# Linux Permissions

# Overview

| Special | | | User | | | Group | | | Others | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SUID | SGID | STICK | r | w | x | r | w | x | r | w | x |
| 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |

## Owner, Group and Other

| Item | Description |
|---|---|
| User | The user is the owner of the files. The user of a file or directory can be changed with the chown [3]. command.Read, write and execute privileges are individually set for the user with 0400, 0200 and 0100 respectively. Combinations can be applied as necessary eg: 0700 is read, write and execute for the user. |
| Group | A group is the set of people that are able to interact with that file. The group set on a file or directory can be changed with the chgrp [4]. command.Read, write and execute privileges are individually set for the group with 0040, 0020 and 0010 respectively. Combinations can be applied as necessary eg: 0070 is read, write and execute for the group. |
| Other | Represents everyone who isn't an owner or a member of the group associated with that resource. Other is often referred to as "world", "everyone" etc.Read, write and execute privileges are individually set for the other with 0004, 0002 and 0001 respectively. Combinations can be applied as necessary eg: 0007 is read, write and execute for other. |

## Read Write and Execute Permissions

| Item | Description |
|---|---|
| Read: | Allows files to be read. Is denoted with "r" in the output of the ls command. |
| Write: | Allows files to be written. Is denoted with "w" in the output of the ls command. |
| Execute: | Execute permissions allow binary files to be executed but they also control whether a directory is searchable. For example if a directory has permissions of 0600 you cannot use the cd command to "change directory" into it, nor can you list it's contents. Execute permissions are denoted with an "x" in the output of ls. |

## Special Modes

| Item | Description |
|---|---|
| setuid: | Binary executables with the setuid bit (chmod u+s path) can be executed with the privileges of the file's owner. Due to it's nature it should be used with care. In octal, the setuid bit is set with 4000 e.g: "chmod 4755 path". setuid has no effect if the user does not have execute permissions. setuid is represented with a lower-case "s" in the output of ls. In cases where it has no effect it is represented with an upper-case "S". |

| Item | Description |
|------|-------------|
| setgid: | Binary executables with the setgid bit (chmod g+s path) can be executed with the privileges of the file's group.<br>A useful property is to set the setgid bit on a directory so that all files and directories newly created within it inherit the group from that directory.<br>In octal, the setgid bit is represented by 2000 e.g: "chmod 2755 path".<br>setgid has no effect if the group does not have execute permissions.<br>setgid is represented with a lower-case "s" in the output of ls. In cases where it has no effect it is represented with an upper-case "S". |
| Sticky bit: | The sticky bit (chmod +t path) was introduced for use with executables as a way of telling an operating system to keep the text segment of the program in swap space after the process had terminated. This was a performance feature designed to make subsequent execution of the program faster.<br>The sticky bit is more commonly used on directories where it allows the files or directories within to only be moved or deleted by that object's owner, the directory owner, or the super-user.<br>In octal, the sticky bit is set with 1000 e.g: "chmod 1755 path".<br>The sticky bit has no effect if other does not have execute permissions.\\The sticky bit is represented with a lower-case "t" in the output of ls. In cases where it has no effect it is represented with an upper-case "T". |

# Links

- [Permission calculator](#)
- [[https://chmodcommand.com|]chmod command]

From:

[https://wiki.oscardegroot.nl/](https://wiki.oscardegroot.nl/) - **HomeWiki**

Permanent link:
**https://wiki.oscardegroot.nl/doku.php?id=linux:system:permissions**

Last update: **2022/01/15 11:38**