**USER AND GROUP MANAGEMENT**

**A user is a person who utilize a computer or network service. Linux is set to be secure because one user cannot access file of other user without its permission .**

**There are five types of user**

**1)Super User (root user)**

**2)System User**

**3)Standard User(Local user)**

**4)Network User**

**5)Sudo User**

**(UID :- Unique / User Identification Number )**

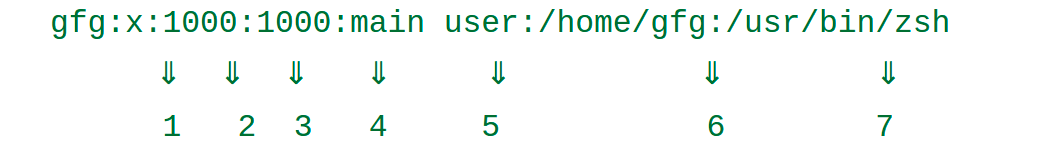
**(GID :- Group Identification Number)**

1. **Super User (UID - 0) :- Super user are those user who has all privileges of Linux system .On all Linux system by default there is the user “ root “ also known as the “ super user “.**

**This account is used for managing linux root for instance , can create other user account on the system. For performing some task root privileges are required. Some example are installing software , managing user and creating partition on disk devices.**

1. **System User (UID – 1 to 999) :-System accounts are used by the services in Linux system . these account or user generally created when services are installed in system. It runs processes and services. (There are no login shell)**
2. **Standard User (Local User) (UID – 1000 to 60,000+ ) :- Local user account or standard user accounts are for the people who had work on the system and who need limited access to the resources on the system. These user accounts typically have a password that is used for authenticating the user to the system.**
3. **Network User :- User who has access to the network resourses.**
4. **Sudo user :- User having special permission.**

* **ADDING NEW USER**
* **useradd <user name>**
* **adduser <user name>**
* **Adding new local user means creating user account.**
* **User can be added by root user or using root user privileges.**
* **Whenever new user has been added some files get affected.**
* **These files hold user account related information.**
* **Also whenever new user is created by default its home directory and mail account also has been generated.**
* **New users are created using some skeleton files located in /etc/skel directory. These files are hidden and copied into home directory of newly created user.**
* **Files Affected By Newly Added User**
* **/etc/passwd :- It stores user profile related information The /etc/passwd file is the most important file in Linux operating system.** 
  + **This file stores essential information about the users on the system.**
  + **This file is owned by the root user and to edit this file we must have root privileges.**
  + **But try to avoid edit this file. Now let’s see actually how this file look**
* **This file contains one entry per line. That means it stores one user’s information on one line.**
* **The user information contains seven fields and each field is separated by the colon ( : )symbol. Each entry in the /etc/passwd file looks like this:**



**Now let’s understand each field one by one:**

**Eg. Tail -3 /etc/passwd**

**The /etc/passwd file is a colon-separated file that contains the following information:**

* **User name.**
* **Encrypted password.**
* **User ID number (UID)**
* **User's group ID number (GID)**
* **Full name of the user (GECOS)**
* **User home directory.**
* **Login shell.**

1. **Username: This field stores the usernames which are used while login into the system. The length of this field is between 1 and 32 characters.**
2. **Password: This field store the password of the user. The x character indicates the password is stored in /etc/shadow file in the encrypted format. We can use the passwd command to update this field.**
3. **User ID(UID): User identifier is the number assigned to each user by the operating system to refer the users. The 0 UID is reserved for the root user. And 1-99 UID are reserved for other predefined accounts. And 100-999 are reserved by the system for administrative and system accounts/groups.**
4. **Group ID(GID): Group identifier is the number indicating the primary group of users. Most of the time it is the same as the UID.**
5. **User ID Info (GECOS): This is a comment field. This field contains information like the user phone number, address, or full name of the user. This field is used by the finger command to get information about the user.**
6. **Home directory: This field contains the absolute path of the user’s home directory. By default, the users are created under the /home directory. If this file is empty, then the home directory of that user will be /**
7. **Login shell: This field store the absolute path of the user shell. This shell is started when the user is log in to the system.**

**cat /etc/passwd**

* 1. **/etc/shadow :- It stores user password policies.**

**Eg. Tail -1 etc/shadow**

**Linuxb18 : !! : 19300 : 0 : 99999 : 7 : : :**

**1 2 3 4 5 6 7 8 9**

**It contains 9 fields and each field is separated by colon.**

**##shadow file ===>/etc/shadow (store password ,password policy)**

**9 fields divide with help of colon:-**

**1)username (unique name , no space bwt username) :-This is unique name for the user .User names are important to match a user to his password on linux their can be no spaces in the username**

**2) encrypted password (password use RSA algorithm):-The field contains all that is needed to store the password in secure way.**

**3)last password change date from 1st jan 1970 :- Many things on linux refer to this date which on linux is considered the beginning days.**

**4)minimum password change (by default it is 0) :- That means user cannot change password ,before the mentioned days , after immediately changing the password .**

**5)maximum password change days (by default it is 99999) :- User must have to change password after mentioned days .**

**6)warning days (by default 7) :- this field is to warn user when a forced password change is upcoming by default it is set to 7 days .**

**7)inactive days (0) :- use this field to enforce a password change . After password expiry user can no longer login.**

**8)expire days :- An admin can set this field to disable an account. This is typically a better approach than removing an account , as well all associated properties and files of the account will be kept but it can be used no longer to authenticate on your server.**

**9)future purpose :- this is reserved field for future use.s**

1. **/etc/group :- It stores group information.**
2. **/etc/gshadow :- Stores group password and members list.**
3. **Home directory and mail account of new user**

**ls / home**

**ls /var/spool/mail**

1. **Skeleton files :-**
2. **.bash\_logout :- if this file is missing user will be unable to logout from the system.**

1. **.bash\_profile :- If these files are missing home directory will not be assign to new user**
2. **.bashrc :- if these files are missing user will unable to login to the system.**

**Ls -a /etc/skel :- to show skeleton files**

**Ls -a /home/linuxb18 :- skeleton files that copied into home directory.**

* **Password Management**
* **passwd <username> :- Password is a secrete phrase that can be use to login to the system.**
* **“ passwd ” command is used to assign or change the password of any user .**
* **Whenever password is assign to user it will, get stored in /etc/shadow file in encrypted format.**
* **Only root user can change password of any user, but local user can change their own password**
* **Password should follows some rule such as follows:**
* **Password must be 8 characters long**
* **It should not contain username**
* **It cannot accept old password**
* **Any dictionary name is not allowed**
* **Password should not be too simplistic**

## **Difference Between “useradd” and “adduser” Linux Commands**

**The main objective of the “useradd” and the “adduser” is the same for adding a new user to the Linux system. However, they are different at the execution and implementation levels.**

**This section comprises these differences in the form of the table:**

| **useradd Command** | **adduser Command** |
| --- | --- |
| **It is a low-level native binary compiled.** | **It is the high-level “Perl” script that utilizes the “useradd” in the background.** |
| **It does not provide an interactive prompt.** | **It is more interactive and user-friendly.** |
| **It is a soft link to the “adduser”.** | **The “adduser” command is not present in most distributions.** |
| **It creates a “/home” directory with its “-m” option for the new user.** | **It creates the “/home” directory by default.** |
| **Adds the new user in multiple groups at the same time.** | **It needs to add a new user into multiple groups separately.** |
| **It does not ask for extra information for the user at the time of creation.** | **Asks for a series of additional information such as “Full-name”, “Romm Number”, “Work Home” etc.** |

**View And Change Password Policy :-**

* **chage(change age) :- command is use to view or modify password policy.**
* **chage <options> <parameter> < username>**
* **-l :-list /view password policy**
* **-m :- min days between password change.**
* **-M :- maximum days between password change.**
* **-W :- number of days of warning.**
* **-I :- number of inactivation days**
* **-E :- expiry date of user account.**
* **-d :- force to change password.**
* **Adding User with Customized Setting.**
* **useradd <option> <parameters> <username>**
* **-u :- user ID**
* **-g :- primary group**
* **-c :- comment**
* **-d :- Home directory**
* **-S :- login shell**
* **-G :- secondary group**
* **-r :- system user**
* **-e :- account expiry date**
* **-o :- non unique, allow to create user with duplicate UID.**
* **-P :-Password**
* **Modify User with Customized Setting**
* **Usermod :- command is used to modify existing users setting.**
* **usermod <option> <parameters> <username>**
* **-u :- user id**
* **-g :- primary group.**
* **-c :- comment.**
* **-d :- home directory**
* **-S :- login shell**
* **-G :- secondary group**
* **-l :- login name**
* **-L :- lock user password**
* **-U :- unlock user password**
* **-m :- modify directories**
* **-a :- append**
* **Remove User From System.**
* **userdel :- command is use to remove or delete user account from system.**
* **userdel <username>**
* **-f :- forcefully remove user account**
* **-r :- users home directory will be removed along with the home directory itself and the user.**

**GROUP ADMINISTRATION / MANAGEMENT**

* **Linux user can be member of two different kinds of group .**
* **First is the Primary group .**
* **Every user must be member of primary group and there is only one primary group.**
* **When creating files the primary group becomes group owner of these files.**
* **User can also access all files their primary group has access to. The user’s primary group membership is defined in /etc/passwd.**
* **The group itself stored in the /etc/group configuration file.**
* **Besides the mandatory primary group ,users can be member of one or more secondary group as well.**
* **Secondary groups are important to get access to files.**
* **groupadd :-command is used to add secondary or supplementary group in system. Group information are stored in /etc/group.\**
* **syntax :- groupadd <groupname>**
* **grpunconv :- hides gshadow file .**
* **grpconv :- unhides gshadow file.**
* **In group to add member another command is**
* **usermod -aG <groupname> <username>**
* **gpasswd -M <user1,user2,user3> <group name>**

1. **/etc/group :- It stores group information.This file contains 4 fields.**
   1. **Group name :- As suggested by name of the field this contain the name of the group.**
   2. **Redirected group password :- This feature is hardly used anymore. A group password can be used by the users that want to join the group. On a temporary basis. So that access to files the group has access to allow.**
   3. **GID (Group ID) :- A unique numeric group identification number .**
   4. **List of member :- Here you find the names of users that are members of this group as a secondary group .**

**( Note :- That it does not show user that are member of their group as their primary group )**

1. **/etc/gshadow :- This file is used to store password of group . It also store admin and member list of group.**

**It contains 4 fields.**

* + 1. **Group name**
    2. **Encrypted Password**
    3. **Admin of Group**
    4. **Member list**
* **Adding group with customized setting**
* **Groupadd <options> <parameter> <group name>**
* **-g :-for group ID**
* **-O :- non uniq ID**
* **-f :- forcefully**
* **Modify existing group with customize setting.**
* **groupmod <options> <parameter> <group name>**
* **-g :- group ID**
* **-n :- group name**
* **-O :- non uniq ID**

**Command**

1. **gpasswd :- This command is used to give password to group. It also can be used to add members and members and assigned admin to the group.**
2. **gpasswd <group name> :- set group password**
3. **gpasswd -r <group name > :- remove group password.**

**Options :- -a :- add members in group**

**-M :- set list of multiple members of group**

**-A :- assign user as group admin.**

**-d :- remove user from group.**

**-A ”” :- remove admin.**

* **groupdel :- deletes group.**
* **-f :- forcefully.**