KYRIAKI ILIADOU

6/4/2024

File permissions in Linux. LAB

Project description

The research team at my organization have to update if the existing team users permissions on the file system are comply with authorization that should be given or if needs to modify the permissions to authorize the appropriate users and to remove any unauthorized access to help keeps system secure.

Check file and directory details.



To check file and directory permissions I used the Linux command to display the permissions in all files and hidden files as well.

The first line displays the command ls -la and the below lines the output . The code lists all contents of the projects directory.

The returned of the ls command includes a subdirectory named drafts ,and five other files, the command -la, returned a hidden file named . project\_x.txt

The 10 -character string in the first column represents the permissions set on each file or directory.

Describe the permissions string

The 10-character string can be reconstructed to update the authorization of who could have access the file and the specific permissions.

.

The 1st character could be d or hyphen (-), indicates the file type such as d for directory or hyphen (-) for normal files.

The 2nd to 4th character indicates the user( u ) , the permissions are read (r) and write (w) and execute (x), when they are missing and the character is hyphen (-) does mean that there isn’t granted access for this user.

The 5th to 7tn characters indicates the group (g) the permissions are read(r) and write (w)and execute(x), when they are missing and the character is hyphen (-) does mean that there isn’t granted access for this group.

The 8th to 10 characters indicates the other user ( u) the permissions are read (r) and write (w)and execute(x), when they are missing and the character is hyphen(-) does mean that there isn’t granted access for the other.

An example: for the file project\_t.txt below will be explained the characters such as

-rw-rw-r—

The first hyphen (- ) indicates that the project\_t.txt is file and not a directory.

The 2nd,5th and 8th character are all ( r ) it indicates that there is permission for read ( r ) to owners user,group,other .

The 3rd and 6th character are ( w ) indicates that granted access for write only to user and group.

No one has permission execute for project\_t.txt.

Change file permissions

The organization determined that other shouldn’t have write access to any of their files. So, I used the permissions that previously returned to remove the write permisiion form other user.

The below screenshot indicates the code I used:



The first line is the command chmod o-w project\_k.txt that will remove the write permission from the owner other for the file project\_k.txt

The second line is the command of the display ls -la , to secure that everything changed correctly.

Change file permissions on a hidden file

The research team decided that no one has access to the hidden file .project\_x.txt.

The below screenshot demonstrate the code that I used to change permission.



The first line is the command chmod u-w,g-w,g+r .project\_x.txt will allow only the read permission for the user and group and no write for anyone.

The chmod command changes the permissions on files and directories.

The first argument displays the changes on the permissions, the second argument specifies the file or directory. The hidden file is displayed with a dot at the beginning.

Change directory permissions

The organization decided to grant access to drafts directory only to researcher 2 user, which does mean that no one than researcher 2 has execute permissions to the drafts directory.

The below screenshot displays the code I used to do so.



The first line is the command chmod g-x drafts will give permission

Only to. **researcher2** to access the **drafts** directory and its contents.

The group execute permission removed from the drafts.

Summary

I changed permissions to comply with the organization’s demands to the files and directories. The basic code to check if the changes has be done successfully was the code ls -la, the code for the changes is chmod command.

With these modifications in read, write and execute authorization on the files access the researcher team will operate with more security for the file system.