Gestión de usuarios

Joaquín Seoane Pascual
joaquin@dit.upm.es

Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid

5 de noviembre de 2001

Índice General

Gestión de usuarios

- Mecanismo de identificación.
- Mecanismo de autentificación.
- Dar de alta o baja.
- Ajuste de entorno cómodo.
- Ajuste de prerrogativas y limitaciones.

Identificación de usuarios

- Para procesos Unix:
  - Bajo nivel (núcleo): uid, gid, grupos.
  - Alto nivel (tabla asociativa): nombres de usuario y de grupo.
- Para aplicaciones: depende.
  - ppp.
  - Servicios WEB privados, bases de datos.
  - Sistemas de ficheros remotos.
  - ...

Autentificación de usuarios

- Depende del servicio.
- Debería ser transparente e intercambiable:
  - Contraseña fija.
  - Contraseña de una vez.
  - Tarjeta *inteligente*.
  - Huella digital, iris,...
- Deberían poderse intercambiar las bases de datos.

Prerrogativas y limitaciones

- Asignación de directorio de trabajo (*cuenta*).
- Permisos de acceso a ficheros, dispositivos, etc.
- Servicios a los que puede acceder.
- Buzón de correo.
- Programas que puede ejecutar.
- Desde donde puede acceder, cómo y cuándo.
- Limitación de recursos: disco, procesador, memoria virtual, procesos, etc.

Bases de datos de usuarios

- Tradicional (contraseñas cifradas visibles).
- Contraseñas ocultas.
- Local (fichero) o remoto (NIS, LDAP, Radius, NCP, SMB, Kerberos, ...).

Base de datos de usuarios tradicional

- `/etc/passwd` y `/etc/group`, con contraseña cifrada legible.
- Especifica uid, gid principal, nombre para identificar (GECOS), directorio y *shell*.
- Puede cambiarse gid con:
  - `newgrp` (posiblemente dando contraseña).
  - Cambiándose a directorio *setgid*.
- Extensible a la red.
- Vulnerable por aplicación de diccionarios y algoritmo de cifrado.

Base de datos en la sombra

- La base de datos se divide en dos:
  - `/etc/passwd` (legible, con x en contraseña) y `/etc/shadow` (ilegible).
  - `/etc/group` y `/etc/gshadow`.
- Nunguna ventaja en red.
- Añade plazos de mantenimiento y cambio de contraseñas y mantiene duraciones.
- Requiere que los ficheros públicos y privados estén sincronizados.
- En Debian se pasa con `shadowconfig on|off`

Mantenimiento de cuentas

- Altas (Debian): `adduser, addgroup`.
  Configurables con `/etc/adduser.conf`:
  - Asigna rangos de usuarios y grupos asignables y contabiliza los asignados.
  - Política de creación de grupos.
  - Cuota inicial de disco.
  - Crea directorio de cuenta según política.
  - Pasa esqueletos: `/etc/skel`.
- Cambio de información: `passwd, chfn, chsh, chage, usermod, groupmod`.
- Bajo nivel: `useradd, groupadd, userdel, groupdel`.
- Muy bajo nivel: editando bases de datos tradicionales.

Mantenimiento descentralizado de grupos

- A veces es interesante nombrar un administrador de grupo.
- Lo nombra el administrador del sistema.
- Le delega las altas y bajas en el grupo y la contraseña para visitantes.
- A través de `gpasswd`.

Entorno privado inicial y entorno común

- Los esqueletos proporcionan configuraciones aceptables y sugieren políticas.
- Difícil cambiar políticas con los esqueletos: mejor entorno común:
  - General: `/etc/environment`, para:
    LANG, LANGUAGE, EDITOR, VISUAL, PAGER,..
  - Por herramienta (cambiable):
    `/etc/profile, /etc/inputrc, /etc/lynx.cfg,` ...
  - Cambiable (`/etc/pine.conf`)
    y no cambiable (`/etc/pine.conf.fixed`).

Internacionalización y localización

- Internacionalización (i18n): Programas aptos para diversos entornos.
- Localización (l10n): configuración para un entorno.
- Locales:
  - LC_CTYPE: clasificar caracteres en letras, números, puntuación, etc...
  - LC_COLLATE: reglas de ordenación de caracteres.
  - LC_NUMERIC: reglas de escritura de números.
  - LC_MONETARY: moneda.
  - LC_TIME: representación de fecha y hora.
  - LC_MESSAGES: idioma (mensajes, documentación).
  - LANG: idioma y país (eg: es_ES, es_CO, en_UK).
  - LANGUAGE: lista de idiomas aceptables (eg: es:en:fr).

Límites y restricciones

- Cuotas de disco (temporal y estricta):
  Paquete `quota`, montaje con opciones `usrquota,grpquota`, Necesita activación en el núcleo.
- Contraseñas (cracklib, comprobación al cambiar configurable).
- Terminales seguros: `/etc/securetty`.
- Shells aceptables: `/etc/shells`.
- Quiénes entran desde dónde: `/etc/security/access.conf`.
- Quiénes entran y cuándo: `/etc/security/time.conf`.
- Cuántos recursos de procesador pueden consumir: `/etc/security/limits.conf`.

Contabilidad

- Registrar uso de disco `quota` o `find`...
- Registrar entradas y salidas:
  `/var/log/wtmp`, visible con `last`.
- Registro de aplicaciones utilizadas y recursos consumidos:
  Paquete `acct`, visible con `sa -u`, etc... Necesita activación en el núcleo.
- Registro de recursos de red...

Separación de políticas y mecanismo

- Tradicionalmente cada aplicación autentificaba sus usuarios:
  - Dificultad de política común y reconfiguración.
  - Reinventar siempre la rueda.
  - Separación configurable.
    - Transparente (POSIX): `/etc/nsswitch.conf`.
    - Módulos de autentificación apilables (PAM):
      - Autenticación: identifica asigna uid/gid.
      - Cuentas: permisos (hora, lugar,..), recursos.
      - Sesiones: entrada y salida.
      - Contraseñas.

Módulos de autentificación apilables (PAM)