
Unidad 4: Gestión de Usuarios y Grupos

VI Curso de Introducción a la Administración de Servidores GNU/LINUX
Extensión Universitaria. Universidad de Sevilla
Febrero-Abril 2009

Autor: Jorge Juan <jjchico@gmail.com>

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/>

Contenidos

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

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

- Los permisos para cada conjunto (propietario, grupo, otros) son de tres tipos:
 - Lectura (r)
 - Escritura (w)
 - Ejecución (x)
- Existen tres permisos especiales:
 - Persistente (t)
 - Propietario efectivo (s)
 - Grupo efectivo (s)
- El significado de los permisos es diferente si se trata de una carpeta o un archivo.

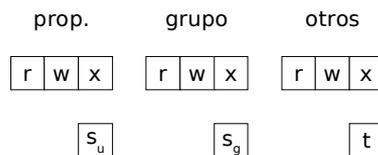
Permisos

- Archivos. Permisos convencionales
 - Lectura (r): acceder al contenido del archivo
 - Escritura (w): modificar el contenido del archivo
 - Ejecución (x): ejecutar el archivo como un programa (ejecutable binario o script)
- Archivos. Permisos especiales (sólo afecta a ejecutables)
 - Persistente (t): el código del programa permanece cargado en memoria aun cuando el programa ha finalizado (obsoleto)
 - Propietario efectivo (s): el proceso se ejecuta con privilegios del propietario del archivo, no del usuario que lo ejecuta
 - Grupo efectivo (s): el proceso se ejecuta con privilegios del grupo del archivo, no del grupo del usuario que lo ejecuta (poco útil)

Permisos

- Carpetas. Permisos convencionales
 - Lectura (r): listar contenidos de la carpeta
 - Escritura (w): crear nuevos archivos o carpetas en la carpeta
 - Ejecución (x): acceder a la carpeta (controla la ejecución de "cd")
- Carpetas. Permisos especiales
 - Persistente (t): sólo el propietario de la carpeta o el propietario del contenido puede borrar/modificar el contenido (usado en /tmp)
 - Propietario efectivo (s): (no se usa)
 - Grupo efectivo (s): el contenido creado hereda el grupo de la carpeta, no del proceso que lo crea. Carpetas creadas heredan el bit de grupo efectivo.

Permisos



- x -> x
- s -> x + s
- S -> sólo "s"
- t -> x + t
- T -> sólo "t"

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

Permisos

- Gestionar permisos. 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>
- Gestionar permisos
 - Comando chmod

Permisos. chmod

```

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

Permisos. chmod

especial	prop.	grupo	otros
s_u s_g t	r w x	r w x	r w x
0 0 0	1 1 0	1 0 0	0 0 0
(0)	6	4	0
0 1 0	1 1 1	1 0 1	1 0 1
2	7	5	5

chmod [-R] <código octal> <rutas>

-
- 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
```

Contenidos

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

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
- Permisos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- **Usuarios y grupos especiales**
- Cuotas de disco
- 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 acceso a dispositivos
 - 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
- Permisos
- Gestión de usuarios y grupos
 - Entorno gráfico
 - Interfaz de comandos
 - Archivos de configuración
- Usuarios y grupos especiales
- **Cuotas de disco**
- Límites

Cuotas de disco. Introducción

- El sistema de cuotas de disco permite establecer límites al espacio ocupado en un sistema de archivos por un usuario o grupo de usuarios
- Los límites no son aplicables a carpetas independientes
- Ayuda a evitar fallos por saturación del sistema de archivos
- Solo pueden aplicarse cuotas a los sistemas de archivos que lo soportan: ext3, reiserfs, xfs, ...

Cuotas de disco. Configuración

- Soporte para cuotas en el kernel: suele estar incluido.
- Instalación de programas de control de cuotas (paquete "quota")
- Incluir opción al montar los s.f. en /etc/fstab

```
# /etc/fstab: static file system information.
#
# <file system> <mount point> <type> <options> <dump> <pass>
...
/dev/hda1 / ext3 defaults,usrquota,grpquota 0 1
/dev/hda5 /home reiserfs defaults,usrquota,grpquota 0 2
...
```

- Iniciar el sistema de cuotas, preferiblemente sin actividad en el sistema (runlevel 1)

```
# quotacheck -avug
...
```

Cuotas de disco. Activar/desactivar

- La aplicación de cuotas puede activarse o desactivarse con “quotaon” y “quotaoff”

```
# quotaon /dev/hda5
...
# quotaon -av
...
# quotaoff -a
...
```

- El estado de activación de cuotas puede consultarse con “quotaon -p”:

```
# quotaon -pa
group quota on /home (/dev/hda5) is off
user quota on /home (/dev/hda5) is on
group quota on /opt (/dev/hda6) is off
user quota on /opt (/dev/hda6) is on
```

Cuotas de disco. Editar

- La cuota asignada a un usuario se edita con edquota

```
# edquota jjchico
...
Disk quotas for user jjchico (uid 1000):
Filesystem  blocks      soft    hard    inodes    soft    hard
/dev/hda5   253876    400000  500000     0         0         0
/dev/hda6   1340144      0         0    22202     0         0
```

- También puede asignarse a un usuario las mismas cuotas que a otro usuario de referencia

```
# edquota -p jjchico bellido
#
```

Cuotas de disco. Comprobar

- Para ver las cuotas de todos los usuarios:

```
# repquota /home
...
# repquota -a
...
```

- Para comprobar la consistencia de la información de cuotas (automáticamente al iniciar):

```
# quotacheck -a
...
```

Contenidos

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