

CAPÍTULO 2

Usuarios y grupos

Gestión básica de usuarios

Linux es un sistema multiusuario; eso quiere decir que puede ser utilizado por varias personas, pudiendo cada una de ellas particularizar el sistema a su gusto. Más aún, cada una tendrá su propio espacio de almacenamiento para guardar sus archivos privados.

Al mismo tiempo los usuarios se distribuyen en grupos, de forma que aquellos que comparten alguna actividad se encuentran perteneciendo a uno de estos grupos. De esta forma es fácil permitir o prohibir a determinados usuarios que utilicen algún recurso (una impresora, Internet, la grabadora de CD-ROM, ...).

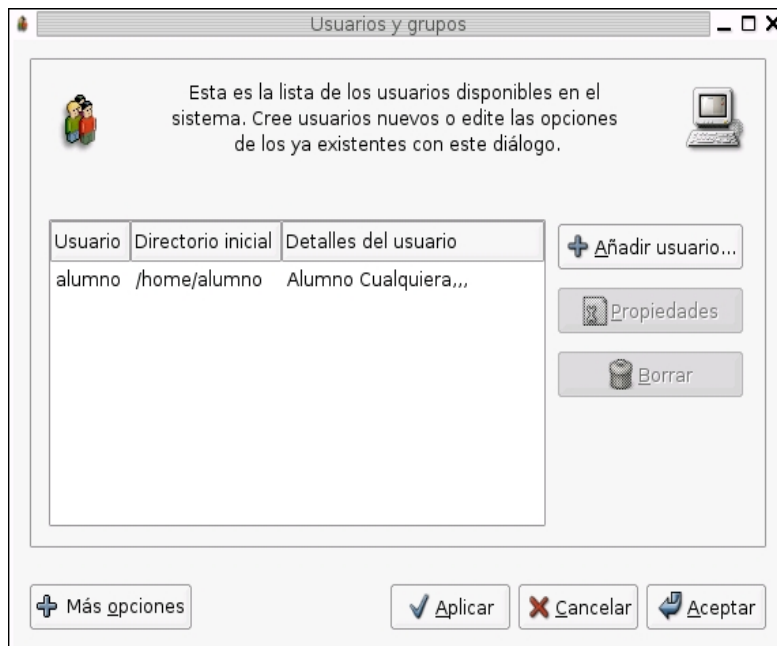
Cada usuario se identifica ante el sistema con un nombre de usuario, también llamado “login”, y una contraseña o “password”. De esta manera para que el usuario pueda acceder al sistema debe introducir correctamente ambos elementos; en caso contrario el sistema no permitirá la entrada. Al conjunto de cada una de estas parejas login-password se le denomina “cuenta”.

En todo sistema Linux existe siempre un usuario especial cuyo nombre es “root”, conocido también como “superusuario” o “administrador”. Éste es el responsable del buen funcionamiento del sistema; ya veremos que cada vez que tengamos que realizar alguna tarea importante para el sistema deberemos introducir su contraseña.

Pero éste no debe ser el único usuario que exista, ya que su utilización frecuente puede originar fallos de seguridad o pérdida de datos (incluso la pérdida total del sistema). Para solucionar esto la persona encargada de la administración utilizará la cuenta de root sólo cuando sea estrictamente necesario (para efectuar cambios en el sistema por ejemplo), mientras que para el resto de acciones que necesite (escribir documentos, conectarse a Internet, ...) utilizará una cuenta con menores privilegios (y por lo tanto menos peligrosa)

Para tratar usuarios y grupos se utiliza una herramienta llamada

“Usuarios y grupos”, localizada en el menú: Aplicaciones -> Herramientas del Sistema -> Panel de Control. Tras pulsar sobre ella verás una ventana como ésta (aunque antes te va a pedir la contraseña de root).



Podemos ver que consta de una parte central, con la lista de los usuarios que existen en ese momento, y a su derecha se muestran las opciones que se pueden realizar. Sólo las iluminadas están disponibles (las sombreadas no lo están por ahora). Según la imagen sólo existe un usuario, llamado “alumno”, cuyo directorio inicial es “/home/alumno” y cuyo nombre real es “Alumno Cualquiera”.

Para crear un nuevo usuario hay que pulsar en “Añadir usuario...”; veremos la ventana con el formulario de la imagen anterior; no todos los campos son necesarios, pero suele ser buena idea poner la mayor información posible.

Editor de cuentas de usuario

Configuración básica

Nombre de usuario:

Nombre rreal:

Información de contacto

Ubicación en la oficina:

Teléfono del trabajo:

Teléfono del domicilio:

Contraseña

☒ Establecer la contraseña a mano

Contraseña del usuario:

Confirmación:

☐ Generar una contraseña aleatoria

Contraseña establecida a:

En primer lugar se necesita el nombre de usuario; éste será su “login” para acceder al sistema; es muy recomendable que tenga entre 4 y 8 caracteres, comience por una letra, esté en minúsculas y no contenga ni espacios ni signos de puntuación (ni la letra “ñ”); nombres incorrectos serían:

peperodriguezvazquez 1pepe PepeRodríguez pepe.rodri

Aunque es posible poner algunos de estos nombres, a la larga sólo te causarán problemas (te lo aseguro). Nombres válidos serían:

peperv pepe1 peperodri

En el apartado “Nombre real” se debe poner el nombre y apellidos de la persona; aquí sí que se pueden poner mayúsculas, espacios, tildes ...

Los tres siguientes apartados se mantienen por compatibilidad con los antiguos sistemas Unix; puedes obviarlas si quieres.

El campo “Contraseñas” también es obligatorio; tenemos dos opciones: establecerla a mano (debemos escribirla dos veces, para evitar equivocaciones) o que el sistema la genere por nosotros (aleatoriamente). Una buena contraseña debería tener entre 6 y 8 caracteres, y contener letras (algunas en mayúsculas), números, símbolos de puntuación, ... Pero recuerda que debes memorizarla ya que hay que introducirla cada vez que quieras entrar en el sistema. Para ver algunas contraseñas “buenas”, selecciona la opción aleatoria y pulsa “Generar una contraseña” varias veces. Y por supuesto, nunca se te ocurra poner algo que tenga que ver con tu nombre, tu edad o tu mascota (una de las principales

formas de entrar en un sistema vienen por aquí). Observa que por seguridad aparecen “*” en lugar de los caracteres.

Así que rellena los campos necesarios con los datos adecuados y pulsa “Aceptar”; volveremos a la pantalla principal, donde ahora aparece el usuario que acabas de crear.

La opción de “Propiedades” muestra la misma pantalla que la de “Añadir usuario...” pero con los datos que se introdujeron para él anteriormente, pudiendo modificarse ahora según se quiera. Para que esté disponible esta opción hay que seleccionar previamente un nombre de la lista.

Por último, el botón “Borrar” elimina el usuario; como medida de precaución pide confirmación ya que la eliminación es irreversible. Al eliminar un usuario no se elimina su directorio personal ni su contenido, por lo que habrá que realizarlo a mano si es necesario.

Gestión avanzada de usuarios

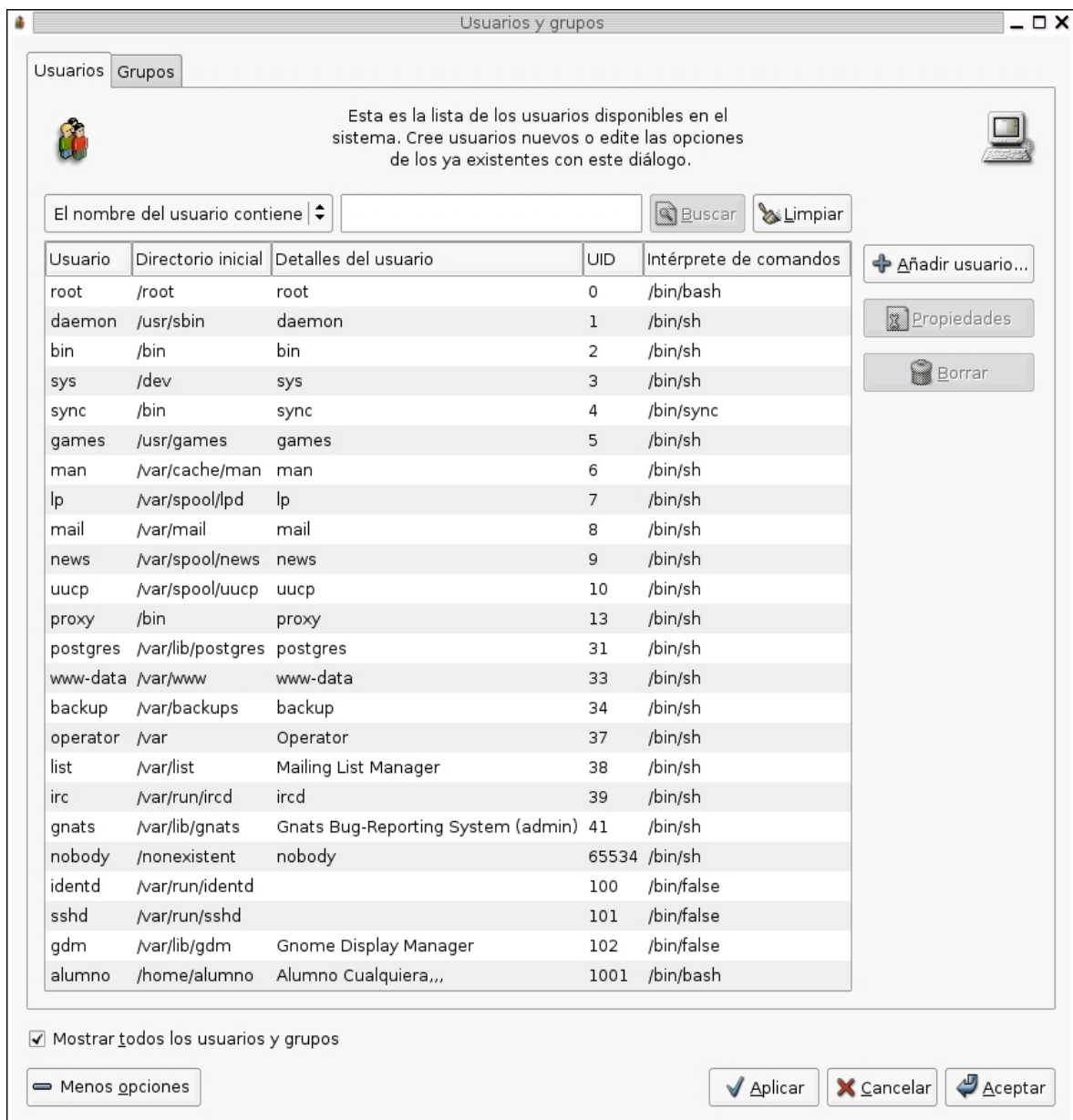
Antes se comentó que siempre existe un usuario llamado “root”, pero sin embargo en esta lista no aparece. Esto es debido a que por defecto y mientras no digamos lo contrario lo que vemos es la lista de usuarios “reales”, es decir, asociados a personas humanas. En realidad existen tres tipos de cuentas diferentes que se utilizan en Linux:

- Cuentas de usuario completas: También llamadas cuentas de “shell”, es la que acabamos de ver, asociada a una persona que puede introducir su login y contraseña y acceder al sistema para utilizar los programas y aplicaciones que hay en él.
- Cuentas de acceso restringido: Son cuentas en las que el usuario sólo tiene acceso a servicios específicos del sistema (por ejemplo el correo electrónico) y por ello no disponen de “shell” o intérprete de comandos. La razón para ello es que una “shell” es potencialmente peligrosa, ya que permite cierta libertad de movimientos y ejecución de ciertos programas.
- Cuentas para programas y “daemons” (demonios): Algunos programas necesitan identidades propias para funcionar; esta es una medida de seguridad ya que generalmente cuando un programa se ejecuta lo hace con los privilegios que tiene el usuario que lo ha ejecutado; esto es realmente peligroso para root. En su lugar se crean unos usuarios “ficticios” que sólo tienen los privilegios adecuados para realizar la tarea para la que han sido

llamados.

Para poder ver todas esas cuentas de usuario, debes pulsar en “Mas opciones”; verás la lista completa y además información adicional sobre cada uno. El último de la lista es el usuario que has creado; observa cómo en la última columna aparece “/bin/bash”, que es el intérprete de comandos que utilizan generalmente los usuarios. El primero de la lista es “root”, que también utiliza esa misma “shell”. El resto son cuentas para programas y demonios, de los cuales algunos tienen “shell” (/bin/sh) y otros no (/bin/false).

Además de esta información, vemos una columna denominada UID (siglas de “Usuary Identifier”, o identificador de usuario); cada usuario (sea del tipo que sea) dispone de un UID, que lo identifica de forma única mediante un número. Es de esta forma como el sistema se refiere a los usuarios (para él no somos más que un número), aunque a nuestros ojos utilicemos el nombre de usuario. Hay algunos números reservados, como el “0” para root; los usuarios “normales” se empiezan a numerar en Debian a partir del 1000 (en RedHat, por ejemplo, lo hacen a partir del 500), reservándose los números inferiores para programas y demonios (no te preocupes por esto, cada programa sabe qué UID usar).



Si el número de usuarios es muy elevado se pueden hacer búsquedas por nombre de usuario, por UID, ... En cualquier momento podemos volver a la vista básica desmarcando la opción “Mostrar todos los usuarios y grupos”

Ahora que tienes activada la opción de “Más opciones”, en la ventana de crear usuarios aparecen dos nuevas pestañas; observa la siguiente imagen:

The screenshot shows a window titled "Editor de cuentas de usuario" with three tabs: "Cuenta", "Avanzado", and "Otros grupos". The "Avanzado" tab is selected. It contains three sections: "Perfil de usuario", "Configuración avanzada", and "Configuraciones opcionales".

- Perfil de usuario:** A dropdown menu for "Perfil:" is set to "Default". To its right is a button with a user icon and the text "Editar perfiles de usuario...".
- Configuración avanzada:** This section contains four fields:
 - "Grupo principal:" is a dropdown menu set to "\$user".
 - "Intérprete de comandos:" is a dropdown menu set to "/bin/bash".
 - "Directorio inicial:" is a text field containing "/home/\$user".
 - "ID del usuario:" is a dropdown menu set to "1001".
- Configuraciones opcionales:** This section contains three password policy settings, each with a numeric input field and up/down arrows:
 - "Máximo número de días que se puede usar una contraseña:" is set to "99999".
 - "Mínimo número de días entre cambio de contraseñas:" is set to "0".
 - "Número de días entre el aviso y la expiración de la contraseña:" is set to "7".

At the bottom right of the window are two buttons: "Cancelar" (with a red X icon) and "Aceptar" (with a blue checkmark icon).

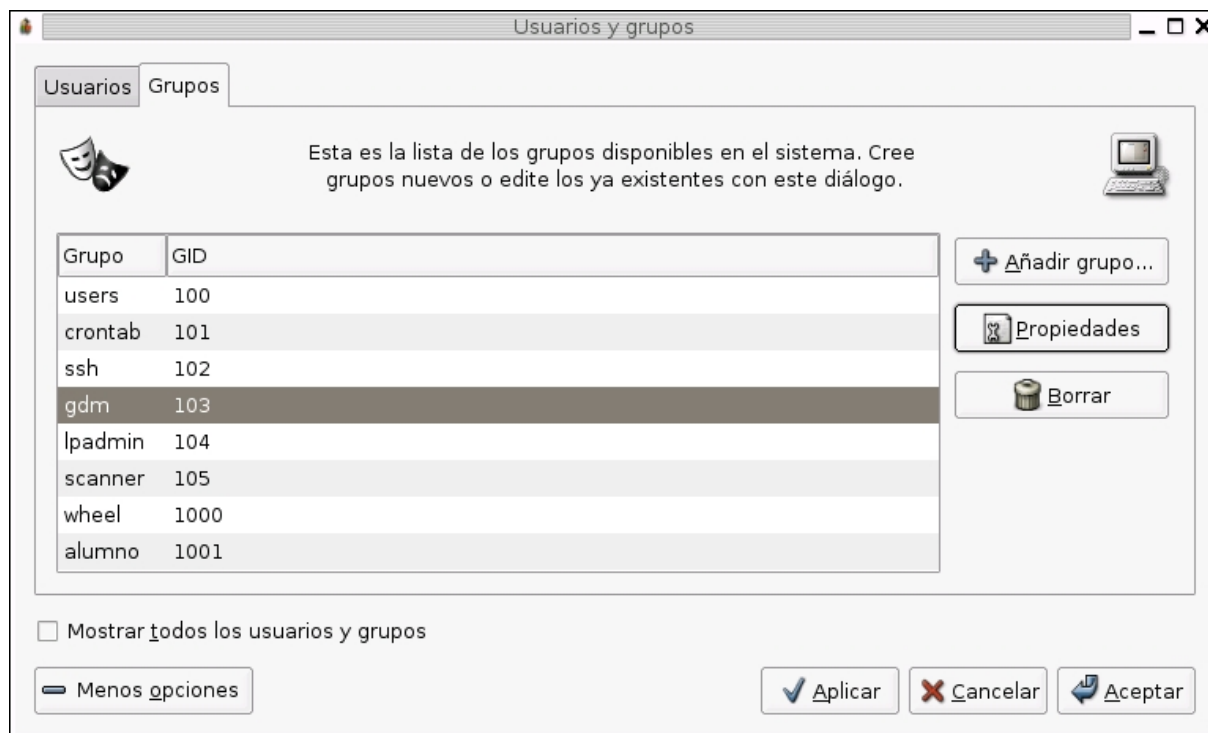
Ahora puedes modificar otros parámetros que antes ni se podían ver, como el intérprete de comandos a utilizar, el directorio inicial, el UID, ... Hablaremos de los grupos en el apartado siguiente. Las configuraciones opcionales tratan sobre la contraseña, y son:

- Máximo número de días ... : Indica cuándo caduca la contraseña; pasados esos días el usuario no podrá acceder al sistema; es una forma de obligar a que el usuario cambie la contraseña cada cierto tiempo.
- Mínimo número de días ... : Especifica cuántos días deben pasar para que el usuario pueda cambiar de nuevo la contraseña.
- Número de días ... : Se mostrará un aviso al usuario esta cantidad de días antes de que la contraseña expire.

Gestión de grupos

Después de lo que acabamos de ver la gestión de grupos te resultará sencilla, ya que guarda muchas similitudes con la de usuarios.

En la vista avanzada hay dos pestañas, una la de usuarios (que ya hemos



visto) y la de grupos, que tiene este aspecto:

Si los usuarios tenían un identificador, los grupos no van a ser menos, lo que pasa que ahora se denomina GID ("Group Identifier", identificador de grupo); de esta forma a cada grupo se le asigna a la hora de crearlo un número que es único. En la imagen anterior aparece la lista abreviada, para verla completa pulsa en "Mostrar todos los usuarios y grupos"; por ejemplo el grupo "gdm" se utiliza para definir los usuarios que tendrán login gráfico.

Hay una cosa que merece la pena resaltar; cada vez que se añade un usuario, se crea automáticamente un grupo con su mismo nombre dentro del cual se incluye dicho usuario. De esta forma, si creamos el usuario "alumno" (cuyo UID es 1001) se creará un grupo (formado de momento por él únicamente) que se llama "alumno" (con GID 1001, observa la imagen anterior). Este grupo se denomina "grupo principal del usuario"; un usuario podrá pertenecer a uno o más grupos, pero nunca podrá abandonar su grupo principal (que, por otro lado, se puede cambiar, pero siempre debe estar definido este grupo principal).

Para añadir un usuario a un grupo, tan sólo selecciona el grupo y pulsa "Añadir grupo...", donde podrás introducir el nombre, su GID (suele ser buena idea aceptar la sugerencia que se nos hace) y qué usuarios pertenecen al grupo;

fíjate que sólo aparecerán en la lista los usuarios “reales”.

Una advertencia: a veces, para que los cambios sean visibles, hay que salir de la aplicación y volver a acceder a ella; otras veces basta con pulsar el botón de “Aceptar” o “Aplicar”.



Por último, recuerda no confundir usuarios con grupos, aunque tengan el mismo nombre se refieren a cosas distintas.

Ejercicios

- 1) Crea 5 usuarios, llamados usu1, usu2, usu3, usu4 y usu5. Crea contraseñas aleatorias para todos.
- 2) Modifica usu1 para que su contraseña sea la palabra “ejemplo”
- 3) Crea dos grupos, llamados “pares” e “impares”; añade usu2 y usu4 al grupo “pares” y usu1, usu3 y usu5 al “impares”.
- 4) Añade el usuario usu1 al grupo usu3 y el usuario usu3 al grupo usu1.

- 5) Borra el usuario usu3 y usu5. ¿Siguen existiendo los grupos usu3 y usu5? ¿Por qué crees que ocurre esto?
- 6) Vuelve a crear el usuario usu3 y establece para él un UID mayor que el que tenga usu4 (por ejemplo 1100). ¿Cuál es el grupo principal de usu3? ¿Se ha creado algún grupo nuevo? ¿Por qué?

Soluciones

- 3) Ten cuidado de no repetir el GID, recuerda que debe ser único; cualquier número por encima de 1000 (y que no esté ocupado) puede servirte.
- 4) Para incluir a un usuario en un grupo puedes hacerlo desde el menú de grupos o el de usuarios; observa cómo el grupo principal no aparece en la lista.
- 5) Si sales y vuelves a entrar de la aplicación verás que el grupo usu5 ha desaparecido, mientras que usu3 sigue existiendo. Esto es así porque en usu3 sigue habiendo usuarios (recuerda que metiste a usu1 en este grupo en el ejercicio anterior); un grupo (por encima del GID 1000) se elimina cuando no quedan usuarios en el grupo.
- 6) El grupo principal de usu3 resulta ser el grupo usu3 (que ya existía), pero observa que el UID y el GID no coinciden en número; esto no supone ningún problema para el sistema. Por eso no se crea ningún grupo nuevo (no puede haber dos grupos con el mismo nombre).