# REGISTROS DEL SISTEMA – LOGS



Mantener un registro de lo que sucede en el sistema es de vital importancia para conocer y optimizar su funcionamiento, así como para solucionar posibles problemas en el mismo. Las dos maneras más populares de gestionar estos registros son:

- **rsyslog** es un gestor tradicional gestiona diversos ficheros en texto plano.
- **systemd-journald** mantiene un registro más sofisticado y seguro, pero menos abierto a otros programas.

Otros programas más antiguos eran syslog y syslog-ng, que tenían un funcionamiento parecido a rsyslog.

El sistema suele guardar los registros en `/var/log/` donde puede haber a su vez diversos subdirectorios según sea necesario

## rsyslog

Tiene su fichero de configuración en `/etc/rsyslog.conf` o en ficheros dentro de `/etc/rsyslog.d/` . Sus lineas principales seleccionan el tipo de mensaje y le indican dónde se tiene que guardar. El selector de mensajes consta de dos partes `facility.priority`

**facility** (el origen de los mensajes) puede tomar los siguientes valores:

- `auth`
- `authpriv`
- `cron`
- `daemon`
- `ftp`
- `kern`
- `lpr`
- `mail`
- `makr`
- `news`
- `security`
- `syslog`
- `user`
- `uucp`
- `local0` to `local7`

**priority** puede tomar los siguientes valores:

- `debug`
- `info`
- `notice`
- `warning (or warn)`
- `err (or error)`
- `crit`
- `alert`
- `emerg (or panic)`

# REGISTROS DEL SISTEMA - LOGS

| Selector | Description |
|---|---|
| *.* | Todos los mensajes |
| *.info | Todos mensajes de info |
| kern.* | Todos los mensajes del kernel |
| mail.err | Los mensajes de error del correo |
| cron,lpr.warn | Los warning de cron y de lpr |
| cron.err;cron.!alert | Los errores de cron, pero NO las alertas |
| mail.=err | Solo los errores de mail |
| *.info;mail.none;lpr.none | Todos los mensajes de info excepto los de mail y lpr |

**logger** es un comando que sirve para insertar lineas en los ficheros de logs. La opción más importante es la `-p`, en la que indicamos la `facilidad.prioridad` del mensaje (si no se indica sería `user.notice`). Con `-t` insertaríamos una etiqueta en el mensaje. Se guardará antes de los dos puntos que separan al mensaje en si

```
logger "hola mundo"
```

```
logger -p user.warning -t misavisos "ha ocurrido algo raro"
```

**logrotate** se utiliza para "rotar" los ficheros de log. Es decir, para aplicar unas determinadas políticas según vaya pasando el tiempo: borrarlos, comprimirlos, moverlos, ...

Su fichero de configuración es `/etc/logrotate.conf` o los que se encuentren en el directorio `/etc/logrotate.d/`

## Ejemplo de fichero de configuración

```
{
   rotate 7
   daily
   missingok
   notifempty
   delaycompress
   compress
   size 50M
   postrotate
      invoke-rc.d rsyslog rotate > /dev/null
   endscript
}
```

NÚMERO DE ROTACIONES

FRECUENCIA

NO PRODUCIRÁ ERROR SI EL FICHERO NO EXISTE

NO ROTAR SI ESTÁ VACÍO

NO COMPRIME LA ULTIMA ROTACIÓN, PERO SÍ LA ANTERIOR

COMPRIMIR LOG ROTADO (GZIP)

TAMAÑO MÁXIMO DEL FICHERO DE LOG

LANZAR ORDENES DESPUÉS DE ROTAR

## Comandos para revisar logs de texto

- `tail`
- `tail -f`
- `grep -E regex`
- `less`