Linux: Sistemas de ficheros y permisos

Alberto Molina Coballes

IES Gonzalo Nazareno

16 de enero de 2021

Recordamos los permisos tradicionales UNIX sobre ficheros:

- Esquema ugoa
- Permisos especiales (SUID, SGID, sticky bit)
- Es una implementación de un sistema de DAC (*Discretionary Access Control*) ya que los usuarios pueden modificar los permisos (chmod)

En el inicio fue ugoa

- Tradicionalmente en UNIX se definen los permisos de ficheros para usuario (u), grupo (g), otros (o) o todos (a)
- Los tres permisos básicos son lectura (r), escritura (w) y ejecución (x)
- Para borrar un fichero necesitamos permiso de escritura y ejecución en el directorio padre
- Un usuario tiene un grupo principal y puede pertenecer a otros grupos
- Los permisos iniciales de un fichero se definen mediante la orden `umask`
- Se puede cambiar el grupo principal en una sesión con `newgrp`
- Notación octal: rwx = 111, rw- = 110, etc.

Permisos especiales de ficheros

- Al establecer *set user identification* (`suid`) sobre un fichero ejecutable, este lo puede ejecutar otro usuario con los permisos del propietario.
- Si el propietario es superusuario puede ser arriesgado
- Ficheros con bit de suid activado:

  `find / -perm /4000`
- Al establecer *set group identification* (`sgid`) sobre un fichero ejecutable, ocurre lo mismo que con suid, pero ahora se aplican los permisos del grupo propietario
- Ficheros con bit de sgid activado:

  `find / -perm /2000`

Permisos especiales de ficheros

- sgid sobre un directorio: Todos los ficheros que se creen heredan el grupo propietario del directorio
- suid y sgid se indican con (s)
- Al activar el *sticky bit* en un directorio, sólo el propietario del fichero podrá borrarlo
- Utilizado en directorios donde varios usuarios pueden escribir (por ejemplo /tmp)
- Muy interesante combinado con sgid
- sticky bit se indica con (t)