

Version : **2021.01**

Updated : 2021/10/24 19:57

# LCE501 - Managing Users and Groups

## Contents

- **LCE501 - Managing Users and Groups**
  - Contents
  - Presentation
    - /etc/nsswitch.conf
    - The getent Command
    - The /etc/group and /etc/gshadow files
    - The /etc/passwd and /etc/shadow files
  - Commands
    - Groups
      - groupadd
      - groupdel
      - groupmod
      - newgrp
      - gpasswd
    - Users
      - useradd
      - userdel
      - usermod
      - passwd
      - chage
  - Configuration
  - LAB #1 - Managing Users and Groups
  - LAB #2 - su and su -

- sudo

## Presentation

Managing users is easier if a clear group strategy is implemented. Under Red Hat, each user is assigned to a primary group and can also be a member of up to 15 secondary groups.

<note important> **Important** - In order to put into practice the examples in this lesson, you need to become the root user by entering the **su -** command using the password **fenestros**. </note>

The databases used for managing user and groups are configured in the **/etc/nsswitch.conf** file. In our case the passwd, shadow and group directives are set to **files**. This indicates that the following files are used as databases :

- **/etc/passwd**,
- **/etc/shadow**,
- **/etc/group**.

### **/etc/nsswitch.conf**

```
[root@centos8 ~]# cat /etc/nsswitch.conf
# Generated by authselect on Mon Apr 19 11:54:28 2021
# Do not modify this file manually.

# If you want to make changes to nsswitch.conf please modify
# /etc/authselect/user-nsswitch.conf and run 'authselect apply-changes'.
#
# Note that your changes may not be applied as they may be
# overwritten by selected profile. Maps set in the authselect
# profile takes always precedence and overwrites the same maps
# set in the user file. Only maps that are not set by the profile
# are applied from the user file.
#
```

```
# For example, if the profile sets:
#   passwd: sss files
# and /etc/authselect/user-nsswitch.conf contains:
#   passwd: files
#   hosts: files dns
# the resulting generated nsswitch.conf will be:
#   passwd: sss files # from profile
#   hosts: files dns # from user file
```

```
passwd:      sss files systemd
group:       sss files systemd
netgroup:    sss files
automount:   sss files
services:    sss files
...
shadow:      files sss
...
```

In this file :

- **sss** indicates the use of the **System Security Services Daemon** (SSSD).
  - SSSD has its origins in the **FreeIPA** (Identity, Policy and Audit) and provides Linux/Unix networks with similar functionalities as those provided by Microsoft Active Directory Domain Services to Windows™ networks,
  - For more information, consult [this page](#).
- **files** indicates the use of local text files in **/etc**,
- **systemd** indicates the use of the **nss-systemd** plugin which uses the **Name Service Switch** (NSS) function found in the **GNU C Library** (glibc).

## The gentent Command

The **getent** command is used to query the database. The command takes the following form:

```
getent database key
```

As an example, to query the user database for the trainee record, you would use the following command:

```
[root@centos8 ~]# getent passwd trainee
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
```

To query which users belong to a specific group, you would use the following command :

```
[root@centos8 ~]# getent group mail
mail:x:12:
```

By using the getent command without a key, you can list the entire database :

```
[root@centos8 ~]# getent 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
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
libstoragemgmt:x:996:993:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
cockpit-ws:x:995:991:User for cockpit-ws:/nonexisting:/sbin/nologin
```

```
sssd:x:994:990:User for sssd:/:/sbin/nologin
setroubleshoot:x:993:989::/var/lib/setroubleshoot:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
chrony:x:992:988::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
cockpit-wsinstance:x:991:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
rngd:x:990:986:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin
gluster:x:989:985:GlusterFS daemons:/run/gluster:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
saslauthd:x:988:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
dnsmasq:x:983:983:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
```

## The /etc/group and /etc/gshadow files

To see a list of the current groups, use the following command:

```
[root@centos8 ~]# cat /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:
wheel:x:10:
cdrom:x:11:
```

```
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
dbus:x:81:
utmp:x:22:
utempter:x:35:
input:x:999:
kvm:x:36:qemu
render:x:998:
systemd-journal:x:190:
systemd-coredump:x:997:
systemd-resolve:x:193:
tss:x:59:
polkitd:x:996:
printadmin:x:995:
unbound:x:994:
libstoragemgmt:x:993:
ssh_keys:x:992:
cockpit-ws:x:991:
sssd:x:990:
setroubleshoot:x:989:
sshd:x:74:
chrony:x:988:
slocate:x:21:
tcpdump:x:72:
```

```
trainee:x:1000:  
cockpit-wsinstance:x:987:  
rngd:x:986:  
gluster:x:985:  
qemu:x:107:  
rpc:x:32:  
rpcuser:x:29:  
saslauth:x:76:  
libvirt:x:984:  
radvd:x:75:  
dnsmasq:x:983:  
screen:x:84:
```



**Important** : Note that GID ( Group ID ) of root is always **0** that the GIDs of standard, non-system, users start at 1000. The system user GIDs are between 1 and 99 and between 201 and 999.

This file has one line per group. In each line there are four fields separated by the **:** character.

- The unique group name,
- The group password. An **x** in this field indicates that we are using the **/etc/gshadow** file to store encrypted passwords. A **!** in this field indicates that the group has no password and that the use of the **newgrp** command is not possible. We will detail the **newgrp** command later,
- The unique GID,
- The list of users who have the group as a secondary group.

To see the contents of the **/etc/gshadow** file, use the following command:

```
[root@centos8 ~]# cat /etc/gshadow  
root:::  
bin:::  
daemon:::  
sys:::
```

```
adm:::
tty:::
disk:::
lp:::
mem:::
kmem:::
wheel:::
cdrom:::
mail:::
man:::
dialout:::
floppy:::
games:::
tape:::
video:::
ftp:::
lock:::
audio:::
users:::
nobody:::
dbus:!:
utmp:!:
utempter:!:
input:!:
kvm:!:qemu
render:!:
systemd-journal:!:
systemd-coredump:!:
systemd-resolve:!:
tss:!:
polkitd:!:
printadmin:!:
unbound:!:
libstoragemgmt:!:
```

```
ssh_keys:!::  
cockpit-ws:!::  
sssd:!::  
setroubleshoot:!::  
sshd:!::  
chrony:!::  
slocate:!::  
tcpdump:!::  
trainee:!::  
cockpit-wsinstance:!::  
rngd:!::  
gluster:!::  
qemu:!::  
rpc:!::  
rpcuser:!::  
saslauth:!::  
libvirt:!::  
radvd:!::  
dnsmasq:!!::  
screen:!::
```

This file has one line per group. In each line there are four fields separated by the `:` character.

- The unique group name from the **/etc/group** file,
- The encrypted group password. If this is empty, only the users who are members of the group can use the `newgrp` command. If the field contains a `!`, an `x` or a `*` it indicates that no one can use the `newgrp` command,
- The group administrator if one exists,
- The list of users who have the group as a secondary group.

To check if these two files have any anomalies or errors, use the following command:

```
[root@centos8 ~]# grpck -r  
[root@centos8 ~]#
```



**Important** : The **-r** switch is used to check the files without making any automatic changes to them.

Two other usefull commands are:

- **grpconv**
  - this command regenerates a new **/etc/gshadow** file from the **/etc/group** file and an existing **/etc/gshadow** file if it exists,
- **grpunconv**
  - this command regenerates a new **/etc/group** file from the **/etc/gshadow** file and an existing **/etc/group** file if it exists and then deletes the **/etc/gshadow** file.

## The **/etc/passwd** and **/etc/shadow** files



**Important** : Note that user names under Linux are limited to 32 characters and can contain upper case characters, lower case characters, numbers (except as the first character of the user name) and the majority of punctuation characters. However certain utilities such as **useradd** do not recognise upper case characters, lower case characters, numbers, punctuation characters (except **\_** and **..** **useradd** also accepts the **\$** character, but only as the last character of the user name in which case the account name is considered to be a machine. In addition, certain utilities limit the number of chracters to just **8**.

To see a list of the current users, use the following command:

```
[root@centos8 ~]# cat /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
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
libstoragemgmt:x:996:993:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
cockpit-ws:x:995:991:User for cockpit-ws:/nonexisting:/sbin/nologin
sssd:x:994:990:User for sssd:/:/sbin/nologin
setroubleshoot:x:993:989:/:/var/lib/setroubleshoot:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
chrony:x:992:988:/:/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
cockpit-wsinstance:x:991:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
rngd:x:990:986:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin
gluster:x:989:985:GlusterFS daemons:/run/gluster:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
saslauth:x:988:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
dnsmasq:x:983:983:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
```



**Important** : Note that the UID of root is always **0**. Standard user UIDs start at 1000 whilst system accounts range from 1 to 99 and from 201 to 999.

This file has one line per user. In each line there are seven fields separated by the **:** character.

- A unique user name,
- The user password. An **x** in this field indicates that we are using the **/etc/shadow** file to store encrypted passwords,
- The UID,
- The GID of the user's primary group,
- A comment. This field is often called the **GECOS** field,
- The user's home directory,
- The user's shell.

To see the contents of the **/etc/shadow** file, use the following command:

```
[root@centos8 ~]# cat /etc/shadow
root:$6$9Sa1IumuSlJc8EBg$8jGU/4xGCXy64QuBSMyK0C6/FWs41rdY5tzF5/7yHG6FRS2Y2e0JIcst1JbcvNoqMPDU4lpZ6THW97jwGuQNf1::
0:99999:7:::
bin:!:18264:0:99999:7:::
daemon:!:18264:0:99999:7:::
adm:!:18264:0:99999:7:::
lp:!:18264:0:99999:7:::
sync:!:18264:0:99999:7:::
shutdown:!:18264:0:99999:7:::
halt:!:18264:0:99999:7:::
mail:!:18264:0:99999:7:::
operator:!:18264:0:99999:7:::
games:!:18264:0:99999:7:::
ftp:!:18264:0:99999:7:::
nobody:!:18264:0:99999:7:::
dbus:!!!:18390:!!!!:
```

```
systemd-coredump:!!:18390::::::  
systemd-resolve:!!:18390::::::  
tss:!!:18390::::::  
polkitd:!!:18390::::::  
unbound:!!:18390::::::  
libstoragemgmt:!!:18390::::::  
cockpit-ws:!!:18390::::::  
sssd:!!:18390::::::  
setroubleshoot:!!:18390::::::  
sshd:!!:18390::::::  
chrony:!!:18390::::::  
tcpdump:!!:18390::::::  
trainee:$6$p4H0AHX7UAzw1nQh$VZL12Lye.mR8v1IP2e4f0PCW8DzHj2MMAaA7r2ZLoTnQN7Ziskce3bo/xTMu1bXZm5GebJjSw7.X5tABVNoJ2  
/::0:99999:7:::  
cockpit-wsinstance:!!:18736::::::  
rngd:!!:18736::::::  
gluster:!!:18736::::::  
qemu:!!:18736::::::  
rpc:!!:18736:0:99999:7:::  
rpcuser:!!:18736::::::  
saslauth:!!:18736::::::  
radvd:!!:18736::::::  
dnsmasq:!!:18736::::::
```

In each line there are eight fields separated by the **:** character:

- The unique user name from the **/etc/passwd** file,
- The encrypted user password. This field can also hold one of the following :
  - **!!** - the user password has not yet been set and the account is blocked,
  - **\*** - the account is blocked,
  - **empty** - the user can connect with an empty password,
- The number of days between the **01/01/1970** and the date of the last change of the password,
- The number of days that the current password is valid. A **0** in this field means that the password will never expire,
- The number of days until the next password change,

- The number of days before the the next password change that the user will receive a notification,
- The number days after the password expiration date that the account will be deactivated if the user does not change the password,
- The number of days, starting from the **01/01/1970**, until the account deactivation.

To check if these two files have any anomalies or errors, use the following command:

```
[root@centos8 ~]# pwck -r
user 'cockpit-ws': directory '/nonexisting' does not exist
user 'cockpit-wsinstance': directory '/nonexisting' does not exist
user 'rngd': directory '/var/lib/rngd' does not exist
user 'saslauth': directory '/run/saslauthd' does not exist
pwck: no changes
```

<note important> **Important** - The **-r** switch is used to check the files without making any automatic changes to them. </note>

Two other usefull commands are:

- **pwconv**
  - permet de régénérer le fichier **/etc/shadow** à partir du fichier **/etc/passwd** et éventuellement du fichier **/etc/shadow** existant
- **pwunconv**
  - permet de régénérer le fichier **/etc/passwd** à partir du fichier **/etc/shadow** et éventuellement du fichier **/etc/passwd** existant puis supprime le fichier **/etc/shadow**

## Commands

### Groups

#### groupadd

This command is used to create groups.

---

## Command Line Switches

```
[root@centos8 ~]# groupadd --help
```

```
Usage: groupadd [options] GROUP
```

### Options:

|                         |                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------|
| -f, --force             | exit successfully if the group already exists,<br>and cancel -g if the GID is already used |
| -g, --gid GID           | use GID for the new group                                                                  |
| -h, --help              | display this help message and exit                                                         |
| -K, --key KEY=VALUE     | override /etc/login.defs defaults                                                          |
| -o, --non-unique        | allow to create groups with duplicate<br>(non-unique) GID                                  |
| -p, --password PASSWORD | use this encrypted password for the new group                                              |
| -r, --system            | create a system account                                                                    |
| -R, --root CHROOT_DIR   | directory to chroot into                                                                   |
| -P, --prefix PREFIX_DIR | directory prefix                                                                           |



**Important** : It is possible to create two or more groups having the same GID.



**Important** : Note the use of the **r** switch which is used to create a system group.

## groupdel

This command is used to delete groups..

## Command Line Switches

```
[root@centos8 ~]# groupdel --help
```

```
Usage: groupdel [options] GROUP
```

### Options:

|                         |                                                        |
|-------------------------|--------------------------------------------------------|
| -h, --help              | display this help message and exit                     |
| -R, --root CHROOT_DIR   | directory to chroot into                               |
| -P, --prefix PREFIX_DIR | prefix directory where are located the /etc/* files    |
| -f, --force             | delete group even if it is the primary group of a user |

## groupmod

The command is used to modify an existing group.

## Command Line Switches

```
[root@centos8 ~]# groupmod --help
```

```
Usage: groupmod [options] GROUP
```

### Options:

|                          |                                                     |
|--------------------------|-----------------------------------------------------|
| -g, --gid GID            | change the group ID to GID                          |
| -h, --help               | display this help message and exit                  |
| -n, --new-name NEW_GROUP | change the name to NEW_GROUP                        |
| -o, --non-unique         | allow to use a duplicate (non-unique) GID           |
| -p, --password PASSWORD  | change the password to this (encrypted)<br>PASSWORD |
| -R, --root CHROOT_DIR    | directory to chroot into                            |
| -P, --prefix PREFIX_DIR  | prefix directory where are located the /etc/* files |

## newgrp

This command is used to temporarily change the user's primary group.

### Command Line Switches

```
[root@centos8 ~]# newgrp --help
Usage: newgrp [-] [group]
```

## gpasswd

This command is used to administer the **/etc/group** file.

### Command Line Switches

```
[root@centos8 ~]# gpasswd --help
Usage: gpasswd [option] GROUP
```

#### Options:

|                                |                                          |
|--------------------------------|------------------------------------------|
| -a, --add USER                 | add USER to GROUP                        |
| -d, --delete USER              | remove USER from GROUP                   |
| -h, --help                     | display this help message and exit       |
| -Q, --root CHROOT_DIR          | directory to chroot into                 |
| -r, --delete-password          | remove the GROUP's password              |
| -R, --restrict                 | restrict access to GROUP to its members  |
| -M, --members USER,...         | set the list of members of GROUP         |
| -A, --administrators ADMIN,... | set the list of administrators for GROUP |

Except for the -A and -M options, the options cannot be combined.

## Users

### useradd

This command is used to add users.

The exit codes of the useradd command are :

| Exit Code | Description                          |
|-----------|--------------------------------------|
| 1         | Cannot update the passwd file        |
| 2         | Invalid syntax                       |
| 3         | Invalid option                       |
| 4         | UID in use                           |
| 6         | Group does not exist                 |
| 9         | Username in use                      |
| 10        | Cannot update the group file         |
| 12        | Cannot create user's home directory  |
| 13        | Cannot create user's mail spool file |

### Command Line Switches

```
[root@centos8 ~]# useradd --help
Usage: useradd [options] LOGIN
       useradd -D
       useradd -D [options]
```

#### Options:

```
-b, --base-dir BASE_DIR    base directory for the home directory of the
                           new account
```

|                              |                                                          |
|------------------------------|----------------------------------------------------------|
| -c, --comment COMMENT        | GECOS field of the new account                           |
| -d, --home-dir HOME_DIR      | home directory of the new account                        |
| -D, --defaults               | print or change default useradd configuration            |
| -e, --expiredate EXPIRE_DATE | expiration date of the new account                       |
| -f, --inactive INACTIVE      | password inactivity period of the new account            |
| -g, --gid GROUP              | name or ID of the primary group of the new account       |
| -G, --groups GROUPS          | list of supplementary groups of the new account          |
| -h, --help                   | display this help message and exit                       |
| -k, --skel SKEL_DIR          | use this alternative skeleton directory                  |
| -K, --key KEY=VALUE          | override /etc/login.defs defaults                        |
| -l, --no-log-init            | do not add the user to the lastlog and faillog databases |
| -m, --create-home            | create the user's home directory                         |
| -M, --no-create-home         | do not create the user's home directory                  |
| -N, --no-user-group          | do not create a group with the same name as the user     |
| -o, --non-unique             | allow to create users with duplicate (non-unique) UID    |
| -p, --password PASSWORD      | encrypted password of the new account                    |
| -r, --system                 | create a system account                                  |
| -R, --root CHROOT_DIR        | directory to chroot into                                 |
| -P, --prefix PREFIX_DIR      | prefix directory where are located the /etc/* files      |
| -s, --shell SHELL            | login shell of the new account                           |
| -u, --uid UID                | user ID of the new account                               |
| -U, --user-group             | create a group with the same name as the user            |
| -Z, --selinux-user SEUSER    | use a specific SEUSER for the SELinux user mapping       |



**Important :** It is possible to create two or more users having the same UID.



**Important** : Note the use of the **r** switch which is used to create a system user. In this case the home directory of the user is **not** created.

## userdel

This command is used to delete users.

### Command Line Switches

```
[root@centos8 ~]# userdel --help
Usage: userdel [options] LOGIN
```

#### Options:

|                         |                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| -f, --force             | force some actions that would fail otherwise<br>e.g. removal of user still logged in<br>or files, even if not owned by the user |
| -h, --help              | display this help message and exit                                                                                              |
| -r, --remove            | remove home directory and mail spool                                                                                            |
| -R, --root CHROOT_DIR   | directory to chroot into                                                                                                        |
| -P, --prefix PREFIX_DIR | prefix directory where are located the /etc/* files                                                                             |
| -Z, --selinux-user      | remove any SELinux user mapping for the user                                                                                    |



**Important** : Note that when you delete a user, the UID associated with the account can be re-used. The maximum permissible number of accounts was **65 536** under the **2.2.x** kernel. Recent kernels allow up to 4,2 Billion accounts.

## usermod

This command is used to modify an existing user.

### Command Line Switches

```
[root@centos8 ~]# usermod --help
Usage: usermod [options] LOGIN
```

#### Options:

|                              |                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| -c, --comment COMMENT        | new value of the GECOS field                                                                                      |
| -d, --home HOME_DIR          | new home directory for the user account                                                                           |
| -e, --expiredate EXPIRE_DATE | set account expiration date to EXPIRE_DATE                                                                        |
| -f, --inactive INACTIVE      | set password inactive after expiration to INACTIVE                                                                |
| -g, --gid GROUP              | force use GROUP as new primary group                                                                              |
| -G, --groups GROUPS          | new list of supplementary GROUPS                                                                                  |
| -a, --append                 | append the user to the supplemental GROUPS mentioned by the -G option without removing the user from other groups |
| -h, --help                   | display this help message and exit                                                                                |
| -l, --login NEW_LOGIN        | new value of the login name                                                                                       |
| -L, --lock                   | lock the user account                                                                                             |
| -m, --move-home              | move contents of the home directory to the new location (use only with -d)                                        |
| -o, --non-unique             | allow using duplicate (non-unique) UID                                                                            |
| -p, --password PASSWORD      | use encrypted password for the new password                                                                       |
| -R, --root CHROOT_DIR        | directory to chroot into                                                                                          |
| -P, --prefix PREFIX_DIR      | prefix directory where are located the /etc/* files                                                               |
| -s, --shell SHELL            | new login shell for the user account                                                                              |
| -u, --uid UID                | new UID for the user account                                                                                      |
| -U, --unlock                 | unlock the user account                                                                                           |

```
-v, --add-subuids FIRST-LAST  add range of subordinate uids
-V, --del-subuids FIRST-LAST  remove range of subordinate uids
-w, --add-subgids FIRST-LAST  add range of subordinate gids
-W, --del-subgids FIRST-LAST  remove range of subordinate gids
-Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```



**Important** : Notez l'option **-L** qui permet de verrouiller un compte.

## passwd

This command is used to create or change a user's password.

### Command Line Switches

```
[root@centos8 ~]# passwd --help
Usage: passwd [OPTION...] <accountName>
  -k, --keep-tokens      keep non-expired authentication tokens
  -d, --delete           delete the password for the named account (root only); also removes password lock if
any
  -l, --lock             lock the password for the named account (root only)
  -u, --unlock           unlock the password for the named account (root only)
  -e, --expire           expire the password for the named account (root only)
  -f, --force            force operation
  -x, --maximum=DAYS     maximum password lifetime (root only)
  -n, --minimum=DAYS     minimum password lifetime (root only)
  -w, --warning=DAYS     number of days warning users receives before password expiration (root only)
  -i, --inactive=DAYS    number of days after password expiration when an account becomes disabled (root only)
  -S, --status           report password status on the named account (root only)
```

```
--stdin          read new tokens from stdin (root only)
```

**Help options:**

```
-?, --help      Show this help message  
--usage        Display brief usage message
```



**Important** : Note the **-I** switch which blocks a user account by placing a **!** character in front of the user's encrypted password.

## chage

This command is used to set the minimum number of days before a password change, the maximum number of days before a password change, the expiration warning days value and to set the password inactive after the expiration of a pre-defined numbers of days.

### Command Line Switches

```
[root@centos8 ~]# chage --help  
Usage: chage [options] LOGIN
```

**Options:**

```
-d, --lastday LAST_DAY    set date of last password change to LAST_DAY  
-E, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE  
-h, --help                display this help message and exit  
-I, --inactive INACTIVE   set password inactive after expiration  
                           to INACTIVE  
-l, --list                show account aging information  
-m, --mindays MIN_DAYS    set minimum number of days before password  
                           change to MIN_DAYS
```

|                          |                                                               |
|--------------------------|---------------------------------------------------------------|
| -M, --maxdays MAX_DAYS   | set maximum number of days before password change to MAX_DAYS |
| -R, --root CHROOT_DIR    | directory to chroot into                                      |
| -W, --warndays WARN_DAYS | set expiration warning days to WARN_DAYS                      |

## Configuration

The default behaviour of the **useradd** command is configured by the contents of the **/etc/default/useradd** file:

```
[root@centos8 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

In this file we can find:

- **GROUP** - indicates the default primary group for a new user when the useradd command is used with the **-N** switch. If the switch is not used, the user's primary group will be either the group specified by the **-g** switch or a group having the same name as the user,
- **HOME** - indicates the directory under which all home directories will be created but only if this behaviour is authorized in the **/etc/login.defs** file,
- **INACTIVE** - The number days after the password expiration date that the account will be deactivated if the user does not change the password. A -1 in this field deactivates this behaviour,
- **EXPIRE** - indicates in the above example that the password will never expire,
- **SHELL** - indicates the shell to be assigned to the user,
- **SKEL** - indicates the directory in which are stored the files that will be copied to the user's home directory upon creation,
- **CREATE\_MAIL\_SPOOL** - indicates if the user's mailbox will be created.

This information can also be viewed by using the **useradd** command:

```
[root@centos8 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

To see a list of the files in **/etc/skel**, use the following command:

```
[root@centos8 ~]# ls -la /etc/skel
total 24
drwxr-xr-x.  2 root root  62 Apr 19 11:50 .
drwxr-xr-x. 106 root root 8192 Apr 20 10:17 ..
-rw-r--r--.  1 root root  18 Jul 21  2020 .bash_logout
-rw-r--r--.  1 root root 141 Jul 21  2020 .bash_profile
-rw-r--r--.  1 root root 376 Jul 21  2020 .bashrc
```



**Important** : Note that with **Red Hat** and **CentOS** the **.bash\_profile** file replaces the **.profile** file used in other distributions such as Debian.

To identify a user's UID, GID and secondary groups, if any, use the following command:

```
[root@centos8 ~]# id trainee
uid=1000(trainee) gid=1000(trainee) groups=1000(trainee)
```

To identify the user's groups we can also use the following command:

```
[root@centos8 ~]# groups trainee
trainee : trainee
```

The ranges of UIDs and GIDs that can be used are configured in the **/etc/login.defs** file:

```
...
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                1000
UID_MAX                60000
# System accounts
SYS_UID_MIN            201
SYS_UID_MAX            999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                1000
GID_MAX                60000
# System accounts
SYS_GID_MIN            201
SYS_GID_MAX            999
...
```

## LAB #1 - Managing Groups and Users

Create three groups, **group1**, **group2** et **group3**. The GID of **group3** needs to set at **1807** :

```
[root@centos8 ~]# groupadd groupe1; groupadd groupe2; groupadd -g 1807 groupe3
```

Now create three users **fenestros1**, **fenestros2** and **fenestros3**. The three users have as their primary group **group1**, **group2** and **group3**

respectively. **fenestros2** is also a member of **group1** and **group3**. **fenestros1** has a GECOS of **tux1**:

```
[root@centos8 ~]# useradd -g groupe2 fenestros2; useradd -g 1807 fenestros3; useradd -g groupe1 fenestros1
[root@centos8 ~]# usermod -G groupe1,groupe3 fenestros2
[root@centos8 ~]# usermod -c "tux1" fenestros1
```

Now look at the bottom of the **/etc/passwd** file:

```
[root@centos8 ~]# tail /etc/passwd
gluster:x:989:985:GlusterFS daemons:/run/gluster:/sbin/nologin
qemu:x:107:107:qemu user:///sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
saslauth:x:988:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radvd:x:75:75:radvd user:///sbin/nologin
dnsmasq:x:983:983:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
fenestros2:x:1001:1002:~/home/fenestros2:/bin/bash
fenestros3:x:1002:1807:~/home/fenestros3:/bin/bash
fenestros1:x:1003:1001:tux1:/home/fenestros1:/bin/bash
```

Now look at the bottom of the **/etc/group** file:

```
[root@centos8 ~]# tail /etc/group
rpc:x:32:
rpcuser:x:29:
saslauth:x:76:
libvirt:x:984:
radvd:x:75:
dnsmasq:x:983:
screen:x:84:
groupe1:x:1001:fenestros2
groupe2:x:1002:
groupe3:x:1807:fenestros2
```

Create a password for **group3**:

```
[root@centos8 ~]# gpasswd groupe3
Changing the password for group groupe3
New Password: fenestros
Re-enter new password: fenestros
```



**Important** : Note that the passwords will **not** be visible.

Now look at the bottom of the **/etc/gshadow** file:

```
[root@centos8 ~]# tail /etc/gshadow
rpc:!::
rpcuser:!::
saslauth:!::
libvirt:!::
radvd:!::
dnsmasq:!::
screen:!::
groupe1:!::fenestros2
groupe2:!::
groupe3:$6$c0nWua0.7BveY$qZ9070RU.vE0h1Ycka.VCL1Im0obgxJg8g3SvWnEA3YiZc9TB3CXEU/8nnNNAg5fBAhct7PNUXdPXwsSsY0Zg0: :
fenestros2
```



**Important** : Note the presence of an encrypted password for **group3**.

Make **fenestros1** administrator of **group3** :

```
[root@centos8 ~]# gpasswd -A fenestros1 groupe3
```

Now look at the bottom of the **/etc/gshadow** file again:

```
[root@centos8 ~]# tail /etc/gshadow
rpc:!:
rpcuser:!:
saslauth:!:
libvirt:!:
radvd:!:
dnsmasq:!:
screen:!:
groupe1:!:fenestros2
groupe2:!:
groupe3:$6$c0nWua0.7BveY$qZ9070RU.vE0hlYcka.VCL1Im0obgxJg8g3SvWnEA3YiZc9TB3CXEU/8nnNNAg5fBAhct7PNUXdPXwsSsY0Zg0:f
enestros1:fenestros2
```



**Important** : **fenestros1** can now use the group password to add or remove users from the group.

Try to delete **group3**:

```
[root@centos8 ~]# groupdel groupe3
groupdel: cannot remove the primary group of user 'fenestros3'
```



**Important** : Note that you cannot remove the primary group of an existing user.

Delete user **fenestros3** :

```
[root@centos8 ~]# userdel fenestros3
```

Try to delete **group3** again:

```
[root@centos8 ~]# groupdel groupe3
```



**Important** : This time the command does not return an error even though user **fenestros2** has the group as a secondary group.

If you delete a user without using the **-r** switch, the user's files remain on the system:

```
[root@centos8 ~]# ls -ld /home/fenestros3
drwx-----. 2 1002 groupe3 62 Apr 20 14:28 /home/fenestros3
```

In order to remove the files use the **find** command:

```
[root@centos8 ~]# find /home -user 1002 -exec rm -rf {} \;
find: '/home/fenestros3': No such file or directory
[root@centos8 ~]# ls -ld /home/fenestros3
ls: cannot access '/home/fenestros3': No such file or directory
```



**Important** : The final error is normal. All it means is that there are no more files to delete.

Now create the passwords for users **fenestros1** et **fenestros2**:

```
[root@centos8 ~]# passwd fenestros1
Changing password for user fenestros1.
New password: fenestros1
```

```
BAD PASSWORD: The password contains the user name in some form
Retype new password: fenestros1
passwd: all authentication tokens updated successfully.
[root@centos8 ~]# passwd fenestros2
Changing password for user fenestros2.
New password: fenestros2
BAD PASSWORD: The password contains the user name in some form
Retype new password: fenestros2
passwd: all authentication tokens updated successfully.
```



**Important** : Note that the passwords will not be visible. Note also that the rules for creating passwords do not apply to passwords created by root.

## LAB #2 - su et su -

You are now going to become **fenestros2**, at first without his environment settings and then with his environment settings.

Firstly check where you are:

```
[root@centos8 ~]# pwd
/root
```

Use the **su** (switch user) command to become **fenestros2** without his environment settings:

```
[root@centos8 ~]# su fenestros2
[fenestros2@centos8 root]$ pwd
/root
```

Note that you are still in the `/root` directory. This means that despite becoming `fenestros2`, you still have root's environment settings.



**Important** : Environment settings include, amongst other things, the user's home directory and the value of the **PATH** variable.

Type **exit** to become **root** again:

```
[fenestros2@centos8 root]$ exit  
exit
```

Use the **su** - (switch user) command to become **fenestros2** with his environment settings:

```
[root@centos8 ~]# su - fenestros2  
Last login: Thu Oct 15 18:30:54 CEST 2015 on pts/0  
[fenestros2@centos8 ~]$ pwd  
/home/fenestros2
```



**Important** : Note that you have landed in fenestros2's home directory. Also note that root can become any user on the system **without** any knowledge of the user's password.

Type **exit** to become **root** again:

```
[fenestros2@centos8 ~]$ exit  
logout  
[root@centos8 ~]#
```

## sudo

The sudo command allows a user to execute a command as root or as another user. The effective UID and GID of the user invoking sudo are those of the target user, allowing for a simple but effective way of delegating system administration.

The sudo command is configured by the contents of the **/etc/sudoers** file:

```
[root@centos8 ~]# cat /etc/sudoers
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias      FILESERVERS = fs1, fs2
# Host_Alias      MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem

## Command Aliases
## These are groups of related commands...
```

```
## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables,
/usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, /usr/bin/systemctl start, /usr/bin/systemctl stop,
/usr/bin/systemctl reload, /usr/bin/systemctl restart, /usr/bin/systemctl status, /usr/bin/systemctl enable,
/usr/bin/systemctl disable

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

#
# Refuse to run if unable to disable echo on the tty.
#
Defaults    !visiblepw
```

```
#
# Preserving HOME has security implications since many programs
# use it when searching for configuration files. Note that HOME
# is already set when the the env_reset option is enabled, so
# this option is only effective for configurations where either
# env_reset is disabled or HOME is present in the env_keep list.
#
Defaults    always_set_home
Defaults    match_group_by_gid

# Prior to version 1.8.15, groups listed in sudoers that were not
# found in the system group database were passed to the group
# plugin, if any. Starting with 1.8.15, only groups of the form
# %:group are resolved via the group plugin by default.
# We enable always_query_group_plugin to restore old behavior.
# Disable this option for new behavior.
Defaults    always_query_group_plugin

Defaults    env_reset
Defaults    env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults    env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
```

```
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
## user MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root ALL=(ALL) ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
```



**Important** : Note the presence of the **%wheel ALL=(ALL) ALL** line. This line has the following format **<WHO> <FROM WHERE> = (<AS WHO>) <WHAT>**. This line



effectively states that all members of the wheel group (%wheel) can execute all commands on the system from anywhere, as anyone. To edit the **/etc/sudoers** file you **must** use the **visudo** command