Capítulo 7
Permisos de acceso a los archivos

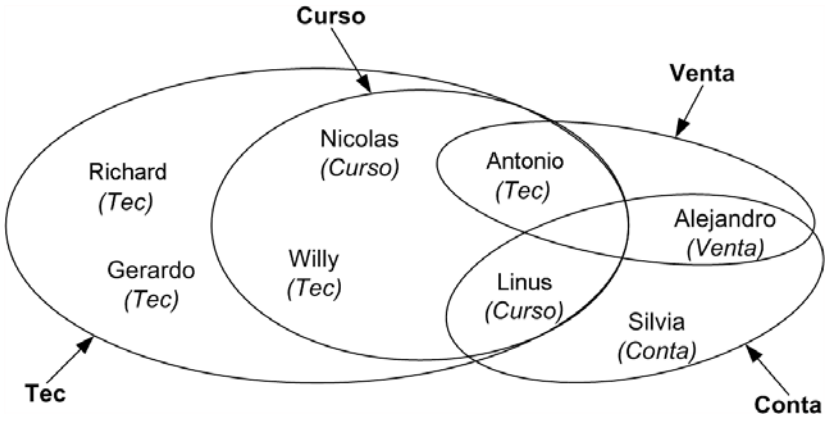
1. Conceptos de cuentas de usuario y de grupos

El sistema GNU/Linux es multiusuario, por tanto las personas que lo usan deben identificarse para asegurar la confidencialidad de los datos contenidos en los archivos. En efecto, no sería aceptable que el usuario "Nicolas" pudiera consultar los archivos personales de "Richard" sin el permiso de este.

Cada una de estas personas dispone por tanto de una "cuenta de usuario" en el sistema; pueden utilizarlo tras ser claramente identificadas. Sin embargo, está permitido compartir archivos entre colaboradores y existe una noción de "grupo de usuarios" en GNU/Linux.

Un usuario debe ser miembro obligatoriamente de un grupo de usuarios en un sistema Unix como GNU/Linux: su grupo principal es el utilizado al crear archivos. Por el contrario, puede pertenecer a otros varios grupos: sus grupos secundarios determinan sus derechos de acceso a los archivos creados por otros miembros de los grupos.

Por ejemplo, si se representa los diferentes servicios de una empresa con su personal, puede observarse que, si bien cada individuo tiene una función primaria (indicada entre paréntesis), algunos pueden asumir varias misiones:



Se observa aquí que:

– Richard y Gerardo pertenecen al servicio técnico (Tec).
– Nicolas, que es ante todo formador (Curso), también forma parte del servicio técnico (Tec).
– Willy, que pertenece al servicio técnico (Tec) principalmente, también trabaja en el departamento de formación (Curso).
– Linus es un formador (Curso) que colabora con los departamentos técnicos (Tec) y de contabilidad (Conta).
– Antonio, del servicio técnico (Tec), ofrece sus competencias al servicio comercial (Venta) y también da clases (Curso).
– Alejandro es un comercial (Venta) que se ocupa también de tareas administrativas (Conta).
– Silvia forma parte únicamente del departamento de contabilidad (Conta).

Para identificar a todos estos usuarios a nivel del sistema operativo, se les atribuye un número único: el UID (*User's ID*); el propietario de un archivo se determina por este número en Unix. Estos usuarios están dotados también de un nombre de usuario único (*login*) y de una contraseña (*password*) para que puedan autenticarse al conectarse al sistema.

De la misma manera, los grupos de usuarios se representan por un nombre único al que se asocia un identificador único: el GID (*Group ID*). Este número se utiliza también para determinar el grupo propietario de un archivo.

1.1 Jerarquía de usuarios

Los usuarios, y por consiguiente las cuentas de usuario, no son todas iguales en Unix. Se pueden distinguir tres tipos de cuentas:

`root`

Es el usuario más importante del sistema desde el punto de vista de la administración. No se ve afectado por los derechos de acceso a los archivos y puede hacer más o menos de todo en el sistema, excepto escribir en un sistema de archivos montado en lectura exclusiva (CD-ROM). Su UID igual a 0 le confiere su especificidad. Este "superusuario" se encarga de las tareas administrativas del sistema. Para evitar errores al trabajar, es muy recomendable utilizar la cuenta administrativa sólo para las tareas que requieren los derechos de superusuario.

`bin`, **`daemon`**, **`sync`**, **`apache`**...

Existe en el sistema una serie de cuentas que no se asignan a personas físicas. Estas cuentas sirven para facilitar la administración de los derechos de acceso de ciertas aplicaciones y demonios. Los UID comprendidos entre 1 y 999 se utilizan generalmente para estas cuentas.

`linus`, **`nicolas`**...

Todas las demás cuentas de usuario se asocian a personas reales; su función es permitir a los usuarios estándar conectarse y utilizar los recursos del equipo. El UID de un usuario es normalmente un número superior o igual a 1000.

Observación

Se denominan "demonios" los programas que se ejecutan como tarea en segundo plano, como un servidor web o un servidor de impresión.

Al igual que las cuentas de usuario, existen diferentes tipos de grupos en un sistema GNU/Linux que permiten dar derechos comunes a una serie de usuarios:

root

Su GID es 0 y es el grupo principal del administrador.

bin, **daemon**, **sync**, **apache**...

Estos grupos tienen la misma función que las cuentas del mismo nombre y permiten dar los mismos derechos de acceso a una serie de aplicaciones. Por convención, los grupos del sistema tienen un GID comprendido entre 1 y 999.

curso, **tec**...

Estos grupos representan una serie de personas reales que deben acceder a los mismos archivos. Típicamente, tienen un GID superior o igual a 1000.

1.2 Comandos útiles

Los comandos **id** y **groups** permiten mostrar información sobre los grupos. El primero da el UID del usuario, el GID de su grupo principal y los GID de todos los grupos a los que pertenece. El segundo sólo proporciona la lista completa de los grupos pero acepta varios nombres de usuario como argumentos:

```
[nicolas]$ whoami
nicolas
[nicolas]$ id
uid=1000(nicolas) gid=1000(curso) grupos=1000(curso),1001(tec)
[nicolas]$ id richard
uid=1002(richard) gid=1001(tec) grupos=1001(tec)
[nicolas]$ groups
curso tec
[nicolas]$ groups gerardo alejandro willy root
antonio : tec curso venta
alejandro : venta conta
willy : tec curso
root : root
```

2. Permisos de Unix

Los permisos de acceso a los archivos determinan las acciones que pueden emprender los usuarios.

Observación

La mayoría de los problemas de instalación, configuración y funcionamiento de las aplicaciones en GNU/Linux se debe a derechos de acceso mal adjudicados.

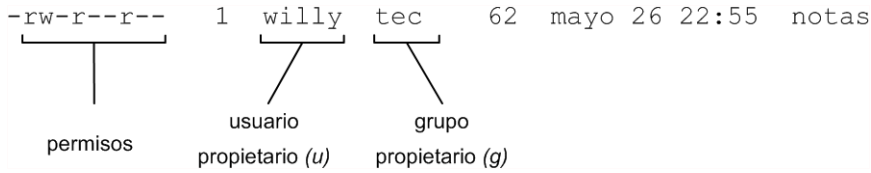
En primer lugar, es necesario saber que los derechos de acceso en Linux se definen por:

- Una cuenta de usuario: propietario del archivo, es en principio el usuario que lo ha creado.
- Un grupo: este grupo es generalmente el grupo principal del propietario del archivo, pero puede ser modificado por este y tomar el valor de uno de sus grupos secundarios.
- Los otros: esta entidad representa toda persona distinta del propietario y que no es miembro del grupo citado anteriormente.

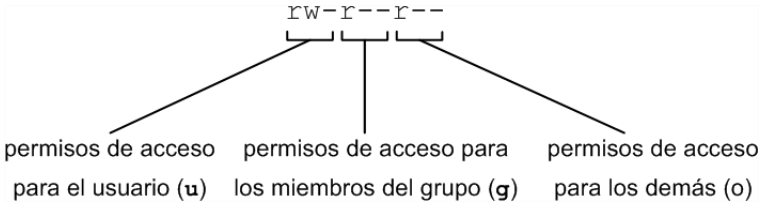
Observación

Los derechos de acceso a un archivo se llaman también "modos" en Unix.

Los derechos, el usuario y el grupo propietarios de un archivo pueden verse con el comando **`ls -l`**:



En este último ejemplo, el archivo pertenece al usuario **willy** y al grupo **tec**; los nueve caracteres **rw-r--r--** definen los derechos de acceso a este archivo para el usuario **willy** (user o **u**), los miembros del grupo **tec** (group o **g**) y los demás (other u **o**). Más exactamente, estos caracteres se distribuyen así:



Todo usuario está asociado, pues, a una de estas entidades para determinar los permisos vigentes.

Observación

Atención: si el usuario es propietario del archivo, se aplican los permisos del propietario, y no los del grupo, aunque el usuario sea también miembro de ese grupo.

El comando GNU **ls** puede añadir un carácter adicional a la sucesión de nueve derechos Unix estándar cuando las autorizaciones especiales están ubicadas. Un punto '**.**' señala un contexto de seguridad SELinux específico y un '**+**' indica que se utiliza otro método de autorización, como las ACL (*Access Control Lists*).

2.1 Permisos estándar

Los permisos de acceso fundamentales en los archivos y directorios en Unix/Linux son los permisos de lectura **r** (*Read*), escritura **w** (*Write*) y ejecución **x** (*eXecute*).

Estos permisos –definidos para las entidades **u**, **g** y **o**– aparecen en el orden **r**, seguido de **w**, seguido de **x** con el comando **ls -l**. Cuando uno de estos caracteres se reemplaza por un guión, significa que el permiso asociado no está otorgado.