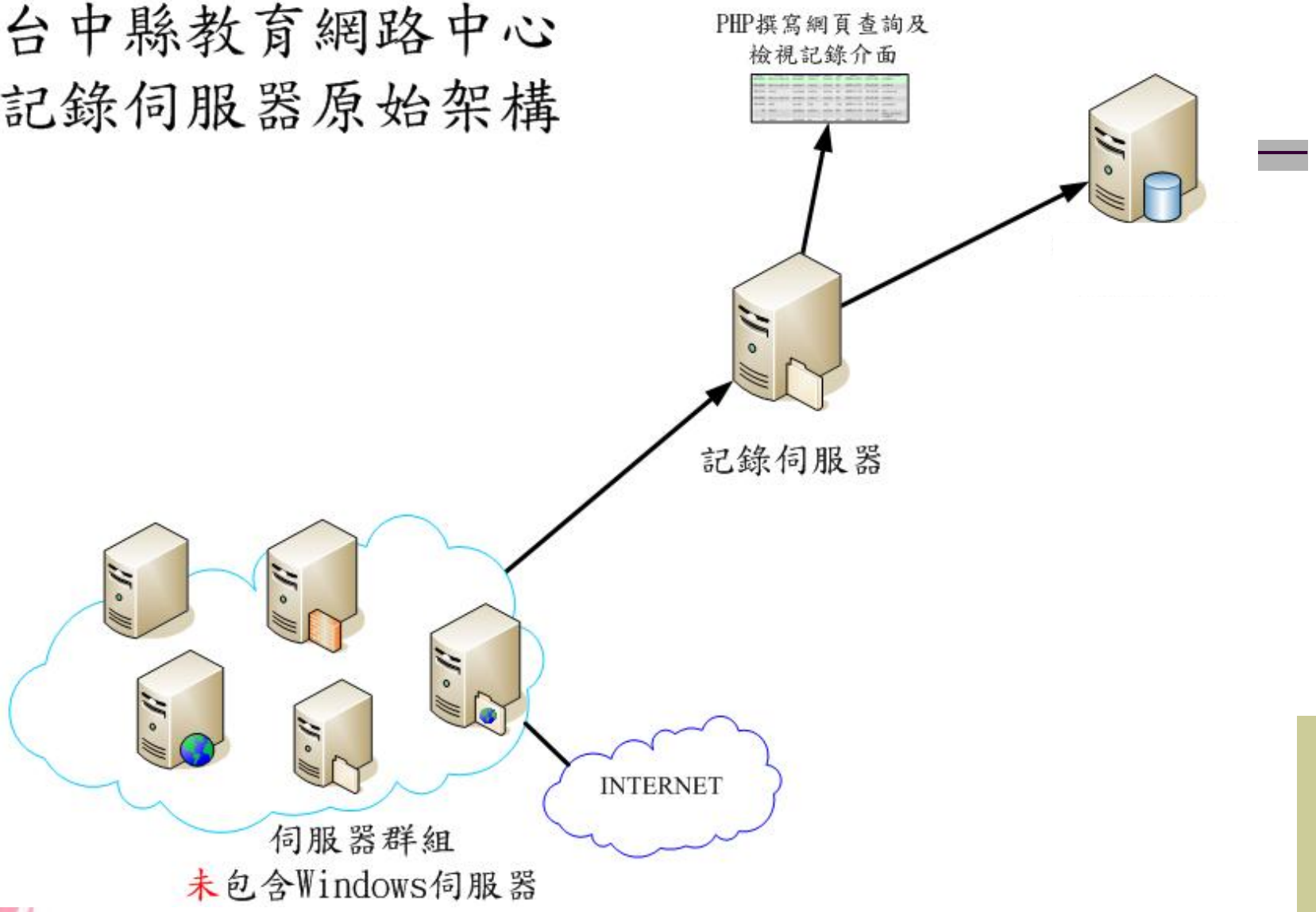
設計實作記錄伺服器--以台中縣網為例

報告人
張本和 台中縣教育網路中心
axer@ms1.boe.tcc.edu.tw
日期：99.12.1

Syslog簡介

- “syslog” 名稱最早出現在 unix 系統，最初目的只是單純是為了記錄sendmail的訊息。
- linux, bsd, solaris等 unix-like 的系統也沿用此一名稱。
- log在Windows系統下有另一個名稱，叫作eventlog，他的格式和syslog 完全不同也不相容。
- 系統的訊息如存取、錯誤、排程或是程式的訊息都會寫到syslog 以供管理人未來查詢除錯使用。
- syslog 使用很久但卻沒有任何標準去規定他的記錄格式，造成許多的syslog判讀及分析困難：
  2001年 RFC3164 - The BSD Syslog Protocol
  2009年 RFC 5424 - The Syslog Protocol

台中縣教育網路中心
記錄伺服器原始架構



Syslog 的各種格式範例

CISCO WS-C6509-E Router (Version 12.2(33)SXH4)

<188>746609: Nov 18 07:33:37: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet3/16 (2), with Switch GigabitEthernet0/33 (3).

CISCO FWSM Firewall Version 3.2(7) PIX

<186>Nov 18 2009 14:01:23: %FWSM-2-106016: Deny IP spoof from (::) to ff02::1:ff9b:54b3 on interface outside

Freebsd 6.2 syslogd

<38>Nov 18 17:23:01 sshd[13247]: Accepted keyboard-interactive/pam for axer from 163.17.40.11 port 62757 ssh2

Linux syslogd

<86>sshd[31860]: pam_unix(sshd:session): session opened for user axer by (uid=0)

DLINK 3000 Switch

<138>Nov 11 01:26:24 192.168.44.2 CRIT: Unit 1, Back Fan failed

Syslog-ng 1.6

<28>Nov 20 22:02:29 dns named[41283]: client 163.17.90.16#57503: RFC 1918 response from Internet for 38.1.168.192.in-addr.arpa

Syslog-ng 2.0

<78>Nov 10 13:10:01 dns2 crond[1336]: (root) CMD (env LANG=C /usr/bin/mrtg /home/mrtg/mrtg.schools.cfg.utf8 /home/mrtg/schools/)

原本收集記錄檔的作法

- 採用 syslog-ng 收攏資料庫，但有以下缺點：
  - 只能將資料收錄到資料庫，並無報警的功能。
  - 有無法辨視格式的問題。
  - freebsd + syslog-ng+ mysql 的組合會在收錄一段時間後「自動停止」；linux+ syslog-ng + mysql的組合亦同。

syslog-ng + mysql 是使用一個 "pipe" 當作中間人，讓資料庫和 syslog-ng 進行溝通，例如在 syslog-ng.conf的設定：

```
destination d_mysql {
pipe("/tmp/mysql.pipe"
template("INSERT INTO logs (host, facility, priority, level, tag, date, time, program, msg)
VALUES ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL', '$TAG', '$YEAR-$MONTH-
$DAY', '$HOUR:$MIN:$SEC', '$PROGRAM', '$MSG' );\n") template-escape(yes));}
```

並在 shell 下執行一個 pipe 導入的方法：

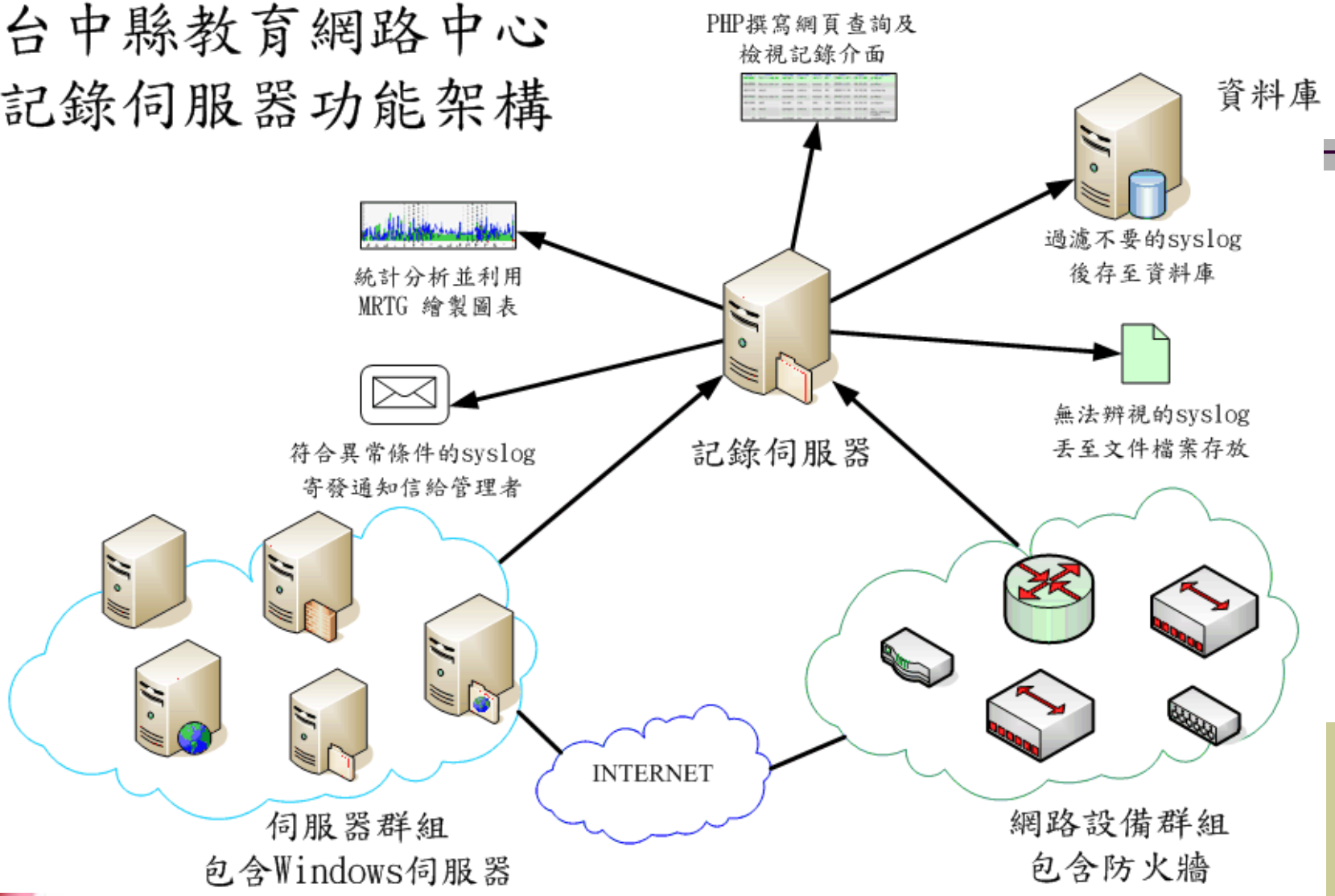
```
$ mysql -uaxer -p1234 --database=logdb < /tmp/mysql.pipe &
```

改善收集記錄檔的作法

- 採用 perl 作為開發工具，自行撰寫記錄檔收集伺服器—具有多執行緒、多監聽埠的程式。
- 能處理Windows 的eventlog。修改 winlogd 讓eventlog可以轉為 syslog，同時也可看到正常的中文字

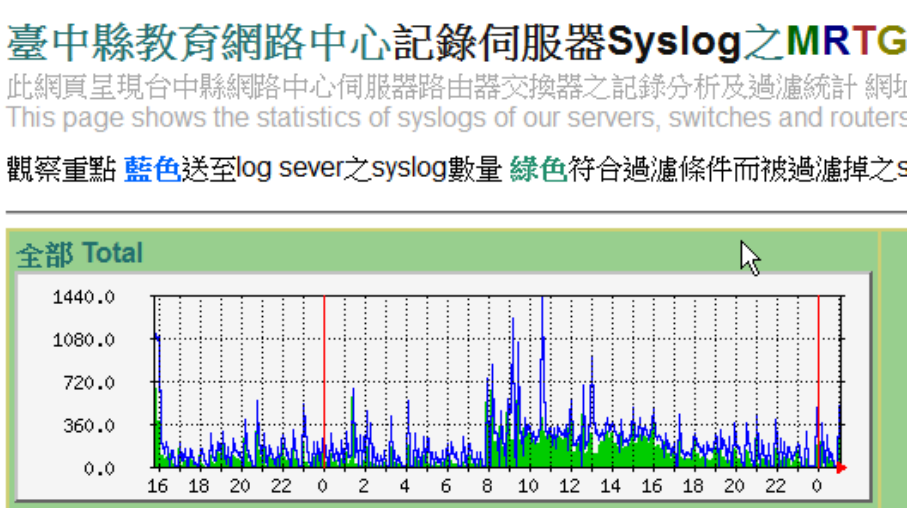
  <155>Dec 14 16:00:35 spade TermServDevices[1111]: 無法辨識印表機 HP Color LaserJet 5500 PCL6 所需的驅動程式 HP Color LaserJet 5500 PCL6。在您重新登入前，請連絡系統管理員來安裝驅動程式。
- 能將syslog 的資料送給 mrtg 測繪。
- 能過濾掉不重要的syslog，並能將過濾後的syslog 存入資料庫。
- 能自動發出通知信，並能設定篩選規則。

台中縣教育網路中心
記錄伺服器功能架構

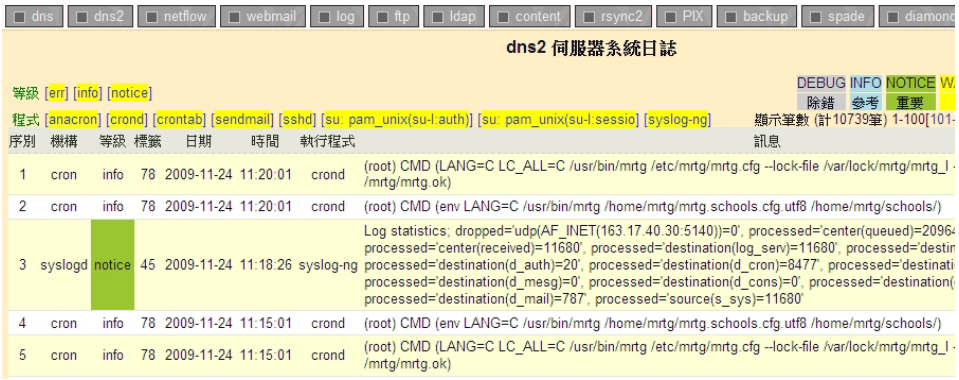


程式實作經驗分享(一)

- 繪製總量繪製圖表
  http://log.tcc.edu.tw



- 網頁的查詢界面



程式實作經驗分享(二)

- 2010/9/1至2010/10/25的記錄筆數如右表。

- 解析syslog的正規表達式例

```
/^<(\d+)>(\d+:\s)?
([A-Za-z]+\s+\d+(\s\d+)?\s)?
(\d+:\d+:\d+:?\s)?
([A-Za-z\.]+\s|[\d\.:]+\s)?
([^\[\s]+)(\[\d+\])?:\s?(.*)/
```

-

伺服器	筆數
dns	4184
dns2	24332
dns3	18746
ftp.tcc.edu.tw	437769
last	303
ldap	19002
ms1.boe.tcc.edu.tw	6977
netflow.tcc.edu.tw	48412
rsync.tcc.edu.tw	13663
rsync2	168
spade	29791
syslogd	52
webmail	3261
www	13454

結論

- 經過實際測繪發現，單位中的 syslog在每五分鐘的統計中曾高達 1608 筆記錄；每五分鐘週平均量約230筆記錄。
- 其中過濾掉的低重要性 syslog 平均約170 筆，占約75%，剩餘的寫入資料庫，一週的量約為17萬筆。被濾掉的部分約為存入資料庫筆數的4倍。
- 程式安裝稍微麻煩，客製化支援台中縣網網路設備，若要支援其他網路設備則必須些微調整。