Red Hat Enterprise Linux 9

RHCSA – SA 1 LAB BOOK

Chapter 6 – Managing Local Users and Groups

A] User:

- Entity accessing computer resources.
- Each user is identified by unique identification Number called userid (uid).

Types of User's:

a) **Root User:** This is also called super user and would have complete control of the system.
A super user can run any commands without any restriction.
Prompt: (#).

b) **System User:** Created by software.
Example: if we install ssh application, system will create ssh user and ssh group.
By default User manager does not show system users.

c) **Normal User:** They are create by root user for different purpose.
Prompt: ($).

User UID's:

Users	UID till RHEL 6	UID from RHEL 7
Root	0	0
System user	1-499	1-999
Normal User	500 – 60000	1000-60000

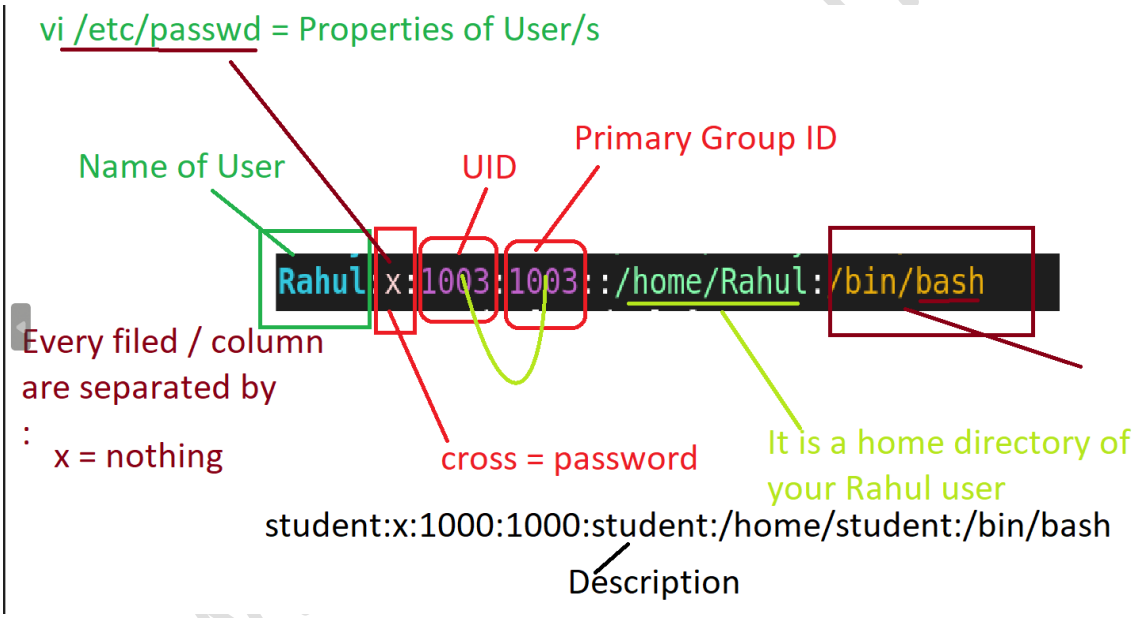
Note:

/etc/passwd: Mapping of username and user id.

These user id ranges are defined in **/etc/login.defs** configuration file.

Properties of user:

1. Name
2. Password
3. UID
4. Primary GID
5. Description (Gecos Field)
6. Home Directory
7. Shell
8.



Note:

/etc/passwd: Above properties are mentioned in this file.

B] Group:

- It is a collection of those users, who has the same privileges on specific resource.
- Each group is identified by unique identification Number called groupid(gid).

Types of Group:

a) **Primary Group:** Auto created group while adding users
They are created for security purpose.
Username and Primary Group name are same.
uid and primary group id are same.

b) **Secondary Group:** They are created for specific purpose.

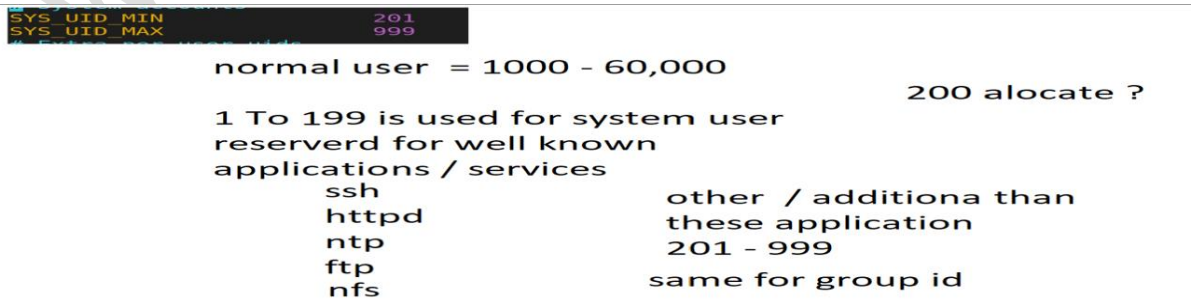
User GID's:

Group Name	GID till RHEL6	GID from RHEL 7
Root group	0	0
System group	1-499	1-999
Normal Group	500-60000	1000-60000

Note:

The Range of uid and gid is specified in **/etc/login.defs.**

/etc/group: it stores mapping of gid and groupname.



Important configuration files for User Administration

1] /etc/login.defs: User related configurations

2] /etc/passwd: User properties

3] /etc/group: Group properties

4] /etc/shadow = It stored the properties of users password.

5] /etc/gshadow = It stores the properties of group password

6] /etc/skel = It is directory that contains environment related files for user accounts.

Note: These files will be copied to user's home directory after adding user account.

All these files are hidden files

C] How to create a user + Explanation about important configuration files of User Admin

1. To create a user use the below command:

➔

Syntax: useradd <username>

OR

Syntax: adduser <username>

E.g., useradd user1

```
[root@localhost /]# useradd U1
[root@localhost /]# cd /home
[root@localhost home]# ls
student  U1
[root@localhost home]#
```

OR

adduser user1

```
[root@localhost /]# adduser U2
[root@localhost /]# cd /home
[root@localhost home]# ls
student  U1  U2
[root@localhost home]#
```

2. To modify properties of existing user:

➔

Syntax: usermod –c "<Description>" <username>

E.g., usermod –c "This is the test user" U1

Whereas,

usermod = Using this command you can modify the description / comment part of the current / existing user.

-c = Used to set the comment.

"This is the test user" = This line under double quotes is nothing but the actual description / comment which is set using **"-c" and "usermod" command.**

```
[root@localhost /]# getent passwd U1
U1:x:1001:1001::/home/U1:/bin/bash
[root@localhost /]# usermod -c "This is the test user" U1
[root@localhost /]# getent passwd U1
U1:x:1001:1001:This is the test user:/home/U1:/bin/bash
[root@localhost /]#
```

<u>Following files and directories will be modified after adding user account:</u>

1. /etc/passwd = Files get updated.

➔

Command 1: cat /etc/passwd

Command 2: getent passwd testuser

Whereas,

Getent = Get Entry

testuser = User Name

Note: Fields in /etc/passwd file:

testuser: x: 2001:2001::/home/testuser:/bin/bash

2. /etc/shadow = Files get updated.

➔

Command 1: cat /etc/shadow

Command 2: getent shadow testuser

Notes: Fields in /etc/shadow file:

Mohan:!!: 19520:0:99999:7:::

"!!:" Password is not set yet.

3. /etc/group = Files get updated.

➔

Command 1: cat /etc/group

Command 2: getent group G1

Notes: Fields in /etc/group file:

G1: x: 2003:

4. How directory with username gets created in /home

➔

Command 1: cd /home

Command 2: ls –l

Command 3: cd testuser

Command 4: ls

Command 5: ls –a

Note: There are hidden files. Hidden files starts with (dot).

.bashrc: This is get executed when we open new terminal.

.bash_profile: This gets executed when user logs in.

5. Mail file gets created with username in /var/spool/mail.

➔

Command 1: ls –l /var/spool/mail

Note: This is a blank file in which all mail gets stored.

D] Modifying Properties of Users:

1. –u: user id: Modify user id manually. Can be user with useradd and usermod.

➔

Command 1: usermod –u 2000 testuser

Command 2: getent passwd testuser

2. –c: comment: add comment manually. Can be used with useradd and usermod.

➔

Command 1: usermod –c "Tester" testuser

Command 2: getent passwd testuser

3. –d: Change home directory: Use with only useradd command.

➔

Command 1: mkdir /home/sales

Command 2: useradd –d /home/sales/testuser3 testuser3

4. –s: Change shell environment: Can used with useradd and usermod.

E] Two types of shell:

Sr.No	Interactive Shell	Non-Interactive Shell
1	Shell where we can execute commands.	We cannot execute commands.
2	It is assigned to normal users.	Mostly assigned to application users.
3	**Examples:** • sh (Bourne Shell) • csh (C Shell) • ksh (Korn Shell) • bash (Bourne Again Shell)	**Examples:** • False

Note:

All available shells can be listed using: /etc/shells file

Command: cat /etc/shells

Shells are either present in /bin OR /sbin

Command: usermod –s /sbin/nologin testuser

Command: useradd –s /bin/sh testuser5

Command: getent passwd testuser testuser5

Try to using login:

su – testuser

Note: You will get a message as this account is currently not available.

su – testuser5

$ echo $BASH

F] Adding & Modifying a Group:

1. groupadd: User to create group.

➔

Command 1: groupadd iVERTEX

Command 2: getent group iVERTEX

Note: When we add group two files get update.

Command 1: cat /etc/group

Command 2: cat /etc/gshadow : It stored password in encrypted format for groups.

2. groupmod: User to modify group properties.

G] Modifying Properties of Group:

1. –g: groupid: groupid can be used with groupadd and groupmod.

➔

Command 1: groupmod – g 2002 iVERTEX

Command 2: getent group iVERTEX

2 –n: used to rename the group. Used with only groupmod command..

➔

Command 1: groupmod – n marketing iVERTEX

Command 2: getent group iVERTEX

H] Adding users in different groups:

#useradd with (-g, -G option)

#usermod with (-g, -aG option)

#gpasswd with (-a, -d, -M option)

H-1] Add user in primary group:

1. –g: option:

➔

#groupadd OnInstall

#useradd –g OnInstall Oracle

#id Oracle

#usermod –g OnInstall testuser

#id testuser

Note: id: Gives user id and group ids of primary and secondary group.

H-2] Add user in secondary group:

1. –G: Secondary group used with useradd command.

➔

#useradd –G iVERTEX marketing testuser6

#id testuser6

2. –aG:

Whereas,

-a = Append

-G = Secondary Group, used with usermod command.

➔

#usermod –aG iVERTEX marketing oracle

#id testuser

Note: We can use "groups" command also

 # groups oracle

3. gpasswd: Used to add and remove user from group.

Syntax: gpasswd <option> <values> < groupname>

Options:

-a: To add user in group.

-d: To delete user from a group.

-M: To add list of users in a group.

Example:

#useradd u1

#gpasswd –a u1 iVERTEX

#gpasswd –d u2 iVERTEX

#getent group iVERTEX

#gpasswd –d testuser iVERTEX

#gpasswd –d oracle iVERTEX

#getent group iVERTEX

#getent group marketing

#gpasswd –M testuser6, oracle, u1, u2, marketing

#getent group marketing

I] Password Aging Policies

1. /etc/shadow: It stores password in encrypted format and password policies.

#getent shadow testuser

Explanation of properties after fetching /etc/shadow:

Policies are:

Encryption Algorithm:

MD5: Message Digest 5 (1)

SHA 256: Secure Hashing Algorithm 256 (5)

SHA 512: Secure Hashing Algorithm 512 (6)

Last Days: Number of days (Since January 1, 1970) since the password was last changed.

Minimum Days: Number of days before password may be changed.

Maximum Days: Number of days after which password must be changed.

Warning Days: Number of days to warn user of an expiring password (7 for a full week).

Inactive Days: Number of days after password expires that account is disabled.

Account Expiry: Has been number of days since January 1, 1970 that an account disabled.

2. chage: Command is used to list and changed the password policies of user accounts.

END