**File Permissions**

Every file and directory on Linux System is assigned 3 types of owners

1. **User** (Owner): A user is the owner of file.
2. **Group**: A user-group can contain multiple users. All users belonging to a group will have the same Linux group permissions access to the file.
3. **Others**: When you set the permission for others, it also referred as set permissions for the world.

**Permissions: 3 Permissions for all owners**

**Read:** This permission gives you the authority to open and read a file.

**Write:** The write permission gives you the authority to modify the contents of a file.

**Execute:** If the execute permission is not set, you might still able to see/modify the program code, but not run it.

r : read permission

w : write permission

x : execute permission

- : no permission

-rwxrw-r--

Here first (0) - represents the file type.

Then the next 3 characters are for Owner

Then the next 3 characters are for Group

And last 3 characters are for Others

* Owner can read, write and execute
* Group can read and write
* Others (World) can only read

**Setting Permission**

Syntax: chmod <groupName>=<permissions> <fileName>

e.g., chmod u=rwx,g=rw,o=r file1.txt

**Octal permission**

Binary Octal Permissions

000 0 ---

001 1 --x

010 2 -w-

011 3 -wx

100 4 r--

101 5 r-x

110 6 rw-

111 7 rwx

777 = rwxrwxrwx

764 = rwxrw-r--

e.g., chmod 764 file1.txt

**umask**

While creating a file or directory, by default a set of permissions are applied. These default permissions are viewed by umask command.

For safety reason all Unix systems doesn’t provide execution permissions to newly created files.

Adding execution permission is up to you.

**Setting the mode during creation of file/directory**

Syntax: mkdir –m <mode> <fileName>

e.g., mkdir –m 777 file1.txt