

## User Administration

### 1. How to add a user:

```
# useradd <username>
```

### 2. Creating User with preferred home directory:

```
# useradd -d <dir-name> <username>
```

for existing users:

```
# mkdir <dir-name>
```

```
# usermod -d <dir-name> <username>
```

```
# chown <username>:<groupname> <dir-name>
```

```
# cd /etc/skel/ ; cp .bashprofile .bashrc <dir-name>
```

### 3. Creating user with preferred SHELL:

Before performing this command get a list of shells supported by your distribution using “cat /etc/shells”

```
# useradd -s <shell-name> <username>
```

Example: `useradd -s /bin/sh admin`

for existing users:

```
# usermod -s <shell-name> <username>
```

other commands:

```
# chsh -s <shell-name> <username>
```

### 4. Block login access to a user:

```
# useradd -s /sbin/nologin <username>
```

for existing user:

```
# usermod -L <username>
```

### 5. Unblock login access to a user:

```
# usermod -s /bin/bash <username>
```

```
# usermod -U <username>
```

### 6. How to set expiry date for a user:

```
# useradd -e <YYYY-MM-DD> <username>
```

for existing users:

```
# usermod -e <YYYY-MM-DD> <username>
```

other tools:

```
# chage -E <YYYY-MM-DD> <username>
```

```
[root@client ~]# 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

[root@client ~]#
```

7. to check ID details of a user:

```
# id <username>
```

8. Adding a primary group to a user:

```
# useradd -g <group-name> <username>
```

the above command avoids creating a default group while user creation.

for existing users:

```
# usermod -g <group-name> <username>
```

9. Adding a secondary group to a user:

```
# useradd -G <group-name> <username>
```

if you want to add multiple groups as secondary use -a to append :

```
# useradd -aG <group-name1>,<group-name2>,<group-name3> <username>
```

for existing users:

```
# usermod -aG <group-name1>,<group-name2>,<group-name3> <username>
```

```
# usermod -g <groupname> <username> ; # this command will overwrite the
default group
```

10. Renaming a User:

```
# usermod --login <new-username> <old-username>
```

to change user's name along with home dir

```
# usermod --login <new-username> --move-home --home (new-homedir-path) <old-username>
```

```
# pkill -u <old-username>
```

```
# pkill -9 -u <old-username>
```

#### 11. Changing id for users & groups

```
# useradd -u <uid> -g <gid> <username>
```

```
# useradd -u <uid> <username>
```

#### 12. Ignore creating home dir

```
# useradd -M <username>
```

#### 13. Adding a group

```
# groupadd <groupname>
```

#### 14. Renaming a group

```
# groupmod -n <new-groupname> <old-groupname>
```

#### 15. Delete a group

```
# groupdel <groupname>
```

#### 16. Delete a User

```
# userdel -r <username>
```

#### 17. Removing a user from group

```
# gpasswd -d <username> <groupname>
```

while creating a user 6 different events created together

1. /var/spool/mail/username → mail

2. /etc/shadow → user passwd

3. /etc/passwd → user info

4. /etc/skel/ → creates standard files for users (default)

5. /etc/group → group info

6. /home/username → (home dir)

if you delete a user without '-r' option mail and home dir will not be deleted

#### 18. display primary & secondary group info

```
# groups <username>
```

help references:

```
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

[root@client ~]# _
```

```
[root@client ~]# 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

```
[root@client ~]# _
```

```
[root@client ~]# 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

```
[root@client ~]# _
```

```
[root@client ~]# 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
  -R, --root CHROOT_DIR      directory to chroot into
  -P, --prefix PREFIX_DIR    directory prefix

[root@client ~]#
```

```
[root@client ~]# 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
  -R, --root CHROOT_DIR      directory to chroot into
  -P, --prefix PREFIX_DIR    prefix directory where are located the /etc/* files

[root@client ~]#
```