LPI 107.1 - Manage user and group accounts and related system files

Curs 2021 - 2022

ASIX M01-ISO 107 Administrative Tasks

Manage user and group accounts and related system files

Description

Key concepts:

- ❏ Add, modify and remove users and groups.
- ❏ Manage user/group info in password/group databases.
- ❏ Create and manage special purpose and limited accounts.

Commands and files:

- ❏ /etc/passwd
- ❏ /etc/shadow
- ❏ /etc/group
- ❏ /etc/skel/
- ❏ chage
- ❏ getent
- ❏ groupadd
- ❏ groupdel
- ❏ groupmod
- ❏ passwd
- ❏ useradd
- ❏ userdel
- ❏ usermod

User and system account files

- /etc/passwd. User accounts
- /etc/shadow. User passwords and password policy

/etc/passwd

/etc/passwd

```
loginID:x:UID:GID:comment:home_directory:login_shell
```

Description /etc/passwd

login

Login name of the user.

passwd

x indicates that the encrypted password has been stored in /etc/shadow file.

UID

User ID assigned by the system (root 0).

GID

Primary Group ID.

GECOS/Comment

Comments, if any, are specified in this field. Note that commas are not delimiters, only colons. (General Electric Comprehensive Operating System).

Home_directory

Absolute path of the default home directory of the user.

Login_shell

Absolute path of the user's login shell.

```
#1
$ head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin

$ ls -l /etc/passwd
-rw-r--r--. 1 root root 3079 Oct 31 14:33 /etc/passwd
```

/etc/shadow

/etc/shadow

```
loginID:password:lastchg:min:max:warn:inactive:expire
```

Description /etc/shadow:

login

Login name of the user.

password

Encrypted password. Note: An empty field indicates no password is required to log in. An asterisk * or exclamation mark ! indicates an inaccessible account (typically system) with no password. A password field that starts with ! followed by the encrypted password, indicates the password is locked.

lastchange

Number of days between January 1, 1970, and the last password change.

min

Minimum number of days that the current password can be changed by the user; a value of 0 means “no minimum password age”.

max
: Maximum number of days remaining for the password to expire; a value of 99999 means “no maximum password age”.

warn
: Number of days prior to password expiry that the user is warned.

inactive
: Number of days after password expiry that the user account remains active.

expire
: Date indicating when the password is deleted and user name will become inactive

Reserved field
: Reserved for future use

```
#2
# head /etc/shadow
root:$6$cDH7FhijkxAZVpkH$qJefPoJTZAiDJhNflgseGOGDQeIjYmMTMjagslqpjFCo31Ncv7PzawZnLC0/iHZ
2X71XkYyH3CDJAIYCdmNqR.::0:99999:7:::
bin:*:17416:0:99999:7:::
daemon:*:17416:0:99999:7:::
adm:*:17416:0:99999:7:::
lp:*:17416:0:99999:7:::
sync:*:17416:0:99999:7:::
shutdown:*:17416:0:99999:7:::
halt:*:17416:0:99999:7:::
mail:*:17416:0:99999:7:::
operator:*:17416:0:99999:7:::

# ls -l /etc/shadow
----------. 1 root root 1726 Oct 31 14:33 /etc/shadow
```

Special accounts

0-100	system accounts root, ftp mail, etc
101-999	system / service accounts
1000-...	user accounts

Some accounts can’t run interactive sessions, only run services.

- /etc/login.defs
- UID_MIN, UID_MAX
- SYS_UID_MIN
- SYS_UID_MAX

```
#3
# grep /sbin/nologin /etc/passwd | head
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
```

```
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

```
#4
$ cat /etc/login.defs
…
# Min/max values for automatic uid selection in useradd(8)
#
UID_MIN                  1000
UID_MAX                 60000
# System accounts
SYS_UID_MIN               201
SYS_UID_MAX               999
# Extra per user uids
SUB_UID_MIN            100000
SUB_UID_MAX         600100000
SUB_UID_COUNT           65536

#
# Min/max values for automatic gid selection in groupadd(8)
#
GID_MIN                  1000
GID_MAX                 60000
# System accounts
SYS_GID_MIN               201
SYS_GID_MAX               999
# Extra per user group ids
SUB_GID_MIN            100000
SUB_GID_MAX         600100000
SUB_GID_COUNT           65536
...
```

Managing user accounts: create / modify / delete

- create the user account
- assign an user's password (activate the account)

- modify an user account

- delete the user account
- delete the user account and the user's home directory

Create accounts

- create the user account
- assign an user's password (activate the account)

- useradd
- useradd [options] user
- useradd -D
- /etc/default/useradd

Usual useradd interactive options:

-n -N No user private group, usually in Red hat. Must be used with -g.
-s user's default login shell (one of /etc/shells).
-u user UID
-g primary group, GID
-G alternate groups, user is member of.
-m create home directory
-M do not create the home directory
-k home directory skeleton. Must be used with -m.
-b home directory basedir (/basedir/username)
-d directory home

```
#6
# useradd pere1

# useradd -n -m -s /bin/bash -u 2001 -g 100 -k /etc/skel -b /home pere2

# useradd -m -G users, wheel -d /home/pojects pere3

# tail -n3 /etc/passwd
pere:x:1007:1007::/home/pere:/bin/bash
pere2:x:2001:100::/home/pere2:/bin/bash
pere3:x:2002:2007::/home/pojects:/bin/bash

# tail -n3 /etc/shadow
pere:!!:18931:0:99999:7:::
pere2:!!:18931:0:99999:7:::
pere3:!!:18931:0:99999:7:::

# tail -n 2 /etc/group
pere:x:1007:
pere3:x:2007:
```

Default useradd values

- /etc/default/useradd
- useradd -D
- useradd -D options

```
#7
# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes

# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

```
#8
# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes

# useradd -D -s /bin/sh  -g wheel

# useradd -D
GROUP=10
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes

# useradd -N  pere4

# tail -1 /etc/passwd
pere4:x:2003:10::/home/pere4:/bin/sh

# useradd -D -s /bin/bash  -g users
```

Home directory temple: /etc/skel

- /etc/skel
- /etc/skel_student…
- useradd -m -k absolute-path-skel-directory user

- Only to the new users.
- File permissions and ownership change to the user.
- Usual files:
  - .bashrc - contains alias definitions, enables shell features, etc.
  - .bash_profile - contains variable definitions and one-time-only commands to set the user's environment.
  - .bash_logout - contains actions to take when logging out.
  - .mozilla (with predetermined bookmarks)

```
#9
 ls -la /etc/skel
drwxr-xr-x.   3 root root  4096 Apr  7  2021 .
drwxr-xr-x. 159 root root 12288 Oct 31 20:49 ..
-rw-r--r--.   1 root root    18 Jun  2  2020 .bash_logout
-rw-r--r--.   1 root root   141 Jun  2  2020 .bash_profile
-rw-r--r--.   1 root root   376 Jun  2  2020 .bashrc
drwxr-xr-x.   4 root root  4096 Jan 29  2020 .mozilla
```

```
#10
# mkdir /etc/skel_students
# cp /etc/skel/.* /etc/skel_students/
cp: -r not specified; omitting directory '/etc/skel/.'
cp: -r not specified; omitting directory '/etc/skel/..'
cp: -r not specified; omitting directory '/etc/skel/.mozilla'

# echo "normes de funcionament " > /etc/skel_students/NORMES.md
# echo "calendari " > /etc/skel_students/Calendari.md
```

```
# ls -la /etc/skel_students/
total 36
drwxr-xr-x.   2 root root  4096 Oct 31 21:02 .
drwxr-xr-x. 159 root root 12288 Oct 31 21:01 ..
-rw-r--r--.   1 root root    18 Oct 31 21:00 .bash_logout
-rw-r--r--.   1 root root   141 Oct 31 21:00 .bash_profile
-rw-r--r--.   1 root root   376 Oct 31 21:00 .bashrc
-rw-r--r--.   1 root root    11 Oct 31 21:02 Calendari.md
-rw-r--r--.   1 root root    24 Oct 31 21:01 NORMES.md

# useradd -m -k /etc/skel_students pere5

# tail -1 /etc/passwd
pere5:x:2004:2008::/home/pere5:/bin/bash

# ls /home/pere5
Calendari.md  NORMES.md

# ls -la /home/pere5
total 28
drwx------.  2 pere5 pere5 4096 Oct 31 21:02 .
drwxr-xr-x. 16 root  root  4096 Oct 31 21:02 ..
-rw-r--r--.  1 pere5 pere5   18 Oct 31 21:00 .bash_logout
-rw-r--r--.  1 pere5 pere5  141 Oct 31 21:00 .bash_profile
-rw-r--r--.  1 pere5 pere5  376 Oct 31 21:00 .bashrc
-rw-r--r--.  1 pere5 pere5   11 Oct 31 21:02 Calendari.md
-rw-r--r--.  1 pere5 pere5   24 Oct 31 21:01 NORMES.md
```

Modify user accounts

- usermod [options] user
- usermod [-u -g -a -G -s -d -L -U -c] user
- usual options:
    - -L lock
    - -U unlock
    - - s shell
    - -g primary group (gid)
    - -G alternate group comma separated list (gids or gnames). Inconditianall.
    - -aG to append the new groups (persisting the old ones)
    - -d new user home directory
    - -c change the comment field GECOS
    - -l change the login name

```
#11
# usermod -g users -aG wheel,bin -s /bin/sh -L pere

# grep "^pere:" /etc/passwd
pere:x:1007:100::/home/pere:/bin/sh

# grep "^pere:" /etc/shadow
pere:!!:18931:0:99999:7:::

# finger pere
Login: pere                             Name:
Directory: /home/pere               Shell: /bin/sh
Never logged in.
No mail.
No Plan.

# id pere
uid=1007(pere) gid=100(users) groups=100(users),1(bin),10(wheel)
```

Delete users accounts

- userdel user
- userdel -r user

The –r option only deletes the user's home directory and mail spool; any other files owned by the user in other directories must be deleted manually. The recommendation is to search for these files owned by the user using the find command before deleting the user account. In addition to the files the user may have processes, print jobs, scheduled jobs and mail in the system, the administrator is responsible to delete all the stuff.

```
#12
# tail -n5 /etc/passwd
pere:x:1007:100::/home/pere:/bin/sh
pere2:x:2001:100::/home/pere2:/bin/bash
pere3:x:2002:2007::/home/pojects:/bin/bash
pere4:x:2003:10::/home/pere4:/bin/sh
pere5:x:2004:2008::/home/pere5:/bin/bash

# userdel -r pere5
# userdel -r pere4
# userdel -r pere3
# userdel -r pere2

# userdel  pere
userdel: group pere not removed because it is not the primary group of user pere.

# ls -a /home/pere/
.  ..  .bash_logout  .bash_profile  .bashrc  .mozilla

# useradd -g users pere
useradd: warning: the home directory /home/pere already exists.
useradd: Not copying any file from skel directory into it.
Creating mailbox file: File exists

# userdel -r pere
userdel: group pere not removed because it is not the primary group of user pere.

# groupdel pere
```

Managing passwords

- Assign passwords
- root → whatever
- user → password rues

- passwd
- passwd [options -l -u -e -S]
- lock / unlock / password-less
- password policy

```
#13
# useradd pere
# passwd pere
```

```
Changing password for user pere.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.

# passwd -S pere
pere PS 2021-10-31 0 99999 7 -1 (Password set, SHA512 crypt.)

# tail -1 /etc/passwd
pere:x:1007:1007::/home/pere:/bin/bash

# tail -1 /etc/shadow
pere:$6$f9GEZgsW7W.vvzoD$SmT5.WygJKKMtPvhWkNNkieMo0PGge6d0PZSjYTlheAMFvmRbMeVRSIzx1E8Amf
GADWsokcWClHy6BNZwfht5/:18931:0:99999:7:::
```

```
#14
# passwd -l pere
Locking password for user pere.
passwd: Success

# passwd -S pere
pere LK 2021-10-31 0 99999 7 -1 (Password locked.)

# tail -1 /etc/shadow
pere:!!$6$f9GEZgsW7W.vvzoD$SmT5.WygJKKMtPvhWkNNkieMo0PGge6d0PZSjYTlheAMFvmRbMeVRSIzx1E8A
mfGADWsokcWClHy6BNZwfht5/:18931:0:99999:7:::

# passwd -u pere
Unlocking password for user pere.
passwd: Success

# passwd -S pere
pere PS 2021-10-31 0 99999 7 -1 (Password set, SHA512 crypt.)

# tail -1 /etc/shadow
pere:$6$f9GEZgsW7W.vvzoD$SmT5.WygJKKMtPvhWkNNkieMo0PGge6d0PZSjYTlheAMFvmRbMeVRSIzx1E8Amf
GADWsokcWClHy6BNZwfht5/:18931:0:99999:7:::

# passwd -d pere
Removing password for user pere.
passwd: Success

# passwd -S pere
pere NP 2021-10-31 0 99999 7 -1 (Empty password.)

# tail -1 /etc/shadow
pere::18931:0:99999:7:::
```

Command passwd -S information:

- Name of the user.
- status (P usable, L locked, NP no password).
- Date when the password was last changed.
- Minimum number of days that must pass before the current password can be changed by the user.
- Maximum number of days remaining for the password to expire.
- Number of days prior to password expiry that the user is warned.
- Number of days after password expiry that the user account remains active.

Password Policy

- password policy
- aging

- /etc/login.defs
- chage

/etc/login.defs

PASS_MAX_DAYS

Maximum number of days a password is valid. A value of 99999 means “no maximum password age”.

PASS_MIN_DAYS

Minimum number of days a password is valid. A value of 0 means “no minimum password age”.

PASS_WARN_AGE

Number of days before password expiry that a warning message is given

/etc/login.defs

```
#15
$ cat /etc/login.defs
…
# 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_MIN_LEN   Minimum acceptable password length.
#       PASS_WARN_AGE  Number of days warning given before a password expires.
#
PASS_MAX_DAYS  99999
PASS_MIN_DAYS  0
PASS_WARN_AGE  7
...
```

The chage command is used to update information related to password expiration. Using this command, the administrator can enforce a password changing and expiry policy for specific user accounts.

- Min days. Min days required to change to password (prevent change)
- Max days. Max days password is vàlid (force change periodically)
- Warning period. Warning message n days before change password date.
- Inactivity period. Set the inactivity period after passwd maxdays.
- Expiry date. Set the expiry date of the account (not password)

- Force the user to change password in the next login.
- Force the user to change password periodically.
- Prevent the user to revert to old passwd (no allow change password immediately).
- Set an expiration date.

```
# 16
# passwd -S pere
pere NP 2021-10-31 0 99999 7 -1 (Empty password.)

# chage -l pere
Last password change                                    : Oct 31, 2021
Password expires                                        : never
Password inactive                                       : never
Account expires                                                : never
Minimum number of days between password change                 : 0
Maximum number of days between password change                 : 99999
Number of days of warning before password expires       : 7
```

```
# chage -W 3 -m 5 -M 90  pere

# chage -l pere
Last password change                                    : Oct 31, 2021
Password expires                                        : Jan 29, 2022
Password inactive                                       : never
Account expires                                                 : never
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 3

# chage -E 2022-01-29 pere

# chage -E $(date -d +180days +%Y-%m-%d) pere

# chage -l pere
Last password change                                    : Oct 31, 2021
Password expires                                        : Jan 29, 2022
Password inactive                                       : never
Account expires                                                 : Apr 29, 2022
Minimum number of days between password change          : 5
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 3
```

Group accounts

- /etc/group
- groupadd, groupmod, groupdel
- groups, getent, id

Every user is associated with at least one group known as their primary group. Recall that the user's primary group is stored in the fourth field of the /etc/passwd file. Any additional group membership will be indicated in the /etc/group file, which is used to store group account information. A user can be a member of multiple groups, but at any point in time, only one group will be the user's primary group.

```
group_name:password:GID:group_list
```

Description of /etc/grup

gname
: Name of the group

password
: This field is blank for most of the groups. An x in this field indicates there might be a group password in the /etc/gshadow file

GID
: The Group ID

user_list
: Comma separated list of the user ids who are members of this group

```
#17
```

```
# head /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:

# head /etc/gshadow
root:::
bin:::
daemon:::
sys:::
adm:::
tty:::
disk:::
lp:::
mem:::
kmem:::
```

```
#18
# id pere
uid=1007(pere) gid=1007(pere) groups=1007(pere)

# groups pere
pere : pere
# getent passwd pere
pere:x:1007:1007::/home/pere:/bin/bash

# getent group pere
pere:x:1007:
```

```
# 19
# groupadd golf

# groupadd -g 2010 students

# groupadd -g 2011 teachers

# tail -n3 /etc/group
golf:x:2007:
students:x:2010:
teachers:x:2011:
```

```
# usermod -g golf -aG users,students pere
# id pere
uid=1007(pere) gid=2007(golf) groups=2007(golf),100(users),2010(students)

# tail -n3 /etc/group
golf:x:2007:
students:x:2010:pere
teachers:x:2011:
```

```
# useradd pere2

# usermod -G students,golf pere2
# id pere2
uid=1008(pere2) gid=1008(pere2) groups=1008(pere2),2007(golf),2010(students)

# tail -n3 /etc/group
students:x:2010:pere,pere2
teachers:x:2011:
pere2:x:1008:
```

```
#20
# groupmod -n mygolf -g 2012 golf

# grep "^mygolf:" /etc/group
mygolf:x:2012:pere2
```

- group must not be primar group for any user to be deleted
- Private groups are automatically deleted when the user is deleted and no other users have the group as a primary group

```
#21
# groupdel teachers
# groupdel students

# groupdel mygolf
groupdel: cannot remove the primary group of user 'pere'

# groupdel pere2
groupdel: cannot remove the primary group of user 'pere2'
```

```
# userdel -r pere2

# groupdel pere2
groupdel: group 'pere2' does not exist
```

```
# userdel -r pere
userdel: group pere not removed because it is not the primary group of user pere.

# groupdel mygolf
# groupdel pere
```

Group Administrators

- /etc/gshadow
- gpasswd [-A]
- newgrp

Descriptio /etc/gshadow

gname
: Valid existing group name.

encrypted password
: Used when a user who is not a member of the group wants to gain permission to this group. An exclamation mark at the beginning of the password indicates it is locked.

administrartors
: Comma-separated list of group administrators.

members
: Comma-separated list of group users that will not be prompted for a password

Other files and commands

- /etc/login.defs
- finger [user]
- chsh
- chfn

/etc/login.defs

The /etc/login.defs file In Linux, the /etc/login.defs file specifies the configuration parameters that control the creation of users and groups. In addition, the commands shown in the previous sections take default values from this file.

UID_MIN and UID_MAX
: The range of user IDs that can be assigned to new ordinary users.

GID_MIN and GID_MAX
: The range of group IDs that can be assigned to new ordinary groups.

CREATE_HOME
: Specify whether a home directory should be created by default for new users.

USERGROUPS_ENAB
: Specify whether the system should by default create a new group for each new user account with the same name as the user, and whether deleting the user account should also remove the user's primary group if it no longer contains members.

MAIL_DIR
: The mail spool directory.

PASS_MAX_DAYS
: The maximum number of days a password may be used.

PASS_MIN_DAYS
: The minimum number of days allowed between password changes.

PASS_MIN_LEN
: The minimum acceptable password length.

PASS_WARN_AGE
: The number of warning days before a password expires.

```
#22
$ grep -v "#" /etc/login.defs | grep -v "^$"
MAIL_DIR        /var/spool/mail
UMASK           022
HOME_MODE       0700
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
UID_MIN                  1000
UID_MAX                 60000
SYS_UID_MIN               201
SYS_UID_MAX               999
SUB_UID_MIN            100000
SUB_UID_MAX         600100000
SUB_UID_COUNT           65536
GID_MIN                  1000
GID_MAX                 60000
SYS_GID_MIN               201
```

```
SYS_GID_MAX               999
SUB_GID_MIN            100000
SUB_GID_MAX         600100000
SUB_GID_COUNT           65536
ENCRYPT_METHOD SHA512
USERGROUPS_ENAB yes
CREATE_HOME    yes
```

```
#23
# finger root
Login: root                             Name: root
Directory: /root                    Shell: /bin/bash
Last login Sun Oct 31 14:37 (CET) on pts/2
No mail.
No Plan.

# id root
uid=0(root) gid=0(root) groups=0(root)
```

```
# finger pere
Login: pere                             Name:
Directory: /home/pere               Shell: /bin/bash
Never logged in.
No mail.
No Plan.

# chfn pere
Changing finger information for pere.
Name []: pere pou prat
Office []: escola del treball
Office Phone []: 935550055
Home Phone []: 930000000
Finger information changed.

# finger pere
Login: pere                             Name: pere pou prat
Directory: /home/pere               Shell: /bin/bash
Office: escola del treball, 935550055      Home Phone: 930000000
Never logged in.
No mail.
No Plan.
# grep "^pere:" /etc/passwd
pere:x:1011:1011:pere pou prat,escola del
treball,935550055,930000000:/home/pere:/bin/bash
```

```
# finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone   Host
ecanet              *:0              Oct 31 12:46                           (:0)
```

```
# chsh -s /bin/sh pere
Changing shell for pere.
Shell changed.

# finger pere
Login: pere                             Name: pere pou prat
Directory: /home/pere               Shell: /bin/sh
Office: escola del treball, 935550055      Home Phone: 930000000
Never logged in.
No mail.
No Plan.
```

```
#25
# getent passwd  pere
pere:x:1011:1011:pere pou prat,escola del treball,935550055,930000000:/home/pere:/bin/sh

# getent group   pere
pere:x:1011:

# getent group   users
```

```
users:x:100:
# getent passwd  | head
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin

# getent group  | head
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
```

Example Exercises

[users]

1. create user pere using /bin/sh as shell, uid 2020, primary group users, secondary group wheel and bin.
2. create directory /tmp/project. Create user marta using primary group users and home directory /tmp/project.
3. Define as default user options home primary group wheel and /bin/sh as shell. Create user anna.

4. modify user anna assigning /etc/bash shell, primary group users, append secondary groups wheel and bin.
5. create an pue skeleton and create a new user called jan using this skeleton.
6. revert the changes in exercice 3.

7. delete users and home directories created in the previous exercices.

[groups]

8. create group dads
9. create group moms
10. create user pere with primary group dads and secondary groups users and moms.
11. modify group dads, change the name and the gid.
12. delete the group moms
13. delete the group dads. Do whatever is necessary…

[password policies]

14. create user pere without password (password-less)
15. lock the user pere
16. unlock the user pere.

17. user pere should change the password in the next login.
18. user pere account expires in three days.

19. Realitza els exercicis indicats a: 107.1 Manage user and group accounts and related system files
20. Realitza els exercicis del Question-Topics 107.1.