

Ejercicios prácticos para Linux

Gestión de logs en Linux

En Linux, los logs (registros de eventos) son fundamentales para la administración del sistema y la seguridad. Permiten saber qué ocurre en el sistema operativo, aplicaciones y servicios.

◆ 1. Ubicación de los logs

La mayoría de los registros están en la carpeta:

`/var/log/`

Algunos ficheros importantes:

- `/var/log/syslog` → eventos generales del sistema (Debian/Ubuntu).
- `/var/log/messages` → eventos del sistema (CentOS/RHEL).
- `/var/log/auth.log` → accesos y autenticaciones (inicios de sesión, sudo, SSH).
- `/var/log/kern.log` → mensajes del kernel.
- `/var/log/dmesg` → información de arranque y hardware.
- `/var/log/apache2/access.log` y `error.log` → logs de servidor web Apache.

```
~/Documents/box > ls /var/log/syslog /var/log/messages /var/log/auth.log /var/log/kern.log /var/log/dmesg /var/log/apache2/access.log /var/log/apache2/error.log
ls: cannot access '/var/log/messages': No such file or directory
ls: cannot access '/var/log/dmesg': No such file or directory
/var/log/apache2/access.log /var/log/apache2/error.log /var/log/auth.log /var/log/kern.log /var/log/syslog
~/Documents/box > the /var/log directory's files under control. We also saw
```

◆ 2. Visualización de logs

Comandos básicos para leer registros:

`cat /var/log/syslog`

```
~/Documents/box > sudo cat /var/log/syslog
[sudo] password for kali:
cat: /var/log/syslog: No such file or directory
```

`less /var/log/auth.log`

```
~/Documents/box > sudo less /var/log/auth.log
/var/log/auth.log: No such file or directory
```

`tail -n 50 /var/log/syslog` # últimas 50 líneas

```
~/Documents/box > tail -n 50 /var/log/dpkg.log
2025-09-23 11:32:44 status unpacked libtorsocks:amd64 2.5.0-1
2025-09-23 11:32:44 status half-configured libtorsocks:amd64 2.5.0-1
2025-09-23 11:32:44 status installed libtorsocks:amd64 2.5.0-1
2025-09-23 11:32:44 configure tor-geoipdb:all 0.4.8.16-1 <none>
2025-09-23 11:32:44 status unpacked tor-geoipdb:all 0.4.8.16-1
2025-09-23 11:32:44 status half-configured tor-geoipdb:all 0.4.8.16-1
2025-09-23 11:32:44 status installed tor-geoipdb:all 0.4.8.16-1
2025-09-23 11:32:44 configure torsocks:all 2.5.0-1 <none>
2025-09-23 11:32:44 status unpacked torsocks:all 2.5.0-1
2025-09-23 11:32:44 status half-configured torsocks:all 2.5.0-1
2025-09-23 11:32:44 status installed torsocks:all 2.5.0-1

~/Documents/box > tail -n 50 /var/log/syslog
tail: cannot open '/var/log/syslog' for reading: No such file or directory
```

`tail -f /var/log/syslog` # ver en tiempo real

```
~/Documents/box > tail -f /var/log/dpkg.log
2025-09-23 12:52:29 configure lastlog2:amd64 2.41.1-1 <none>
2025-09-23 12:52:29 status unpacked lastlog2:amd64 2.41.1-1
2025-09-23 12:52:29 status half-configured lastlog2:amd64 2.41.1-1
2025-09-23 12:52:29 status installed lastlog2:amd64 2.41.1-1
2025-09-23 12:52:29 trigproc man-db:amd64 2.13.1-1 <none>
2025-09-23 12:52:29 status half-configured man-db:amd64 2.13.1-1
2025-09-23 12:52:29 status installed man-db:amd64 2.13.1-1
```

◆ 3. Filtrado y búsqueda

- `grep`: buscar patrones específicos.

`grep "Failed" /var/log/auth.log`

```
~/Documents/box > grep "installed" /var/log/dpkg.log
2025-05-29 19:02:39 status half-installed base-passwd:amd64 3.6.7
2025-05-29 19:02:39 status installed base-passwd:amd64 3.6.7
2025-05-29 19:02:39 status half-installed base-files:amd64 1:2025.2.0
2025-05-29 19:02:40 status installed base-files:amd64 1:2025.2.0
2025-05-29 19:02:40 status half-installed dpkg 1.22.18+kali1
2025-05-29 19:02:40 status installed dpkg:amd64 1.22.18+kali1
2025-05-29 19:02:40 status half-installed libc6:amd64 2.41-6
```

- `awk`: contar o procesar datos.

`awk '/Failed/ {count++} END {print count}' /var/log/auth.log`

```
~/Documents/box > awk '/installed/ {count++} END {print count}' /var/log/dpkg.log
8428
```

- sed: extraer y mostrar partes concretas.

sed -n '/sshd/p' /var/log/auth.log

```
~/Documents/box > sed -n '/lastlog/p' /var/log/dpkg.log
2025-05-29 19:02:46 install liblastlog2-2:amd64 <none> 2.41-4
2025-05-29 19:02:46 status half-installed liblastlog2-2:amd64 2.41-4
2025-05-29 19:02:46 status unpacked liblastlog2-2:amd64 2.41-4
2025-05-29 19:02:51 configure liblastlog2-2:amd64 2.41-4 <none>
2025-05-29 19:02:51 status unpacked liblastlog2-2:amd64 2.41-4
2025-05-29 19:02:51 status half-configured liblastlog2-2:amd64 2.41-4
2025-05-29 19:02:51 status installed liblastlog2-2:amd64 2.41-4
2025-09-17 07:52:05 upgrade liblastlog2-2:amd64 2.41-4 2.41.1-1
```

◆ 4. Servicios de gestión de logs

- rsyslog → estándar en muchas distros; recoge y guarda logs.
 - Configuración: /etc/rsyslog.conf

```
~/Documents/box > cat /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability
```

- Servicio: systemctl status Rsyslog

```
~/Documents/box > systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-09-23 13:27:54 CEST; 45s ago
     Invocation: 04b396ce2cc44439834c936fa352b614
   TriggeredBy: ● syslog.socket
      Docs: man:rsyslogd(8)
            man:rsyslog.conf(5)
            https://www.rsyslog.com/doc/
   Main PID: 4215 (rsyslogd)
```

```
~/Documents/box > rsyslogd
rsyslogd: cannot create '/run/systemd/journal/syslog': Address already in use [v8.2506.0 try https://www.rsyslog.com/e/2145 ]
rsyslogd: imuxsock does not run because we could not acquire any socket [v8.2506.0]
rsyslogd: activation of module imuxsock failed [v8.2506.0]
rsyslogd: imklog: cannot open kernel log (/proc/kmsg): Permission denied.
rsyslogd: activation of module imklog failed [v8.2506.0 try https://www.rsyslog.com/e/2145 ]
rsyslogd: error writing pid file (creation stage)
: Permission denied
rsyslogd: run failed with error -3000 (see rsyslog.h or try https://www.rsyslog.com/e/3000 to learn more)
rsyslog startup failure: error reading "fork pipe": No such file or directory
```

- journalctl → sistema de logs binarios de systemd.
 - Ejemplo:
 - journalctl -xe # eventos recientes con detalle

```
~/Documents/box > journalctl -xe
Sep 23 13:25:44 kali kernel: 11:25:44.567440 dnd No guest source window
Sep 23 13:25:44 kali kernel: 11:25:44.574411 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ
Sep 23 13:25:44 kali kernel: 11:25:44.579536 dnd No guest source window
Sep 23 13:27:43 kali sudo[4042]: kali : TTY=pts/1 ; PWD=/home/kali/Documents/box ; USER=root
Sep 23 13:27:43 kali sudo[4042]: pam_unix(sudo:session): session opened for user root(uid=0) by
Sep 23 13:27:54 kali systemd[1]: Reload requested from client PID 4136 ('systemctl') (unit sess
Sep 23 13:27:54 kali systemd[1]: Reloading...
Sep 23 13:27:54 kali systemd-sshd-generator: Configuration directory '/etc/ssh/' does not exist
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: SysV service '/etc/init.d/inetsim' lacks a native sy
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: Please update package to include a native sy
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: ! This compatibility logic is deprecated, ex
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: SysV service '/etc/init.d/stunnel4' lacks a
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: Please update package to include a native sy
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: ! This compatibility logic is deprecated, ex
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: SysV service '/etc/init.d/ptunnel' lacks a n
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: Please update package to include a native sy
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: ! This compatibility logic is deprecated, ex
Sep 23 13:27:54 kali (sd-exec[4183]: /usr/lib/systemd/system-generators/systemd-sshd-generator
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: SysV service '/etc/init.d/dns2tcp' lacks a n
Sep 23 13:27:54 kali systemd-sysv-generator[4201]: Please update package to include a native sy
```

- journalctl -u ssh # logs del servicio SSH

```
~/Documents/box > journalctl -u ssh
-- No entries --
```

- journalctl --since "1 hour ago"

```
~/Documents/box > journalctl --since "1 hour ago"
Sep 23 12:32:49 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:32:49 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:32:49 kali kernel: audit: type=1400 audit(1758623569.104:213): apparmor="DENIED"
Sep 23 12:33:18 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:33:18 kali kernel: audit: type=1400 audit(1758623598.424:214): apparmor="DENIED"
Sep 23 12:33:44 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:33:44 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:33:44 kali kernel: audit: type=1400 audit(1758623624.700:215): apparmor="DENIED"
Sep 23 12:33:56 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:33:56 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:33:56 kali kernel: audit: type=1400 audit(1758623636.844:216): apparmor="DENIED"
Sep 23 12:34:10 kali rtkit-daemon[787]: Supervising 8 threads of 5 processes of 1 users.
Sep 23 12:34:10 kali kernel: audit: type=1400 audit(1758623650.220:217): apparmor="DENIED"
```

◆ 5. Rotación de logs (logrotate)

Los logs crecen mucho con el tiempo → logrotate los rota, comprime y elimina viejos.

- Configuración: /etc/logrotate.conf y /etc/logrotate.d/

```
~/Documents/box > ls /etc/logrotate.d/
alternatives bootlog gvmdb mariadb openvas-scanner redis-server speech-dispatcher wtmp
apache2 btcp linuxserver mosquitto postgresql-common rsyslog stunnel4
apt this tutor dpkg we l macchanger nginx logrotate sane-utils d h tor
```

- Ejemplo de rotación semanal y mantener 4 copias:
- /var/log/syslog {

- weekly
- rotate 4
- compress
- missingok
- }

```
~/Documents/box > cat /var/log/syslog
2025-09-23T13:27:54.300490+02:00 kali systemd[1]: Listening on syslog.socket - Sys
2025-09-23T13:27:54.300693+02:00 kali systemd[1]: Starting rsyslog.service - Syste
2025-09-23T13:27:54.300840+02:00 kali rsyslogd: imuxsock: Acquired UNIX socket '/r
emd. [v8.2506.0]
2025-09-23T13:27:54.300659+02:00 kali kernel: Linux version 6.12.38+kali-amd64 (de
ian 14.2.0-19) 14.2.0, GNU ld (GNU Binutils for Debian) 2.44) #1 SMP PREEMPT_DYNAM
2025-09-23T13:27:54.301157+02:00 kali kernel: Command line: BOOT_IMAGE=/boot/vmlin
76-4eda-bb32-2e0c8f148825 ro quiet splash
2025-09-23T13:27:54.301159+02:00 kali kernel: BIOS-provided physical RAM map:
2025-09-23T13:27:54.301160+02:00 kali kernel: BIOS-e820: [mem 0x0000000000000000-0
2025-09-23T13:27:54.301160+02:00 kali kernel: BIOS-e820: [mem 0x0000000000009fc00-0
2025-09-23T13:27:54.301160+02:00 kali kernel: BIOS-e820: [mem 0x000000000000f0000-0
2025-09-23T13:27:54.301161+02:00 kali kernel: BIOS-e820: [mem 0x00000000000100000-0
2025-09-23T13:27:54.301162+02:00 kali kernel: BIOS-e820: [mem 0x00000000000dfff0000-0
```

◆ 6. Centralización y análisis

En entornos grandes, los logs se envían a un servidor central:

- Syslog centralizado (rsyslog/envío remoto).
- Herramientas modernas:
 - ELK Stack (Elasticsearch, Logstash, Kibana)
 - Splunk
 - Graylog

📄 Ejercicios prácticos (para alumnos)

1. Ver logs del sistema en tiempo real

`tail -f /var/log/syslog`

```
~/Documents/box > tail -f /var/log/syslog
2025-09-23T13:32:11.642941+02:00 kali kernel: 11:32:11.640475 dnd
2025-09-23T13:32:11.659146+02:00 kali kernel: 11:32:11.655620 dndHGCM
58) from host
2025-09-23T13:32:11.659156+02:00 kali kernel: 11:32:11.656498 dnd
2025-09-23T13:32:11.682951+02:00 kali kernel: 11:32:11.680038 dndHGCM
58) from host
2025-09-23T13:32:11.683014+02:00 kali kernel: 11:32:11.682703 dnd
2025-09-23T13:32:11.715345+02:00 kali kernel: 11:32:11.712009 dndHGCM
58) from host
```



- 2.

g

```
~/Documents/box > grep "Failed" /var/log/auth.log
```


- ### 3.

av

```
~/Documents/box > awk '/Failed/ {count++} END {print count}' /var/log/auth.log
```

- 4.**

jd

```
~/Documents/box > journalctl -u ssh --since "today"
```

- 5.

```
~/Documents/box > sudo touch /etc/logrotate.d/linuxserver
```

```
~/Documents/box > sudo logrotate -f /etc/logrotate.d/linuxserver
```

[illegible]

Lastlog2

```
~/Documents/box > lastlog2 --user kali
Username      Port      From      Latest
kali          tty7      :0         Tue Sep 23 13:10:40 +0200 2025
```

```
~/Documents/box > lastlog2 --time 5
Username      Port      From
kali          tty7      :0
lightdm       tty7      :0
```

```
~/Documents/box > lastlog2 --user kali --time 10
Username      Port      From      Latest
kali          tty7      :0         Tue Sep 23 13:10:40 +0200 2025
```