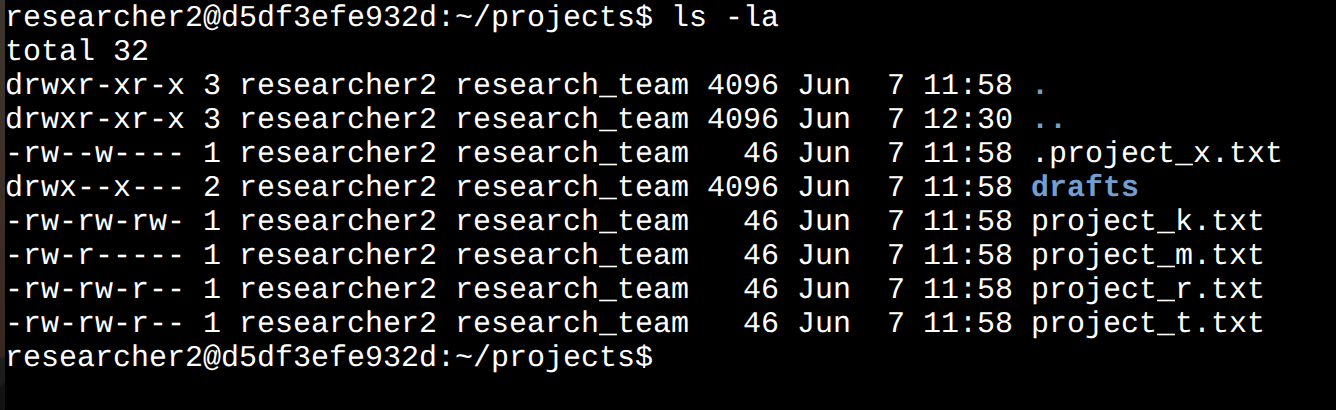
# Autorisations de fichiers sous Linux

## Description du projet

L'équipe de recherche de mon organisation doit mettre à jour les autorisations de fichiers pour certains fichiers et répertoires du répertoire *project.* Les autorisations ne correspondent pas actuellement au niveau d'autorisation requis. La vérification et la mise à jour de ces autorisations contribueront à la sécurité du système. Pour ce faire, j'ai effectué les opérations suivantes :

## Vérifier les détails du fichier et du répertoire

Le code suivant montre comment j’ai utilisé les commandes linux pour lister le contenu et les autorisations du répertoire projects. Les autorisations des fichiers du répertoire project sont les suivantes :



La première ligne de la capture affiche la commande saisie et les autres lignes le résultat. j’ai utilisé la commande ls pour lister le contenu du répertoire et l’option -la pour avoir une liste détaillée montrant les permissions et affichant les fichiers cachés. La sortie de la commande montre l'existence d’un répertoire nommé drafts , d’un fichier masqué nommé .project\_x.txt et de 4 autres fichiers textes . Chaque entrée commence par une chaîne de 10 caractères indiquant comment les autorisation des fichiers sont paramétrées .

## Décrivez la chaîne d'autorisations

La chaîne des 10 caractères peut être décomposé pour déterminer qui a accès aux fichiers et quels sont ses autorisations :

* Le premier caractère indique le type de fichier. d indique qu'il s'agit d'un répertoire. Un trait d'union (-) désignerait un fichier standard.
* Les caractères 2 à 4 correspondent aux autorisations de lecture (r), d'écriture (w) et d'exécution (x) de l'utilisateur. Lorsque l'un de ces caractères est remplacé par un trait d'union (-), l'utilisateur ne dispose pas de l'autorisation correspondante.
* Les caractères 5 à 7 correspondent aux autorisations de lecture (r), d'écriture (w) et d'exécution (x) du groupe. Lorsque l'un de ces caractères est remplacé par un trait d'union (-), le groupe ne dispose pas de l'autorisation correspondante.
* Les caractères 8 à 10 correspondent aux autorisations de lecture (r), d'écriture (w) et d'exécution (x) pour le type de propriétaire correspondant aux autres utilisateurs. Ce type de propriétaire englobe tous les autres utilisateurs du système, en dehors de l'utilisateur et du groupe. Lorsque l'un de ces caractères est remplacé par un trait d'union (-), ces autres utilisateurs ne disposent pas de l'autorisation correspondante.

Dans la liste de répertoires développée, le deuxième bloc de texte correspond à l'utilisateur propriétaire du fichier. Le troisième bloc de texte correspond au groupe propriétaire du fichier.  
  
Par exemple pour le fichier project\_t.txt , le caractère (-) indique qu’il s’agit d’un fichier , les caractères 2 à 4 et 5 à 7 indiquent que l'utilisateur et le groupe ont l’autorisation de de lecture et d’écriture mais pas d’exécution , les caractères 8 à 10 indiquent que les autres utilisateurs ont l’autorisation de lecture uniquement , ils n’ont pas l’autorisation d’écriture et d’exécution .

## Modifier les autorisations des fichiers

L’organisation ne veut pas que les autres utilisateurs aient accès l’autorisation d’écriture sur les fichiers du répertoire.Seul le fichier project\_k.txt accordaient l’autorisation d’écriture aux autres utilisateurs La capture suivante montre comment j’ai utilisé les commandes Linux pour supprimer l’autorisation d’écriture aux autres utilisateurs pour ce fichier.



J’ai utilisé la commande chmod qui sert à modifier les autorisations pour un fichier ou un répertoire . Je l’ai accompagné de l’option o-w pour signifier que je retire aux autres utilisateur (o) l’autorisation d’écriture (w) et de la cible c'est-à-dire le fichier project\_k.txt . J’ai ensuite utilisé la commande ls -la pour vérifier que l'opération fut un succès.

## Modifier les autorisations de fichier sur un fichier caché

Dans le répertoire projects se trouve le fichier .project\_x.txt , un fichier masqué qui a été archivé et stipule que personne ne doit pouvoir écrire mais que l'utilisateur et le groupe doivent pouvoir encore le lire. La capture suivante montre comment j’ai utilisé les commandes linux pour accomplir cette tâche



J’ai utilisé la commande de modification de permissions chmod suivit des options u-w , g-w, g+r pour indiquer que je retire l’autorisation d’écriture à l’utilisateur et au groupe ( les autres utilisateurs ne possédaient pas cette autorisation) et j’accorde l’autorisation de lecture au groupe (l’utilisateur possédait déjà cette autorisation ) suivit de la cible (.project\_x.txt ). Enfin j’ai utilisé la commande ls -la pour confirmer que les modifications ont été apportées.

## Modifier les autorisations du répertoire

L’organisation souhaite que seul l'utilisateur researcher2 doit pouvoir accéder au répertoire drafts et à son contenu. Cela signifie que seul researcher2 doit disposer de droits d'exécution. Pour cela j’ai utilisé les commandes Linux suivantes :



J’ai utiliser la commande de modification des permissions chmod suivi de l’option g-x pour indiquer que je retirait au groupe (research\_team) la permission d’exécution pour que seul l’utilisateur researcher2 ait cette permission, suivit de la cible ( répertoire drafts ) . Puis j’ai utilisé la commande ls-la pour confirmer la modification.

## Résumé

J’ai modifier les autorisation ser certains fichiers et répertoire pour correspondre au niveau d’autorisation de l’organisation . J’ai utilisé la commande de modification des autorisations chmod et de liste ls -la pour lister les fichiers, leurs autorisations .