

Tips and Tricks

Trucos para usuarios linux

- [Como convertir ficheros .flac a .mp3 en el shell de linux con ffmpeg](#)
- [Teclas Inicio \(Home\) y Final \(End\) en ZSH y oh-my-zsh con Powershell](#)
- [Linux, paquetes instalados desde el shell](#)
- [Cómo instalar y activar el repositorio EPEL en Centos 7/8](#)
- [Conocer el tamaño de unas carpetas ignorando los enlaces duros \(rsync\)](#)
- [Ssh se sale \(break\) de un ciclo \(loop\) en un script bash](#)
- [Redis Failed to start Advanced key-value store.](#)
- [Comando find con -maxdepth excluyendo el propio directorio](#)
- [Du y los ficheros o directorios ocultos](#)
- [Como vaciar o eliminar emails antiguos en dovecot sin usar find](#)
- [rc.local en sistemas Debian usando systemd. Ejemplo redis](#)
- [Bad Bots y la pesadilla del tráfico. Htaccess en Apache 2.4](#)
- [Sudo sin contraseña](#)

Como convertir ficheros .flac a .mp3 en el shell de linux con ffmpeg

Introducción

Algunas veces me descargo o me pasan algun disco de música clasica en forma [.flac](#) y la verdad, ni tengo el equipo para tal audición, ni tanto espacio en mis saturados discos. Asi que lo mejor es convertirlos a [.mp3](#) (también puedes hacerlo a .ogg si eres muy OpenSource (aunque mp3 ya es formato abierto)

Convertir todos los ficheros .flac de un directorio a .mp3 con ffmpeg en linux con el shell

Bueno, ni que decir tiene que debes tener instalado **ffmpeg** y los codecs, pero eso lo dejo para otro momento.

Rekursivo

```
find -name "*.flac" -exec ffmpeg -i {} -acodec libmp3lame -ab 128k {}.mp3 \;
```

Un solo nivel

```
find -maxdepth 1 -name "*.flac" -exec ffmpeg -i {} -acodec libmp3lame -ab 128k {}.mp3 \;
```

Enlaces

- [man ffmpeg](#)
- [find](#)
- [Los 28 comandos más útiles de FFmpeg](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Teclas Inicio (Home) y Final (End) en ZSH y oh-my-zsh con Powershell

Introducción

La verdad es que me encanta usar [ZHS](#) en combinación de [Oh-My-Zsh](#) y el tema [PowerLevel10k](#) pero tenía un problema con las teclas Inicio (Home) y Fin (End) que no funcionan. Al final lo solucioné y te cuento como lo hice.

Solución al problema

Para probar si te va a funcionar antes de editar el fichero de configuración de zsh, te aconsejo que ejecutes en el terminal y después pruebes las teclas:

```
> bindkey "\033[1~" beginning-of-line  
> bindkey "\033[4~" end-of-line
```

Si te funciona (debería), es necesario editar el fichero `~/.zshrc` y añadirlo.

Después ejecuta:

```
> source ~/.zshrc
```

Enlaces

- [Candrew34 en github -> Cannot using home/end key after install oh-my-zsh](#)
- [List of zsh bindkey commands](#)

- [Binding Keys in Zsh – jdhaos’s blog](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Linux, paquetes instalados desde el shell

Introducción

A veces necesitamos conocer que paquetes tenemos instalados en nuestra distribución linux. Y no usamos un entorno gráfico.

Distribuciones basadas en .deb

Para conocer qué paquetes están instalados en nuestra distribución linux, desde el shell ejecutaremos

```
# apt list --installed | grep nginx
```

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

```
nginx/stable,now 1.18.0-2~focal amd64 [installed,upgradable to: 1.20.1-1~focal]
```

Distribuciones basadas en .rpm

```
rpm -qa | grep apache  
ea-apache24-mod_bwllimited-1.4-47.52.2.cpanel.x86_64  
...  
ea-apache24-2.4.48-3.12.1.cpanel.x86_64  
...
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Cómo instalar y activar el repositorio EPEL en Centos 7/8

Introducción

El repositorio EPEL (Extra Packages for Enterprise Linux) es un repositorio de un grupo de Fedora que crea, mantiene y administra una serie de paquetes **.rpm** ausentes o presentes en versiones anticuadas, para mejorar las capacidades de las distros basadas en Redhat (RHEL, CentOS, Scientific Linux, Fedora)

Sus instalación en un servidor con cPanel requiere ciertas normas para evitar problemas posteriores, que algunas veces pueden ser bastante graves para nuestro sistema.

Instalación EPEL (CentOs 7/8)

Instalación EPEL (CentOs 7/8)

```
[root@centos7 ~]# yum -y install epel-release
Complementos cargados:fastestmirror
Loading mirror speeds from cached hostfile
* base: mirror.tedra.es
* extras: mirror.tedra.es
* updates: mirror.tedra.es
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete epel-release.noarch 0:7-11 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas
```



```
=====
=====
=====
Package                Arquitectura          Versión
Repositorio            Tamaño
=====
=====
=====
Instalando:
  epel-release          noarch              7-11
extras                  15 k
=====

Resumen de la transacción
=====
=====
=====

Instalar 1 Paquete

Tamaño total de la descarga: 15 k
Tamaño instalado: 24 k
Downloading packages:
epel-release-7-
11.noarch.rpm                                     | 15 kB
00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando   : epel-release-7-11.noarch      1/1
  Comprobando  : epel-release-7-11.noarch      1/1

Instalado:
  epel-release.noarch 0:7-11

¡Listo!
```

Desactivación (cpanel consejo)

Por defecto un repositorio se instalan activados, lo cual es bastante peligroso en un servidor con cPanel o con otro panel intrusivo (el 99,9% lo son)

Deberemos editar el fichero de configuración del repositorio `/etc/yum.repos.d/epel.repo` editando la línea `enable=1` a `enable=0`

```
[epel]
name=Extra Packages for Enterprise Linux 7 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/7/$basearch
metalink=https://mirrors.fedoraproject.org/metalink?repo=epel-7&arch=$basearch
failovermethod=priority
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
```

Cuando queramos instalar o actualizar algún paquete del repositorio epel deberemos usar la opción `--enablerepo=epel` en nuestro comando yum

Ejemplo

```
[root@centos7 ~]# yum --enablerepo=epel -y install snapd
```

Verificacion doble de desactivación

Como es importante, deberíamos hacer una doble verificación de que el repositorio no está activo, con el comando `yum repolist` que en caso de no estar activo, no lo mostrará.

```
[root@centos7 ~]# yum repolist
Complementos cargados:fastestmirror
Loading mirror speeds from cached hostfile
* base: mirror.tedra.es
* extras: mirror.tedra.es
* updates: mirror.tedra.es
```

id del repositorio	nombre del repositorio	estado
base/7/x86_64	CentOS-7 - Base	10.072
extras/7/x86_64	CentOS-7 - Extras	498
updates/7/x86_64	CentOS-7 - Updates	2.579
repolist: 13.149		

Conocer los paquetes disponibles en EPEL

Es un comando sencillo que mostrará la lista de paquetes del repositorio.

```
[root@centos7 ~]# yum --disablerepo="*" --enablerepo="epel" list available
Complementos cargados:fastestmirror
Loading mirror speeds from cached hostfile
* epel: mirror.eixamcoop.cat

Paquetes disponibles
0ad.x86_64                0.0.22-1.el7          epel
0ad-data.noarch           0.0.22-1.el7          epel
0install.x86_64           2.11-1.el7            epel
2048-cli.x86_64           0.9.1-1.el7           epel
2048-cli-nocurses.x86_64  0.9.1-1.el7           epel
...
```

Lista de paquetes de EPEL disponibles

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Conocer el tamaño de unas carpetas ignorando los enlaces duros (rsync)

Rsync, enlaces duros y du

En mi trabajo uso rsync con un sistema de enlaces duros, como el **Time Machine** de Apple. Y a veces es bueno saber o conocer, el tamaño de las carpetas ignorando los enlaces duros, en los que esta basado este sistema de backup continuo.

du

```
$ du -hc --max-depth=1 path/  
24G   rsync/2022-03-17-065908  
1.6M  rsync/2022-03-17-072202  
1.2G  rsync/2022-03-17-105858  
1.1G  rsync/2022-03-17-074333  
79.9G rsync/  
79.9G total
```

- [Man page command du](#)
- [How to get folder size ignoring hard links?](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como esta, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Ssh se sale (break) de un ciclo (loop) en un script bash

Introducción

Uso [Rsync time backup](#) para algunos proyectos, pero el caso de uno en particular con más de 8TB de ficheros a mantener en backup, y con múltiples usuarios, prefiero usar una estrategia de copia de seguridad por usuario.

Cuando programé el script bash rápido para hacer este trabajo, me encontré que la finalización del script se alcanzaba tras leer el completar la primera copia de seguridad.

Tras finalizar correctamente el proceso de sincronización.

El problema es que **ssh** lee desde la entrada estándar, por lo tanto, se come todas las líneas restantes.

Solución al problema en ssh

```
ssh $USER@$SERVER "COMMAND_IN_REMOTE" < /dev/null
```

También podemos usar `ssh -n` en lugar de la redirección a ninguna parte.

“-n” Redirects stdin from /dev/null (actually, prevents reading from stdin). This must be used when ssh is run in the background. A common trick is to use this to run X11 programs on a remote machine. For example, `ssh -n shadows.cs.hut.fi emacs &` will start an emacs on shadows.cs.hut.fi, and the X11 connection will be automatically forwarded over an encrypted channel. The ssh program will be put in the background. (This does not work if ssh needs to ask for a password or passphrase; see also the -f option.)

Solución en Rsync time backup

En este software no hay posibilidad de modificar o usar el parámetro -n así que solo se puede hacer vía redirección a ninguna parte `< /dev/null`

```
while IFS= read -r line
do
  case $line in
    appdata_ociz9efdik2y|transmission-daemon|updater-ociz9efdik2y)
      continue
      ;;
    *)
      echo "$line"
      /srv/mypath/diwan/rsync-time-backup/rsync_tmbackup.sh --rsync-set-flags "-D -zz --numeric-ids --links --
hard-links -rlt --no-perms --no-group --no-owner --itemize-changes" --strateg
y "1:1 7:7 30:30" -p 9999 root@mypath.domain.net:/data/"$line" /srv/storage/mypath/rsync/"$line" < /dev/null
      ;;
    esac
done < "$input"
```

Agradecimientos

- [ssh breaks out of while-loop in bash - duplicate](#)
- [While loop stops reading after the first line in Bash](#)
- [ssh\(1\) - Linux man page](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Redis Failed to start Advanced key-value store.

Introducción

En algún momento nuestro servidor **Redis** falla, y deja de estar operativo. Reiniciamos pero no arranca y en su lugar muestra un error cuando hacemos un `sudo systemctl status redis-server`

```
jun 02 17:43:33 abkrim-nox systemd[1]: Failed to start Advanced key-value store.
```

Por más que lo intentamos no lo consigue. Veamos que podemos hacer.

Analizando el problema

Systemctl logs

```
journalctl -xeu redis-server.service
[+] The job identifier is 3699 and the job result is done.
jun 02 17:45:14 abkrim-nox systemd[1]: redis-server.service: Start request repeated too quickly.
jun 02 17:45:14 abkrim-nox systemd[1]: redis-server.service: Failed with result 'exit-code'.
[+] Subject: Unit failed
[+] Defined-By: systemd
[+] Support: http://www.ubuntu.com/support
[+]
[+] The unit redis-server.service has entered the 'failed' state with result 'exit-code'.
jun 02 17:45:14 abkrim-nox systemd[1]: Failed to start Advanced key-value store.
```

Bueno ya tenemos una pista pero viendo los logs (bendita bitácora) podemos obtener más información.

```
sudo tail -n100 /var/log/redis/redis-server.log
...
7471:M 02 Jun 2022 17:48:00.413 * DB loaded from base file appendonly.aof.66.base.rdb: 0.000 seconds
```



```
7471:M 02 Jun 2022 17:48:00.893 # Bad file format reading the append only file appendonly.aof.66.incr.aof:
make a backup of your AOF file, then use ./redis-check-aof --fix <filename.manifest>
```

Con esto vemos que nuestra configuración de redis esta configurado para usar una estrategia AOF (append-only file) para evitar perdidas de datos en caso de una terminación brusca (energía, kill - 9,..) que no permita la escritura de los datos activos a disco.

```
appendonly yes
```

Y además de esto, nuestro fichero AOF esta corrupto. Así pues hay que recuperarlo.

Reparando el fichero AOF

El comando general es `redis-check-aof -fix` ahora falta encontrar tanto el binario de la utilidad como el fichero.

En mi caso un Ubuntu 22.04 con redis instalado vía repositorio, siendo la versión 6.7

```
➤ sudo ls -l /var/lib/redis
```

```
total 16K
```

```
17170880 4,0K drwxr-x--- 3 redis redis 4,0K jun  2 20:19 .
```

```
16777254 4,0K drwxr-xr-x 94 root  root  4,0K may 31 10:43 ..
```

```
17170910 4,0K drwxr-x--- 2 redis redis 4,0K jun  2 18:34 appendonlydir
```

```
17170564 4,0K -rw-rw---- 1 redis redis 1,6K jun  2 20:19 dump.rdb
```

```
➤ sudo ls -l /var/lib/redis/appendonlydir
```

```
total 836K
```

```
17170910 4,0K drwxr-x--- 2 redis redis 4,0K jun  2 18:34 .
```

```
17170880 4,0K drwxr-x--- 3 redis redis 4,0K jun  2 20:19 ..
```

```
17171350 4,0K -rw-rw---- 1 redis redis 1,6K jun  2 18:34 appendonly.aof.67.base.rdb
```

```
17171130 820K -rw-r----- 1 redis redis 815K jun  2 20:21 appendonly.aof.67.incr.aof
```

```
17171294 4,0K -rw-r----- 1 redis redis  92K jun  2 18:34 appendonly.aof.manifest
```

Así pues el comando sería

```
sudo /usr/bin/redis-check-aof --fix /var/lib/redis/appendonlydir/appendonly.aof.manifest
```

```
Start checking Multi Part AOF
```

```
Start to check BASE AOF (RDB format).
```

```
[offset 0] Checking RDB file appendonly.aof.66.base.rdb
[offset 26] AUX FIELD redis-ver = '7.0.0'
[offset 40] AUX FIELD redis-bits = '64'
[offset 52] AUX FIELD ctime = '1653893946'
[offset 67] AUX FIELD used-mem = '5178616'
[offset 79] AUX FIELD aof-base = '1'
[offset 81] Selecting DB ID 0
[offset 3048] Checksum OK
[offset 3048] \o/ RDB looks OK! \o/
[info] 19 keys read
[info] 9 expires
[info] 9 already expired
RDB preamble is OK, proceeding with AOF tail...
AOF analyzed: filename=appendonly.aof.66.base.rdb, size=3048, ok_up_to=3048, ok_up_to_line=1, diff=0
BASE AOF appendonly.aof.66.base.rdb is valid
Start to check INCR files.
AOF appendonly.aof.66.incr.aof format error
AOF analyzed: filename=appendonly.aof.66.incr.aof, size=64241117, ok_up_to=64238121,
ok_up_to_line=4261202, diff=2996
This will shrink the AOF appendonly.aof.66.incr.aof from 64241117 bytes, with 2996 bytes, to 64238121 bytes
Continue? [y/N]: y
Successfully truncated AOF appendonly.aof.66.incr.aof
All AOF files and manifest are valid
```

Después de esto ya podremos iniciar redis

```
› sudo systemctl restart redis-server
› sudo systemctl status redis-server
● redis-server.service - Advanced key-value store
   Loaded: loaded (/lib/systemd/system/redis-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 17:56:19 CEST; 7min ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
  Main PID: 12969 (redis-server)
    Status: "Ready to accept connections"
     Tasks: 6 (limit: 38330)
   Memory: 3.9M
      CPU: 1.538s
  CGroup: /system.slice/redis-server.service
          └─12969 "/usr/bin/redis-server 127.0.0.1:6379" "" "" "" "" "" "" "" ""
```

```
jun 02 17:56:18 abkrim-nox systemd[1]: Starting Advanced key-value store...
```

```
jun 02 17:56:19 abkrim-nox systemd[1]: Started Advanced key-value store.
```

Enlaces

- [Redis persistence](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Comando find con -maxdepth excluyendo el propio directorio

Comando find con -maxdepth excluyendo el propio directorio

A veces es necesario ejecutar este comando de manera recursiva pero queremos obviar el propio directorio desde el que se ejecuta como por ejemplo para eliminar todos directorios de una carpeta de rsync con enlaces duros de forma ordenada.

```
find . -maxdepth 1 -type d | sed -r '/^\./d'
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Du y los ficheros o directorios ocultos

El comando du y los ficheros ocultos

Muchas veces al usar el comando `du` para localiza directorios con elevado o anormal consumo de espacio en disco nos topamos, con un directorio en el que la información que `du` nos ofrece no se ajusta a nivel directorio con el nivel subdirectorios.

```
> du -sh *
1,3G  api
7,1G  investigo
5,2G  sitelight
1,4G  sitelight2

> cd investigo
> du -sh *
179M  investigo/backup
20K   investigo/conf
408K  investigo/logs
275M  investigo/sitelight
3,2G  investigo/web
```

Nos faltan casi 4 Gb.

Comando du incluyendo los directorios ocultos

```
du -hs investigo/.[^.]*
4,0K  investigo/.bash_history
4,0K  investigo/.bash_logout
4,0K  investigo/.bashrc
3,4G  investigo/.cache
604K  investigo/.config
8,0K  investigo/.emacs.d
4,0K  investigo/.gitconfig
32K  investigo/.java
96K  investigo/.local
4,0K  investigo/.mysql_history
32M  investigo/.npm
18M  investigo/.oh-my-zsh
92K  investigo/.p10k.zsh
4,0K  investigo/.profile
4,0K  investigo/.shell.pre-oh-my-zsh
20K  investigo/.ssh
4,0K  investigo/.Xauthority
8,0K  investigo/.yarn
4,0K  investigo/.yarnrc
48K  investigo/.zcompdump
52K  investigo/.zcompdump-coresitelight-5.8
116K  investigo/.zcompdump-coresitelight-5.8.zwc
28K  investigo/.zsh_history
12K  investigo/.zshrc
```

- [Man page command du](#)
- [du command does not parse hidden directories](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como esta, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Como vaciar o eliminar emails antiguos en dovecot sin usar find

Dovecot y los comandos olvidados

Muchas veces, y me incluyó yo, por vaguería y algo de desconocimiento, pues una se acostumbra a lo fácil, usamos una combinación de `find` para hacer un vaciado de alguna cuenta o carpeta de correo que se llenó.

Pues bien, eso es mejor hacerlo con las herramientas del propio Dovecot (si es este el sistema de servidor IMAP que usamos)

Eliminación de correos IMAP por antigüedad

Ejemplo

```
doveadm expunge -u jane.doe@example.org mailbox Spam savedbefore 2w
```

Obtener la lista de buzones

Dado que los buzones se escriben en el shell de distinta manera, para usarse en el comando es bueno obtener la lista

```
doveadm mailbox list -u jane.doe@example.org
```

Archive

Mantenimientos
Mantenimientos/mysql
ASSP
Seguridad
Seguridad/inmunifyAV
Seguridad/Wordfence
Services
Services/Failed
LFD
[Gmail]
[Gmail]/Importantes
Junk
Trash
Sent
Drafts
INBOX

Purgado por asunto

```
doveadm expunge -u jane.doe@example.org mailbox 'Mantenimientos/mysql' HEADER Subject "Palabra Clave"
```

Purgado mas complejo HEADER y BODY

```
doveadm expunge -u jane.doe@example.org mailbox 'Mantenimientos/mysql' HEADER Subject "Palabra Clave"  
BODY "Otro texto"
```

- Consulta la documentación de Dovecot - Expunge
- [doveadm: Delete messages older than date](#)

Eliminación por linea de asunto

Ejemplo

```
doveadm expunge -u jane.doe@example.org mailbox INBOX subject Cron
```


Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

rc.local en sistemas Debian usando systemd. Ejemplo redis

Introducción

Algunos servicios como **redis** pueden requerir de ciertas configuraciones del sistema para su mejor funcionamiento, como puede ser **Transparent Huge Pages (THP)** desactivado. Si puedes desactivarlo porque no afecta a otros servicios de tu servidor (atento a esto, que no es salir por la calle del medio sin pensar en las implicaciones) es bueno hacerlo.

```
3336867:M 04 Dec 2023 18:05:32.941 # WARNING you have Transparent Huge Pages (THP) support enabled in
your kernel. This will create latency and memory usage issues with Redis. To fix this issue run the command
'echo never > /sys/kernel/mm/transparent_hugepage/enabled' as root, and add it to your /etc/rc.local in order to
retain the setting after a reboot. Redis must be restarted after THP is disabled.
```

Solución

La solución pasa por desactivarlo en el sistema

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

Pero necesitamos ejecutar esto al reinicio, o perdermos la configuración deseada. La opción normal sería añadirlo al script de arranque, como muchos dicen, en `/etc/rc.local` pero distros basadas en Debian, o otras basadas en RedHat, no tiene ese fichero porque usan ya de hace tiempo **systemd** para la gestión de estas cuestiones.

Crear un Servicio systemd para Desactivar THP

Crear un Archivo de Servicio systemd: Abre un nuevo archivo en el directorio de servicios de systemd con un editor de texto como nano o vim. Por ejemplo:

```
sudo nano /etc/systemd/system/disable-thp.service
```

Donde añadimos

```
[Unit]
Description=Disable Transparent Huge Pages (THP)

[Service]
Type=oneshot
ExecStart=/bin/sh -c 'echo never > /sys/kernel/mm/transparent_hugepage/enabled'

[Install]
WantedBy=multi-user.target
```

Lo habilitamos

```
sudo systemctl daemon-reload
sudo systemctl enable disable-thp.service
sudo systemctl start disable-thp.service
```

Verificamos

```
cat /sys/kernel/mm/transparent_hugepage/enabled
always madvise [never]
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Bad Bots y la pesadilla del tráfico. Htaccess en Apache 2.4

Cada vez esta pero el tema. Un ejercito de web scrappers, de personas dedicadas a vivir de crear contenido falso, indexable, o de robar imágenes, pulula por la red.

Una de las mejores formas de acabar con ellos es denegarles el acceso, en nuestro fichero

`.htaccess`

.htaccess anti bad bots

La cuesgtión es añadir la lista de robots no deseados en nuestro fichero `.htaccce` usando para ello las directivas `setenvif`

```
# Start Bad Bot Prevention
<IfModule mod_setenvif.c>
# SetEnvIfNoCase User-Agent ^$ bad_bot
SetEnvIfNoCase User-Agent "^12soso.*" bad_bot
SetEnvIfNoCase User-Agent "^192.comAgent.*" bad_bot
SetEnvIfNoCase User-Agent "^1Noonbot.*" bad_bot
...

<Limit GET POST PUT>
    Order Allow,Deny
    Allow from all
    Deny from env=bad_bot
</Limit>
</IfModule>
# End Bad Bot Prevention
```

- `<IfModule mod_setenvif.c>` Esta directiva comprueba si el módulo `mod_setenvif` está habilitado. Si lo está, se ejecuta el código dentro de este bloque.
- `SetEnvIfNoCase User-Agent "^12soso.*" bad_bot`: Esta directiva establece una variable de entorno llamada `bad_bot` si el User-Agent comienza con "12soso".
- `<Limit GET POST PUT>`: Esta directiva limita las reglas dentro de este bloque a los métodos HTTP especificados (GET, POST y PUT).
- `Order Allow,Deny`: Define el orden en el que se aplican las reglas de acceso. Primero se aplican las reglas `Allow` y luego las reglas `Deny`.
- `Allow from all`: Permite el acceso a todos por defecto.
- `Deny from env=bad_bot`: Deniega el acceso a cualquier solicitud que tenga la variable de entorno `bad_bot` establecida.
- los `</` cierra la directiva correspondiente

La lista

Hay muchas, pero [esta lista](#) es un buen punto de partida y se actualiza regularmente. Incluso puedes mantenerla con algun pequeño script.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Sudo sin contraseña

Configuración y uso de `sudo` en sistemas linux

Introducción sobre el comando `sudo`

¿Qué Hace `sudo`?

El comando `sudo` (Super User DO) permite a un usuario autorizado ejecutar comandos con privilegios de otro usuario, normalmente el usuario root. Es una herramienta fundamental para la administración de sistemas, ya que facilita la realización de tareas que requieren permisos elevados sin necesidad de cambiar de usuario.

Alcances en seguridad y confiabilidad

- **Seguridad:** `sudo` mejora la seguridad al permitir un control granular sobre quién puede ejecutar qué comandos. Registra todas las actividades realizadas, lo que facilita la auditoría y el seguimiento de acciones administrativas.
- **Confiabilidad:** Reduce la necesidad de compartir la contraseña de root, limitando el acceso a privilegios elevados únicamente a usuarios específicos y comandos determinados.

Ubicación de su configuración

La configuración de `sudo` se encuentra principalmente en el archivo `/etc/sudoers`. Además, se pueden añadir configuraciones específicas en el directorio `/etc/sudoers.d/`.

En MacOS lo ficheros `/etc` realmente estan en `/private/etc/`

Usar `visudo` para la edición (aconsejado)

Editar el archivo `/etc/sudoers` directamente puede ser arriesgado, ya que un error de sintaxis puede bloquear el acceso administrativo. Por ello, se recomienda utilizar el comando `visudo`, que verifica la sintaxis antes de aplicar los cambios.

Hacer un backup antes de editar

Antes de modificar el archivo `sudoers`, es prudente realizar una copia de seguridad:

```
sudo cp /etc/sudoers /etc/sudoers.backup_$(date +%Y%m%d)
```

Este comando crea una copia del archivo `sudoers` con la fecha actual, facilitando la restauración en caso de errores.

Editar con `visudo`

Para editar el archivo `sudoers` de manera segura:

```
sudo visudo
```

Este comando abre el archivo en el editor predeterminado configurado para `visudo` (generalmente `nano` o `vi`) y verifica la sintaxis al guardar.

Diferentes posibilidades de configuración

Permitir `sudo` sin pedir contraseña

Para que un usuario pueda ejecutar comandos con `sudo` sin necesidad de ingresar una contraseña, añade la siguiente línea en el archivo `sudoers`:

```
usuario ALL=(ALL) NOPASSWD:ALL
```

Ejemplo:

```
javier ALL=(ALL) NOPASSWD:ALL
```

Permitir `sudo` sin pedir contraseña pero limitado a algunos comandos

Para otorgar permisos de `sudo` sin contraseña pero restringidos a comandos específicos:

```
usuario ALL=(ALL) NOPASSWD:/ruta/al/comando1, /ruta/al/comando2
```

Si tenemos mas d eun comando puede ser mas pratico usar una variable, un fichero de `.conf` específico.

```
touch /etc/sudoers.d/mi_usuario_sudo  
visudo -f /etc/sudoers.d/mi_usuario_sudo
```

Añade la configuración deseada (es un ejemplo)

```
Cmnd_Alias PRTG = /usr/sbin/csf, /usr/local/directadmin/scripts/letsencrypt.sh, /usr/bin/ls, /usr/bin/cat,  
/usr/bin/tail  
admin ALL=(ALL) NOPASSWD: PRTG
```

Guardar y cerrar.

Ejemplo:

```
javier ALL=(ALL) NOPASSWD:/usr/bin/systemctl restart nginx, /usr/bin/systemctl status nginx
```

Atención: En sistemas como macOS, una configuración incorrecta que elimina la solicitud de contraseña puede bloquear el acceso administrativo si no existe otro usuario con privilegios de superadministrador.

Usar `/etc/sudoers.d/` para configuraciones específicas de usuarios

En lugar de modificar directamente el archivo `sudoers`, es posible crear archivos individuales para cada usuario en el directorio `/etc/sudoers.d/`. Esto facilita la gestión y evita conflictos.

Creación de un Archivo de Configuración para un Usuario

1. Crear el Archivo:

```
sudo nano /etc/sudoers.d/usuario
```

2. Añadir las Reglas de `sudo`:

Permitir `sudo` sin contraseña:

```
usuario ALL=(ALL) NOPASSWD:ALL
```

Permitir `sudo` sin contraseña pero limitado a ciertos comandos:

```
usuario ALL=(ALL) NOPASSWD:/usr/bin/systemctl restart nginx, /usr/bin/systemctl status nginx
```

3. Guardar y Cerrar el Archivo:

Presiona `Ctrl + X`, luego `Y` y `Enter` para guardar los cambios.

4. Verificar la Sintaxis:

`visudo` automáticamente verifica la sintaxis al editar el archivo. Sin embargo, puedes comprobar manualmente ejecutando:

```
sudo visudo -cf /etc/sudoers.d/usuario
```

Este comando validará la configuración e informará de cualquier error.

Resumen de comandos clave

Crear una copia de seguridad del archivo sudoers

```
sudo cp /etc/sudoers /etc/sudoers.backup_$(date +%Y%m%d)
```

Editar el archivo sudoers de manera segura

```
sudo visudo
```

Permitir a un usuario ejecutar todos los comandos sin contraseña

```
usuario ALL=(ALL) NOPASSWD:ALL
```

Permitir a un usuario ejecutar comandos específicos sin contraseña

```
usuario ALL=(ALL) NOPASSWD:/ruta/al/comando1, /ruta/al/comando2
```

Crear un archivo de configuración específico para un usuario

```
sudo nano /etc/sudoers.d/usuario
```

Verificar la sintaxis de un archivo en sudoers.d

```
sudo visudo -cf /etc/sudoers.d/usuario
```

Consideraciones Adicionales

- **Permisos de Archivos:** Asegúrate de que los archivos en `/etc/sudoers.d/` tengan permisos correctos (generalmente 0440) para evitar problemas de seguridad.

```
sudo chmod 0440 /etc/sudoers.d/usuario
```

- **Evitar Errores de Sintaxis:** Siempre utiliza `visudo` o editores diseñados para manejar la configuración de `sudo` para prevenir errores que puedan bloquear el acceso administrativo.
- **Uso Responsable de `NOPASSWD`:** Otorgar permisos sin contraseña debe hacerse con cautela, limitando el acceso solo a los comandos estrictamente necesarios para minimizar riesgos de seguridad.
- **Documentación y Auditoría:** Mantén una documentación clara de las configuraciones realizadas y revisa periódicamente los permisos otorgados para asegurar que siguen siendo necesarios y seguros.
- En **MacOS** una configuración errónea del usuario administrador puede ser fatal y muy complicada la recuperación del desastre. Se recomienda por esto y por muchas más cosas, tener siempre un segundo usuario SuperAdmin en un sistema MacOS

Conclusión

El uso adecuado de `sudo` es esencial para la administración segura y eficiente de sistemas Linux. Configurarlos correctamente, utilizando herramientas como `visudo` y aplicando buenas prácticas de seguridad, garantiza que los usuarios puedan realizar tareas administrativas sin comprometer la integridad y seguridad del sistema.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido se entrega, tal y como está, sin que ello implique ninguna obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).