

logs

gestión de logs

- [rsyslogd](#)
- [loganalyzer](#)
- [logstatsh](#)

usuario

para ver el contenido de estos ficheros (binarios) se puede usar utmpdump

- `/var/log/wtmp` → últimos accesos al sistema → `$ last (-i para ver IP en lugar de host) (-f fichero de otro sistema)`
- `/var/log/btmp` → últimos accesos fallidos al sistema → `$ lastb`

resumen syslog

- syslogd como demonio de gestión de logs
- `/etc/syslog.conf`
- cosas que se pueden logear:
 - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7
- eventos
 - ??
- ejemplos:
 - `*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages`
 - logear de todos, los eventos **info** excepto de aquellos que están marcados con **.none**
 - `authpri.* /var/log/secure`
 - logear todos los eventos de **authpriv**

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:log:start?rev=1479172033>

Last update: **14/11/2016 17:07**

