FILE DI LOG: IMPORTANZA ED ANALISI (base)

Yvette (vodka) Agostini - vodka@s0ftpj.org

CNR MILANO – 4 novembre 2003

Copyright

Introduzione

- cosa sono?
- perchè servono?
- dove vado a cercarli?
- come li gestisco?
- come li interpreto?

FILE DI LOG: cosa sono?

Sono informazioni diagnostiche che il sistema ci rende disponibili in diversa misura a seconda del livello di controllo impostato

- l'hardware tramite il kernel
- i demoni (sshd, telnetd, inetd, ecc...)
- gli applicativi (mysql, ...)
- gli utenti

FILE DI LOG: esempi (1)

Esempi di log generati dall'hardware:

Jun 4 18:09:43 dhcpclient1 kernel: ide0: BM-DMA at 0xf000-0xf007, BIOS settings: hda:pio hdb:pio

Jun 6 14:45:53 dhcpclient1 kernel: eth0 : Setting promiscuous mode

Esempi di log generati dagli utenti:

yagostini	pts/0	xxx-223.xxx.xxx	Thu Jun 6 15:56	still logged in
tvasta	pts/0	xxx-21.xx.xxx	Thu Jun 6 15:30 - 15:42	(00:12)

FILE DI LOG: esempi (2)

Esempi di log generati da demoni:

sendmail

Jun 2 04:02:03 xxxx sendmail[24976]: g52221tb024971: to=yagostini@xxx.it, ctladdr=<root@xxx.xxx.it> (0/0), delay=00:00:02, xdelay=00:00:01, mailer=esmtp, pri=270564, relay=mail.xxx.it. [xxx.xx.xxx.xx], dsn=2.0.0, stat=Sent (<200206020202.g52221OJ024969@mail.xxx.it> Queued mail for delivery)

Apache

xx.xxx.xx.xx - - [19/Dec/2001:16:22:33 +0100] "GET /apache_pb.gif HTTP/1.1" 200 2326

Cron

Jun 2 04:32:00 hostname CROND[29556]: (root) CMD (/usr/local/bin/CheckDefang.sh > /dev/null 2>&1)

FILE DI LOG: esempi (3)

Esempi di log generati da applicativi:

Un generico script di backup

Finished backup at Fri Apr 19 00:00:00 CEST 2002

Starting backup at Sat Apr 20 00:00:00 CEST 2002

Squirrelmail (webmail)

xxx.xx.xx.xxx - - [18/Feb/2002:15:07:30 +0100] "GET /squirrelmail/ HTTP/1.0" 302

0 "-" "Lynx/2.8.4rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6b"

FILE DI LOG: esempi “maliziosi”

Tracce (fingerprint) di attacchi e probe:

Apache error_log ATTACCO NIMDA

[Tue Jun 11 04:09:11 2002] [error] [client xxx.xx.xxx.x] File does not exist: /www/virtualhosts/www.nomesito.com/MSADC/root.exe
(error_log di apache che segnala un attacco NIMDA)

Sshd messages o custom MASS SCANNER

Jun 9 09:39:25 sshd[17060]: scanned from xxx.xx.xxx.xx with SSH-1.0-SSH_Version_Mapper. Don't panic.
(messages log file, evidenzia la signature di un version scanner per sshd)

FILE DI LOG: perchè servono? (1)

Ovvero, scene di vita quotidiana

Conoscere il comportamento in condizioni normali, lo stato "a regime" del sistema

=

capacita' di cogliere "a colpo d'occhio" eventuali anomalie

Questo principio vale sia in termini di sicurezza da attacchi esterni che in termini di garanzia del servizio.

Esempi pratici? Backup falliti, hardware che si usura e segnala nei log errori ricorrenti (tipico con i dischi), malconfigurazioni lievi di qualche servizio, ecc.

FILE DI LOG: perchè servono? (2)

Ovvero, prevenire è meglio che curare

RICONOSCERE TEMPESTIVAMENTE

UN PROBLEMA AUMENTA LE CHANCES

DI PREVENIRE DANNI

Nella peggiore delle ipotesi, almeno si è in possesso di dati preziosi per porre rimedio

FILE DI LOG: dove li trovo?

Di solito li trovate in /var/log

Alcuni possono essere in /var/adm/log

Potrebbero essere inviati a una macchina remota

Potrebbero essere "dirottati" su una tty

Potrebbero essere inviati a una stampante

Per togliersi ogni dubbio si guarda /etc/syslog.conf

FILE DI LOG: come li gestisco? (1)

syslogd e syslog.conf

- **syslogd** è un demone che consente di loggare in modi diversi tutti i messaggi:

    - di sistema
    - del kernel (tramite **klogd,** che raccoglie i messaggi dal kernel e li invia a syslogd)
    - dei demoni attivi

- il comportamento di syslogd è configurabile tramite il file **/etc/syslog.conf**

FILE DI LOG: come li gestisco? (2)

syslog.conf, facilty, severity, azioni

/etc/syslog.conf indica in sostanza a syslogd:

Cosa & **Dove** & **Come** loggare

La sintassi usata è:

Facility.severity **luogo (e/o azione)**

• 24 possibili facility (kern, user, mail, cron, local2, ecc..)

• 8 possibili severity (emerg, alert, crit, err, warn, notice, info, debug)

FILE DI LOG: come li gestisco? (3a)

Un esempio commentato

```
*.=info;*.=notice;*.=warning;
auth,authpriv.none;
cron,daemon.none;
mail,news.none          /var/log/messages
```

Tutti i messaggi con severity pari a:
info, notice e warning
Eccetto quelli provenienti da facilities:
auth,authpriv,cron,daemon,mail,news
Vanno nel file /var/log/messages
segue

FILE DI LOG: come li gestisco? (3b)

Un esempio commentato

```
*.alert                          *
```

Tutti i messaggi con severity > o = ad alert
Vanno a tutti gli utenti collegati

```
kern.!alert; \
*.=debug;*.=info;\
*.=notice;*.=warn                /dev/tty8
```

Tutti i messaggi con severity = debug, info, notice e warn

Tranne quelli provenienti da kern con severity > o = ad alert

vengono visualizzati su /dev/tty8

FILE DI LOG: come li gestisco? (3)

Ovvero, comunicare con syslogd

..volessi comunicare con syslogd?

• perl: modulo **sys::syslog**

• shell scripting: logger e’ un comando che consente di inviare messaggi a syslogd con facility.severity impostabili

• C: #include <syslog.h>

Man page e howto online sono esaurienti a sufficienza per compiti di ordinaria amministrazione

FILE DI LOG: come utilizzarli? (1)

On the fly

- Per verificare se e come hardware nuovo viene riconosciuto dal sistema
- Per controllare il funzionamento di un demone in seguito a modifiche
- Per controllare comportamenti “anomali

Il comando più comodo è: tail

FILE DI LOG: come utilizzarli? (2)

A cadenza

- Per controllare che non vi siano deviazioni ingiustificate dei parametri comportamentali del sistema
- Per eseguire statistiche sull'utilizzo dei servizi
- Per abitudine

I comandi più comodi sono: more, tail, grep

FILE DI LOG: come utilizzarli (3)
e non venirne sopraffatti

• possono essere molti e “ingombranti”

• fan venire il mal di testa per come sono “fitti” di informazioni

• non si “correlano” da soli

• si “accumulano”

Percio’.....strumenti di gestione e analisi!!!

FILE DI LOG: interpretazione (1)

- Buon senso
  - Esperienza
    - Pazienza
      - Curiosità

Se la configurazione di syslog.conf rispecchia le nostre esigenze, siamo già a buon punto.

Oltre a ciò:

grep, sed, perl, shell scripting agevolano l'interpretazione

FILE DI LOG: analizzarli (2)

- In ambienti complessi e/o a rischio e' necessario non solo analizzare, ma anche **correlare** i log di differenti macchine e servizi.
    - Raccolta centralizzata (consolidamento)
    - Uniformazione di log con formati differenti
        - firewall
        - differenti sistemi operativi
        - apparati di rete
        - Intrusion Detection System
        - antivirus, ecc

Necessita' di strumenti avanzati e complessi

Risorse per approfondire

Man page di: Syslogd, syslog.conf, tail, more, grep, logger:

BSD Syslog Protocol (RFC 3164):
http://www.ietf.org/rfc/rfc3164.txt

Tools di vario genere (anche per altri OS):

http://online.securityfocus.com/cgi-bin/sfonline/tools.pl?platid=-1&cat=2&offset=0

Active Security Monitoring and Containment with Cross Technology Correlation: The Next Generation in Computer Security Technology:
http://online.securityfocus.com/guest/10414

Log analysis resource by Tina Byrd:

http://www.counterpane.com/log-analysis.html

Log analysis mailing list:

http://lists.shmoo.com/mailman/listinfo/loganalysis

Ringraziamenti

Valerio [Hypo] Verde

amover@libero.it

s0ftpj.org

http://www.s0ftpj.org

Fabio (naif) Pietrosanti

http://fabio.pietrosanti.it

FILE DI LOG: IMPORTANZA ED ANALISI (base)

CNR MILANO – 4 novembre 2003

Contatti:

yvette.agostini@ieo-research.it

vodka@s0ftpj.org