rsyslogd

/etc/rsyslog.conf

Els fitxers de configuració del servei de resgitres del sistema tenen el següent format:

```
facility.priority    action
```

on:

- Facility: identifica el tipus d'eina que genera el missatge de log. els diferents valors són:
  - kern (0): utilitzat pel nucli quan genera missatges
  - user (1): reservat per aplicacions d'usuari del sistema per a missatges a mida
  - mail (2): utilitzat per servidors de correu i eines de processat de correu
  - daemon (3): és una mena de calaix de sastre. Tots els serveis que no utilitzen cap altra facility generen missatges amb aquesta
  - auth (4): utilitzat per les aplicacions que gestionen les autoritzacions del sistema (PAM, login, sudo, ...). En distribucions utilitzen authpriv
  - syslog (5): missatges generats de forma interna per syslog
  - authpriv (10): utilitzat per les aplicacions que gestionen les autoritzacions del sistema (PAM, login, sudo, ...). En distribucions antigues també existeix auth o security
  - cron (15): utilitzat per eines de gestió de tasques programades (com cron o anacron)
  - local0-7 (16-23): reservat per usos específics
- Priority: indica la importància del missatge. Els valors possibles són:
  - debug: mostra la màxima informació possible. Útil per provar aplicacions però no recomanable en sistemes en producció
  - info: missatges d'informació
  - notice: missatges que no són errors però que s'haurien de tenir en compte
  - warning: avisos importants que no són errors però que poden tenir certa repercusió en el sistema
  - error: missatges d'error
  - crit: missatges d'error importants, com errors de maquinari
  - alert: missatges d'errors crítics que han de ser solucionats inmediatament
  - emerg: missatges molts greus que comporten que la màquina deixarà de funcionar inmediatament (si no ho ha fet ja)
- action: permet descriure l'acció a realitzar amb el missatge generat
  - /path/to/file: envia el missatge al fitxer indicat
  - @server: envia els missatges a un equip remot
  - |/dev/xconsole: envia el missatge a una consola que estigui oberta
  - /dev/ttyX: envia el missatge a una tty indicada
  - [USER1],[USER2]: envia els missatges als usuaris especificats que tinguin una sessió iniciada
  - *: envia els missatges a tots els usuaris que tinguin una sessió iniciada

Si estem enviant els esdeveniments a un fitxer, podem trobar-nos una configuració com la següent:

```
kern.*   -/var/log/kern.log
```

Aquest símbol "-" davant de la ruta del fitxer de log indica que no es faci una crida a la funció fsync(), encarregada de fer un volcat del kernel buffer en aquell precís moment i de generar un registre

commit en el fitxer de journal per a cada operació d'escriptura. Això permet alliberar al sistema d'una càrrega excessiva de transaccions en el journal quan es tracta de logs amb gran activitat.

Servidor de logs

Els esdeveniments generats per les aplicacions es poden enviar a un equip remot (amb la opció @SERVER dins de /etc/rsyslog.cong). Per tal que aquest equip "SERVER" accepti els missatges s'han de fer algunes modificacions en el seu fitxer /et/rsyslog.conf. S'ha de permetre l'enviament dels missatges a través del port 514 definit per rsyslog:

```
# vi /etc/rsyslog.conf
...
# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
...
```

Això el que fa (després de reiniciar el servei) és obrir connexions als ports indicats:

```
$ netstat -punta4 | grep 514
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
2781/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*
2781/rsyslogd
```

També s'han de crear els templates que es vulguin per guardar els diferents registres. Per exemple:

```
# vi /etc/rsyslog.conf
...
$template clientAuth, "/var/log/rsyslog/%HOSTNAME%/auth.log"
$template clientLog, "/var/log/rsyslog/%HOSTNAME%/syslog"

authpriv.*                                      ?clientAuth
*.info,mail.none,authpriv.none,cron.none    ?clientLog
...
```

Una vegada creat el directori /var/log/rsyslog i reiniciat el servei el nostre servidor rebrà els missatges de logs de les màquines remotes

```
$ ls /var/log/rsyslog/*
/var/log/rsyslog/client1:
auth.log  syslog

/var/log/rsyslog/client2:
auth.log  syslog
```

```
/var/log/rsyslog/localhost:
auth.log  syslog
```