主從式稽核記錄

報告人:吳惠麟
Email:skysea6312@gmail.com

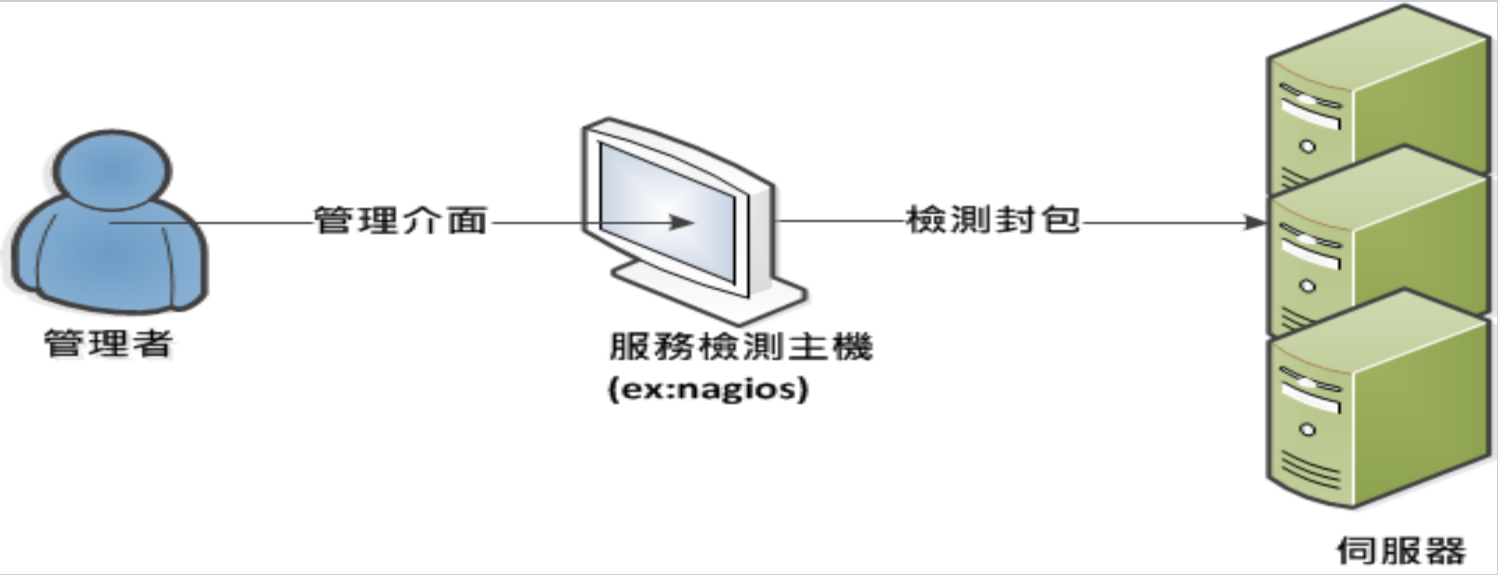
大綱

- rsyslog with mysql
- Sagan IDS

環境設定

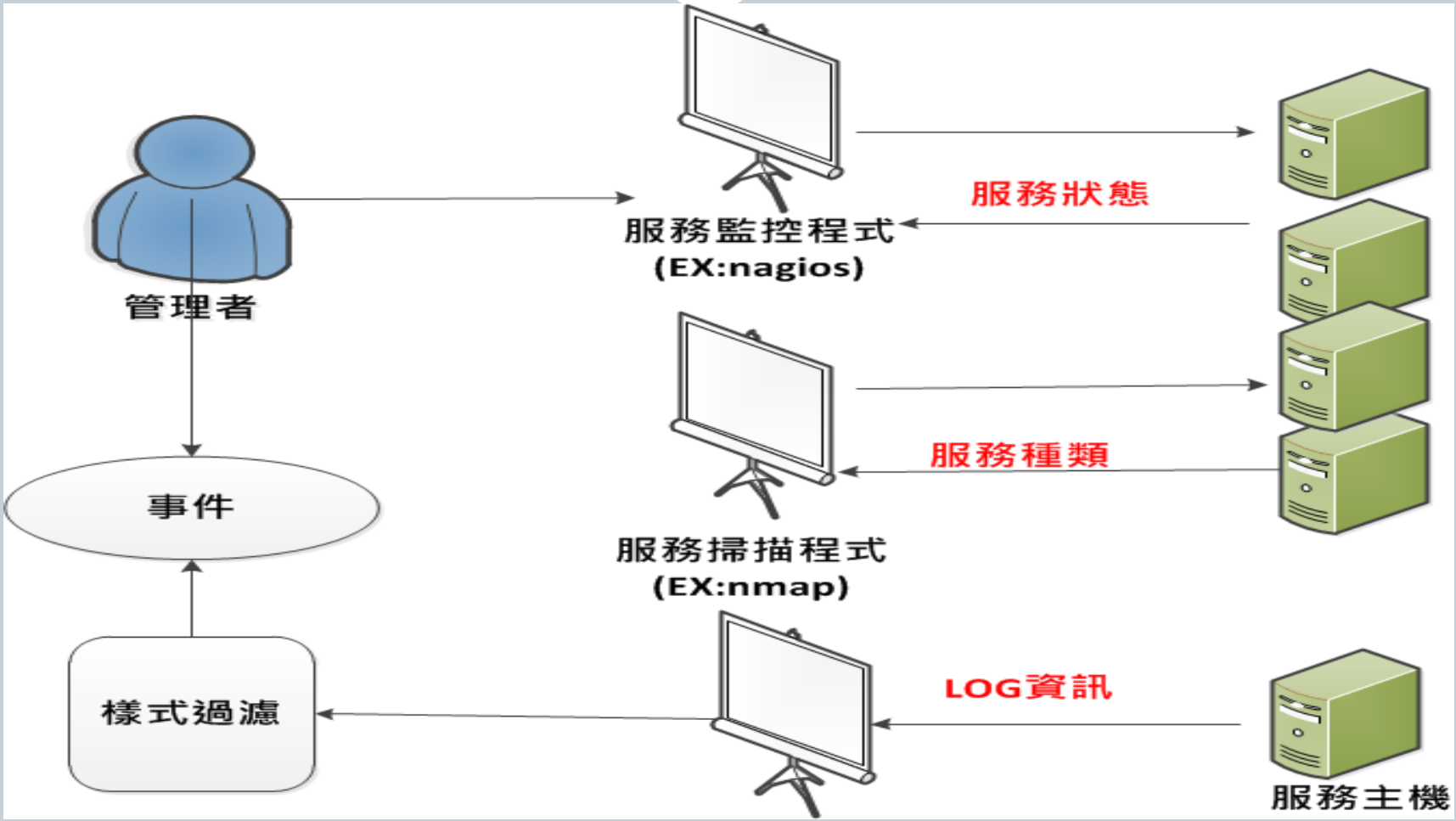
- iptables –F
- /usr/local/apache2/bin/apachectl start
- /usr/local/mysql5/bin/mysqld_safe &
- /usr/local/rsyslog/sbin/rsyslogd -f /usr/local/rsyslog/etc/rsyslog.conf
- http://localhost/loganalyzer #LOG介面
- /usr/local/sagan/sbin/sagan -f /usr/local/sagan/etc/sagan.yaml -D

這樣就夠了嗎

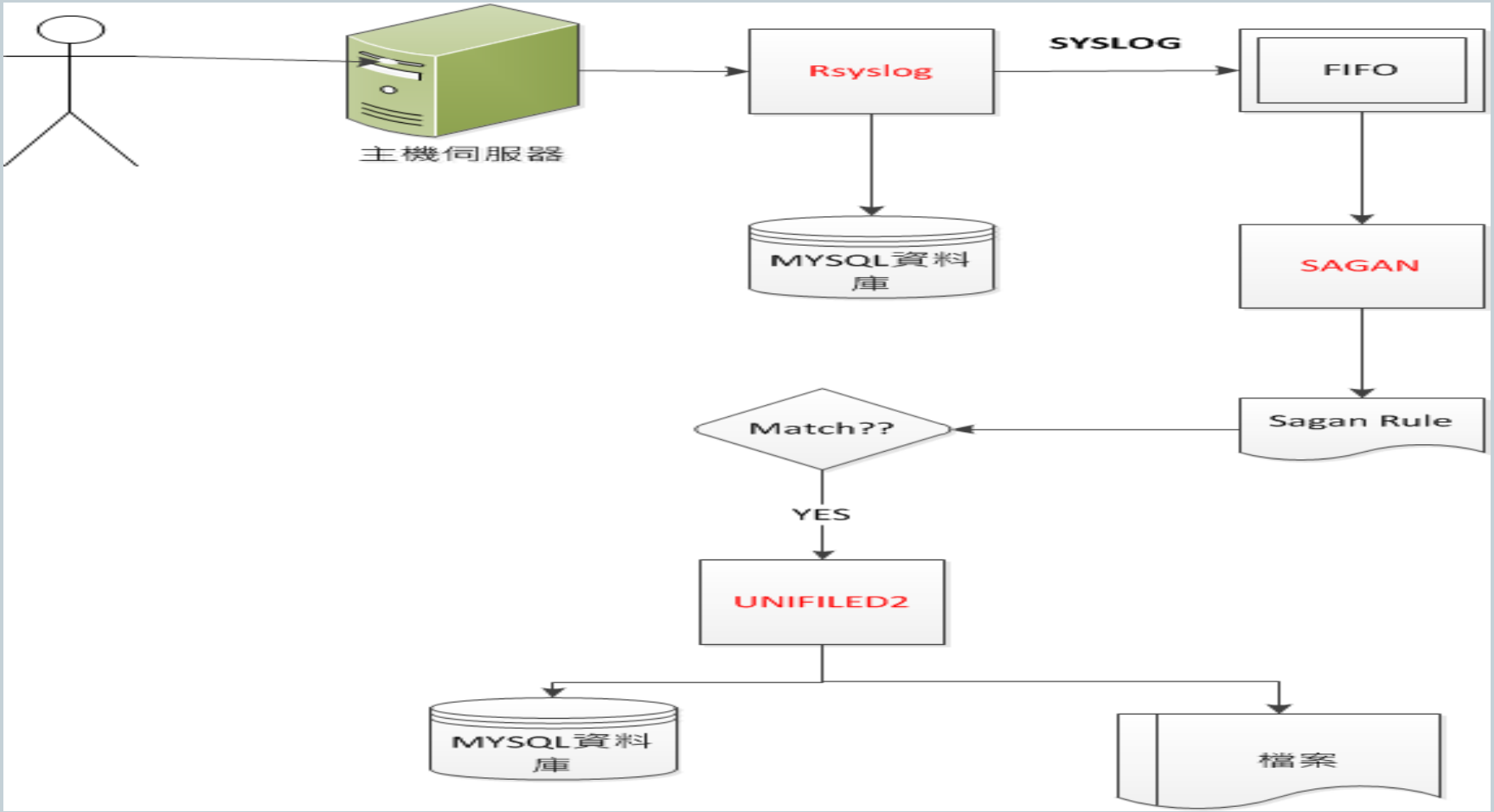


Q:多出的服務??
Q:伺服器細節部份(如登入)

架構


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

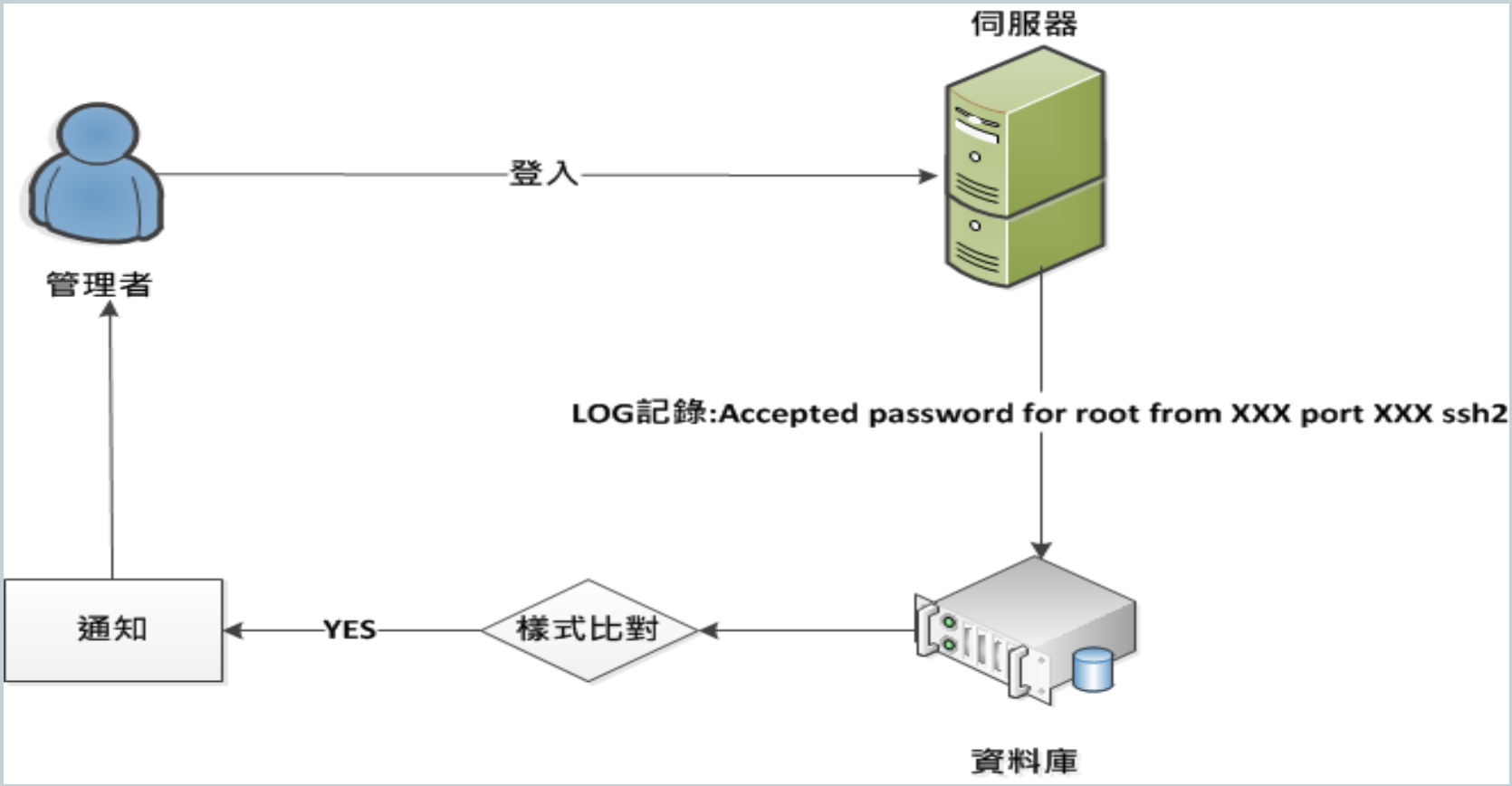
系統架構


主機伺服器
Rsyslog
SYSLOG
FIFO
MYSQL資料庫
SAGAN
Sagan Rule
Match??
YES
UNIFILED2
MYSQL資料庫
檔案

LOG

- 我想要
  - 有人登入系統時能即時告知
  - 有人不斷的在TRY我的系統能即時告知
  - …….

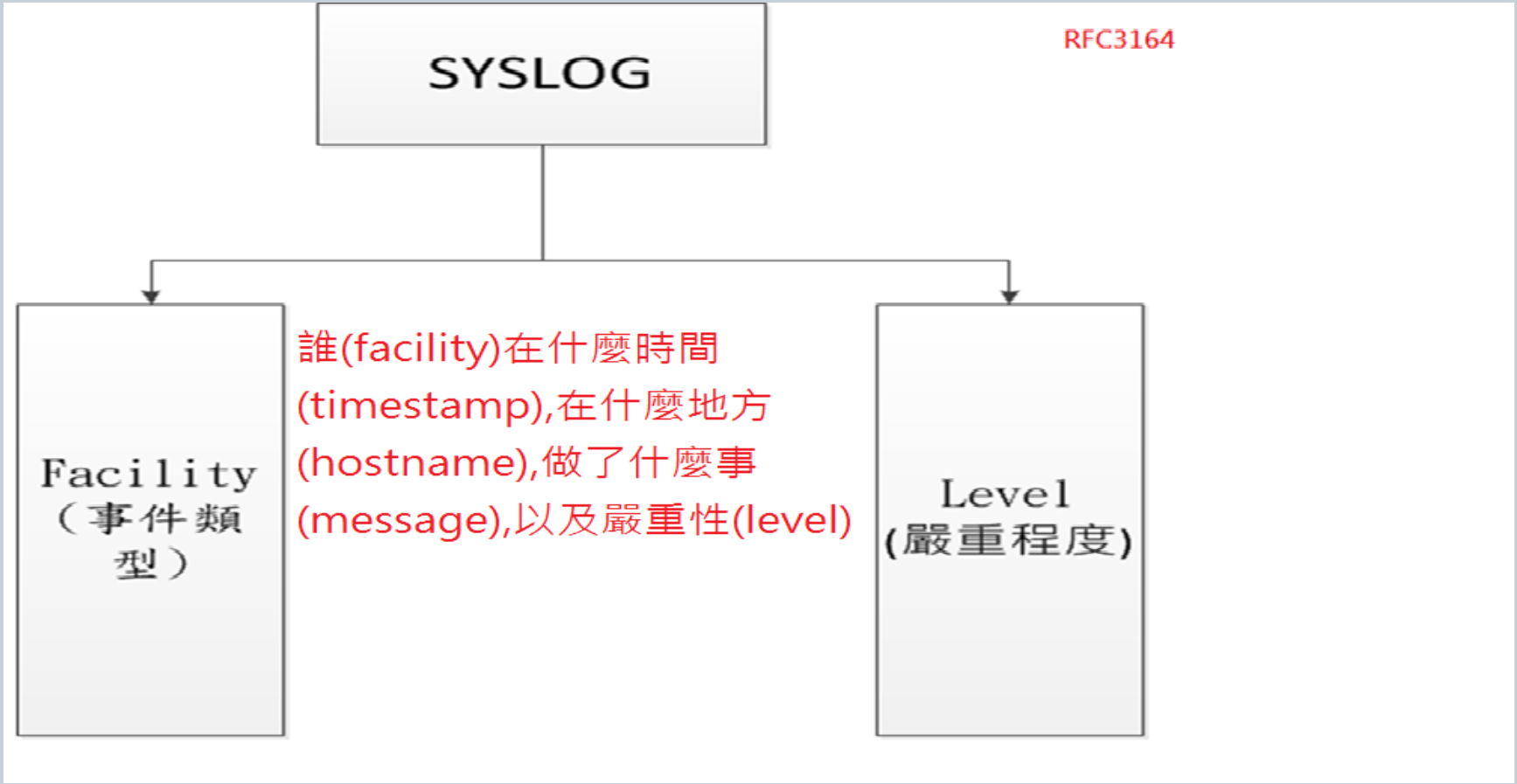
LOG


伺服器
登入
管理者
LOG記錄:Accepted password for root from XXX port XXX ssh2
通知
YES
樣式比對
資料庫

syslog

- 傳遞記錄檔訊息的標準
- 主從式的架構
  - 中央控管式的LOG伺服器
- UDP／TCP PROTOCOL

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)

Facility(事件類型)

Numerical Code	Facility	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	cron	clock daemon
10	security	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock	clock daemon (note 2)
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

Priority(Level,嚴重性)

Numerical Code	Severity	Description
0	emerg	system is unusable
1	alert	action must be taken immediately
2	crit	critical conditions
3	error	error conditions
4	warning	warning conditions
5	notice	normal but significant condition
6	info	informational messages
7	debug	debug-level messages

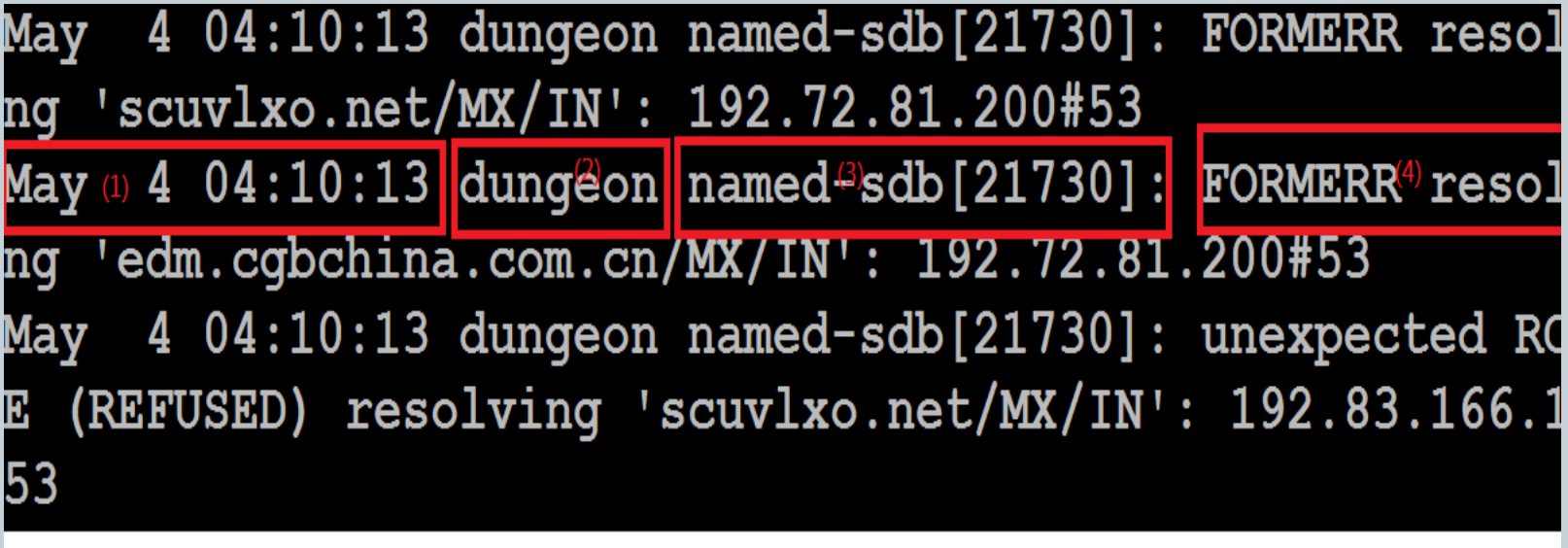
Facility

事件類型	說明
LOG_AUTH(LOG_AUTHPRIV)	與認證相關的事件(如login)均需記錄下來
LOG_CRON	例行性排程程式(如cron at)的事件均需記錄下來
LOG_DAEMON	記錄常駐程式相關事件的記錄
LOG_FTP	記錄與FTP程式相關事件的記錄
LOG_KERN	記錄核心(kernel)相關事件所發生的相關記錄
LOG_LPR	記錄列印(printer)相關事件所發生的相關記錄
LOG_MAIL	記錄與郵件收發相關事件所發生的相關記錄
LOG_NEWS	記錄與新聞群組相關事件所發生的相關記錄
LOG_SYSLOG	記錄與系統相關事件所發生的相關記錄
LOG_LOCAL0~ LOG_LOCAL7	保留給使用者使用

LEVEL()

嚴重程度	說明
LOG_INFO	僅是一些基本的資訊說明，無任何的嚴重性
LOG_NOTICE	系統還是正常，但有發生了一些需要注意的資訊
LOG_WARNING	系統發生了一些警示訊息，但還不至於影響相關常駐程式(daemon)的運作
LOG_ERR	系統發生了重大的錯誤訊息，這些訊息通常是用來說明常駐程式(daemon)無法啟動的原因
LOG_CRIT	系統發生了比重大錯誤（error）還要嚴重的錯誤訊息，通常這已到達系統臨界點 (critical)
LOG_ALERT	系統發生了嚴重錯誤的資訊
LOG_EMERG	這是最嚴重的等級，通常發生此類錯誤，是指系統已經發生了幾乎當機的情況

syslog format



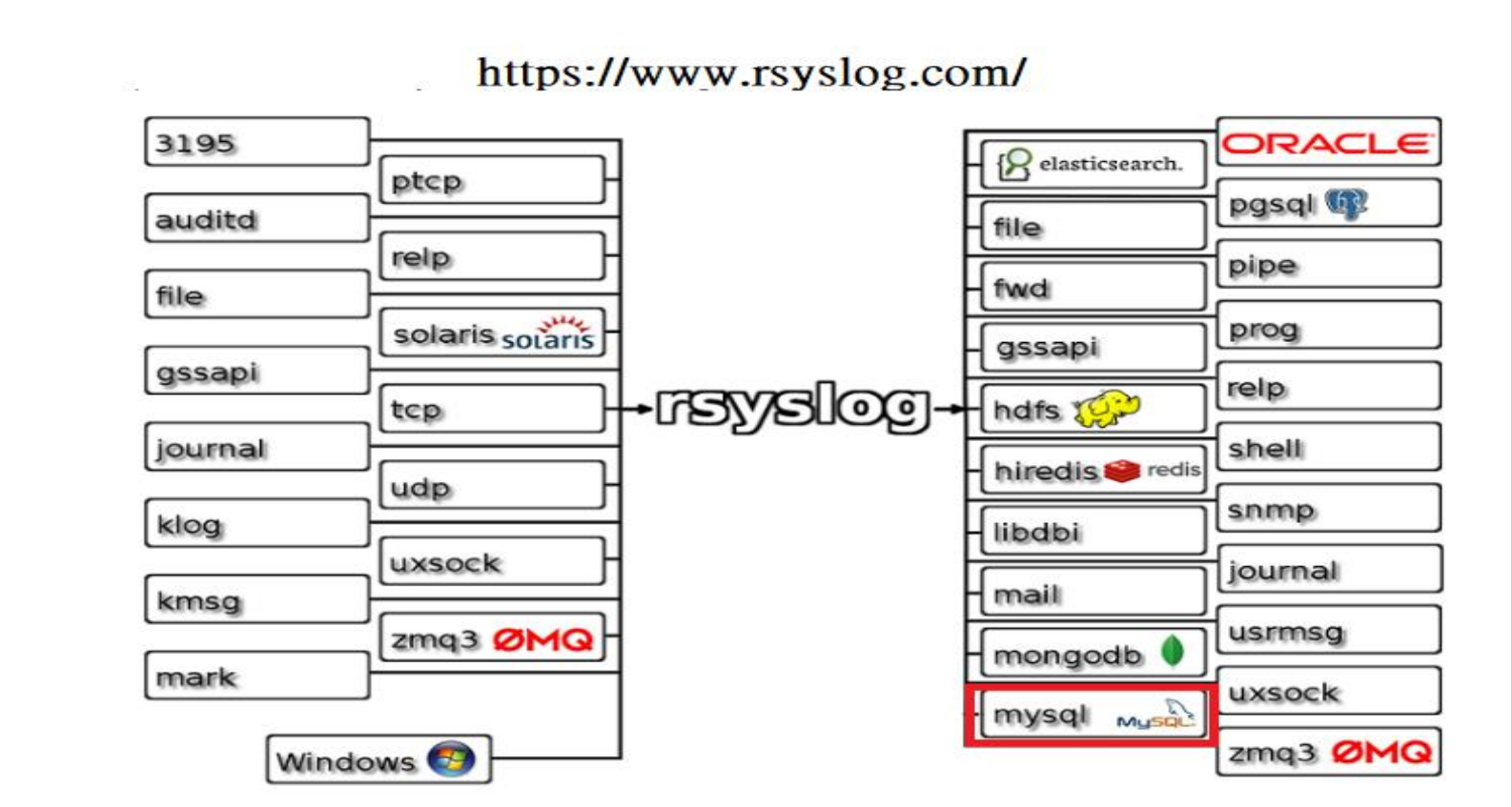
(1)發生時間 (2)主機名稱 (3)程式名稱 (4)訊息

cat /var/log/secure | more

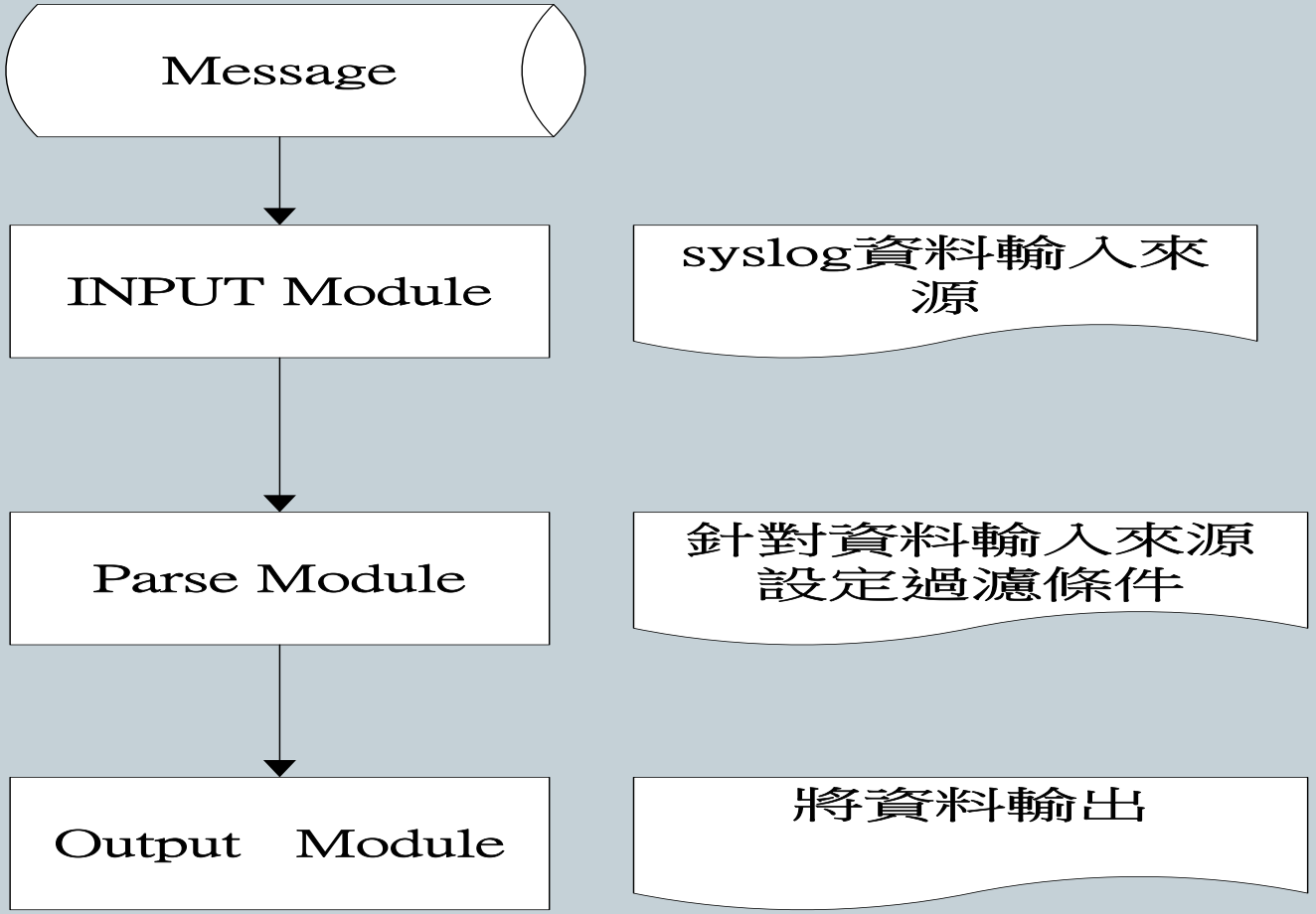
常見的syslog檔案

檔名	說明
/var/log/messages	儲存系統上比較通用的訊息
/var/log/maillog	郵件伺服器的相關記錄
/var/log/secure	系統安全的相關資訊
/var/log/cron	儲存cron常駐程式所產生的資訊，cron是一種定時執行的程式

rsyslog


https://www.rsyslog.com/
3195
auditd
file
gssapi
journal
klog
kmsg
mark
Windows
ptcp
relp
solaris
tcp
udp
uxsock
zmq3
rsyslog
elasticsearch.
file
fwd
gssapi
hdfs
hiredis
redis
libdbi
mail
mongodb
mysql
ORACLE
pgsql
pipe
prog
relp
shell
snmp
journal
usrmsg
uxsock
zmq3

rsyslog架構


Message
INPUT Module
syslog資料輸入來源
Parse Module
針對資料輸入來源設定過濾條件
Output Module
將資料輸出

Input module

模組類型	模組名稱	模組說明
INPUT	imuxsock	接收系統所產生的 log 記錄，這是預設系統所使用的，在本解決方案中，也將使用此模組來當成 INPUT 模組
	imudp.	利用 UDP 通訊協定取得 LOG 記錄，通常用來接收遠端傳來的 syslog 資訊，提供的選項如下 $UDPServerRun ＜埠號(514)＞ 設定以埠 514 為預設接收遠端傳來的 syslog 資訊

Output module

Output Modules

Output modules process messages. With them, message formats can be transformed and messages be transmitted to various different targets. They are generally defined via action configuration objects.

- omamqp1: AMQP 1.0 Messaging Output Module
- omelasticsearch: Elasticsearch Output Module
- omfile: File Output Module
- omfwd: syslog Forwarding Output Module
- omhdfs: Hadoop Filesystem Output Module
- omhiredis: Redis Output Module
- omhttpfs: Hadoop HTTPFS Output Module
- omjournal: Systemd Journal Output
- omkafka: write to Apache Kafka
- omlibdbi: Generic Database Output Module
- ommail: Mail Output Module
- ommongodb: MongoDB Output Module
- ommysql: MySQL Database Output Module
- omoracle: Oracle Database Output Module
- PostgreSQL Database Output Module (ompgsql)
- ompipe: Pipe Output Module
- omprog: Program integration Output module
- omrelp: RELP Output Module
- omruleset: ruleset output/including module
- omsnmp: SNMP Trap Output Module
- omstdout: stdout output module (testbench tool)
- omudpspoof: UDP spoofing output module
- omusrmsg: notify users
- omuxsock: Unix sockets Output Module
- GuardTime Log Signature Provider (gt)
- Keyless Signature Infrastructure Provider (ksi)
- KSI Signature Provider (rsyslog-ksi-ls12)

properties

名稱	說明
%FROMHOST%	主機名稱
%fromhost-ip%	主機IP (Local inputs (imklog)為 127.0.0.1)
%programname%	程式名稱
%syslogfacility%	facility
%syslogpriority%	priority

REF:https://www.rsyslog.com/doc/v8-stable/configuration/properties.html

rsyslog組態設定

```
$ModLoad imuxsock.so
$ModLoad ommysql.so
```

INPUT

```
*.*        /var/log/messages
```

OUTPUT

類型.嚴重性　　儲存的檔案名稱

```
*.* :ommysql:<DBHOST>,<DBNAME>,<DBUSER>,<DBPWD>
```

輸出至資料庫

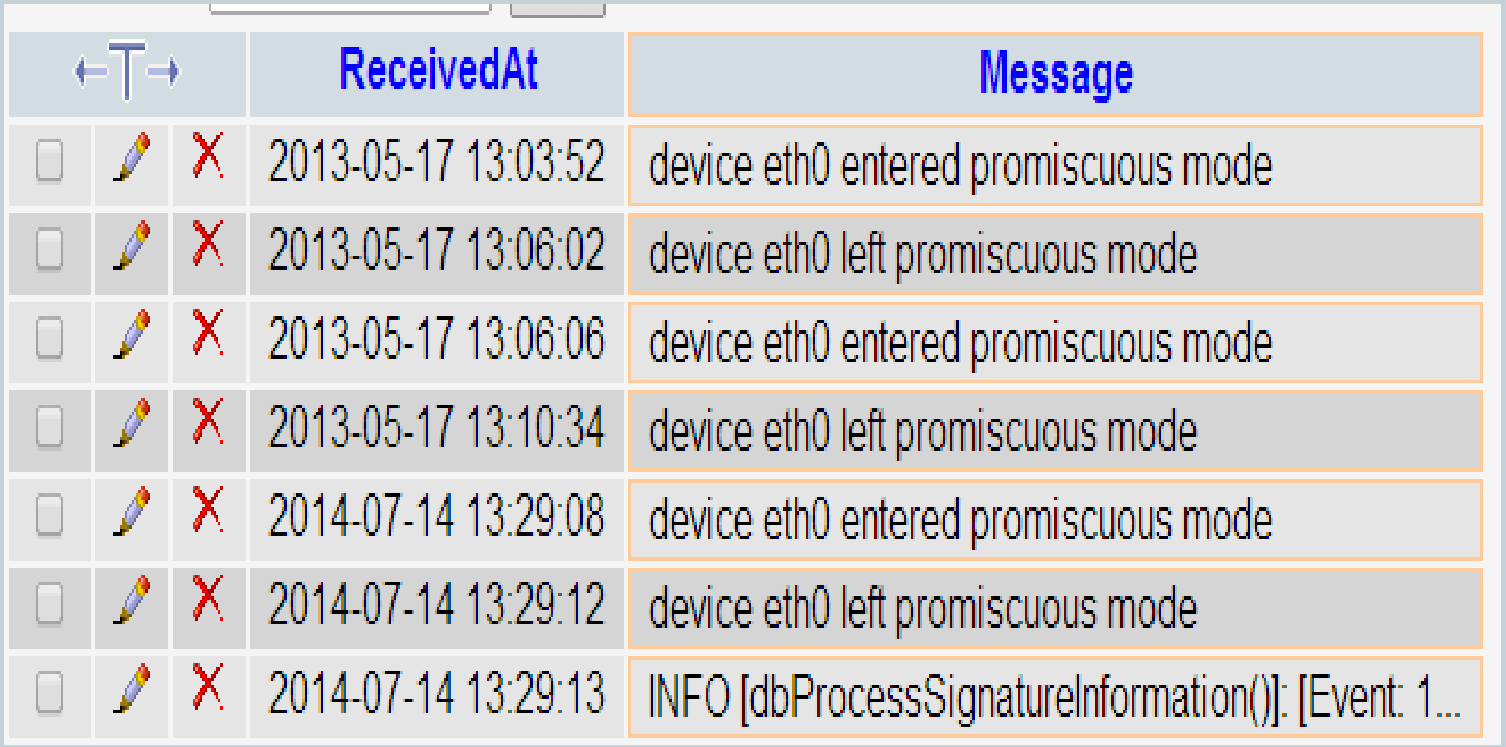
SYSLOG樣式-ssh brute force

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...

SYSLOG樣式-email

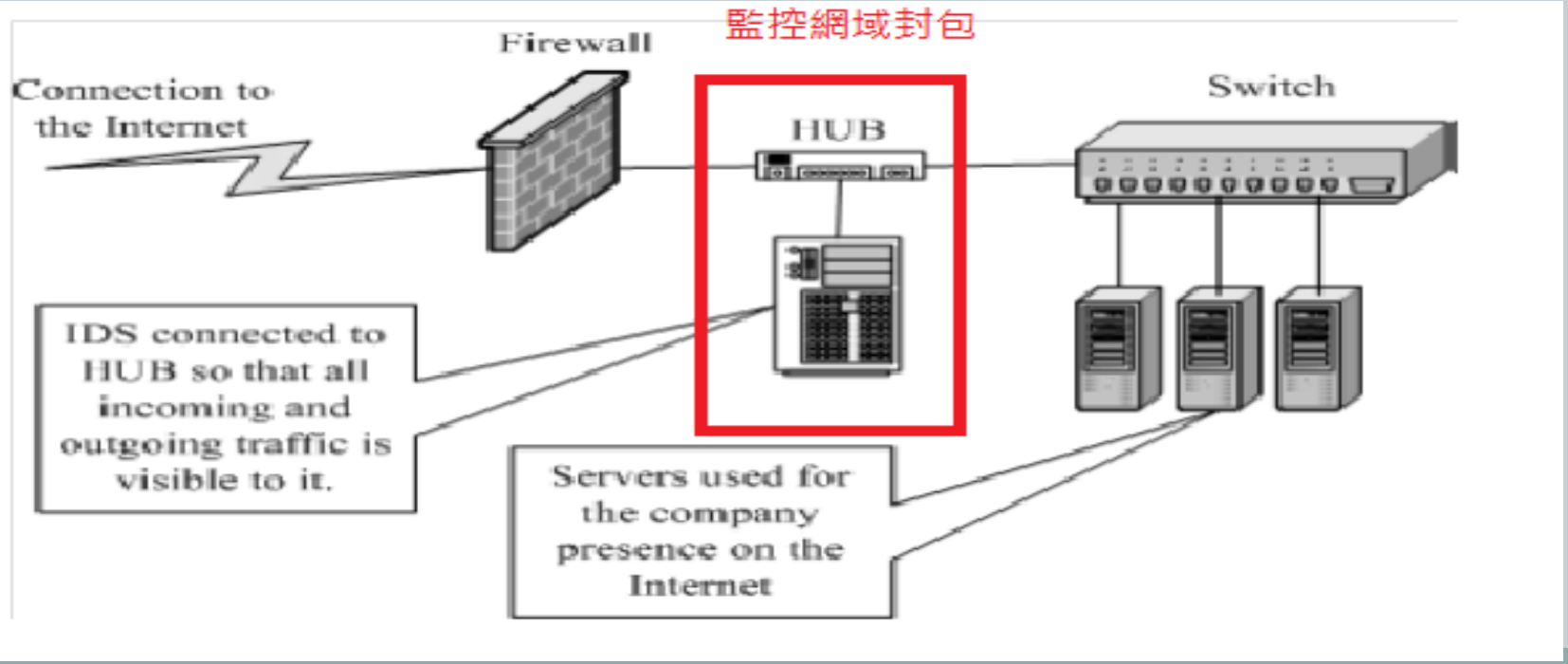
ReceivedAt	messageID	Message
2014-07-10 13:00:05	952D386D80DB	client=unknown[140.117.101.6]
2014-07-10 13:00:05	952D386D80DB:	to=<...tw>, relay=mg.moe...
2014-07-10 13:00:05	952D386D80DB:	to=<...>, relay...
2014-07-10 13:00:05	952D386D80DB:	to=<...>, re...
2014-07-10 13:00:05	952D386D80DB:	to=<...>, relay=...
2014-07-10 13:00:05	952D386D80DB:	to=<...>, re...
2014-07-10 13:00:05	952D386D80DB:	from=<service@cert.tanet.edu.tw>, s...
2014-07-10 13:00:05	952D386D80DB:	message-id=<20140710050005.952D386D...
2014-07-10 13:00:06	952D386D80DB:	to=<...>, orig_t...
2014-07-10 13:00:06	952D386D80DB:	to=<...>, or...
2014-07-10 13:00:07	952D386D80DB:	to=<...>, ori...
2014-07-10 13:00:08	952D386D80DB:	to=<...>, relay=gmail...
2014-07-10 13:00:08	952D386D80DB:	to=<...>, relay=g...
2014-07-10 13:00:08	952D386D80DB:	to=<...>, rela...
2014-07-10 13:00:11	952D386D80DB:	to=<...>, relay=...
2014-07-10 13:00:11	952D386D80DB:	to=<...>, relay=sp...
2014-07-10 13:02:05	952D386D80DB:	to=<...>, relay=none, ...
2014-07-10 13:02:05	952D386D80DB:	to=<...>, relay=none, ...
2014-07-10 13:02:06	952D386D80DB:	to=<...>, relay=none...
2014-07-10 13:27:11	952D386D80DB:	from=<service@cert.tanet.edu.tw>, s...
2014-07-10 13:27:11	952D386D80DB:	to=<...>, relay=mail02...
2014-07-10 13:27:11	952D386D80DB:	to=<...>, relay=mail02...
2014-07-10 13:27:11	952D386D80DB:	to=<...>, relay=mail...
2014-07-10 13:27:11	952D386D80DB:	removed

SYSLOG樣式-cron

ReceivedAt	Message
2012-12-24 17:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 18:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 19:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 20:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 21:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 22:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-24 23:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 00:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 01:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 02:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 03:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 04:01:01	(root) CMD (run-parts /etc/cron.hourly)
2012-12-25 04:02:01	(root) CMD (run-parts /etc/cron.daily)

入侵偵測系統(IDS)

- 網路型入侵偵測系統(NIDS)
  - 以snort 為代表
  - 以系統無關，部署在網域中
  - 誤判率較高



入侵偵測系統(IDS)

- 主機型入侵偵測系統(HIDS)
  - Sagan (https://quadrantsec.com/sagan_log_analysis_engine/)
    - HIDS
    - 以監控系統syslog方式判別主機事件
    - 規則(rule)與snort規則設定相同

Sagan-組態說明

- var FIFO /var/run/sagan2.fifo
  - 設定FIFO檔案位置
- var SAGANLOGPATH /var/log/sagan
  - 設定偵測到符合rule所記錄的資訊
- var RULE_PATH /usr/local/sagan/rules
  - 設定放置RULE檔案的目錄位置
- sagan_host 主機IP
  - 設定放置sagan主機運作的ip資訊

Sagan-rule

(1) (2) (3)

alert syslog $EXTERNAL_NET any -> $HOME_NET any (msg:"[OPENSSH] login information"; content: "Accepted password";) (4)

Sagan-rule-(1)

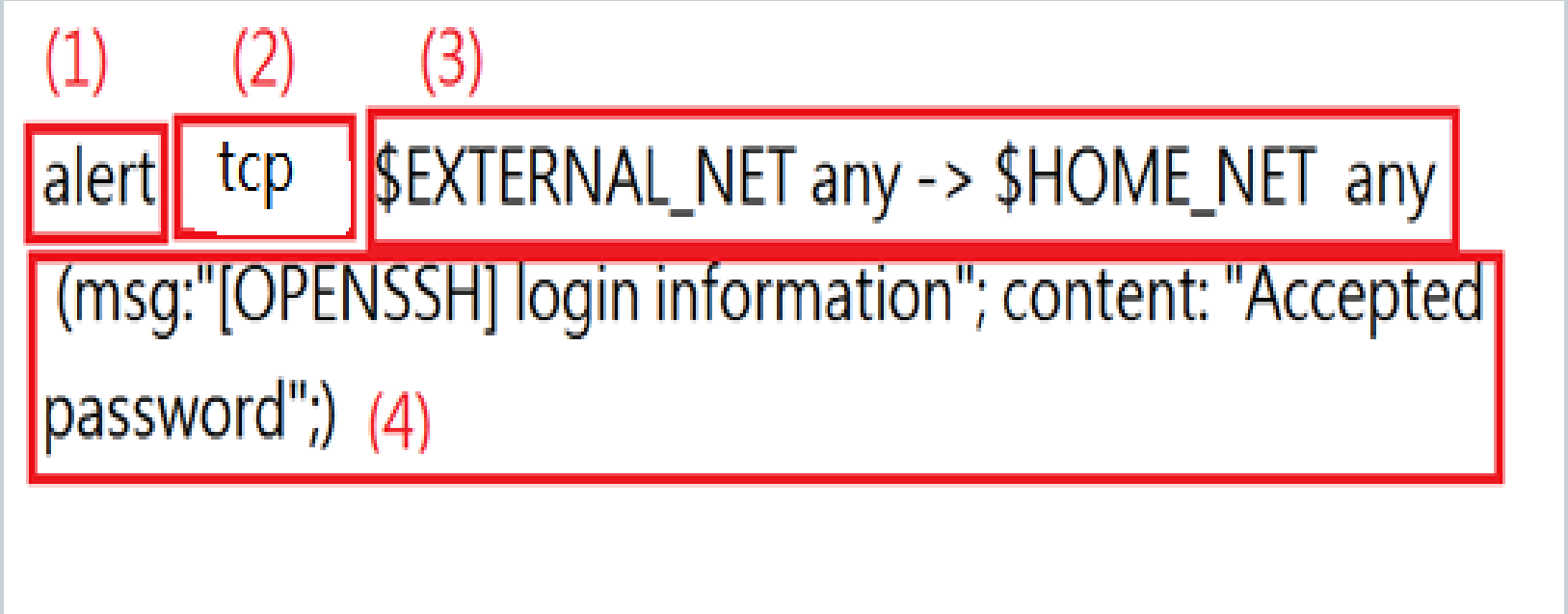
- action
  符合條件時的動作
  - alert:發出警告訊息
  - drop:記錄

(1) (2) (3)

```
alert syslog $EXTERNAL_NET any -> $HOME_NET  any
 (msg:"[OPENSSH] login information"; content: "Accepted
password";) (4)
```

Sagan-rule-(2)

- 通訊協定 (Sagan 1.1.6 之後採用any)
  - any tcp udp icmp



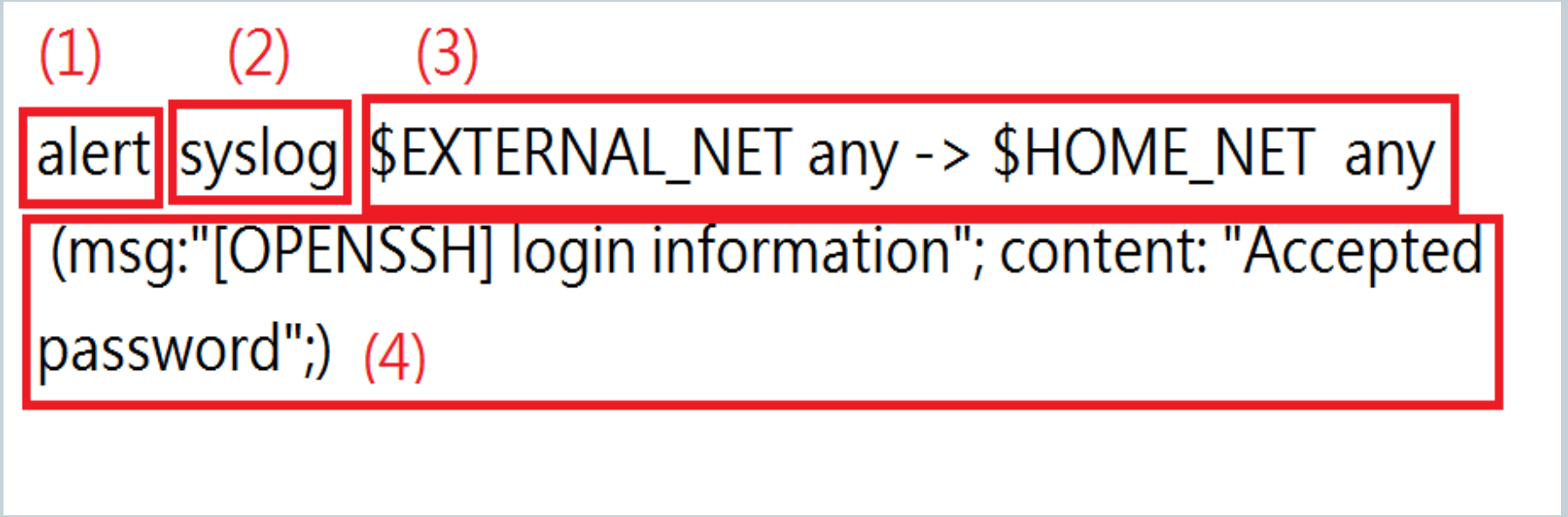
Sagan-rule-(3)

- external_net sport=>home_net dport
  - external_net:外部來源IP (any)
  - sport:外部來源的通訊埠 (any)
  - home_net:目地IP
  - dport:目地IP的通訊埠

```
(1)     (2)     (3)
alert syslog $EXTERNAL_NET any -> $HOME_NET  any
 (msg:"[OPENSSH] login information"; content: "Accepted
password";) (4)
```

Sagan-rule-(4)

- 規則細項
  - msg:設定訊息字串
  - content:設定查詢條件字串



Sagan-rule-(4)

- 規則細項
  - classtype:定義rule所屬的類別
  - facility:設定僅解析所設定的facility種類的log
    ex:facility: daemon
  - level:設定僅解析所設定level種類的log
  - program:設定僅解析某個程式所產生的syslog
  - nocase:不分大小寫的查詢
  - sid:signatures 編號
  - content: “search” 搜尋字串
  - threshold: type limit, track by_src, count 5, seconds 300
    (設定門檻值,個別IP在300秒內觸發5次以上)

Sagan-rule-example

```
alert syslog $EXTERNAL_NET any -> $HOME_NET any (msg:
    "[SYSLOG] Kernel log daemon terminating";
     content: "kernel log daemon terminating"; nocase;
     classtype: program-error;
reference:url,wiki.quadrantsec.com/bin/view/Main/5000126; sid:
    5000126; facility: kern; rev:1;)
```

alert.log(輸出)

```
[**] [1:5000022] [OPENSSH] Invalid or illegal user [Brute Force] [10/1] [**]
[Classification: attempted-user] [Priority: 1] [127.0.0.1]
[Alert Time: 10-09-2018 09:52:57.285208]
2018-10-09 09:52:57 199.195.250.21:53696 -> 192.168.2.1:22 authpriv info
Message: Invalid user usuario from 199.195.250.21 port 53696
[Xref => http://wiki.quadrantsec.com/bin/view/Main/5000022]
```

暴力攻擊

本機

```
openssh.rules:alert any $EXTERNAL_NET any -> $HOME_NET any (msg:"[OPENSSH] Inval
id or illegal user [Brute Force] [10/1]"; pcre: "/invalid user|illegal user/i";
content:!"input_userauth_request"; xbits: set,brute_force,21600; default_proto:
tcp; default_dst_port: $SSH_PORT; classtype: attempted-user; program: sshd; norm
alize; parse_src_ip: 1; parse_port; after: track by_src, count 10, seconds 300;
threshold:type limit, track by_src, count 1, seconds 300; reference: url,wiki.qu
adrantsec.com/bin/view/Main/5000022; sid: 5000022; rev:17;)
```

RULE

~ The end~

感謝您的聆聽