

Solución 3.1: Configuración de ACLs en Linux

Descripción de la tarea

Esta documentación detalla la configuración de listas de control de acceso (ACLs) en un sistema Linux para gestionar los permisos de acceso a archivos y directorios dentro de un entorno empresarial.

Esquema de Usuarios y Grupos

Cuenta	Grupo Principal	Grupos Secundarios	Shell
sis	sistemas	sudo	bash
des	desarrollo	sudo	bash
exp	explotacion	sudo	bash

Cada usuario tendrá su carpeta personal en `/home` y una contraseña por defecto `abc123...`

Permisos por Grupo

- A. Grupo `sistemas`** Deben tener permisos de lectura, escritura y ejecución en los directorios y subdirectorios. Permisos de lectura y escritura en todos los archivos existentes en el árbol. Pero lo que NO tendrán es permisos de ejecución en los ficheros existentes dentro del subdirectorio binarios.
- B. Grupo `desarrollo`** Deben tener acceso de lectura, escritura y ejecución en todos los directorios del árbol. En los ficheros del directorio raíz y del directorio fuentes sólo de lectura y escritura. Y en los ficheros del directorio binarios tendrán permisos de lectura, escritura y ejecución.
- C. Grupo `explotacion`** Este grupo debe tener acceso en modo lectura y ejecución sobre los ficheros del directorio binarios. Para poder ver lo que hay y navegar por los directorios, tendrán sobre ellos permisos de lectura y ejecución. Eso sí, NO podrán ni acceder al directorio fuentes.
- D. Otros usuarios** El resto de los usuarios del sistema no deben tener ningún tipo de acceso a ninguno de los ficheros o subdirectorios.
- E. ACLs por defecto** Los archivos nuevos que se vayan creando en esos directorios deben tener los mismos permisos que tienen en este momento los archivos existentes.

Estructura de Directorios

```
datosEmpresa/  
|-- fichero1  
|-- fichero2  
|-- fuentes/  
|   |-- fichero3  
|   |-- fichero4  
|-- binarios/
```

```
|-- fichero5  
|-- fichero6
```

Solución

1. Creación del Árbol de Directorios

Creamos árbol de directorios→ en una partición montada con las ACLs activadas.

```
root@debian:~# mkdir -p /datosEmpresa/fuentes /datosEmpresa/binarios  
root@debian:~# echo "Hola" > /datosEmpresa/fichero1  
root@debian:~# echo "Hola" > /datosEmpresa/fichero2  
root@debian:~# echo "Hola" > /datosEmpresa/fuentes/fichero3  
root@debian:~# echo "Hola" > /datosEmpresa/fuentes/fichero4  
root@debian:~# echo "Hola" > /datosEmpresa/binarios/fichero5  
root@debian:~# echo "Hola" > /datosEmpresa/binarios/fichero6
```

```
root@debian:~# tree /datosEmpresa/  
/datosEmpresa/  
├── binarios  
│   ├── fichero5  
│   └── fichero6  
├── fichero1  
├── fichero2  
└── fuentes  
    ├── fichero3  
    └── fichero4
```

2. Creación de Grupos

Creamos los grupos necesarios.

```
root@debian:~# groupadd sistemas  
root@debian:~# groupadd desarrollo  
root@debian:~# groupadd explotacion  
  
root@debian:~# tail -3 /etc/group  
sistemas:x:1006:  
desarrollo:x:1007:  
explotacion:x:1008:
```

3. Creación de Usuarios

Creamos los usuarios.

```
root@debian:~# useradd -d /home/sis -m -p "$(mkpasswd 'abc123..')" -g sistemas -G
sudo -s /bin/bash sis
root@debian:~# useradd -d /home/des -m -p "$(mkpasswd 'abc123..')" -g desarrollo -
G sudo -s /bin/bash des
root@debian:~# useradd -d /home/exp -m -p "$(mkpasswd 'abc123..')" -g explotacion
-G sudo -s /bin/bash exp

root@debian:~# tail -3 /etc/passwd
sis:x:1003:1006::/home/sis:/bin/bash
des:x:1004:1007::/home/des:/bin/bash
exp:x:1005:1008::/home/exp:/bin/bash
```

4. Configuración de ACLs

Eliminamos todas las ACLs, también las default (si aún no configuramos ninguna ACL esta operación no tiene efecto, quedarían como recién creadas).

```
root@debian:~# sudo setfacl -b -k -R /datosEmpresa
```

A. Grupo sistemas

Configuramos al grupo sistemas en todo el árbol como rw-.

```
root@debian:~# setfacl -Rm g:sistemas:rw /datosEmpresa
```

En todos los directorios: rwx.

```
root@debian:~# setfacl -m g:sistemas:rwx /datosEmpresa /datosEmpresa/fuentes
/datosEmpresa/binarios
```

B. Grupo desarrollo

```
root@debian:~# setfacl -R -m g:desarrollo:rw /datosEmpresa
root@debian:~# setfacl -m g:desarrollo:rwx /datosEmpresa /datosEmpresa/fuentes
/datosEmpresa/binarios
root@debian:~# setfacl -m g:desarrollo:rwx /datosEmpresa/binarios/*
```

C. Grupo explotacion

De momento explotacion puede acceder a fuentes porque seguimos teniendo permisos con other. En el apartado D lo resolvemos.

```
root@debian:~# setfacl -m g:explotacion:r-x /datosEmpresa /datosEmpresa/binarios
/datosEmpresa/binarios/*
```

D. Restringir Acceso a Otros Usuarios

```
root@debian:~# setfacl -R -m o::- /datosEmpresa
```

E. Configuración de ACLs por defecto

```
root@debian:~# setfacl -d -m g:sistemas:rw- /datosEmpresa /datosEmpresa/binarios
/datosEmpresa/fuentes/
root@debian:~# setfacl -d -m g:desarrollo:rw- /datosEmpresa /datosEmpresa/fuentes
root@debian:~# setfacl -d -m g:desarrollo:rw- /datosEmpresa/binarios
root@debian:~# setfacl -d -m g:explotacion:r-x /datosEmpresa/binarios
root@debian:~# setfacl -d -m o::- /datosEmpresa /datosEmpresa/binarios
/datosEmpresa/fuentes/
```