LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Configurare

Prima sarcina care trebuie indeplinita pentru monitorizarea logurilor este identificare locatiei acestora. Fisierul de configurare syslog.conf stabileste locatia logurilor precum si cantitatea si tipul de mesaje salvate.

Fiecare rand din fisierul syslog.conf reprezinta o regula de logare si este formata dintr-un SELECTOR si o ACTIUNE. Selectorul si actiunea sunt separate de unul sau mai multe spatii sau tab. Randurile care incepe cu #(diez) reprezinta comentarii si sunt ignorate.

Exemplu:

```
# Log all the mail messages.
mail.info                       /var/log/maillog
```

Selectorul este mail.info, iar actiunea este /var/log/maillog

Un selector este format din 2 parti separate prin .(punct) si anume: facility si priority.

Facility reprezinta tipul de mesaj logat si poate fi: auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0, local1, local2, local3, local4, local4, local6 si local7.
*(asterix) inseamna orice facilitate.

Prioritatea reprezinta un cod care indica cantitatea de mesaje logate. In ordine crescatoare a prioritatii, dar in ordine descrescatoare a cantitatii de mesaje logate prioritatile sunt: debug, info, notice, warning, warn (echivalent cu warning), err, error (echivalent cu err), crit, alert, emerg, panic (echivalent cu emerg). Prioritatile error, warn si panic sunt considerate invechite si nu se recomanda a mai fi folosite.
*(asterix) inseamna orice prioritate.

In momentul specificarii unei prioritati pentru o facilitate, mesajele cu prioritate mai mare sunt de asemenea incluse.
Exemplu: auth.err include si auth.crit, autch.alert si auth.emerg

Pentru a selecta doar mesajele de o anumita prioritate si nu si pe cele cu prioritate mai mare se foloseste semnul =(egal).
Exemplu: auth.=err selecteaza doar mesajele cu prioritatea err nu si pe cele cu prioritatea crit, alert sau emerg.

Semnul !(semnul exclamarii) are rolul de a exclude mesajele de o anumite prioritate sau mai mare.
Exemplu: mail.!crit va exclude mesajele cu prioritate crit, alert sau emerg.

Pentru a exclude toate mesajele pentru o facilitate se foloseste prioritatea none. Exemplu: mail.none

Cealalta componenta pe langa SELECTOR a fiecarui rand din syslog.conf, ACTIUNEA, stabileste termenul generic si abstract numit logfile sau locatia catre care se redirecteaza logurile pentru o anumita facilitate si prioritate.

Un logfile poate fi:

a) fisier normal

Se specifica obligatoriu folosind calea absoluta.
Exemplu:

```
authpriv.*                      /var/log/secure
```

Fisierul poate fi precedat de semnul -(minus) caz in care acesta nu mai este sincronizat (salvat) dupa fiecare mesaj logat ci numai dupa ce mai multe mesaje sunt salvate intr-un buffer. Avantajul este cresterea performante, iar dezavantajul este pierderea de informatie in cazul unui crash.
Exemplu:

```
authpriv.*                      -/var/log/secure
```

b) user
Mesaje de tip log pot fi redirectate la consola/terminalul la care userul este logat. Daca se doreste trimiterea mesajelor catre mai multi useri acestia se separa cu virgula.
Exemplu:

```
kern.crit               root,admin
```

c) remote host
In cazul unei retele in care se gasesc mai multe servere sau echipamente ale caror loguri trebuie urmarite este mai eficient ca acestea sa fie redirectate catre un host remote. In acest mod avem un loc centralizat de logare.

Nota

In cazul compromiterii unui server sau a intregului sistemul una dintre primele activitati ale Crackerului este "sa-si stearga urmele" adica sa stearga logurile referitoare la activitata sa pentru a nu putea fi descoperit de admin. Logarea pe un sistem remote rezolva aceasta problema fiindca stergerea logurilor de catre cracker presupune compromiterea inclusiv a serverului pe care se logheaza.

Pentru logarea remote se foloseste semnul @ in fata actiunii.
Exemplu: `authpriv.alert @192.168.0.15`

d) named pipe
Logurile pot fi redirectate inclusiv catre fisiere speciale numite named pipes care anterior trebuie create folosind comanda mkfifo.
Exemplu: `kern.=debug |/usr/adm/debug`

Important

Dupa fiecare modificare a fisierului /etc/syslog.conf sau /etc/rsyslog.conf in functie de versiune, daemonul syslogd sau rsyslogd trebure restartat. Exemplu: /etc/init.d/rsyslog restart

Fisiere standard in care se pastreaza logurile:

- /var/log/messages - reprezinta fisierul principal cu loguri al sistemului in care se salveaza informatii de la majoritatea serverelor
- /var/log/wtmp - reprezinta un fisier binar care pastreaza informatii despre logarile in sistem;
- /var/log/boot.log - pastreaza informatii despre procesul de butare;
- /var/log/secure - pastreaza informatii despre actiuni legate de securitate (logare prin ssh, comanda su etc);
- /var/log/cron - pastreaza informatii despre cron daemon;
- /var/log/dmesg - pastreaza informatii despre kernel si hardware;

Exemplu syslog.conf:

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                  -/var/log/maillog

# Log cron stuff
cron.*                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                 *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                /var/log/boot.log
```

Resurse

- syslog.conf
- Syslog Forums
- Troubleshooting with syslog

Syslog

Durata: 4.52 min
Marime: 2.26MB