Gestion des autorisations – Journal d'intervention

Lorsque j'ai accédé au répertoire `projects`, j'ai rapidement constaté que les autorisations attribuées aux fichiers et aux dossiers ne correspondaient pas aux règles de sécurité souhaitées par mon organisation. L'objectif était clair : ajuster les permissions pour que chaque utilisateur, groupe ou tiers ne dispose que du niveau d'accès requis, ni plus, ni moins.

Étape 1 : Observation de l'état initial

Pour effectuer un état des lieux, j'ai lancé la commande `ls -la`. Cette commande m'a permis d'afficher non seulement les fichiers visibles, mais également les fichiers cachés. Les résultats ont révélé :

- un répertoire nommé `drafts`,
- un fichier masqué `.project_x.txt`,
- ainsi que plusieurs fichiers de projet supplémentaires.

```
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

La colonne d'ouverture de chaque ligne affichait une chaîne de 10 caractères. C'est cette chaîne qui indiquait précisément les droits associés à chaque entrée.

Étape 2 : Interprétation des permissions

En analysant ces chaînes, j'ai décomposé les informations comme suit :

- Le premier caractère identifie le type : un `d` pour un dossier, un `-` pour un fichier classique.
- Les trois caractères suivants indiquent ce que l'utilisateur propriétaire est autorisé à faire : lecture (r), écriture (w), exécution (x).
- Les trois caractères suivants indiquent les permissions du groupe.
- Les trois derniers sont dédiés aux autres utilisateurs du système.

Par exemple, en examinant `project_t.txt`, j'ai vu `-rw-rw-r--`. Cela signifiait qu'il s'agissait d'un fichier classique, avec lecture et écriture autorisées pour l'utilisateur et le groupe, et uniquement la lecture pour les autres.

Étape 3 : Suppression des autorisations non conformes

Selon la politique interne de mon organisation, aucun utilisateur extérieur (other) ne doit pouvoir modifier un fichier. En consultant les permissions précédentes, j'ai remarqué que `project_k.txt` permettait encore l'écriture à cette catégorie.

```
researcher2@5d738f0f927b:~/projects$ chmod o-w project_k.txt
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-rw--w---- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

J'ai donc utilisé la commande `chmod` pour retirer ce droit, puis j'ai relancé `ls -la` afin de confirmer la prise en compte de cette modification.

Étape 4 : Intervention sur un fichier caché

Le fichier `.project_x.txt` avait été archivé récemment. Il devait rester consultable mais en mode lecture seule, même pour

l’utilisateur propriétaire et le groupe.
J’ai donc effectué les manipulations suivantes :

- suppression de l’écriture pour l’utilisateur (u-w),
- suppression de l’écriture pour le groupe (g-w),
- ajout de la lecture pour le groupe (g+r).

```
researcher2@3213bbc1d047:~/projects$ chmod u-w,g-w,g+r .project_x.txt
researcher2@3213bbc1d047:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec 20 15:36 ..
-r--r----- 1 researcher2 research_team   46 Dec 20 15:36 .project_x.txt
drwx--x--- 2 researcher2 research_team 4096 Dec 20 15:36 drafts
-rw-rw-rw- 1 researcher2 research_team   46 Dec 20 15:36 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec 20 15:36 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec 20 15:36 project_t.txt
researcher2@3213bbc1d047:~/projects$
```

Ce fichier étant précédé d’un point, j’ai confirmé qu’il s’agissait bien d’un fichier masqué.

Étape 5 : Restriction d’accès sur un répertoire

Le dossier drafts contenait des données sensibles réservées exclusivement à l’utilisateur researcher2. Pour empêcher quiconque d’y accéder, j’ai supprimé le droit d’exécution pour les autres utilisateurs.
Comme le droit d’exécution est celui qui permet d’entrer dans un répertoire, seule researcher2 conserve désormais la capacité d’accéder à son contenu. Le groupe, qui avait auparavant ce droit, a été restreint grâce à chmod.

```
researcher2@5d738f0f927b:~/projects$ chmod g-x drafts
researcher2@5d738f0f927b:~/projects$ ls -la
total 32
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 .
drwxr-xr-x 3 researcher2 research_team 4096 Dec  2 15:27 ..
-r--r----- 1 researcher2 research_team   46 Dec  2 15:27 .project_x.txt
drwx------ 2 researcher2 research_team 4096 Dec  2 15:27 drafts
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_k.txt
-rw-r----- 1 researcher2 research_team   46 Dec  2 15:27 project_m.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_r.txt
-rw-rw-r-- 1 researcher2 research_team   46 Dec  2 15:27 project_t.txt
researcher2@5d738f0f927b:~/projects$
```

Conclusion de l’intervention

Au terme de cette série d’actions, j’ai rétabli un environnement conforme aux attentes de sécurité :

- j’ai d’abord observé les autorisations existantes avec `ls -la`,
- puis j’ai ajusté les permissions une par une à l’aide de `chmod`,
- j’ai retiré les droits d’écriture inutiles,
- j’ai sécurisé un fichier caché,
- et j’ai verrouillé l’accès d’un répertoire sensible à un seul utilisateur désigné.

Ce processus a assuré un contrôle précis des accès tout en garantissant la conformité avec les exigences de l’organisation.