Download Logstash



Want to upgrade? We'll give you a hand. [Migration Guide](#) »

Version: 6.1.2

Release date: January 16, 2018

Notes: View detailed [release notes](#).
Not the version you're looking for? View [past releases](#).
Java 8 is required for Logstash 6.x and 5.x.

Downloads: [TAR.GZ](#) sha

[ZIP](#) sha

[DEB](#) sha

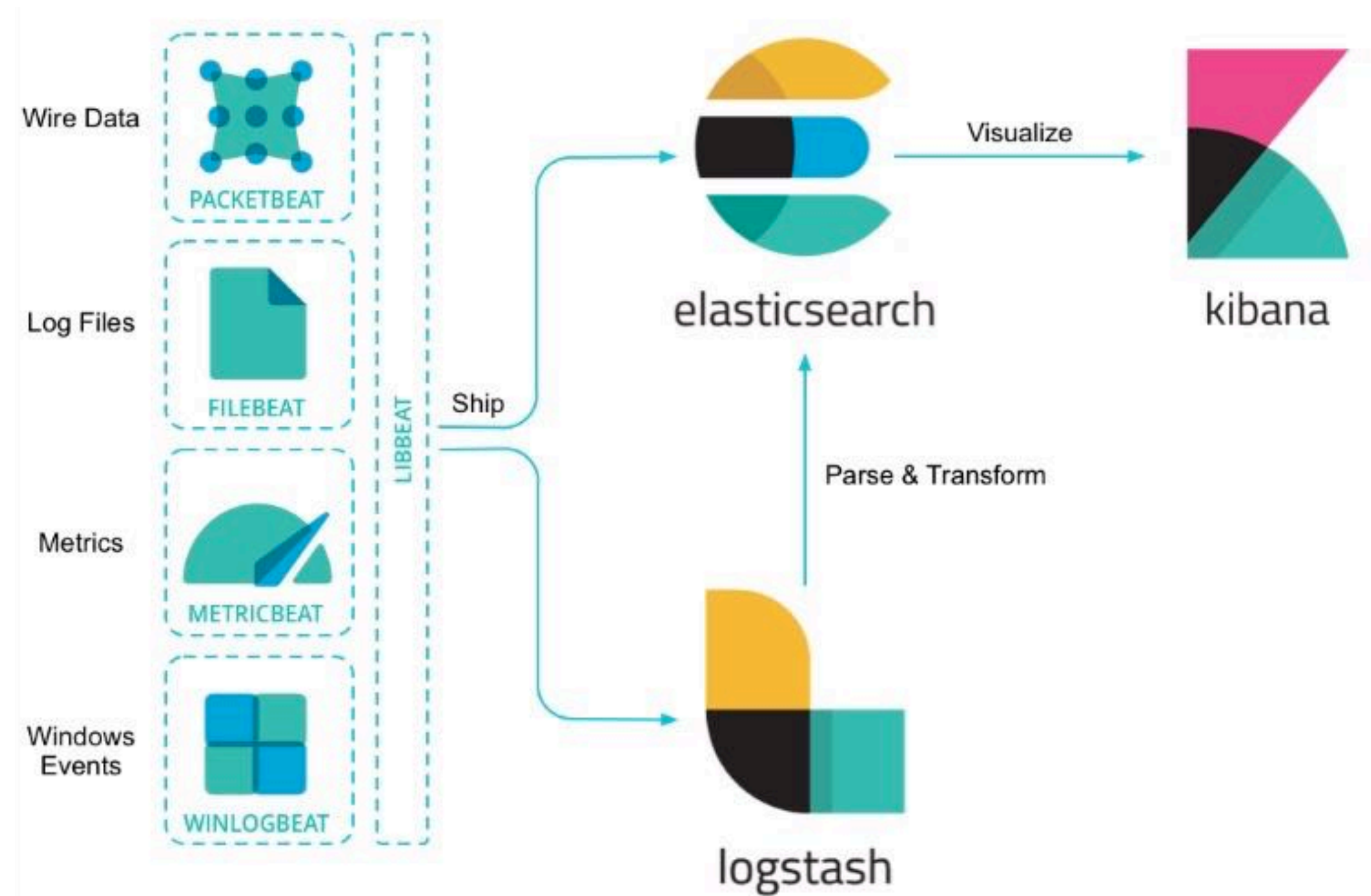
[RPM](#) sha

Step3: 安裝 beats

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

這個步驟安裝與否皆可，此次未用到
關於 beats 的簡介可參考下方網址

<http://www.itread01.com/articles/1488761834.html>



Step4: 當安裝完成時，開啟 cmd 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: 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、
sourcedb_path

kafka

監聽資訊

stdin

自行輸入

Filter

csv

separator、columns

grok

定義資料格式

mutate

資料型態轉換

geoip

地理位置

Output

elasticsearch

hosts、index

stdout

輸出結果



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$
```

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=rKy4sFblZ3U>

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

-
-
-