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	sl, jefe	bash
des	desarrollo	sl, jefe	bash
exp	explotacion	sl, jefe	bash

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

Requisitos de Permisos

Se debe conseguir lo siguiente:

Consideraciones Previas

- Si se tienen permisos completos sobre un directorio, éstos serán: **rwx**
- Sobre un archivo, los permisos pueden ser:
  - **r--** para lectura.
  - **rw-** para lectura y escritura.
  - **r-x** si es ejecutable y queremos ejecutarlo.

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.

```
$ sudo mkdir datosEmpresa
$ cd datosEmpresa/
$ sudo touch fichero1 && sudo touch fichero2 && sudo mkdir fuentes
$ sudo mkdir binarios
$ cd fuentes/
$ sudo touch fichero3 && sudo touch fichero4
$ cd ..
$ cd binarios/
$ echo '#!/bin/bash' | sudo tee fichero5
$ echo 'echo hola5' | sudo tee -a fichero5
$ echo '#!/bin/bash' | sudo tee fichero6
$ echo 'echo hola6' | sudo tee -a fichero6
$ cd .. && cd ..
$ tree
```

```
.
└── datosEmpresa
├── binarios
│ ├── fichero5
│ └── fichero6
├── fichero1
├── fichero2
└── fuentes
├── fichero3
└── fichero4
4 directories, 6 files
```

2. Creación de Grupos

Creamos los grupos necesarios.

```
$ grupos=( 'sl' 'sistemas' 'desarrollo' 'explotacion' )
$ for g in "${grupos[@]}"; do sudo groupadd $g; done
```

3. Creación de Usuarios

Creamos los usuarios.

```
$ sudo useradd -d /home/sis -m -p "$(mkpasswd 'abc123..')" -g sistemas -G
sl,$(groups jefe | cut -d ' ' -f 4- | tr ' ' ',') -s /bin/bash sis
$ sudo useradd -d /home/des -m -p "$(mkpasswd 'abc123..')" -g desarrollo -G
sl,$(groups jefe | cut -d ' ' -f 4- | tr ' ' ',') -s /bin/bash des
$ sudo useradd -d /home/exp -m -p "$(mkpasswd 'abc123..')" -g explotacion -G
sl,$(groups jefe | cut -d ' ' -f 4- | tr ' ' ',') -s /bin/bash exp
```

4. Configuración de ACLs

A. Grupo `sistemas`

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

```
$ sudo setfacl -b -k -R datosEmpresa/
```

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

```
$ sudo setfacl -R -m g:sistemas:rw datosEmpresa/
```

En todos los directorios: rwx.

```
$ sudo setfacl -m g:sistemas:rwx datosEmpresa/ datosEmpresa/fuentes
datosEmpresa/binarios
$ getfacl -R datosEmpresa/

# file: datosEmpresa/
# owner: root
# group: root
user::rwx
group::r-x
group:sistemas:rwx
mask::rwx
other::r-x
```

B. Grupo `desarrollo`

```
$ sudo setfacl -R -m g:desarrollo:rw datosEmpresa/
$ sudo setfacl -m g:desarrollo:rwx datosEmpresa/ datosEmpresa/fuentes/
datosEmpresa/binarios/
$ sudo setfacl -m g:desarrollo:rwx datosEmpresa/binarios/*
$ getfacl -R datosEmpresa/
# file: datosEmpresa/
# owner: root
# group: root
user::rwx
group::r-x
group:sistemas:rwx
group:desarrollo:rwx
mask::rwx
other::r-x
```

C. Grupo `explotacion`

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

```
$ sudo setfacl -m g:explotacion:r-x datosEmpresa/ datosEmpresa/binarios/
datosEmpresa/binarios/*

$ getfacl -R datosEmpresa/
# file: datosEmpresa/
# owner: root
# group: root
user::rwx
group::r-x
group:sistemas:rwx
group:desarrollo:rwx
group:explotacion:r-x
mask::rwx
other::r-x
```

D. Restringir Acceso a Otros Usuarios

```
$ sudo setfacl -R -m o::- datosEmpresa/
$ sudo getfacl -R datosEmpresa/
# file: datosEmpresa/
# owner: root
# group: root
user::rwx
```

```
group::r-x
group:sistemas:rwx
group:desarrollo:rwx
group:explotacion:r-x
mask::rwx
other::---
```

E. Configuración de ACLs por Defecto

```
$ sudo setfacl -d -m g:sistemas:rw- datosEmpresa/ datosEmpresa/binarios/
datosEmpresa/fuentes/
$ sudo setfacl -d -m g:desarrollo:rw- datosEmpresa/ datosEmpresa/fuentes/
$ sudo setfacl -d -m g:desarrollo:rwx datosEmpresa/binarios/
$ sudo setfacl -d -m g:explotacion:r-x datosEmpresa/binarios/
$ sudo setfacl -d -m o::- datosEmpresa/ datosEmpresa/binarios/
datosEmpresa/fuentes/
$ sudo getfacl -R datosEmpresa/
# file: datosEmpresa/
# owner: root
# group: root
…
other::---
default:user::rwx
default:group::r-x
default:group:sistemas:rw-
default:group:desarrollo:rw-
default:mask::rwx
default:other::---
```