

What are Permissions?

This lesson will tell you everything you need to know about permissions in GNU/Linux.

In Linux, each file or directory follows certain set of rules and restrictions regarding who can access the file and change its content. These rules or *access modes* are commonly referred as *permissions* in Bash. Permissions are sometimes very useful as it gives us the benefit of hiding certain things from other users or make them non-editable for them.

Types of Permissions:

Based on the kind of actions a user can perform on a file, the three basic type of permissions are:

- Read
- Write
- Execute

Symbolical Permissions:

Mode	Meaning
r	Read the file
w	Write/Delete the file
x	Execute the file or search the directory

Numerical Permissions:

Given below is a list of numerical modes which can be changed for the owner, group users, and everyone else. A symbolical equivalent is also mentioned in the next column.

Mode	Meaning
0	000 -> --- -> None
1	001 -> --x -> Execute Only
2	010 -> -w- -> Write only
3	011 -> -wx -> Write and Execute
4	100 -> r-- -> Read only
5	101 -> r-x -> Read and Execute
6	110 -> rw- -> Read and Write
7	111 -> rwx -> Read, Write & Execute