#This File is written by Sayali Jadhav

1)What are File Permissions?

In Linux, there are three types of owners for a file.

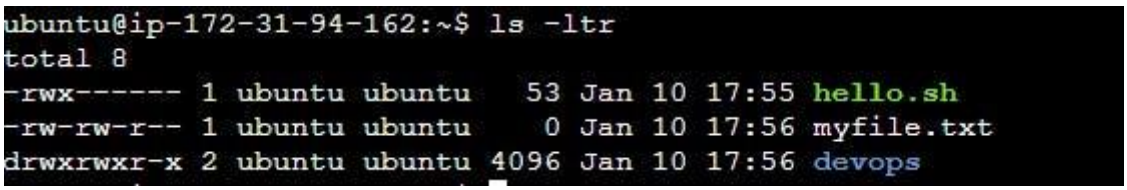
User - The user permissions apply only the owner of the file or directory, they will not impact the actions of other users. user can also be called default owner of the file.

Group - It is a collection of users. If you assign certain permission to a group same permission will be shared by all the members of group.

Others - Any user that is not a owner of file or doesn't belong to the group can be categorized as others.

Linux file permissions for all three categories of users:
i)Read permission: Read permission allow users to open and read the file only.
ii)Write permission: It allows the user to modify the file.
iii)Executable permission: It allows the user to run an executable script.

we can find permissions of files and folders using a long listing **(ls -ltr)** on a Linux terminal.



In the output above, **d** represents a directory and **-** represents a regular file.

The **chmod** command enables you to change the permissions on a file.

Syntax of chmod:

chmod permissions filename

Permissions can be changed using two modes:
i)Symbolic mode
ii)Absolute mode

Symbolic mode:

The permissions for a file or directory can be set for the owner, for the group that the file belongs to, and for all other users. The "**u**", "**g**", and "**o**" options stand for the user, group, and others, respectively. The "**+**" and "**-**" signs are used to add and remove permissions, respectively. The "**x**" permission allows a file to be executed. The "**w**" permission allows a file to be modified. The "**r**" permission allows a file to be read or a directory to be listed.

Ex: chmod u+x file.txt

chmod o-r file.txt

Absolute mode :-

In absolute mode we have to use numbers to assign permissions.

Ex: chmod 777 file.txt

chgrp command is used to change the group ownership of the file or directory.

2)Read about ACL and try out the commands getfacl and setfacl

The "**getfacl**" and "**setfacl**" commands are used to get and set file access control lists (ACLs) in Linux. ACLs allow you to specify fine-grained permissions for files and directories beyond the standard user, group, and other permissions.

i)If ACL is not enabled in our file system

Command to install acl: sudo apt install acl.

```
ubuntu@ip-172-31-94-162:~$ sudo apt install acl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  acl
```

ii)getfacl

The output of the "**getfacl**" command will show the ACLs for the file, including the owner, group, and permissions for each user and group.

```
ubuntu@ip-172-31-94-162:~$ getfacl file.txt
# file: file.txt
# owner: ubuntu
# group: ubuntu
user::rw-
group::rw-
other::r--
```

iii)setfacl

"**setfacl**" is used to set or modify the ACLs of a file or directory.

For example, to give read and execute permissions to "user2" and read permission to "user3" for a file called "myfile" you would run

setfacl -m u:user2:rx,u:user3:r myfile

The "**-m**" option tells "**setfacl**" to modify the existing ACLs of the file. The "**u:user2:rx**" and "**u:user3:r**" values specify the permissions to set for "**user2**" and "**user3**" respectively.