開源碼網管系統暨漏洞分析

報告人:吳惠麟

講師簡介

- 吳惠麟
- Experience
  - TACERT工程師
  - 桓基科技研發工程師
  - 諮安科技研發副理
- 著作
  - 開源碼架構之網路安全防禦解密(ISBN：9789863470601)
  - 資訊安全原理與實驗(ISBN:9789861815534)
  - 期刊技術實戰作者
- Certified：
  - LPIC Level 1
  - ISO 27001:2005 LA (ISMS)
  - BS 10012:2009 LA (PIMS)
- Contact
  - xfile.lin@msa.hinet.net

大綱

- 網站系統漏洞
  - Apache killer (cve-2011-3192)
  - Slowloris(cve-2007-6750)
  - Shell shock (CVE-2014-6271)
- 社交工程
  - Falsh CVE-2015-5119
  - Unicode attack
- 開源碼網管系統

D.o.S (Apache Killer)

加強 Apache 伺服器保安 刻不容緩

發布日期: 30 / 09 / 2011

最後更新: 03 / 10 / 2011

根據 NetCraft 統計資料，截止 2011 年9月，現時約 65 % 網站是使用 Apache，所以，任何針對 Apache的致命攻擊，對互聯網網站都是事關重大的。

在 2011 年8月24日在互聯網上有一位 IT保安研究人員發佈了一個針對 Apache伺服器 Range/Request-Range 標頭漏洞 (CVE-2011-3192) 的攻擊試驗程式 (Apache Killer)，發現可導致阻斷服務攻擊。

現時網站要傳送體積較大的檔案可以利用內容分割功能 (Partial Content)，分拆多個不同的 Bytes 段落方式進行傳送。Apache伺服器收到請求後，會對個別 Bytes 段落產生獨立程序進行處理以增加效率。所以，如果以Range/Request-Range 標頭將檔案分析為大量細小或重疊的Bytes 段落會令Apache伺服器需要產生大量程序應付請求，導致系統不勝負荷。

測試證實只需一台普通電腦執行該程式便可以令一台 Apache伺服器在幾分鐘內資源耗盡而癱瘓。這個漏洞只影響 2.2 及 2.0 版本，1.3 版本則不受影響。HKCERT 已經在8月29日發佈保安公告，提醒用戶儘快處理。

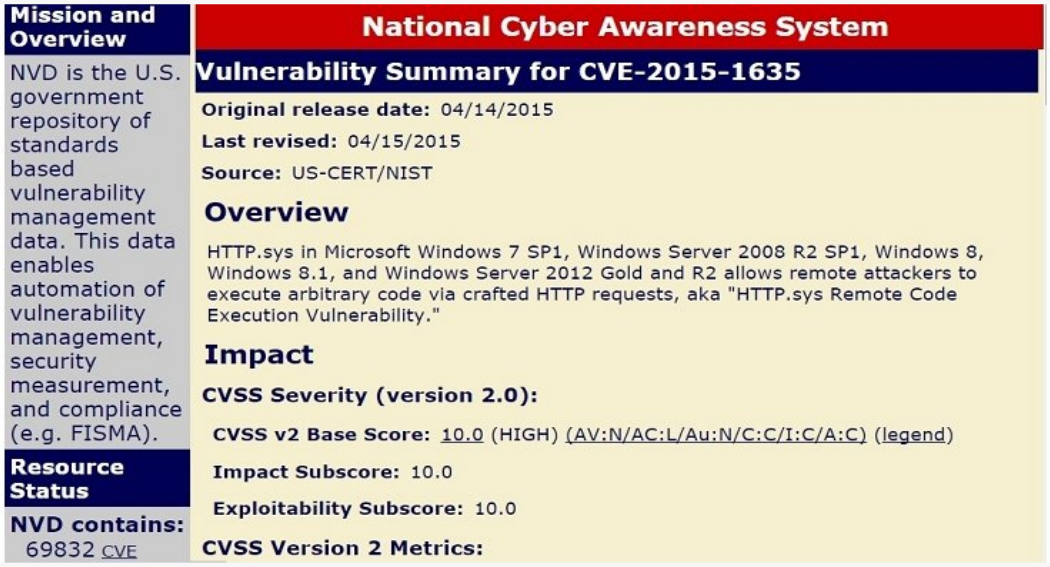
IIS Range

微軟IIS驚爆HTTP.sys死亡漏洞，一Ping系統恐癱瘓， SANS警告駭客正大肆搜尋肉票伺服器

微軟IIS網頁伺服器出現重大漏洞，資安專家評估，嚴重程度超越Shellshock漏洞，全球現有7千萬臺微軟網頁伺服器恐受影響。SANS更發現，已偵測到駭客大型搜尋行動，掃描全網際網路，尋找有此漏洞的微軟IIS網頁伺服器

HTTP.sys未檢查RANGE參數值,只要輸入超出Range參數範圍的值,就可能讓系統CRASH

文/ 黃彥棻 | 2015-04-20 發表



Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
69832 CVE

National Cyber Awareness System

Vulnerability Summary for CVE-2015-1635

Original release date: 04/14/2015

Last revised: 04/15/2015

Source: US-CERT/NIST

Overview

HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

IIS Rang Test

```
[root@140-117-101-164 ~]# telnet 140.117.72.138 80
Trying 140.117.72.138...
Connected to 140.117.72.138.
Escape character is '^]'.
GET / HTTP/1.1
Host: MS15034
Range: bytes=0-18446744073709551615

HTTP/1.1 416 Requested Range Not Satisfiable
Content-Type: text/html
Last-Modified: Thu, 08 Oct 2015 03:18:05 GMT
Accept-Ranges: bytes
ETag: "852bd9f2771d11:0"
Server: Microsoft-IIS/7.5
Date: Thu, 08 Oct 2015 07:20:57 GMT
Content-Length: 362
Content-Range: bytes */689
```

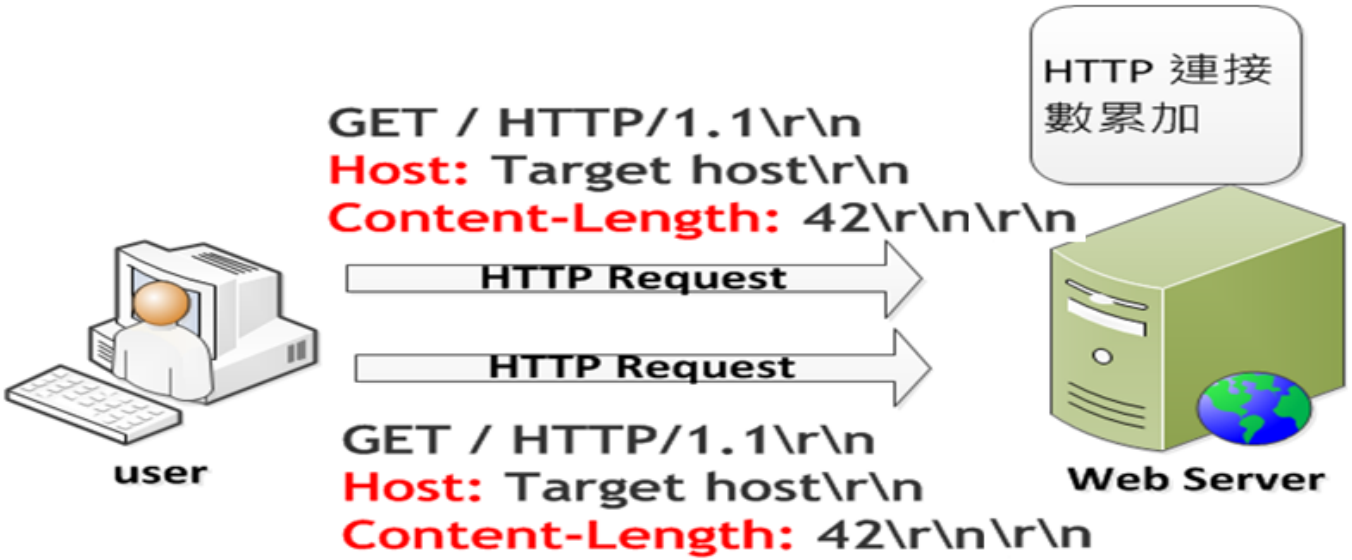
Request Header

CVE-2015-1635 (MS15034)

修正ms15-034漏洞

- 安裝編號為ms15-034.aspx的修正程式
- https://technet.microsoft.com/zh-tw/library/security/ms15-034.aspx

Slowloris



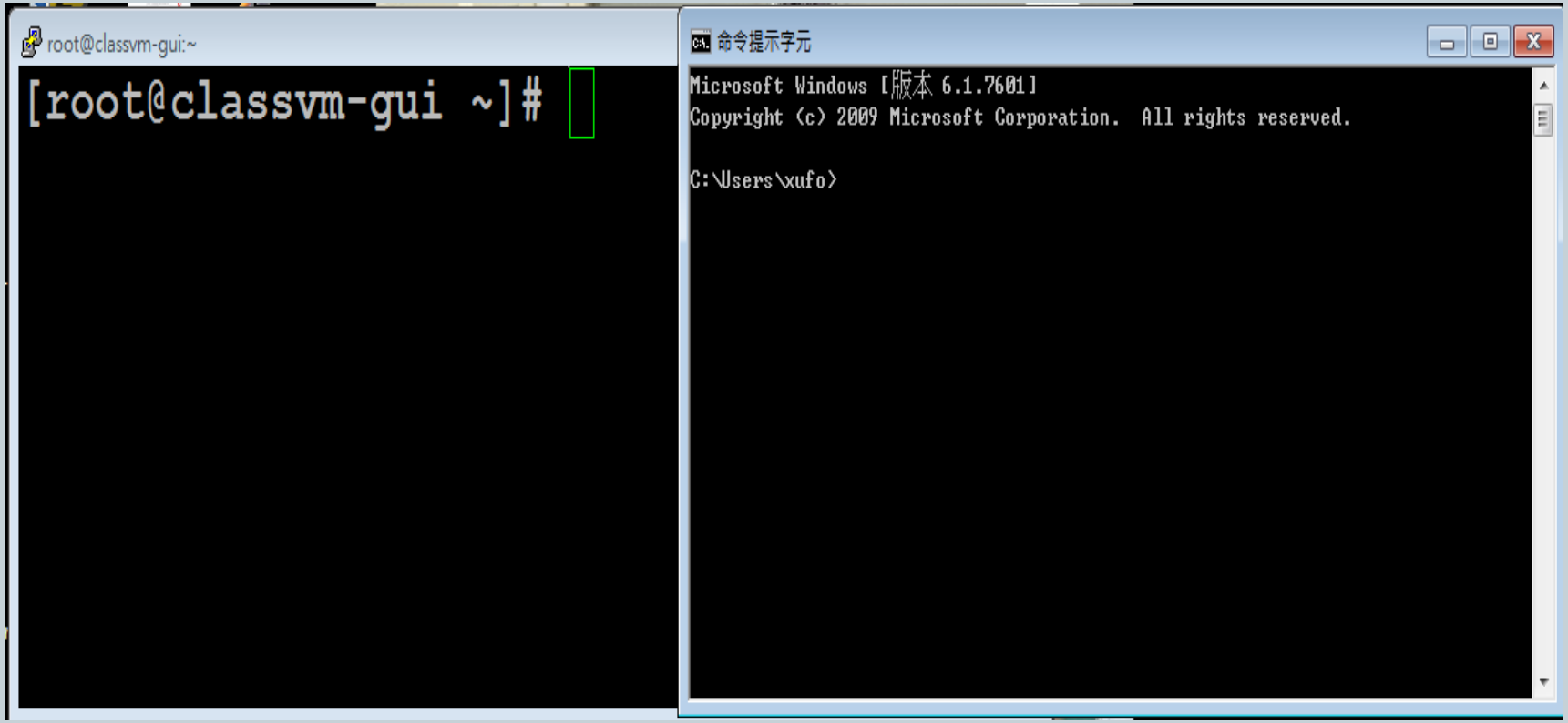
Slowloris HTTP DoS

Slowloris建議

- 檢查單一 ip 來源的 連線 情形, 給予數量或是逾時的一些限制
  - Apache Server
    - mod_antiloris , mod_reqtimeout , mod_limitipconn

ShellShock

- Bash 對環境變數的解析
- Gnu bash 4.3之前



ShellShock 測試

- env VAR='() { :;}; echo Bash is vulnerable!' bash -c "echo Bash Test

```
[root@classvm-gui ~]# env VAR='() { :;}; echo Bash is vulnerable!'
 bash -c "echo Bash Test"
Bash is vulnerable!
Bash Test
```

test-cgi

- Apache 預設測試檔案(cgi-bin/test-cgi)
- 利用環境變數顯示HTTP相關資訊

```
#!/bin/sh

# disable filename globbing
set -f

echo "Content-type: text/plain; charset=iso-8859-1"
echo

echo CGI/1.0 test script report:
echo

echo argc is $#. argv is "$*".
echo

echo SERVER_SOFTWARE = $SERVER_SOFTWARE
echo SERVER_NAME = $SERVER_NAME
echo GATEWAY_INTERFACE = $GATEWAY_INTERFACE
echo SERVER_PROTOCOL = $SERVER_PROTOCOL
echo SERVER_PORT = $SERVER_PORT
echo REQUEST_METHOD = $REQUEST_METHOD
echo HTTP_ACCEPT = "$HTTP_ACCEPT"
echo PATH_INFO = "$PATH_INFO"
echo PATH_TRANSLATED = "$PATH_TRANSLATED"
echo SCRIPT_NAME = "$SCRIPT_NAME"
echo QUERY_STRING = "$QUERY_STRING"
echo REMOTE_HOST = $REMOTE_HOST
echo REMOTE_ADDR = $REMOTE_ADDR
echo REMOTE_USER = $REMOTE_USER
echo AUTH_TYPE = $AUTH_TYPE
echo CONTENT_TYPE = $CONTENT_TYPE
echo CONTENT_LENGTH = $CONTENT_LENGTH
```

社交工程-瀏覽器

虎奇摩的 Flash 廣告

未經證實

抓到短期大量擴散勒索軟體的兇手 ~ 台灣雅虎奇摩的 Flash 廣告

摘要：

這篇文章可以解釋為什麼在短時間內會有大量的crypz(勒索病毒)系列的受害者突然出現，然後一定時間後就迅速減少

共同特徵：

1.瀏覽了雅虎或雅虎奇摩(沒錯，是tw.yahoo.com)

2.使用了過舊的FLASH且預設為啟動，FALSH版本為21.0.0.213以及之前的因為存在共通的漏洞而中獎，此漏洞已於五月中有更新補上，但如果沒有即時更新一樣中獎，而且最可怕的是，只要"看到"就會中獎

3.絕大部分使用IE瀏覽器，也有極少數使用IE以外瀏覽器，原因就是FLASH沒有即時更新，這次反而不是IE本身的漏洞

4.雅虎於6/8~6/9之間收到通報把相關連結下架，推測問題連結應於五月底至六月初之間(最早受害者於6/3~6/4大量發難)

社交工程-瀏覽器

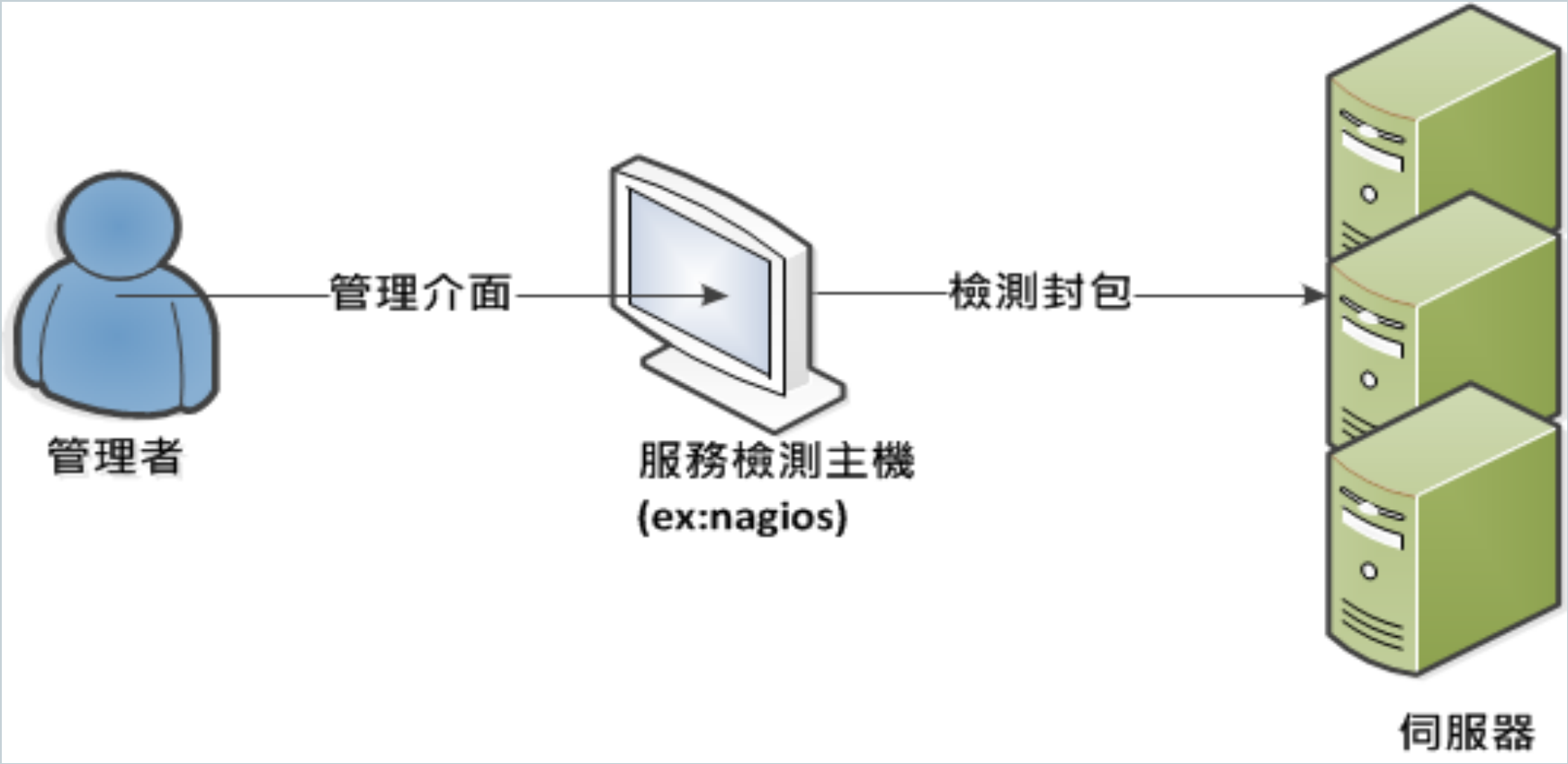
- 未修正的瀏覽器插件(adobe flash)->惡意FLASH
  - Falsh CVE-2015-5119

社交工程-Unicode

發布編號	ICST-ANA-2010-0006	發布時間	Mon Aug 09 00:00:00 CST 2010
事故類型	公告資訊	發現時間	Wed Aug 04 00:00:00 CST 2010
通告名稱	[內容更正] 駭客偽冒行政院院長室發送社交工程攻擊信件		
內容說明	＊因前封警訊影響平台漏列Windows系列平台，且建議措施不夠清楚，請各資安聯絡人參考本更新警訊進行防護措施。 技術服務中心於近日接獲通報，駭客偽冒行政院院長室發送社交工程攻擊信件，內文中包含有關人員之簽名檔，製作惡意程式(使用RTLO方法)誘使使用者點擊，以取得使用者權限或執行遠端程式。當使用者點擊這類檔案時，可能於受攻擊成功後遭植入惡意程式，攻擊者將可控制受害系統執行任意惡意行為。 該手法係利用作業系統解讀檔案名稱時，若遇到Unicode控制字元，會改變檔案名稱的顯示方式進行攻擊。駭客可以在檔案名稱中，插入特定的Unicode控制字元，導致作業系統在顯示該檔案名稱時，誤導使用者。 例如，駭客可能將惡意程式命名為：提醒[202E]TXT.SCR，即會顯示為：提醒RCS.TXT，讓收件人誤以為是純文字檔，提升點擊的機率。 本中心已發現使用該弱點之惡意文件，經由電子郵件進行攻擊。建議使用者參照以下建議措施來防堵這類的攻擊手法。		
影響平台	1. 所有Microsoft作業系統 2. 常見Linux平台之圖形介面(如KDE與GNOME)在支援Unicode時亦受影響		

心目中的完整網管系統?

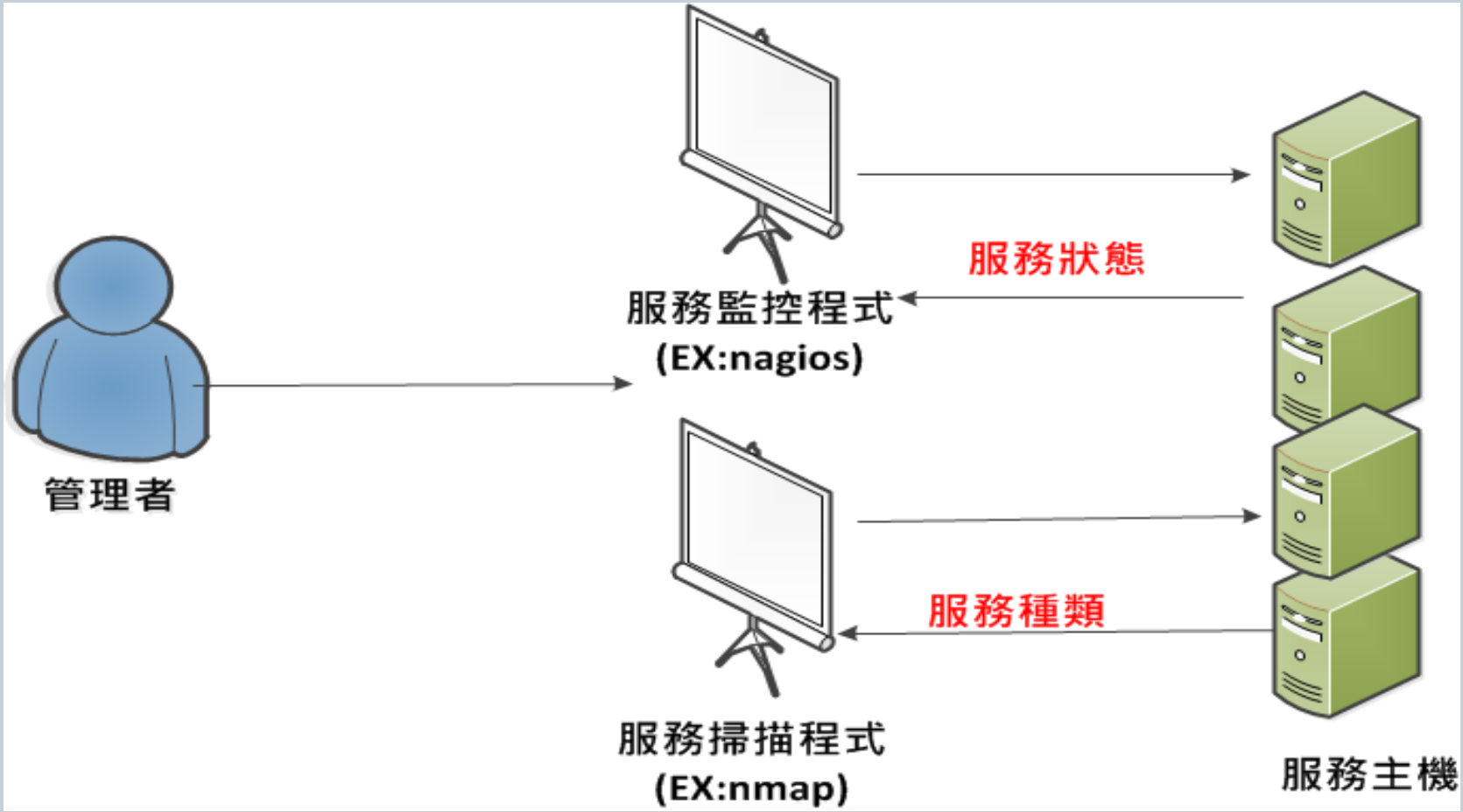
服務狀態掃描



服務狀態掃描的限制

- 僅能偵測已知的服務
- 未知的服務?

服務種類掃描



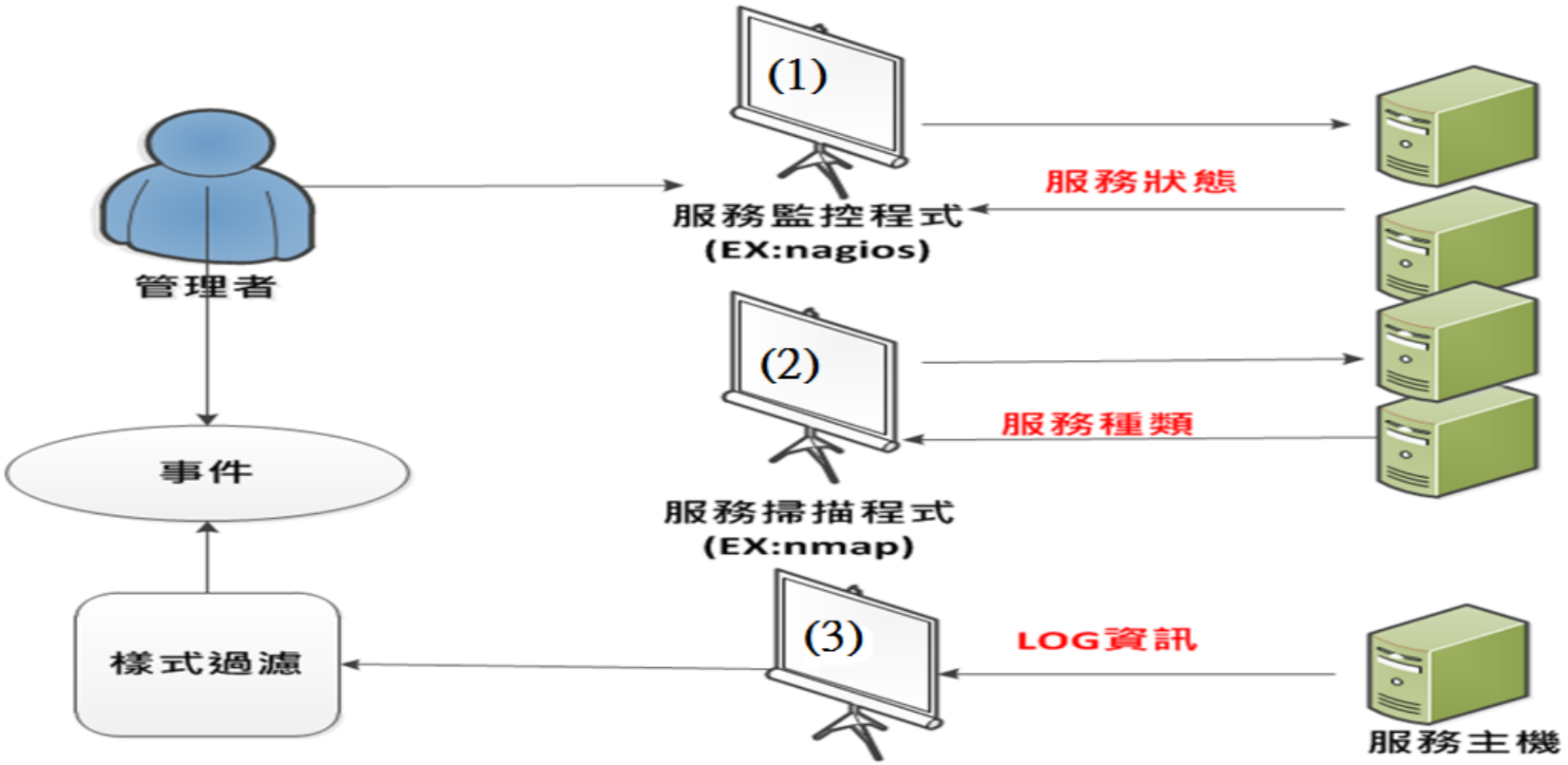
服務種類掃描的限制

- 當事件發生時,能即時告知
  - 當有人登入至系統時
  - 當有人使用隨身碟時
  - ……

LOG

- 魔鬼藏在LOG中
  - 登入事件? 任何事件?
- 如果主動回報LOG資訊
- LOG樣式→系統事件

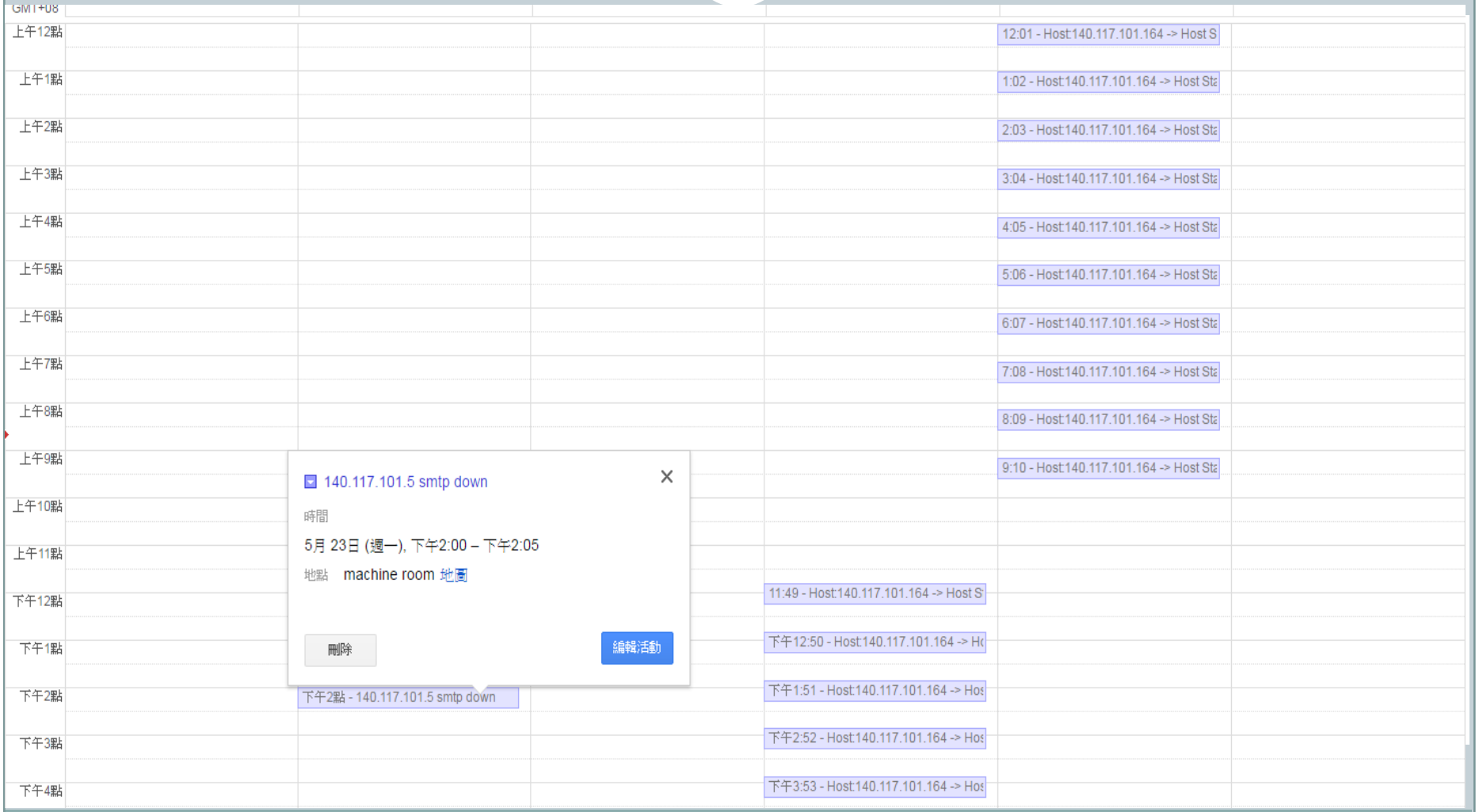
網管系統


(1)
服務狀態
服務監控程式
(EX:nagios)
管理者
(2)
服務種類
事件
服務掃描程式
(EX:nmap)
(3)
LOG資訊
樣式過濾
服務主機

結合google行事曆的服務偵測

軟體名稱	官方網址	說明
gcalcli	github.com/insanum/gcalcli	命令列型式的google行事曆管理軟體
Nagios 4.0.8	www.nagios.org	網路服務偵測軟體

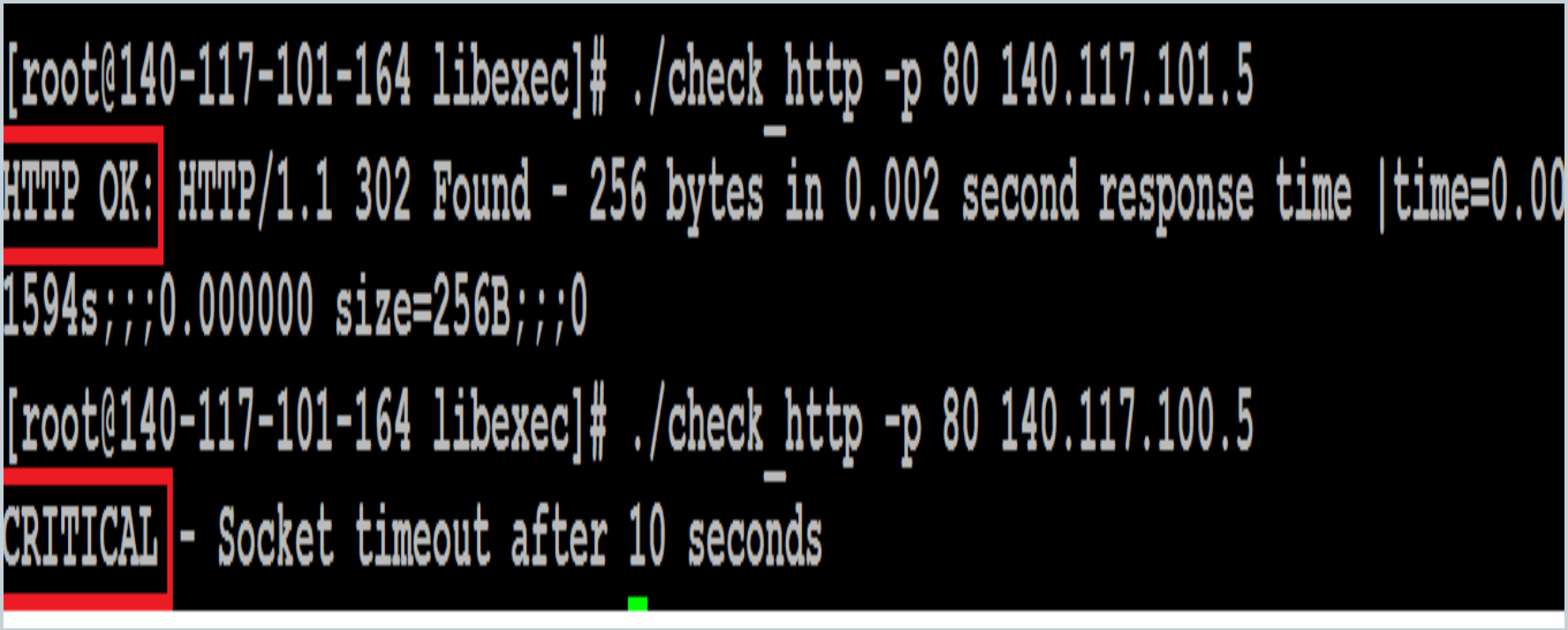
服務狀態偵測-Nagios



Nagios plug_in

```
check_apt                check_ldap               check_real
check_breeze             check_ldaps              check_rpc
check_by_ssh             check_load               check_sensors
check_clamd              check_log                check_simap
check_cluster            check_mailq              check_smtp
check_dhcp               check_mrtg               check_spop
check_disk               check_mrtgtraf           check_ssh
check_disk_smb           check_nagios             check_ssmtp
check_dummy              check_nntp               check_swap
check_file_age           check_nntps              check_tcp
check_flexlm             check_nt                 check_time
check_ftp                check_ntp                check_udp
check_http (檢查HTTP服務)  check_ntp_peer           check_ups
check_icmp               check_ntp_time           check_uptime
check_ide_smart          check_nwstat             check_users
check_ifoperstatus       check_oracle             check_wave
check_ifstatus           check_overcr             negate
check_imap               check_ping               urlize
check_ircd               check_pop                utils.pm
check_jabber             check_procs              utils.sh
```

Plug_in


[root@140-117-101-164 libexec]# ./check_http -p 80 140.117.101.5
HTTP OK: HTTP/1.1 302 Found - 256 bytes in 0.002 second response time |time=0.00
1594s;;;0.000000 size=256B;;;0
[root@140-117-101-164 libexec]# ./check_http -p 80 140.117.100.5
CRITICAL - Socket timeout after 10 seconds

googlecl

- http://github.com/insanum/gcalcli
  - 命令列型式的google行事曆管理軟體
    - 支援目前google服務所採用的OAUTH2認證方式
    - 可列出目前行事曆中的所記載的事項
    - 可新增或刪除或尋找行事曆中所記載的事項

Googlecl install

執行指令	
yum install python	安裝gcalcli所需的python模組
pip install --upgrade google-api-python-client	所需的python模組
pip install --upgrade python-dateutil	
pip install --upgrade python-gflag	
pip install --upgrade gcalcli	

Googlecl 授權

```
# gcalcli list --noauth_local_webserver

Go to the following link in your browser:

    https://accounts.google.com/o/oauth2/auth?scope=https%3A%2F%2Fwww.googleapis
.com%2Fauth%2Fcalendar            %2Fwww.googleapis.com%2Fauth%2Furlshortener&re
direct_uri=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&response_type=code&client_id=2328
67          s.googleusercontent.com&access_type=offline (1)取得授權碼網址

Enter verification code: 4/SRT( (2)授權碼    HwF9cI              vHA8YP2qYrTcU
Authentication successful.
```

(1)以瀏覽器瀏覽授權網址取得授權碼並輸入

Googlecl 指令新增

Googlecl 新增

參數	參數說明
--calendar	行事曆名稱
--title	事件標題
--where	所在地點
--when	事件時間，格式為「月/日/西元年 時:分」
--duration	持續時間(分)
--description	詳細內文
--reminder [時間]	設定在該事件的設定時間多久之前需通知行事曆的擁有者,形式如下 Popup Email Sms(not work)

Nagios 參考

- 以Nagios不間斷監控系統服務
  - http://netadmin.pcuser.com.tw/article_content.aspx?sn=1101030006
- 指令列串接**Google**日曆 打造超炫全自動系統日誌
  - http://netadmin.pcuser.com.tw/article_content.aspx?sn=1605130016&jump=2

服務偵測

軟體名稱	官方網址	說明
nmap	nmap.org	服務掃描軟體
pbnj	pbnj.sourceforge.net	以資料庫儲存nmap的輸出

服務類型偵測-nmap

- 服務類型偵測軟體
- 支援NSE (Nmap Scripting Engine)
- 可擴充成弱點掃描軟體

服務偵測-nmap

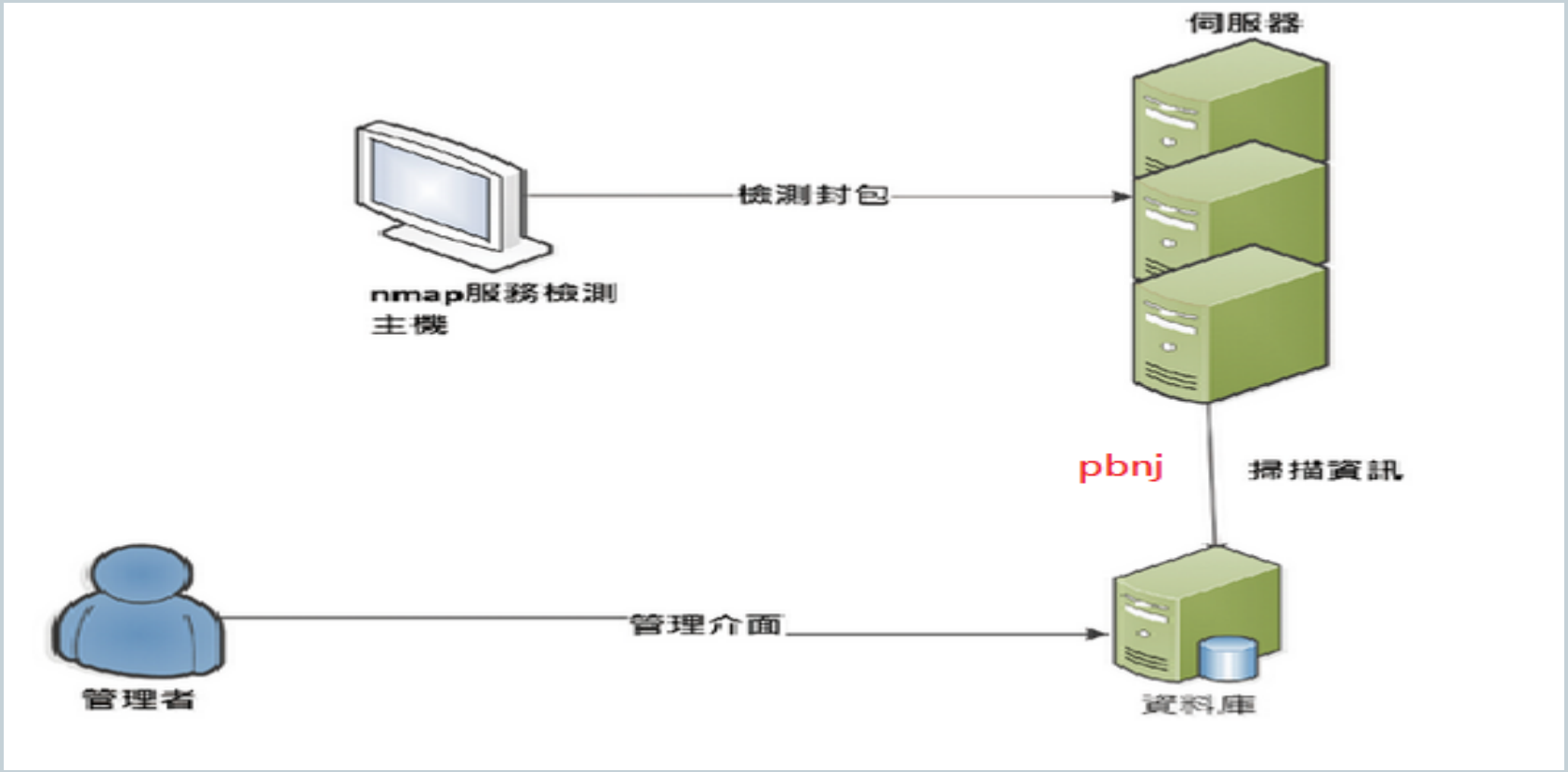
```
[root@140-117-101-164 bin]# ./nmap -sV 127.0.0.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-14 14:15 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000053s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE VERSION
21/tcp   open     ftp     vsftpd 3.0.2
22/tcp   filtered ssh
80/tcp   filtered http
3306/tcp open     mysql   MySQL 5.5.45
Service Info: OS: Unix
```

服務名稱

pbnj

- Perl 程式
- nmap輸出至資料庫

Nmap-pbnj



pbnj

```
[root@140-117-101-164 pbnj]# scanpbnj 140.117.100.5


---------------------------------------
Starting Scan of 140.117.100.5
Machine is already in the database
Checking Current Services
        = ftp:21 is (2.0.6) vsftpd
        = ssh:22 is (5.0) OpenSSH
        = smtp:25 is (unknown version) Postfix smtpd
        = http:80 is (2.0.63) Apache httpd
Scan Complete for 140.117.100.5
```

Pbnj-mysql資料

service	state	port	protocol	version	banner	machine_updated	updated_on
ssh	up	22	tcp	5.0	OpenSSH	1444806651	Wed Oct 14 15:10:51 2015
smtp	up	25	tcp	unknown version	Postfix smtpd	1444806651	Wed Oct 14 15:10:51 2015
http	up	80	tcp	2.0.63	Apache httpd	1444806651	Wed Oct 14 15:10:51 2015
ftp	up	21	tcp	2.0.6	vsftpd	1444807383	Wed Oct 14 15:23:03 2015
ftp	down	21	tcp	2.0.6	vsftpd	1444807451	Wed Oct 14 15:24:11 2015

state

up:目前正常運作中

down:原來正常運作,目前停止運作

Nmap 弱掃(heartbleed)

- NSE(Nmap Scripting Engine)

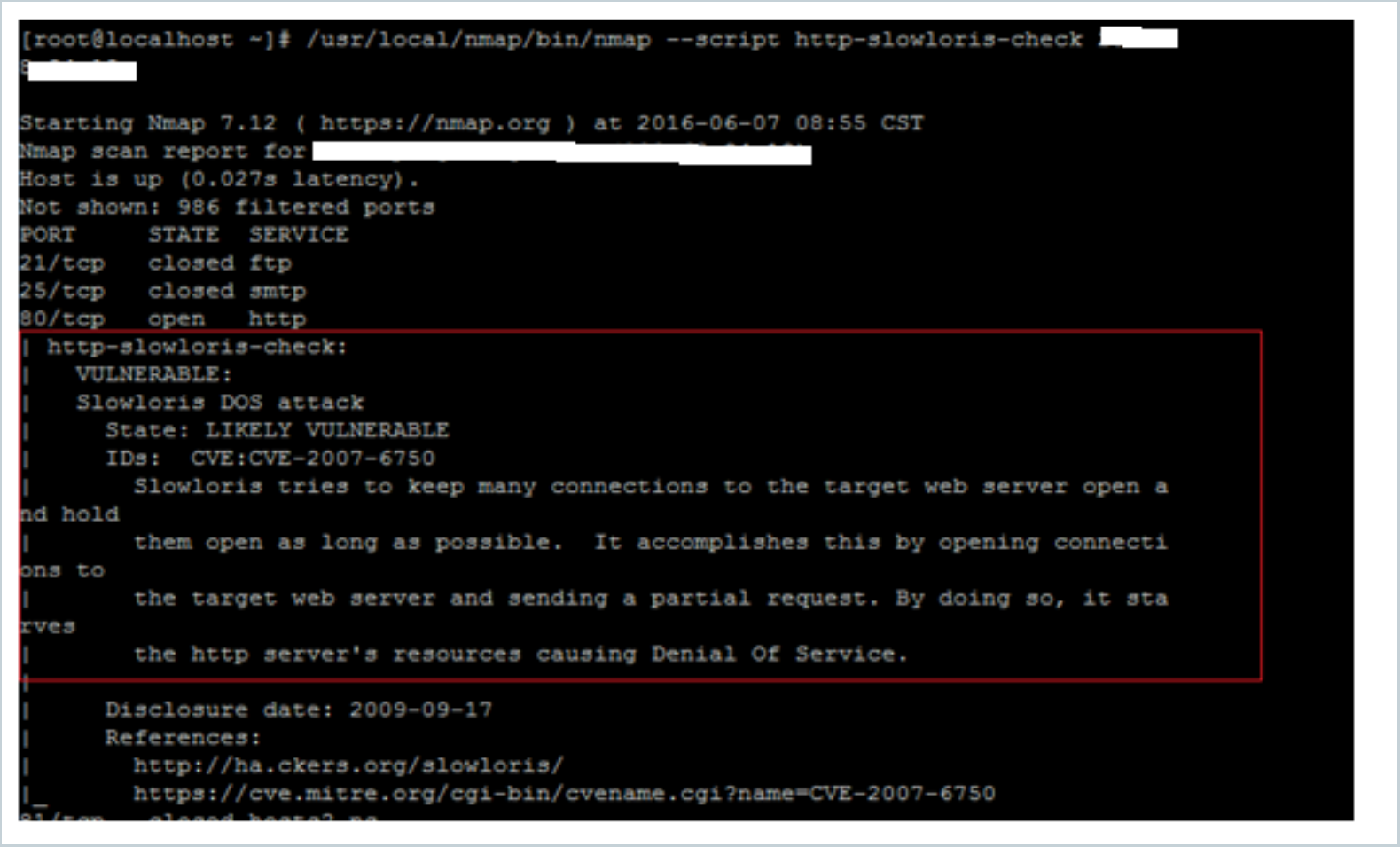
```
nmap -p 443 --script ssl-heartbleed <target>
```

Script Output

```
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to
|     State: VULNERABLE
|     Risk factor: High
|     Description:
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://www.openssl.org/news/secadv_20140407.txt
|_      http://cvedetails.com/cve/2014-0160/
```

有漏洞

Nmap 弱掃(slowloris)



Nmap-NSE

- https://nmap.org/nsedoc/scripts/

nmap 參考

- **輕鬆擴充nmap掃描能力**
  - http://www.netadmin.com.tw/article_content.aspx?sn=1312030002
- **掌握網路服務狀態 以利察覺主機可疑活動**
  - http://60.199.248.203/article_content.aspx?sn=1504080004

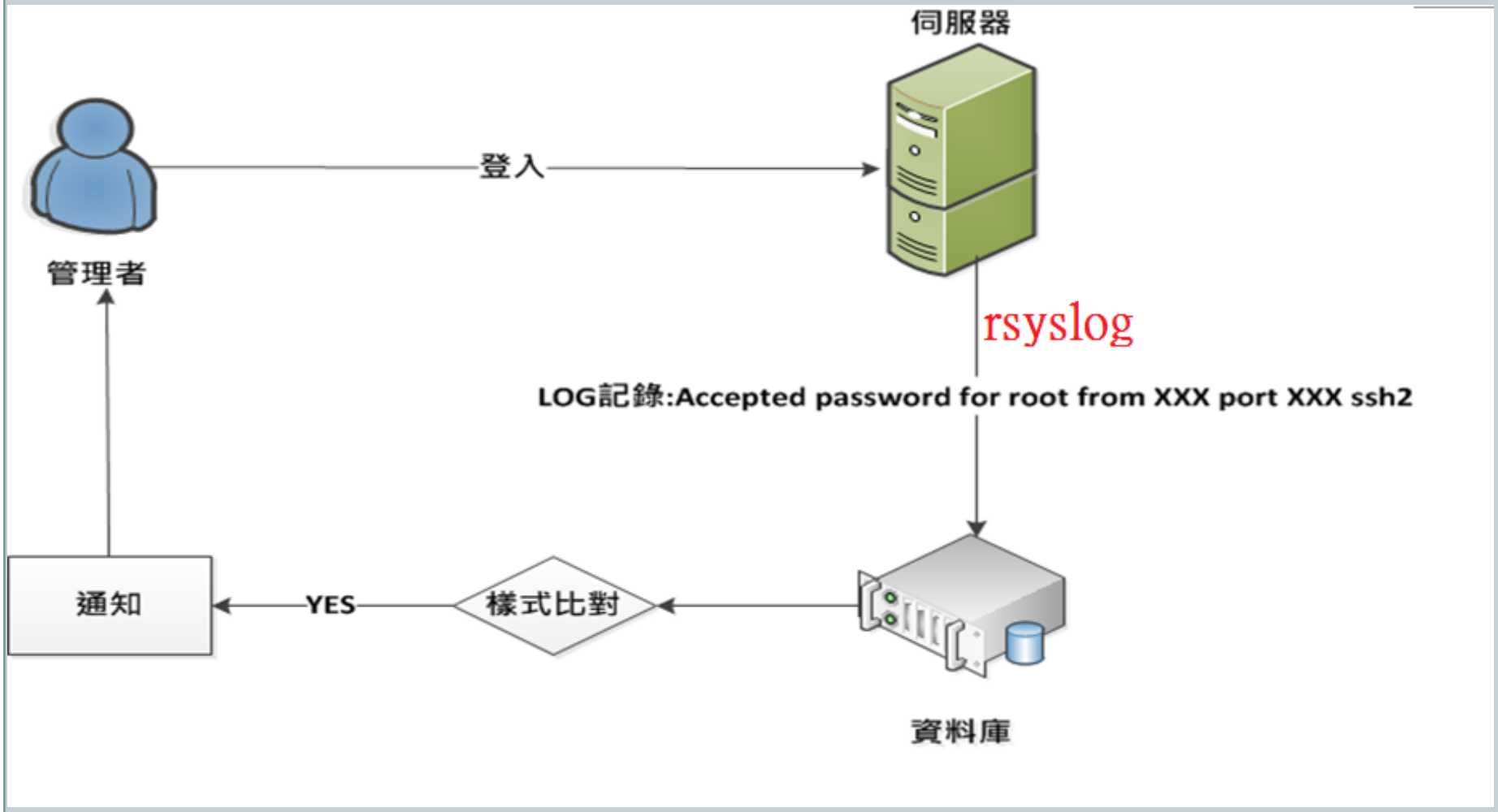
LOG

- 我想要
  - 有人登入系統時能即時告知
  - 有人不斷的在TRY我的主機能即時告知
  - ……

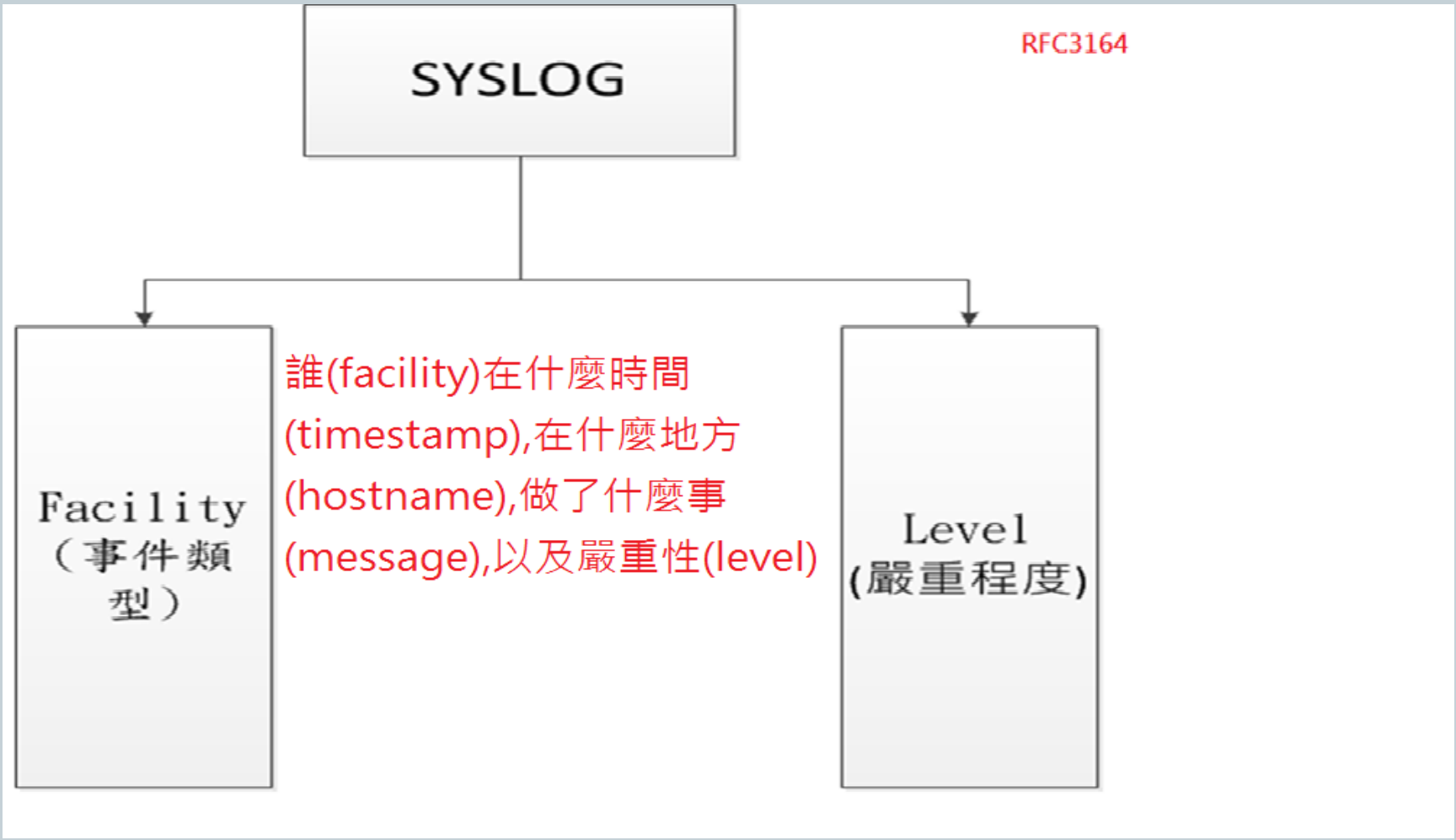
LOG

軟體名稱	官方網址	說明
Event Log	code.google.com/p/eventlog-to-syslog/	將微軟的EVENT LOG傳遞至syslog 伺服器
LOG Parser	www.microsoft.com/en-us/download/details.aspx?id=24659	以SQL指令來取得微軟event log的命令列型式工具
rsyslog	www.rsyslog.com	LINUX系統的syslog 程式
mysql	www.mysql.com	儲存LOG資訊的資料庫

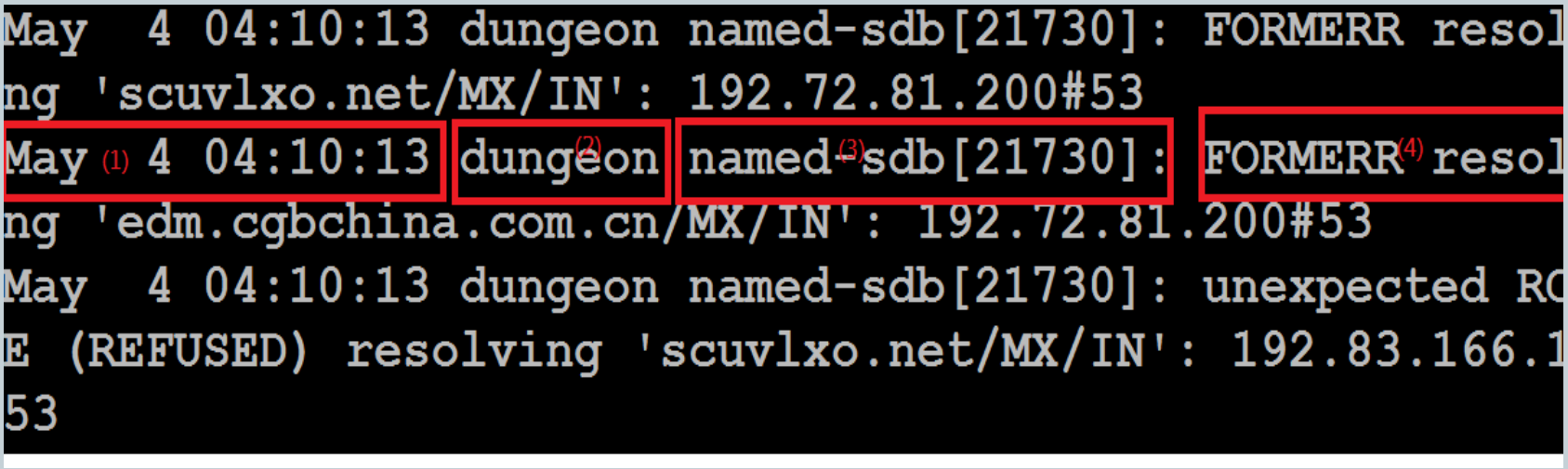
LOG流程-linux系統



syslog


SYSLOG
RFC3164
Facility
（事件類
型）
誰(facility)在什麼時間
(timestamp),在什麼地方
(hostname),做了什麼事
(message),以及嚴重性(level)
Level
(嚴重程度)

Syslog format



(1)發生時間 (2)主機名稱 (3)程式名稱 (4)訊息

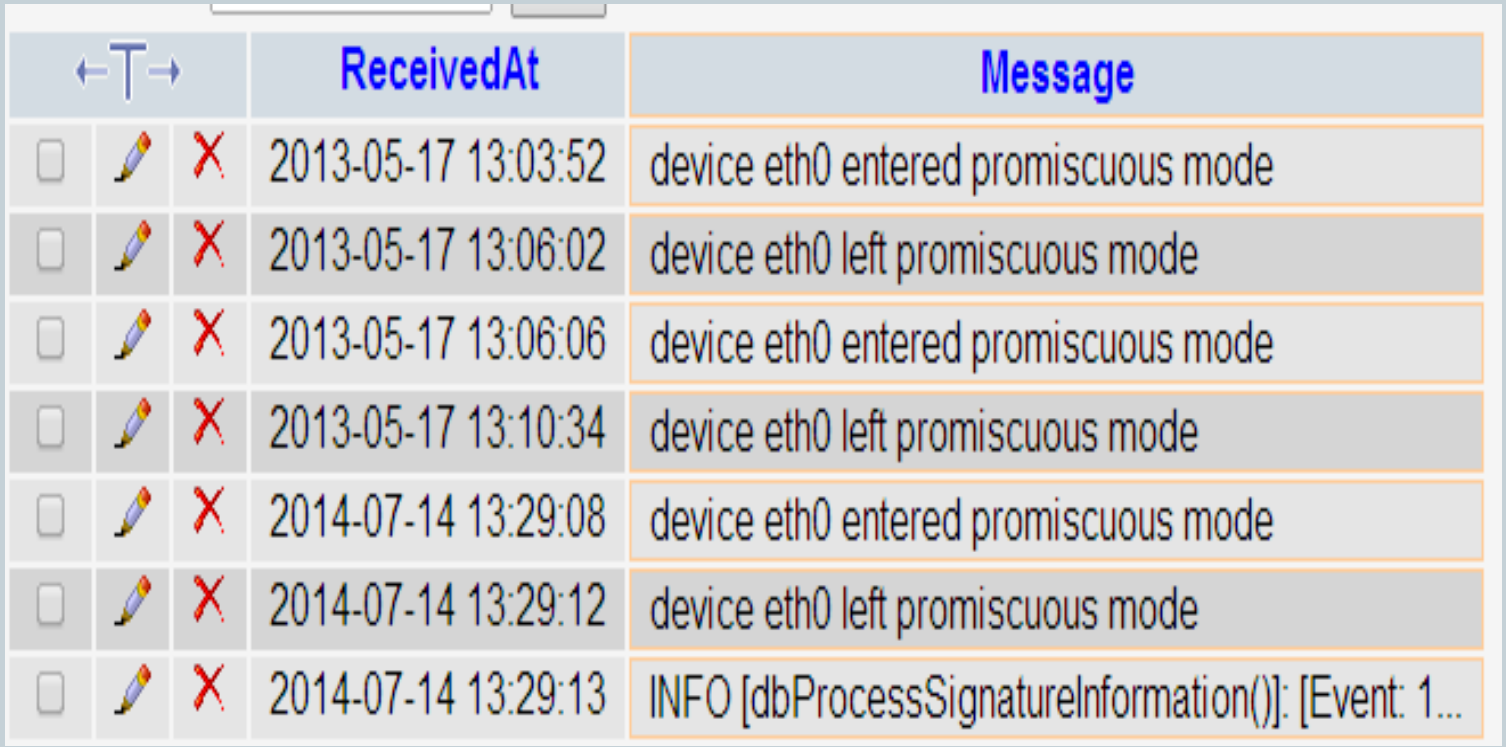
SYSLOG樣式-ssh brute force

ReceivedAt	Message
2014-01-21 10:12:00	Failed password for invalid user leonob from 61.3...
2014-01-21 10:12:03	Failed password for invalid user ftpuser from 61....
2014-01-21 10:12:05	Failed password for root from 61.36.24.57 port 55...
2014-01-21 10:12:08	Failed password for root from 61.36.24.57 port 56...
2014-01-21 10:12:11	Failed password for root from 61.36.24.57 port 57...
2014-01-21 10:12:14	Failed password for root from 61.36.24.57 port 57...
2014-01-21 10:12:17	Failed password for root from 61.36.24.57 port 58...
2014-01-21 10:12:20	Failed password for root from 61.36.24.57 port 58...
2014-01-21 10:12:23	Failed password for root from 61.36.24.57 port 59...
2014-01-21 10:12:26	Failed password for root from 61.36.24.57 port 60...
2014-01-21 10:12:29	Failed password for root from 61.36.24.57 port 32...
2014-01-21 10:12:32	Failed password for root from 61.36.24.57 port 33...
2014-01-21 10:12:35	Failed password for invalid user oracle from 61.3...
2014-01-21 10:12:38	Failed password for root from 61.36.24.57 port 35...
2014-01-21 10:12:41	Failed password for root from 61.36.24.57 port 37...
2014-01-21 10:12:44	Failed password for root from 61.36.24.57 port 38...
2014-01-21 10:12:47	Failed password for root from 61.36.24.57 port 39...
2014-01-21 10:12:50	Failed password for root from 61.36.24.57 port 39...
2014-01-21 10:12:53	Failed password for root from 61.36.24.57 port 41...
2014-01-21 10:12:56	Failed password for root from 61.36.24.57 port 41...
2014-01-21 10:13:00	Failed password for root from 61.36.24.57 port 42...
2014-01-21 10:13:03	Failed password for root from 61.36.24.57 port 43...

SYSLOG樣式-imap brute force

←T→	ReceivedAt	Message
☐	2014-06-02 06:14:40	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:36	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:36	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:32	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:32	imap-login: Disconnected: user=<access>, method=P...
☐	2014-06-02 06:14:32	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:28	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:28	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:28	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:28	imap-login: Disconnected: user=<access>, method=P...
☐	2014-06-02 06:14:24	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:24	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:24	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:24	imap-login: Disconnected: user=<access>, method=P...
☐	2014-06-02 06:14:20	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:20	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:20	imap-login: Disconnected: user=<pwrchute>, method...
☐	2014-06-02 06:14:20	imap-login: Disconnected: user=<account>, method=...
☐	2014-06-02 06:14:20	imap-login: Disconnected: user=<access>, method=P...
☐	2014-06-02 06:14:16	pam_unix(dovecot:auth): authentication failure; l...
☐	2014-06-02 06:14:16	pam_unix(dovecot:auth): authentication failure; l...
☑	2014-06-02 06:14:16	pam_unix(dovecot:auth): authentication failure; l...

SYSLOG樣式-promiscuous

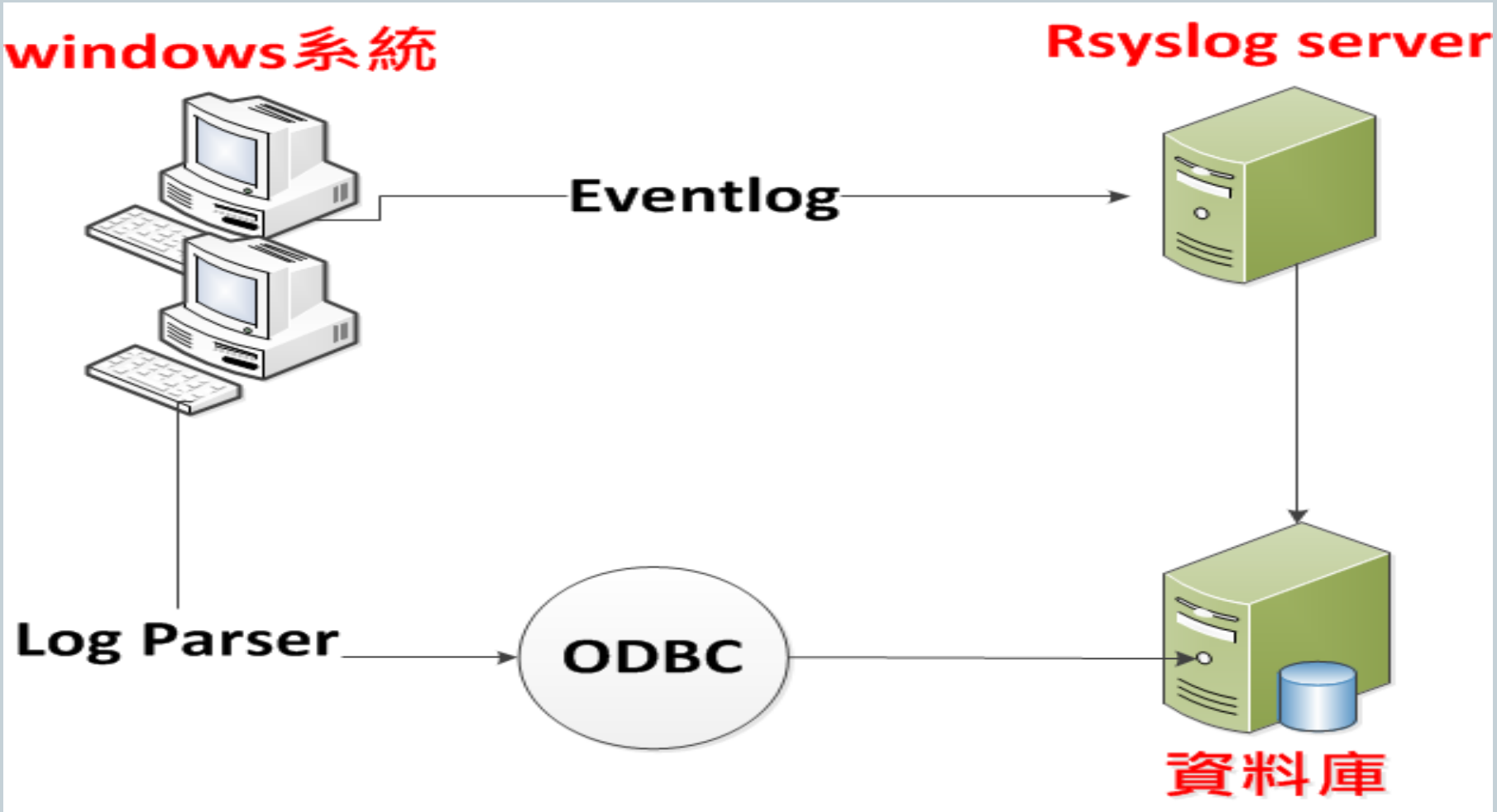


ReceivedAt	Message
2013-05-17 13:03:52	device eth0 entered promiscuous mode
2013-05-17 13:06:02	device eth0 left promiscuous mode
2013-05-17 13:06:06	device eth0 entered promiscuous mode
2013-05-17 13:10:34	device eth0 left promiscuous mode
2014-07-14 13:29:08	device eth0 entered promiscuous mode
2014-07-14 13:29:12	device eth0 left promiscuous mode
2014-07-14 13:29:13	INFO [dbProcessSignatureInformation()]: [Event: 1...

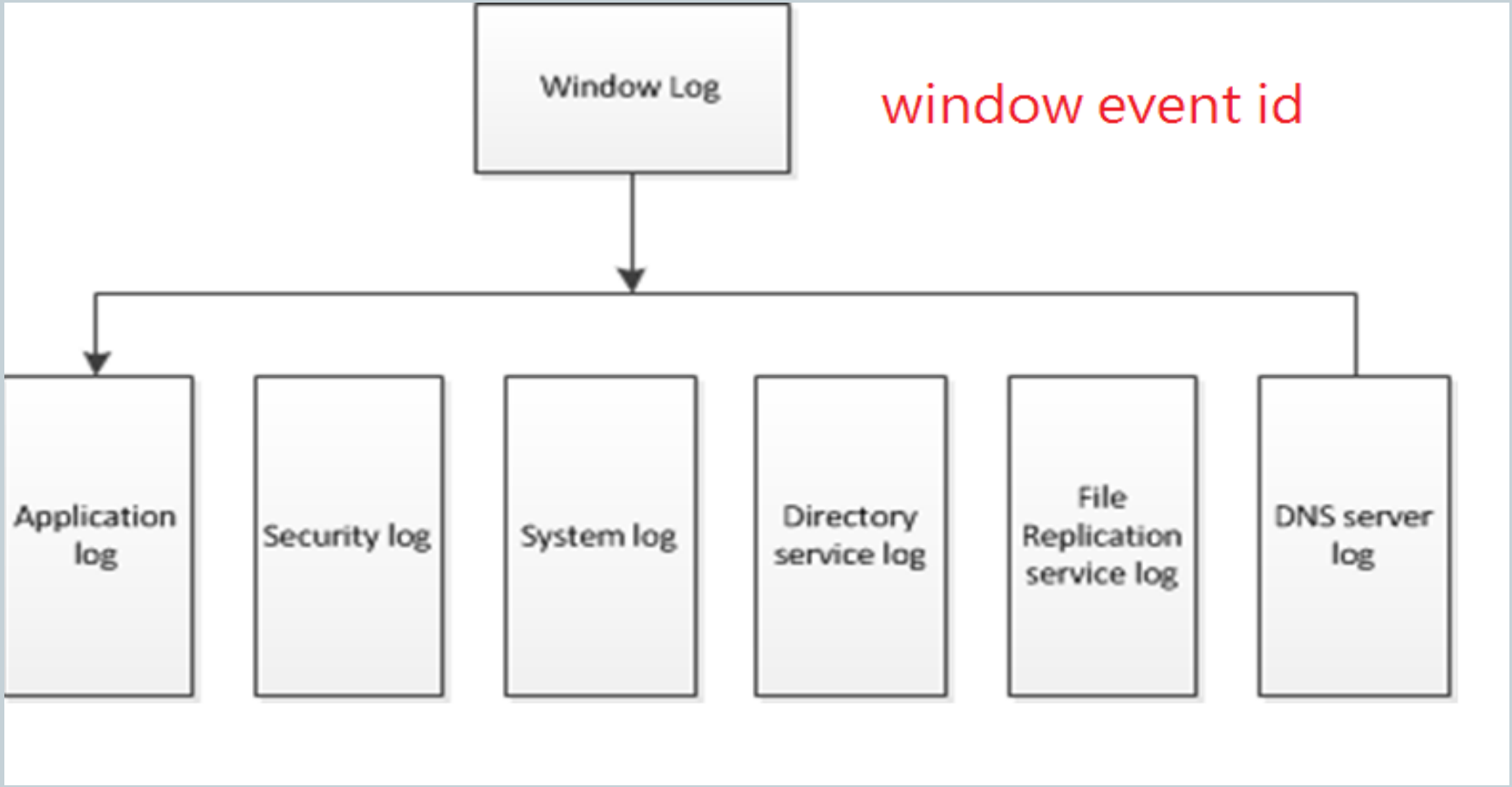
SYSLOG樣式-login

ReceivedAt	Message
2014-01-21 09:59:20	Accepted password for root from 140.117.71.25 por...
2014-01-21 13:53:13	Accepted password for root from 140.117.71.25 por...
2014-01-21 16:34:31	Accepted password for root from 140.117.71.25 por...
2014-01-22 08:54:47	Accepted password for root from 140.117.71.25 por...
2014-01-22 09:01:42	Accepted password for root from 140.117.71.25 por...
2014-01-22 10:08:23	Accepted password for root from 140.117.71.25 por...
2014-01-22 10:12:58	Accepted password for root from 140.117.71.25 por...
2014-01-22 14:11:19	Accepted password for root from 140.117.71.25 por...
2014-01-22 19:45:40	Accepted password for root from 59.127.71.103 por...
2014-01-23 08:55:03	Accepted password for root from 140.117.71.25 por...
2014-01-23 09:38:06	Accepted password for root from 140.117.71.25 por...

Log –windows 系統



Windows event log

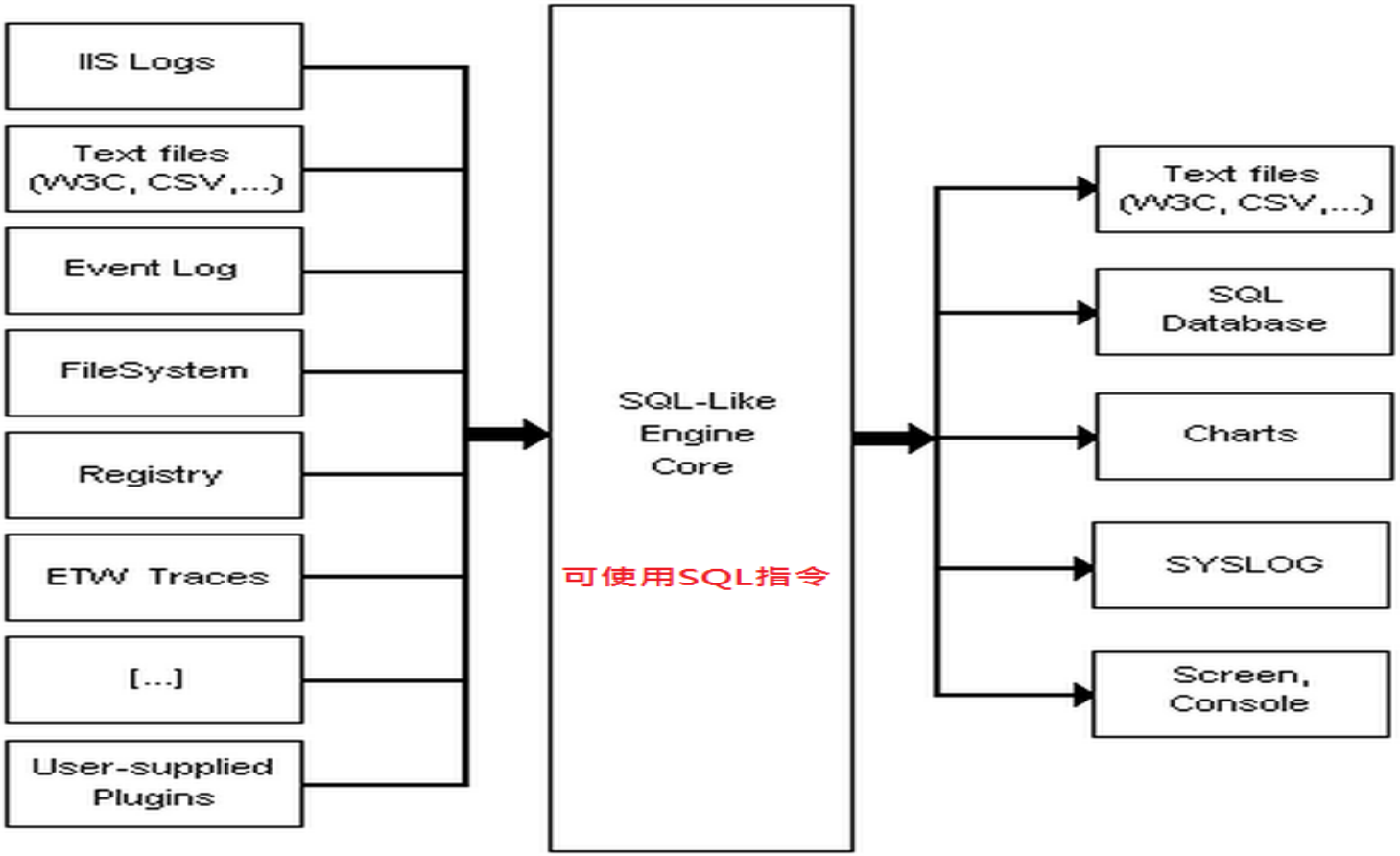


eventLog-syslog資訊

LOG Parser

- 記錄分析工具
  - 以sql指令解析文字型態的log檔案
  - 支援windows系統各種格式的log

LOG Parser


IIS Logs
Text files (W3C, CSV,...)
Event Log
FileSystem
Registry
ETW Traces
[...]
User-supplied Plugins
SQL-Like Engine Core
可使用SQL指令
Text files (W3C, CSV,...)
SQL Database
Charts
SYSLOG
Screen, Console

LOG Parser

- 語法
  - Logparser –i:[輸入源] –o:[輸出] “ SQL查詢指令 ”

LOG Parser-輸入源

輸入源名稱	說明
IISW3C	IIS 輸出的 W3C 格式記錄檔(預設)
BIN	IIS 輸出的二進位記錄檔
IISODBC	IIS 的 ODBC 記錄檔
HTTPERR	輸出的httperr.log (6.0之後提供)
URLSCAN	URL scan 工具掃瞄輸出的記錄檔
CSV	CSV（Comma Separated Values）格式文字檔
TSV	TSV（Tab Separated Values）格式文字檔
XML	XML 資料檔
W3C	W3C 格式記錄檔

LOG Parser-輸入源

輸入源名稱	說明
EVT	Windows 事件檢視器
FS	檔案系統
REG	登錄資料庫（Registry）

LOG Parser-輸出

輸出源名稱	說明
W3C	W3C格式
XML	XML格式
TSV	輸出以 Tab 符號分隔的記錄檔
SYSLOG	輸出syslog格式資訊
NAT	輸出可讀式表格化欄位格式（readable tabulated column format）的記錄檔。
IIS	輸出 IIS 記錄檔（非 W3C）格式的記錄檔
SQL	可輸出至資料庫
CSV	輸出CSV格式
CHART	將資料輸出成圖表

LOG Parser-Example

```
D:\iislog>LogParser.lnk  -i:EVT -o:NAT "SELECT top 1  *  FROM System"
EventLog RecordNumber TimeGenerated       TimeWritten         EventID EventType
EventTypeName     EventCategory EventCategoryName SourceName Strings
          ComputerName  SID    Message
                Data
                                欄位名稱
-------- ------------ ------------------- ------------------- ------- ---------
-------------- ------------ --------------- ---------- ----------------
--------- ------------ ------ ------------------------------------------
---------------- ------

System   1            2015-04-10 18:23:39 2015-04-10 18:23:39 6011    4
Information event 0            None                EventLog   37L4247F27-25!WIN-N
E1GD9ISO81 37L4247F27-25 <NULL> 這台電腦的 NetBIOS 名稱及 DNS 主機名稱已經從 37L
4247F27-25 變更為 WIN-NE1GD9ISO81。 <NULL>  取得系統事件
```

LOG實作資訊

- 輸出Windows主機Eventlog 透過Syslog存入MySQL
  - **http://**netadmin.pcuser.com.tw/**article_content.aspx?sn=1602030005**
- 將LOGPARSE 產出的資料以ODBC寫入資料
  - http://netadmin.pcuser.com.tw/article_content.aspx?sn=1512030004

感謝您的聆聽