

M01 Sistemes Informàtics

CFGS Desenvolupament d'Aplicacions Multiplataforma

UF1. Instal·lació, configuració i explotació del sistema informàtic.

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

NF2.1

Configuració i explotació de sistemes informàtics

Administració d'usuaris i grups en Linux

Administració Linux

Linux és un sistema operatiu multiusuari perquè una de les seves característiques principals és la capacitat de gestionar diferents usuaris en un mateix sistema.

Té també la capacitat de donar suport a diferents usuaris que treballin de manera simultània al mateix equip, localment o a través de la xarxa.

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. De fet, un usuari no pot ni llegir ni modificar els arxius propis d'altres usuaris

Administració Linux

En les versions modernes de Linux ja creem per defecte un usuari durant la instal·lació. Aquest usuari no té drets d'administració, és un usuari que pot utilitzar el sistema però no administrar-lo (és un perfil d'usuari predeterminat).

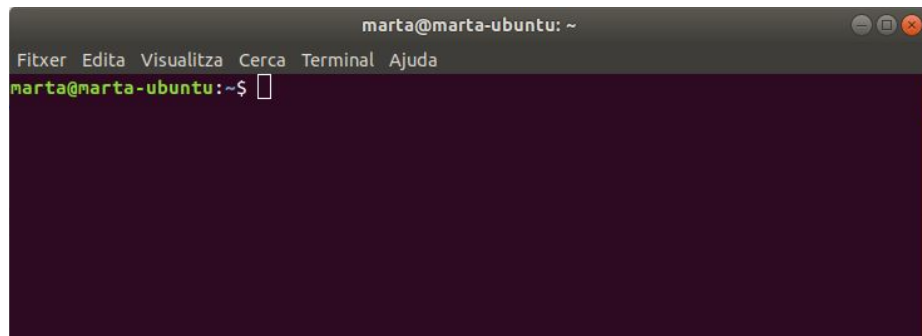
En el procés d'instal·lació també haurem d'assignar la contrasenya d'administrador (root).

L'usuari una vegada instal·lat el sistema podrà realitzar operacions a nivell d'usuari, però si necessita fer accions d'una complexitat superior requerirà l'administrador del sistema. Per a fer-ho necessitarem deixar el ratolí i obrir la **Terminal o Consola**.

La Terminal

Característiques principals:

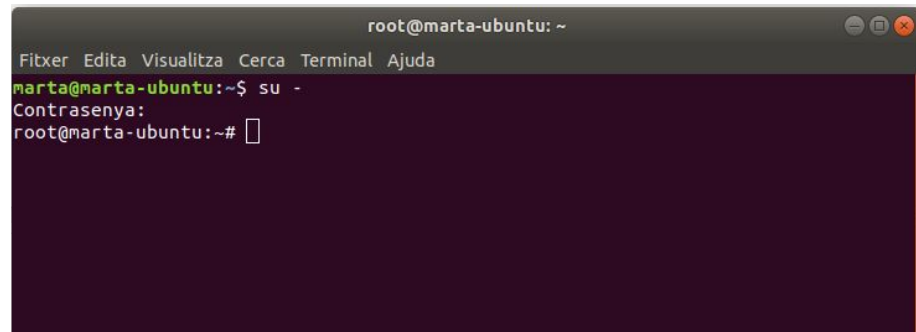
- Accés des del menú d'aplicacions → Utilitats o Alt + Cntrl + T
- Ens dóna control del sistema
- Té un **indicador d'ordres** (command prompt) que serveix per indicar-nos quan el sistema està preparat per rebre una nova ordre. L'indicador mostra el nom d'entrada de l'usuari i el directori de treball actual. El directori personal de l'usuari es representa mitjançant el caràcter `~`.
- El format serà: [usuari@host dir]
on **usuari** serà el nom d'accés,
host el nom de la màquina i
i **dir** serà una indicació de la nostra ubicació actual en el sistema d'arxius.



La Terminal

Característiques principals:

- Si l'indicador d'ordres es visualitza en pantalla amb el caràcter \$ seguit del cursor per escriure aleshores vol dir que l'usuari encara no té privilegis d'administració
- En moltes distribucions, per iniciar una sessió com a usuari administrador hem d'escriure la següent ordre: `usuari@localhost ~ $ su`
- Ens demanaran la contrasenya
- Moltes de les tasques d'administració en sistemes Linux requereixen la modificació de fitxers de configuració.
- Normalment aquests arxius es troben dins del directori `/etc`.

A screenshot of a terminal window titled 'root@marta-ubuntu: ~'. The window has a menu bar with 'Fitxer', 'Edita', 'Visualitza', 'Cerca', 'Terminal', and 'Ajuda'. The terminal shows the prompt 'marta@marta-ubuntu:~\$' followed by the command 'su -'. Below this, it says 'Contrasenya:' and then 'root@marta-ubuntu:~#', indicating a successful switch to the root user. A cursor is visible at the end of the root prompt.

```
root@marta-ubuntu: ~
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
marta@marta-ubuntu:~$ su -
Contrasenya:
root@marta-ubuntu:~#
```

bash vs dash

En els entorns Linux, l'interpret d'ordres més utilitzat actualment és bash (bourne again shell), tot i que s'està començant a estendre la utilització de l'interpret dash.

Tipus d'ordres

Diccionari d'ordres

Ordres bàsiques

ls	Mostra una llista d'arxius en el directori de treball actual
cd directori	Canvia al directori especificat
passwd	Canvia la contrasenya de l'usuari actual
file nomarxiu	Mostra el tipus d'arxiu de l'arxiu nomarxiu
pwd	Mostra el directori de treball actual
exit o logout	Tanca la sessió actual
info ordre	Mostra les pàgines d'informació referents a l'ordre
man ordre	Mostra les pàgines del manual referents a l'ordre

Opcions de les comandes

Les opcions indiquen a una ordre que tingui un comportament diferent de l'habitual. Afegir una opció a una ordre és escriure-hi al darrera una lletra normalment precedida per un guió (-)

Per exemple: `ls -a`. L'opció `-a` indica a `ls` que mostri tots els arxius, fins i tot els ocults.

Les ordres també permeten que s'indiqui sobre quins paràmetres s'ha d'actuar. Un exemple seria `ls /etc` que mostraria tots els arxius de la carpeta `/etc`.

Algunes ordres requereixen paràmetres obligatòriament, i per a altres els paràmetres són opcionals.

Quan un paràmetre és opcional, s'acostuma a escriure entre claudàtors en la descripció de la sintaxi de l'ordre (els claudàtors no s'han d'introduir en la línia de comandes).

Opcions de les comandes

ls --help	Mostra l'ajuda breu de l'ordre ls
man ls	Mostra el manual de l'ordre ls

Comprovant l'ajuda en línia d'una ordre, podem saber si l'ordre accepta opcions i paràmetres i quins d'aquests són vàlids.

Usuaris a Linux

Els usuaris a Unix/linux s'identifiquen per un número únic d'usuari **User ID o UID**.

Cada usuari forma part d'un grup principal d'usuari, identificat també per un número únic de grup **Group ID o GID**.

Tot i això, l'usuari pot formar part d'altres grups apart del principal.

Usuaris a Linux. Usuari root

Usuari root:

- També es pot dir superusuari o administrador
- El seu UID (User ID) és 0
- És el compte d'usuari amb privilegis sobre tot el sistema
- Té accés total a tots els arxius i directoris amb independència de propietari i permisos
- Controla l'administració de comptes d'usuari
- Pot executar tasques de manteniment del sistema
- Pot instal·lar software al sistema
- Pot modificar o reconfigurar el Kernel, controladors, etc.

Usuaris a Linux. Usuaris del sistema

Usuaris del sistema:

- Exemples: bin, daemon, adm, lp, sync, shutdown, mail, operator, squid, apache, etc.
- No tenen tots els privilegis de l'usuari root però depenent del compte assumeixen privilegis del root.
- No tenen contrasenyes ja que són comptes que no estan definits per iniciar sessions. Per això també se les pot anomenar com a comptes de “no inici de sessió” (nologin)
- Es creen, generalment, automàticament en el moment de la instal·lació de Linux o de l'aplicació.
- Generalment s'assignen UID entre l'1 i el 100 (definits a /etc/login.defs)

Usuaris a Linux. Usuaris individuals

Usuaris individuals:

- Cada usuari disposa d'un directori de treball, ubicat generalment a /home.
- Cada usuari pot personalitzar el seu entorn de treball.
- Tenen només privilegis complerts en el seu directori de treball.
- Per seguretat, sempre és millor treballar com un usuari individual en comptes de root. Quan es requereixi fer ús de comandes específiques del root podrem utilitzar la comanda *su*.
- Generalment s'assignen UID superiors a 500.

Arxiu. /etc/passwd

Tots els comptes d'usuari es troben definits a l'arxiu de configuració '**passwd**' dins del directori /etc. Aquest arxiu és de text (tipus ASCII), es crea en el moment de la instal·lació amb l'usuari root, els usuaris del sistema i els comptes que s'hagin indicat en el moment de la instal·lació.

L'arxiu /etc/passwd conté una línia per a cada usuari similar a les següents:

```
root:x:0:0:root:/root:/bin/bash
```

```
minion:x:501:500:Minion Banana:/home/minion:/bin/bash
```

Els camps estan separats per **dos punts (:)**

Analitzem cada camp →

Camp 1	És el nom de l'usuari, l'identificador d'inici de sessió. Ha de ser únic.
Camp 2	La 'x' indica la contrasenya encriptada de l'usuari, també indica que s'està utilitzant l'arxiu /etc/shadow. Si no es fa ús d'aquest arxiu veuríem quelcom semblant a això: 'uXCc12r5gt78uuu6R'.
Camp 3	Número identificador de l'usuari (UID). Ha de ser únic. 0 per al root 1 al 100 comptes de sistema usuaris individuals a partir del 101 o en les distribucions més recents a partir del 500.
Camp 4	Identificador del grup (GID). És el grup principal de l'usuari però pot aparèixer en altres, això ho configurarem al /etc/groups.
Camp 5	Comentaris o el nom complet de l'usuari.
Camp 6	Directorio de treball (Home) on es situa l'usuari després de l'inici de sessió.
Camp 7	Shell que utilitzarà l'usuari de manera predeterminada.

Arxiu. /etc/shadow

Anteriorment (en sistemes Unix) les contrasenyes xifrades s'emmagatzemaven en l'arxiu /etc/passwd. El problema és que 'passwd' és un arxiu que pot ser llegit per a qualsevol usuari del sistema encara que només pugui ser modificat pel root.

Així doncs, amb qualsevol equip potent, avui en dia, i amb un bon programa per desxifrar contrasenyes es podrien "crackejar" contrasenyes dèbils. En aquest sentit és important donar una data de caducitat a les contrasenyes i regenerar-les sovint.

L'arxiu 'shadow' soluciona aquest problema ja que només hi pot accedir l'usuari root. Es pot entendre com una extensió del 'passwd' ja que no només emmagatzema una contrasenya encipada sinó que té altres camps de control sobre la contrasenya.

*Hi ha dos algorismes d'enciptació de les contrasenyes: MD5 i DES. MD5 és un mètode fort d'enciptació.

Arxius. /etc/shadow

L'arxiu '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.

*Evitar contrasenyes molt òbvies com ara dates de naixement, 123456, qwerty però evitar també 123k\$%!asdfMDasd123 ja que són impossibles de recordar.

Alguns consells:

- Incloure signes de puntuació
- Barrejar majúscules i minúscules
- Llargada mínima de 8 caràcters
- Substituir caràcters per altres d'aspectes semblants. Ex: \$ per S
- No donar mai la contrasenya a ningú ni deixar-la anotada
- No enviar-la per correu electrònic
- Canviar la contrasenya sovint.

Arxius. /etc/shadow

L'arxiu /etc/shadow conté una línia per a cada usuari, similar a les següents:

```
root:ghy675gjuXCc12r5gt78uuu  
6R:10568:0:99999:7:7:-1::
```

```
minion:rfgf886DG778sDFFDRR  
u78asd:10568:0:-1:9:-1:-1::
```

Els camps estan separats per **dos punts (:)**

Analitzem cada camp →

Camp 1	Nom del compte de l'usuari
Camp 2	Contrasenya xifrada o encriptada. Un '*' indica que és un compte que no té login 'nologin'
Camp 3	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.
Camp 4	Número de dies mínim que han de passar perquè la contrasenya es pugui tornar a canviar
Camp 5	Número de dies màxim que han de passar per canviar la contrasenya. El '-1' significa que no s'ha de canviar. A partir d'aquesta dada es pot obtenir la data d'expiració de la contrasenya.
Camp 6	Número de dies abans de l'expiració de la contrasenya en que s'avisarà a l'usuari a l'inici de la sessió
Camp 7	Número de dies després de l'expiració en que la contrasenya s'inhabilitarà si no s'ha canviat.
Camp 8	Data de caducitat del compte. S'expressa en dies transcorreguts des de l'1 de gener del 1970 (epoch)
Camp 9	Reservat

Arxius. /etc/group

Aquest arxiu guarda la relació dels grups als que formen part els usuaris del sistema. Conté una línia per a cada usuari amb tres o quatre camps per usuari:

```
root:x:0:root
ana:x:501:
minion:x:502:ventas,supervisores,produccion
```

Actualment en crear un usuari amb `useradd` es crea també automàticament el seu grup principal de treball GID amb el mateix nom que el d'usuari. És a dir si s'afegeix l'usuari 'minion' també es crearà el grup 'minion'.

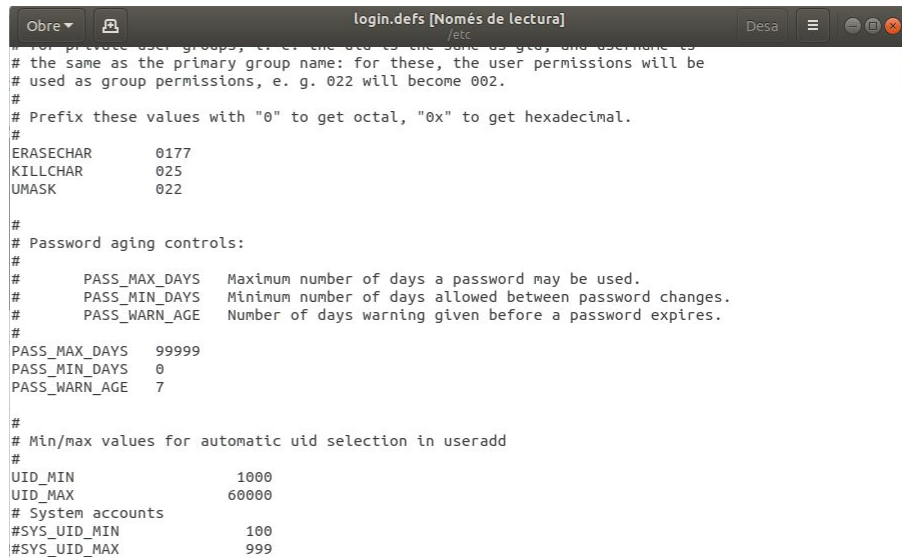
Hi ha un fitxer anomenat '`/etc/gshadow`' que conté informació encriptada sobre els grups d'usuari

Camp 1	Indica l'usuari
Camp 2	La 'x' indica la contrasenya del grup, que no existeix, si n'hi hagués, mostraria un 'hash' encriptat
Camp 3	És el Group ID (GID) o identificador del grup.
Camp 4	És opcional i indica la llista de grups secundaris als que forma part l'usuari

Arxius. /etc/login.defs

A l'arxiu de configuració /etc/login.defs estan definides les variables que controlen els aspectes de la creació d'usuaris i dels camps de shadow utilitzades per defecte. Algunes variables interessants d'estudiar són:

- PASS_MAX_DAYS: número màxim de dies de validesa d'una contrasenya
- PASS_MIN_LEN: número mínim de caràcters en una contrasenya
- UID_MIN: valor mínim per al UID pels usuaris individuals quan s'afegeix un nou usuari
- CREATE_HOME: directori per defecte que se li assigna a un usuari



```
login.defs [Només de lectura]
# For private user groups, let the user be the same as the primary group, and use the user
# the same as the primary group name: for these, the user permissions will be
# used as group permissions, e. g. 022 will become 002.
#
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
#
ERASECHAR      0177
KILLCHAR       025
UMASK          022

#
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS  99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN        1000
UID_MAX        60000
# System accounts
#SYS_UID_MIN    100
#SYS_UID_MAX    999
```

Afegir un usuari

Per tal d'afegir un usuari utilitzarem les comandes **useradd** o **adduser**. Les opcions més comuns i importants són les que trobareu en la següent taula →

-c	Afegeix un comentari al moment de crear l'usuari (camp 5 'passwd')
-d	Director de treball o home de l'usuari (camp 6 'passwd')
-e	Data d'expiració del compte. Format AAAA-MM-DD (camp 8 'shadow')
-g	Número de grup principal de l'usuari (GID) (camp 4 'passwd')
-G	Altres grups als que pot formar part l'usuari (separat per comes)
-r	Crea un compte del sistema, el seu UID serà menor al definit en etc/login.defs en la variable UID_MIN, no es crearà el directori d'inici.
-s	Shell per defecte de l'usuari quan entra al sistema. Si no s'especifica serà bash
-u	UID de l'usuari, si no s'indica aquesta opció automàticament s'establirà el següent número disponible a partir de l'últim creat.

Afegir un usuari

Si fem `useradd + “nom d’usuari”` `#> useradd minion`

Es crearà l’usuari i un grup, així com les entrades corresponents als arxius `/etc/passwd`, `/etc/shadow` i `/etc/group`. També es crearà el directori d’inici o de treball: `/home/minion` i els arxius de configuració que van dins d’aquest directori.

Les dates d’expiració de contrasenya, per defecte, queden molt àmplies així que en principi no hi ha problema amb que el compte caduqui. Per tant ens quedarà afegir la contrasenya de l’usuari i algun comentari o identificador del compte.

`#> useradd -d /usr/juan -s /bin/csh -u 800 -c "Juan Perez Hernandez" juan`

Amb aquesta comanda estem canviant el directori d’inici, el shell per defecte i l’UID.

Modificar un usuari

Per tal de modificar o actualitzar un usuari ja existent farem ús de la comanda **usermod**. Les opcions més comuns són →

-c	Modifica el comentari de l'usuari (camp 5 'passwd')
-d	Modifica el directori de treball o home de l'usuari (camp 6 'passwd')
-e	Modifica la data d'expiració del compte. Format AAAA-MM-DD (camp 8 'shadow')
-g	Canvia el número de grup principal de l'usuari (GID) (camp 4 'passwd')
-G	Modificar altres grups als que pot formar part l'usuari (separat per comes)
-l	Canvia el login o el nom de l'usuari (camp 1 de 'passwd' o 'shadow')
-L	Bloqueja el compte d'usuari, no esborra res només el deshabilita
-s	Canvia el shell per defecte de l'usuari quan entra al sistema.
-u	Canvia el UID de l'usuari
-U	Desbloqueja un compte previament bloquejat amb l'opció -L

Modificar un usuari

Si volem canviar el nom de l'usuari de minion a minion.banana farem:

```
#> usermod -l minion.banana minion
```

En la majoria dels casos el nom del directori d'inici es canviarà de manera automàtica, si no fos així hauríem de fer:

```
#> usermod -d /home/minion.banana minion.banana
```

Altres canvis o modificacions que podem fer són:

```
#> usermod -c "supervisor de area" -s /bin/ksh -g 505 minion.banana
```

D'aquesta manera modifiquem el comentari del compte, el shell i el grup principal de l'usuari.

Si volem deshabilitar un usuari perquè ningú faci servir el seu compte farem:

```
#> usermod -L minion.banana
```

Eliminar un usuari

Si volem eliminar un usuari haurem de fer ús de la comanda **userdel** per eliminar tot el compte de l'usuari. Podem fer-ho de tres maneres diferents:

```
#> userdel minion.banana
```

Si no posem cap opció més eliminarem el compte d'usuari de 'passwd' i de 'shadow' però no eliminarem el seu directori de treball, d'aquesta manera s'eliminarà el compte però no la informació.

```
#> userdel -r minion.banana
```

Amb aquesta opció eliminarem el directori de treball amb els arxius que hi hagi dins. El compte no es podrà eliminar si l'usuari està loguejat al sistema en el moment d'executar la comanda.

```
#> userdel -f sergio
```

L'opció -f és igual que l'opció -r, elimina tot l'usuari, compte, directori i arxius però sense tenir en compte si l'usuari està actualment treballant al sistema. És una opció “més radical” i podria causar inestabilitat al sistema així que es fa servir en casos molt aïllats.

Modificar la contrasenya

Mitjançant la comanda `passwd` caldrà fer els següents passos:

```
#> passwd minion.banana
```

Changing password for user prueba.

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

```
#>
```

L'usuari root és l'únic que pot realitzar aquesta tasca a qualsevol usuari. Els usuaris individuals poden canviar la seva contrasenya en qualsevol moment escrivint `passwd` (sense el seu nom d'usuari al darrera).

El sistema guardarà la contrasenya encriptada, en cap cas l'original.

L'administrador del sistema haurà de seguir una política de gestió de les contrasenyes, és a dir, establir les contrasenyes permeses i prohibides, la freqüència de canvi, la recuperació de contrasenyes...

Modificar la contrasenya

La comanda `passwd` té integrada la validació de contrasenyes comuns, curtes, de diccionari... així que si per exemple si intentem canviar la contrasenya i posar 'qwerty' el sistema ens mostrarà el següent error:

```
$> passwd
Changing password for user prueba.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
$>
```

En escriure 'qwerty' el sistema detecta que és una seqüència coneguda i ens mostra el missatge de "BAD PASSWORD: it is based on a dictionary word", tot i això, ens deixa continuar si la verifiquem. És a dir, el sistema ens avisa que la contrasenya és dèbil però permet establir-la si realment es desitja.

Afegir un grup

Per tal d'afegir un nou grup farem ús de la comanda **groupadd**
#groupadd nomgrup

Podrem modificar paràmetres de configuració amb l'ordre **groupmod** o eliminar-los mitjançant **groupdel**.
El resultat el trobarem a `/etc/group`.

Un usuari pot pertànyer a més d'un grup. Això és especialment útil per gestionar l'accés d'usuaris de diferents grups a un mateix recurs.

També es pot canviar el grup al qual forma part un usuari després d'haver-lo creat. Per defecte es crea un nou grup d'usuaris per a cada usuari que afegim al sistema.

L'ordre **usermod** permet canviar el grup primari d'un usuari després d'haver-lo creat.

Monotoritzar usuaris

La monitorització de l'activitat de l'usuari és una tasca fonamental de l'administrador del sistema per comprovar com es fan servir els recursos del sistema.

Les ordres principals de monitorització de l'activitat dels usuaris són:

- `w`: dóna informació sobre quins usuaris estan autenticats en el sistema, des de quin moment han iniciat la sessió i què estan fent. Cap usuari es pot amagar del superusuari. Podem utilitzar, com a paràmetre de l'ordre `w`, el nom d'un usuari concret per mostrar només què està fent aquell usuari.
- `ac` podem veure el temps total de connexió d'un usuari al sistema. Si no està instal·lada per defecte, la podem instal·lar amb l'ordre `#apt-get install acct`. Aquesta ordre accedeix al fitxer `/var/log/wtmp` per obtenir la informació.
- `last`: cerca en el fitxer `/var/log/wtmp` i fa una llista de tots els usuaris que han iniciat i aturat la sessió des de la seva creació
- `lastb`: mostra tots els intents fallits d'autenticació o d'inici de sessió al sistema. És útil per determinar si un usuari legítim té problemes per accedir al sistema o si estan intentant hackejar comptes.

Resum de comandes

Existeixen altres comandes que s'utilitzen poc en l'administració d'usuaris però que permeten personalitzar més detalladament els usuaris.

adduser	Afegir usuari
chage	Permet canviar o establir paràmetres de les dates de control de la contrasenya
id	Mostra el UID i els grups als que forma part
gpasswd	Administra la contrasenya de grups (/etc/group i /etc/shadow)
groupadd	Afegeix grups al sistema (/etc/group)
groupdel	Elimina grups del sistema

Resum de comandes

groupmod	Modifica grups del sistema
groups	Mostra els grups als que forma part un usuari
pwconv	Estableix la protecció shadow (/etc/shadow) a l'arxiu /etc/passwd
pwunconv	Elimina la protecció shadow (/etc/shadow) a l'arxiu /etc/passwd
useradd	Afegeix un usuari al sistema
userdel	Elimina usuaris del sistema
usermod	Modifica usuaris

Resum d'arxius

Arxius d'administració i control d'usuaris:

/etc/group	Usuaris i els seus grups
/etc/gshadow	Contrasenyes encriptades dels grups
/etc/passwd	Usuaris del sistema
/etc/shadow	Contrasenyes encriptades i control de dates d'usuari del sistema