Linux Users & Groups

Users & groups

- User:
  - Users are either people or accounts which have permission to login to the system
  - Each user will have unique UID Number
  - Example : user1, user2 etc
  - Root user will have all the administrative rights with UIS of “0”
- Group:
  - Some or all users can be part of Groups
  - Groups can be made for different purposes
  - Each group will have unique GID Number
  - Example: HRD, Business, Purchase

Linux Account

- Username
  - Account name created to login into the system
- Password
  - By default all users are created with home directories in /home and users will be owners of home directory.
  - Path of home directory can be changed also
  - Root account home directory is /root

Linux Accounts

- No two users will have same UID
- Login: login name give to users
- Home dir; default path once the user logs in to the system.
- shell: default shell environment for users logged in
- Fullname: Full name of user
- UID: id of user created
- GID: group Id of the user

  example: id user1

Authentication Methods

- Password file in local system
- NIS – Network Information service
- LDAP – lightweight Directory Access Protocol
- Windows domains: local and domain based.

Linux local authentication

- /etc/passwd: Holds users account information
- /etc/shadow: holds user passwd in encrypted format
- /etc/group: holds users group information

/etc/passwd file

- There are 7 fields separated by “:”
- Username: Password:UID:GID:FullName:Home dir:Default shell
- Username:username is the login name supplied at the time of logging into the system
- Password: secret information given by users for authentication purpose. The encrypted format of password is stored in /etc/shadow file.
- UID: User Identification Number and its unique to each user
- GID: Group ID of user. Usually username and groupname will be same.
  - User can be part of multiple groups

/etc/passwd file

- FullName: Fullname and department, company name can be given here for reference purposes. This filed also called as “comments field”
- Home dir: This is the path for user home directory once user logs in.
- Default shell: This is the shell environment user gets once user logs in.

/etc/shadow file

- This file has 8 fields seprated by “:”
- Username:Password:Last modified:min days:Max days: Days warn:disabled days:expire
- Username: This is the username as given in /etc/passwd file
- Password: secret information of user in encrypted form
- Last modified: This filed displays number of days since the password last changed
- Min days: This field displays the minimum number of days required before a password can be changed. In this example, it is set to 0 days
- Max days:This field displays the maximum number of days before a password must be changed. In this example, it is set to 99999 days. Effectively, this means a passwordisn’trequired

/etc/shadow file

- Days warn: This field displays the number of days prior to password expiration that the user will be warned of the pending expiration. In this case, it's set to 7 days
- Disabled days: DaysThis field displays the number of days to wait after a password has expired to disable the account.
- Expire:This field displays the number of days since January 1, 1970 after which the account will be disabled. In this example, it is set to a null value, indicating the account never expires.

Managing User Accounts

- Using useradd
- Using passwd
- Using usermod
- Using userdel

Useradd – adding user

- The syntax for adding users to system
  - useradd [OPTIONS]
  - -D defaults
  - -c or –comment
  - -d or –home-dir
  - -G –groups
  - -h –help
  - -u –uid
  - -s –shell etc

passwd – set/change password

- Users can set or change password using “passwd” command
  - passwd
- Root user can change password of any user
  - Passwd <username>
- Options:
    - -l lock the account
    - -u unlock the account
    - -d removes users passwd
    - -n, -x, -w, -I sets options for password field.

Usermod – user modifications

- Usermod – user details can be modified with usermod command
  - usermod [OPTIONS]
  - OPTIONS:
    - -c edit users Fullname
    - -g sets users default group
    - -G sets additional group
    - -p sets password
    - -U unlocks user account if it is locked by –L option

Userdel – delete user

- Userdel – the command to delete the user account
  - Userdel <username>

Linux Groups

- Group file is present in /etc/group
- /etc/group file is composed of
  - Group:password:GID:users
    - Group: Group name
    - Password: password can be set for group
    - GID: group identification number
    - Users; members of the group

Managing Groups

- Groupadd
- Groupmod
- groupdel

Groupadd – adding the group

- Groupadd <groupname>
  - -g specify a GID
  - -p specify password

  Example: groupadd dbda

Groupmod – Modify the group

- Groupmod [OPTIONS] <groupname>
  - -g chane the GID
  - -p change the password

  Example: groupadd –g 213 dbda

Groupdel – Delete the group

- Groupdel <groupname>

  Example: groupadd dbda

Managing ownership

- You can specify a different user and/or group as the owner of a given file or directory. To change the user who owns a file, you must be logged in as root. To change the group that owns a file, you must be logged in as root or as the user who currently owns the file.
  - Using **chown**
  - Using chgrp

Chown command

- The chown utility can be used to change the **user**or **group**that owns a file or **directory**
  - Chown user:group <dir>
  - Example: chown sreek:sreek dbda

  You can use the –R option with chown to change ownership on many files at once recursively.

Chgrp command

- You can also use **chgrp** to change the group that owns a file or directory
- Group can be changed with chown command also
  - Chgrp <file> <dir>
  - Example: chgrp dbda /tmp/file1