# 日誌分析基礎

## 網路環境日誌分類

### UNIX/LINUX 系統日誌

##### 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

```

### Windows 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

```

## Web日誌分析

#### 網路設備日誌

```

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

```

```

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

```

#### 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)

```

## 用LogParser分析Windows系統日誌

#### LogParser 概述

```

LogParser 可以實現對不同日誌的分析 是微軟自己的日誌分析工具

```

#### 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

```

## Iptables 日誌分析

```

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

```

## 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

```

## 建立日誌分析系統

### Syslog協議

```

Syslog是一種標準協議(RFC3164)是負責記錄event的後台程式

紀錄內容包括 核心、系統程式及使用者自行開發程式的運行情況

使用UDP協定 通過514port連線

Syslogd啟動時讀取配置文件/etc/syslog.conf

1. 常見日誌收集方式分三種:

>文本方式

>SNAP Trap 方式

>Syslog 方式

2.日誌的標準化

不同設備的日誌格式不同

需要將不同格式的日誌轉化為統一格式

3.主流日誌格式介紹

目前主流設備產生的日誌格式有三種

>Syslog

>Traffic log

>國際通用的WELF

(WebTrends Enhanced Log Format)

```

### Syslog 日誌紀錄的事件

```

Syslog紀錄的系統事件有:

1.系統內核產生的0~7級，包括相關的硬件問題

2.網路部份產生的0~7級。

3.安全模塊部分，如Iptaable

4.高可用性部分產生的0~7級

5.設備驅動程式的0~7級

6.各類系統daemon產生的0~7級，如SNMP模塊

7.系統服務模塊，如WWW、DNS、MAIL、Squid、各種防病毒軟體

8.第三方和應用程式，如Tripwire、TCP Wrapper、Snort、CheckPoint等

9.系統管理過程中產生的Syslog

10.用戶寫在/etc/services中的服務程序

11.用戶開發程序使用Syslog API產生的日誌

```

### Syslog的安全漏洞

```

Syslog是以明文形式存儲數據，入侵者可以從/var/log/下或從/var/adm/下(Solaris9/10)獲取數據。

但需要root權限，而這些可能因為人為或程序錯誤而發生。

```

### Rsyslog

```

Rsyslog是因應syslog協議的不足而誕生的

支援TSL(SSL)加密技術保證安全

近幾年的LINUX都換成了Rsyslog

```

### Syslog-ng

```

Syslog-ng是Syslog更高級的替代工具

```

### 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

```

### 用Splunk

```

Splunk 能處理常規的日誌格式

對所有日誌進行索引 然後可以交叉查詢

```