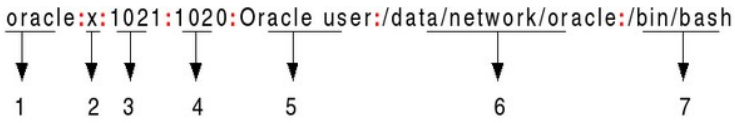
ASO – Permisos i gestió d'usuaris

Les bases de dades del sistema

/etc/passwd

Aquest arxiu conté informació sobre els usuaris del sistema la qual és requerida durant el procés de login. És accessible (r) per tots els usuaris, ja que moltes comandes l'utilitzen per a mapejar l'UID amb el nom d'usuari, buscar el home de l'usuari i executar el seu shell.

És un fitxer de text pla que conté una entrada (línia) per cada usuari del sistema. Els camps estàn separats per un símbol de '**:**'. Té un total de set camps:



1. **username:** Utilitzat en el login de l'usuari. Entre 1 i 32 caràcters.
2. **Password:** Un caràcter "x" indica que el password encriptat es troba en l'arxiu /etc/shadow. Per a fer canvis de password es fa servir la comanda **passwd** que calcula el hash i el guarda a /etc/shadow.
3. **UID:** Cada usuari té assignat un ID. UID=0 està reservat per l'usuari root, el rand de 1-99 està reservat per usuaris predefinits del sistema (utilitzar serveis sense privilegis root). Els UID de 100 a 999 estàn reservats per les comptes del sistema.
4. **GID:** Cada grup té assignat un ID. Aquest es el ID del grup primari de l'usuari.
5. **UID Info:** Camp de comentari. Un string d'informació extra sobre l'usuari.
6. **Director home:** Path absolut al directori home de l'usuari. Si no es posa per defecte s'utilitza "/".
7. **Command/shell:** Path absolut al shell. Normalment es un shell, però no es estrictament necessari que sigui un shell.

/etc/group

És un fitxer de texte on es defineixen els grups on pertanyen els usuaris d'un sistema Unix/Linux. L'ús de grups permet atorgar permisos a diferents tipus d'usuaris sobre arxius de manera organitzada.

```
<nomgrup>:<password>:<GID>:<llista d'usuaris separats per coma>
aso:x:24:rserral,aso23,professor
```

Generalment el password no s'utilitza en els grups i sol estar en blanc, es pot fer servir per implementar grups privilegiats. Existeixen grups especials:

wheel: Grup d'usuaris amb privilegis d'administració.
nobody: Grup especial per NFS
users: Tots els usuaris hi pertanyen.

/etc/shadow

Aquest arxiu és el que conté els passwords dels usuaris en un format encriptat (conté els hash dels passwords realment). Conté una entrada per cada usuari llistat en /etc/passwd.

1. username: Login name.
2. password: El teu password encriptat. Normalment té un format de: `$id$salt$hashed` on `$id` és l'algorisme utilitzat per a hashejar el password (p.e 1 és MD5).
3. Últim canvi de password: Dies des de 1 de Gener de 1970 que el password es va canviar per ultim cop.
4. Minim: Minim nombre de dies requerit entre els canvis de password.
5. Maxim: El nombre màxim de dies que el password de l'usuari serà valid, més tard serà forçada a canviar-lo.
6. Warn: El nombre de dies abans de que caduqui el password perquè l'usuari sigui avisat de canviar-lo.
7. Inactiu: Nombre de dies des de que el password ha caducat en que l'usuari es deshabilitarà.
8. Expire: Dies des de 1 de Gener de 1970 en que el compte es deshabilitarà

passwd per a canviar el password.
chage permet canviar la política d'expiració.

/etc/aliases

Base de dades d'alias d'e-mail. Permet redireccionar el mail.

Comandes bàsiques per a la gestió

useradd (adduser) / userdel – Afegir / eliminar un usuari.
usermod – Modificar tot excepte el username.
passwd – Editar el password.
newusers – creació de nous usuaris en batch.
vipw – editar de forma segura (fa lock) l'arxiu /etc/passwd

groupadd / groupdel – afegir / eliminar un grup
groupmod- Modificar tot excepte el groupname
gpasswd / passwd -g – Editar el password del grup.
newgrp, sg – Afegir grups en batch
vigr – Editar l'arxiu /etc/groups

Desactivació i baixa d'usuaris

Desactivació d'un usuari (temporal - indefinit)
→ Invalidar el password
    → Afegir un caràcter il·legal (*****) al camp password de /etc/passwd.
    → Això permet recuperar el seu password antic si es necessita (no l'elimina).
→ Invalidar el seu intèrpret de comandes:
    → Canviar-lo per un altre (/bin/false | /bin/nologin)
    → Això informa a l'usuari que ha estat desactivat.
    → Avisa a l'admin si l'usuari intenta entrar al sistema.

Baixa d'un usuari

Hem d'estar segurs que aquest usuari ja no necessitarà el seu compte. El procés és:

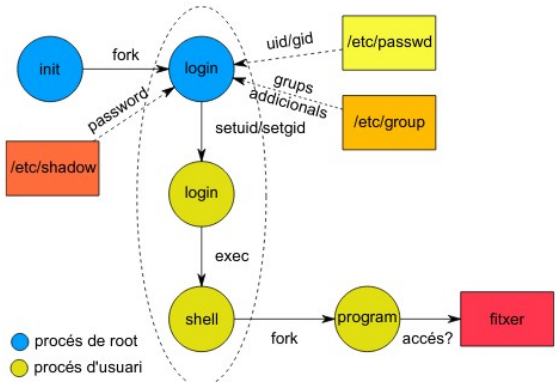
1. Comprovar que l'usuari no estigui treballant en la màquina.
2. Desactivar el compte (Apartat anterior).
3. Fer un backup de les seves dades.
4. Esborrar les dades.
5. Eliminar l'usuari de les BD del sistema (shadow, passwd, group).
6. Afegir una redirecció al seu correu electrònic (/etc/aliases).

Bases de gestió d'usuaris

Assignació de UIDs – No reciclar-los mai.
Assignació de usernames – Guardar despatx i telèfon de contacte dels usuaris.
Organització del home

→ Plana: (/home/<usuari>)
→ Jeràrquica, diferents nivells de directoris:
→ /home/<dpt>/<user>
→ pot ser en múltiples discs.

El procés de login:



Primer de tot té lloc el procés de **init**. Un cop acaba surt el prompt del user i password (login). A continuació el procés comprova les credencials d'usuari verificant-ho als respectius fitxers /etc/passwd i /etc/group i /etc/shadow. Si coincideix comença a buscar les propietats de l'usuari. Sinó repetiex el prompt de credencials fins a 3 vegades. Es recullen les propietats de l'usuari i les variables de sessió de les BDs del sistema i fa un setuid/setgid i finalment s'inicia l'usershell perquè l'usuari pugui executar comandes.

Elevació de privilegis

Utilitzant crides a SetUID / SetGID. S'ha de tenir en compte que treballar com a root es perillós ja que podem cagar-la molt, i per moltes coses és innecessari. El millor és tenir un usuari administrador i elevar els privilegis quan sigui necessari. Per a fer-ho:

→ **su [usuari] [-c comanda]**: Permet canviar d'usuari i executar comandes com aquell usuari. Per defecte sempre es root (si no especifiquem l'usuari).
→ **sudo [comanda]:** Permet executar una comanda com un altre usuari. L'admin pot especificar les comandes que cada usuari pot executar utilitzant sudo.

Permisos i proteccions

	Fitxers	Directoris
r	Llegir els continguts	Llistar els continguts
w	Escriure/Modificar les continguts	Afegir/esborrar fitxers
x	Executar	Accedir al directori
SetUID	S'executa amb l'UID del propietari	No té efecte
SetGID	S'executa amb l'GID del propietari	Els fitxers es creen amb el mateix grup propietari que el directori
Sticky Bit	No té efecte	Només els propietaris dels fitxers el poden esborrar

El format dels permisos es el següent:

(-, d) rwx rwx rwx propietari grup

Tenim 3 tipus de permisos: Lectura, escriptura i execució. Tant en fitxers normals com en directoris. S'apliquen en tres àrees: Propietari, grup i altres. Les principals comandes per la gestió dels permisos són:

chown: canviar el propietari.
chgrp: canviar el grup
chmod: canviar els permisos

Bit Set-UID/Set-GID (s): Si el bit SetUID està actiu, qualsevol executant aquella comanda (o arxiu) herederà els permisos del propietari de l'arxiu. El mateix amb el SetGID.
Bit Sticky (t) – Només als directoris: Si el directori té el bit sticky actiu, llavors aquells arxius de dins només poden ser eliminats per el propietari del directori/arxiu o l'usuari root. Això fa que no puguis borrar arxius d'altres usuaris en directoris publics.