Implementar Listas de Control de Acceso

Comandos ACL

Los comandos que usaremos para crear, modificar, eliminar o consultar las *ACL* son:

setfacl : Crea una lista de acceso para un determinado directorio o archivo.

getfacl: Consulta las propiedades de una ACL

Ejemplo práctico 1

IMPORTANTE:

Antes de crear una lista de acceso, por ejemplo del directorio '**/home/usuarios/sistemas**' es conveniente realizar un respaldo de los permisos existentes, para que en caso de que queramos anular la *ACL* en un futuro, podamos usar este backup.

Crear un backup de los permisos para '/home/usuarios/sistemas':

$ getfacl -R /home/usuarios/sistemas > /home/usuarios/Desktop/persistemas.bak

Restaurar los permisos de un directorio en caso de que apliquemos una ACL errónea:

$ setfacl --restore=permsistemas.bak

Con el backup realizado, procederemos a implementar la ACL.

Lo primero será dejar 'limpio' el directorio, es decir, anularemos otras posibles listas de acceso que este pudiese tener o incluso si tuviese una ACL por defecto.

Esto lo haremos con el siguiente comando:

$ sudo setfacl -b -k -R /home/usuarios/sistemas

- **-b** Eliminamos la posible ACL que ya pudiese tener el directorio
- **-k** Eliminamos la posible ACL default que pudiese tener el directorio
- **-R** Aplicamos los cambios de forma recursiva

Ahora con el directorio limpito vamos a crear la ACL, acción que podremos realizar mediante el uso de dos parámetros: '**s**' o '**m**'.

Si quisiéramos crear una ACL eliminando una ya existente usaríamos '***s***', si por el contrario queremos modificar una ACL o crearla si no existe usaremos '***m***'.

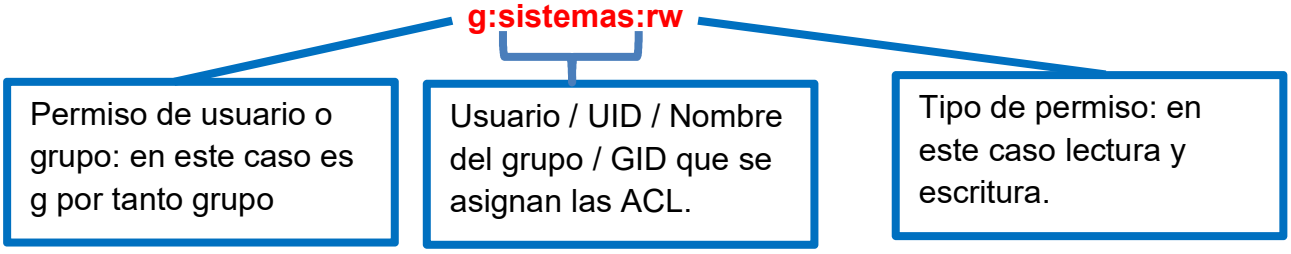
Nosotros usaremos '***m***' ya que antes hemos eliminado todo lo relacionado con ACL en el directorio.

$ sudo setfacl -R -m g:sistemas:rw

Aquí igualmente hemos aplicado de forma recursiva (**-R**) el comando.

Vamos a desglosar la cadena '**g:sistemas:rw**' para ver qué significado tiene cada uno de sus campos.

- Indicar si se trata de una ACL de usuario (**u**) o de grupo (**g**): En nuestro caso, de grupo.
- El segundo campo es el **nombre del grupo** (podemos pasar el GID igualmente): sistemas.
- El tercer y último campo son los **permisos** de la ACL, podemos pasar en valor octal como con chmod: rw.

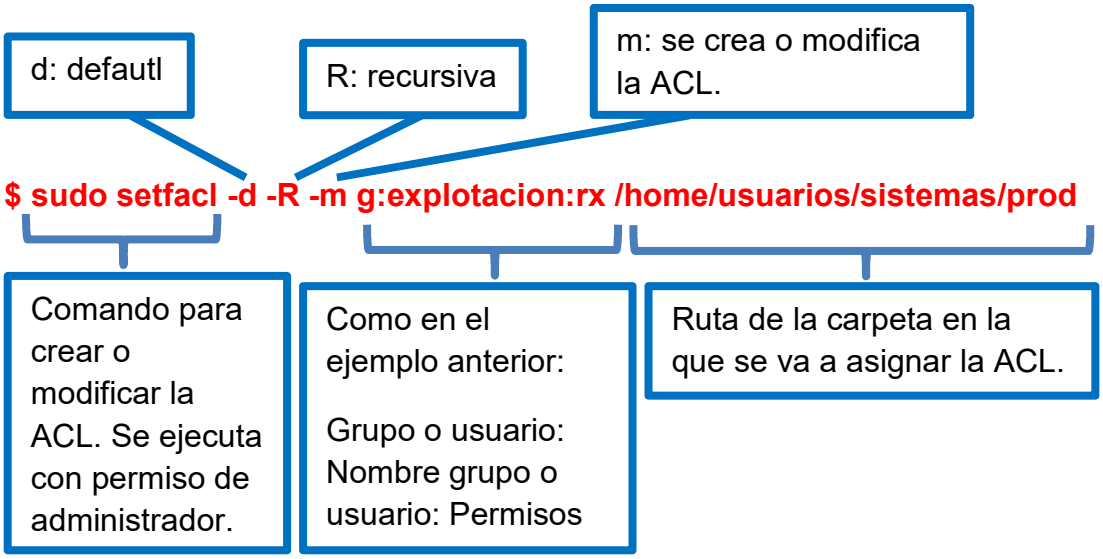


Ejemplo práctico 2

Ahora vamos a darle al grupo de explotación permisos de lectura y acceso para el subdirectorio */home/usuarios/sistemas/prod*

Además algo que no hemos hecho en la anterior ACL es crearla como **default**, **esto implica que cada subdirectorio o archivo que se cree bajo *./prod* heredará los permisos**, muy útil para no tener que andar modificando la ACL continuamente (cada vez que se cree contenido).

Usaremos la opción '**-d**'



Comprobación

Una vez terminadas la tarea de *setear la ACL* es conveniente usar el comando **getfacl** para comprobar como ha quedado todo:

$ sudo getfacl /home/usuarios/sistemas

```
# file: home/usuarios/sistemas
# owner: nebul4ck
# group: nebul4ck
user::rwx
group::r-x
group:sistemas:rw-
mask::rwx
other::r-x
```

Nota: Si hemos usado la opción '**-d**' (default) **getfacl** mostrará además estás entradas:

```
default:user::rwx
default:group::r-x
default:group:sistemas:rw-
default:mask::rwx
default:other::r-x
```

Dónde:

- **user**: permisos para nebul4ck
- **group**: permisos del grupo nebul4ck
- **group**:sistemas: permisos rw- para el grupo sistemas (habrá tantas entradas como ACL hayamos asignado)
- **mask**: Esa entrada se puede manipular con setfacl y permite especificar el máximo de permisos que se pueden asignar en dicho fichero con las ACLs de usuario y grupo.
- **Other**: Es la entrada de los permisos generales o globales del modelo UGO (usergroupother).