Understanding Linux File Permissions

Linux file permissions help control **who** can access a file and **how** they can use it. Every file has three permission categories:

Permission Categories

- **User (u)** → Owner of the file
- **Group (g)** → Users in the file's group
- **Others (o)** → Everyone else
- **Nothing (-)**→Nothing

Types of Permissions

- **r** → Read
- **w** → Write
- **x** → Execute

Common file-type characters:

Symbol	Meaning
-	**Regular file**
d	**Directory**
l	**Symbolic link**
c	Character device file
b	Block device file
s	Socket
p	Named pipe (FIFO)

Numeric Values

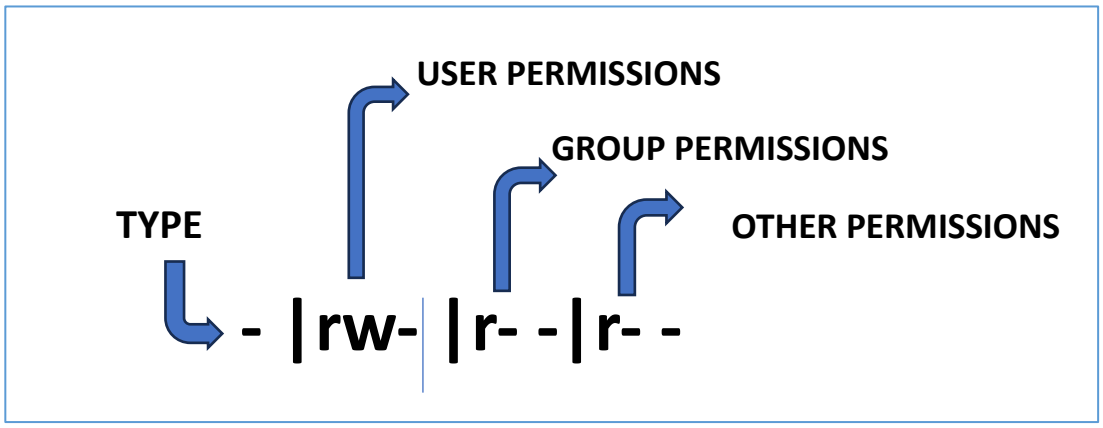
Permission	Value
No permission	**0**
Execute only	**1**
Write only	**2**
Write + Execute	**3**
Read only	**4**
Read + Execute	**5**
Read + Write	**6**
Read + Write + Execute	**7**

Checking Permissions

- ls -l file.txt

Modifying Permissions

- chmod 755 file.txt
- chmod u+r file.txt
- chmod g-w file.t
- chmod o+x file.txt



File Permissions with ACL (Access Control List)

ACLs allow you to give **more specific permissions** to a file or directory without changing the basic user/group/other permissions.

What ACL allows:

- Assign custom permissions to **any user**
- Assign custom permissions to **any group**
- Apply permissions **recursively** to folders

1. getfacl – View ACL Permissions

Use getfacl to check all ACL entries on a file or directory.

View ACL of a file

- getfacl file.txt

View ACL of a directory

- getfacl folder/

View ACL recursively

getfacl -R folder/

Example Output

file: file.txt

owner: user1

group: staff

user::rw-

user:john:r--

group::r--

mask::rw-

other::r--

2. setfacl – Set or Modify ACL Permissions

setfacl allows you to grant custom permissions to users and groups.

Add permission for a user

- setfacl -m u:john:rw file.txt

Add permission for a group

- setfacl -m g:developers:r file.txt

Remove ACL entry

- setfacl -x u:john file.txt

Apply ACL recursively to a folder

- setfacl -R -m u:john:rwx folder/