

EXPERTO 3 (Secretarios). Comandos permisos

El programa `sudo` (del inglés super user do) es una utilidad de los sistemas operativos tipo Unix, como GNU/Linux, BSD, Mac OS X o Mac OS 11, que permite a los usuarios ejecutar programas con los privilegios de seguridad de otro usuario (normalmente el usuario `root`) de manera segura, convirtiéndose así temporalmente en el otro usuario durante la ejecución del programa. Se instala por defecto en `/usr/bin`.

Por defecto, el usuario debe autenticarse con su contraseña al ejecutar `sudo`. Una vez se ha autenticado el usuario, y si el archivo de configuración `/etc/sudoers` permite dar al usuario acceso al comando requerido, el sistema lo ejecuta.

Existe la opción de habilitar el parámetro `NOPASSWD` con el fin de evitar introducir la contraseña de usuario a la hora de ejecutar el comando.

El archivo de configuración `/etc/sudoers` especifica qué usuarios pueden ejecutar qué comandos en nombre de qué otros usuarios. Como `sudo` es muy estricto con el formato de este archivo, y cualquier error podría causar problemas serios, existe la utilidad `visudo`; ésta opción sirve para comprobar que el fichero `/etc/sudoers` no está siendo utilizado desde otra sesión del usuario `root`, evitando de esta forma la multiedición con posibles corrupciones del fichero.

Un ejemplo de consola, donde el usuario no tiene acceso:

```
[user@hostname ~]$ sudo emacs /etc/sudoers
```

chmod ("change mode", cambiar modo en el idioma inglés) es una llamada al sistema y su comando asociado en el sistema operativo UNIX (estandarizados en POSIX y otros estándares) que permite cambiar los permisos de acceso de un fichero o directorio.

Las opciones del comando `chmod` se especifica del siguiente modo:

```
$ chmod [modificadores] permisos fichero/directorio
```

modificadores es opcional, y puede tomar los valores:

- **-f**: no visualiza los posibles mensajes de error que puedan ocurrir debido a conflictos en la asignación de permisos.
- **-v**: lista los ficheros y directorios a los que se les va aplicando el comando a medida que el mismo se ejecuta
- **-h**:
- **-R**: aplica el comando `chmod` recursivamente a todos los ficheros y de los subdirectorios.
- **-H**:
- **-L**:
- **-P**:
- **-c**: igual a `-v` con excepción que solo lista los ficheros modificados.
- **-E**:

El orden y compatibilidad de los modificadores está dada por:

```
[-fhv] [-R [-H | -L | -P]] [-c | -E]
```

Esto significa que **f**, **h** y **v** pueden ser usados todos a la vez, e independientemente de los valores de los demás modificadores; **H**, **L** y **P** son ignorados salvo que se especifique explícitamente la opción **R**

permisos corresponde a uno de los modos que se describen a continuación, y enumera los tipos de permisos que se brindan a las clases de usuarios.

Por lo tanto, las clases de usuarios a los cuales se les puede asignar los permisos básicos anteriormente mencionados son:

u – usuario: dueño del fichero o directorio

g – grupo: grupo al que pertenece el fichero

o – otros: todos los demás usuarios que no son el dueño ni del grupo

a – todos: incluye al dueño, al grupo y a otros

fichero/directorio fichero o directorio al cual se otorga el permiso

Posee 3 modificadores que permiten realizar la tarea:

- "+" – añade un modo
- "-" – elimina un modo
- "=" – especifica un modo (sobrescribiendo el modo anterior)