Práctica 4.4

Listas de control de acceso (ACL)	
OBJETIVOS	Manejar configuraciones complejas de permisos sobre archivos gracias al sistema de listas de control de acceso (ACL – Access Control Lists).
DOCUMENTACIÓN	"Red Hat System Administrator 's Guide". Sección sobre ACL. Páginas de manual sobre las ACL: **`man acl, man setfacl, man getfacl`**
TIEMPO ESTIMADO	1 hora en laboratorio

1 Conceptos básicos

ACL = Access Control Lists = Listas de Control de Acceso

Utilidad: el esquema básico de Linux (basado en las categorías de propietario, grupo propietario y otros usuarios y permisos) de acceso a los ficheros es poco flexible. La funcionalidad de ACL aumenta esta flexibilidad. Por ejemplo:

- Tenemos un fichero cuyo propietario es el usuario **`root`** con permisos **`755`** (en octal) y se quiere dar acceso de escritura al usuario ***pepe*** y sólo a él. Con el esquema básico no se podría hacer, pero con las ACL sí se puede.
- Tenemos un fichero con acceso pleno (**rwx**) para el grupo ***alumnos***, pero queremos que un usuario ***pepe*** que pertenece a ese grupo NO tenga ningún acceso al fichero. Con el esquema básico no se podría hacer, pero con las ACL sí se puede.

Con las ACL, se pueden dar y quitar permisos discrecionalmente a cualquier usuario o grupo.

2 Configurar las ACL en el sistema

Para utilizar la ACL se deben cumplir dos condiciones:

1. Que el sistema de fichero que alberga a los archivos a los que se les quiere aplicar soporte esta funcionalidad. En relación con esta condición, hay que decir que en los sistemas de archivos antiguos como los de tipo **`ext2`** o **`ext3`** la funcionalidad de ACL está soportada, sin embargo, para utilizarla es necesario especificar la opción **`acl`** cuando se monta un sistema de archivos de este tipo. En sistemas de archivos actuales, tales como **`ext4`**, no es necesario especificar esta opción cuando se procede a montarlos. Las ACL pueden utilizarse también en sistemas de archivos en red, como por ejemplo NFS o SAMBA, siempre y cuando el sistema servidor que proporciona estos tipos de sistemas de archivo esté configurado para soportar esta funcionalidad.
2. Que esté instalado el paquete que contiene los componentes requeridos para usarla. El nombre de este paquete es ***`acl`***.

3 Trabajar con ACL

Para trabajar con ACL, lo primero que se debe hacer es verificar que las dos condiciones anteriores se cumplen. La primera tarea que se propone es que se prepare el sistema para utilizar las ACL.

Las utilidades que usaremos serán las siguientes:

- **`setfacl`** para aplicar permisos ACL sobre ficheros y directorios. Su sintaxis típica es:

  ```
  # setfacl –(m|x|b) regla fichero
  ```

  Las sintaxis admisibles para la regla que se especifica en la orden están descritas en las fuentes de documentación especificadas al principio de esta ficha. Una misma orden puede contener varias reglas separadas por coma.
- **`getfacl`** para consultar los permisos ACL sobre ficheros y directorios. Su sintaxis típica es:

  ```
  # getfacl fichero
  ```

Aplicar ACL a un fichero o directorio

Darle permisos de acceso a un usuario:

`# setfacl -m u:usuario1:rw fichero`

Obtener ACL de un fichero

`# getfacl fichero`

Darle permisos a un grupo:

`# setfacl -m g:usuario1:r fichero`

Dar permisos a usuarios y grupos en una misma orden usando múltiples reglas

`# setfacl -m u:invitado:rwx,g:alumnos:r-x fichero`

Quitarle los ACL a un usuario:

`# setfacl -x u:usuario1: fichero`

Eliminar todas las ACL de un archivo

`# setfacl -b fichero`

ACL por defecto en un directorio

Un directorio puede tener ACL que se aplican por defecto a todos los ficheros que se creen en ese directorio. Estas reglas se aplican por defecto y no afectan a los permisos que pudiera tener los usuarios y grupos de usuarios especificados en la ACL que pudiera tener el directorio. Por tanto, las reglas de acceso específicas de usuarios o grupos de usuarios prevalecen sobre las reglas ACL por defecto. Sin embargo, son heredadas por todos los ficheros descendientes del directorio.

Al archivo creado por el **root** cuya ruta es **/tmp/acl/proyecto/fichero2** se le establece permiso de lectura y escritura al usuario **usuario1**:

```
# setfacl -m u:usuario1:rw /tmp/acl/proyecto/fichero2
```

Al directorio **/tmp/acl/proyecto** se le establece una regla de control de acceso por defecto para el usuario **usuario1**:

```
# setfacl -m d:usuario1:r /tmp/acl/proyecto
```

En el mismo directorio se establece otra regla de control de acceso para los usuarios que no pertenezcan al grupo propietario.

```
# setfacl -m d:o:r /tmp/acl/proyecto
```

Máscara efectiva

La máscara efectiva de la ACL de un fichero es el conjunto máximo de permisos que pueden aplicarse con ACL a un usuario o grupo. Así, por ejemplo, si la máscara efectiva de la ACL de un fichero es "r-x" y se intenta establecer los permisos de acceso **"rwx"** a un usuario para ese fichero, entonces el usuario en cuestión no tendrá permiso de acceso. Se trata de un atributo opcional de la ACL de un fichero.

Establecer regla ACL para permitir al usuario "usuario1" leer el archivo **/tmp/acl/fichero**

```
# setfacl -m u:usuario1:r /tmp/acl/fichero
```

Establecer la regla para permitir al usuario "invitado" modificar el archivo **/home/usuario1/acl/fichero**

```
# setfacl -m u:invitado:r /tmp/acl/fichero
```

Establecer la máscara efectiva de acceso al archivo **/home/usuario1/acl/fichero**

```
# setfcal -m m::r /tmp/acl/fichero
```

4 Tareas propuestas

1. Comprobar que se tiene instalado el paquete **`acl`.** En caso de no tenerlo, entonces instalarlo.
2. En el directorio **`/tmp`**, crear un directorio para pruebas de ACL (**`pruebaACL`**), y dentro de él crear un fichero (**`fichACL`**). Mostrar las listas de control de acceso asociadas al nuevo fichero.
3. Dar permiso de lectura y escritura al usuario **`usuario1`** sobre **`fichACL`**.
4. Entrar con el usuario **`usuario1`** y verificar que puede acceder (o no) a **`fichACL`**. ¿Por qué ocurre esto? A continuación, conceder al usuario **`usuario1`** permisos de lectura y ejecución sobre **`fichACL`**.
5. Comprobar que puede leerse el fichero **`fichACL`**, pero que no pueden crearse otros ficheros dentro del directorio **`pruebaACL`**.
6. Cambiar la máscara efectiva de acceso a **`fichACL`** de forma que no sea posible modificarlo.
7. Establecer una lista de control de acceso por defecto para el directorio **`pruebaACL`**, de forma que los usuarios pertenecientes a la categoría “otros usuarios” tengan permisos de lectura y ejecución.