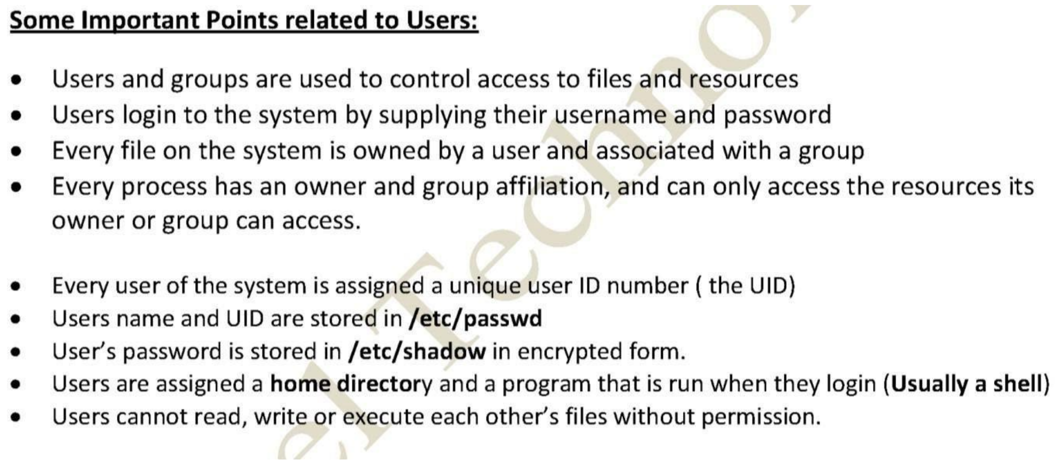
5. Users & Groups.

USERS



Some Important Points related to Users:

- Users and groups are used to control access to files and resources
- Users login to the system by supplying their username and password
- Every file on the system is owned by a user and associated with a group
- Every process has an owner and group affiliation, and can only access the resources its owner or group can access.

- Every user of the system is assigned a unique user ID number (the UID)
- Users name and UID are stored in **/etc/passwd**
- User's password is stored in **/etc/shadow** in encrypted form.
- Users are assigned a **home director**y and a program that is run when they login (**Usually a shell**)
- Users cannot read, write or execute each other's files without permission.

Types of user

TYPE	EXAMPLE	USER ID (ID)	GROUP ID (GID)	HOME DIR	SHELL
ROOT	root	0	0	/root	/bin/bash
REGULAR	imran, vagrant	1000 to 60000	1000 to 60000	/home/username	/bin/bash
SERVICE	ftp, ssh, apache	1 to 999	1 to 999	/var/ftp etc	/sbin/nologin

In Linux there are three types of users.

1. Super user or root user
Super user or the root user is the most powerful user. He is the administrator user.

2. System user
System users are the users created by the softwares or applications. For example if we install Apache it will create a user apache. These kinds of users are known as system users.

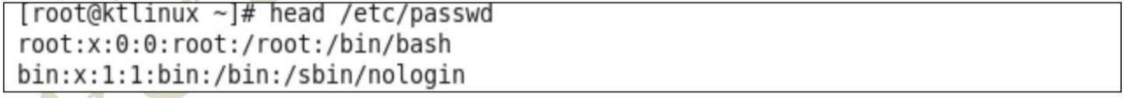
3. Normal user
Normal users are the users created by root user. They are normal users like Rahul, Musab etc. Only the root user has the permission to create or remove a user.

Whenever a user is created in Linux things created by default:-

- A home directory is created(/home/username)
- A mail box is created(/var/spool/mail)
- unique UID & GID are given to user

Passwd file

1. /etc/passwd



```
[root@ktlinux ~]# head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
```

The above fields are

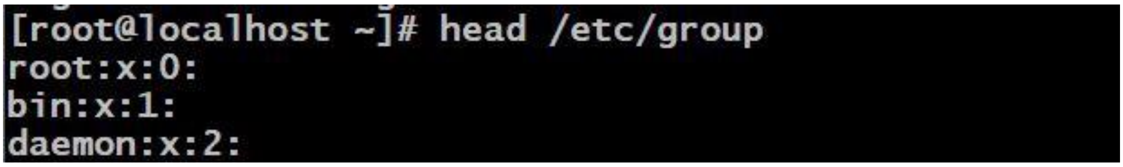
- **root** =name
- **x**= link to password file i.e. /etc/shadow
- **0** or **1**= UID (user id)
- **0** or **1**=GID (group id)
- **root** or **bin** = comment (brief information about the user)
- **/root** or **/bin** = home directory of the user
- **/bin/bash** or /**sbin/nologin** = shell

Group file

2. /etc/group

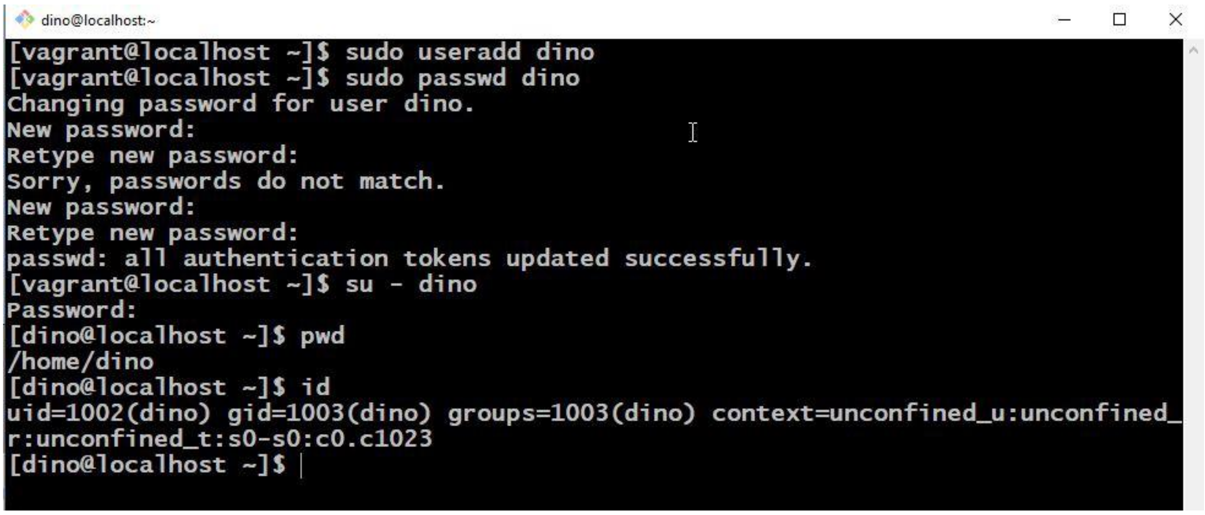
The file /etc/group stores group information. Each line in this file stores one group entry.

```
Group name, group password, GID, group members
```



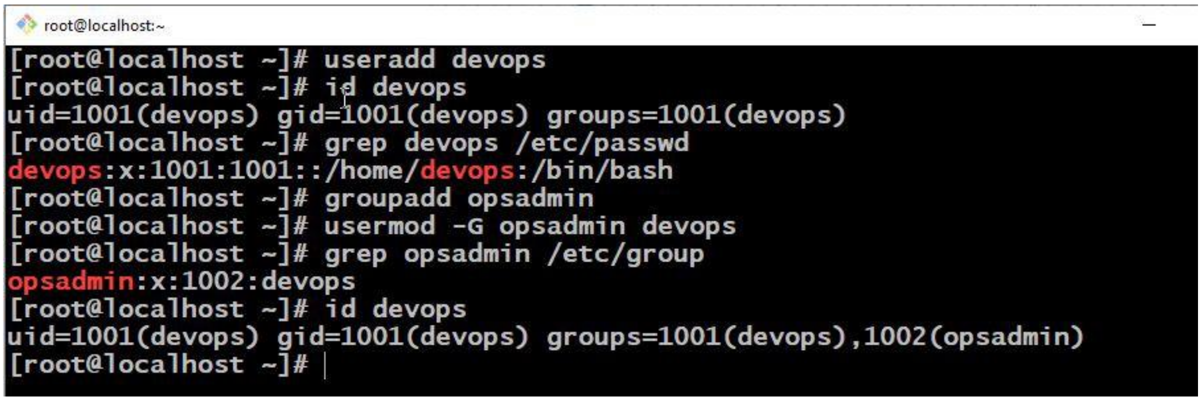
```
[root@localhost ~]# head /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
```

ADD USER, SET PASSWORD & SWITCH TO USER



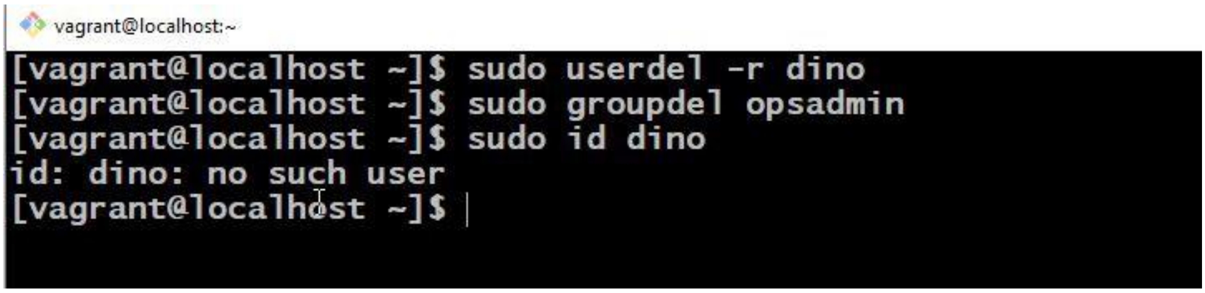
```
[vagrant@localhost ~]$ sudo useradd dino
[vagrant@localhost ~]$ sudo passwd dino
Changing password for user dino.
New password:
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[vagrant@localhost ~]$ su - dino
Password:
[dino@localhost ~]$ pwd
/home/dino
[dino@localhost ~]$ id
uid=1002(dino) gid=1003(dino) groups=1003(dino) context=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[dino@localhost ~]$
```

ADD USER, GROUP & USER INTO GROUP



```
[root@localhost ~]# useradd devops
[root@localhost ~]# id devops
uid=1001(devops) gid=1001(devops) groups=1001(devops)
[root@localhost ~]# grep devops /etc/passwd
devops:x:1001:1001::/home/devops:/bin/bash
[root@localhost ~]# groupadd opsadmin
[root@localhost ~]# usermod -G opsadmin devops
[root@localhost ~]# grep opsadmin /etc/group
opsadmin:x:1002:devops
[root@localhost ~]# id devops
uid=1001(devops) gid=1001(devops) groups=1001(devops),1002(opsadmin)
[root@localhost ~]#
```

DELETE USER & GROUP



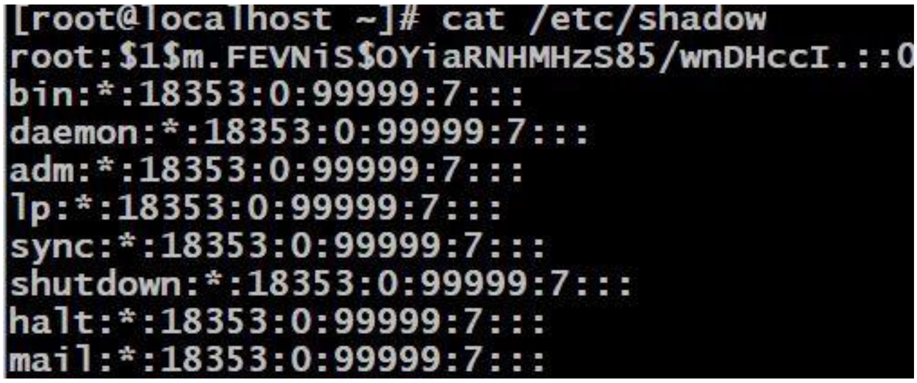
```
[vagrant@localhost ~]$ sudo userdel -r dino
[vagrant@localhost ~]$ sudo groupdel opsadmin
[vagrant@localhost ~]$ sudo id dino
id: dino: no such user
[vagrant@localhost ~]$
```

3. The /etc/shadow file

This file stores users' password and password related information. Just like */etc/passwd* file, this file also uses an individual line for each entry.

1. Username
2. Encrypted password
3. Number of days when password was last changed
4. Number of days before password can be changed
5. Number of days after password must be changed
6. Number of days before password expiry date to display the warning message

7. Number of days to disable the account after the password expiry
8. Number of days since the account is disabled
9. Reserved field



```
[root@localhost ~]# cat /etc/shadow
root:$1$m.FEVNiS$OYiaRNHMHzS85/wnDHccI.::0
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
```

USER & GROUP cheatsheet

COMMANDS	DESCRIPTION
useradd	Creates user in RedHat
adduser	Creates user in ubuntu
id	Shows user info
groupadd	Creates group
usermod -G grpnam usrname	Adds user to group
passwd	set/reset password
userdel -r	removes user with home dir
groupdel	removes group
last	shows last login in system
who	who is logged into system
whoami	username
`lsof -u user`	`List files opened by user`