[EKL Image For Docker](https://elk-docker.readthedocs.io/)

*如果想自己製作，直接前往 p5.*

1. 下載 ELK image

(以下二擇一即可。此範例選用 snoppy103/elk)

$ sudo docker pull sebp/elk （官網:latest）

$ sudo docker pull snoppy103/elk （複刻板:v7.12.0）

2. 編輯 sysctl.conf，增加引數 (檔案最後新增一行)

$ sudo nano /etc/sysctl.conf

vm.max\_map\_count=262144

重啟生效

$ sudo sysctl -p

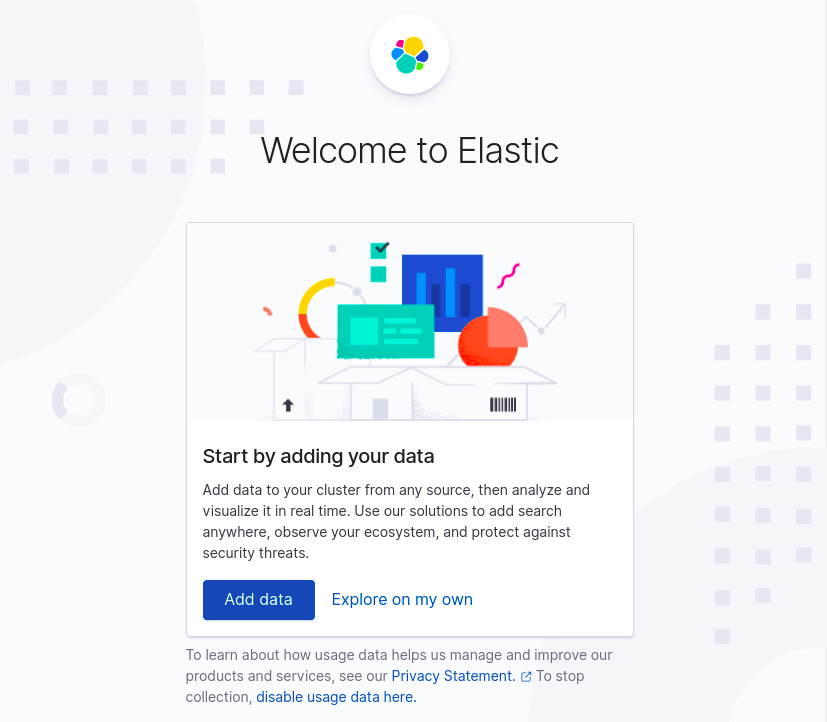
(若系統重啟或者 Docker Desktop 重啟，則需重新手動執行以上命令)

3. 使用以下命令從映像運行容器：[粗斜體部份自行更改]

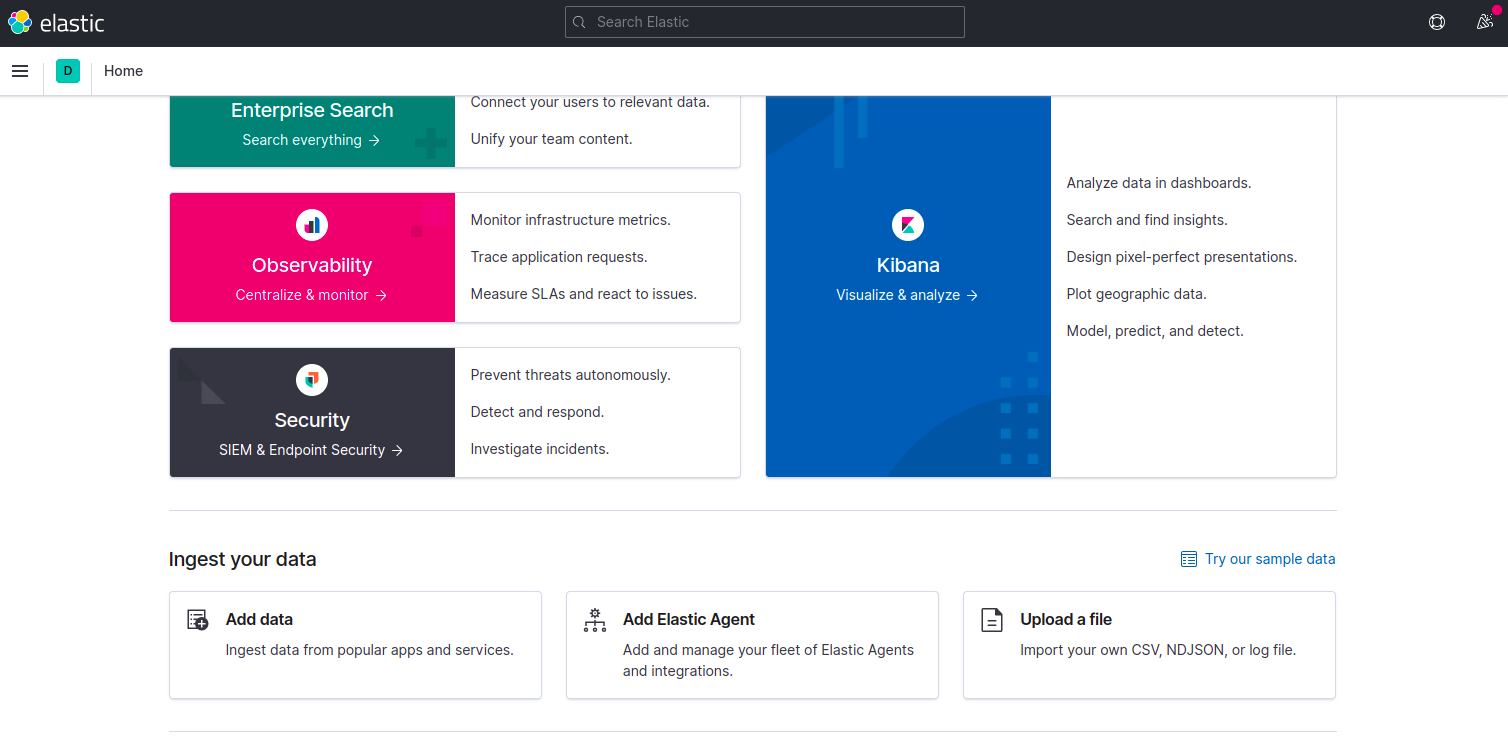
$ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name ***elk-t1*** ***snoppy103/elk***

4. 開啟瀏覽器：[粗斜體部份自行更改]

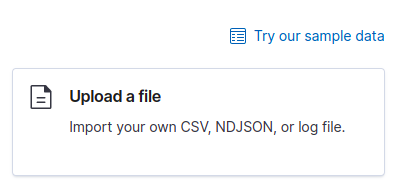
範例：***[192.106.105.230]***:5601



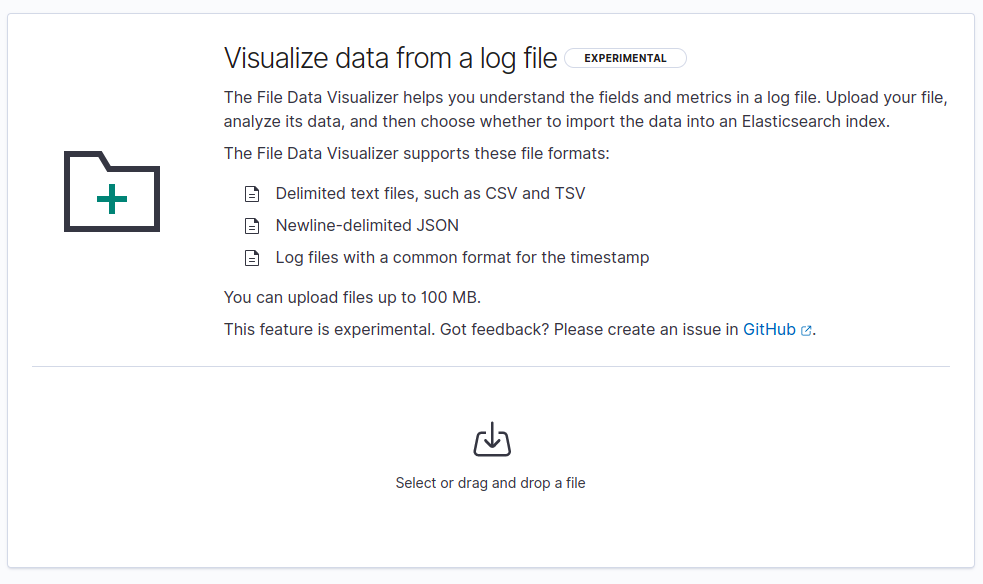
稍微往下，頁面呈現



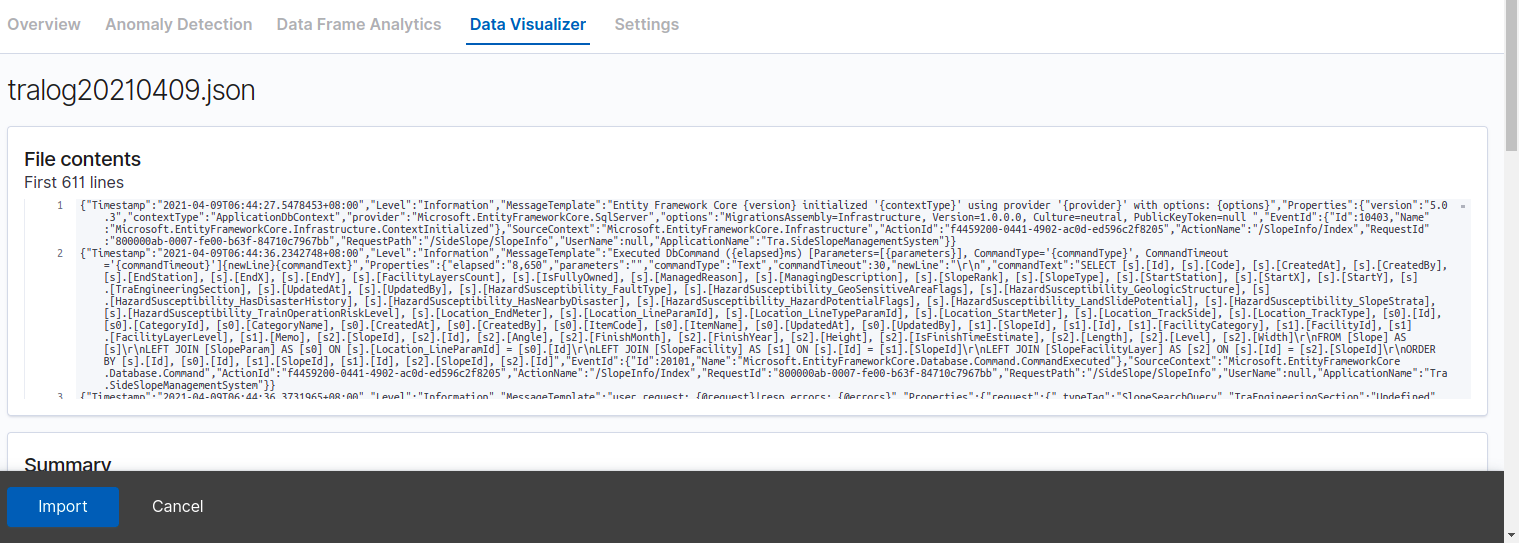
如果已經有 log 檔，選擇：



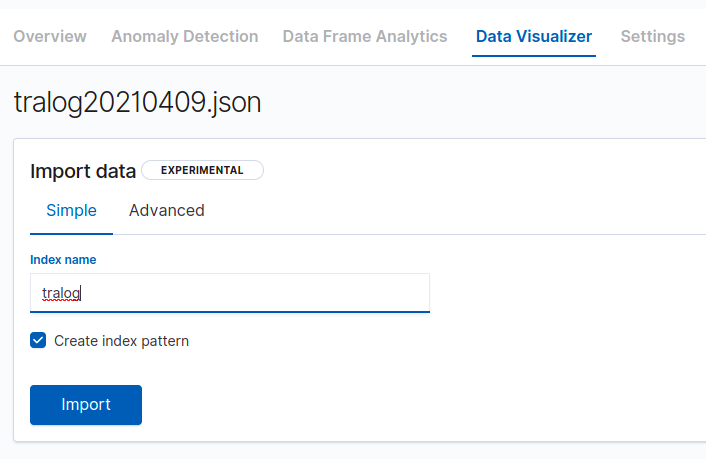
將 log 檔，拉進來。



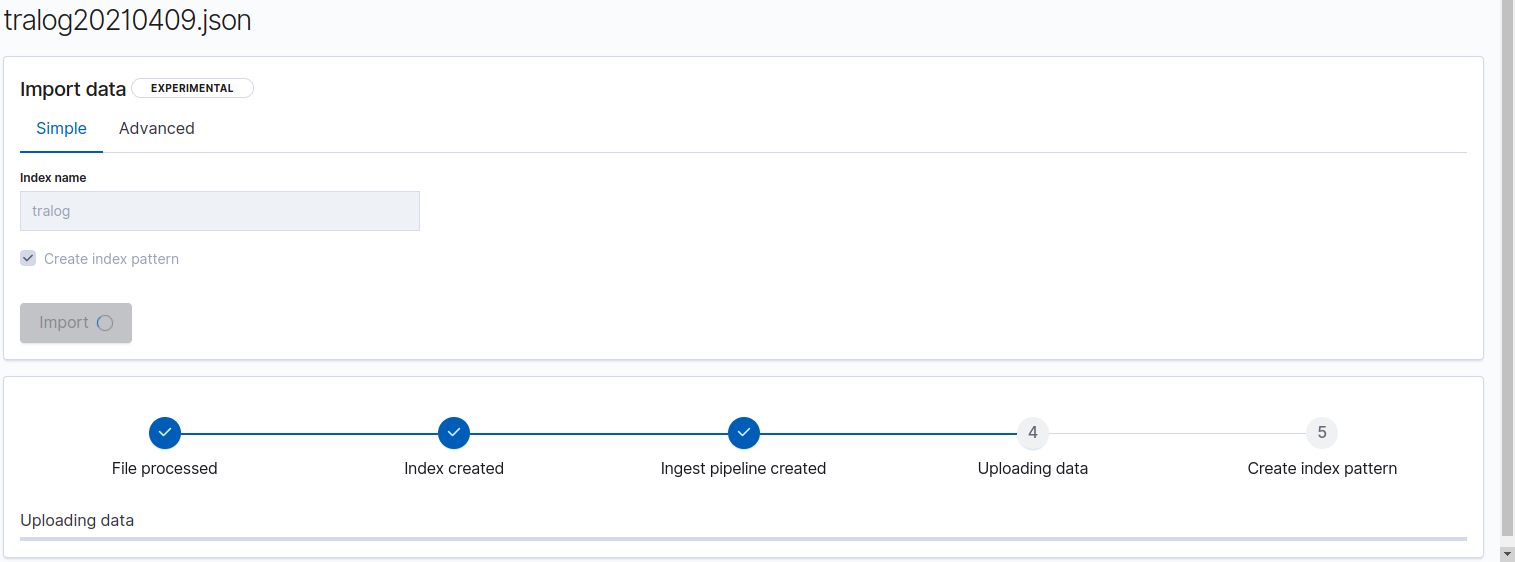
範例：



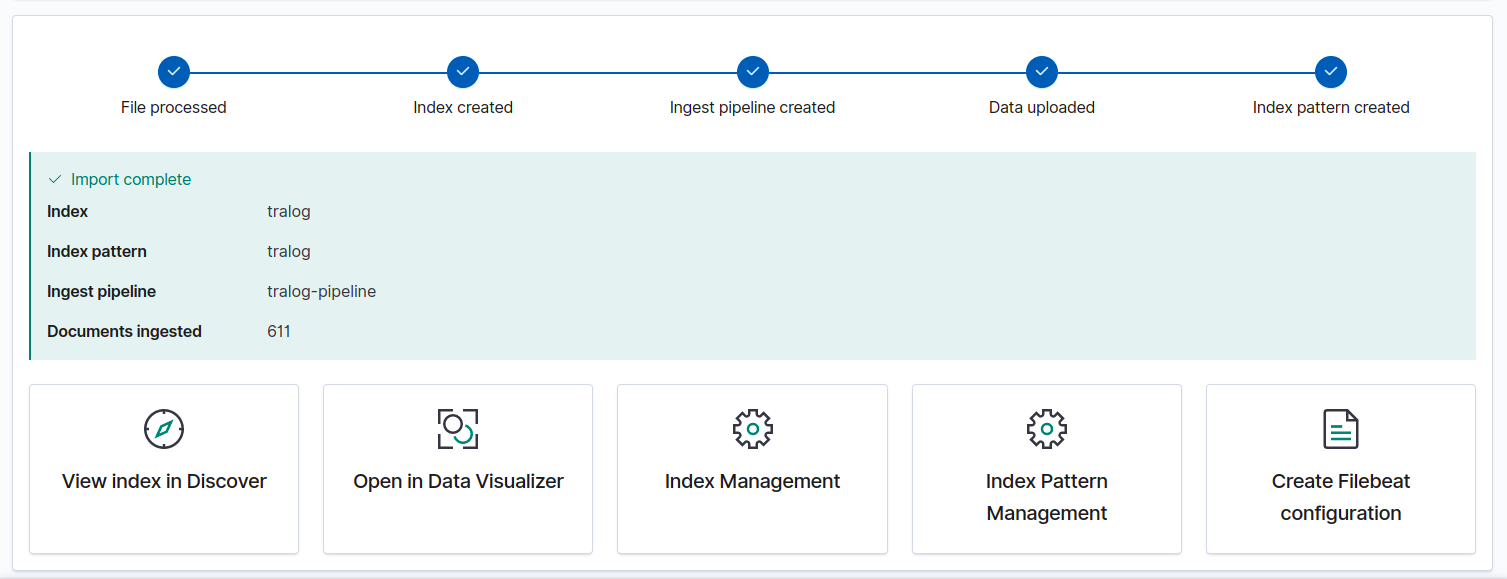
給 log 命名（標籤）



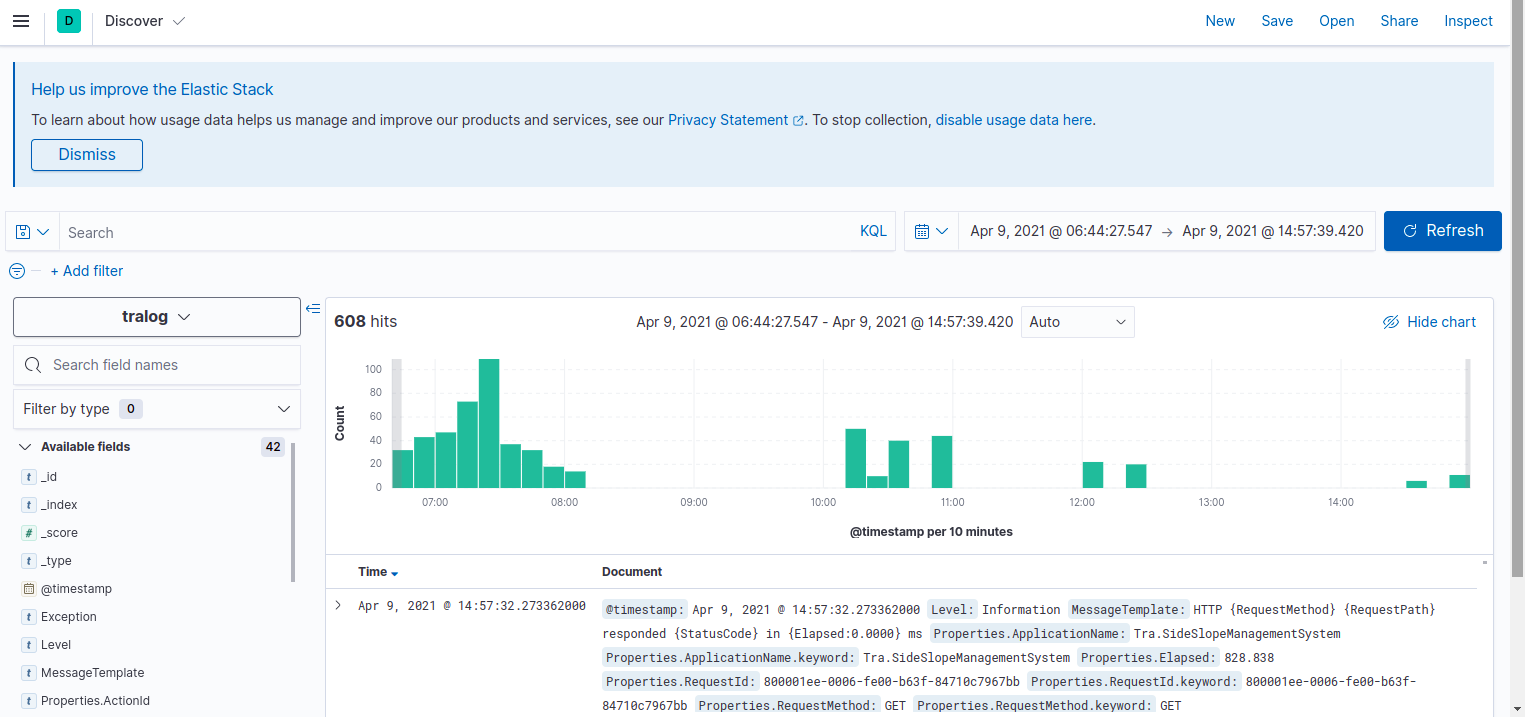
檔案讀取



完成，下方五個為如何檢視。



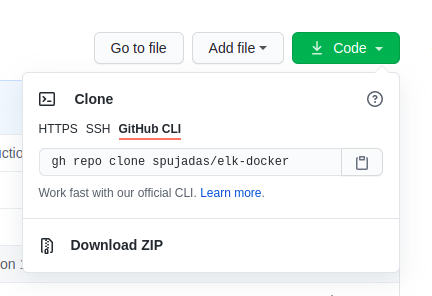
範例：view index in Discover



如何自己 build ELK Images

前往網址下載檔案：

<https://github.com/spujadas/elk-docker>



解壓縮並前往目錄：

Ununtu 20.04 & CentOS 7

$ unzip elk-docker-master; cd eelk-docker-master

***開始前請確認是否有安裝好 docker***

***開始前請確認是否有安裝好 docker***

啟動 docker

*CentOS7 (Ubuntu* 不須執行此行*):*

$ sudo systemctl start docker

建立 container [粗斜體部份自行更改]

*CentOS7 & Ubuntu 20.04:（C:約 29 min; U:約 2 min）*

$ sudo docker build -t ***elk-t1*** .

查看 Images

$ sudo docker images

之後，步驟請回到 p1 [2.] 繼續執行。

\*\* 若想將 Image 打包成 tar 檔：[粗斜體部份自行更改]

$ sudo docker save ***snoppy103/elk*** > ***snoppy103-elk***.tar

還原成 Image：[粗斜體部份自行更改]

$ sudo docker load < ***snoppy103-elk***.tar

\*\* 若想將 Image 上傳至自己的 Docker-Hub：

(如果想將 Image 上傳卻沒有 [Docker Hub](https://hub.docker.com/) 請[自行申請](https://ithelp.ithome.com.tw/articles/10191139))

將 Docker Image 加上標籤

$ sudo docker tag ***elk-t1 snoppy103/elk***

(sudo docker tag "Image Name" "docker hub username"/"Image Name")

登入 Docker-Hub

$ sudo docker login

將標籤好的 Docker Image 推上 Docker-Hub

$ sudo docker push ***snoppy103/elk***

(sudo docker push "docker hub username/"Image Name")

網頁登入 [Docker Hub](https://hub.docker.com/) 可查看推上去的 Image

(需要一些時間約 15 分鐘)

