File permissions in Linux

Project description

The research team needs to update the file permissions for certain files and directories within the `project` directory. The permissions do not currently reflect the level of authorisation that should be given. Through the use of Linux commands, existing permissions will be examined and modified so that they would match the authorisation.

Check file and directory details

The command used to check permissions was `ls -la`. The `ls` command lists out files and directories in the current working directory, in this case the directory was `projects`. The options used with the command was `-la` which shows the permissions of files, directories, and also any hidden files.

The current file permissions are displayed in the output.

```
researcher2@dfd29ad27392:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 13:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 14:31 ..
-rw--w---- 1 researcher2 research_team   46 Mar 26 13:56 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Mar 26 13:56 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Mar 26 13:56 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Mar 26 13:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_t.txt
```

Describe the permissions string

The 10-character string on the left of each row of the input indicates the file, and directory permissions. For example, `project_t.txt` has file permissions of `-rw-rw-r--`.

- The first character of the string indicates whether the permissions are for a file or a directory, `d` is for directory and `-` is for file.
- The 2nd to 4th characters indicate the permissions for the user, 2nd character or `r` is for read permission, 3rd character or `w` is for write permission, and 4th character or `x` is for execute permission. If `-` is in place on any of those characters it indicates that they do not have that access. In `project_t.txt` case, the user has read and write permissions but not execute permission.

- The 5th to 7th characters indicate the permissions for the user group, the letters work the same way as previous. In `project_t.txt` case, the user group has read and write permissions but not execute permission.
- The 8th to 10th characters indicate the permissions for the other users in the system, the letters work the same way as previous. In `project_t.txt` case, the other users have read permission but not write or execute permissions.

Change file permissions

The organisation does not allow other users to have write access to any files. I used the command `chmod o-w project_k.txt` to remove write access from the other users.
`chmod` is the command used to change the permissions of files and directories.
The first argument, `o-w`, indicates that the write permission was to be removed from the others group. The first letter is the owner type, the next is the operator for adding, removing, or setting permissions, the letter after the operator is the permission type.
The second argument indicates that the changes were to be made to the `project_k.txt` file.

The output after using `ls -la` again shows that the permission for `project_k.txt` has been changed.

```
researcher2@dfd29ad27392:~/projects$ chmod o-w project_k.txt
researcher2@dfd29ad27392:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 13:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 14:31 ..
-rw--w---- 1 researcher2 research_team   46 Mar 26 13:56 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Mar 26 13:56 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Mar 26 13:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_t.txt
```

Next, the organisation does not allow the user group to be able to read the `project_m.txt` file. I used the command `chmod g-r project_m.txt` to remove the read permission from the user group.
The `-` operator indicates that the permission is to be removed from the owner type.

The output after using `ls -la` again shows that the permission for `project_m.txt` has been changed.

```
researcher2@dfd29ad27392:~/projects$ chmod g-r project_m.txt
researcher2@dfd29ad27392:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 13:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 14:31 ..
-rw--w---- 1 researcher2 research_team   46 Mar 26 13:56 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Mar 26 13:56 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_k.txt
-rw------- 1 researcher2 research_team   46 Mar 26 13:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_t.txt
```

Change file permissions on a hidden file

The hidden file `.project_x.txt` was revealed due to the `-a` option as part of the `ls -la` command. It was archived by the research team using the `.` prefix. The file should not have write permissions for anyone, but the user and group should be able to read the file. I used the command `chmod u-w,g=r .project_x.txt` to modify the permissions of the file.
The `=` operator indicates that the user group was to be given the read permission only.

The output after using `ls -la` again shows that the permission for `.project_x.txt` has been changed.

```
researcher2@dfd29ad27392:~/projects$ chmod u-w,g=r .project_x.txt
researcher2@dfd29ad27392:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 13:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 14:31 ..
-r--r----- 1 researcher2 research_team   46 Mar 26 13:56 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Mar 26 13:56 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_k.txt
-rw------- 1 researcher2 research_team   46 Mar 26 13:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_t.txt
```

Change directory permissions

Only the user, `researcher2`, should be allowed to access the `drafts` directory and its content. I used the command `chmod g-x` to remove the execute permission from the user group.

The output after using `ls -la` again shows that the permission for `drafts` has been changed.

```
researcher2@dfd29ad27392:~/projects$ chmod g-x drafts
researcher2@dfd29ad27392:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 13:56 .
drwxr-xr-x 3 researcher2 research_team 4096 Mar 26 14:31 ..
-r--r----- 1 researcher2 research_team   46 Mar 26 13:56 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Mar 26 13:56 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_k.txt
-rw------- 1 researcher2 research_team   46 Mar 26 13:56 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Mar 26 13:56 project_t.txt
```

Summary

Throughout the projects, I used the command `chmod` to modify permissions for different owner types to comply with the level of authorisation the organisation wanted. First `ls -la` was used to check permission of all the files and directories. I then used `chmod` to modify the permissions.