**Linux users, groups and permissions**

https://www.linode.com/docs/guides/linux-users-and-groups/

What are Linux User and Group Permissions?

Linux/Unix operating systems have the ability to multitask in a manner similar to other operating systems. However, Linux’s major difference from other operating systems is its ability to have multiple users. Linux was designed to allow more than one user to have access to the system at the same time. In order for this multiuser design to work properly, there needs to be a method to protect users from each other. This is where permissions come in to play.

Read, Write, & Execute Permissions

Permissions are the “rights” to act on a file or directory. The basic rights are read, write, and execute.

* Read: a readable permission allows the contents of the file to be viewed. A read permission on a directory allows you to list the contents of a directory.
* Write: a write permission on a file allows you to modify the contents of that file. For a directory, the write permission allows you to edit the contents of a directory (e.g. add/delete files).
* Execute: for a file, the executable permission allows you to run the file and execute a program or script. For a directory, the execute permission allows you to change to a different directory and make it your current working directory. Users usually have a default group, but they may belong to several additional groups.

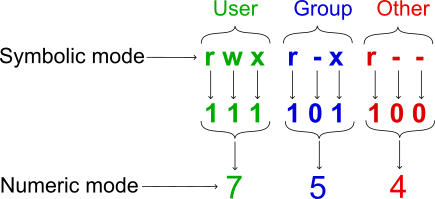
Viewing File Permissions

To view the permissions on a file or directory, issue the command ls -l <directory/file>. Remember to replace the information in the <directory/file> with the actual file or directory name. Below is sample output for the ls command:

-rw-r--r-- 1 root root 1031 Nov 18 09:22 /etc/passwd

The first ten characters show the access permissions. The first dash (-) indicates the type of file (d for directory, s for special file, and - for a regular file). The next three characters (rw-) define the owner’s permission to the file. In this example, the file owner has read and write permissions only. The next three characters (r--) are the permissions for the members of the same group as the file owner (which in this example is read only). The last three characters (r--) show the permissions for all other users and in this example it is read only.

Graphical user interface, application

Description automatically generated 

We can modify file permissions via the following command

chmod 777 <My file>

Please note, that it is highly recommended to do tests on this command on our files, not the system files!

Viewing, creating and deleting Users and Groups

To view information about users, issue the command cat /etc/passwd.

Here is the description of the lines of passwd file:

Shape

Description automatically generated with medium confidence

To view information about users, issue the command cat /etc/group.

Here is the description of the lines of passwd file:

Shape

Description automatically generated with medium confidence

We can add new user by the command:

useradd mariam

We can delete the user by the command:

passwd mariam

Note, that it is highly recommended to do all the tests on our test users, not the system users!

We can change the password for user by the command:

passwd mariam

Do experiments of the following commands:

groupadd comping

groupdel comping

usermod -a -G groupname

groups

getent group

deluser <user> <group>