Apache Log 管理設定及解析

※紀錄檔的功用：可協助系統管理員快速發現問題發生的原因。

※紀錄檔的種類：

1. 錯誤記錄檔(ErrorLog)：
   紀錄 Apache 伺服器處理請求過程中發生錯誤的錯誤訊息。
   在 Linux 中通常命名為 error_log，存放在/var/log/httpd
   在 Windows 中通常命名為 error.log，存放位置視情況而定

2. 存取記錄檔(CustomLog)：
   紀錄 Apache 伺服器處理的所有的請求。
   在 Linux 中通常命名為 access_log，存放在/var/log/httpd
   在 Windows 中通常命名為 access.log，存放位置視情況而定

※紀錄檔的存放及格式之設定：httpd.conf 或 httpd-vhost.conf

※有關存取記錄檔(CustomLog)的設定：

1. LogFormat：用來事先設定 [記錄 Log 的格式]，並指定一個暱稱 (在設定 CustomLog 時使用)

   常見的設定有下列幾組：

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" combined
LogFormat "%V %h %l %u %t \"%r\" %>s %b" vcommon
LogFormat "%V %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" vcombined
```

   下面兩組 v 開頭的暱稱設定，主要差在開頭的 %V，因為在使用相對網址進行 request 時，%r 只能記錄到相對網址的部分，需要加上 %V 來輔助確認進入的是哪一個網站。

2. CustomLog：用來設定 access log 記錄的檔案與格式

   例如用 logs/access_log 當作記錄檔，並使用暱稱為 common 的格式

```
CustomLog "logs/access_log" common
```

   註：若要解讀出使用者的作業系統和瀏覽器，要用 combined

(以上參照：https://www.bear2little.net/wordpress/?p=339)

最佳實務

1. Apache 的記錄檔 ErrorLog 及 CustomLog 檔案過大，會影響到網站運行
2. CustomLog 檔案每天備存一次

```
[access log]
#  將原本設定註解
# CustomLog logs/access_log
#  新增設定(每天備存一次，86400 秒  =  一天)
CustomLog "|bin/rotatelogs.exe logs/httpd/access.%Y-%m-%d.log 86400" common
```

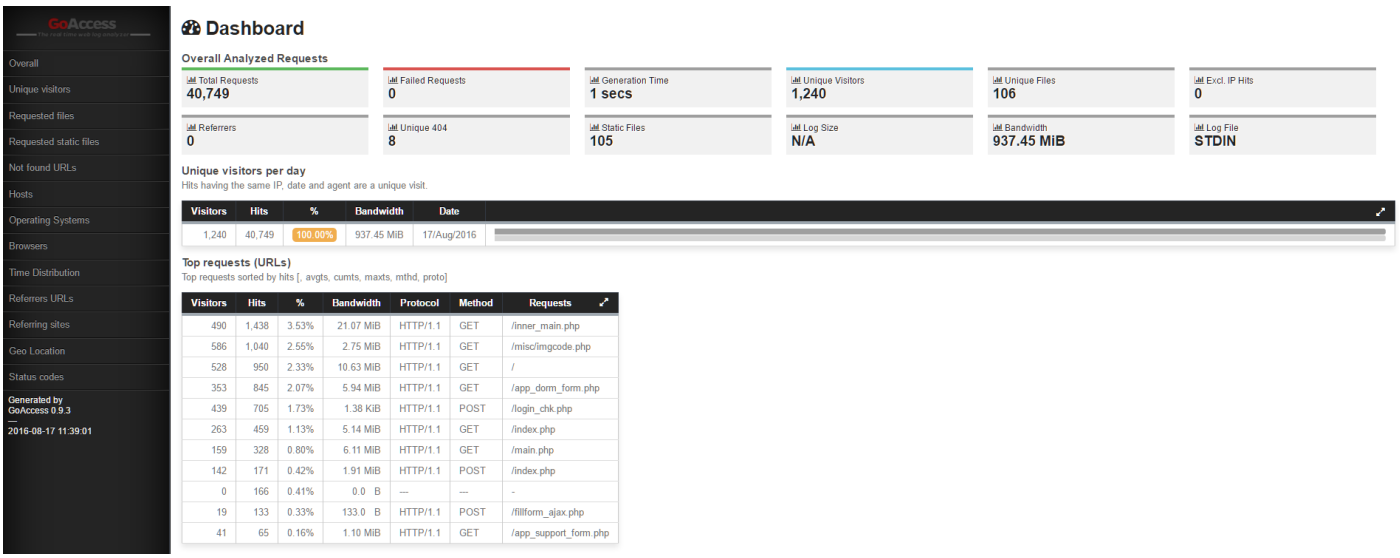
3. ErrorLog 檔案依容量備存

```
[error log]
#  將原本設定註解
# ErrorLog logs/error_log
#  新增設定(檔案超過 40M 備存一次)
ErrorLog "|bin/rotatelogs.exe logs/httpd/error.%Y-%m-%d.log 40M"
```

4. 若於 Linux 主機內有設定 logrotate，則可不用做上述設定(2.和 3.可忽略)。
   ➔ 透過/etc/cron.daily/logrotate 定期執行 logrotate 程式，以達成此目的
   主要設定檔：/etc/logrotate.conf
   各 log file 的單獨設定檔：/etc/logrotate.d/　　(會被 logrotate.conf 讀入)

(以上參照：http://blog.nux.tw/2013/03/apache-accesserror-log.html)

※存取紀錄檔(CustomLog)的解讀
可使用國人自行開發的 goaccess 套件進行彙整解讀。
http://www.openfoundry.org/tw/foss-programs/8228-goaccess-apache-log-



※HTTP 狀態碼，特別注意 4xx(找不到或無權處理)或 5xx(伺服器程式執行錯誤)開頭。