Contents

[**User and Group Management** 3](#_Toc485032611)

[**Types of Users in Linux** 3](#_Toc485032612)

[**User Creation** 3](#_Toc485032613)

[ Create a user 3](#_Toc485032614)

[ Create user with specific UID 3](#_Toc485032615)

[ Create a user with specific GID 3](#_Toc485032616)

[ Grant root access to new user 3](#_Toc485032617)

[ Grant root access to existing user, 3](#_Toc485032618)

[ Create a user with a different home directory 3](#_Toc485032619)

[ Create a user with a different home directory with -m option 4](#_Toc485032620)

[ Create a user without home directory 4](#_Toc485032621)

[ Create a user with comment 4](#_Toc485032622)

[ Create a user with password expiry date 4](#_Toc485032623)

[ Create a user with account expiry date 4](#_Toc485032624)

[ Add user in other groups (secondary groups) 4](#_Toc485032625)

[ Instead of having same name group as primary group, add other group as primary group 4](#_Toc485032626)

[ Check username, groupname with UID, GID 5](#_Toc485032627)

[ Create a user with specific login shell 5](#_Toc485032628)

[ Create a user with specific skel directory 5](#_Toc485032629)

[ Set/change user account password 5](#_Toc485032630)

[ To reset the user account password when user forgets password 5](#_Toc485032631)

[ To delete the user 5](#_Toc485032632)

[ **Notes:** 5](#_Toc485032633)

[**Relevant files for useradd command** 6](#_Toc485032634)

[**File: /etc/passwd: User account information** 6](#_Toc485032635)

[**File: /etc/passwd: Secure user account information** 7](#_Toc485032636)

[**File: /etc/group: Group information** 7](#_Toc485032637)

[**General Commands regarding user creation** 8](#_Toc485032638)

[ View account information using getent 8](#_Toc485032639)

[ Command: id -To search user/group by its UID/GID 8](#_Toc485032640)

[ To list out total users 8](#_Toc485032641)

[ To count total number of users 8](#_Toc485032642)

[ To get username by its UID 8](#_Toc485032643)

[**Lock/Unlock User Account:** 8](#_Toc485032644)

[**Lock/Disable user Account**: 8](#_Toc485032645)

[ Method-1 (using passwd) 8](#_Toc485032646)

[ Method-2 (using usermod) 9](#_Toc485032647)

[**Unlock/Enable user Account:** 9](#_Toc485032648)

[ Method-1 (using passwd) 9](#_Toc485032649)

[ Method-2 (using usermod) 9](#_Toc485032650)

[**To check the status of lock/unlock user accounts** 9](#_Toc485032651)

[**Chage Command** 10](#_Toc485032652)

[ To see User password expiry information 10](#_Toc485032653)

[ To extend user account expiry time 10](#_Toc485032654)

[ To force the user account to be locked after number of inactive days 10](#_Toc485032655)

[ **To force the user to change the password at first login** 11](#_Toc485032656)

[ **Disable password aging for an user account** 11](#_Toc485032657)

[**Group Creation** 11](#_Toc485032658)

[ Create a group 11](#_Toc485032659)

[ Create a group with specific GID 11](#_Toc485032660)

[ To delete a group 11](#_Toc485032661)

[**Usermod Command:** 11](#_Toc485032662)

[**Groupmod Command:** 11](#_Toc485032663)

# **User and Group Management**

## **Types of Users in Linux**

* There are 3 types of users in Linux,

|  |  |
| --- | --- |
| **User/Type of account** | **UID** |
| Root User/ Super User | 0 |
| System User | 1 to 499 |
| Normal User | 500 onwards |

## **User Creation**

* Create a user,
* Command: useradd <username>
* Example: useradd vv1
* Create user with specific UID,
* Command: useradd -u <UID> <username>
* Example: useradd -u 525 vv2: It will create user vv2 with UID of 525.
* It is useful in DC-DR scenario.
* Create a user with specific GID,
* Command: useradd -g <GID> <username>
* Example: useradd -g 526 vv2: It will create user vv2 with GID of 526.
* Grant root access to new user,
* Command: useradd -o -u 0 -g 0 <username>
* You will not be able to delete this created user.
* To delete created user, UID of the user must be changed in /etc/passwd.
* Grant root access to existing user,
* UID and GID of that user must be changed to 0 from /etc/passwd file.
* Create a user with a different home directory,
* Command: useradd -d <directory> <username>
* Example: useradd -d /home/vaibhav v5: The user v5 is created with home directory of /home/vaibhav
* Here, the directory should not exist otherwise default settings will not be copied from /etc/skel.
* Create a user with a different home directory with -m option,
* Command: useradd -d <directory> -m <username>
* Here, -m option creates directory if it doesn’t exist.
* Create a user without home directory,
* Command: useradd -M <username>
* Example: useradd -M vv20
* It will create user vv20 without its home directory. Although, /home/vv20 home directory will be appeared in /etc/passwd file. But the directory will not be accessible as it doesn’t exist.
* Create a user with comment,
* Command: useradd -c “comment” <username>
* Example: useradd -c “test user” vv3
* Create a user with password expiry date,
* Command: useradd -f <number of days> <username>
* It means that password will be expired after mentioned days since the user account is created.
* Create a user with account expiry date,
* Command: useradd -e YYYY-MM-DD <username>
* Example: useradd -e 2017-06-06 vv4
* It is useful when the user is granted access for limited time.
* The user account will be disabled on expiry date.
* Add user in other groups (secondary groups),
* Command: useradd -G <groupname> <username>
* Example: useradd -g v4 v5
* Example: useradd -g v4,v5,v6,v7 vv10
* User vv10 is added to groups v4, v5, v6 and v7.
* The group v4, v5, v6, v7 must exist before creating the user.
* Instead of having same name group as primary group, add other group as primary group,
* Command: useradd -g <groupname> <username>
* Example: useradd -g vbhv v5
* It will set primary group as vbhv for the user v5.
* The group vbhv must exist before creating the user.
* Check username, groupname with UID, GID,
* Command: id <username>
* Create a user with specific login shell,
* Command: useradd -s <shell> <username>
* Example: useradd -s /bin/bash v1
* Create a user with specific skel directory,
* Command: useradd -k <directory> <username>
* Set/change user account password,
* Command: passwd <username>
* To reset the user account password when user forgets password,
* Login as root.
* Command: passwd <username>
* To delete the user,
* Command: userdel <username>

### **Notes:**

* Default directory for the user is /home/<username>
* By default, same name of group is created while creating new user. For an example, while creating new user named test, the same group named test created.
* For creating user with duplicate (non-unique) UID, use -o option.
* For creating system account, use -r option.
* Automatic UID selection in useradd,

UID\_MIN: 500

UID\_MAX: 60000

* Automatic GID selection in useradd,

GID\_MIN: 500

GID\_MAX: 60000

* UID and GID are unique.

## **Relevant files for useradd command**

|  |  |
| --- | --- |
| File | Description |
| /etc/passwd | User account information  username, UID, GID, home directory, shell |
| /etc/shadow | secure user account information  username, password, last change, min ,max, warning, inactive, expire |
| /etc/group | group information  groupname, GID, members of group |
| /etc/default/useradd | default information  default home directory  default expire time  default shell  default directory from which date is fetched  default mail spool setting |
| /etc/skel | directory containing default files  .bash-profile, .bashrc, etc.. |
| /etc/login.defs | System wide settings  UID\_MIN, UID\_MAX, GID\_MIN, GID\_MAX |

## **File: /etc/passwd: User account information**

Format:

Name: Password placeholder: UID: Primary GID: Comment: Home directory: Shell



|  |  |  |
| --- | --- | --- |
| **Field name** | **Description** | **Example** |
| Name | name of user | root |
| Password placeholder | Password is stored in /etc/shadow file, not in the /etc/passwd | x |
| UID | User ID of the user | 0 |
| Primary GID | GID of primary group | 0 |
| Comment | comments | root |
| Home directory | user’s home directory | /root |
| Shell | user’s login shell | /bin/bash |

## **File: /etc/passwd: Secure user account information**

Format:

Name: Password: last change: min: max: warn: inactive: expire: reserved



|  |  |  |
| --- | --- | --- |
| **Field name** | **Description** | **Example** |
| Name | name of user | root |
| Password | password in encrypted form | $6$Za…..14Uw0 |
| Last change | number of days that last time password was changed considered since January 1,1970 | 17218 |
| min | number of days , the user has to wait to change the password again | 0 |
| max | number of days , the user must change the password at least every mentioned days to avoid the account being unlocked | 99999 |
| warn | warning message to change password before mentioned number of days | 7 |
| inactive | if user ignores max password limit, within mentioned days, password can be changed |  |
| expire | Since January 1,1970 account is locked but not deleted |  |
| reserved | reserved for future purpose |  |

## **File: /etc/group: Group information**

Format:

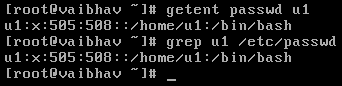
Name: password placeholder: GID: users list



|  |  |  |
| --- | --- | --- |
| **Field name** | **Description** | **Example** |
| Name | Group name | testg |
| Password placeholder | Password is stored in /etc/shadow file, not in the /etc/passwd | x |
| GID | Primary GID of group | 505 |
| users list | members of the group | user1,user2,user3 |

## **General Commands regarding user creation**

* View account information using getent,
* Command: getent passwd <username>
* Command: grep “<username>” /etc/passwd



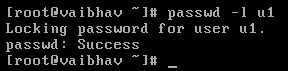
* Command: id -To search user/group by its UID/GID,
* Command: id : It will display user account information of logged in user
* Command: id -u : It will display UID of logged in user
* Command: id -g : It will display GID of logged in user
* Command: id -u <username> : It will display UID of mentioned user
* Command: id -g <username> : It will display primary GID of mentioned user
* Command: id -G <username> : It will display all GID of mentioned user
* To list out total users,
* Command: cut -d: -f1 /etc/passwd
* To count total number of users,
* Command: cut -d: -f1 /etc/passwd | wc -l
* Command: getent passwd | wc -l
* To get username by its UID,
* Command: getent passwd <UID> | cut -d: -f1

## **Lock/Unlock User Account:**

### **Lock/Disable user Account**:

#### Method-1 (using passwd):

* Command: passwd -l <username>
* Example: passwd -l u1



#### Method-2 (using usermod):

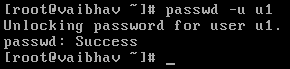
* Command: usermod -L <username>
* Example: usermod -L u1



**Unlock/Enable user Account:**

#### Method-1 (using passwd):

* Command: passwd -u <username>
* Example: passwd -u u1



#### Method-2 (using usermod):

* Command: usermod -U <username>
* Example: usermod -U u1



### **To check the status of lock/unlock user accounts**

* The status can be checked from /etc/shadow file.
* If there is double/single exclamation (!) at the starting of 2nd field then the user account is locked.
* If there is double exclamation (!!) then the user account is locked by passwd command.



* If there is single exclamation (!) then the user account is locked by usermod command.

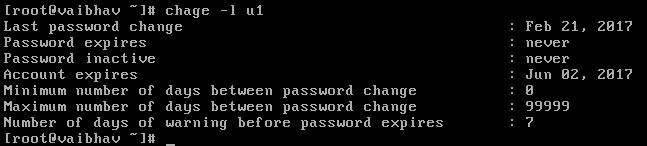


* If user account is locked by passwd command, it must be unlocked by passwd command only to unlock the user account successfully.
* If user account is locked by usermod command, it can be unlocked by passwd command or usermod command.
* So it is always advisable to use passwd command to lock/unlock user account.

**Chage Command:**

|  |  |
| --- | --- |
| **Option** | **Description** |
| -l or --list | show user account aging information |
| -E | user account expiry date |
| -m | minimum days |
| -M | maximum days |
| -W | Warning |
| -i or --inactive | Inactive days |

* Chage : Change age
* It is useful to change user’s password’s aging/expiry information.
* To see User password expiry information,
* Command: chage -l <username>
* Example: chage -l u1



* To extend user account expiry time,
* Command: chage -E <YYYY-MM-DD> <username>
* Example: chage -E 2017-06-03 u1



* To force the user account to be locked after number of inactive days,
* Command: chage -I <number of days> <username>
* Example: chage -I 10 vv5
* It will lock user account vv5 if user doesn’t chage password after 10 days since account expired.
* **To force the user to change the password at first login**,
* Command: chage -d 0 <username>
* Example: chage -d 0 u1
* **Disable password aging for an user account**,
* -m 0: It will set minimum number of days between password changed to 0.
* -M 99999: It will set maximum number of days between password changed to 99999.
* -E -1: It will set account expires to never.
* -I -1: It will set password inactive to never.
* Command: chage -m 0 -M 99999 -E -1 -I(capita i) -1 <username>

**Group Creation**:

* Create a group,
* Command: groupadd <groupname>
* Example: groupadd vv25
* Create a group with specific GID,
* Command: groupadd -g <GID> <groupname>
* To delete a group,
* Command: groupdel <groupname>

## **Usermod Command:**

* Usermod command is used to modify user account.
* All options of useradd command are applicable for usermod command.

## **Groupmod Command:**

* Groupmod command is used to modify group account.
* All options of groupadd command are applicable for groupmod command.