CAPÍTULO 4

Administración de los usuarios

UNIX/Linux se diseñó desde las bases hasta convertirse en un sistema operativo para múltiples usuarios. Un sistema operativo de este tipo no será de mucha utilidad sin usuarios. Y esto nos lleva al tema de administración de los usuarios en Linux. Asociado con cada usuario se encuentra equipaje de cada uno. Este equipaje podría incluir archivos, procesos, recursos y otra información. Al tratar con un sistema de múltiples usuarios, para un administrador de sistemas es necesario que haya comprendido bien lo que constituye un usuario (y todo lo que es el equipaje de éste), un grupo y cómo interactúan estos entre sí.

En los sistemas de computadoras, se usan las cuentas de usuarios con el fin de determinar quién tiene acceso a qué. La capacidad de un usuario para tener acceso a un sistema se determina por medio de si existe o no ese usuario y si tiene los permisos apropiados para usar tal sistema.

En este capítulo, examinaremos la técnica para administrar los usuarios en un solo anfitrión. Empezaremos por examinar los archivos actuales de base de datos que contienen la información acerca de los usuarios. De allí, examinaremos las herramientas del sistema de las que se dispone para administrar los archivos en forma automática.

¿QUÉ CONSTITUYE EXACTAMENTE UN USUARIO?

En Linux, cada archivo y cada programa debe ser propiedad de un *usuario*. Cada usuario tiene un identificador único llamado la *ID del usuario (UID).* También, cada usuario debe pertenecer por lo menos a un *grupo*, una colección de usuarios establecida por el administrador del sistema. Los usuarios pueden pertenecer a varios grupos. Como los usuarios, los grupos también tienen identificadores únicos, llamados *ID de los grupos (GID)*.

La accesibilidad de un archivo o programa se basa en sus UID y GID. Un programa en ejecución hereda los derechos y permisos del usuario que lo llama (con SetUID y SetGID, los cuales se discuten en "Comprensión de los programas SetUID y SetGID" más adelante en este capítulo, se crea una excepción a esta regla). Los derechos de cada usuario se pueden definir en una de dos maneras: como los de un *usuario normal* y los de un *usuario raíz*. Los usuarios normales sólo pueden tener acceso a lo que poseen o a lo que se les ha dado permiso de ejecutar; el permiso se concede porque el usuario pertenece al grupo del archivo o porque el archivo es accesible a todos los usuarios. A los usuarios raíz se les permite el acceso a todos los archivos y programas del sistema, sin importar si la raíz les pertenece o no. A menudo, al usuario raíz se le conoce como *superusuario*.

Si usted está acostumbrado a Windows, puede hallar un paralelismo entre la administración de usuarios del sistema y la administración de usuarios de Linux. Por ejemplo, las UID son comparables a las SID (ID del sistema) de Windows. Contrastando con Windows NT, puede hallar el modelo de seguridad de Linux simplista de manera exasperante: usted es usuario raíz o no lo es. Los usuarios normales no pueden tener los privilegios de los raíz, de la misma manera que, en NT, a ese tipo de usuarios no se les puede conceder el acceso del administrador. Aun cuando este enfoque es un poco menos común, en Linux también puede implementar el control del acceso de grano más fino a través del uso de las listas de control de acceso (ACL), como lo puede hacer con Windows. ¿Cuál sistema es mejor? Depende de lo que usted desea y de a quién le pregunte.

Dónde se guarda la información del usuario

Si el lector ya ha usado hasta la administración de los usuarios de Windows 2000, está familiarizado con la herramienta Active Directory (Directorio activo) que se encarga de los detalles sustanciales de la base de datos de los usuarios. Esta herramienta resulta conveniente, pero dificulta el desarrollo de sus propias herramientas administrativas, dado que la única otra manera de leer o manipular la información de los usuarios es a través de una serie de LDAP, Kerberos o llamadas programáticas del sistema.

Como contraste, Linux toma el camino del UNIX tradicional y conserva toda la información de los usuarios en archivos directos de texto. Esto resulta benéfico por la sencilla razón de que permite hacer cambios a la información de los usuarios, sin necesidad de alguna otra herramienta que no sea un editor de textos, como **vi**. En muchos casos, los sitios más grandes sacan ventaja de estos archivos de texto al desarrollar sus propias herramientas de administración de los usuarios, de modo que no sólo pueden crear cuentas nuevas sino también hacer adiciones en forma automática al directorio telefónico corporativo, a las páginas Web, etcétera.

Sin embargo, es posible que los usuarios y grupos que trabajan con el estilo de UNIX por primera vez prefieran adherirse a las herramientas básicas de administración de los usuarios que vienen con la distribución de Linux. Más adelante, en este capítulo, discutiremos esas herramientas en "Herramientas para administración de los usuarios". Por ahora, examinemos los archivos de texto en los que se almacena la información de los usuarios y los grupos, en Linux.

El archivo /etc/passwd

En el archivo **/etc/passwd** se almacena la concesión de acceso (login) al usuario, la entrada cifrada de la contraseña, la UID, la GID predeterminada, el nombre (a veces llamado GECOS), el directorio inicial y el shell de la concesión de acceso. Cada línea en el archivo representa información acerca del usuario. Las líneas se forman con varios campos estándar, delimitándose cada campo por medio de dos puntos. En la figura 4-1, se ilustra una entrada muestra de un archivo **passwd**, con sus diversos campos.

En las secciones que siguen, se discuten con detalle los campos del archivo **/etc/passwd.**

Campo del nombre del usuario

Este campo también se conoce como el de concesión de acceso o de la cuenta. En él se almacena el nombre del usuario en el sistema. El nombre del usuario debe ser una cadena única y que identifica también de manera única un usuario del sistema. Los diferentes sitios usan métodos distintos para generar los nombres de concesión de acceso de los usuarios. Un método muy común es usar la primera letra del nombre (o primer nombre) del usuario y anexar el apellido (o apellidos) de éste. Por lo común, esto funciona porque las posibilidades son relativamente remotas de que se tengan usuarios con el mismo nombre y el mismo apellido (o mismos apellidos). Desde luego, existen diversas variaciones de este método. Por ejemplo, para un usuario cuyo nombre es "Ying" y su apellido es "Yang", se le puede asignar un nombre de usuario de "yyang".

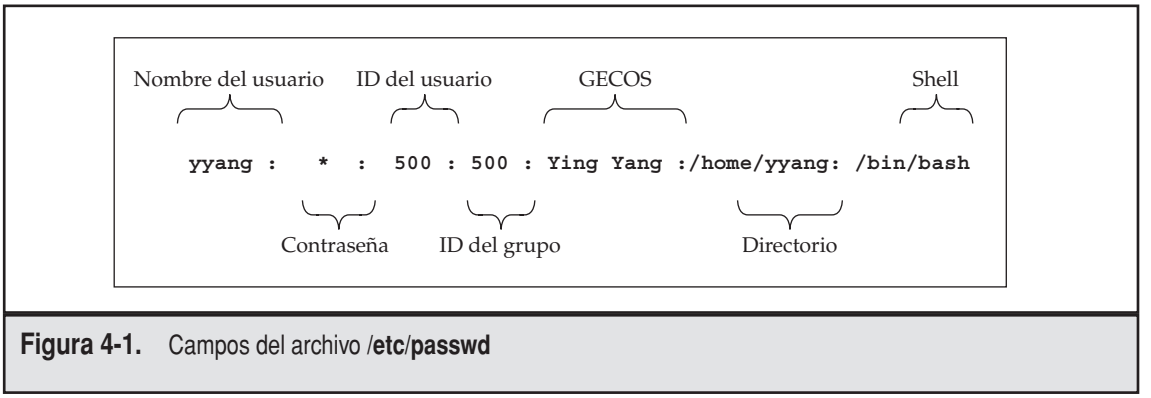

Figura 4-1. Campos del archivo /**etc**/**passwd**

Campo de la contraseña

Este campo contiene la contraseña cifrada del usuario. En la mayor parte de los sistemas Linux modernos, este campo contiene una letra *x* para indicar que, en el sistema, se están usando contraseñas sombra (lo que se discute con detalle más adelante). Todas las cuentas de usuarios en el sistema deben tener una contraseña o, al menos, etiquetarlos como imposibles para dejarlos entrar. Esto es crucial para la seguridad del sistema; las contraseñas débiles hacen que un sistema sea comprometedor, sólo que mucho más sencillo.

En realidad, la filosofía que se encuentra detrás de las contraseñas es bastante interesante, en especial porque en la actualidad todavía dependemos en una parte significativa de ella. La idea es sencilla: en lugar de confiar en archivos protegidos para mantener las contraseñas en secreto, el sistema cifraría la contraseña utilizando un algoritmo desarrollado por AT&T (y aprobado por la National Security Agency, Agencia Nacional de Seguridad) y que se conoce con el nombre de Data Encryption Standard (DES, Norma de cifrado de datos) y deja el valor cifrado a la vista del público. Lo que originalmente hizo que esto fuera seguro era que el algoritmo de cifrado era difícil de descifrar por medio de la computación. Lo más que pudo hacer la mayor parte de los muchachos fue un ataque a fuerza bruta al diccionario, en donde sistemas automatizados realizarían repeticiones de uno a otro lado de un gran diccionario y se atendrían a la naturaleza de los usuarios de tomar palabras del idioma como sus contraseñas. Mucha gente trató de descifrar el propio DES, pero como era un algoritmo abierto que cualquiera podía estudiar, se hizo mucho más a prueba de balas, antes de que en realidad se desplegara.

Cuando los usuarios hicieran entrar sus contraseñas en un mensaje para solicitar el acceso, esa contraseña se cifraría. A continuación, el valor cifrado se compararía contra la entrada de contraseña del usuario. Si los dos valores cifrados coincidían, se permitiría que el usuario entrara al sistema. El algoritmo real para realizar el cifrado era, desde el punto de vista computacional, suficientemente fácil que un solo cifrado no sería demasiado tardado. Sin embargo, las decenas de miles de cifrados que se necesitarían para un ataque al diccionario sería prohibitivamente tardado.

Pero entonces se presentó un problema: se cumplió la ley de Moore sobre la duplicación de la velocidad del procesador cada 18 meses y las computadoras domésticas se volvieron lo bastante poderosas y rápidas que los programas fueron capaces de realizar un ataque a fuerza bruta al diccionario en el transcurso de días, en lugar de semanas o meses. Los diccionarios se hicieron más grandes y el software, más inteligente. Por consiguiente, fue necesario volver a evaluar la naturaleza de las contraseñas. Una solución ha sido mejorar el algoritmo empleado para realizar el cifrado de las contraseñas. En algunas distribuciones de Linux se sigue la trayectoria trazada por el sistema operativo FreeBSD y se utiliza el esquema MD5. Esto ha aumentado la complejidad relacionada con el descifrado de las contraseñas, lo cual, cuando se usa en conjunción con las contraseñas sombra (que se discuten más adelante), funciona bastante bien. (Por supuesto, ¡esto es suponiendo que usted logra que sus usuarios elijan contraseñas buenas!)

SUGERENCIA La elección de contraseñas buenas siempre es una tarea. De manera inevitable, sus usuarios preguntarán: "Entonces, ¡Oh Todopoderoso Administrador del Sistema!, ¿con qué se forma una buena contraseña?". Aquí tiene su respuesta: una palabra que no sea de un idioma (no inglés, no español, no alemán, no una palabra del lenguaje humano), de preferencia con mayúsculas, minúsculas, números y puntuación mezclados; en otras palabras, una cadena que tenga el aspecto de un ruido de la línea. Bien, esto es del todo bonito y maravilloso, pero qué pasa si una palabra es demasiado difícil para recordar, la mayor parte de la gente hará pedazos su propósito al escribirla y conservarla en un lugar que se vea con facilidad. De modo que lo mejor es ¡hacerla fácil de memorizar! Una buena técnica podría ser elegir una frase y, a continuación, tomar la primera letra de cada palabra de ella. Por tanto, la frase "coffee is VERY GOOD for you and me" se convierte en ciVG4yam. La frase se puede memorizar, incluso si la contraseña resultante no lo es.

Campo de la ID del usuario (UID)

En este campo se almacena un número único que el sistema operativo y otras aplicaciones usan para identificar al usuario y determinar los privilegios de acceso. Es el equivalente numérico del campo del nombre del usuario. La UID debe ser única para cada usuario, con la excepción de la UID 0 (cero). Cualquier usuario que tiene una UID de 0 tiene acceso raíz (administrativo) y, como consecuencia, la plena ejecución del sistema. Por lo común, el único usuario que tiene esta UID específica tiene la raíz de concesión de acceso. Se considera una mala práctica permitir que cualesquiera otros usuarios o nombres de usuarios tengan una UID de 0. Esto difiere de manera notable de los modelos de Windows NT y 2000, en los cuales cualquier número de usuarios puede tener privilegios administrativos.

A veces, distribuciones diferentes de Linux adoptan esquemas distintos de numeración UID. Por ejemplo, en Fedora y RHEL, se reserva la UID 99 para el usuario "nadie", en tanto que en Linux de SuSE se usa la UID 65534 para el usuario "nadie".

Campo de la ID del grupo (GID)

El campo siguiente en el archivo **/etc/passwd** es la entrada de la ID del grupo. Es el equivalente numérico del grupo primario al que pertenece el usuario. Este campo también desempeña un papel importante en la determinación de los privilegios de acceso del usuario. Se debe hacer notar que, además de un grupo primario del usuario, un usuario puede pertenecer también a otros grupos (se encuentra más acerca de esto en la sección "El archivo /etc/group").

GECOS

En este campo se pueden almacenar varios trozos de información de un usuario. Puede actuar como un lugar de reserva para la descripción del usuario, nombre completo (nombre y apellidos), número telefónico, etcétera. Este campo es opcional y, como resultado, se puede dejar en blanco. También es posible almacenar entradas múltiples en este campo, sencillamente al separar las entradas diferentes con una coma.

NOTA GECOS es un acrónimo de General Electric Comprehensive Operating System (Sistema operativo detallado de General Electric) (ahora conocido como GCOS) y es un remanente de los primeros días de la computación.

Como una nota histórica al pie, la liga de GECOS a UNIX se origina en el hecho de que en los Bell Labs, durante la creación de UNIX, se usaron máquinas GCOS para imprimir. Para dar cabida al uso de los servicios de impresión basados en GCOS, se agregó un campo más al archivo **/etc/passwd**.

Directorio

Éste suele ser el directorio inicial del usuario, pero también puede ser cualquier lugar arbitrario en el sistema. Cada usuario que en realidad ingresa al sistema necesita un lugar para los archivos de configuración que son únicos para él. Este lugar, conocido como *directorio inicial*, permite a cada usuario trabajar en un entorno personalizado, sin tener que cambiar el entorno personalizado por otro usuario; incluso si los dos son admitidos en el sistema al mismo tiempo. En este directorio, a los usuarios se les permite conservar no sólo sus archivos de configuración sino también sus archivos de trabajo regular.

Scripts de arranque

En Linux, los scripts de arranque no son del todo parte de la información almacenada en la base de datos de los usuarios. Sin embargo, desempeñan un papel muy importante en la determinación y control del entorno del usuario. En particular, en Linux, los scripts de arranque suelen almacenarse bajo el directorio inicial del usuario…y, por ello, la necesidad de mencionarlos mientras se está tocando el tema del campo directorio (directorio inicial) en el archivo **/etc/passwd**.

Linux/UNIX se estructuró desde su puesta en marcha como un entorno de usuarios múltiples. A cada usuario se le permite tener sus propios archivos de configuración; por tanto, el sistema aparenta estar personalizado para cada usuario en particular (incluso si se admiten otras personas al mismo tiempo). La personalización del entorno de cada usuario por separado se hace a través del uso de los scripts shell, la ejecución de archivos de control y cosas semejantes. Estos archivos pueden contener una serie de comandos que van a ser ejecutados por el shell que arranca cuando a un usuario se le concede el acceso. Por ejemplo, en el caso del shell BASH, uno de sus archivos de arranque es el **.bashrc** (sí, se tiene un punto adelante del nombre del archivo; los nombres de archivos precedidos por puntos, también llamados archivos punto, se esconden de las listas de directorios normales). Puede concebir los scripts shell en la misma forma que en los archivos por lotes, excepto que aquellos pueden ser mucho más capaces. En particular, el script **.bashrc** tiene una naturaleza semejante al **autoexec.bat** en el mundo de Windows.

En varios paquetes de software de Linux se usan opciones específicas y que se pueden personalizar en directorios o archivos que empiezan con un **.**, en cada directorio inicial de usuario. Algunos ejemplos son **.mozilla** y **.kde**. A continuación se dan algunos archivos punto (.) que se encuentran presentes en el directorio inicial de cada usuario:

- **.bashrc/.profile** Archivos de configuración para BASH.
- **.tcshrc/.login** Archivos de configuración para tcsh.
- **.xinitrc** Este script anula el script predeterminado que se llama cuando usted es admitido en X Window System.
- **.Xdefaults** Este archivo contiene opciones predeterminadas que usted puede especificar para las aplicaciones en X Window System.

Cuando crea una cuenta de usuario, también se crean un conjunto de archivos punto predeterminados para ese usuario; esto es principalmente por conveniencia, para ayudar el inicio del usuario. Las herramientas de creación del usuario que se discuten más adelante le ayudan a realizar esto en forma automática. Los archivos predeterminados se almacenan bajo el directorio **/etc/skel**.

En beneficio de la uniformidad, la mayor parte de los sitios colocan los directorios iniciales en **/home** y nombran el directorio de cada usuario con el nombre de entrada de ese usuario. De este modo, si por ejemplo el nombre con el que usted fue admitido fuera "yyang", su directorio inicial sería **/home/yyang**. La excepción de esto es para algunas cuentas especiales del sistema, co-

mo la cuenta de un usuario raíz o un servicio del sistema. En Linux, suele fijarse que el directorio inicial del superusuario (del raíz) sea **/root** (pero para la mayor parte de las variantes de UNIX, como Solaris, es tradicional que el directorio inicial sea /). Un ejemplo de un servicio especial del sistema que podría necesitar un directorio específico de trabajo podría ser para un servidor Web cuyas páginas Web se manejan desde el directorio **/var/www/**.

En Linux, la decisión de colocar los directorios iniciales bajo **/home** es estrictamente arbitraria, pero en realidad provoca sentido de organización. De hecho, al sistema no le interesa en dónde coloquemos los directorios iniciales, en tanto que la ubicación para cada usuario se especifique en el archivo de contraseñas.

Shell (intérprete de comandos)

Cuando los usuarios son admitidos al sistema, esperan un entorno que les pueda ayudar a ser productivos. Este primer programa que los usuarios encuentran se llama *shell*. Si usted ha usado el lado del mundo de Windows, podría igualar esto con command.com, Program Manager (Administrador de programas) o Windows Explorer (Explorador de Windows) (no debe confundirse con Internet Explorer, el cual es un navegador de la Web).

Bajo UNIX/Linux, la mayor parte de los shells se basan en textos. Un shell popular predeterminado para el usuario en Linux es el Bourne Again Shell, abreviado como BASH. Linux viene con varios shells que se pueden elegir; puede ver una lista de la mayor parte de ellos en el archivo **/etc/shells**. Decidir cuál es el shell correcto para usted es, en cierto modo, como elegir una cerveza favorita; lo que es bueno para usted no lo es para todos pero, todavía, ¡todos tienden a ponerse a la defensiva respecto a su elección!

Lo que hace a Linux tan interesante es que en realidad no tiene que adherirse a la lista de shells que se suministra en **/etc/shells**. En lo más estricto de las definiciones, la entrada de la contraseña para cada usuario no le presenta una lista de cuál shell ejecutar, tanto como le presenta la lista de cuál programa ejecutar primero por el usuario. Por supuesto, la mayor parte de los usuarios prefieren que el primer programa que ejecuten sea un shell, como BASH.

El archivo /etc/shadow

Éste es el archivo de contraseñas cifradas. En él se almacena la información de las contraseñas cifradas para las cuentas de los usuarios. Además de la contraseña cifrada, en el archivo **/etc/shadow** también se almacena la información opcional acerca del envejecimiento de la contraseña o expiración. La introducción del archivo sombra ocurrió debido a la necesidad de separar las contraseñas cifradas del archivo **/etc/passwd**. Esto se hizo necesario en virtud de que fue creciendo la facilidad con la cual las contraseñas cifradas podían ser descifradas con el aumento en el poder de procesamiento de las computadoras de consumo (PC domésticas). La idea fue mantener el archivo **/etc/passwd** de manera que pudiera ser leído por todos los usuarios, sin almacenar las contraseñas cifradas en él, y, a continuación, hacer que el archivo **/etc/shadow** sólo pudiera ser leído por el raíz u otros programas privilegiados que requieren el acceso a esa información. Un ejemplo de ese tipo de programas sería el programa login (de concesión de acceso).

Se podría uno preguntar: "¿por qué no sólo hacer que el archivo **/etc/passwd** pudiera ser leído sólo por el raíz u otros programas privilegiados?" Bien, eso no es tan sencillo. Al tener el archivo de contraseñas abierto durante tantos años, el resto del software del sistema que creció en torno a él dependió del hecho de que ese archivo siempre podía ser leído por todos los usuarios. Cambiar esto sencillamente haría que el software fallara.

Precisamente como en el archivo **/etc/passwd**, cada línea en el **/etc/shadow** representa información acerca del usuario. Los renglones se forman por varios campos estándar, delimitándose cada uno de ellos por medio de dos puntos. Los campos son

- Nombre para obtener el acceso
- Contraseña cifrada
- Días transcurridos a partir del 1 de enero de 1970 en que la contraseña se cambió por última vez
- Días antes de los cuales la contraseña puede ser cambiada
- Días después de los cuales debe cambiarse la contraseña
- Días antes de que expire la contraseña en que debe avisarse al usuario
- Días después de que expire la contraseña en que se desactiva esa cuenta
- Días transcurridos a partir del 1 de enero de 1970 en que se desactiva esa cuenta
- Un campo reservado

Enseguida, se presenta una entrada muestra del archivo **/etc/shadow** para la cuenta mmel del usuario:

```
mmel:$1$HEWdPIJ.$qX/RbB.TPGcyerAVDlF4g.:12830:0:99999:7:::
```

El archivo /etc/group

El archivo **/etc/group** contiene una lista de los grupos, con un grupo por línea. Cada entrada de grupo en el archivo tiene cuatro campos estándar, con cada uno de ellos delimitado por dos puntos, como en los archivos **/etc/passwd** y **/etc/shadow**. Cada usuario del sistema pertenece por lo menos a un grupo, considerándose a ése como el grupo predeterminado del usuario. Entonces, si es necesario, los usuarios se pueden asignar a grupos adicionales. El lector recordará que el archivo **/etc/passwd** contiene la ID del grupo predeterminado (GID) de cada usuario. Esta GID se aplica al nombre del grupo y otros miembros del mismo en el archivo **/etc/group**. La GID debe ser única para cada grupo.

Asimismo, como en el archivo **/etc/passwd**, el mundo debe poder leer el archivo de grupos, de modo que las aplicaciones puedan probarse por asociaciones entre usuarios y grupos. Los campos de cada línea en el archivo **/etc/group** son

- **Nombre del grupo** El nombre del grupo
- **Contraseña del grupo** Ésta es opcional, pero si se fija permite que usuarios que no son parte del grupo se unan al mismo
- **ID del grupo (GID)** El equivalente numérico del nombre del grupo
- **Miembros del grupo** Una lista separada por comas

Enseguida se da una entrada muestra de un grupo en el archivo **/etc/group**:

```
bin:x:1:root,bin,daemon
```

Esta entrada es para el grupo "bin". La GID para el grupo es 1 y sus miembros son el raíz, bin y daemon.