Red Hat System Administration I

UNIT 5

Managing Local Linux Users and Groups

Objectives

- Explain the role of users and groups on a Linux system and how they are understood by the computer.
- Run commands as the superuser to administer a Linux system.
- Create, modify, lock, and delete locally defined user accounts.
- Create, modify, and delete locally defined group accounts.
- Lock accounts manually or by setting a password-aging policy in the shadow password file

What is a user?

- Every process (running program) on the system runs as a particular user. Every file is owned by a particular user. Access to files and directories are restricted by user. The user associated with a running process determines the files and directories accessible to that process
- The id command is used to show information about the current logged-in user. Basic information about another user can also be requested by passing in the username of that user as the first argument to the id command.
- every file have user and group
- every processes have user and group

About users messages

- /etc/passwd
  - username:password:UID:GID:GECOS:/home/dir:shell

UID
is a user ID, a number that identifies the user at the most fundamental level.
GID
is the user's primary group ID number. Groups will be discussed in a moment.
GECOS
field is arbitrary text, which usually includes the user's real name.
/home/dir is the location of the user's personal data and configuration files.
SHELL
is a program that runs as the user logs in. For a regular user, this is normally the program that provides the user's command line prompt.

What is a group?

- Every user has exactly one primary group. For local users, the primary group is defined by the GID number of the group listed in the third
- The users in the same group have the same permission

About group message

- /etc/group
  - groupname:password:GID:list of users in this group

Switching users with su

- **su [-] <username>**

```
[student@desktopX ~]$su -
Password:redhat
[root@desktopX ~]#
```

How to create users and groups

- useradd + ops +username
  - options
    - -u userid
    - -g initial group
    - -G Additional group
    - -d home directory
    - -c gecos
    - -s shell

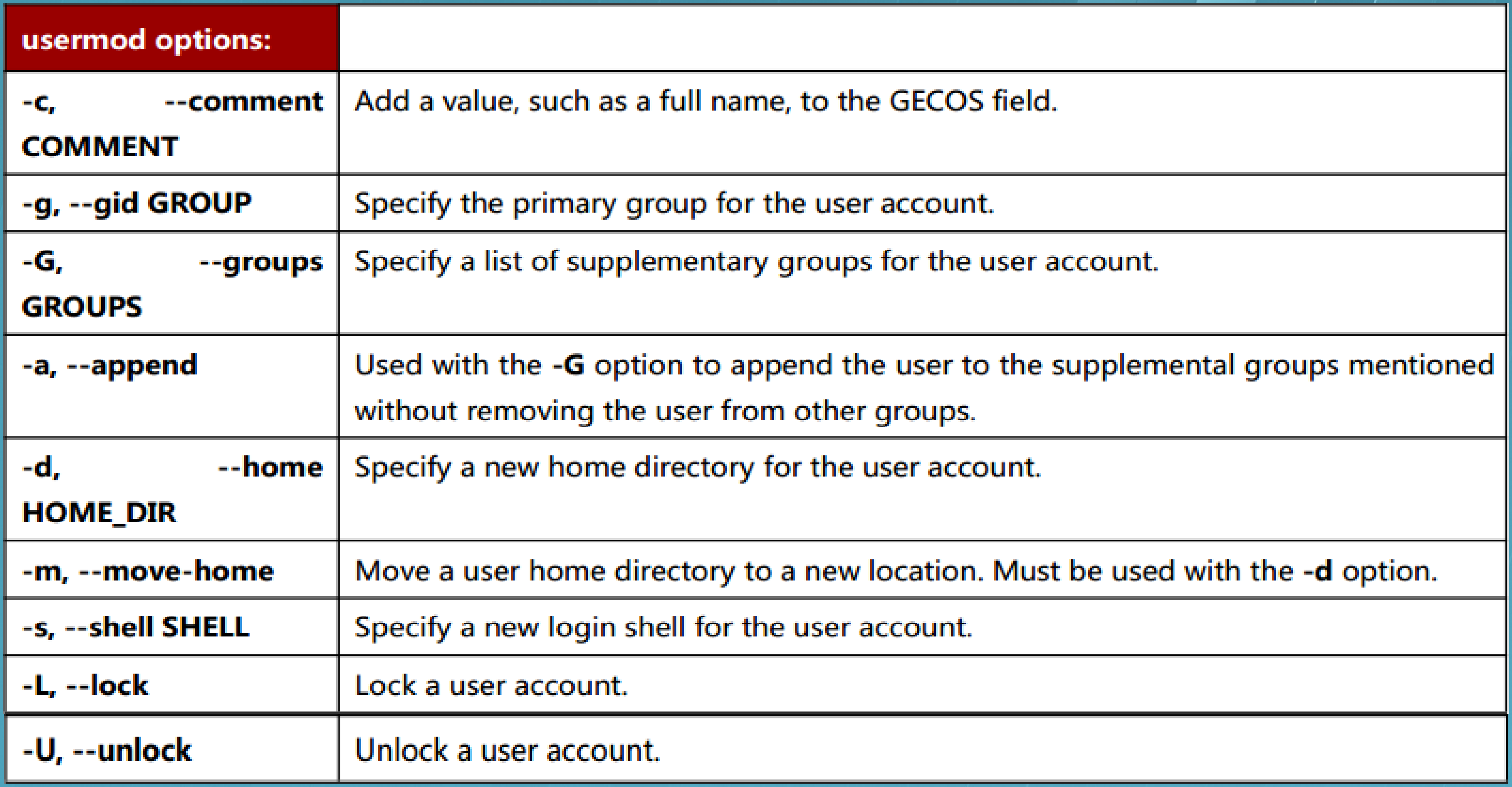
- groupadd +ops +groupname
  - options
    - -g

Managing local users

usermod command

usermod + options + username

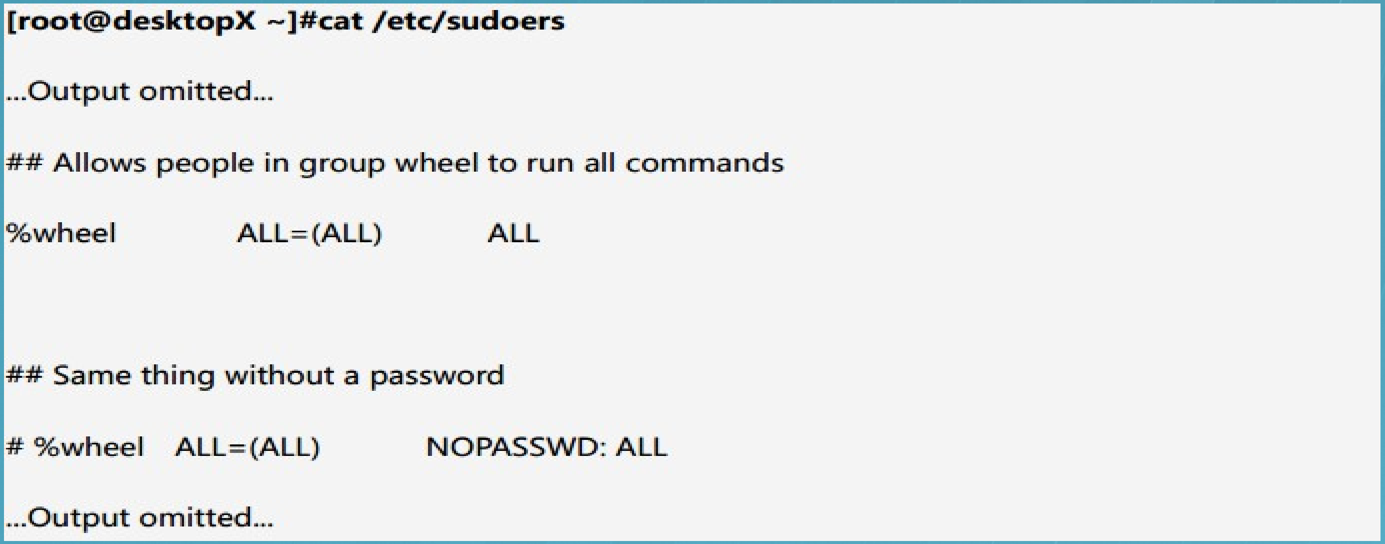
many options mean:



usermod options:	
-c, --comment COMMENT	Add a value, such as a full name, to the GECOS field.
-g, --gid GROUP	Specify the primary group for the user account.
-G, --groups GROUPS	Specify a list of supplementary groups for the user account.
-a, --append	Used with the **-G** option to append the user to the supplemental groups mentioned without removing the user from other groups.
-d, --home HOME_DIR	Specify a new home directory for the user account.
-m, --move-home	Move a user home directory to a new location. Must be used with the **-d** option.
-s, --shell SHELL	Specify a new login shell for the user account.
-L, --lock	Lock a user account.
-U, --unlock	Unlock a user account.

Running commands as root with sudo

- The sudo command allows a user to be permitted to run a command as root
- visudo



```
[root@desktopX ~]#cat /etc/sudoers

...Output omitted...

## Allows people in group wheel to run all commands

%wheel          ALL=(ALL)          ALL



## Same thing without a password

# %wheel    ALL=(ALL)          NOPASSWD: ALL

...Output omitted...
```

How to use sudo

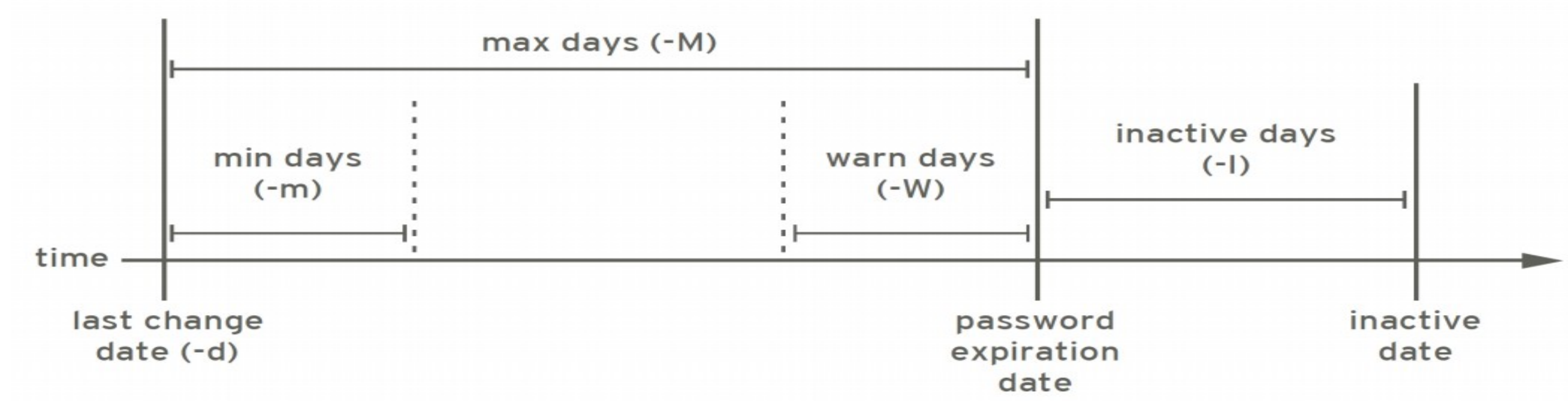
- visudo to edit /etc/sudo
- use sudo call authorized command

```
[student@serverX ~]$ sudo usermod -L username
[sudo] password for student:password
```

.Managing User Passwords

- The users authentication message is in the /etc/shadow
- /etc/shadow

  name: password: lastchange: minage: maxage: warning: inactive: expire: blank
- passwd can motify user's passwd
- chage can motify user's data message



Lab

<lab1>
Ensure that newly created users have passwords which must be changed every 30 days.
<lab2>
Create a new group named consultants with a GID of 40000.
<lab3>
Create three new users: sspade, bboop, and dtracy, with a password of default and add them to the supplementary group consultants. The primary group should remain as the user private group.
<lab4>
Determine the date 90 days in the future and set each of the three new user accounts to expire on that date.
<lab5>
Change the password policy for the bboop account to require a new password every 15 days.
<lab6>
Additionally, force all users to change their password on first login.
When you finish, run the lab localusers grade evaluation script to confirm you have done

That's all