Tema 4.

Gestión de Usuarios

Administración de Sistemas Operativos

Administración de Sistemas Operativos y Periféricos

Mª Pilar González Férez

Índice

1. Introducción

- Definición de **usuario** o **user**
  - Persona que trabaja en el sistema (edita ficheros, ejecuta programas, etc.)
  - **Pseudo-usuario**: entidad que puede ejecutar programas o poseer ficheros (normalmente tienen identificadores de 0 a 100)
- Características de un usuario:
  - Nombre de usuario, (también conocido como *logname* o *username*)
  - Identificador de usuario (UID) $\Rightarrow$ internamente el sistema identifica al usuario por su UID, y no por su nombre
  - Grupos a los que pertenece (GID's)
- Ficheros de configuración:
  - `/etc/passwd` $\Rightarrow$ Información de las cuentas de usuarios
  - `/etc/shadow` $\Rightarrow$ Password encriptados e información de «envejecimiento» de las cuentas
  - `/etc/group` $\Rightarrow$ Definición de los grupos y usuarios miembros

2. Usuarios

Añadir un nuevo usuario al sistema

- Pasos a realizar (herramientas específicas los hacen automáticamente):
  1. Decidir el nombre de usuario, el UID, y los grupos a los que va a pertenecer (grupo primario y grupos secundarios)
  2. Introducir los datos en los ficheros `/etc/passwd` y `/etc/group` (poniendo la contraseña "*" para bloquear la cuenta y que no se pueda usar)
  3. Asignar un password a la nueva cuenta
  4. Si las **shadow** están activas, «reactivarlas»
  5. Establecer los parámetros de «envejecimiento» de la cuenta
  6. Crear el directorio «HOME» del nuevo usuario, establecer el propietario y grupo correspondiente y los permisos adecuados
  7. Copiar los ficheros de inicialización (`.bash_profile`, `.bashrc`,...)
  8. Establecer otras facilidades: quotas, mail, permisos para imprimir, etc.
  9. Ejecutar cualquier tarea de inicialización propia del sistema
  10. Probar la nueva cuenta

2. Usuarios (ii)

Fichero `/etc/passwd`

- Contiene la lista de usuarios definidos en el sistema
- Formato: *nombre:password:uid:gid:gecos:home:shell*
  - nombre ⇒ Nombre del usuario, **logname** o **username**
  - password ⇒ contraseña cifrada o:
    - «*» o «!!» ⇒ la cuenta está desactivada o bloqueada
    - «x» ⇒ las *shadow* están activas, la contraseña cifrada se guarda en `/etc/shadow`
  - uid ⇒ identificador del usuario
  - gid ⇒ identificador del grupo primario al que pertenece
  - gecos ⇒ campo de información referente al usuario (nombre, teléfono, . . .)
  - home ⇒ Path del directorio «HOME» del usuario
  - shell ⇒ Intérprete de órdenes que se ejecutará al entrar al sistema
- `/usr/sbin/vipw` ⇒ Para editar el fichero manualmente
- El usuario propietario es el **root** y el grupo **root**
- ¡OJO! Sus permisos son *rw_r___r___*

2. Usuarios (iii)

Contraseñas

- `passwd <nombre_usuario>` $\Rightarrow$ asignar contraseña a un usuario (o cambiarla)
- A la hora de elegir una buena contraseña:
  - No utilizar:
    - Tu nombre o parte de él, o de alguien cercano a ti
    - Nº's significativos para ti o alguien cercano a ti
    - Algún nombre, nº, lugar, gente, etc., asociado a tu trabajo
    - Palabra que esté en un diccionario (español, inglés, etc.)
    - Nombre de gente famosa, lugares, películas, relacionadas con publicidad, etc.
  - Consejos:
    - Introducir 2 o más caracteres extras, símbolos especiales o de control
    - Escribir mal las palabras
    - Utilizar mayúsculas y minúsculas, pero no de forma evidente
    - Concatenar, embeber o mezclar 2 o más palabras, o partes de palabras
    - Usar caracteres poco comunes, como por ejemplo $, &, # , ^

2.3 Contraseñas

- La contraseña se debe cambiar cuando:
  - Se sospecha que alguien la ha podido conocer o averiguar
  - Un usuario se marcha del trabajo $\Rightarrow$ cambiar todas las que conozca
  - Un administrador del sistema se va: TODAS
  - Se despide a un usuario o a un administrador
  - Se sospecha que alguien ha conseguido el fichero con las contraseñas (tanto `/etc/passwd` como `/etc/shadow`)
  - Un intruso ha conseguido entrar en el sistema
- Periódicamente, se debe forzar a que los usuarios cambien sus contraseñas, incluido el administrador
- Por otro lado, si se obliga a los usuarios a cambiar su contraseña con mucha frecuencia, lo normal es que elijan malas contraseñas, fáciles de adivinar
- El administrador debe cambiar su password periódicamente

2. Usuarios (iv)

Shadow passwords

- Permiten que las contraseñas encriptadas no se guarden en el fichero `/etc/passwd` sino en `/etc/shadow` (que es más seguro)
- `/etc/shadow` tiene los permisos *r*_____, el usuario propietario es el **root** y el grupo propietario el **root**
- Este fichero guarda para cada una de las cuentas del sistema, la **contraseña encriptada** junto con su información de **envejecimiento**
- En el campo «password» del fichero `/etc/passwd` aparecerá una «x» (indicando que las "shadow" están activas)
- Por defecto, están activas y se actualizan automáticamente
- *nom:pass:changed:minlife:maxlife:warn:inactive:expired:unused*
  - **nom** $\Rightarrow$ nombre del usuario, logname o username
  - **pass** $\Rightarrow$ contraseña encriptada
- `pwconv` $\Rightarrow$ crear y actualizar el fichero `/etc/shadow`
- `pwunconv` $\Rightarrow$ desactivar los shadow passwords

2. Usuarios (v)

Restricciones de tiempo

- Para las cuentas de los usuarios se pueden establecer restricciones de tiempo o envejecimiento respecto a su validez o su contraseña
- Los valores se guardan en el fichero `/etc/shadow`:
  - **changed** $\Rightarrow$ fecha del último cambio de password
  - **minlife** $\Rightarrow$ nº de días que han de pasar para poder cambiar la contraseña
  - **maxlife** $\Rightarrow$ nº de días máximo que puede estar con la misma contraseña sin cambiarla
  - **warn** $\Rightarrow$ cuántos días antes de que la contraseña expire (*maxlife*) será informado sobre ello, indicándole que tiene que cambiarla
  - **inactive** $\Rightarrow$ nº de días después de que la contraseña expire que la cuenta se deshabilitará de forma automática si no ha sido cambiada
  - **expired** $\Rightarrow$ fecha en la que la cuenta expira y se deshabilita de forma automática

2.5 Restricciones de tiempo

- Los valores los establece el administrador con las órdenes `chage` o con `passwd`
- El fichero `/etc/login.defs` tiene los valores por defecto
- El uso de la orden `chage`
  - *`chage -d ult_día usuario`* $\Rightarrow$ fecha del último cambio de password
  - *`chage -m min_días usuario`* $\Rightarrow$ nº de días que han de pasar para poder cambiar la contraseña
  - *`chage -M max_días usuario`* $\Rightarrow$ nº de días máximo que puede estar con la misma contraseña sin cambiarla
  - *`chage -W warn_días usuario`* $\Rightarrow$ cuántos días antes de que la contraseña expire (maxlife) será avisado de ello, indicándole que tiene que cambiarla
  - *`chage -I inac_días usuario`* $\Rightarrow$ nº de días después de que la contraseña expire que la cuenta se deshabilitará de forma automática si la contraseña no ha sido cambiada
  - *`chage -E exp_días usuario`* $\Rightarrow$ fecha en la que la cuenta expira y se deshabilita de forma automática

2. Usuarios (vi)

Ficheros de inicialización

- En el directorio `/etc/skel` se guardan unos ficheros «personalizados» que se copian cuando se crea una cuenta al directorio *HOME* asignado
- Posteriormente, cada usuario podrá personalizar los suyos (están en su `$HOME`)
- Los ficheros de inicialización son guiones shell que realizan determinadas tareas como inicializar variables, ejecutar funciones específicas, establecer los alias, etc.
- Estos ficheros dependen del intérprete de órdenes seleccionado:

Se ejecuta al hacer un login (PATH, variables de entorno, umask, funciones de inicialización, etc.)	`.bash_profile` en Bourne Again Shell (bash) `.profile` en Bourne Shell (sh) `.login` en C Shell (csh)
Cada vez que se ejecuta un shell (alias, var. del propio shell, etc.)	`.bashrc` en Bourne Again Shell (bash) `.cshrc` en C Shell (csh)
Al salir del sistema el usuario (al finalizar la sesión)	`.bash_logout` en Bourne Again Shell (bash) `.logout` en C Shell (csh)

2. Usuarios (vii)

Asignar o cambiar de intérprete de órdenes

- En el último campo del fichero `/etc/passwd` se establece el intérprete de órdenes que se ejecuta al entrar al sistema
- En el fichero `/etc/shells` se indican los shells permitidos (¡Ojo! Si se prohibe un shell, no se podrá elegir con `chsh`, pero los usuarios que ya lo tenían asignado lo seguirán usando sin problemas)
- Con la orden `chsh` el usuario puede cambiar su shell, (el nuevo ha de estar entre los permitidos)
- Si un usuario no tiene asignado ningún intérprete de órdenes, se usará el shell por defecto `/bin/sh`
- Si se desea que el usuario no pueda entrar al sistema se le puede asignar `/bin/false` o `/bin/nologin`
- También se puede establecer como shell un fichero ejecutable $\Rightarrow$ cuando el usuario entre al sistema se ejecuta, y, al finalizar la ejecución, el usuario sale del sistema (no llega a hacer un login realmente)

2. Usuarios (viii)

Cuentas restrictivas

- Estas cuentas permiten limitar las acciones de los usuarios en el sistema, haciendo que tengan determinadas restricciones
- Se pueden crear de dos formas:
  - Asignando como shell un fichero ejecutable que realiza una tarea determinada y al terminarla el usuario sale del sistema:
    - Usuario para realizar las copias de seguridad $\Rightarrow$ como shell tiene un ejecutable (guión shell) para esta tarea
    - Uno para que apague el sistema, y que ejecutará la orden `shutdown`
    - ★ Los usuarios restrictivos de este tipo tienen que tener los permisos necesarios para poder hacer la tarea asignada. Estos permisos se asignan a nivel de identificador de usuario. (¿Qué usuario puede apagar el sistema?)
    - ★ Estos usuarios no llegan a “entrar” al sistema pues no ejecutan un shell del tipo `/bin/bash`

2. Usuarios (ix)

Cuentas restrictivas

- Se pueden crear de dos formas: (continúa...)
  - Usando el shell restrictivo `/bin/rbash`
    - `rbash` es un enlace simbólico a `/bin/bash`
    - Este intérprete se comporta como un intérprete normal, salvo que el usuario no puede hacer determinadas tareas, como:
      - Cambiar de directorio
      - Establecer o modificar los valores de `SHELL` o `PATH`
      - Especificar nombre de órdenes que contengan /
      - Usar la redirección
      - Utilizar la orden interna `exec` para reemplazar el shell por otro programa
    - `/bin/rbash` es equivalente a ejecutar `/bin/bash -r`
    - A estos usuarios se tiene que limitar los ficheros que pueden ejecutar, copiándolos a un directorio y que su `PATH` sea sólo ese directorio. En otro caso, con un `PATH` “normal”, es casi como si no tuviesen restricciones

2. Usuarios (x)

Herramientas para crear/modificar cuentas de usuario

- Las herramientas automáticas para la creación de cuentas de usuario suelen realizar todas las tareas básicas del proceso, a excepción de las específicas (quotas o impresión, etc.)
- `adduser` (o `useradd`) $\Rightarrow$ crear cuentas de usuario, o modificar cuentas ya existentes. Toma los valores por defecto de `/etc/default/useradd` y de `/etc/login.defs`
- `usermod` $\Rightarrow$ modificar cuentas
- `userdel` $\Rightarrow$ eliminar cuentas (por defecto no borra el directorio `HOME`)
- `newusers` $\Rightarrow$ crea cuentas de usuarios utilizando la información introducida en un fichero de texto, que ha de tener el formato del fichero `/etc/passwd`
- `system-config-users` $\Rightarrow$ herramienta en modo gráfico

3. Grupos

- Los grupos son «colecciones» de usuarios que comparten recursos o ficheros del sistema
- Con los grupos se pueden garantizar permisos concretos para un conjunto de usuarios, sin tener que repetirlos cada vez que se desee aplicarlos
- Características de un grupo
  - Nombre del grupo, o *groupname*
  - Identificador del grupo (GID) $\Rightarrow$ internamente el sistema identifica al grupo por este número
- El fichero de configuración es `/etc/group`, con el formato: *nombre:*:gid:lista de usuarios*
  - nombre $\Rightarrow$ nombre del grupo
  - gid $\Rightarrow$ identificador del grupo
  - lista de usuarios que pertenecen al grupo, separados por «,»
- P.ej., *aso:*:519:pilar,alvaro,juan,eduardo,aso01,aso02,aso03*

3. Grupos (ii)

- Definición:
  - Implícita: nuevo GID en el 4º campo de `/etc/passwd`
  - Explícita: nueva entrada en `/etc/group`
  - ★ Normalmente sólo se definen explícitamente
- Tipos de grupos:
  - **Primario** ⇒ el grupo especificado en el fichero `/etc/passwd`
  - **Secundarios** ⇒ los otros grupos a los que pertenece, que son los indicados en `/etc/group`
- Cómo actúan los grupos:
  - Al crear un fichero se establece como grupo propietario el **grupo activo** del usuario en ese momento
  - Al determinar los permisos sobre un fichero, por ejemplo para leerlo o modificarlo, se usan todos los grupos a los que pertenece
  - ★ El **grupo activo** suele ser el **primario**, salvo que se haya cambiado con `newgrp`

3. Grupos (iii)

- `groupadd grupo` ⇒ crear un nuevo grupo
- `groupmod grupo` ⇒ modificar un grupo existente
- `groupdel grupo` ⇒ eliminar un grupo
- `newgrp grupo` ⇒ cambiar de grupo activo (lanza un shell con ese grupo)
- `gpasswd grupo` ⇒ asignar una contraseña a un grupo
  - Si un grupo tiene contraseña, un usuario que la conozca podrá trabajar con ese grupo, a pesar de no pertenecer él. Al ejecutar la orden `newgrp grupo` introducirá la contraseña y pasará a ser su grupo primario
  - `/etc/gshadow` ⇒ contiene la información de seguridad de los grupos (grupo, contraseña, y también los miembros). (Idea parecida al `/etc/shadow`)
- `gpasswd -a user grupo` ⇒ añadir un usuario a un grupo
- `groups [usuario]` ⇒ lista los grupos a los que pertenece un usuario
- `id [usuario]` ⇒ lista el identificador del usuario y los grupos a los que pertenece

4. Usuarios y grupos estándar

Usuarios estándar

- **root** $\Rightarrow$ Cuenta del administrador
- **bin**, **daemon**, **lp**, **sync**, **shutdown**, etc. $\Rightarrow$ Tradicionalmente usados para poseer ficheros o ejecutar servicios
- **mail**, **news**, **ftp** $\Rightarrow$ Asociados con herramientas o facilidades
- **postgres**, **mysql**, **xfs** $\Rightarrow$ Creadas por herramientas instaladas en el sistema para administrar y ejecutar sus servicios
- **nobody** o **nfsnobody** $\Rightarrow$ Usada por NFS y otras utilidades

Grupos estándar

- **root**, **sys**
- **bin**, **daemon**, **adm**, **lp**, **disk**, **mail**, **ftp**, **nobody**, etc.
- **kmem** $\Rightarrow$ Grupo propietario de los programas para leer la memoria del kernel
- **users**