
Unidad 4: Gestión de Usuarios y Grupos

**Centro de Formación Permanente
Universidad de Sevilla
Abril-Junio 2010**

Jorge Juan <jjchico@dte.us.es> Abril, 2010

Usted es libre de copiar, distribuir y comunicar públicamente la obra y de hacer obras derivadas bajo las condiciones de la licencia Attribution-Share alike de Creative Commons.

Puede consultar el texto completo de la licencia en <http://creativecommons.org/licenses/by-sa/3.0/>

Abril-Junio, 2010

Administración de Servidores GNU/Linux

1

Contenidos

- Usuarios y grupos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- Usuarios y grupos especiales
- Permisos
- Límites

Abril-Junio, 2010

Administración de Servidores GNU/Linux

2

Usuarios y grupos

- GNU/Linux es un sistema:
 - Multiusuario: varias personas pueden trabajar con el sistema, que proporciona mecanismos de protección de datos de cada usuario.
 - Multitarea: varios procesos (de varios usuarios) pueden ejecutarse a la vez
 - De tiempo compartido: los procesos se ejecutan todos todo el tiempo
- Cuenta de usuario: datos e información de cada usuario. Cada usuario posee un nombre de usuario y una clave para acceder al sistema.
- Grupo de usuarios: cada usuario puede pertenecer a uno o varios grupos
- Permisos: sistema de protección de datos de un usuario respecto de otros.

Usuarios y grupos

- Características de las cuentas de Usuario:
 - Nombre de usuario (“username”)
 - Identifica al usuario dentro del sistema (cada usuario lleva asociado un número de identificación)
 - Clave (password)
 - para acceder al sistema
 - Grupo principal del usuario
 - En Ubuntu “por defecto” se crea un grupo de mismo nombre que el “username”
 - Carpeta personal
 - Donde el usuario guarda sus propias carpetas y archivos (por defecto en /home/username)
 - Otros grupos a los que pertenezca el usuario

Contenidos

- Usuarios y grupos
- **Gestión de usuarios y grupos**
 - **Entorno gráfico**
 - **Interfaz de comandos**
 - **Archivos de configuración**
- Usuarios y grupos especiales
- Permisos
- Límites

Gestión de usuarios y grupos en entorno gráfico

- Sistema -> Administración -> Usuarios y grupos
 - Permite la gestión completa de usuarios y grupos
 - Gestión sencilla de asignación a grupos del sistema mediante "Privilegios del usuario"
 - Propiedades -> Privilegios del usuario

Gestión de usuarios y grupos en interfaz de comandos

- Añadir usuarios:
 - # adduser <username>
- Asignar un usuario a un grupo
 - # adduser <username> <groupname>
- Borrar usuarios:
 - # userdel <username>
- Añadir grupos:
 - # addgroup <groupname>
- Borrar grupos:
 - # groupdel <groupname>

Gestión de usuarios y grupos en interfaz de comandos

- Modificando propiedades de los usuarios y grupos (usermod, groupmod). Ejemplos:
 - # usermod -d /home/profes/pepe -m
cambia la carpeta del usuario pepe a /home/profes/pepe. -m hace que se mueva todo el contenido.
 - # usermod -l joseg pepe:
cambia nombre de usuario pepe por joseg.
 - # usermod -g profes pepe
cambia grupo principal del usuario pepe a profes.
 - #groupmod -n profesores profes
cambia el nombre del grupo profesores a profes

Cambios de propietario/grupo

- Desde el administrador de archivos
 - Menú contextual -> Propiedades -> Permisos
- Cambiar propietarios de archivos/carpetas
 - `chown [-R] <usuario> <ruta>`
 - `chown [-R] <usuario>:<grupo> <ruta>`
- Cambiar grupo de un archivo/carpetas
 - `chgrp [-R] <grupo> <ruta>`

Gestión de usuarios y grupos. Archivos de configuración

- Opciones por defecto al crear usuarios:
 - `/etc/adduser.conf`
- Contenido inicial de las nuevas cuentas de usuarios:
 - `/etc/skel`
- Ficheros con información sobre usuarios y grupos.
Normalmente no se editan "a mano"
 - `/etc/passwd`: Usuarios, ID, grupo principal, carpeta inicio, shell, etc.
 - `/etc/shadow`: continen los passwords encriptados de los usuarios.
 - `/etc/group`: Grupos, miembros de cada grupo.
 - Se usa "vipw" y "vigr" para editarlos con seguridad

Contenidos

- Usuarios y grupos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- **Usuarios y grupos especiales**
- Permisos
- Límites

Usuarios y grupos especiales

- Usuarios y/o grupos empleados por el sistema para realizar tareas concretas con privilegios restringidos
 - cupsys: administrador de impresoras
 - mail: gestor de correo
 - www-data: servidor web
 - ...
- Grupos para el control de privilegios
 - cdrom: control de las unidades de cd o dvd
 - floppy: control de las unidades de diskette
 - audio: control de los dispositivos de audio
 - admin: dota de permisos de administrador del sistema a sus miembros (a través de sudo)

Usuarios y grupos especiales. Superusuario

- Superusuario = administrador = root
- Superusuario -> privilegios ilimitados
- Los sistemas GNU/Linux se configuran para realizar el mínimo de tareas empleando el superusuario
- Convertirse en otro usuario
 - `$ su [-] <nuevo_usuario>`
- Ejecutar un comando como superusuario (sólo usuarios grupo admin)
 - `$ sudo ...`
- Convertirse en root permanentemente
 - `$ sudo -s`
 - `$ sudo su`

Contenidos

- Usuarios y grupos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- Usuarios y grupos especiales
- **Permisos**
- Límites

Permisos

- Cada archivo/carpeta tiene un propietario y está asignado a un grupo (al que normalmente pertenece el propietario)
- Cada archivo/carpeta posee tres conjuntos de permisos que controlan el acceso de:
 - El propietario (user)
 - Miembros del grupo al que pertenece el archivo (group)
 - Otros usuarios (other)

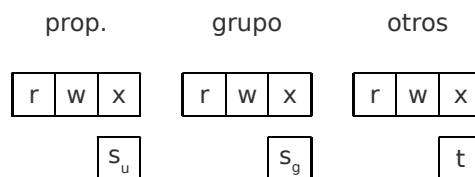
Permisos básicos

	r (lectura/ listado)	w (escritura)	x (ejecución/ acceso)
Archivo	se puede leer el contenido del archivo	se puede cambiar el contenido del archivo	se puede ejecutar el archivo como un programa
Carpeta	se puede listar el contenido de la carpeta	se pueden crear archivos en la carpeta	se puede establ

Permisos especiales

	set-uid (su)	set-gid (sg)	sticky (t)
Archivo (ejecutable)	ejecución con privilegios del propietario	ejecución con privilegios del grupo (no se usa)	hacer residente (no se usa)
Carpeta	(no se usa)	crea nuevos archivos con el grupo de la carpeta padre	permiso de escritura sólo para propietario del archivo (/tmp)

Permisos. Notación



- lectura: r
- escritura: w
- ejecución: x
- set-uid: s
- set-gid: S
- sticky: t
- x -> x
- s -> x + s
- S -> sólo "s"
- t -> x + t
- T -> sólo "t"

Permisos

- Gestionar permisos. Administrador de archivos
 - Menú contextual -> Propiedades -> Permisos
- Gestionar permisos
 - Comando chmod
- Cambiar propietarios de archivos/carpetas
 - # chown [-R] <usuario> <ruta>
 - # chown [-R] <usuario>:<grupo> <ruta>
- Cambiar grupo de un archivo/carpeta
 - # chgrp [-R] <grupo> <ruta>

Permisos. chmod

```

                                r
                                w
                                x
                                X
chmod [-R]  u  +  X  <rutas>
              g  -  s
              o  =  t
              a
                                u
                                g
                                o
```

Permisos. chmod

especial	prop.	grupo	otros												
<table border="1"><tr><td>s_u</td><td>s_g</td><td>t</td></tr></table>	s_u	s_g	t	<table border="1"><tr><td>r</td><td>w</td><td>x</td></tr></table>	r	w	x	<table border="1"><tr><td>r</td><td>w</td><td>x</td></tr></table>	r	w	x	<table border="1"><tr><td>r</td><td>w</td><td>x</td></tr></table>	r	w	x
s_u	s_g	t													
r	w	x													
r	w	x													
r	w	x													
<table border="1"><tr><td>0</td><td>0</td><td>0</td></tr></table>	0	0	0	<table border="1"><tr><td>1</td><td>1</td><td>0</td></tr></table>	1	1	0	<table border="1"><tr><td>1</td><td>0</td><td>0</td></tr></table>	1	0	0	<table border="1"><tr><td>0</td><td>0</td><td>0</td></tr></table>	0	0	0
0	0	0													
1	1	0													
1	0	0													
0	0	0													
(0)	6	4	0												
<table border="1"><tr><td>0</td><td>1</td><td>0</td></tr></table>	0	1	0	<table border="1"><tr><td>1</td><td>1</td><td>1</td></tr></table>	1	1	1	<table border="1"><tr><td>1</td><td>0</td><td>1</td></tr></table>	1	0	1	<table border="1"><tr><td>1</td><td>0</td><td>1</td></tr></table>	1	0	1
0	1	0													
1	1	1													
1	0	1													
1	0	1													
2	7	5	5												

chmod [-R] <código octal> <rutas>

Permisos

- Ejemplos

```
$ chmod g+r carta.txt
$ chmod a+x programa
$ chmod go-rw proyecto.odt
$ chmod g+s mi_carpeta
$ chmod -R a+rX carpeta_web
$ chmod g=u carta.txt
$ chmod 775 carpeta_web
$ chmod 2750 proyecto
```

Permisos

- La combinación de usuarios, grupos y permisos permite establecer múltiples políticas de privacidad.
- Ejemplos:
 - Contenido privado del usuario: quitar todos los permisos a grupo y otros
 - Compartir contenido privado entre varios usuarios
 - Crear un grupo con todos los usuarios implicados
 - Asociar contenidos a ese grupo
 - Establecer permisos de grupo: ej: lectura+escritura
 - Quitar todos los permisos para otros
 - Contenido público que sólo algunos usuarios pueden modificar
 - Como anterior, con permiso de lectura/acceso para otros

Contenidos

- Usuarios y grupos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- Usuarios y grupos especiales
- Permisos
- **Límites**

Límites de recursos

- Existen diversos sistemas para imponer límites a los usuarios y sus procesos, como:
 - tamaño máximo de archivo
 - máximo número de archivos abiertos
 - máxima cantidad de memoria asignable
 - tiempo de CPU máximo
 - máximo número de proceso
 - máximo número de accesos al sistema
 - máxima prioridad de los procesos
- Estos límites se configuran mediante reglas en el archivo **/etc/security/limits.conf** y otros similares

Límites de recursos

- Por otra parte, existen diversos programas que proporcionan límites horarios o de tiempo de acceso al sistema (timeoutd, etc.)
- La utilidad de estos sistemas de limitación de recursos está sobre todo en:
 - Estaciones de trabajo con gran número de usuarios, lo cual es cada vez menos frecuente.
 - Servidores con servicios complejos que tiendan a ocupar muchos recursos, como medida para evitar que se colapse el sistema.