
Gestión de cuentas de usuario

Diseño y Administración de Sistemas y Redes

Juan Céspedes <cespedes@gsync.es>



Curso 2005–2006



Usuarios y grupos

- Cada usuario tiene un identificador (*UID*), un grupo principal al que pertenece (*GID*), una serie de grupos adicionales, un nombre de usuario (*login*), un directorio de trabajo ($\$HOME$).
- Cada usuario puede tener dos tipos de recursos en un sistema UNIX: procesos y ficheros.
- Cada proceso tiene asociado un UID, un GID y una serie de grupos adicionales.
- Cada proceso tiene asociado únicamente un UID y un GID.
- La orden `id` nos da el UID, el GID y los grupos adicionales del proceso que ejecuta la orden.

Usuarios y grupos (2)

- Cada UID y cada GID puede tener asociado un nombre, especificado en los ficheros `/etc/passwd` y `/etc/group`, respectivamente.
- La información de `/etc/passwd` y `/etc/group` la utilizan diversas órdenes de administración, pero su existencia no es imprescindible para que un sistema funcione.
- Del mismo modo, si la información de estos ficheros no es coherente, el sistema seguirá funcionando, pero algunas órdenes pueden fallar de distintas maneras.

`/etc/passwd`

- Contiene la información de todos los usuarios del sistema.
- Contenido: líneas con campos separados por dos puntos:
`login:passwd:UID:GID:info:home-dir:shell`
- El campo "`passwd`" contiene la contraseña cifrada (con DES o con MD5) y puede estar en otro fichero, en el `/etc/shadow`.
- El campo "`info`" contiene el nombre real del usuario e información adicional como el teléfono, etc.
- En algunos sistemas, puede haber información externa (NIS, LDAP...)
- Programas que lo utilizan directamente: `login`, `su`, `passwd`.

/etc/group

- Nombres de grupos del sistema, y miembros de cada grupo.
- Contenido: líneas con campos separados por dos puntos:
nombre:passwd:GID:lista-logins
- “*lista-logins*” son usuarios separados por comas que pertenecen a ese grupo.
- El campo “*passwd*” no se suele utilizar, casi siempre está bloqueado (“*”). Lo utilizan únicamente las órdenes **sg** y **newgrp**. Si se usa, puede estar en otro fichero, en el `/etc/gshadow`.
- En algunos sistemas, puede haber información externa (NIS, LDAP...)

/etc/shadow

- Si existe, contiene las contraseñas cifradas de los usuarios del sistema.
- Contenido: líneas con campos separados por dos puntos:
login:passwd:a:b:c:d:e:f:g
 - a*: momento en que la *passwd* fue cambiada por última vez.
 - b*: días que deben pasar antes de que pueda cambiarse.
 - c*: días después de los cuales la *passwd* debe cambiarse.
 - d*: días antes de la expiración para avisar al usuario.
 - e*: días después de la expiración para desactivar la cuenta.
 - f*: momento en que la cuenta se ha desactivado.
 - g*: campo reservado.

Añadir un usuario al sistema

- Elegir un *login*, un UID y un GID para el nuevo usuario.
- Decidir a qué grupos adicionales debe pertenecer.
- Modificar `/etc/passwd`, `/etc/shadow`, `/etc/group`.
- Crear el directorio HOME (normalmente `/home/login`), con el UID y el GID adecuados.
- Copiar los ficheros de inicio de la cuenta (desde `/etc/skel`).
- Todas estas tareas están automatizadas y las lleva a cabo la orden `adduser`.

Desactivar un usuario del sistema

- Bloquear su contraseña en el `/etc/passwd` o `/etc/shadow` (añadiendo un carácter “-” o “*”, por ejemplo).
- Eliminar sus tareas periódicas (`/var/spool/cron`).
- Revisar `/etc/aliases` y `.forward` por si el usuario tuviera acciones a realizar con el correo recibido.
- Revisar sus ficheros de personalización, haciendo hincapié en `.forward` `.rhosts` `.shosts` `.ssh/authorizedkeys`

Eliminar un usuario del sistema

- Hay que deshacer el proceso de creación de cuenta: modificación de `/etc/passwd`, `/etc/shadow`, `/etc/group`.
- Eliminar `/home/login` y cualquier otro fichero que pueda tener en el sistema (en el `/tmp`, etc).
- Eliminar sus tareas periódicas (`/var/spool/cron`).
- Eliminar su correo (`/var/mail/login`).
- La orden `deluser` se encarga de hacer la mayor parte de estas tareas.

Elección de la palabra clave

- El campo `passwd` en el `/etc/passwd` y el `/etc/shadow` se encuentra cifrado para evitar que los usuarios (y administradores) puedan conocer las contraseñas de otros usuarios.
- Se usa un cifrado de un solo sentido: no existe algoritmo para averiguar la contraseña a partir de estos ficheros.
- Pero se pueden probar varias contraseñas, hasta millones por segundo (John the Ripper).
- Es imprescindible elegir palabras clave seguras, que no aparezcan en diccionarios, evitando nombres o fechas significativas, combinando símbolos, y de la mayor longitud posible.

Ficheros de personalización

- Residen en el directorio de inicio (`$HOME`).
- Cada intérprete, cada programa, cada orden puede usar ficheros distintos.
- Su nombre suele comenzar por “.”
- `bash: .profile .bash_profile .bashrc .bash_history`
- `ssh: .rhosts .shosts .ssh/`
- *e-mail*: `.forward`

Usuarios especiales

- No todas las líneas del `/etc/passwd` corresponden con usuarios físicos.
- Super-usuario: `uid=0` (su *login* es normalmente `root`).
- Otros usuarios del sistema: se utilizan para:
 - tareas específicas de administración
 - propietarios de determinados ficheros del sistema
 - ejecución de determinadas aplicaciones (bases de datos, servidores de web, ftp, e-mail, noticias, etc)
- Normalmente, los usuarios normales tienen UIDs entre el 1000 y el 30000.

Proceso de *login*

- Para que un usuario *entre* en el sistema, algún servicio (*getty*, *ssh*, *telnetd*, etc) ejecuta un proceso de *login*:
 - Se comprueba el nombre de usuario y la contraseña (en el */etc/passwd* y */etc/shadow*).
 - Se comprueban posibles restricciones de acceso (contraseña caducada, etc) en el */etc/shadow*.
 - Registro de usuarios: */var/run/utmp*, */var/log/wtmp*.
 - *setuid()*, *setgid()*, *setgroups()*.
 - *chdir(HOME)*.
 - *exec(SHELL)*.

Registro de usuarios

- Cada vez que un usuario realiza un proceso de *login* o de *logout* en el sistema, se modifican los ficheros */var/run/utmp* y */var/log/wtmp*.
- Ambos son ficheros con contenido binario, no se pueden consultar ni editar directamente con un editor de texto.
- */var/run/utmp*: usuarios conectados.
 - Se puede consultar con *"who"*, *"w"* o *"finger"*.
- */var/log/wtmp*: registro de usuarios pasados.
 - Se puede consultar con *"last"* o *"who /var/log/wtmp"*.

Cambio de contraseña

- Para cambiar la contraseña y otros datos se utilizan las órdenes `passwd` (contraseña), `chfn` (info), `chsh` (*shell*):
 - Estas órdenes tienen *set-uid* para que un usuario normal pueda modificar información privilegiada.
 - Antes de nada, piden la *passwd* del usuario para verificar que es quien dice ser.
 - Bloquean cada fichero a modificar para asegurar exclusión de accesos.
 - Realizan las modificaciones.
 - Desbloquean ficheros.

Cambios de usuario y grupo

- `su` ejecuta otra *shell* bajo un usuario distinto.
- `sg` y `newgrp` ejecutan una *shell* con distinto GID.
 - Estas órdenes tienen *set-uid* para poder realizar las llamadas al sistema `setuid()`, `setgid()` y `setgroups()`.
 - “`su`” sin argumentos cambia a usuario con `uid=0` (`root`).
 - “`su`” pide la contraseña del usuario destino (salvo si el origen es `root`).
 - “`sg`” y “`newgrp`” permiten cambiar el GID a otro grupo al que pertenezcamos (según el `/etc/group`) sin contraseña, o piden contraseña del grupo nuevo.