File permissions in Linux

Project description

In this project, I will examine file and directory permissions from the current working directory that I am working at. The goal is to ensure that every file and directory permissions have been aligned with the corporate policy and implement the least privilege principle. I am using several linux commands to work with the file and directory such as `cd` and `ls` (along with its applicable options). To change the permissions of files and directories, I will use the chmod command along with its applicable arguments.

Check file and directory details

The current files and directories permissions are as follows:
project_k.txt

- User = read, write,
- Group = read, write
- Other = read, write

project_m.txt

- User = read, write
- Group = read
- Other = none

project_r.txt

- User= read, write
- Group = read, write
- Other = read

project_t.txt

- User = read, write
- Group = read, write
- Other = read

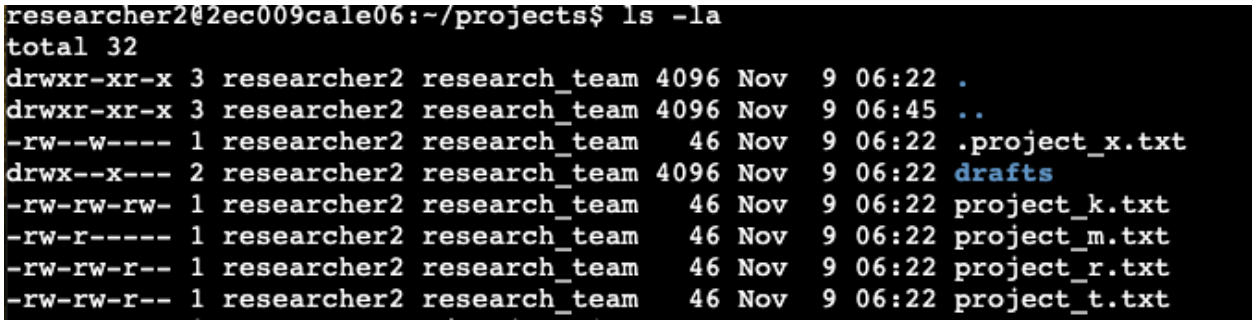
.project_x.txt

- User = read, write
- Group = write
- Other = none

There is also one subdirectory inside the projects directory named **drafts**. The permissions on drafts are:
User = read, write, execute
Group = execute

Other = none

Following are screenshots of the activity of checking the files and directories permission (including the command)



`ls -la` will list all files and directories along with their permissions as well as showing the hidden files (-a options)

Describe the permissions string

Lets take an example of `project_k.txt` file where the permissions (on the leftmost) state `-rw-rw-rw-`

The explanation of this 10 character strings that represent file permissions are as follows:

1. The **first character represents** the type of object whether it is a directory or a file. If it is a directory, the character in this part will be `d`, while it will be `-` if it is file. Therefore because `project_k.txt` is file then the first character will be `-`
2. The **following three characters** represent the permission for the user where `r` represents read access, `w` represent write access and `x` represent execute permissions (if file is executable). In `project_k.txt` file, `rw-` permissions means that the user has read and write access while execute access is missing.
3. The **next three characters** represent the permissions for a group, will consist of several users. In this case, `project_k.txt` has `rw-` permissions for `research_team` group which means anyone in that group is able to read and write the files.
4. The **last three characters** represent the permissions for other users (anyone who has access to the system). And similar to users and group, the other users have read and write permissions to `project_k.txt` file

Change file permissions

Company policies stated that other users should not have write access to any files. In this case, `project_k.txt` file still gives write access to other users. We need to modify this using following command

```
chmod o-w project_k.txt
```

And here is the result

```
researcher2@2ec009ca1e06:~/projects$ chmod o-w project_k.txt
researcher2@2ec009ca1e06:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:45 ..
-rw--w---- 1 researcher2 research_team   46 Nov  9 06:22 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov  9 06:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov  9 06:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_t.txt
```

The command will remove write access (-w) for others (o) so the argument for chmod command will be o-w followed by file name.

Change file permissions on a hidden file

The hidden file `.project_x.txt` is an archive file where no one should have write access to it. However users and groups should still be able to read the file. Therefore using the following command, the permissions of this file will be changed.

```
chmod u-w,g-w,g+r .project_x.txt
```

```
researcher2@2ec009ca1e06:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@2ec009ca1e06:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:45 ..
-r--r----- 1 researcher2 research_team   46 Nov  9 06:22 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Nov  9 06:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov  9 06:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_t.txt
```

The command will remove write access for user (u-w), remove write access to group (g-w) and add read access to group (g+r)

Change directory permissions

The directory `draft` should be accessed by researcher2 user only, therefore, access to group and other users should be removed. The following command will change the permissions

```
chmod g-x drafts
```

```
researcher2@2ec009ca1e06:~/projects$ chmod g-x drafts
researcher2@2ec009ca1e06:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:22 .
drwxr-xr-x 3 researcher2 research_team 4096 Nov  9 06:45 ..
-r--r----- 1 researcher2 research_team   46 Nov  9 06:22 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Nov  9 06:22 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Nov  9 06:22 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Nov  9 06:22 project_t.txt
```

The command will remove execute access for group (g-x)

Summary

Above are examples on how to work in Linux to manage access and authorization to files and folders. By incorporating several commands such as ls and chmod as well as understanding the meaning of character in file attributes we can manage all the files and directories so it can comply to company policies and implement least privilege principle