ELK說明

|  |  |  |
| --- | --- | --- |
| Logstash是一個日誌數據處理系統 | Elasticsearch儲存log | Kibana進行數據可視化的呈現 |
|  | | |

名詞與觀念

* index: Elasticsearch的index相當於一個資料庫。
* type: 相當於資料庫的一個表。
* id: 唯一值，類似資料庫的主鍵 Primary Key。
* node: 節點是Elasticsearch實例(Instance)，可以看成叢集(Cluster)中的一個節點。一台機器可以執行多個實例，但是同一台機器上的實例在配置上要確保http和tcp Port不同。
* cluster: 代表一個叢集，叢集中有多個節點，其中有一個會被選爲主節點，這個主節點是可以通過選舉産生的，主從節點是對於集群內部來說的。
* document: 稱之爲文檔，它代表了一個能被索引的最小數據單元。在一個Index或者Type中，可以存儲很多個文檔。雖然文檔是儲存在Index中，但實際上，它必需被索引或分配到Index中的一個Type上。
* shards: 代表索引的分片，Elasticsearch可以把一個完整的索引分成多個分片，好處是可以把一個大的索引拆分成多個，分布到不同的節點上，構成分布式搜索，加快處理速度。分片的數量只能在索引創建前指定，如果索引創建後不能更改。
* replicas: 代表索引副本，Elasticsearch可以設置多個索引的副本，副本的作用一是提高系統的容錯性，當個某個節點某個分片損壞或丟失時可以從副本中恢復。二是提高Elasticsearch的查詢效率，Elasticsearch會自動對搜索請求進行負載均衡。

1. docker與docker-compose須事先安裝
2. centos主機增加 max\_map\_count (內核設置需要至少設置為262144)

echo 262144 > /proc/sys/vm/max\_map\_count

or

vim /etc/sysctl.conf

加入vm.max\_map\_count=262144

1. selinux設定

chcon -R system\_u:object\_r:admin\_home\_t:s0 docker-elk/

1. 下載 https://github.com/gitqoo/elk.git
2. mkdir ./elasticsearch/data #用於掛載elasticsearch的data

chmod g+rwx ./elasticsearch/data #**給予elasticsearch寫入權限，不然安裝會出錯**

參考<https://github.com/elastic/elasticsearch-docker/issues/21>

於docker-elk目錄下執行docker-compose up –d，會依據docker-compose.yml安裝ELK

相關說明位置

\docker-elk\docker-compose.yml #檔案內有說明

\docker-elk\logstash\pipeline\logstash.conf #檔案內有說明

\docker-elk\logstash\Dockerfile #logstash版本設定位置

\docker-elk\kibana\Dockerfile #kibana版本設定位置

docker-elk\elasticsearch\Dockerfile #elasticsearch版本設定位置

\docker-elk\logstash\config\ logstash.yml #elasticsearch密碼修改位置

\logstash\pipeline\logstash.conf #elasticsearch密碼修改位置

\kibana\config\kibana.yml #elasticsearch密碼修改位置

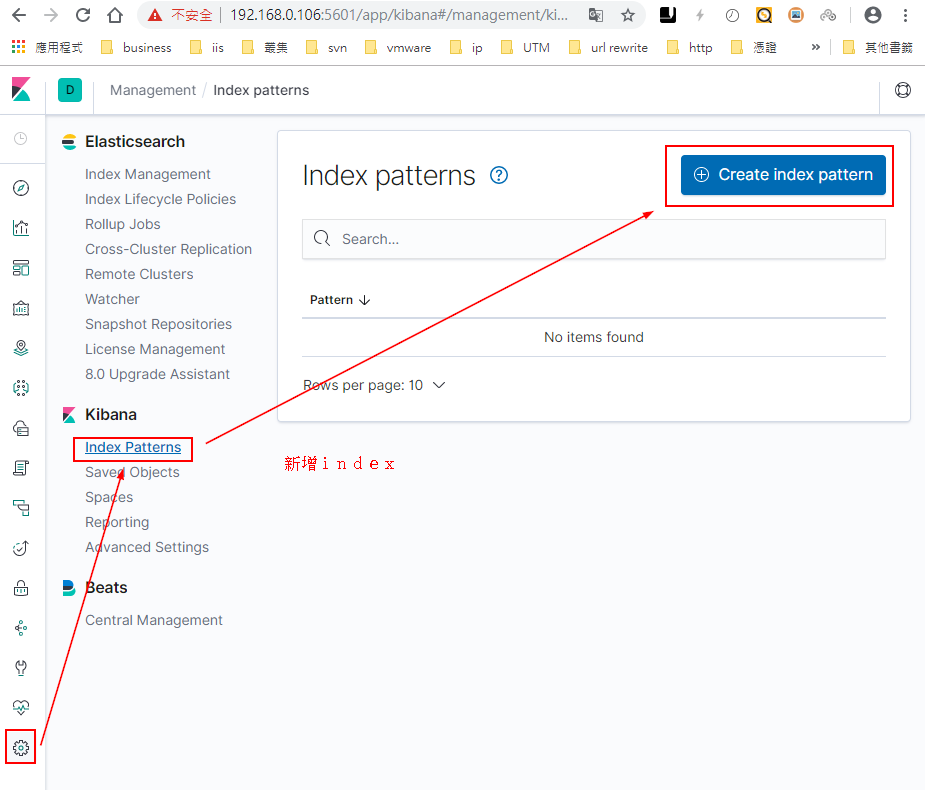
1. 測試

透過nc 192.168.0.106 5000 < test.log 測試把test.log內容丟給logstash

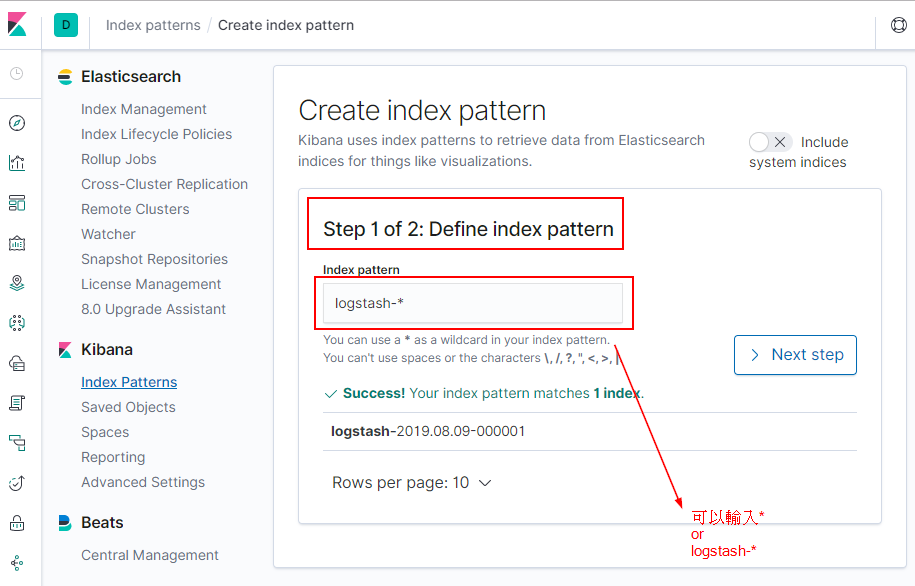
test.log內容隨便打別空白就好

1. ELK簡易index操作

新增index



step 1 輸入\* or logstash-\*



step 2 選擇@timestamp

step 3 按下discovery看log

