Monitorización del sistema

Joaquín Seoane Pascual
joaquin@dit.upm.es

Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid

5 de noviembre de 2001

Índice General

Registro de eventos

- Muchos servicios registran sus eventos significativos .
- A veces se puede especificar nivel de verbosidad.
- A veces se hace en ficheros o `stderr`.
- Los registros deberían ir a `/var/log`.
- Conviene clasificar los eventos según prioridad y especificar distintas acciones para ellos.
- Suele usarse `syslog`.
- Los ficheros crecen indefinidamente.

syslogd

- Configurable (`/etc/syslog.conf`).
- *Facilidades* predefinidas: `auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, syslog, user, uucp, local0..local7`.
- *Importancias* predefinidas: `emerg, alert, crit, err, warning, notice, info, debug`.
- Registro en: fichero, terminal de usuario, todos los terminales, fifo, red.
- Depurable con (`logger -p facilidad.importancia mensaje`)
- `klogd` se ocupa de los mensajes del núcleo.

Ejemplos en `syslog.conf`

```
auth,authpriv.*              /var/log/auth.log
kern.*                       -/var/log/kern.log
mail.info                    -/var/log/mail.info
mail.warn                    -/var/log/mail.warn
mail.err                     /var/log/mail.err
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none      -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none           -/var/log/messages
*.emerg                      *
*.emerg                      @loghost
```

Rotación de registros

- Evitar que llenen el disco.
- Guardar copia de los viejos comprimidos.
- Rotación diaria, semanal, mensual.
- Deben forzarse cieros permisos.
- A veces hay que hacer algo con los responsables (señal SIGHUP).
- Programas de ayuda `savelog, logrotate, ...`

Acciones periódicas

- Acciones con determinada periodicidad (programable).
- Programas `cron` (máquinas siempre encendidas) o `anacron` (estaciones).
- `cron`:
  - Configuración global: `/etc/crontab`
  - Configuraciones personales: `/var/spool/cron/crontabs`
- Generalmente se disciplinan e independizan las tareas periódicas:
  - `/etc/cron.daily/*`
  - `/etc/cron.monthly/*`
  - `/etc/cron.weekly/*`
- Para ajustes más finos, separados por paquetes: `/etc/cron.d/`

Ejemplo de /etc/crontab

```
SHELL=/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user command
05 13 * * * root test -e /usr/sbin/anacron || \
                          run-parts --report /etc/cron.daily

27 13 * * 7 root test -e /usr/sbin/anacron || \
                          run-parts --report /etc/cron.weekly

32 13 1 * * root test -e /usr/sbin/anacron || \
                          run-parts --report /etc/cron.monthly
```