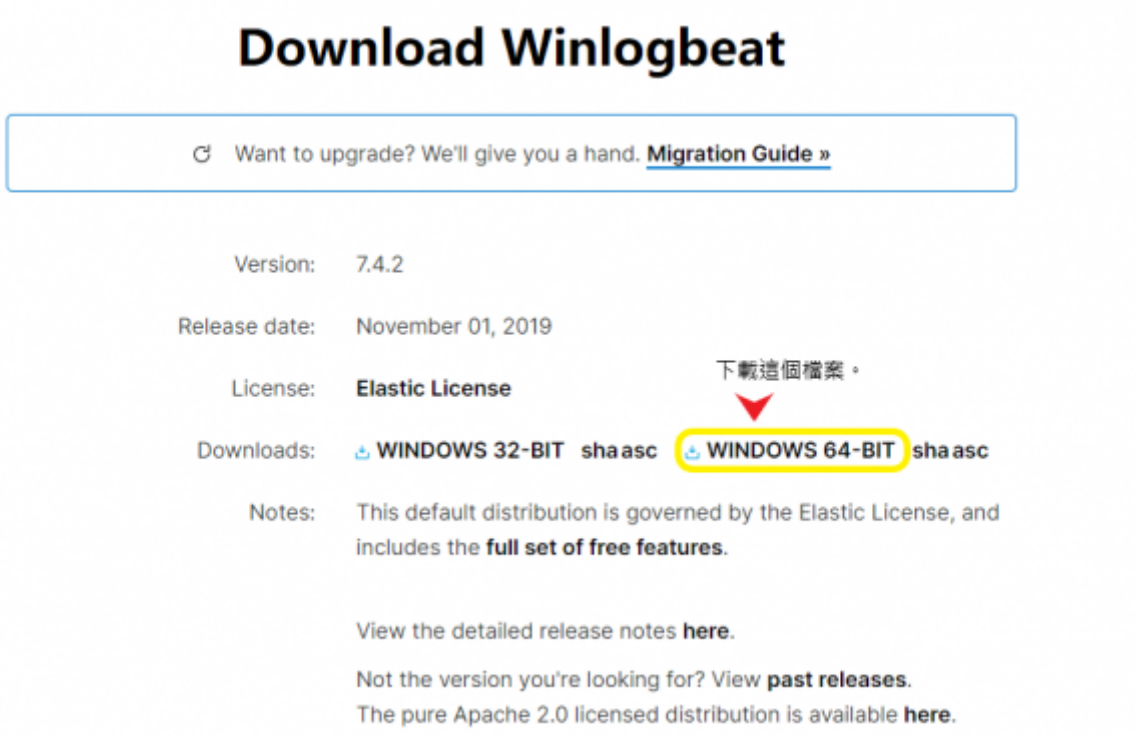
Winlogbeat 安裝與設定

安裝步驟

1. 至 winlogbeat官方網站下載後解壓縮。



2. 將解壓縮後的資料匣名稱去掉版本號改成 winlogbeat並搬移至 C:\Program Files\ 下。
3. 使用文字編輯器修改 C:\Program Files\winlogbeat\winlogbeat.yml 設定檔，需修改參數為“name:“與 ” hosts:“內容如下：

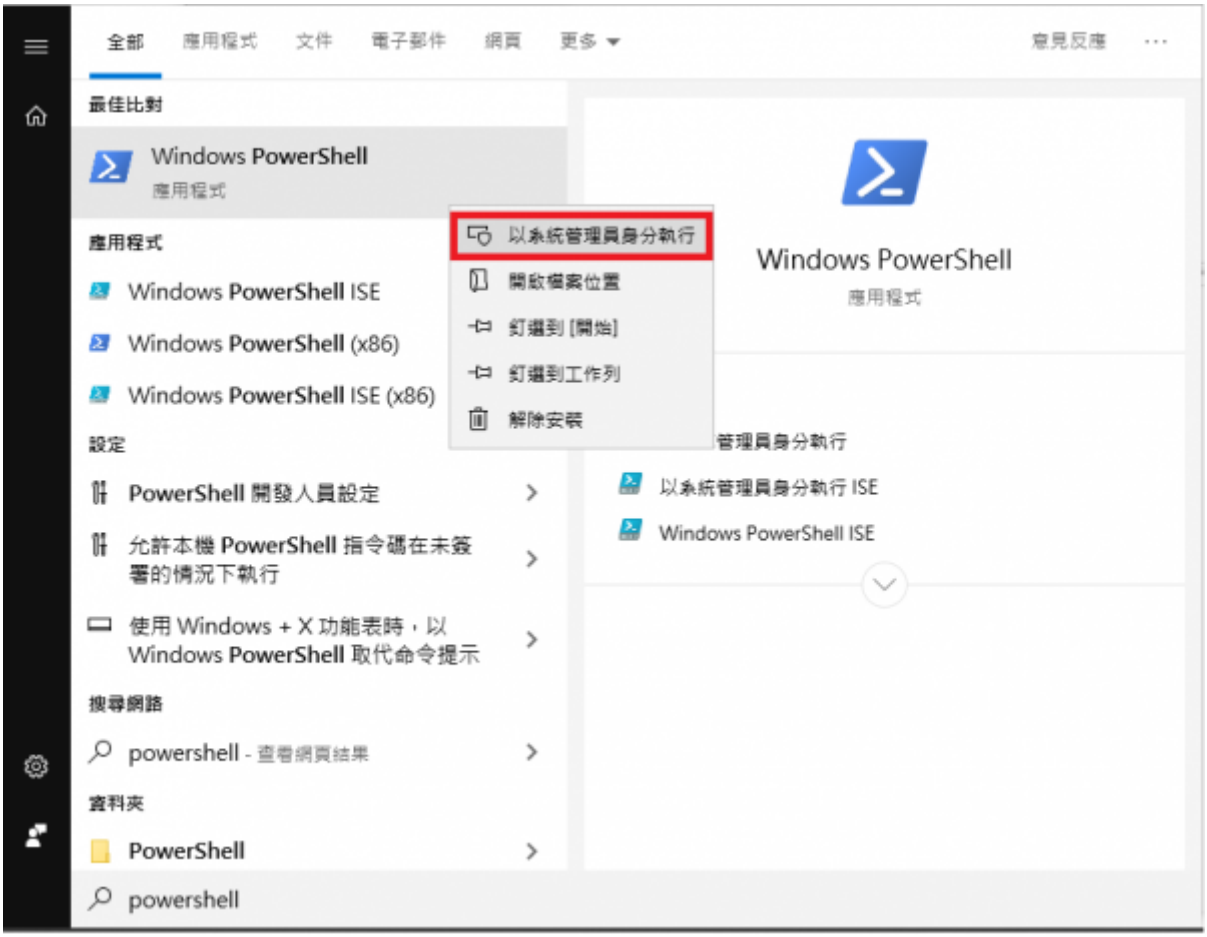
```
...
    #================================== General
=====================================
    name: cc_win10_64.127       #請依下列規則命名，勿輸入此範例名稱
            #命名規則：單位名稱_作業系統類型+版本_IP3.IP4
            #其中，作業系統名稱+版本可以是 windows10、win10、redhat8、ubuntu1404 等
容易辨識的資訊即可。
                                    #IP3.IP4 為 IP address 的第 3、4碼，如 IP 為
140.114.33.44 的 IP3.IP4 即為 33.44
            #注意：name: 後須空一格
            #請將原 #name: 前的"#"號刪除
...
    #------------------------- Elasticsearch output ----------------------
-------
    output.elasticsearch:
      hosts: ["elk.cc.nthu.edu.tw:9200"]  #注意：hosts: 後須空一格
```

```
...
```

作業系統類型+版本的範例如下：

作業系統	填寫範例 1	範例 2
Windows 10 企業版	window10	win10
Windows server 2016	windows2016	win2016
Red Hat Linux 9	redhat9	
Ubuntu 19.10	ubuntu1910	ubuntu19

4. 到 winlogbeat 的資料夾，測試設定檔是否正確(下列紅字部分為輸入的指令)
請先以系統管理員身分執行 Powershell 應用程式，如下圖所示：



在 Powershell 視窗內，輸入下列指令(紅字部分)

```
PS cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml -e
```

5. 執行安裝(服務)

```
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1
```

***注意** 如果因權限問題發生錯誤，才需要輸入以下指令：

```
powershell.exe -ExecutionPolicy UnRestricted -File .\install-service-
winlogbeat.ps1
```

出現安全警示訊息，如下圖：

請輸入 R ([R] Run once)執行一次。

6. 啟用服務

```
PS Start-Service winlogbeat
```

注意事項

1.如有需要請修改防火牆規則，增加一條 ” 允許 ” 對 140.114.64.0/255.255.255.0 PORT 9200(TCP)的連出流量規則