winlogbeat建立

* 下載網址：<https://www.elastic.co/downloads/past-releases>

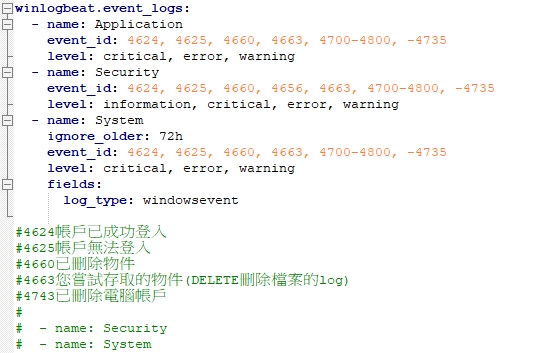
將下載的檔案解壓縮並放到自己喜歡的路徑，ex D:/ELK-Sz/winlogbeat

* 解壓縮後檔案如圖

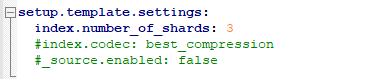


* 設定winlogbeat.yml

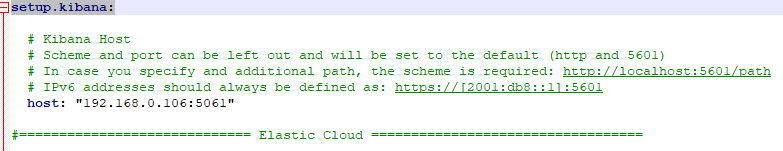
winlogbeat.event\_logs



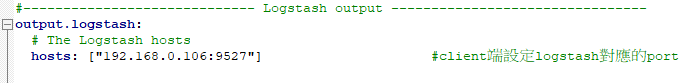
setup.template.settings



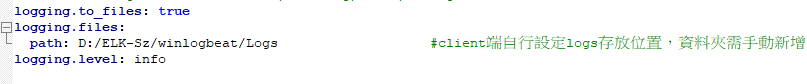
setup.kibana



output.logstash



logging.to\_files



* 測試

cd進入路徑D:/ELK-Sz/winlogbeat

測試指令：

winlogbeat test config



* 啟動

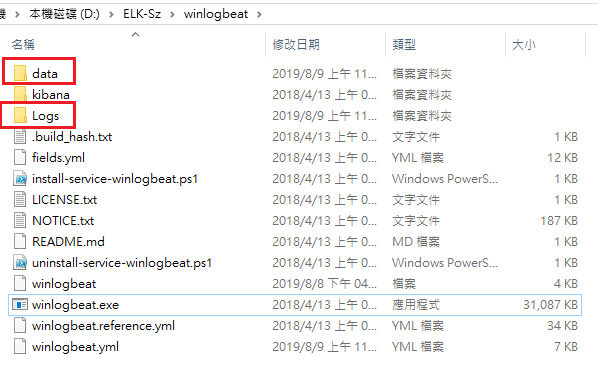
啟動指令：

winlogbeat



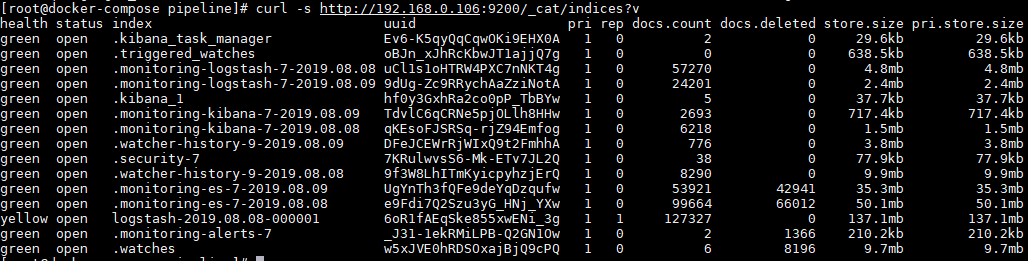
* 是否已開始傳送資料

會看到自動產生data與logs資料夾，代表開始傳送資料了

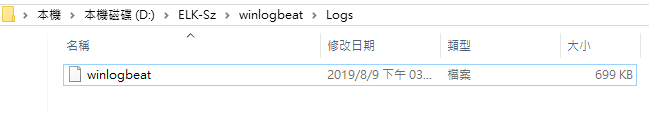


* 檢查log是否真的傳進來

curl -s <http://192.168.0.106:9200/_cat/indices?v>



or

剛自動產生的logs資料夾內也可以看到  


* 使用powershell把winlogbeat轉成服務

指令參數：

Executionpolicy：為殼層指定新的執行原則

Unrestricted ：任何腳本檔皆可被執行

轉服務指令：

powershell.exe -executionpolicy unrestricted -file.\install-service-winlogbeat.ps1

啟動服務

net start winlogbeat

刪除服務

sc delete winlogbeat

* winlogsbeat服務建立完成

