Managing Users and Groups

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 upto 15 secondary groups.

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

Groups

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

```
[root@centos ~]# cat /etc/group
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
lp:x:7:daemon
mem:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:mail,postfix
uucp:x:14:
man:x:15:
games:x:20:
gopher:x:30:
video:x:39:
```

```
dip:x:40:
ftp:x:50:
lock:x:54:
audio:x:63:
nobody:x:99:
users:x:100:
dbus:x:81:
utmp:x:22:
utempter:x:35:
desktop_admin_r:x:499:
desktop_user_r:x:498:
floppy:x:19:
vcsa:x:69:
rpc:x:32:
rtkit:x:497:
avahi-autoipd:x:170:
cdrom:x:11:
tape:x:33:
dialout:x:18:
wbpriv:x:88:
pulse:x:496:
pulse-access:x:495:
fuse:x:494:
haldaemon:x:68:haldaemon
ntp:x:38:
saslauth:x:76:
postdrop:x:90:
postfix:x:89:
abrt:x:173:
rpcuser:x:29:
nfsnobody:x:65534:
gdm:x:42:
stapusr:x:156:
stapsys:x:157:
```

```
stapdev:x:158:
sshd:x:74:
tcpdump:x:72:
slocate:x:21:
trainee:x:500:
vboxsf:x:501:
```

<note important> Note that GID (Group ID) of root is always **0** that the GIDs of standard, non-system, users start at 500. </note>

This file has one line per group. In each line there are four fields seperated 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@centos ~]# cat /etc/gshadow
root:::
bin:::bin,daemon
daemon:::bin,daemon
sys:::bin,adm
adm:::adm,daemon
tty:::
disk:::
lp:::daemon
mem:::
kmem:::
wheel:::
mail:::mail,postfix
uucp:::
man:::
```

```
games:::
gopher:::
video:::
dip:::
ftp:::
lock:::
audio:::
nobody:::
users:::
dbus:!::
utmp:!::
utempter:!::
desktop_admin_r:!::
desktop_user_r:!::
floppy:!::
vcsa:!::
rpc:!::
rtkit:!::
avahi-autoipd:!::
cdrom:!::
tape:!::
dialout:!::
wbpriv:!::
pulse:!::
pulse-access:!::
fuse:!::
haldaemon:!::haldaemon
ntp:!::
saslauth:!::
postdrop:!::
postfix:!::
abrt:!::
rpcuser:!::
nfsnobody:!::
```

```
gdm:!::
stapusr:!::
stapsys:!::
stapdev:!::
sshd:!::
tcpdump:!::
slocate:!::
trainee:!!::
vboxsf:!::
```

This file has one line per group. In each line there are four fields seperated 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 noone 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 anomolies or errors, use the following command:

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

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

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 thens deletes the **/etc/gshadow** file.

Users

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

```
[root@centos ~]# 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
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
saslauth:x:497:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
```

```
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:496:1::/var/run/vboxadd:/bin/false
```

<note important> Note that the UID of root is always **0**. Standard user UIDs start at 500 whilst system accounts range form 1 to 499. </note>

This file has one line per user. In each line there are seven fields seperated 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 users 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@centos ~]# cat /etc/shadow
root:$6$pQn9Y2MFsNBnK9F7$cjqbC6SNRHn1kGE0yCuHEB.vhYNeycWOvAyJuuEbslo3n3qhRcp6p3lEG/YuxwMRtiZ.qIddmVpuTvTEmOa0W.:1
6003:0:99999:7:::
bin:*:15628:0:99999:7:::
daemon:*:15628:0:99999:7:::
adm:*:15628:0:99999:7:::
lp:*:15628:0:99999:7:::
sync:*:15628:0:99999:7:::
shutdown:*:15628:0:99999:7:::
halt:*:15628:0:99999:7:::
mail:*:15628:0:99999:7:::
uucp:*:15628:0:99999:7:::
operator:*:15628:0:99999:7:::
games:*:15628:0:99999:7:::
```

```
gopher:*:15628:0:99999:7:::
ftp:*:15628:0:99999:7:::
nobody:*:15628:0:99999:7:::
dbus:!!:16003::::::
vcsa:!!:16003::::::
rpc:!!:16003:0:99999:7:::
rtkit:!!:16003::::::
avahi-autoipd:!!:16003::::::
pulse:!!:16003::::::
haldaemon:!!:16003::::::
ntp:!!:16003::::::
saslauth:!!:16003::::::
postfix:!!:16003::::::
abrt:!!:16003::::::
rpcuser:!!:16003::::::
nfsnobody:!!:16003::::::
gdm:!!:16003::::::
sshd:!!:16003::::::
tcpdump:!!:16003::::::
trainee:$6$mTKZrZa/PLvGVQ31$RWh2JTMzAclOuhGZXbocPYHssP2DmXyeU7sbK6gpMxuPrYrBK9cn43ti1SSa70YGWJ7n8EXQlyBA8gIZe5xIG
.:16003:0:99999:7:::
vboxadd:!!:16003::::::
```

In each line there are eight fields seperated 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 anomolies or errors, use the following command:

```
[root@centos ~]# pwck -r
user 'adm': directory '/var/adm' does not exist
user 'uucp': directory '/var/spool/uucp' does not exist
user 'gopher': directory '/var/gopher' does not exist
user 'ftp': directory '/var/ftp' does not exist
user 'avahi-autoipd': directory '/var/lib/avahi-autoipd' does not exist
user 'pulse': directory '/var/run/pulse' does not exist
user 'saslauth': directory '/var/empty/saslauth' does not exist
user 'vboxadd': directory '/var/run/vboxadd' does not exist
pwck: no changes
```

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

Two other usefull commands are:

- **pwconv**
  - this command regenerates a new **/etc/shadow** file from the **/etc/passwd** file and an existing **/etc/shadow** file if it exists,
- **pwunconv**
  - this command regenerates a new **/etc/passwd** file from the **/etc/shadow** file and an existing **/etc/passwd** file if it exists and thens deletes the **/etc/shadow** file.

Commands

Groups

groupadd

This command is used to create groups.

Command Line Switches

```
[root@centos ~]# groupadd --help
Usage: groupadd [options] GROUP

Options:
  -f, --force                   exit successfully if the group already exists,
                                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
                                (non-unique) GID
  -p, --password PASSWORD       use this encrypted password for the new group
  -r, --system                  create a system account
```

groupdel

This command is used to delete groups..

Command Line Switches

```
[root@centos ~]# groupdel --help
groupdel: group '--help' does not exist
```

groupmod

The command is used to modify an existing group.

Command Line Switches

```
[root@centos ~]# 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)
                                PASSWORD
```

newgrp

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

Command Line Switches

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

gpasswd

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

Command Line Switches

```
[root@centos ~]# gpasswd --help
gpasswd: unrecognized option '--help'
Usage: gpasswd [option] GROUP

Options:
  -a, --add USER                add USER to GROUP
  -d, --delete USER             remove USER from GROUP
  -r, --remove-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

Exit Code	Description
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@centos ~]# useradd --help
Usage: useradd [options] LOGIN

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
  -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
```

userdel

This command is used to delete users.

Command Line Switches

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

Options:
  -f, --force                   force removal of files,
                                even if not owned by user
  -h, --help                    display this help message and exit
  -r, --remove                  remove home directory and mail spool
  -Z, --selinux-user            remove SELinux user from SELinux user mapping
```

usermod

This command is used to modify an existing user.

Command Line Switches

```
[root@centos ~]# 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
                                him/her 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
  -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
  -Z, --selinux-user            new SELinux user mapping for the user account
```

passwd

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

Command Line Switches

```
[root@centos ~]# 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)
  -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
```

Configuration

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

```
[root@centos ~]# 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 roup 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@centos ~]# 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@centos ~]# ls -la /etc/skel
```

```
total 36
drwxr-xr-x.   4 root root  4096 Oct 25 10:30 .
drwxr-xr-x. 113 root root 12288 Oct 27 17:00 ..
-rw-r--r--.   1 root root    18 Jul 18 15:15 .bash_logout
-rw-r--r--.   1 root root   176 Jul 18 15:15 .bash_profile
-rw-r--r--.   1 root root   124 Jul 18 15:15 .bashrc
drwxr-xr-x.   2 root root  4096 Nov 12  2010 .gnome2
drwxr-xr-x.   4 root root  4096 Oct 25 09:33 .mozilla
```

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

```
[root@centos ~]# id trainee
uid=500(trainee) gid=500(trainee) groups=500(trainee)
```

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

```
[root@centos ~]# 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           500
UID_MAX         60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN           500
GID_MAX         60000
```

```
...
```

LAB #1 - Managing Groups and Users

Create three groups, **group1**, **group2** et **group3**. The GID of **group3** needs to set at **807** :

```
[root@centos ~]# groupadd group1; groupadd group2; groupadd -g 807 group3
```

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@centos ~]# useradd -g group2 fenestros2; useradd -g 807 fenestros3; useradd -g group1 fenestros1
[root@centos ~]# usermod -G group1,group3 fenestros2
[root@centos ~]# usermod -c "tux1" fenestros1
```

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

```
[root@centos ~]# cat /etc/passwd
...
fenestros2:x:501:503::/home/fenestros2:/bin/bash
fenestros3:x:502:807::/home/fenestros3:/bin/bash
fenestros1:x:503:502:tux1:/home/fenestros1:/bin/bash
```

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

```
[root@centos ~]# cat /etc/group
...
group1:x:502:fenestros2
group2:x:503:
group3:x:807:fenestros2
```

Create a password for **group3**:

```
[root@centos ~]# gpasswd group3
Changing the password for group group3
New Password: fenestros
Re-enter new password: fenestros
```

<note important> Note that the passwords will not be visible. </note>

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

```
[root@centos ~]# cat /etc/gshadow
...
group1:!::fenestros2
group2:!::
group3:$6$C1Itl7VHeUq05g$Mr2Re7ry6Gnp3.Ad2Ym50H9P5WIDgDZpx/woEgcPTYAqba3v71xX6Er1RP9OuK0Hw/DVRYaI/qiq/GJ1b3PkH1::
fenestros2
```

<note important> Note the presence of an encrypted password for **group3**. </note>

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

```
[root@centos ~]# gpasswd -A fenestros1 group3
```

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

```
[root@centos ~]# cat /etc/gshadow
...
group1:!::fenestros2
group2:!::
group3:$6$C1Itl7VHeUq05g$Mr2Re7ry6Gnp3.Ad2Ym50H9P5WIDgDZpx/woEgcPTYAqba3v71xX6Er1RP9OuK0Hw/DVRYaI/qiq/GJ1b3PkH1:f
enestros1:fenestros2
```

<note important> **fenestros1** can now use the group password to add or remove users from the group. </note>

Try to delete **group3**:

```
[root@centos ~]#  groupdel group3
groupdel: cannot remove the primary group of user 'fenestros3'
```

<note important> Note that you cannot remove the primary group of a user. </note>

Delete user **fenestros3** :

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

Try to delete **group3** again:

```
[root@centos ~]# groupdel group3
```

<note important> This time the command does not return an error even though user **fenestros2** had the group as a secondary group. </note>

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

```
[root@centos ~]# ls -ld /home/fenestros3
drwx------. 4 502 group3 4096 Oct 28 18:24 /home/fenestros3
```

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

```
[root@centos ~]# find /home -user 502 -exec rm -rf {} \;
find: `/home/fenestros3': No such file or directory
```

<note important> The final error is normal. All it means is that there are no more files to delete. </note>

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

```
[root@centos ~]# passwd fenestros1
Changing password for user fenestros1.
New password: fenestros1
BAD PASSWORD: it is based on a dictionary word
Retype new password: fenestros1
```

```
passwd: all authentication tokens updated successfully.
[root@centos ~]# passwd fenestros2
Changing password for user fenestros2.
New password: fenestros2
BAD PASSWORD: it is based on a dictionary word
Retype new password: fenestros2
passwd: all authentication tokens updated successfully.
```

<note 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. </note>

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@centos ~]# pwd
/root
```

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

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

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

<note important> Environment settings include, amongst other things, the user's home directory and the value of the **PATH** variable. </note>

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

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

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

```
[root@centos ~]# su - fenestros2
[fenestros2@centos ~]$ pwd
/home/fenestros2
```

<note 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. </note>

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

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

sudo

The sudo command allows a user to execute a command as root or as anoher 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@centos ~]# 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

## 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

#
# Disable "ssh hostname sudo <cmd>", because it will show the password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

#
# Refuse to run if unable to disable echo on the tty. This setting should also be
# changed in order to be able to use sudo without a tty. See requiretty above.
#
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    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC 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
```

<note 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. </note>

To edit the **/etc/sudoers** file you **must** use the following command:

```
# visudo
```

Edit the file by removing the **#** character in front of the following line:

```
...
# %wheel    ALL=(ALL) ALL
...
```

Save the file and exit vi.

~~DISCUSSION:off~~
