Gestión de usuarios en Linux

Equipo docente Sistemas Operativos

Introducción

- CONTENIDOS:
  - 1. Usuarios y perfil de usuarios
  - 2. Grupos y tipos.
  - 3. Ficheros de mantenimiento de los usuarios y grupos.
  - 4. Mantenimiento de las cuentas de usuarios.

- BIBLIOGRAFÍA:
  - Manual de referencia de Red Hat Linux.
  - Manual de personalización de Red Hat Linux.
  - "Utilizando LINUX" (2ª edi.), capítulo 9, Tackett J. y Gunter D., Prentice Hall.
  - "Essential System Administration", capítulo 5, Frisch A., O´Reilly & Associates, Inc.

Objetivos

- Saber cuáles son los atributos básicos que definen el perfil de un usuario del sistema, así como diferentes formas de registrarlas en el sistema.

- Dominar las técnicas, procedimientos y utilidades más usuales para crear, modificar atributos y eliminar usuarios.

- Comprender la necesidad de la creación de grupos de usuarios.

1. Usuarios y perfil de usuarios

- Linux es un sistema operativo multitarea y multiusuario.
- Permite definir distintos usuarios y grupos.
- Cada usuario pertenece a uno o a varios grupos.
- Los permisos y accesos a los archivos, dispositivos y a los recursos se apoyan en la definición de usuarios y grupos.
- El S.O. gestiona y define su política de seguridad a los distintos recursos basándose en los usuarios y grupos.

¿Para que definir usuarios en el sistema?

- Desde el punto de vista de usuario, para poder entrar en el sistema.
- Desde el punto de vista del sistema:
  - Cada recurso tiene un **usuario propietario**.
  - Para gestionar y controlar el acceso a los recursos del sistema.
  - Se definen políticas de acceso y seguridad en base a los usuarios.

Ejemplos de usuarios predefinidos en el sistema

- **root -** El administrador del sistema
- **daemon -** El que ejecuta de los procesos daemon del sistema.
- **bin -** El propietario de los comandos del sistema en /bin /usr/bin
- **sys -** El propietario de los ficheros del sistema
- **cron, ftp, mail, news, usenet -** Propietarios de subsistemas

¿Quién define usuarios en el sistema? El usuario root

Definición de usuario en fución de sus atributos?

Atributos que definen el perfil de un usuario:

- – (LOGIN) - Nombre con el que el usuario se identifica en el sistema
- – (PASWORD) - Palabra clave para acceder al sistema
- – (UID) - Identificador numérico del usuario
- – (GID) - Identificador numérico del grupo
- – (GCOS) - Información adicional sobre el usuario
- – (HOME) - Directorio inicial de trabajo
- – (SHELL) - Intérprete de comandos asignado al usuario
- (.profile, .login, .kshrc) - Información y variables de entorno para ejecutar aplicaciones.

Usuarios estándar

Usuario	UID	GID	Directorio principal	Shell
root	0	0	/root	/bin/bash
bin	1	1	/bin	/sbin/nologin
daemon	2	2	/sbin	/sbin/nologin
adm	3	4	/var/adm	/sbin/nologin
lp	4	7	/var/spool/lpd	/sbin/nologin
sync	5	0	/sbin	/bin/sync
shutdown	6	0	/sbin	/sbin/shutdown
halt	7	0	/sbin	/sbin/halt
mail	8	12	/var/spool/mail	/sbin/nologin
operator	11	0	/root	/sbin/nologin
games	12	100	/usr/games	/sbin/nologin
ftp	14	50	/var/ftp	/sbin/nologin
nobody	99	99	/	/sbin/nologin
rpm	37	37	/var/lib/rpm	/bin/bash
sshd	74	74	/var/empty/sshd	/sbin/nologin
apache	48	48	/var/www	/bin/false

Pseudo conexiones

- Las aplicaciones tienen que tener un propietario.
- Existen usuarios que están asociados a aplicaciones y servicios, con el nombre de la aplicación, (bin, daemon, lp, mail, news, ftp, sshd).
- No queremos que nadie pueda entrar en la máquina con estos nombres de usuarios.
- Se les asocia en el campo shell, el comando que tiene que ser ejecutado:

  /sbin/nologin – existe la cuenta pero está desactivada, presenta el mensaje de /etc/nologin.txt

  /bin/false – no hacer nada.

2. GRUPOS DE USUARIOS

¿Qué es un grupo de usuarios?

- Es una organización lógica de usuarios, hay uno para cada usuario o para un grupo de usuarios.

- Cada recurso tiene un **grupo propietario**. Los grupos son utilizados por el sistema para controlar los accesos a los recursos. Se definen políticas de acceso en base a los grupos.

grupos de usuarios predefinidos en el sistema:

- **system**– Grupo del administrador y al que pueden pertenecer ciertos usuarios.
- **daemon** – Grupo propietario de directorios especiales.
- **kmem** o **mem** – Grupo al que pertenecen programas que pueden acceder a la memoria del núcleo.
- **tty** – Grupo propietario de los archivos especiales de terminales.
- **email, cron**– Grupo al que pertenecen ciertas utilidades o subsistemas.
- **user,users** – Grupo al que pertenecen los usarios ordinarios por defecto.
- **weel** – grupo para usuarios con capacidad de administradores.

Atributos que definen el perfil de un grupo:

– (NOMBREGRUPO) - Nombre del grupo
– (PASWORD) - Palabra clave del grupo
– (GID) - Identificador numérico del grupo
– (LISTAUSUARIOS) - Lista de miembros del grupo

¿Cuentas de usuario?

- Atributos que definen a un usuario y su grupo mas los recursos, ficheros y directorios del usuario.

Grupos estándar

Grupo	GID	Miembros
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
lp	7	daemon, lp
mail	12	mail
games	20	
ftp	50	
nobody	99	
users	100	
rpm	37	rpm
floppy	19	
sshd	74	
apache	48	

3 FICHEROS DE MANTENIMIENTO DE USUARIOS Y GRUPOS

/etc/passwd /etc/group /etc/shadow /etc/gshadow

/etc/passwd

- Contiene la información mas relevante de un usuario.
- Tiene permiso de lectura para todos los usuarios del sistema, debido a que las tareas necesitan acceder a este fichero y leer información del propietario de los recursos.
- Es un fichero texto en el que cada línea corresponde a un usuario.
- Cada línea contiene siete campos separados por dos puntos (:).

LOGIN:PASWORD:UID:GID:GCOS:HOME:SHELL

/etc/passwd

1. LOGIN – Nombre con el que el usuario inicia una sesión en el sistema, es el nombre que los demás usuarios ven al listar los ficheros de ese usuario. Este nombre debe ser único. (santiago). 8 caracteres (glibc2 permite 31)
2. PASWORD – Contiene la contraseña codificada, o bien una **x** indicando que la contraseña codificada esta en el fichero /etc/shadow. **En blanco (¡no debería!)** indica que el usuario no tiene contraseña. (¿*$#&?(#&*+).
3. UID – Número entero 2**16 que identifica al usuario en el sistema, (¡debe ser único!). Los ficheros creados por un usuario guardan en un campo del inode este valor. Los procesos de un usuario guardan este valor en un campo de la tabla de procesos. (510).

/etc/passwd

4. GID- Número entero que identifica al grupo del usuario y con el que trabaja el sistema.

5. GCOS – Información adicional del usuario separada por comas como nombre y apellidos, dirección, telefonos. (Santiago Candela, Dto de informática, 928458700).

/etc/passwd

6. HOME – Directorio principal del usuario, es donde el usuario aterriza cuando entra en el sistema, contiene ficheros de ambiente y configuración para el usuario. (/home/santiago).

7. SHELL – Primer proceso que se ejecuta cuando el usuario entra en el sistema (login). Lo usual es que sea un procesador de comandos que se le asigna al usuario. (bash, ksh, csh).

/etc/group

- Es un fichero texto, visible por todos los usuarios, donde cada línea contiene información asociada a un grupo definido en el sistema.

- Cada línea del fichero contiene cuatro campos separados por dos puntos (:)

NOMBREGRUPO:PASSWORD:GID:LISTAUSUARIOS

/etc/group

1. NOMBREGRUPO – Nombre del grupo. Es el nombre que los usuarios ven como grupo propietario al listar los ficheros. Debe ser único. Se suele crear uno por usuario, y si es necesario uno global para agrupar a varios usuarios. (gsantiago).

2. PASSWORD – Contiene la contraseña codificada del grupo, o bien una **x** indicando que la contraseña codificada esta en el fichero /etc/gshadow. En blanco indica que el grupo no tiene contraseña. Es opcional, pero si se pone aumenta la seguridad de acceso a los recursos del grupo. (¿*$#&?(#&*+).

/etc/group

3. GID: Número entero que identifica al grupo y con el que trabaja el sistema. Debe ser único. Coincide con un identificador de grupo asignado a un usuario en /etc/passwd. (2098).

4. LISTAUSUARIOS – Lista de usuarios (nombre de login no el UID), separados por comas que pertenecen al grupo. (santiago, ana, luis).

/etc/shadow

- Fichero texto ¡solo visible por el root! Se utiliza para guardar las contraseñas de usuarios codificadas.

- Cada línea corresponde a un usuario. Tiene nueve campos separados por dos puntos (:).

LOGIN:CONTRASEÑA:DIAS_CAMBIO:
MIN_CAMBIO:MAX_CAMBIO:DIAS_AVISO:
DIAS_INHABILITAR:TIEMPO_INHABILITAR:RESERVADA

/etc/shadow

- LOGIN - Igual que el campo de /etc/passwd. (santiago)
- CONTRASEÑA - Contraseña de usuario codificada y escrita por el sistema. (¡ No puede estar en blanco!). (¿*$#&?(#&*+).
- DIA_NACIMIENTO – Define la fecha de nacimiento, o de la última modificación, de la contraseña respecto al 1 enero 1970 "unix timestamp" y expresada en días. Lo escribe el sistema.
- MIN_CAMBIO – Número entero, edad mínima en días que tiene que tener la contraseña para que se pueda cambiar. Un cero indica que el usuario puede cambiar la contraseña en cualquier momento. Campo opcional. (15, la contraseña tiene que tener una edad mínima de 15 días para que se pueda cambiar).

/etc/shadow

- MAX_CAMBIO – Número entero, edad máxima en días de la contraseña. Establece el vencimiento de la contraseña. Campo opcional, en blanco no establece edad máxima. (180, a los 180 días expira la contraseña).
- DIAS_AVISO – Número entero que establece los días antes de la edad máxima (MAX_CAMBIO), que el sistema comenzará a solicitar al usuario que cambie la contraseña. (7 una semana antes es usual).

- DIAS_INHABILITAR – Plazo en días que se concede si se caduca la contraseña sin cambiar para que el sistema inhabilite la cuenta del usuario. (2, al cabo de dos días de expirar la contraseña se inhabilita la cuenta).

- TIEMPO_INHABILITAR – Define el número de días después del cual se inhabilitara la cuenta y el usuario no podrá utilizar el sistema. Es opcional si se deja en blanco no inhabilita.

/etc/gshadow

- Fichero para guardar las contraseñas codificadas de los grupos. Solo lo puede ver el root.
- Es un fichero texto, donde cada línea tiene información de un grupo definido en /etc/group. Cada línea tiene cuatro campos separados por dos puntos (:).

- NOMBREGRUPO: CONTRASEÑA: ADMINISTRADORES:MIEMBROS

/etc/gshadow

- NOMBREGRUPO – Nombre del grupo. Igual que /etc/group. (gsantiago).
- CONTRASEÑA - Contraseña del grupo codificada. Si el grupo no tiene contraseña esta en blanco. (¿*$#&?(#&*+).
- ADMINISTRADORES – Lista de nombres de usuarios, separada por comas, que son administradores del grupo y pueden añadir o quitar usuarios al grupo. (santiago, ana).
- MIEMBROS – Lista de nombres de usuarios, separada por comas, que son miembros del grupo. (santiago, ana, luis).

Ficheros de inicialización y entorno de los usuarios

/etc/profile

- Se ejecuta cada vez que un usuario entra en el sistema, el administrador fija variables generales o de entorno por ejemplo umask. Utiliza ficheros de entorno de /etc/profile.d

/etc/login.defs

- Contiene información de configuración para crea usuarios y grupos. Es utilizado por aplicaciones como useradd/adduser y groupadd.

/etc/bashrc

- Define funciones y alias

/etc/default/useradd

- Valores por defecto al crear un usuario, como home, máximo numero de procesos.

Ficheros de inicialización y entorno de los usuarios

/etc/skel

- Directorio con ficheros de configuración. Se copian en el directorio de trabajo de cada usuario. Se utilizan para configurar el entorno grafico, el shell.

~/.bash_profile

- Configura variable PATH, PS1, variables de entorno y llama .bashrc

~/.bashrc

- Define alias y llama a fichero /etc/bashrc

~/.bash_history

- Guarda el historial de los últimos comandos ejecutados, se pueden ver con el comando history

~/.bash_logout

- Se ejecuta cuando el usuario sale con un exit.

Ficheros de inicialización y entorno de los usuarios

/etc/motd

- Contine el mensaje del día, una vez hecho el login.

/etc/issue.net

- Contine el mensaje que aparece en pantalla antes de que el usuario haga login.
- \r muestra la versión del núcleo
- \m muestra la arquitectura de la máquina

/etc/shells

- Contiene los interpretes de comandos definidos en el sistema.

4. Mantenimiento de las cuentas de usuarios

TAREAS DE UN ADMINISTRADOR:

- Crear usuarios
- Modificar atributos
- Desactivar usuarios
- Eliminar usuarios
- Crear grupos
- Añadir o borrar usuarios a grupos
- Eliminar grupos

CREACIÓN DE CUENTAS DE USUARIO, PASOS A SEGUIR:

- Entrar en el sistema como usuario root
- Asignar los identificadores: LOGIN, UID, GID.
- Decidir su intérprete de comandos inicial. SHELL.
- Creación de su directorio de trabajo. HOME
- Asignarle una palabra de paso. CONTRASEÑA
- Establecer sus archivos de inicio de sesión. /etc/skel, /etc/login.defs
- Hacer que sea propietario de su directorio inicial y archivos de inicio de sesión.
- Proporcionarle las utilidades necesarias.
- Activarle utilidades del sistema para el control de uso de recursos.

CREACIÓN DE CUENTAS DE USUARIO

Estas tareas se pueden hacer

- Manualmente: manipulando directamente los archivos (/etc/passwd, group, shadow, gshadow).
- Automáticamente: mediante utilidades (useradd, usermod, userdel, groupadd, groupmod, groupdel, pwconv, chage) que modifican los archivos.

Creación de un usuario manualmente:

- Editando y añadiendo una línea en (/etc/group y /etc/passwd), con el perfil del usuario. En el campo passwd, colocar una x para que se codifique la contraseña en /etc/shadow.

- Editando y añadiendo una línea en los archivos dónde se codifican las contraseñas (/etc/shadow, /etc/gshadow), colocando sus campos acordes a lo colocado en passwd y group.

- Asignarle una palabra de paso (/bin/passwd) al usuario (¡obligatorio!) y al grupo (opcional).

Creación de un usuario manualmente:

- Creación de un directorio de trabajo. MKDIR. (normalmente colgando de /home/).
- Copiar en su directorio los ficheros de inicio y configuración cp /etc/skel
- Hacer propietario al usuario de su directorio de trabajo y ficheros. CHOWN
- Configurar los permisos del grupo propietario. CHGRP.

Creación de cuentas de usuario mediante utilidades

A nivel de línea de comandos (useradd)

- useradd, usermod y userdel — añadir, modificar y eliminar cuentas de usuarios.
- groupadd, groupmod y groupdel — para añadir, modificar y eliminar grupos de usuarios.
- passwd – para colocar una contraseña a un usuario
- gpasswd — para administrar el archivo /etc/gshadow.
- pwck, grpck — para la verificación de contraseñas, grupo y archivos shadow asociados.
- pwconv, pwunconv — Herramientas para la conversión a contraseñas shadow y de vuelta a contraseñas estándar.
- chage – para cambiar la fecha de vencimiento de la contraseña de usuario

Creación de cuentas de usuario mediante utilidades

También se hace uso de los comandos:

- **mkdir** – crear un directorio.
- **chmod** – cambiar permisos.
- **chown** – cambiar propietario.

- **man 5 group, passwd, shadow** – para ver la información de los ficheros.
- **man 8 passwd** - para ver los comandos del administrador del sistema.

Creación de cuentas de usuario mediante utilidades

A nivel de aplicación gráfica

La forma más fácil de manejar usuarios y grupos.

No es estandar, cada distribución de Linux viene con la suya propia.

En Red Hat Configuración del Sistema -> Usuarios y Grupos