



NF2. ADMINISTRACIÓ DE PROGRAMARI BASE

1. Administració d'usuaris i grups locals

1.1 Administració d'usuaris i grups a sistemes Linux

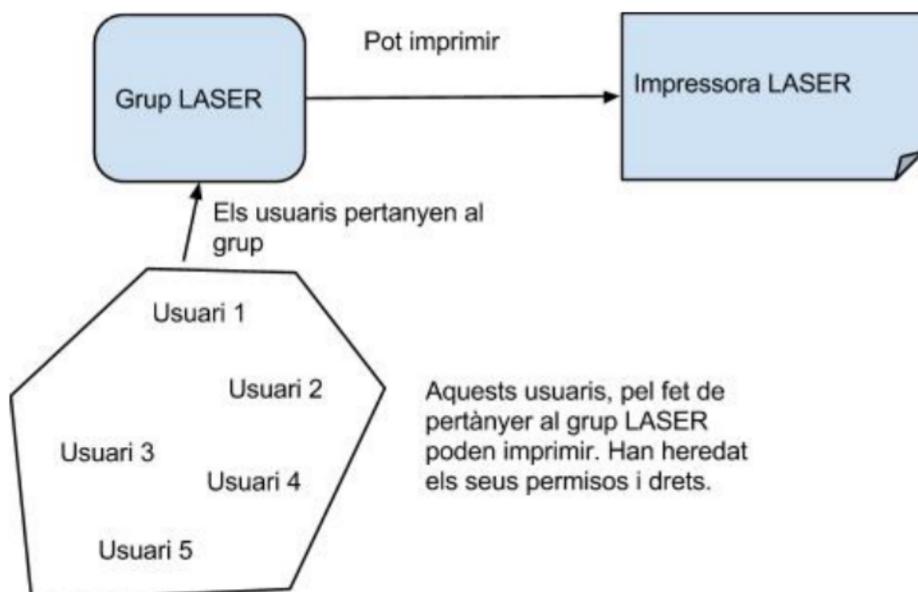
Una de les característiques principals d'un sistema operatiu del tipus GNU/Linux és la capacitat de gestionar diferents usuaris en un mateix sistema. De fet, es diu que el GNU/Linux és un sistema operatiu multiusuari, perquè incorpora totes les eines necessàries per dur a terme aquesta gestió.

A més a més, el GNU/Linux té la capacitat de donar suport a diferents usuaris que treballin de manera simultània a la mateixa màquina, localment, per mitjà d'una xarxa d'àrea local o, fins i tot, per Internet. Cadascun d'aquests usuaris del sistema té assignat un directori personal, dins del qual té tots els permisos possibles (lectura, escriptura, execució). Així doncs, cada usuari pot tenir els seus documents, fitxers descarregats, preferències i aplicacions, sense que hi hagi cap interferència entre ells.

La majoria de sistemes Linux tenen dos modes bàsics de funcionament, que són els següents:

- **Mode de text** (consola de text): mode ràpid i austèr que s'assembla a antics sistemes operatius sense pantalla gràfica, amb ratolí i característiques de multitasca i multiusuari.
- **Mode gràfic**, que sembla que és millor i més vistós però que consumeix força més recursos del sistema.

Tanmateix, un sistema operatiu conté els anomenats grups d'usuaris. Un grup és un conjunt d'usuaris i bàsicament s'empra per a simplificar l'assignació de drets i permisos als usuaris. Per exemple: si volem fer que un conjunt d'usuaris pugui imprimir a través d'una determinada impressora. Una forma seria assignar els permisos necessaris usuari a usuari o bé, la millor forma, crear un grup, donar permisos al grup i ficar a tots els usuaris en aquest grup. Pel fet d'estar en aquest grup *hereta els seus drets i permisos*.





1.1.1 Fitxer amb informació d'usuaris

Als sistemes GNU/Linux, la informació sobre els usuaris està localitzada en el fitxer `/etc/passwd`. Si en mirem el contingut, obtindrem una llista semblant a la següent:

```
mysql:x:120:128:MySQL Server,,,:nonexistent:/bin/false
david:x:1001:1001:David López,,,:/home/david:/bin/bash
libvirt-qemu:x:121:131:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false
alfonso:x:1002:1002:alfonso,,,:/home/alfonso:/bin/bash
jordi:x:1003:1003:jordi,,,:/home/jordi:/bin/bash
```

I descriu el tipus d'informació següent:

```
nom_usuari:contrasenya:UID:GID:comentaris:directori_home:shell_d'accés
```

I cadascun d'aquests paràmetre té el següent significat:

1. Nom d'usuari: *login* de l'usuari (nom que fa servir per a iniciar o fer servir els recursos del sistema).
2. Contrasenya: originalment aquí s'emmagatzemava la contrasenya, en els sistemes actuals i com a garantia de seguretat extra s'emmagatzemen al fitxer `/etc/shadow` només lleigble per `root`
3. UID (*User Identification*): codi d'identificació de l'usuari.
4. GID (*Group Identification*): codi d'identificació del grup a què pertany l'usuari.
5. Directori *home*: definició del directori personal (o per defecte) de l'usuari.
6. *Shell* d'accés: intèrpret d'ordres que utilitza l'usuari en les seves sessions. Un intèrpret de tipus `/bin/false` indicarà que l'usuari no pot iniciar sessió.

1.1.2 Fitxer amb informació de les contrasenyes

Es considera un risc de seguretat mantenir cap contrasenya en el fitxer `/etc/passwd`, perquè qualsevol persona amb drets de lectura pot executar un programa i obtenir les contrasenyes sense gaire dificultat. Per evitar aquest risc, es fan servir contrasenyes ocultes de manera que només aparegui una `x` en el camp de contrasenya del fitxer `/etc/passwd`. Les contrasenyes es desen en el fitxer `/etc/shadow`, al qual només té accés l'usuari administrador.

Un exemple del fitxer `/etc/shadow` podria ser el següent:

```
david:$6$XTjelD$d7yE6xvYrj/x2J8Bt02WsngXPpSEFNX8zFWsw.akmAv5Px.rMPN/ldYrxC12vbsWMGap8
libvirt-qemu:!::16685:0:99999:7:::
alfonso:$6$R7R6AzRH0Aca0gk/$Xyix10FLzNb04x0WuuB14qjx2Iv0kmGRFo0JY6/06tnnDxpsGfLfXMqRT
jordi:$6$51uTX/7bAzizoqxb$77yHMJ7tDgwQpD4PhHJUtkHMizDzfeqzX.3iuT/j2liKp6u0Lr5TfoyjnZFr
```

- Nom d'usuari per iniciar la sessió.
- Contrasenya encriptada de l'usuari.
- El nombre de dies des de l'1 de gener de 1970 fins al darrer canvi de contrasenya. Aquesta data és coneguda en el món de l'UNIX com a *epoch*.



- El nombre de dies que han de passar abans que la contrasenya es pugui canviar. Aquest camp indica un mínim de dies de la validesa de la contrasenya.
- El nombre de dies després dels quals la contrasenya s'ha de canviar. Aquest camp indica un màxim de dies de validesa de la contrasenya. Es pot modificar per forçar el canvi de contrasenya.
- El nombre de dies abans que s'avisi l'usuari que la seva contrasenya expirarà.
- El nombre de dies després del canvi de contrasenya i que fa que s'inhabiliti el compte d'usuari.
- El nombre de dies des de l'1 de gener del 1970 en què el compte d'usuari s'ha desabilitat.
- El darrer camp reservat, que actualment no es fa servir per a res.

Per a l'encriptació de la contrasenya el sistema pot fer servir els següents algoritmes:

- Si la contrasenya està precedida per \$1\$: Es fa servir l'algoritme MD5 de 32 caràcters hexadecimals.
- Si la contrasenya està precedida per \$2\$: Es fa servir l'algoritme *blowfish* (xifratge simètric, depèn de la longitud de la clau).
- Si la contrasenya està precedida per \$5\$: Es fa servir l'algoritme SHA-256 de 64 caràcters hexadecimals.
- Si la contrasenya està precedida per \$6\$: Es fa servir l'algoritme SHA-512 de 128 caràcters hexadecimals.

El fitxer `/etc/shadow` només hauria de tenir permisos de lectura i escriptura per a l'usuari administrador; la resta d'usuaris no hauria de tenir cap permís de lectura ni d'escriptura (cadena de permisos: 600).

1.1.3 Fitxer amb informació de grups

La informació sobre els grups del sistema, i el seu identificador, està localitzada en el fitxer `/etc/group`, i les contrasenyes de grup són en el fitxer `/etc/gshadow`. Si en mirem el contingut, obtindrem una llista semblant a la següent:

```
mysql:x:128:  
david:x:1001:  
lpadmin:x:129:  
libvirt:x:130:  
kvm:x:131:  
libvirt-qemu:x:132:libvirt-qemu  
alfonso:x:1002:  
jordi:x:1003:
```

I descriu el tipus d'informació següent:

`nom_grup:contrasenya:GID:llista_usuaris`

I cadascun d'aquests paràmetre té el següent significat:

1. Nom del grup: nom del grup del sistema.
2. Contrasenya: contrasenya del grup del sistema.
3. GID (Group Identification): codi d'identificació del grup del sistema.



4. Llistat d'usuaris: tots els usuaris que pertanyen a aquest grup.

Linux té dos tipus de grups per als usuaris. Un usuari té un grup principal i pot tenir diversos grups secundaris. No hi ha diferència entre un i altres. No és més important un grup principal que un grup secundari.

El grup principal és obligatori: tot usuari ha de tenir un grup principal i els grups secundaris, que en poden haver molts, són opcionals.

La diferència simplement és en com desa Linux la seva informació (el grup principal d'un usuari s'indica en `/etc/passwd` com a GID, i els secundaris s'indiquen a `/etc/group`) i quan es crea un arxiu o una carpeta (si l'usuari A, crea un arxiu, a aquest se li assignen permisos específics per a l'usuari A, per al grup principal d'A i per a la resta d'usuaris del sistema).

```

/etc/passwd
armand:x:1000:1000:armand,,,:/home/armand:/bin/bash
mysql:x:113:121:MySQL Server:/nonexistent/false

/etc/group
video:x:44:armand
audio:x:45:
plugdev:x:46:armand
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuuid:x:101:
crontab:x:102:
fuse:x:103:
scanner:x:104:saned,armand
messagebus:x:105:
colord:x:106:
lpadmin:x:107:
ssl-cert:x:108:
bluetooth:x:109:armand
netemper:x:110:
netdev:x:111:armand
Debian-exim:x:112:
mlocate:x:113:
ssh:x:114:
avahi:x:115:
pulse:x:116:
pulse-access:x:117:
rtkit:x:118:
saned:x:119:
Debian-cdrom:x:120:
armand:x:1000:
mysql:x:121:
vhnxiusers:x:122:

```

Aquest és el grup principal de l'usuari armand. (Per defecte a Ubuntu, per a cada usuari que es crea se li crea un grup principal amb el mateix nom)

Aquest són grups secundaris als quals pertany l'usuari armand

1.1.4 Eines de gestió d'usuaris i grups en mode text

Només l'usuari administrador del sistema (superusuari o usuari primari) pot administrar els comptes d'usuaris i grups, creant-los de nou, esborrant-los o modificant-ne els comptes. Els usuaris normals, que no tenen drets d'administració, no poden utilitzar cap eina de gestió d'usuaris, ni poden modificar els paràmetres del seu compte d'usuari com, per exemple, el directori personal o la contrasenya.

Creació d'usuaris

Per a crear usuaris en mode text tenim la comanda `adduser`. La sintaxi bàsica d'aquesta comanda és `adduser [opcions] login_usuari` i algunes de les opcions que podem especificar són:

- `--ingroup nom_grup`: Ens permet afegir el nou usuari a un grup ja existent.



- `--uid num_id`: Permet determinar el número d'identificador del nou usuari.
- `--home dir_home`: Permet determinar el direcra.xtec.cat/tori personal del nou usuari.

Aquesta comanda també ens permetrà, posteriorment a la creació de l'usuari, afegir-lo a algun dels grups del sistema, en aquest cas la farem servir de la següent manera: `adduser nom_usuari nom_grup`

Un aspecte interessant és que cada cop que creem un usuari es copia tot els contingut de `/etc/skel` al directori d'usuari del nou usuari que acabem de crear. Així doncs, podem crear un usuari, configurar l'aspecte del seu escriptori (colors, temes, ...), ficar arxius a qualsevol carpeta, configurar el navegador, ... i després copiar tot el directori d'usuari a dins de `/etc/skel`. Així, cada cop que creem un usuari es copiarà aquest contingut i tindrem la seva mateixa configuració.

Esborrament d'usuaris

Per a esborrar usuaris que existeixen al sistema farem servir la comanda `deluser [opcions] login`. Algunes de les opcions que podem afegir són:

- `--remove-home`: Ens permet esborrar el directori personal de l'usuari.
- `--remove-all-files`: Ens permet esborrar tots els fitxers del sistema que pertanyin a l'usuari que estem esborrant.

Aquesta comanda també ens permetrà treure un usuari d'un grup si la fem servir de la següent manera: `deluser usuari grup`

Creació de grups

La comanda que farem servir per a crear grups al sistema Linux serà la següent: `addgroup [opcions] grup`. Algunes de les opcions són:

- `--gid num_gid`: Permet determinar el número d'identificador del nou grup.

Esborrament de grups

La comanda per a esborrar grups del sistema és la següent: `delgroup [opcions] grup`. Algunes de les opcions que admet són:

- `--only_if_empty`: Esborra el grup només si no té cap membre.

Consulta dels grups als que pertany un compte

La comanda que fem servir per a consultar els grups als que pertany un usuari és `id [-ug] [usuari]`.

Els paràmetres més habituals d'aquesta comanda són:

- Sense paràmetres ens mostra els nostres grups. El grups principal i la resta.
- `-u`: Mostra únicament l'identificador d'usuari.
- `-g`: Mostra únicament l'identificador de grup principal.

Canvi del grup principal d'un compte





La comanda que ens permet canviar de grup principal és `newgrp grup`. Evidentment hem de pertànyer al grup que volem establir com a grup principal.

```
david@borriquito:~$ id  
uid=1000(david) gid=1000(david) grups=1000(david),24(cdrom),25(floppy),29(audio),30  
david@borriquito:~$ newgrp cdrom  
david@borriquito:~$ id  
uid=1000(david) gid=24(cdrom) grups=24(cdrom),25(floppy),29(audio),30(dip),44(video)  
david@borriquito:~$ █
```

Per a canviar de contrasenyes fem servir la comanda `passwd [-e] [usuari]`. El paràmetres més comuns d'aquesta comanda són:

- Sense paràmetres ens permet canviar la nostra contrasenya.
- Si afegim l'usuari, podrem canviar la contrasenya de l'usuari triat. Evidentement això només ho podrem fer si som administradors del sistema.
- El paràmetres `-e` ens permet obligar a l'usuari a canviar la seva contrasenya la propera vegada que iniciï sessió.

1.1.5 Eines gràfiques de gestió d'usuaris i grups

Tots els entorns gràfics del sistema Linux tenen programes gràfiques que ens permeten realitzar la gran majoria de les tasques de gestió d'usuaris. La gestió d'usuaris amb aquestes eines és més senzilla i ens ofereix algunes utilitats interessants, com per exemple la generació automàtica de contrasenyes, però és molt menys flexible que la gestió textual, ja que, aquesta última, ens permet la generació d'*scripts* que automatitzen la creació d'usuaris i la seva adscripció a grups.

1.2 Administració d'usuaris i grups a sistemes Windows

«Usuaris i grups locals» és una eina que es pot utilitzar per administrar els usuaris i grups locals a un sistema Windows. Un **usuari** o **grup local** és un **compte al qual es poden concedir permisos i drets des de l'equip**. L'*administrador de la xarxa* administra als *usuaris i grups globals o del domini*. A un **grup local** se li poden afegir **usuaris locals, usuaris globals i grups globals**. Però no es poden afegir usuaris locals a un **grup global**.

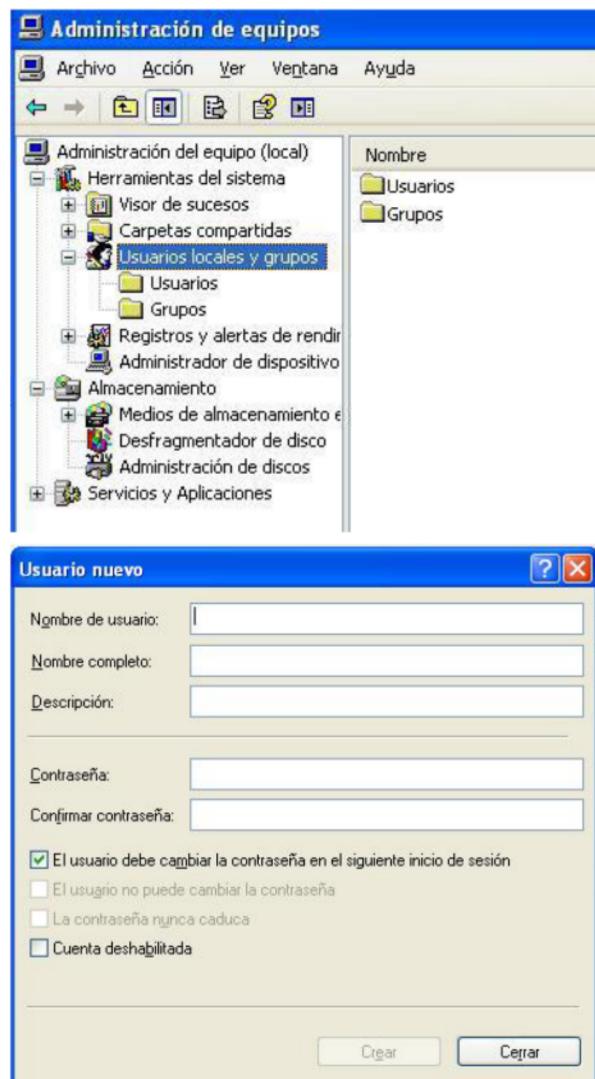
Els usuaris i els grups tenen importància en la seguretat de Windows perquè en assignar-lis drets i permisos, es pot limitar la capacitat dels usuaris i els grups per a dur a terme certes accions. Un **dret** autoritza a un usuari a realitzar certes accions en un equip, com fer còpies de seguretat d'arxius i carpetes o apagar l'equip. Un **permís** és una regla associada amb un objecte (normalment un arxiu, carpeta o impressora) que regula els usuaris que poden tenir accés a l'objecte i de quina manera.

Quan es creen comptes d'usuari i s'assignen a grups, existeixen conseqüències importants relatives a la seguretat. Mira a l'annex l'apartat Configuració de seguretat predeterminada, on s'expliquen els grups predeterminats i les tasques que poden dur a terme.



1.2.1 Crear un compte d'usuari a Windows 7

Obre «Administració d'equips». A «Usuaris locals i grups», fes *click* a «Usuaris». Premem «Acció» i després «Usuari nou».



Escriu la informació corresponent al quadre de diàleg que apareix i activa o desactiva les següents caselles:

- **Contrasenya i confirmació de contrasenya:** L'administrador pot proporcionar una paraula de pas a l'usuari.
- **L'usuari ha de canviar la contrasenya al següent inici de la sessió:** Al proper inici de sessió l'usuari haurà de canviar la seva paraula de pas. Posteriorment ja no haurà de fer-ho. Això permet a l'administrador que l'usuari escollí obligatòriament la seva paraula de pas.
- **L'usuari no pot canviar la contrasenya:** Es pot utilitzar per a comptes d'usuari que han de tenir les paraules de pas fixes, com per exemple tots aquells comptes compartits per molts usuaris. Si no es fixés la paraula de pas, llavors qualsevol usuari podria canviar-la i en arribar un altre que utilitzes aquest compte no podria accedir-hi.



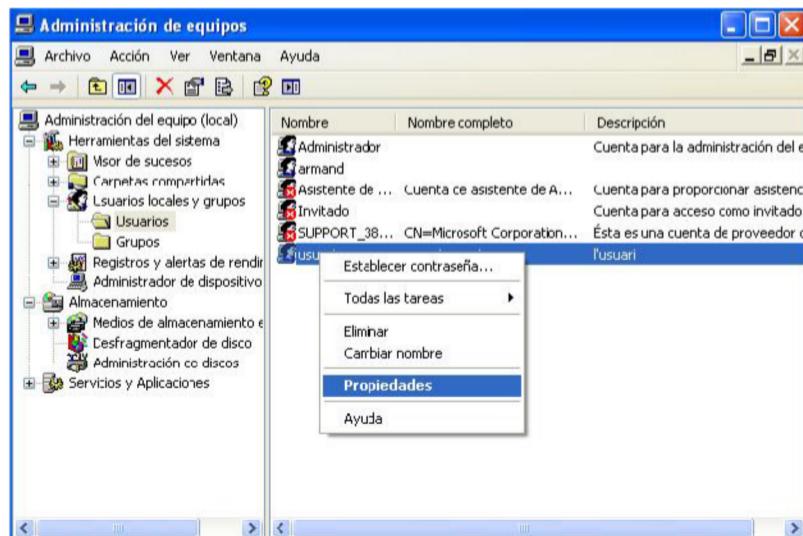
- El compte mai caduca: Si no vols que la paraula de pas expiri.
- Compte deshabilitada: Per deshabilitar un compte i evitar que un usuari la utilitzi. Això pot ser útil en determinats casos, per exemple, quan un usuari se'n va de vacances. Si un compte està deshabilitat apareix una creu sobre la seva icona.

Quan hagis omplert els quadres i activat o desactivat les caselles corresponents podrem «Crear» l'usuari , això no tanca el quadre, i per tant podem seguir creant usuaris fins que fem «Tancar».

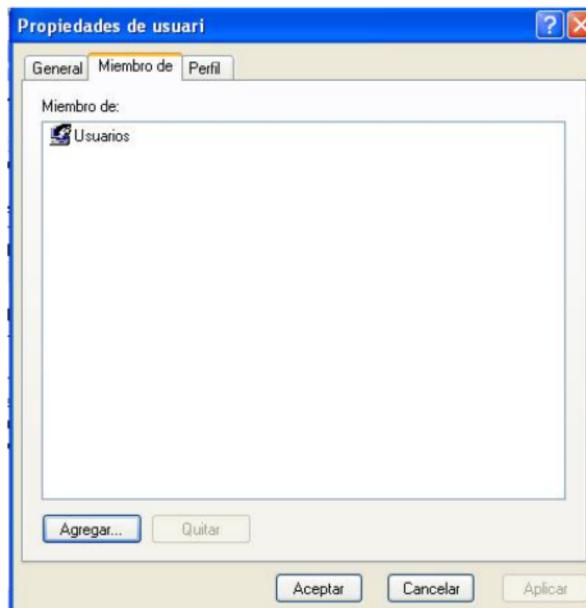
Un nom d'usuari no pot coincidir amb el nom d'un altre usuari o grup. Pot contenir fins a 20 caràcters, en majúscules o minúscules, excepte els següents: " / [] : ; ! = , + * ? < >

Un nom d'usuari no pot contenir només punts (.) o espais en blanc. A «Contrasenya» i «Confirmació de contrasenya», pots escriure una paraula de pas que contingui fins a 127 caràcters. Si s'utilitza Windows 2000/XP en una xarxa que també conté equips amb Windows 95 o Windows 98, s'ha de considerar l'ús de paraules de pas amb menys de 14 caràcters. Windows 95 i Windows 98 admeten paraules de pas de fins a 14 caràcters. Si la paraula de pas és més llarga, és possible que no es puguin iniciar sessions en la xarxa des d'aquest equip.

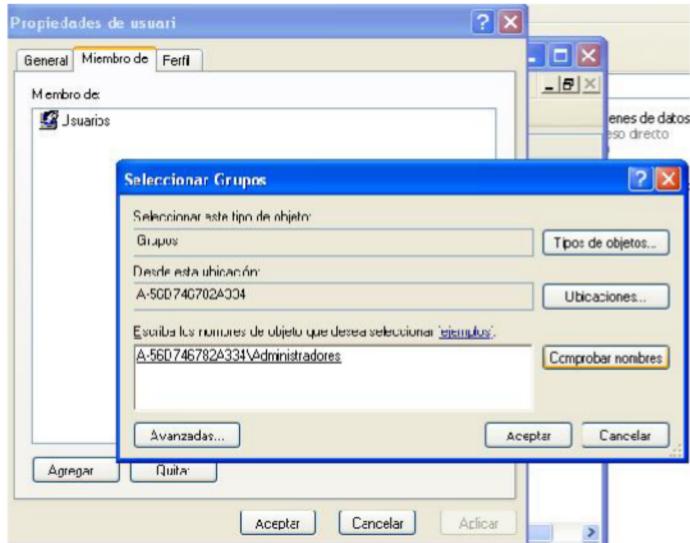
Afegeir un usuari a un grup d'usuaris.



El següent pas és afegir aquest usuari acabat de crear a un grup. Per defecte, Windows XP/7 ens introduceix l'usuari al grup «Usuaris». Si vols modificar el grup al qual pertany accedeix des de l'«Administrador d'equips» a la llista d'usuaris a «Usuaris i grups» i a continuació amb el botó dret selecciona, al menú contextual que apareix l'opció «Propietats».



A la finestra que apareix, activa la pestanya «Membre de». Veuràs que per defecte ja surt el grup «Usuaris». Pitja sobre «Afegir...» i a la finestra emergent fes doble *click* sobre el grup que desitgis. Apareixerà al quadre de sota. Pitjar «Acceptar» per finalitzar.



2. Usuaris i grups predeterminats.

2.1 Usuaris i grups predeterminats a sistemes Linux

A totes les distribucions del GNU/Linux modernes, sempre hem de crear com a mínim un usuari durant el procés d'instal·lació. En la majoria de les distribucions, aquest usuari no té drets d'administració, és a dir: és un usuari que pot utilitzar el sistema, però que no el pot administrar. En aquest sentit podem dir que aquest és el perfil d'usuari predeterminat.



A més de l'usuari predeterminat, en el procés d'instal·lació haurem d'assignar la contrasenya d'administrador. El nom de l'usuari administrador en les diferents variants de l'UNIX i distribucions del GNU/Linux és `root`. A la distribució Ubuntu es crea un usuari que, mitjançant la seva contrasenya, pot accedir a les tasques d'administració. Podem accedir a una consola com a usuari primari si escrivim: `sudo su`

2.2 Usuaris i grups predeterminats a sistemes Windows

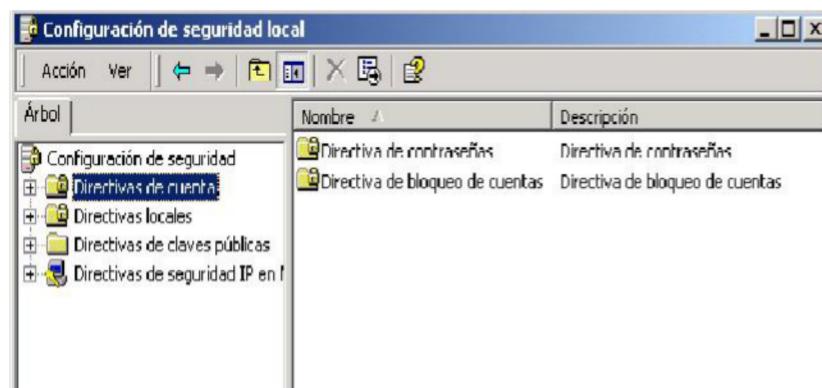
aasdfasfasfdasfas

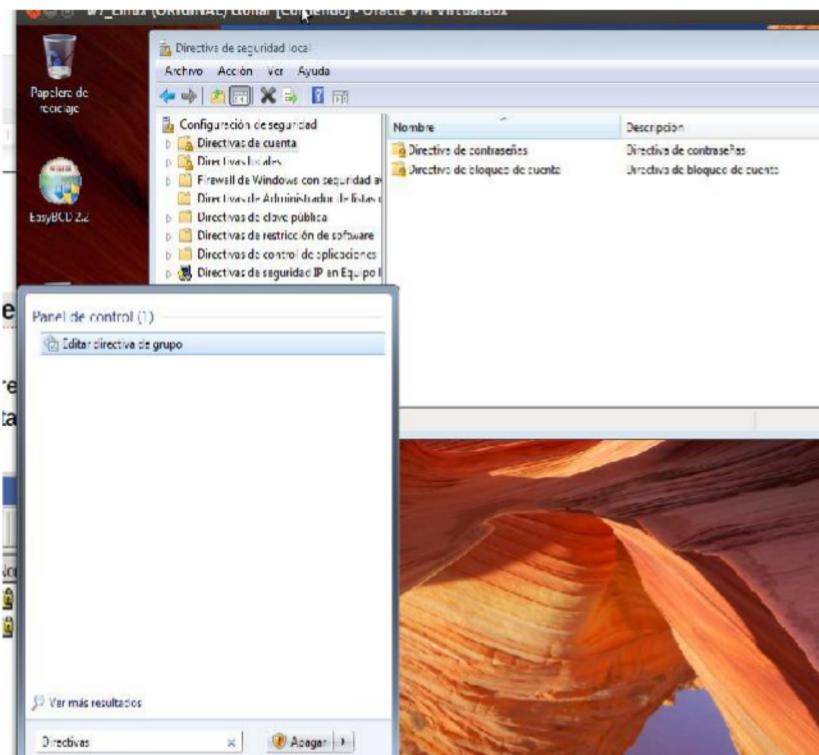
3. Seguretat de comptes d'usuari.

3.1 Seguretat de comptes d'usuari a Windows

Directives de seguretat local. Directives de compte

A «Eines administratives» → «Directives de seguretat local». A la finestra «Configuració de seguretat local» → «Directives de comptes». A «Windows 7 podem buscar-ho, tal com es veu a la imatge.





Les directives de compte ens permeten configurar alguns paràmetres de seguretat relatius als comptes d'usuari, en concret les paraules de pas i el bloqueig de comptes en casos especials.

Directives de bloqueig de comptes

Directiva	Configuración local	Configuración vigente
Duración del bloqueo de cuenta	No está definido	No está definido
Restablecer la cuenta de bloqueos después de	No está definido	No está definido
Umbral de bloqueos de la cuenta	0 intentos de inicio ...	0 intentos de inicio ...

Directiva	Configuración de seguri...
Duración del bloqueo de cuenta	No aplicable
Restablecer el bloqueo de cuenta después de	No aplicable
Umbral de bloqueo de cuenta	0 intentos de inicio de s...

- Llindar de bloqueig de comptes:** Indica el nombre de inicis de sessió fallits necessaris per a bloquejar el compte. De 1 a 999. el valor 0 implica que mai es bloquejarà un compte.
- Duració del bloqueig de compte:** Un cop es bloqueja un compte, aquesta directiva marca el temps que aquest es mantindrà bloquejat. Sobrepassat aquest temps, el compte tornarà a ser operatiu.
- Restablir el compte de bloqueig després de:** Indica el número de minuts que han de transcorrer per a que es reiniciar el comptador d'inicis de sessió erronis. Recorda que si configurem el «Llindar de bloqueig de comptes» a un determinat nombre de fallades, el compte es bloquejarà. Si per exemple, configurem aquesta directiva a 1 minut, quan hagi passat aquest temps, el comptador es posarà a zero.



Aquesta directiva només té sentit si es configura la directiva del llindar d'intents. I ha de ser menor o igual a la durada del bloqueig de compte.

Aquest és el missatge que es dona a l'usuari quan el seu compte ha estat bloquejat:



3.2 Seguretat de comptes d'usuari a Linux

Canvi del comportament de la contrasenya d'un usuari

Hi ha una comanda que ens permet modificar el comportament de la contrasenya d'un usuari. Aquesta comanda és: `chage [opcions] login`. Alguns dels paràmetres que permet aquesta comanda són:

- **-d dies**: Compte el nombre de dies (des de 01-01-1970) transcorreguts des que va canviar la contrasenya per última vegada. També es pot especificar en el format AAAA-MM-DD.
- **-E data**: Modifica la data en què el compte de l'usuari expirarà i serà bloquejada.
- **-I dies**: Modifica quants dies pot romandre un compte amb una contrasenya expirada abans de ser bloquejada.
- **-M dies**: Modifica el nombre màxim de dies durant els quals és vàlida la contrasenya d'usuari. Passats els dies, l'usuari haurà de modificar.
- **-m dies**: Modifica el nombre mínim de dies entre canvi de contrasenya.
- **-l**: Ens mostra la informació de la compta d'usuari en relació al comportament de les seves contrasenyes.

4. Seguretat de contrasenyes.

4.1 Seguretat de contrasenya a Windows

Hem d'accendir a l'apartat de «Directives de Contrasenya» a «Eines administratives» → «Directives de seguretat local».

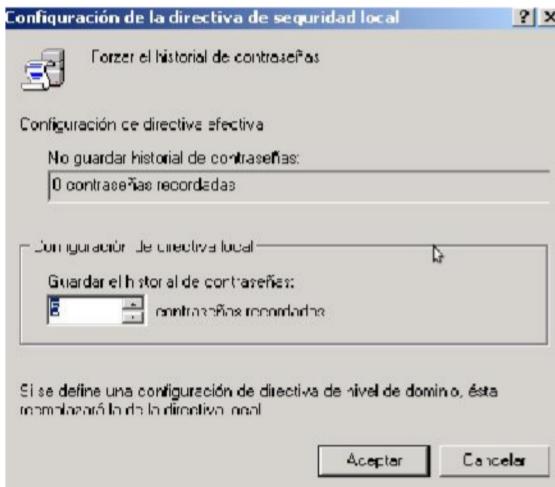
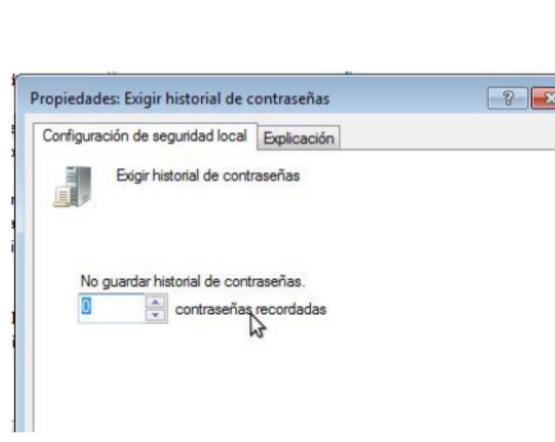


Directiva	Configuración local	Configuración vigente
Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio	Deshabilitada	Deshabilitada
Forzar el historial de contraseñas	0 contraseñas recordadas	0 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Deshabilitada	Deshabilitada
Longitud mínima de la contraseña	0 caracteres	0 caracteres
Vigencia máxima de la contraseña	42 días	42 días
Vigencia mínima de la contraseña	0 días	0 días

A Windows 7, és pràcticament igual:

Directiva	Configuración de seguri...
Almacenar contraseñas con cifrado reversible	Deshabilitada
Exigir historial de contraseñas	0 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Deshabilitada
Longitud mínima de la contraseña	0 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	0 días

- Forçar l'història de contrasenyes:** Aquesta directiva obliga a l'usuari, que en el moment d'haver de canviar una paraula de pas (perquè hagi caducat, per exemple), aquesta no pugui repetir una d'anterior (tant anterior com inqui el nombre de paraules que es recordin a l'historial). Si per exemple, configurem 3 paraules de pas recordades, no podrem introduir una paraula que hagi estat introduïda en les tres ocasions anteriors.

 <p>Configuración de la directiva de seguridad local</p> <p>Forzar el historial de contraseñas</p> <p>Configuración de directiva efectiva</p> <p>No guardar historial de contraseñas: 0 contraseñas recordadas</p> <p>Configuración de directiva local</p> <p>Guardar el historial de contraseñas: 0 contraseñas recordadas</p> <p>Si se define una configuración de directiva de nivel de dominio, ésta sobrescribirá la definición local.</p> <p>Aceptar Cancelar</p>	 <p>Propiedades: Exigir historial de contraseñas</p> <p>Configuración de seguridad local Explicación</p> <p>Exigir historial de contraseñas</p> <p>No guardar historial de contraseñas: 0 contraseñas recordadas</p>	<p>Windows 7</p>
--	--	------------------

Windows XP

- Les contrasenyes han de complir els requeriments de complexitat:** Obliga a que les paraules de pas tinguin un cert grau de complexitat, que per defecte és:
 - La paraula de pas no pot contenir la totalitat o part del nom d'usuari.
 - Al menys ha de tenir sis caràcters de longitud.



- La paraula de pas ha de contenir com a mínim tres dels següents grups de caràcters: (A...Z), (a...z), (0...9) i caràcters no alfanumèrics (per exemple, !,\$#,%)
- Longitud mínima de la contrasenya: De 0 a 14 caràcters. Indicant 0, que és el valor per defecte, permetem que un usuari no tingui paraula de pas. Gens recomanable.
- Vigència màxima i vigència mínima de la contrasenya: La *vigència mínima* establirà el temps que haurà d'esperar un usuari per canviar la seva paraula de pas. El mínim es 0 (es pot canviar immediatament) i el màxim són 999 dies. De totes formes ha de ser sempre menor que la *vigència màxima* que indicarà el temps màxim que pot durar una paraula de pas abans que el sistema requereixi el seu canvi. Posat a zero indica que la paraula mai caducarà. Qualsevol altre valor és possible dins del marge 1...999.
- Emmagatzemar la contrasenya fent servir xifrat reversible per a tots els usuaris del domini: Aquesta directiva, si s'activa, permetria que aplicacions externes poguessin obtenir les paraules de pas dels usuaris per a necessitats pròpies, aplicant un xifrat reversible. Mai activeu aquesta opció a no ser que no hi hagi més remei.

4.2 Seguretat de contrasenyes a Linux

A Linux serà necessari instal·lar una llibreria que ens permeti controlar la complexitat de les contrasenyes. La llibreria s'anomena *libpam-cracklib*.

Una vegada instal·lada la llibreria la configuració de la complexitat de la contrasenya la realitzarem a l'arxiu de text */etc/pam.d/common-password*. Allà podem controlar els següents comportaments:

- Determinar un nombre de diferències entre la nova contrasenya i la vella: afegirem el paràmetre **difok=N** a on N és el nombre de diferències entre la contrasenya nova i la vella per tal d'acceptar-ne la nova.

```
password requisite pam_cracklib.so retry=3 difok=3 minlen=10
```

- Número del llindar de contrasenyes: afegirem el paràmetre **remembre=N** a on N és el nombre de contrasenyes recordades i que no es poden repetir (el sistema les emmagatzema a */etc/security/opasswd*).

```
password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5
```

- Determinar el número mínim de caràcters d'una contrasenya: afegirem el paràmetre **minlen=N** a on N és el nombre mínim de caràcters que volem per a les contrasenyes.

```
password requisite pam_cracklib.so retry=3 difok=3 minlen=10
```

- Determinar la complexitat de la contrasenya: afegirem els paràmetres següents
 - **ucredit=-N:** A on N indica el nombre mínim de majúscules que s'han de fer servir a la contrasenya.
 - **lcredit=-N:** A on N indica el nombre mínim de minúscules que s'han de fer servir a la contrasenya.



- **dcredit=-N:** A on N indica el nombre mínim de díigits que s'han de fer servir a la contrasenya.
- **ocredit=-N:** A on N indica el nombre mínim de símbols que s'han de fer servir a la contrasenya.

```
password requisite pam_cracklib.so retry=3 difok=3 minlen=10 ucredit=-1
lcredit=-2 dccredit=-1 ocredit=-1
```

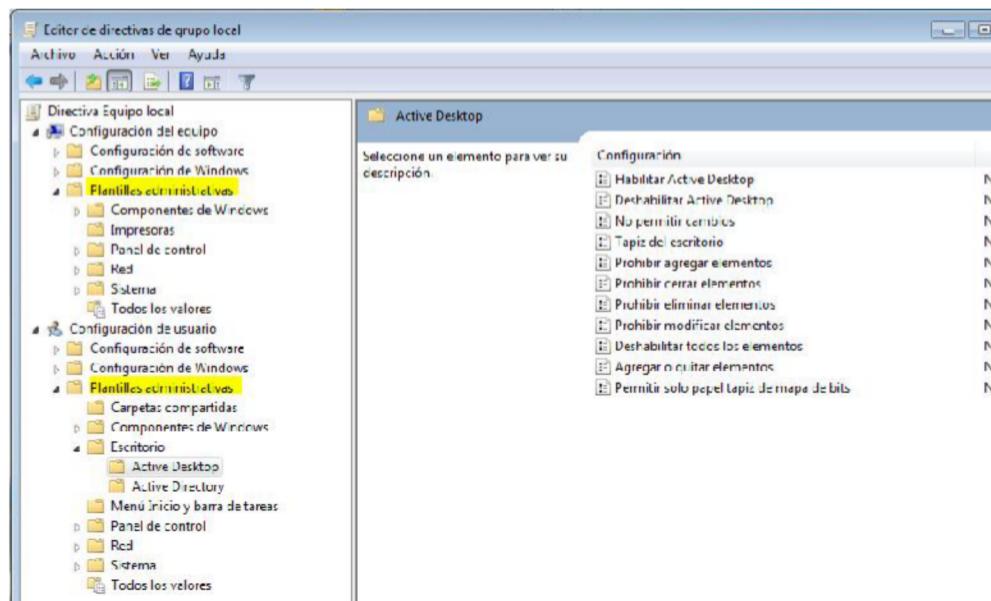
5. Administració de perfils locals d'usuari.

5.1 Administració de perfils locals d'usuari a Linux

Fet pràcticament.

5.2 Administració de perfils locals d'usuari a Windows

A Windows podem definir plantilles que s'aplicaran a tots els usuaris del nostre equip. L'eina bàsica de configuració és l'editor de directives de grup.



Te dues grans branques: Configuració d'equip i configuració d'usuari. Cadascuna permet configurar diverses opcions relacionades amb l'equip o amb els usuaris de l'equip. Aquestes configuracions es poden exportar i importar a o des d'un altre equip.

Per posar un exemple, obrim «Plantilles administratives» de la «Configuració d'usuari» → Escriptorio → *Active Desktop* → Fons d'escriptori. L'activem i introduïm una imatge amb la seva ruta. Quan reiniciem la sessió o entrem a qualsevol usuari (actual o futur), es mostrarà el nou fons d'escriptori.

Hi ha moltes més opcions, la majoria relacionades amb amagar o mostrar elements del propi Windows. A la carptea «Sistema» tenim una opció per iniciar programes de forma automàtica en iniciar sessió.