Administración de recursos

LUIS GERARDO VAZQUEZ RODRIGUEZ

Noviembre 9, 2015

Introducción

Un usuario Unix representa tanto a una persona (usuario real) como a una entidad que gestiona algún servicio o aplicación (usuario lógico o ficticio) Todo usuario definido en el sistema se corresponde con un identificador único (UID) y con una cuenta, donde se almacenan sus datos personales en una zona de disco reservada. Un grupo es una construcción lógica –con un nombre y un identificador (GID) únicos– usada para conjuntar varias cuentas en un propósito común, compartiendo los mismos permisos de acceso en algunos recursos. Cada cuenta debe estar incluida como mínimo en un grupo de usuarios, conocido como grupo primario o grupo principal.

Características generales de una cuenta.

Las características que definen la cuenta de un usuario son:
• Tiene un nombre y un identificador de usuario (UID) únicos en el sistema.
• Pertenece a un grupo principal.
• Puede pertenecer a otros grupos de usuarios.
• Puede definirse una información asociada con la persona propietaria de la cuenta.
• Tiene asociado un directorio personal para los datos del usuario.
• El usuario utiliza en su conexión un determinado intérprete de mandatos, donde podrá ejecutar sus aplicaciones y las utilidades del sistema operativo.
• Debe contar con una clave de acceso personal y difícil de averiguar por parte de un impostor.
• Tiene un perfil de entrada propio, donde se definen las características iniciales de su entorno de operación.
• Puede tener una fecha de caducidad.
• Pueden definirse cuotas de disco para cada sistema de archivos.
• Es posible contar con un sistema de auditoria que registre las operaciones realizadas por el usuario.

Usuarios y grupos predefinidos.

En todos los “dialectos” Unix existen algunos usuarios y grupos predefinidos por el sistema operativo, que se utilizan para la gestión y el control de los distintos servicios ofrecidos por el ordenador.
En especial el usuario root –con UID 0– es el administrador de la máquina, con un control total sobre el sistema. Existe también un grupo root –con GID 0–

con características administrativas, al que pertenece el citado usuario.
Como ejemplo, la siguiente tabla lista algunos de los usuarios y grupos predefinidos en Fedora 13 y en Ubuntu 10.04 Lucid , indicando también las posibles diferencias.

El usuario root definido por defecto.

Ubuntu y Fedora establecen en sus programas de instalación distintas políticas para definir la forma de trabajar por defecto con la cuenta de superusuario (root). Como se puede comprobar en el apartado anterior, en ambos casos la cuenta tiene el mismo nombre y los mismos parámetros de UID y GID. Sin embargo, el programa de instalación de Fedora pide establecer una clave para dicho usuario, mientras que el de Ubuntu no la solicita. Ubuntu no permite conectarse directamente al sistema como root y sólo los usuarios que pertenecen al grupo admin pueden ejecutar órdenes con privilegios usando la orden sudo e introduciendo su propia clave. La siguiente tabla muestra un resumen de las diferencias entre ambos sistemas operativos definiendo la cuenta root.

Clave de acceso.

Como se ha indicado anteriormente, las claves de los usuarios locales de Linux se guardan codificadas en el fichero inaccesible /etc/shadow.
Los algoritmos de codificación de las claves son "de sentido único", o sea que impiden la descodificación directa de las claves. Por lo tanto, cuando un usuario entra en el sistema, se le codifica la clave y se compara con la clave válida encriptada. Si el resultado es correcto, el usuario puede conectarse.
Linux puede utilizar el algoritmo de codificación Crypt, usado en los antiguos sistemas Unix y llamado así por la función del lenguaje C que realiza los cálculos. Este método es inseguro porque usa claves de codificación débiles de 56 bits y las contraseñas sólo pueden tener un máximo de 8 caracteres.
Los nuevos Linux también soportan algoritmos de codificación más potentes como MD5 o SHA, mucho más robustos y que permiten claves más extensas y difíciles de averiguar. El algoritmo MD5 usa claves de 128 bits, mientras que SHA512 –por defecto en Fedora 13 y en Ubuntu 10.04– aumenta dicha longitud hasta los 512 bits.
La siguiente figura muestra la pestaña de opciones de la aplicación gráfica system-config-authentication, para gestión de autentificación en Fedora 13.

Restricciones para tener claves seguras.

El administrador debe recomendar a sus usuarios que creen claves que puedan resultar difíciles de averiguar para un pirata informático. También debe hacer que el sistema cree dificultades al intruso, usando codificaciones complejas y creando restricciones que comprometan al usuario con la seguridad del sistema.
Todos los usuarios del sistema han de tener en cuenta las siguientes recomendaciones con sus claves:
• No usar palabras comunes o números asociados a la persona. 15
• No repetir las claves en distintas máquinas.
• Usar claves de 8 caracteres como mínimo, con al menos 2
caracteres no alfabéticos.

• No usar secuencias de teclado.
• Cambiar la clave periódicamente y no repetir claves anteriores.
• No dejar ni anotar la clave.
• Evitar que otra persona vea teclear la clave.

Permisos.

Uno de los elementos principales de la seguridad en Unix es el buen uso de los permisos para acceder a ficheros y directorios. Todo usuario –no sólo el administrador– debe tener claros los conceptos más básicos para evitar que otro usuario lea, modifique o incluso borre datos de interés.
El usuario administrador –al tener el control completo del sistema– también puede realizar operaciones sobre los ficheros y directorios de cualquier usuario (técnica que puede ser utilizada para evitar que un usuario pueda acceder a su propio directorio personal).
Este hecho hace imprescindible que los responsables de la máquina tengan especial cuidado cuando utilicen la cuenta del usuario root. Los permisos de acceso se dividen principalmente en dos categorías:
• permisos normales,
• permisos especiales.
Por otro lado, los permisos también se subdividen en tres grupos:
• permisos para el propietario,
• permisos para su grupo de usuarios,
• permisos para el resto de usuarios del sistema,
Las listas de control de acceso (ACL) permiten asignar permisos de forma específica a conjuntos de usuarios y grupos.

Permisos normales.

Cada usuario tiene un nombre de conexión único en el ordenador y pertenecerá a uno o varios grupos de usuarios. El propietario de un fichero o directorio puede seleccionar qué permisos desea activar y cuales deshabilitar.
Para comprobarlo de manera más clara, tómese el primer grupo de valores obtenidos con el mandato ls -l, que permitirá observar los permisos. Estos 11 caracteres indican:
• 1 carácter mostrando el tipo: fichero (-), directorio (d), enlace (l), tubería (p), enlace simbólico (l), etc.
• 3 caracteres para los permisos del propietario.
• 3 caracteres para los permisos de otros usuarios del grupo.
• 3 caracteres para los permisos del resto de usuario.
• 1 carácter opcional que indica si hay definida una ACL