

# ACTIVIDAD EVALUABLE

## SEGURIDAD Y ALTA DISPONIBILIDAD

Configuración ACLs  
(Access Control List)

Alejandro Almagro  
Torregrosa

Autor: Manuel Fernández  
Licencia Creative Commons



**Reconocimiento – NoComercial – CompartirIgual (by-nc-sa):** No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

# ACL: Access Control Lists y los permisos en GNU/Linux

Por defecto, la posibilidad de especificar permisos de lectura, escritura y ejecución a los ficheros en Linux está muy limitada; ya que estos solamente se pueden especificar para el propietario, el grupo principal al que pertenece, y para el resto de usuarios.

No podemos especificar que por ejemplo un fichero puede ser leído por 2 grupos de usuarios o que una lista de usuarios puede escribir en un fichero.

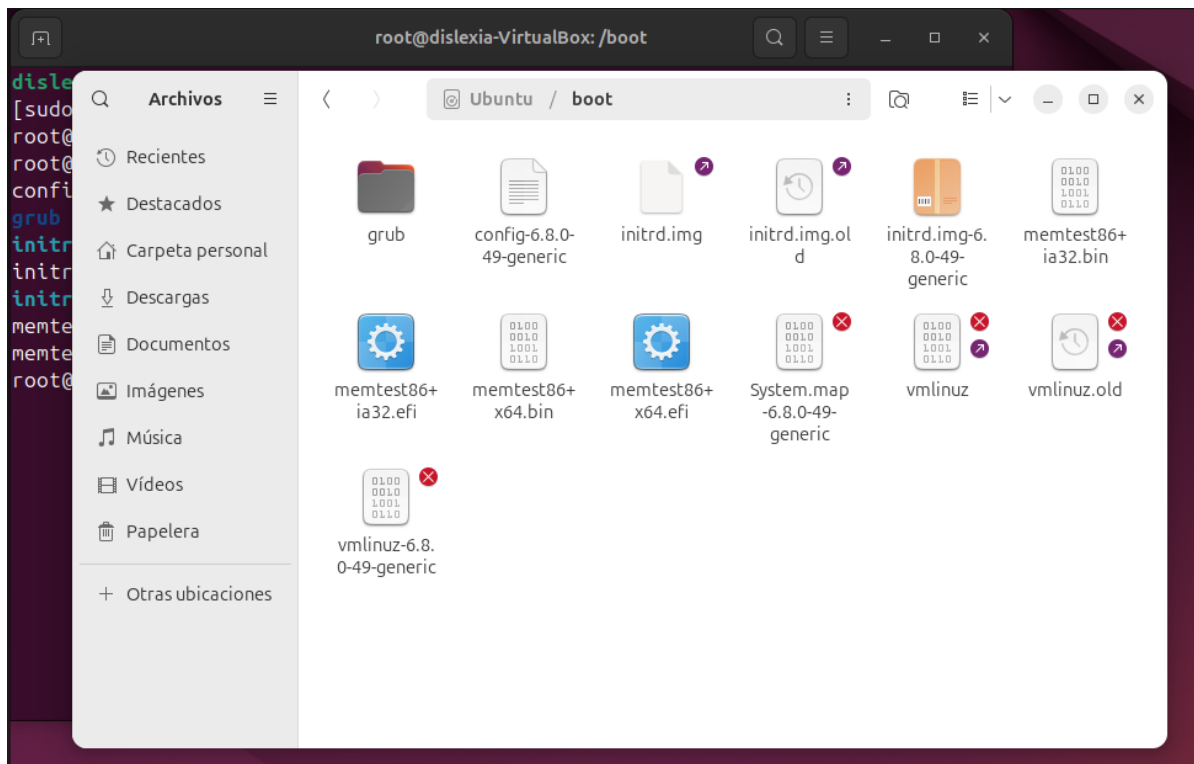
Por fortuna, Linux incorpora la posibilidad de usar ACLs o Listas de Control de Acceso, mediante las cuales cada fichero posee una lista asociada donde se puede especificar con total libertad los permisos relativos a usuarios y/o grupos.

## Comprobar que nuestra versión de Linux tiene ACLs activados:

Lo primero que debemos hacer para hacer uso de las ACLs es comprobar que el kernel (núcleo del SO) de la versión de Linux que tenemos tiene activada esta opción:

```
root@dislexia-VirtualBox:/boot# ls
config-6.8.0-49-generic      memtest86+x64.bin
grub                        memtest86+x64.efi
initrd.img                  System.map-6.8.0-49-generic
initrd.img-6.8.0-49-generic vmlinuz
initrd.img.old              vmlinuz-6.8.0-49-generic
memtest86+ia32.bin          vmlinuz.old
memtest86+ia32.efi
root@dislexia-VirtualBox:/boot#
```

En /boot hay un fichero cuyo nombre es config- seguido de la versión del kernel. Por ejemplo, config-2.6.38-8-generic, en caso de haber varios elige la versión más actual.



Para saber el nombre exacto de nuestro fichero entramos desde el explorador de archivos a la carpeta boot.

Después, simplemente hacemos:

```
root@dislexia-VirtualBox:/# cat /boot/config-6.8.0-49-generic | grep ACL
```

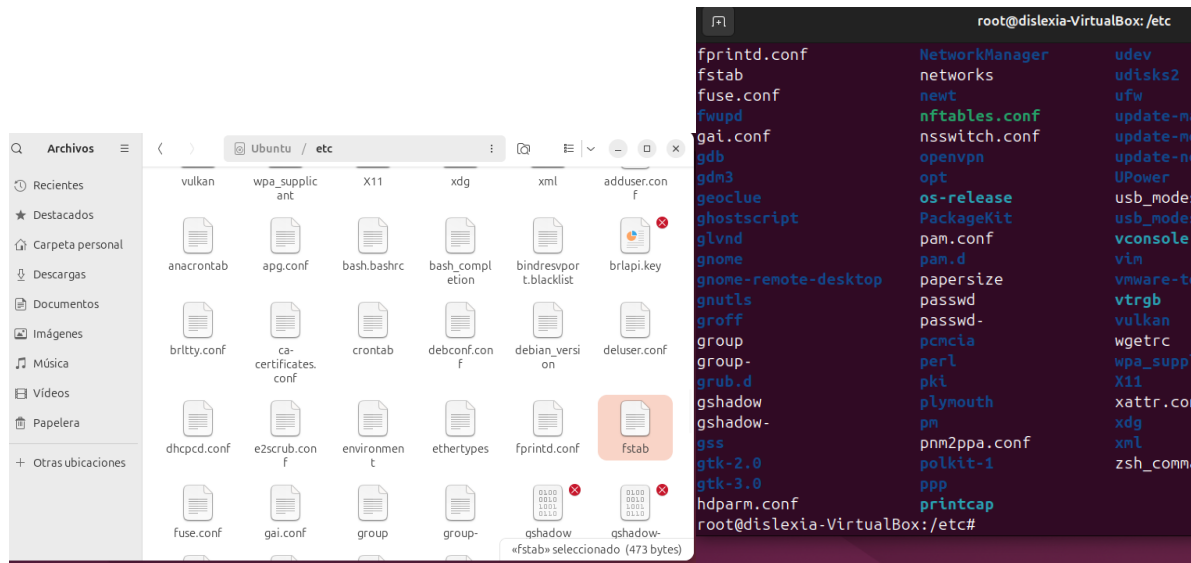
que nos debe mostrar algo similar a la siguiente pantalla:

```
root@dislexia-VirtualBox:/# cat /boot/config-6.8.0-49-generic | grep ACL
CONFIG_XILINX_EMAACLLITE=m
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_REISERFS_FS_POSIX_ACL=y
CONFIG_JFS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
CONFIG_BTRFS_FS_POSIX_ACL=y
CONFIG_F2FS_FS_POSIX_ACL=y
CONFIG_BCACHEFS_POSIX_ACL=y
CONFIG_FS_POSIX_ACL=y
CONFIG_NTFS3_FS_POSIX_ACL=y
CONFIG_TMPFS_POSIX_ACL=y
CONFIG_JFFS2_FS_POSIX_ACL=y
CONFIG_EROF_FS_POSIX_ACL=y
CONFIG_NFS_V3_ACL=y
CONFIG_NFSD_V3_ACL=y
CONFIG_NFS_ACL_SUPPORT=m
CONFIG_CEPH_FS_POSIX_ACL=y
CONFIG_9P_FS_POSIX_ACL=y
root@dislexia-VirtualBox:/#
```

En esta captura podemos ver como tenemos habilitado el soporte de ACLs pues están configurados a "y" (yes).

## Habilitación automática en arranque de ACL en las particiones de nuestro equipo virtual:

Ahora hay que especificar que cuando se monte la partición que contiene los datos, se habilite las ACLs.



El fichero `/etc/fstab` contiene la información relativa a las particiones que se montan durante el arranque y sus opciones. Tendrás que entrar con permisos de administrador, para ello por ejemplo puedes entrar a través del explorador de ficheros con `"sudo nautilus"` y luego en "otras ubicaciones", "equipo", "etc".... En el fichero encontramos algo parecido a lo siguiente:

```
root@dislexia-VirtualBox:/etc# nano fstab
```

```
GNU nano 7.2 fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/6e596d28-fc81-4248-a89d-0a39af114451 / ext4 defaults 0 1
/swap.img none swap sw 0 0
```

Tradicionalmente en este fichero las particiones se especificaban con nombre como /dev/sda1 pero en las últimas versiones de Ubuntu se ha sustituido con un identificador de la partición (UUID) tal como se indica en el fichero y que permite que incluso funcione el fichero si se añade o borran discos.

Al final de la línea en negrita añadimos la opción del montaje con ACLs (**,acl**)

```
/dev/disk/by-uuid/6e596d28-fc81-4248-a89d-0a39af114451 / ext4 defaults,acl 0 1
/swap.img none swap sw 0 0
```

Ahora está habilitado ACL en el arranque.

## Crear y gestionar grupos y usuarios

Ahora instalamos el paquete **acl** que contiene los comandos **getfacl** (para consultar listas ACL) y **setfacl** (para configurar listas ACL).

```
root@dislexia-VirtualBox:/etc# apt-get update && apt-get install acl -y
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
acl ya está en su versión más reciente (2.3.2-1build1.1).
```

Para probar el funcionamiento de las ACLs vamos a crear dos usuarios: **user1** y **user2**. Su contraseña será **123**, el resto de información es irrelevante.

```
root@dislexia-VirtualBox:/home/dislexia# adduser user1
info: Añadiendo el usuario 'user1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Añadiendo el nuevo grupo 'user1' (1001) ...
info: Adding new user 'user1' (1001) with group 'user1 (1001)' ...
info: Creando el directorio personal '/home/user1' ...
info: Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña: 
```

Repetimos el comando con el **user2**, al final si todo se ha echo correctamente debería salir esto:

```
¿Es correcta la información? [S/n] s
info: Adding new user 'user2' to supplemental / extra groups 'users' ...
info: Añadiendo al usuario 'user2' al grupo 'users' ...
root@dislexia-VirtualBox:/home/dislexia#
```

También vamos a crear los grupos siguientes: **contabilidad**, **informatica** y **jefes** (**sin tildes**).

```
root@dislexia-VirtualBox:/home/dislexia# addgroup contabilidad
info: Seleccionando un GID del rango 1000 a 59999 ...
info: Añadiendo el grupo `contabilidad' (GID 1003) ...
root@dislexia-VirtualBox:/home/dislexia# addgroup jefe
info: Seleccionando un GID del rango 1000 a 59999 ...
info: Añadiendo el grupo `jefe' (GID 1004) ...
root@dislexia-VirtualBox:/home/dislexia# addgroup informatica
info: Seleccionando un GID del rango 1000 a 59999 ...
info: Añadiendo el grupo `informatica' (GID 1005) ...
root@dislexia-VirtualBox:/home/dislexia#
```

El usuario user1 pertenece a contabilidad y jefes.

```
root@dislexia-VirtualBox:/home/dislexia# usermod -aG contabilidad user1
root@dislexia-VirtualBox:/home/dislexia# usermod -aG jefes user1
usermod: el grupo «jefes» no existe
root@dislexia-VirtualBox:/home/dislexia# usermod -aG jefe user1
root@dislexia-VirtualBox:/home/dislexia#
```

Si la shell no nos da una respuesta en el comando se habra añadido, si ponemos mal el nombre del grupo nos saltara un error como vemos en la captura.

El usuario user2 pertenece a contabilidad e informatica.

```
root@dislexia-VirtualBox:/home/dislexia# usermod -aG contabilidad user2
root@dislexia-VirtualBox:/home/dislexia# usermod -aG informatica user2
root@dislexia-VirtualBox:/home/dislexia#
```

Para ayudarte en esta tarea, a continuación, tienes los comandos y ejemplos que puedes utilizar:



<code>sudo adduser Maria</code>	Crea un nuevo usuario llamado Maria. Te pide una contraseña y datos extra. <b>Es importante hacerlo como root usando sudo, de lo contrario para introducir la contraseña habría que hacerlo posteriormente usando el comando passwd.</b>
<code>sudo deluser Maria</code>	Elimina el usuario Maria
<code>sudo addgroup inquilinos</code>	Crea el grupo inquilinos
<code>sudo usermod -aG inquilinos Maria</code>	Añade a <i>María</i> al grupo <i>inquilinos</i> . La <i>a</i> viene de <i>append</i> y la <i>G</i> de <i>group</i> .

Para ver los usuarios creados escribimos en la terminal:

```
root@dislexia-VirtualBox:/home/dislexia# cat /etc/passwd
n/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116:./var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117:./var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114:./nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-deskto
p:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
gnome-initial-setup:x:119:65534:./run/gnome-initial-setup:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
dislexia:x:1000:1000:dislexia:/home/dislexia:/bin/bash
user1:x:1001:1001:,,,:/home/user1:/bin/bash
user2:x:1002:1002:,,,:/home/user2:/bin/bash
root@dislexia-VirtualBox:/home/dislexia#
```

## Añadir y modificar permisos

Para añadir a la lista de ACLs se utiliza el comando `setfacl`. Recuerda que si tienes dudas sobre algún comando siempre puedes utilizar la opción `--help` o `-h`.

```
root@dislexia-VirtualBox:/home/dislexia# setfacl --help
setfacl 2.3.2 -- establecer listas de control de acceso a archivo
Uso: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
  -m, --modify=acl          modificar ACL actual(es) de archivo(s)
  -M, --modify-file=arch    leer entradas ACL desde "arch"
  -x, --remove=acl          eliminar entradas desde ACL(s) de archivo(s)
  -X, --remove-file=arch    leer entradas de ACL a borrar desde "arch"
  -b, --remove-all         eliminar todas las entradas ACL extendidas
  -k, --remove-default      eliminar el ACL predeterminado
  --set=acl                 establecer ACL(s) de archivo(s), reemplazando el actual
  --set-file=arch           leer entradas ACL a establecer desde "arch"
  --mask                    recalcular la máscara de permisos efectivos
  -n, --no-mask             no recalcular la máscara de derechos efectivos
  -d, --default              las operaciones afectan al ACL predeterminado
  -R, --recursive           recorrer subdirectorios recursivamente
  -L, --logical              recorrido lógico, siguiendo enlaces simbólicos
  -P, --physical            recorrido físico, sin seguir enlaces simbólicos
```

Crea una carpeta llamada `PracticaACL`. Dentro de ella crea un fichero llamado `ventas` y una carpeta llamada `Productos`. Dentro de la carpeta llamada `productos` crea un fichero llamado `herramientas` y otro llamado `libros`.

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# tree PracticaACL/
PracticaACL/
├── Productos
│   ├── herramientas
│   └── libros
└── ventas
```

Para ver todos los permisos de `PracticaACL` y sus subdirectorios y ficheros tenemos que usar `getfacl` recursivamente. En este ejemplo la carpeta `PracticaACL` se encuentra en el Escritorio por lo que abro una terminal allí y hago lo siguiente:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL
# file: PracticaACL
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: PracticaACL/Productos
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: PracticaACL/Productos/herramientas
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@dislexia-VirtualBox:/home/dislexia/Escritorio#
```

Ahora, vamos a añadir el grupo contabilidad a los permisos de escritura y lectura del fichero *ventas*.


*r: lectura, w: escritura, x: ejecución*

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl -m group:contabilidad:rw PracticaACL/ventas
```

Comprueba los permisos con `getfacl`.

```
getfacl PracticaACL/ventas
```

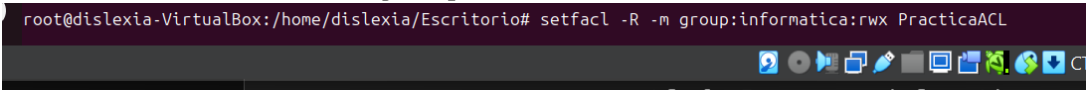
```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl PracticaACL/ventas
# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
group::r--
group:contabilidad:rw-
mask::rw-
other::r--
```



Añade al grupo informática todos los permisos para toda la carpeta *PracticaACL* y su contenido con una sola instrucción.

```
setfacl -R -m group:informatica:rwX PracticaACL
```

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl -R -m group:informatica:rwX PracticaACL
```



Comprueba los permisos con un getfacl recursivo (todo el contenido de la carpeta).

```
getfacl -R PracticaACL
```

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL
# file: PracticaACL
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x

# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
group::r--
group:contabilidad:rw-
group:informatica:rwx
mask::rwx
other::r--

# file: PracticaACL/Productos
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x
```

```
# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--

# file: PracticaACL/Productos/herramientas
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--
```

## Modificar permisos

Nos comunican que el grupo contabilidad no debería poder modificar el fichero ventas, excepto el user1 que sí puede. Por lo que debemos quitarle el permiso de escritura de dicho fichero al grupo y darle permiso únicamente al user1

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl -x group:contabilidad PracticaACL/ventas
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl -m user:user1:rw PracticaACL/ventas
```

Estado final de los permisos:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL
# file: PracticaACL
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x

# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
user:user1:rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--

# file: PracticaACL/Productos
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x
```

```
# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwX
mask::rwX
other::r--

# file: PracticaACL/Productos/herramientas
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwX
mask::rwX
other::r--
```

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio#
```

## Copia de seguridad de ACL

Por último, vamos a guardar una copia de seguridad de los permisos y restaurarla.

Exportar permisos a un fichero:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL > permisosPracticaBackup.txt
root@dislexia-VirtualBox:/home/dislexia/Escritorio# ls
permisosPracticaBackup.txt  PracticaACL
```

El símbolo > se utiliza para escribir en el fichero permisosPracticaACL.txt el resultado del comando getfacl.

Borra todos los permisos de la carpeta PracticaACL dejando los permisos por defecto:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl -R -b PracticaACL
```

Comprueba los permisos con getfacl:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL
# file: PracticaACL
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: PracticaACL/Productos
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```



```
# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: PracticaACL/Productos/herramientas
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@dislexia-VirtualBox:/home/dislexia/Escritorio#
```

Restaura los permisos desde el fichero que creamos antes:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# setfacl --restore=permisosPracticaBackup.txt
```

Comprueba los permisos:

```
root@dislexia-VirtualBox:/home/dislexia/Escritorio# getfacl -R PracticaACL
# file: PracticaACL
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x

# file: PracticaACL/ventas
# owner: root
# group: root
user::rw-
user:user1:rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--

# file: PracticaACL/Productos
# owner: root
# group: root
user::rwx
group::r-x
group:informatica:rwx
mask::rwx
other::r-x
```

```
# file: PracticaACL/Productos/libros
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--

# file: PracticaACL/Productos/herramientas
# owner: root
# group: root
user::rw-
group::r--
group:informatica:rwx
mask::rwx
other::r--

root@dislexia-VirtualBox:/home/dislexia/Escritorio#
```

Esta herramienta nos es útil como sysadmins para poder gestionar permisos en archivos importantes de máquinas como la carpeta "etc" o "boot" en entornos empresariales

He exportado el archivo con los permisos de etc:

```
root@dislexia-VirtualBox:/# getfacl -R etc/ > /home/dislexia/permisosETC.txt
root@dislexia-VirtualBox:/#
```

```
root@dislexia-VirtualBox:/home/dislexia# ls
Descargas Documentos Escritorio Imágenes Música permisosETC.txt Plantillas Público snap Videos
root@dislexia-VirtualBox:/home/dislexia# nano permisosETC.txt
```

```
root@dislexia-VirtualBox: /home/dislexia
GNU nano 7.2 permisosETC.txt
# file: etc/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: etc//group
# owner: root
# group: root
user::rw-
group::r--
other::r--

# file: etc//update-notifier
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

# file: etc//modprobe.d
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

[ 14184 líneas leídas ]
Podemos añadir al usuario local por ejemplo a que tambien pueda
tener control total sobre etc y sus directorios:
root@dislexia-VirtualBox:/# setfacl -R -m u:dislexia:rwx /etc
root@dislexia-VirtualBox:/#
```

Vemos el resultado de este comando:

```
other::r--  
  
# file: etc/apport/crashdb.conf  
# owner: root  
# group: root  
user::rw-  
user:dislexia:rwx  
group::r--  
mask::rwx  
other::r--
```

```
# file: etc/subuid-  
# owner: root  
# group: root  
user::rw-  
user:dislexia:rwx  
group::r--  
mask::rwx  
other::r--
```

```
# file: etc/locale.gen  
# owner: root  
# group: root  
user::rw-  
user:dislexia:rwx  
group::r--  
mask::rwx  
other::r--
```

```
root@dislexia-VirtualBox:/#
```

Revertimos los permisos:

```
root@dislexia-VirtualBox:/home/dislexia# setfacl -R -x u:dislexia /etc
```

Comprobamos que el usuario dislexia ya no este:

```
root@dislexia-VirtualBox: /home/dislexia
# owner: root
# group: root
user::rw-
group::r--
mask::r--
other::r--

# file: etc/subuid-
# owner: root
# group: root
user::rw-
group::r--
mask::r--
other::r--

# file: etc/locale.gen
# owner: root
# group: root
user::rw-
group::r--
mask::r--
other::r--

root@dislexia-VirtualBox: /home/dislexia#
```