Linux Module 4 (Revision Series)

Sem 4 BCA/B.Sc. Computer Science MGU

Common administrative tasks

- System automation: includes user account maintenance, periodic data backups, free disk space checking etc.
- Documentation: A good system admin should document changes, procedures & policies
- Communication: Good system administrator should be a good communicator. All users should aware of what is doing, going to do, what he has done.

- Management of File systems, Software installations, setting up security features, network configurations, management of user accounts.

Types of users in Linux

- Root User: also known as super user & would have complete control of the system. Able to run any commands without any restrictions. This user is assumed as system admin. Default symbol of prompt is: #
- Regular User: Have common privileges to perform standard tasks such as running word processors, database & web browser. Able to store files in their home directory. Default prompt symbol is $.
- System User: These are system accounts those are required for the operation of system specific components eg: mail accounts.

Ways to ask admin privileges

- su command : used to open shell as root user. Once it’s open admin can run any commands without any restrictions.
- Sudo command: gives root privileges to regular user when sudo command is executed.after running one command using sudo. The use will act as a regular user again.
- GUI windows : While using system in GUI mode, if there is a need of root privilege, you are prompted for the root password.

Ways to ask admin privileges

- su command : used to open shell as root user. Once it’s open admin can run any commands without any restrictions.
- Sudo command: gives root privileges to regular user when sudo command is executed.after running one command using sudo. The use will act as a regular user again.
- GUI windows : While using system in GUI mode, if there is a need of root privilege, you are prompted for the root password.

Managing user accounts

Adding users

- Syntax: useradd options username
- After adding user system admin must set initial password for the user using passwd command
- Syntax: passwd options username
- Options used with useradd command:
  - -c “comment” – provides description for new user account.
  - -D – rather than creating a new account, save the supplied information as new default settings for any new account created.
  - -e expiry_date – assigns the expiry date for an account. Date format is YYYY-MM-DD.
- Options used with passwd command:
  - -l Lock the password of specified user
  - -u Unlock the user password

Managing user accounts

Modifying users

- Syntax: usermod options username
- Useful in scenario where we need to change attributes of an existing user such as login name, password, expiry etc.
- Options used with usermod command:
  - -c “comment” – provides description for new user account.
  - -D – rather than creating a new account, save the supplied information as new default settings for any new account created.
  - -e expiry_date – assigns the expiry date for an account. Date format is YYYY-MM-DD.

Managing user accounts

Deleting users

- Syntax: userdel options username
- Options used with userdel command:
  - -f : forces the removal of user even if the user is till logged in. Also forces to remove user's home directory or her mail spool.

Temporary disabling of user accounts

1. Editing /etc/shadow/ file

    - You can disable an account by adding a * or ! At the beginning of the second field in /etc/shadow
    - To unlock account just remove the * or ! Added.
    - Second field is the encrypted password
    - Eg: anto: *$ghujgh#nm$NJKJN
2. Using passwd command.
    - Use –l to lock the account (Adds ! In front of the user password)
    - User –u to unlock the account (You can also remove the ! From /etc/shadow/)

Managing groups

- Groups are useful in case if we want share a set of files with multiple users.
- By default every user is assigned to primary group.
- Root user can assign users to any group

Managing groups

Creating group

- Syntax: groupadd option groupname
- When a group is added to system, the system places the group name in the /etc/group file and gives it a group ID number.
- Options:
  - -p : to set an encrypted password for the group
  - -r : create a system group.
  - -g : used to provide a group id to new group. Should be unique & non-negative.

Managing group

Modifying group

- Syntax: groupmod options groupname
- Useful in scenario where we need to change an existing group on Linux system.
- Options used with groupmod command:
  - -n : name of the group will change into newname
  - -g : to change group id
  - -p: to change password of group

Managing group

Deleting group

- Syntax: groupdel groupname
- Deletes all entries that refer to the group, modifies the system account files, & handled by root user

Changing Permissions & ownerships

For every file & directory on Linux is assigned 3 types of owner

- User: owner of the file, the person who created the file.
- Group: A user group can contain multiple users
- Other: any other users who have access to the files.

3 types of permissions for user, group & other

- Read: Permission which allows user to open and read the contents of the file
- Write: Permission to modify the contents of the file
- Execute: Allows you to execute the file.

Changing Permissions & ownerships

The 9 bits assigned to each file for permissions.

File permission for regular file appears as –rwxrwxrwx.

r : read, x : execute, w: write, - : no permission granted.

To change permission of the file, you need to use the chmod command.

Syntax: chmod permission filename

Supports two modes for modifying permissions:

- Symbolic Mode
- Absolute Mode

Changing Permissions & ownerships

Symbolic mode:

Uses letters & some operators to set permission. When using symbolic mode the chmod command has following syntax:

chmod [u g o a][+ - =] permission filename

u : specifies the user who owns the file

g: specified the group which owns the file

o: specifies other users who are not the members of the group or owner of the file

A: specifies all users available on the system

Changing Permissions

Symbolic mode:

- + : add a permission to file
- - : removes the selected permission from the file
- = : overwrite existing permission of file and add new one.
- Eg: chmod a+x sample.sh
- Eg: chmod go-x sample.sh
- Eg: chmod g=u sample.sh

Changing Permissions

Absolute mode:

Uses numerical values [0 - 7] to set permission.

syntax:

chmod numerical_value filename

Eg: chmod 777 file.txt

-R : to apply changes recursively to multiple files & directory

Number	Permission Type	Symbol
0	No Permission	- - -
1	Execute	- - x
2	Write	- w -
3	Execute + Write	- w x
4	Read	r - -
5	Read + Execute	r - x
6	Read + Write	r w -
7	Read + Write + Execute	r w r

Managing ownerships

To change ownership of user or group for file or directory. The chown command is used.

Syntax: chown options user :group filename

Options:

-f: don’t print error msg about files whose ownership can’t be changed

-R: make changes recursively

-c: reports when a file ownership is changed.

Getting system information - uname

Prints information about current system.

Syntax: uname options

By default without any options, prints kernel name.

Options:

-a: prints all information in order: kernel name, network mode, hostname, kernel release date, kernel version, machine hardware name, hardware platform, OS

-v: prints kernel version

Getting system information - hostname

Displays or set hostname or domain name.

Used to identify system in a network

Syntax: hostname options

To set new hostname: hostname new_name

Options:

-a : displays the alias name of the host.

-d : prints the domain name

-I : display IP address

Installing & removing packages with RPM command

An RPM package is contains all the files that are required to install a software such as word,file server etc.

RPM – Red Hat Package Manager: default package manager to install & remove applications.

Ends with extension: .rpm

Allows admin to install, remove, update, query & manage software packages.

Installing & removing packages with RPM command

5 Basic modes:

1. Install: It is used to install any RPM package.
2. Remove: Used to remove any RPM package
3. Upgrade: Used to update any RPM package
4. Verify: Used to verify an RPM package
5. Query: Used to query an RPM package

Installing & removing packages with RPM command

Syntax: rpm options packagename

Options:

-i : Install the package

-U : update package

-e : remove package

-q: query