# 日誌

```

各式各樣的日誌:日誌格式

作業系統的日誌

Windows作業系統的日誌

Linux作業系統的日誌

伺服器的日誌

Apache伺服器的日誌

網路設備的日誌

iptable日誌

snort日誌

modsecurity日誌

日誌分析

DNS分析工具dnstop

LogParser

彩色日志工具ccze

動態日志查看工具logstalgia

三維日志顯示工具gource

LogAnalyzer

http://www.weithenn.org/2012/03/netadmin-74.html

日誌管理

SAWMILL稽核日誌報表系統

Kiwi\_Syslog\_Server

syslog

http://linux.vbird.org/linux\_basic/0570syslog.php

http://pxnet2768.pixnet.net/blog/post/71799543

https://stackify.com/syslog-101/

```

# 各式各樣的日誌:日誌格式

### 作業系統的日誌

##### Windows作業系統的日誌

```

Windows日誌分三種

1. 系統日誌

2. 安全日誌

3. 應用程式日誌

Windows採binary(二進制)對日誌文件存儲

通常也只用Windows事件查看器(event viewer)或第三方日誌分析工具讀取

```

```

1.Windows 2000 Advanced Server

應用程式：C:\WINNT\system32\config\Appevent.Evt

安全：C:\WINDOWS\System32\config\SecEVENT.Evt

系統：C:\WINDOWS\System32\config\SysEvent.Evt

2.Windows Server 2003企業版

應用程式：C:\WINDOWS\system32\config\Appevent.Evt

安全：C:\WINDOWS\System32\config\SecEVENT.Evt

系統：C:\WINDOWS\System32\config\SysEvent.Evt

3.Windows Server 2008 標準版

應用程式：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全：%SystemRoot%\System32\Winevt\Logs\Security.evtx

系統： %SystemRoot%\System32\Winevt\Logs\System.evtx

4.windows Vista\Windows 7\windows 8\windows 10 日誌情況

應用程式：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全：%SystemRoot%\System32\Winevt\Logs\Security.evtx

系統： %SystemRoot%\System32\Winevt\Logs\System.evtx

```

##### Linux作業系統的日誌

```

UNIX/LINUX分三個子系統:

(1) 登陸時間日誌子系統 存放在var/log/wtm和var/run/utmp

(2) 行程統計日誌子系統

(3) 錯誤日誌子系統 存放在/var/log/messages/

由Sysloge操作(新版用rsyslogd)

```

```

UNIX/Linux日誌文件格式:

1. 基於syslogd的日誌文件

Syslogd依優先程度分8級 0~7

通常是ASCII碼的文件格式

2. 應用程式產生的日誌

通常是ASCII碼的文件格式

程式會將日誌傳往syslogd並統一處理

```

```

大部分應用層的日誌會儲存在/var/log/messages/

Apache的日誌 會儲存於/var/log/httpd/access\_log

Samba 則儲存在/var/log/samba

```

```

操作紀錄日誌文件分兩類

1.對登陸人員進行記錄的lastlog

2.系統郵件伺服器運行時紀錄的maillog

```

### 伺服器的日誌

##### Apache伺服器的日誌

```

Apache 日誌分兩類:

1.access.log

2.error.log

access.log 用於

1.進行網站流量統計

2.查看用戶訪問時間

3.紀錄ip得知用戶來自哪裡

4.紀錄用戶訪問的web資源而知道頁面點擊率

```

```

Apache默認日誌位置在 Apache配置文件/etc/apache2/apache2.conf中定義為

Customlog/var/log/apache2/access\_log.combined

```

### 網路設備的日誌

##### Pix防火牆日誌

```

由Cisco進行研發 主要紀錄:

1. AAA(認證、授權、記帳)

2. Connection(連接)

3. SNMP事件

4. Routing errors(路由錯誤)事件

5. Failover(故障轉移)事件

6. PIX系統管理事件

```

##### WEB 日誌分析

```

Apache 分兩類:

1.access.log

2.error.log

access.log 用於

1.進行網站流量統計

2.查看用戶訪問時間

3.紀錄ip得知用戶來自哪裡

4.紀錄用戶訪問的web資源而知道頁面點擊率

```

```

HTTP 返回狀態代碼(STATUS CODE):

以2開頭表示成功

以3開頭表示定向到了其他位置

以4開頭表示客戶端出了錯誤 (常見如404 未找到)

以5開頭表示伺服器出了錯誤 (常見如503 不可用)

```

##### iptable日誌

```

Iptables日誌大致有五方面:

1.消息發送源ip位址

2.消息目的ip

3.消息流向

4.消息內容

5.應用

任何連接、請求 例如:TCP、UDP、ICMP、流量信息、建立時間等

Iptables日誌都會逐一體現在文件裡面

```

##### snort日誌

```

snort是一個基於libpcap的輕量級網絡入侵檢測系統。

用於檢測可能的入侵企圖；或者使用SPADE插件，使用統計方法對網絡數據進行異常檢測。

    這些模塊包括：HTTP解碼插件，TCP數據流重組插件，端口掃描檢測插件，FLEXRESP插件。以及各種日誌輸入插件等。

```

##### modsecurity日誌

```

ModSecurity是一個Apache模塊，可以充當Web應用防火牆(WAF)。

ModSecurity.主要是用於Web應用程序所以也可以叫做Web應用程序防火牆.

ModSecurity的目的是爲增強Web保護Web應用程序避免遭受攻擊.

```

# 日誌分析

### DNS分析工具dnstop

##### DNS 日誌分析

```

Dns日誌默認送到/var/log/messages文件中。

Dns級別從嚴重到輕分七個級別:

1.critcal

2.error

3.warning

4.notice

5.info

6.debug

7.dynamic

當定義某個級別 系統會記錄含該級別以及比他嚴重的級別的所有信息

假如定義info

則會記錄

Critcal、error、warning、notice、info

這五個級別的信息

一般紀錄到info

```

### LogParser

#### LogParser 結構

```

LogParser 主要有三部分:

1.輸入處理器

2.數據引擎

3.輸出處理器

輸入處理器支持日誌格式外還可以讀取逗號分隔(.CSV)的文件

輸入處理器把每個日誌型態轉換為統一格式

然後數據引擎處理輸入數據產生結果後

輸出處理器接手並且格式化該結果輸出到一個表裡面。

輸出處理器支援多種文件格式

```

### 彩色日志工具ccze

```

Ccze是一款能將linux系統日志加上顏色的工具

讓使用者能迅速查看故障訊息

```

### 動態日志查看工具logstalgia

```

Logstalgia是一款Web站點訪問日誌實時分析的開源工具

可視化過程分為

1.日誌RAW的預處理

2.數據得可視化結構展示

3.視圖繪製

```

### 三維日志顯示工具gource

```

Gource的設計目的是將代碼版本控制系統裡面的日志全部可視化

這款工具可以賦予日志信息顏色、動態顯示

且多了3d層次感

```

### LogAnalyzer

```

http://www.weithenn.org/2012/03/netadmin-74.html

LogAnalyzer工用於搜索、查看和分析網絡活動數據，包括系統日誌、事件日其他日誌。

由於它只將數據展示到我們面前，數據本身需要由另一個程序收集，

比如syslogd，rsyslog（現在是發行版的默認的syslogd），WinSyslog或MonitorWare代理。

LogAnalyzer同樣適用於Linux和Windows。

主要是用PHP編寫的自由軟件，基於GPL的開源應用程序。數據可以從數據庫，也可以從純文本文件而獲得。

```

# 日誌管理

### SAWMILL

```

http://www.etruserve.com.tw/sawmill\_info.htm

Sawmill 8能支援800種以上的設備或應用程式日誌 。

可透過多種網路傳輸方式讀取log檔案進行切割，存入後端資料庫中進行分析、並產生報表。同時可設定條件偵測事件發出郵件警告。

採用SQL相容資料庫，可快速統計、篩選、關聯日誌事件。

內建syslog伺服器，可自動分類存檔，並壓縮10:1大小。

Raw Log完全唯讀，並具有連續SHA-1檢核報表，證明日誌完整性。

具備聚焦功能，可快速靈活產生ISO27001、SOX、HIPAA等客制報表。

具備條件式過濾功能，可以任何關鍵字、時間作為條件顯示報表。

能自訂條件產生各種報表存檔，或以E-Mial排程定時寄出。

支援SNMP網管協定、自我健康檢測與維護、Raw Log自動化SHA-1校驗碼報表及核對機制、

一鍵更新修正日誌格式支援、設定備份至外部磁碟等功能。

運行於64bit，多核心處理器之作業平台，能快速處理大量資料。

```

##### 用Sawmill 搭建日誌平台

```

Sawmil的分析統計可以做到:

1.操作系統

2.ftp服務:用戶登入登出、訪問次數、文件的上傳下載信息及帶寬的佔用

3.web服務:網頁點閱率、頁面停留時間、來源區域分布、點擊路徑分析

4.mail服務:郵件收發人、收發地址、收發狀態、響應路徑、郵件統計

5.firewall服務:可查詢ip、區域分類、分析來源位置、帶寬使用量

6.datebase:數據庫的連接存取、建立、審計異常進入突出狀態

```