# 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.

---

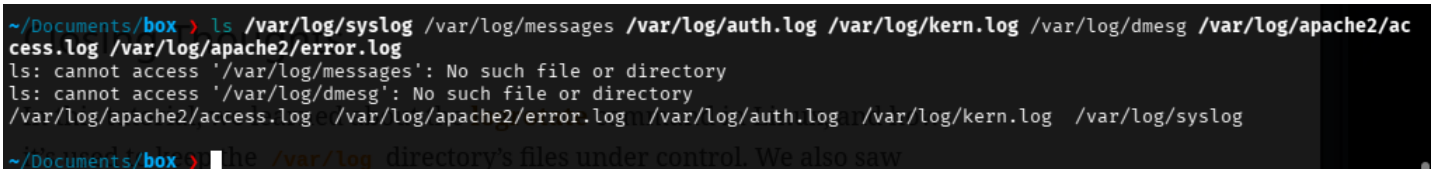
## 🔷 1. Ubicación de los logs

La mayoría de los registros están en la carpeta:

/var/log/

Algunos ficheros importantes:

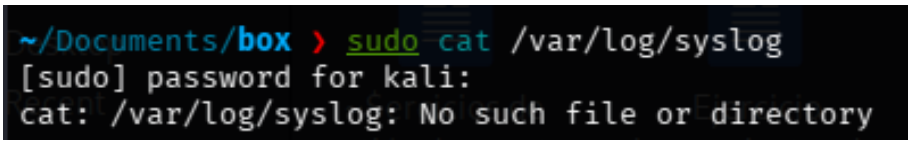
- /var/log/syslog → eventos generales del sistema (Debian/Ubuntu).
- /var/log/messages → eventos del sistema (CentOS/RHEL).
- /var/log/auth.log → accesos y autenticaciones (inicios de sesión, sudo, SSH).
- /var/log/kern.log → mensajes del kernel.
- /var/log/dmesg → información de arranque y hardware.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




## 🔷 2. Visualización de logs

Comandos básicos para leer registros:

cat /var/log/syslog




less /var/log/auth.log

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
```

---

## 🔷 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

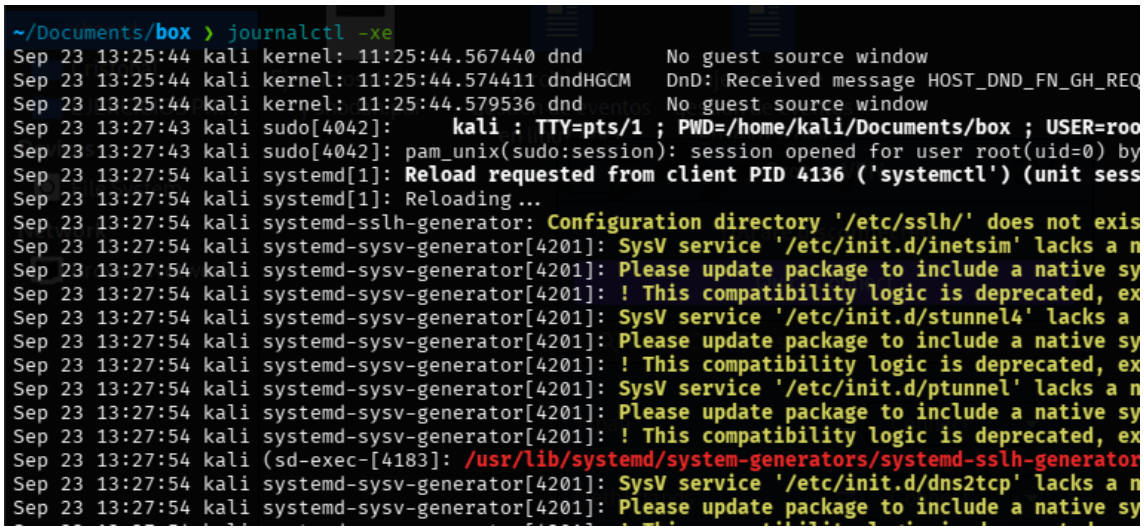
```
~/Documents/box ❯ cat /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system loggi
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)
```

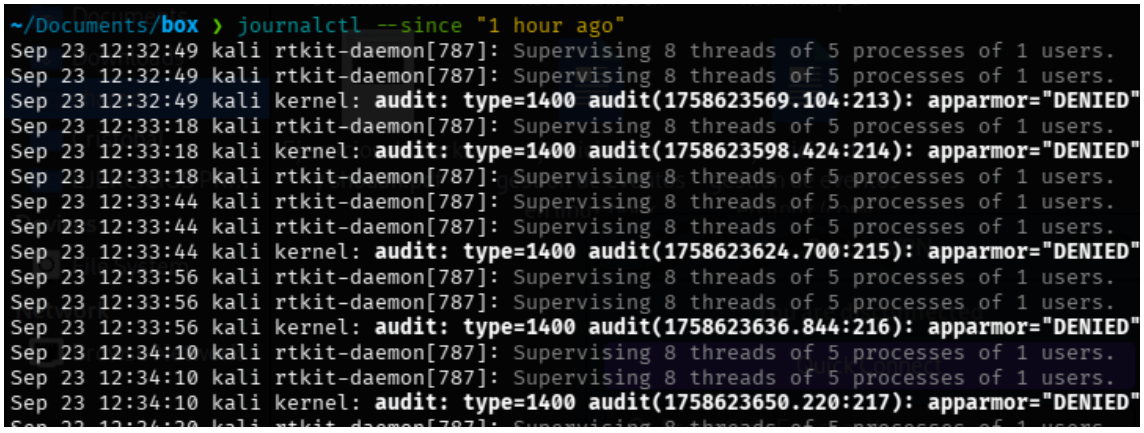
```
~/Documents/box ❯ rsyslogd
rsyslogd: cannot create '/run/systemd/journal/syslog': Address already in use [v8.2506.0 try https:
rsyslogd: imuxsock does not run because we could not acquire any socket  [v8.2506.0]
rsyslogd: activation of module imuxsock failed [v8.2506.0]
rsyslogd: imklog: cannot open 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
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




    - journalctl -u ssh  # logs del servicio SSH


    - journalctl --since "1 hour ago"




---

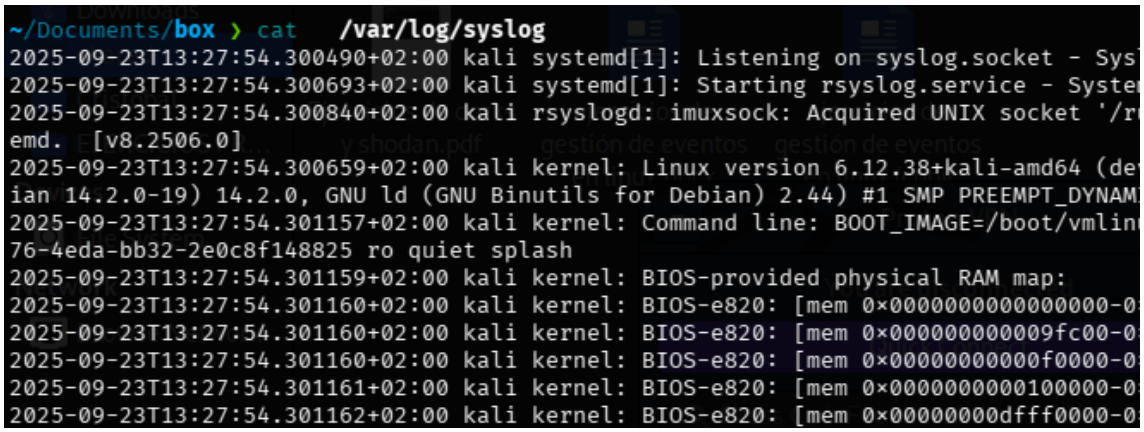
### 🔷 5. Rotación de logs (logrotate)

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

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


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

- weekly
- rotate 4
- compress
- missingok
- }




---

🔷 6. Centralización y análisis

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

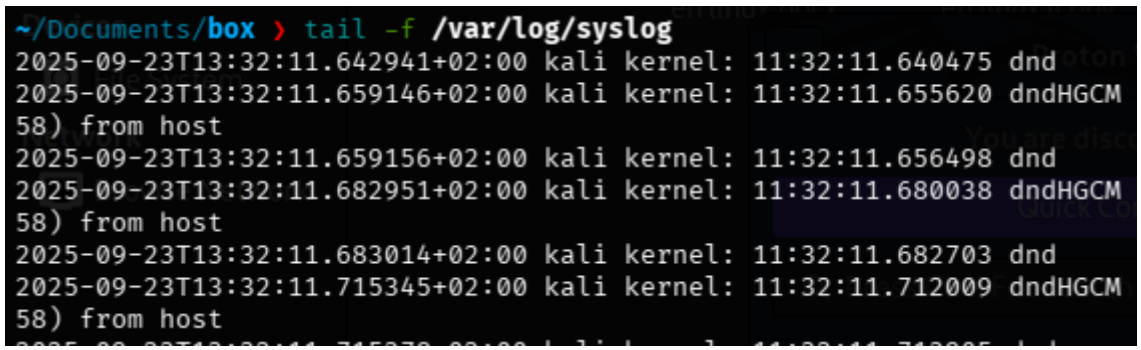
- Syslog centralizado (rsyslog/envío remoto).
- Herramientas modernas:
  - ELK Stack (Elasticsearch, Logstash, Kibana)
  - Splunk
  - Graylog

---

📝 Ejercicios prácticos (para alumnos)

1. Ver logs del sistema en tiempo real

   tail -f /var/log/syslog



👉 ¿Qué pasa si abres otra terminal y haces sudo su?

2. Buscar intentos fallidos de inicio de sesión

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

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

👉 ¿Qué IPs aparecen?

3. Contar cuántos intentos fallidos ha habido hoy

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

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

4. Ver logs del servicio SSH usando systemd

   journalctl -u ssh --since "today"

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

5. Configurar una rotación de logs personalizada con logrotate para un archivo ficticio.

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

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

```
~/Documents/box ❯ sudo logrotate -v /etc/logrotate.d/linuxserver
Ignoring /etc/logrotate.d/linuxserver because it's empty.
acquired lock on state file /var/lib/logrotate/status
Reading state from file: /var/lib/logrotate/status
Allocating hash table for state file, size 64 entries
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
```

# 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
```