LPI 107.1. Gestió d'usuaris i comptes de grup i els fitxers de sistema relacionats

Wikis:

http://acacha.org/mediawiki/index.php/LPI_107.1

Autor: Sergi Tur Badenas

Objectius

107.1. Gestió d'usuaris i comptes de grup i els fitxers de sistema relacionats	
	▪ **Objectiu**: Els candidats han de se capaços d'afegir, eliminar, suspendre o modificar comptes d'usuari. ▪ **Pes**: 5
	**Àrees Clau de Coneixement**: ▪ Afegir, modificar i eliminar usuaris i grups. ▪ Gestionar la informació d'usuaris i grups a les bases de dades password i group. ▪ Crear i gestionar comptes limitades de propòsit específic.
	La següent és una llista parcial de fitxers, termes i utilitats utilitzades: ▪ /etc/passwd ▪ /etc/shadow ▪ /etc/group ▪ /etc/skel ▪ chage ▪ groupadd ▪ groupdel ▪ groupmod ▪ passwd ▪ useradd ▪ userdel ▪ usermod
	**Apunts**: LPI 107.1. Gestió d'usuaris i comptes de grup i els fitxers de sistema relacionats

Autor: Sergi Tur Badenas

Linux. Sistema operatiu multiusuari

- **Sistema Operatiu GNU/Linux**
  - Característica rellevant: sistema multiusuari.
  - Cal disposar d'algun sistema que permeti distingir a cada usuari de la resta.
    - A cada usuaris se li assigna un identificador únic dins del sistema conegut com el **UID (User Identifier)**.
  - El UID no és suficient per establir uns requeriments mínims de seguretat i funcionalitat dins del sistema.
    - Cada usuari, a més de pel seu identificador propi, s'ha de caracteritzar per altres atributs fonamentals com ara la contrasenya d'accés al sistema, un directori propi, etc...

Autor: Sergi Tur Badenas

Comptes d'usuari

- **Compte d'usuari**
  - Estructura de dades administrativa que permet reunir totes les dades associades a un mateix usuari
  - El compte d'usuari engloba al conjunt d'atributs (fonamentals o no) que el caracteritzen i, per extensió, també a tots els fitxers i directoris associats a l'usuari.
  - Cal una base de dades per emmagatzemar els usuaris (pot ser un simple fitxer de text)

Autor: Sergi Tur Badenas

Comptes d'usuari

Camps d'un compte d'usuari

- **Nom de l'usuari (login)**: nom amb el qual l'usuari serà conegut dins del sistema. No poden existir dos noms iguals. S'assigna explícitament per l'administrador en el moment de la creació del compte.No es xifren ni s'oculten, qualsevol usuari del sistema pot conèixer, en principi, els noms de la resta d'usuaris.
- **Paraula de pas (password)**: és aconsellable que cada usuari introdueixi durant el login, a més del seu nom, una contrasenya per verificar la seva identitat. La contrasenya d'un usuari només hauria de ser coneguda per l'usuari, per això les contrasenyes sempre s'oculten per pantalla i es xifren en els fitxers on apareixen. Els usuaris haurien de canviar la contrasenya cada certs temps en busca d'una major seguretat en l'accés al sistema. L'administrador pot obligar als usuaris a canviar la contrasenya cada cert temps imposant una data límit per al canvi.

Autor: Sergi Tur Badenas

Comptes d'usuari

- **Directori d'entrada (directori home)**: directori on es situarà a l'usuari cada vegada que entri al sistema. Quan l'administrador crea el compte d'un nou usuari, pot indicar explícitament quin serà el seu directori d'entrada.
- **Identificador numèric (UID)**: és un identificador com el login però el UID serà sempre un número. Per norma general és un identificador únic. El propi sistema s'encarrega d'assignar automàticament el UID en el moment de la creació del compte d'usuari, encara que l'administrador pot establir-ho. Per conveni, es sol reservar un cert rang de valors (del 0 al 499 per als comptes del sistema, del 500 cap amunt per als usuaris externs al sistema o usuari normals)

Autor: Sergi Tur Badenas

Comptes d'usuari

- **Intèrpret d'ordres (shell)**: indica quin intèrpret d'ordresd'entre els disponibles s'activarà quan l'usuari entri al sistema. Si l'administrador no indica un shell per a l'usuari el propi sistema li assignarà el shell que estigui configurat per defecte del sistema (normalment bash o sh). Per indicar un shell és necessari indicar el camí absolut d'on està ubicat
- **Nom real de l'usuari**: es tracta del nom real de l'usuari, no és imprescindible però pot servir per recordar qui és la persona real propietària d'un compte d'usuari.
- **Grup d'entrada (GID)**: és el grup prioritari del compte d'usuari. La prioritat d'aquest grup s'utilitza per a la política de drets.

Autor: Sergi Tur Badenas

Comptes d'usuari

- **Grups addicionals**: són tots aquells grups dels quals pot ser membre l'usuari, excepte el seu grup d'entrada. Qualsevol dels grups addicionals d'un usuari pot passar a ser el seu grup prioritari en qualsevol moment. No és imprescindible que un usuari sigui membre de grups addicionals, per defecte, aquesta llista estarà buida.
- **Caducitat del compte**: es contempla la possibilitat d'imposar una data de caducitat dels comptes d'usuari. Això evitarà que existeixin en el sistema comptes "abandonades" o oblidades pels seus propietaris consumint recursos inútilment. La data de caducitat es pot indicar de forma absoluta o relativa

Autor: Sergi Tur Badenas

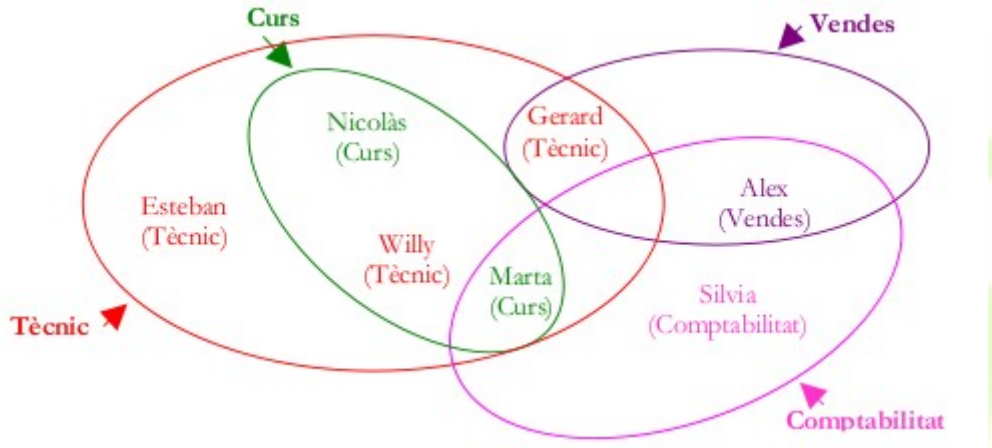
Comptes de grup

Comptes de grup

- A més de poder afegir i eliminar usuaris, l'administrador del sistema té la capacitat de definir i desfer grups d'usuaris. Els grups d'usuaris són agrupacions merament administratives: la existència d'un grup no suposa una relació directa entre els comptes dels usuaris inclosos en el grup.
- Aquestes agrupacions resulten útils a l'hora de facilitar o restringir fàcilment certs permisos a usuaris de similar categoria o necessitats operatives.
- De forma semblant als usuaris, els grups també es caracteritzen per un identificador únic (GID) i per una sèrie d'atributs

Autor: Sergi Tur Badenas

Exemple d'usuaris i grups



- On Esteban, Gerard i Willy són del Servei Tècnic. Willy col·labora amb els formadors i Gerard col·labora amb el servei de Vendes. Nicolàs i Marta són formadors però també col·laboren amb el Servei Tècnic. Marta, a més, col·labora amb el servei de comptabilitat. Àlex és un comercial que a més col·labora amb el servei de comptabilitat. Silvia només pertany al servei de comptabilitat.

Autor: Sergi Tur Badenas

Jerarquia dels usuaris

- **3 tipus de comptes d'usuari**
  - Es poden distingir tres tipus de comptes en UNIX:
    - **root**: és el "superusuari" que s'encarrega de les tasques administratives del sistema. No està afectat pels drets d'accés als arxius i pot fer més o menys de tot al sistema. **El seu UID és 0.**
    - **Usuaris de sistema (bin, daemon, sync, apache...)** : existeixen una sèrie de comptes que no s'assignen a persones físiques. Aquests comptes serveixen per a facilitar l'administració dels drets d'accés de certes aplicacions i dimonis. Aquests comptes solen tenir com a UID un número entre el 1 i el 499. Ordres com useradd o groupadd tenen una opció (-r, --system) que permet crear usuaris o grups de sistema.

Autor: Sergi Tur Badenas

Jerarquia dels usuaris

- **Usuaris**: P. ex. josep, ana ... : la resta de comptes d'usuari s'associen a persones reals; la seva funció és permetre als usuaris estàndards connectar-se i utilitzar els recursos de l'equip. El UID d'un usuari és normalment un número superior a 999.

- **3 tipus de grup**
  - **root**: El seu GID és 0. Grup principal de l'administrador.
  - **Grups de sistema**: P. ex. bin, daemon, sync, apache... Tenen la mateixa funció que els comptes del mateix nom i permeten donar els mateixos drets d'accés a una sèrie d'aplicacions.
  - **Grups d'usuaris**: Aquests grups representen a una sèrie de persones reals que han d'accedir als mateixos arxius. Típicament tenen un GID superior o igual a 500 o 1000.

Autor: Sergi Tur Badenas

Jerarquia dels usuaris

- **Sistema configurable**

```
$ cat /etc/login.defs | grep ID
UID_MIN 1000
UID_MAX 60000
#SYS_UID_MIN               100
#SYS_UID_MAX               999
GID_MIN                   1000
GID_MAX                  60000
#SYS_GID_MIN               100
#SYS_GID_MAX               999
```


Autor: Sergi Tur Badenas

Noms d'usuari

- **GNU/Linux és força flexible amb els noms d'usuari.**
  - L'ordre useradd no estableix gairebé cap restricció als noms d'usuari Linux, es poden utilitzar els següents caràcters (estàndard IEEE Std 1003.1-2001):
    - **Lletres** (minúscules i minúscules): tot i així no es recomana (i algunes aplicacions no deixen) utilitzar majúscules.
    - Números
    - Guions baixos (underscores o _)
    - Punts (periods): De totes maneres no es recomana l'ús.
    - Arrobes (@),
    - Dol·lar ($) al final del nom: Per compatibilitat amb els noms de màquina de Samba.

Autor: Sergi Tur Badenas

Noms d'usuari

- **Recomanacions i restriccions en aplicacions de gestió d'usuaris d'alt nivell**
  - Distribucions com Debian (ordre adduser) proposen noms d'usuari amb les següents característiques:
    - Mida màxima de 256 caràcters: es pot configurar segons els paràmetre LOGIN_NAME_MAX i LOGNAME_MAX (**getconf**)
    - El primer caràcter ha de ser una lletra
    - El fitxer de configuració de l'ordre adduser (**/etc/adduser.conf)** amb NAME_REGEX permet establir restriccions addicionals
    - El dol·lar ($) al final del nom d'usuari es suportat per compatibilitat amb Samba (Samba Machine Accounts).
    - Els noms d'usuaris normals han de ser minúscules. Als noms d'usuari de sistema se'ls permet utilitzar majúscules.

Autor: Sergi Tur Badenas

Paraules de pas. Shadow suite

- **On s'amaguen les paraules de pas**
  - Abans el fitxer /etc/passwd contenia la paraula de pas xifrada (s'utilitzava el xifratge crypt). Actualment aquest fitxer conté:

```
$ cat /etc/passwd | grep sergi
sergi:x:1000:1000:Sergi Tur Badenas,sd,,:/home/sergi:/bin/bash
```

  - Les paraules de pas es guarden xifrades a **/etc/shadow**
  - El sistema de paraules de pas ocultes és el sistema per defecte utilitzat a totes les distribucions Linux modernes. De fet s'està aplicant des de principis dels 90 que va ser quan es va implementar.

Autor: Sergi Tur Badenas

Paraules de pas. Shadow suite

- Al conjunt d'eines que permeten convertir fitxer de passwords tradicionals de Unix al format shadow més als programes de gestió d'usuaris i grups i login se'ls anomena shadow suite o shadow-utils (utilitats shadow).
- L'ordre pwconv converteix un fitxer de format tradicional a shadow (també hi ha la inversa pwunconv).
- Vegeu els exemples de la wiki del curs
- Dos paquets:
  - **login**
  - **passwd**

```
$ dpkg -L login| grep bin
/usr/sbin/nologin
/usr/bin/faillog
/usr/bin/lastlog
/usr/bin/newgrp
/bin/login
/bin/su
/usr/bin/sg
```

```
$ dpkg -L passwd|grep bin
/usr/bin/chage
/usr/bin/chfn
```


Autor: Sergi Tur Badenas

Esquemes d'autenticació

- **Authentication Schemes**
  - Un esquema d'autenticació defineix la forma en que un usuari determinara la seva identitat.
  - Quan paguem amb targeta de crèdit utilitzem un esquema d'autenticació basat en DNI.
  - El més comú en informàtica és la contrasenya, però hi ha altres (clau pública, Smartcards...)
  - L'esquema d'autenticació bàsic de Linux és la contrasenya
- **Terminologia**
  - **Servei**: aplicació que utilitza un esquema d'autenticació

Autor: Sergi Tur Badenas

Name Service Switch

Name Service Switch (NSS)

- Permet reemplaçar fitxers basics de configuració de Unix (per exemple: **/etc/passwd**, **/etc/group**, **/etc/hosts**) per bases de dades centralitzades
- Aquest sistema és configurable mitjançant el fitxer:

```
$ cat /etc/nsswitch.conf
passwd:         compat
group:          compat
shadow:         compat
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
netgroup:       nis
```

- Creat per Sun Microsystems per a Solaris però ha estat "portat" a altres sistemes operatius

Autor: Sergi Tur Badenas

Name Service Switch (NSS)

- **Modulable**
  - Mitjançant paquets es poden suportat diferents bases de dades:

```
$ sudo apt-cache --names-only search libnss
libnss-db - NSS module for using Berkeley Databases as a naming
service
libnss-ldap - NSS module for using LDAP as a naming service
libnss-mdns - NSS module for Multicast DNS name resolution
libnss-lwres - NSS module for using bind9's lwres as a naming service
libnss-mysql - NSS module for MySQL
libnss-mysql-bg - NSS module for using MySQL as a naming service
libnss-pgsql1 - name service switch module using PostgreSQL
```

  - La idea és que el sistema sigui configurable sense haver de tocar codi font (en C s'utilitzen llibreries amb accessos genèrics a bases de dades. Per exemple la funció **gethostbyname()**)

Autor: Sergi Tur Badenas

Name Service Switch (NSS)

- **Bases de dades**
  - **aliases:** Mail aliases
  - **ethers:** números Ethernet numbers,
  - **group:** grups d'usuaris
  - **hosts:** noms de màquina i números
  - **netgroup:** usuaris i màquines de xarxa
  - **networks:** noms i números de xarxes
  - **protocols:** noms i números de protocols
  - **passwd:** paraules de pas dels usuaris.
  - **rpc:** noms i números de crides remotes a procediments
  - **services:** Network services, see Services Database.
  - **shadow:** paraules de pas shadow del usuaris

Autor: Sergi Tur Badenas

Name Service Switch (NSS)

- **Serveis de base de dades**
  - **files**: Fitxers guardats a la carpeta /etc del sistema
  - **compat**: Fitxers guardats a la carpeta /etc del sistema (només password, groups i shadow) compatibles amb l'estil de signes + i -
  - **dns**: Utilitzat per indicar que els hosts utilitzant DNS
  - **hesiod**: hesiod

```
$ ls  /lib/libnss*
/lib/libnss_compat-2.6.1.so
/lib/libnss_files-2.6.1.so
/lib/libnss_mdns4_minimal.so.2
/lib/libnss_mdns_minimal.so.2
/lib/libnss_nisplus.so.2
...
```


Autor: Sergi Tur Badenas

Name Service Switch (NSS)

Accions

- Es poden especificar accions:

```
networks:   nisplus [NOTFOUND=return] files
```

- Les accions s'interpreten de la següent forma:
  - **success**: Sense errors i s'ha trobat el que es buscava a la base de dades. L'acció per defecte és **return**.
  - **notfound**: Sense errors però no s'ha trobat el que es buscava. L'acció per defecte és **continue**.
  - **unavail**: El serveis no esta disponible. L'acció per defecte és **continue**.
  - **tryagain**: El servei no esta disponible temporalment. L'acció per defecte és continue.

Autor: Sergi Tur Badenas

Name Service Switch (NSS)

- **Exemple**

```
networks:   nisplus [NOTFOUND=return] files
```

  - és equivalent a:

```
ethers: nisplus [SUCCESS=return NOTFOUND=return UNAVAIL=continue TRYAGAIN=continue]
```

  - NSS a la wiki del curs
- **NSSwitch per ldap**
  - Instal·lació

```
$ sudo apt-get install libnss-ldap
```


Autor: Sergi Tur Badenas

Autenticació Linux

- **Usuari i contrasenya emmagatzemats en fitxers locals:**
  - **/etc/passwd**: Conté la informació de les comptes d'usuari (llegible per tots els usuaris).
  - **/etc/shadow**: Conté les contrasenyes. Només llegible per root i el grup shadow.
  - **/etc/group**: Conté els grups i els usuaris que hi pertanyen.

```
pete:x:1000:1000:Peter Hernberg,,,1-800-
FOOBAR:/home/pete:/bin/bash
```

```
pete:/3GJllg1o4152:11009:0:99999:7:::
```

```
pasta:x:103:spagetti,fettucini,linguine,vermicelli
```

- **Autenticació Linux a la wiki**

Autor: Sergi Tur Badenas

/etc/passwd

- **Conté la base de dades local d'usuaris.**
  - Fixeu-vos que parlem de base de dades local, és a dir que també hi ha la possibilitat d'utilitzar bases de dades d'usuaris remote, p. ex. LDAP, NIS, etc...

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
....
dansguardian:x:118:127:DansGuardian
User,,,:/var/log/dansguardian:/bin/sh
postfix:x:119:128::/var/spool/postfix:/bin/false
openldap:x:120:130:OpenLDAP Server
Account,,,:/nonexistent:/bin/false
smbguest:x:1004:1006:Samba guest account:/dev/null:/dev/null
pepe:x:1005:1008::/home/pepe:/bin/bash
ntp:x:121:131::/home/ntp:/bin/false
4prova:x:1006:1009::/home/4prova:/bin/sh
```


Autor: Sergi Tur Badenas

/etc/passwd

- Curiosament i contràriament a que indica el seu nom, aquest fitxer ja no sol contindre les paraules de pas. Consulteu shadow suite

- **Camps separats per dos punts**
  - **El login (nom d'usuari)**: és el nom utilitzat per connectar-se al sistema. Ha de ser únic.
  - **Contrasenya**: no es troba en aquest arxiu per raons de seguretat; el caràcter x la reemplaça i indica una referència a l'arxiu /etc/shadow que no és accessible en lectura als usuaris normals. Si no s'indica res és que no hi ha paraula de pas (no recomanat). En sistemes antics es trobava la paraula de pas xifrada amb crypt (actualment s'utilitzen sistemes de xifratge més potents com MD5 o SHA512, vegeu John The Ripper)

Autor: Sergi Tur Badenas

/etc/passwd

- **UID**: identificador del compte d'usuari, normalment és únic.
- **GID**: identificador del grup principal del compte.
- **Nom complert**: anomenat també GECOS nom provinent del sistema operatiu General Electric Comprehensive Operating System, aquest camp lliure i opcional indica, generalment, la identitat real de la persona associada al compte de linux.
- **Directori personal (home directory)**: és el directori de base de l'usuari on es troba en connectar-se.
- **Interpret d'ordres per defecte**: és el programa que es llança a la connexió. El shell predeterminat en GNU/Linux és el bash.
- El manual està a la secció 5 (si no poseu el 5 us mostrarà el manual de l'ordre passwd):
  - **$ man 5 passwd**

Autor: Sergi Tur Badenas

Linux-PAM

- **PAM (Pluggable Authentication Modules) és un mecanisme flexible per l'autenticació d'usuaris**
  - Permet utilitzar sistemes d'autenticació diferents al sistema tradicional d'autenticació (fitxer /etc/passwords) sense necessitat de canviar les aplicacions
  - PAM permet desenvolupar programes amb independència de l'esquema d'autenticació
  - S'utilitzen mòduls d'autenticació en temps d'execució. No cal tornar a compilar per canviar l'esquema d'autenticació
  - PAM és un invent de **SUN** (especificació amb diferents implementacions)
  - **Linux-PAM** és la implementació de PAM a Linux.

Autor: Sergi Tur Badenas

PAM. Configuració

- **Fitxers de la carpeta /etc/pam.d**
  - Alguns sistemes poden tenir la configuració de PAM tota al fitxer /**etc/pam.conf**.
- **Cada fitxer és un servei/aplicació. Exemple:**
  - **/etc/pam.d/login**: configura l'ús de PAM per l'aplicació login.
- **Contenen una llista ordenada de normes amb la següent sintaxi:**

```
type  control  module-path  module-arguments
```


Autor: Sergi Tur Badenas

PAM. Configuració

- **"Types". Separen les normes en diferents àmbits:**
  - **auth**: com determinem que l'usuari és qui diu que és. També s'encarrega de l'assignació de grups.
  - **password**: Proveïx els mecanismes per canviar l'autenticació de l'usuari (contrasenya).
  - **session**: realitza tasques abans i/o després de que l'usuari s'hagi autenticat.
  - **account**: Determina qüestions que no són purament de l'autenticació (la contrasenya ha expirat?, hora i data d'accés correctes?, etc.)

Autor: Sergi Tur Badenas

PAM. Configuració

- **"control". Determina que cal fer un cop l'execució sigui correcta o incorrecta:**
  - **requisite**: Si el modul falla, es denega l'accés a l'usuari immediatament.
  - **required**: denega l'autenticació però es continua l'execució de la resta de mòduls abans de tornar el control a l'aplicació.
  - **sufficient**: El resultat del modul és ignorat si falla. Si és un èxit només serà un èxit de tota la pila si cap mòdul required ha fallat.
  - **optional**: s'ignora el resultat del modul. Només és necessari per tal de que l'autenticació sigui un èxit quan no hi han altres mòduls associats al mateix servei i tipus.

Autor: Sergi Tur Badenas

PAM. Configuració

- **Modules**
  - **module-path:** el nom del modul (allotjat a la carpeta /lib/security) o el camí absolut.
  - **module-arguments:** Arguments per passar al mòdul.
- **Cada fitxer té les normes per un servei (aplicació) "PAM-aware".**
  - Si l'aplicació utilitza PAM es pot canviar la autenticació sense modificar PAM
- **Cada norma executa un mòdul**
  - Es poden combinar les normes per aconseguir autenticacions tan complexes com es desitgi.

Autor: Sergi Tur Badenas

Pila de normes

- **Per a un mateix tipus i servei podem tenir més d'una norma (llista ordenada)**

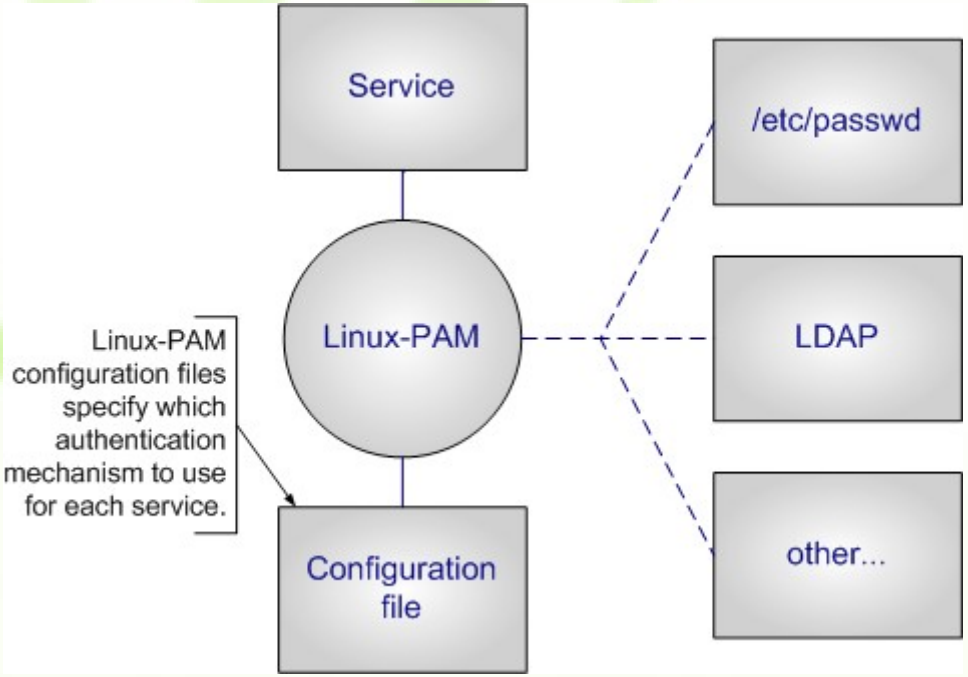
```
 auth        required     pam_nologin.so
 auth        required     pam_securetty.so
 auth        required     pam_env.so
 auth        sufficient
pam_rhosts_auth.so
 auth        required     pam_stack.so
service=system-auth
```

  - Entre mòduls **required** no importa l'ordre.
  - **Requisite** finalitza la llista si no autentica.
  - **Sufficent** no finalitza si hi ha error.
- **L'exemple anterior utilitza mòduls bàsics de Linux**

Autor: Sergi Tur Badenas

PAM. Modules

- **Pam proporciona una sèrie de mòduls bàsics per treballar amb l'autenticació bàsica de Linux**
  - Paquet libpam-modules
  - Es poden afegir mòduls addicionals per treballar amb altres autenticacions



Autor: Sergi Tur Badenas

Gestió d'usuaris i grups

- **L'administrador del sistema disposa de les següents ordres per gestionar els usuaris del sistema:**
  - **useradd**: Permet afegir usuaris a la base de dades d'usuaris (fitxer /etc/passwd i /etc/groups)
  - **usermod**: Permet modificar un usuari que ja existeix a la base de dades.
  - **userdel**: Permet eliminar usuaris
  - **passwd**: permet modificar les paraules de pas
  - **chage**: Permet modificar les dades d'expiració de les paraules de pas dels usuaris.

Autor: Sergi Tur Badenas

Gestió d'usuari i grups

- **També es pot editar directament els fitxers /etc/passwd i /etc/shadow**
  - No és recomanable ja que qualsevol error pot implicar que el sistema deixi de funcionar correctament.
  - En tot cas si s'han d'editar els fitxers directament utilitzeu vipw i vigrp.
  - A vegades cal editar directament els fitxer per què estem accedint al sistema des d'un LIVE-CD o qualsevol altre mitjà de recuperació del sistema.
  - Podeu utilitzar **chroot** per tal de poder utilitzar les ordres useradd i similars

Autor: Sergi Tur Badenas

Gestió d'usuari i grups

- **Gestió de comptes d'usuari personals sense ser administrador**
  - chfn
  - chsh
  - finger, who i whoami
  - passwd
  - expiry
  - gpasswd
  - id i groups
  - Consulteu la wiki del curs

Autor: Sergi Tur Badenas

Canviar el grup

- **Chgrp (change group)**
  - Permet canviar només el grup
    - Sintaxi: `$ chgrp [-R] <grup> <arxiu ...>`
    - -R: aplicar l'ordre de forma recursiva
    - El propietari pot cedir l'arxiu a qualsevol grup al qual pertanyi:
  - El grup per defecte assignat als nous arxius és el grup principal de l'usuari que l'ha creat, a menys que estigui habilitat el permís SGID en el directori on es crea el fitxer.

Autor: Sergi Tur Badenas

id i groups

- **Mostren informació del usuaris i grups**

```
$ groups
sergi adm dialout cdrom plugdev lpadmin admin sambashare
```

```
$ id
uid=506(alex) gid=502(vendes) grupos=502(vendes),503(compta)
$ touch arxiu
$ ls -l arxiu
  -rw-r--r-- 1 alex vendes 0 jun 3 03:58 arxiu
$ chgrp comptabilitat arxiu
  -rw-r--r-- 1 alex compta 0 jun 3 03:58 arxiu
```


Autor: Sergi Tur Badenas

useradd

- **Opcions**
  - **-c**: Una descripció de l'usuari. Camp lliure sense cap mena de funció, més enllà de la funció informativa.
  - **-d**: Indica el camí absolut (PATH) a la HOME de l'usuari
  - **-s**: Indica el camí absolut (PATH) a l'interpret d'ordres per defecte de l'usuari.
  - **-g**: Indica el grup principal de l'usuari
  - **-G**: Indica la resta de grups dels quals es membre l'usuari.
  - **-m**: crea el compte d'usuari i el directori de treball:
  - **-r**: crea un compte del sistema. Tindrà un UID dins del rang reservat als comptes del sistema i no es crearà un directori d'entrada per a aquest compte

Autor: Sergi Tur Badenas

useradd

- **Exemple:**

```
# useradd -m -G
users,admin,administracio,coordinacio,direccio,qualitat -c "Sergi
Tur" sergi
# passwd sergi
Changing password for sergi.
New Password:
Reenter New Password:
Password changed.
```

  - Sinó s'indiquen algunes opcions s'apliquen les opcions per defecte
  - -D: ens permet veure i modificar els paràmetres per defecte de creació d'un compte d'usuari.
  - Si s'indiquen més opcions amb -D, aleshores modifiquem els valors per defecte

Autor: Sergi Tur Badenas

useradd

- **Comprovacions**
  - Per saber si el compte d'usuari s'ha creat de forma correcta es pot mirar el fitxer **/etc/passwd**
  - També es pot utilitzar la comanda **pwck** que controla si el fitxer és correcte.

```
$ sudo pwck
user 'lp': directory '/var/spool/lpd' does not exist
user 'news': directory '/var/spool/news' does not exist
user 'uucp': directory '/var/spool/uucp' does not exist
user 'list': directory '/var/list' does not exist
user 'irc': directory '/var/run/ircd' does not exist
user 'gnats': directory '/var/lib/gnats' does not exist
```


Autor: Sergi Tur Badenas

useradd

- **Opcions per defecte:**
  - Fitxer de configuració:
    - **/etc/default/useradd**

```
$ useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=no
```

```
$ cat /etc/default/useradd | more
# Default values for useradd(8)
#
# The SHELL variable specifies the default login shell on
your
# system.
# Similar to DHSELL in adduser. However, we use "sh" here
because
# useradd is a low level utility and should be as general
# as possible
SHELL=/bin/sh
...
```


Autor: Sergi Tur Badenas

/etc/skel

- **Carpeta HOME per defecte**
  - Utilitzada per ordres com useradd (useradd -m) o adduser
  - Si s'utilitzin altres ordres com adduser (només en sistemes de la família Debian) es crea automàticament la carpeta home també a partir d'skel.
  - Tingueu en compte que es pot configurar useradd per tal d'utilitzar un altre carpeta:

```
# cat /etc/default/useradd | grep skel
# The SKEL variable specifies the directory
containing "skeletal" user
# SKEL=/etc/skel
```

  - NOTA: Cal tenir en compte que qualsevol canvi que feu a la carpeta /etc/skel no s'aplicarà als usuaris ja existents

Autor: Sergi Tur Badenas

Usermod i userdel

- **usermod. Permet modifica un usuari**
  - **Sintaxi**:

```
$ sudo usermod [opcions] LOGIN
```

  - Les opcions són molt similars a les de useradd

```
# Exemple de creació d'usuari a Ubuntu
$ sudo useradd -m usuari
$ sudo usermod -a -G adm,dialout,cdrom,plugdev,lpadmin,admin,sambashare usuari
```

- **userdel**
  - Permet eliminar un usuari

```
$ sudo userdel [opcions] LOGIN
```

    - L'opció -f permet eliminar l'usuari tot i que tingui una sessió d'usuari oberta.

Autor: Sergi Tur Badenas

Gestió de grups

- **L'ordre gpasswd és l'encarregada de gestionar els grups.**
  - La informació dels grups es guarda als fitxers /**etc/group** i /**etc/gshadow**.
- **Els grups Linux poden tenir:**
  - **Administradors**: Poden fer canvis al grup amb l'ordre gpasswd. L'usuari root sempre pot gestionar qualsevol grup. També pode canviar la paraula de pas
  - **Membres**: Usuaris que formen part del grup
  - **Paraula de pas**: la paraula de pas permet accedir al grup a qualsevol usuari sigui o no membre del grup.

Autor: Sergi Tur Badenas

Gestió de grups

- **Afegir un grup**
  - $ sudo groupadd nom_del_grup
  - Només el superusuari pot crear grups.
  - Hi ha grups que es generen automàticament, per exemple al crear un nou usuari se l'afegeix automàticament a un grup anomenat User Private Group (UPG) al qual només pertany aquest usuari
- **Afegir/Eliminar membres a un grup**
  - $ sudo gpasswd -a usuari grup
  - $ sudo gpasswd -d usuari grup

Autor: Sergi Tur Badenas

Gestió de grups

- **Establir els membres d'un grup**
  - $ sudo gpasswd -M sergi,bego casa
- **Assignar paraula de pas**
  - Si el grup té una paraula de pas els membres del grup i poden accedir sense posar-la i la resta d'usuaris l'han de posar.
  - $ sudo gpasswd casa
    - Eliminar: $ sudo gpasswd -r casa
    - Restringir l'accés al grup només als membres
      - $ sudo gpasswd -R casa

Autor: Sergi Tur Badenas

newgrp

- **Permet iniciar un nou interpret d'ordres amb un grup diferent**
  - Útil per crear carpetes o fitxers que siguin propietat d'un grup diferent al nostre grup per defecte.
  - Per tornar al grup per defecte només cal sortir del nou interpret d'ordres.
  - Relacionada amb les ordres de login, login, sudo, su, sg
  - Consulteu la wiki del curs

Autor: Sergi Tur Badenas

Gestió de paraules de pas

- **Ordres:**
  - passwd: gestió de paraules de pas d'usuaris
  - gpasswd: gestió de paraules de pas de grups
- **Fitxers**
  - /etc/passwd i /etc/shadow
- **Bloquejar/activar un compte**
  - $ sudo passwd -l 4prova
  - $ sudo passwd -u usuari

Autor: Sergi Tur Badenas

Expiració de paraules de pas

- **Es pot força la expiració d'una paraula de pas:**
  - $ sudo passwd -e usuari
  - I es poden establir els valors de mínim de dies entre canvi de paraules de pas i màxim de dies de validesa d'una paraula de pas amb l'ordre **chage**.
- **Es pot consultar l'estat de totes les paraules de pas de tots els usuaris amb:**
  - $ sudo passwd -a -S

Autor: Sergi Tur Badenas

Expiració de paraules de pas

```
$ sudo passwd -a -S
...
ntp L 03/14/2010 0 99999 7 -1
4prova L 01/01/1970 0 99999 7 -1
```

- **On hi ha 7 camps:**
  - **Nom usuari**
  - **Estat**: locked password (L), no password (NP), usable password (P).
  - **Data de l'últim canvi de paraula de pas**
  - **Minimum age**: temps mínim en dies que ha de transcórrer entre canvis de paraules de pas.
  - **Maximum age**: màxim número de dies de validesa de la paraula de pas
  - **Warning period**: dies abans de que caduqui la paraula de pas en que es rep un avís que està a punt de caducar.
  - **Inactivity period**: màxim temps en dies que pot estar inactiva la compte.

Autor: Sergi Tur Badenas

chage

- **Change Age**
  - Permet gestionar l'expiració de les paraules de pas. Un usuari pot consultar les dades d'expiració associades a la seva paraula de pas amb:
    - Del nostre usuari **$ chage -l sergi**
    - Tots els usuaris; **$ sudo chage -l**
  - Establir els períodes de vigència de les paraules de pas amb. Les opcions més utilitzades són:
    - **chage –d ul_dia nom_usuari**
      - estableix la data de l'últim canvi de la contrasenya.
    - **chage –m min_dies nom_usuari**
      - número de dies que han de passar per canviar la contrasenya.

Autor: Sergi Tur Badenas

chage

- **chage –M max_dies nom_usuari**
  - número de dies màxim que pot estar amb la mateixa contrasenya sense canviar-la.
- **chage –W warn_dies nom_usuari**
  - indica quants dies abans s'avisarà a l'usuari de que la contrasenya expirarà i que ha de canviar-la.
- **chage –I inac_dies nom_usuari**
  - número de dies que han de passar després de que la contrasenya expiri per a que el compte es deshabiliti de forma automàtica si la contrasenya no ha estat canviada.
- **chage –E exp_dies nom_usuari**
  - número de dies per a que expiri el compte i es deshabiliti de forma automàtica.

Autor: Sergi Tur Badenas

Gestió d'usuaris per lots

- **chpasswd**
  - Permet canviar les paraules de pas de múltiples usuaris de cop, mitjançant un fitxer amb múltiples línies (una per usuari) i cada línia amb el format:
    - **usuari:paraula_de_pas**
  - la paraula de pas ha de ser un text no xifrat (text en clar).
  - Sistema de xifratge del sistema
  - Ubuntu Server 9.10 -> SHA-512
  - Permament: $ sudo chpasswd < paraulesdepas

```
$ sudo useradd pep
$ sudo useradd maria
$ sudo useradd joan
$ sudo joe paraulesdepas
$ chpasswd -S < paraulesdepas
```

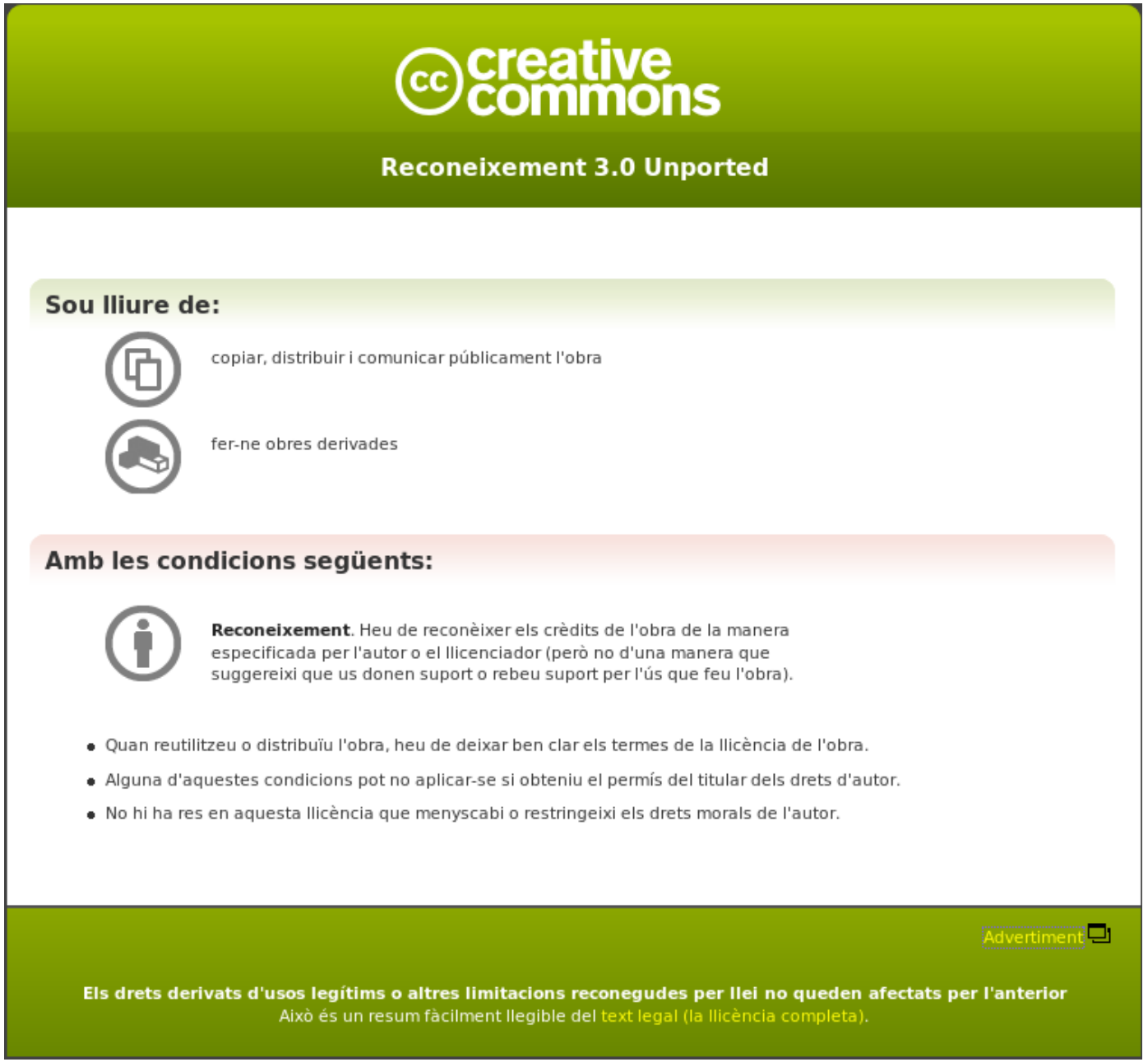

Autor: Sergi Tur Badenas

adduser versus useradd

- **Adduser: assistent disponible a Debian**
  - Dos ordres amb la mateixa funcionalitat però amb diferències importants.
  - De fet podem dir que la majoria de distribucions tenen l'ordre useradd (proporcionada per shadow suite).
  - En canvi només algunes distribucions com Debian utilitzant adduser un **guió de perl** que utilitzant useradd facilita la creació d'usuaris (mitjançant un assistent que va preguntant les dades del nou usuari).
  - A altres distribucions adduser és un enllaç simbòlic a useradd.

Autor: Sergi Tur Badenas

Llicència Creative Commons



http://creativecommons.org/licenses/by/3.0/deed.ca

Autor: Sergi Tur Badenas