

Autorisations de fichiers sous Linux

Descriptif du projet

Comme la demander l'équipe de recherche de mon organisation, ma tâche consiste à examiner les autorisations existantes sur le système des fichiers, ainsi nous devons déterminer si les permissions correspondent à l'autorisation qui devrait être donnée. Si ce n'est pas le cas, nous devons modifier les permissions pour autoriser les utilisateurs appropriés et supprimer tout accès non autorisé.

Vérifier les détails du fichier et du répertoire

Pour vérifier les autorisations des fichiers et répertoires nous utilisons la commande (`ls -la`), ainsi nous obtiendrons tous les fichiers et leurs autorisations même les fichiers cachés. La sortie du commande donne l'image suivante:

```
researcher2@46decb7acf99:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:56 ..
-rw--w---- 1 researcher2 research_team  46 Jan  4 21:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  4 21:03 drafts
-rw-rw-rw- 1 researcher2 research_team  46 Jan  4 21:03 project_k.txt
-rw-r----- 1 researcher2 research_team  46 Jan  4 21:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_t.txt
```

Décrire la chaîne d'autorisations

La chaîne de caractère (par exemple `drwxr-xr-x`) nous informe des paramètres d'autorisation du fichier ou du sous-répertoire. Cette chaîne est composée de dix caractères: la première nous informe si nous faisons face à un fichier normal ou à un sous-répertoire(`d` signifie directory ou répertoire en français), si nous faisons face à un fichier standard à la place de `d` il y aurait un tiret. De la deuxième à la quatrième caractère on observe les autorisations de l'utilisateur (`r` comme read /écrire, `w` comme write/écrire et `x` pour execute/exécuter) le même processus est utilisé de la cinquième à la septième caractère pour l'autorisation du groupe et de la huitième à la dixième caractère pour l'autorisation de l'autre (tout autre utilisateurs du système). A chaque fois qu'une autorisation n'est pas accordée, elle est remplacée par un tiret dans la chaîne de caractère.

Modifier les autorisations des fichiers

L'organisation a déterminé que les autres ne devraient pas avoir accès à certaines autorisations telles que la lecture dans aucun de leur fichier. Pour modifier les autorisations, la commande **chmod** est utilisée, ainsi des modifications devaient être effectuées sur les fichiers (**project_k.txt** et **project_m.txt**):

```
researcher2@46decb7acf99:~/projects$ chmod g-r project_m.txt
```

```
researcher2@46decb7acf99:~/projects$ chmod o-w project_k.txt
```

La vérification de la sortie donne le résultat suivant:

```
researcher2@46decb7acf99:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:56 ..
-rw--w---- 1 researcher2 research_team  46 Jan  4 21:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  4 21:03 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan  4 21:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_t.txt
```

Modifier les autorisations de fichier sur un fichier caché

L'équipe de recherche avait récemment archivé le fichier **project_x.txt**. Ils ne voudraient pas que quiconque ait accès à la lecture sauf l'équipe et l'utilisateur. Pour modifier l'autorisation du fichier caché, la commande a été utilisée:

```
researcher2@46decb7acf99:~/projects$ chmod u=r,g=r .project_x.txt
```

Avec cette commande j'ai écrasé les autorisations antérieures tout en introduisant de nouvelles autorisations. La vérification de la sortie du commande donne le résultat suivant:

```
researcher2@46decb7acf99:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:03 .
drwxr-xr-x 3 researcher2 research_team 4096 Jan  4 21:56 ..
-r--r----- 1 researcher2 research_team  46 Jan  4 21:03 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Jan  4 21:03 drafts
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_k.txt
-rw----- 1 researcher2 research_team  46 Jan  4 21:03 project_m.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_r.txt
-rw-rw-r-- 1 researcher2 research_team  46 Jan  4 21:03 project_t.txt
```

Modifier les autorisations du répertoire

L'organisation a décidé que seul l'utilisateur **researcher2** devrait avoir accès au répertoire **drafts**. Pour modifier l'accès au répertoire la commande suivante est utilisée:

```
researcher2@ece6b61fbf93:~/projects$ chmod g-r drafts
```

En utilisant cette commande le groupe n'a plus la possibilité de lire le répertoire. La vérification de la sortie donne le résultat suivant:

```
drwx----- 2 researcher2 research team 4096 Jan  4 21:43 drafts
```

Résumé

Cette tâche consistait à vérifier si les permissions correspondaient à l'autorisation qui devait être donnée, ainsi corriger toute incohérence. La commande "chmod" a été utilisée de nombreuses fois, car c'est le mode le plus symbolique pour modifier les autorisations.