aurlom

Années
2024-2025

PROJET E5

LABBI AMINE | 2024/2025 | BTS SIO - AURLOM

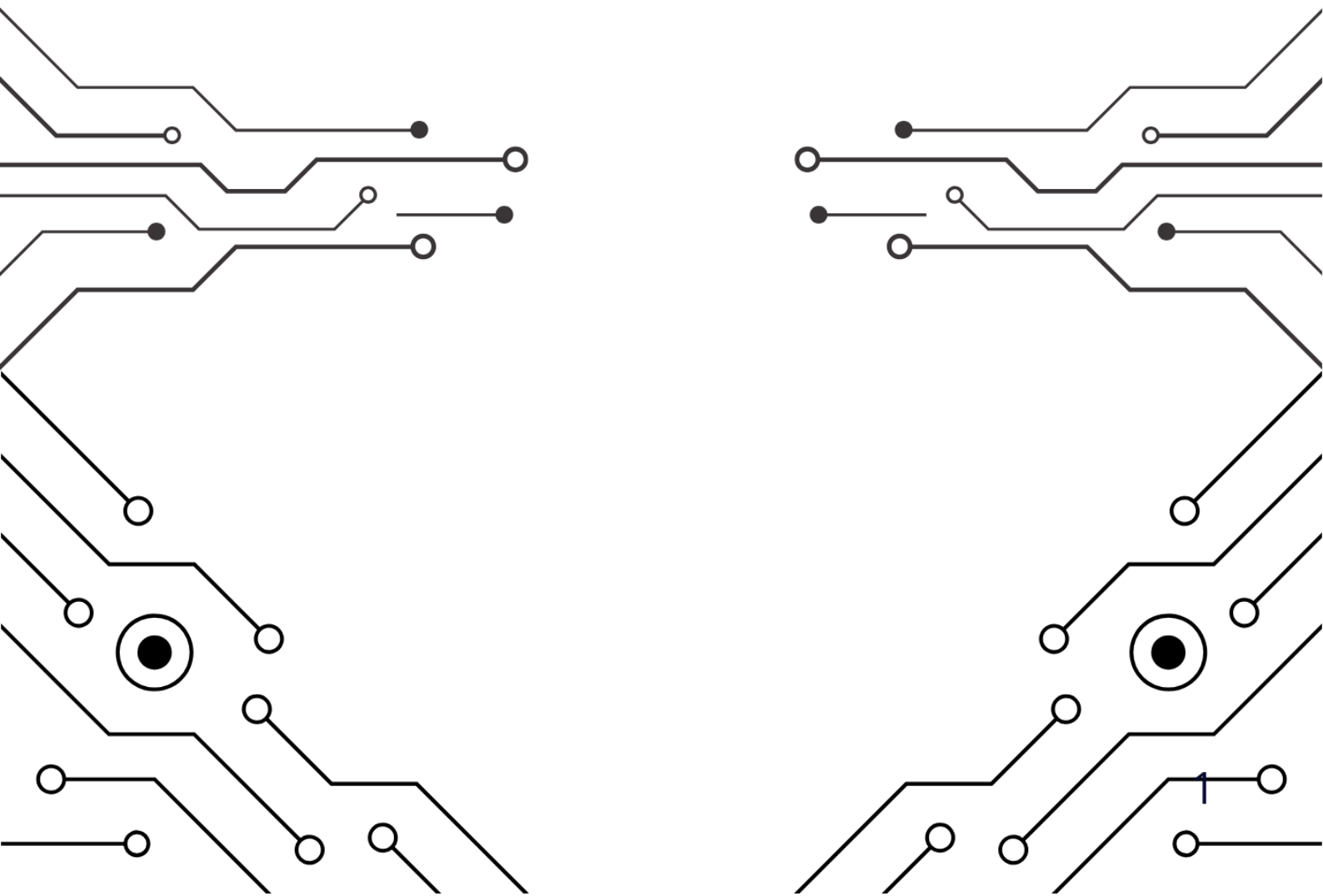

Table des matières

Introduction

Dans un environnement professionnel, la gestion des accès aux fichiers et dossiers est importante pour garantir la sécurité des données, éviter les fuites d'informations et assurer le respect des réglementations telles que le RGPD. Chaque utilisateur doit avoir accès uniquement aux ressources nécessaires à son activité, ce qui nécessite une configuration rigoureuse des permissions.

Défis de Gestion des Permissions

Les entreprises doivent faire face à des défis croissants en matière de gestion des utilisateurs et des droits d'accès. Une mauvaise configuration des permissions peut entraîner :

- Des fuites d'informations sensibles
- Une exposition aux cyberattaques (ransomware, hacking)
- Une non-conformité aux normes de sécurité (ISO 27001, RGPD)
- Une perte de productivité due à des erreurs d'accès

Ce projet vise à démontrer comment une gestion appropriée des permissions sous Linux permet de sécuriser efficacement les accès et d'améliorer l'efficacité au sein d'une infrastructure informatique.

Problématique

L'objectif est de répondre à la question suivante : **Comment organiser efficacement la gestion des droits d'accès aux fichiers et dossiers sous Linux pour assurer la sécurité des données en entreprise ?**

Pour y répondre, nous allons mettre en place un système de gestion des utilisateurs et des permissions basées sur :

- La **création d'utilisateurs et de groupes**
- L'attribution de **permissions spécifiques** sur les dossiers
- La mise en place de **tests de validation des accès**
- L'application des **bonnes pratiques de sécurité**

Objectifs du Projet :

- **Créer une structure claire et organisée** des permissions
- **Définir des règles strictes d'accès** en fonction des utilisateurs et groupes
- **Sécuriser les dossiers sensibles** en appliquant des permissions adaptées
- **Tester et valider** la mise en place des restrictions d'accès
- **Assurer une gestion centralisée** et évolutive des permissions
- **Comparer avec Windows Server** pour analyser les différences avec Linux

Application en Entreprise :

La gestion des droits d'accès est une problématique majeure dans tous les services informatiques. Voici quelques **exemples concrets d'application** en entreprise :

- **Service Comptabilité** : Restreindre l'accès aux fichiers financiers aux seuls membres du service comptable.
- **Service RH** : Assurer que seuls les responsables RH puissent accéder aux données confidentielles des employés.
- **Service IT** : Garantir que seuls les administrateurs système puissent modifier des configurations critiques.

Ce projet illustre une **mise en œuvre pratique et fonctionnelle** qui pourrait être appliquée dans une structure réelle, garantissant une **meilleure sécurité des données**.

Étape 1 : Création d’utilisateurs et gestion des permissions :

Pour commencer, nous passons en mode root afin d'éviter d'utiliser sudo avant chaque commande.

```
amine@debian:~$ su -
Mot de passe :
```

Nous créons deux utilisateurs : John, qui aura accès au dossier Dcompta, et User2, qui ne l'aura pas.

```
root@debian:~# adduser jhon
Ajout de l'utilisateur « jhon » ...
Ajout du nouveau groupe « jhon » (1001) ...
Ajout du nouvel utilisateur « jhon » (1001) avec le groupe « jhon » (1001) ...
Création du répertoire personnel « /home/jhon » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour jhon
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []: jhon
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]
Ajout du nouvel utilisateur « jhon » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « jhon » au groupe « users » ...
root@debian:~#
```

```
root@debian:~# adduser user2
Ajout de l'utilisateur « user2 » ...
Ajout du nouveau groupe « user2 » (1002) ...
Ajout du nouvel utilisateur « user2 » (1002) avec le groupe « user2 » (1002) ...
Création du répertoire personnel « /home/user2 » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour user2
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []: use2
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]
Ajout du nouvel utilisateur « user2 » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « user2 » au groupe « users » ...
root@debian:~#
```

Nous créons ensuite le dossier "dcompta" à la racine et vérifions qu'il a bien été créé.

```
root@debian:~# mkdir dcompta
root@debian:~# ls
dcompta
```

Après avoir exécuté la commande chown pour attribuer le dossier à John, vérifiez si le dossier a bien été attribué.

```
root@debian:~# chown jhon dcompta
root@debian:~# ls -l
total 4
drwxr-xr-x 2 jhon root 4096 11 mars  10:43 dcompta
root@debian:~#
```

Nous ajoutons la commande suivante :

```chmod 700 dcompta```

Afin de permettre uniquement à John d'accéder au fichier.

Pour tester, nous mettons l'invite de commande sur le profil de John.

```
amine@debian:~$ su - jhon
Mot de passe :
jhon@debian:~$
```

La commande cd / est utilisée pour revenir à la racine où se trouve le dossier.

```
jhon@debian:~$ cd /
jhon@debian:/$
```

Lorsque le chemin du fichier dcompta est indiqué, l'accès est accepté, permettant ainsi d'entrer dans le dossier.

```
jhon@debian:/$ cd dcompta
jhon@debian:/dcompta$
```

Nous vérifions si la commande *chmod* a été correctement intégrée au fichier.

```
jhon@debian:~$ su - user2
Mot de passe :
user2@debian:~$ cd /
user2@debian:/$ cd dcompta
-bash: cd: dcompta: Permission non accordée
user2@debian:/$
```

Comme nous pouvons le constater, l'accès a été refusé pour l'utilisateur user2.
```

Étape 2 : Gestion des groupes et accès avancés

Nous nous reconnaiton au compte « amine »

```
user2@debian:~$ su - amine
Mot de passe :
amine@debian:~$
```

Nous ajoutons un utilisateur pour tester le groupe. Le tex et John auront accès au dossier compta, tandis que user2 n'aura pas l'autorisation d'y accéder.

```
amine@debian:~$ sudo adduser tex
[sudo] Mot de passe de amine :
Ajout de l'utilisateur « tex » ...
Ajout du nouveau groupe « tex » (1003) ...
Ajout du nouvel utilisateur « tex » (1003) avec le groupe « tex » (1003) ...
Création du répertoire personnel « /home/tex » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour tex
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]
Ajout du nouvel utilisateur « tex » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « tex » au groupe « users » ...
amine@debian:~$
```

Nous créons le groupe compta via la commande `groupadd` et vérifions qu'il a bien été créé via la commande `cat / [chemin du fichier] `.

```
amine@debian:~$ sudo groupadd compta
amine@debian:~$ cat /etc/group
```

Le groupe est bien visible.

```
compta:x:1004:
```

Avec la commande usermode -AddGroup, l'utilisateur jhon et tex sont ajoutés au groupe.

```
amine@debian:~$ sudo usermod -aG compta jhon
amine@debian:~$ sudo usermod -aG compta tex
amine@debian:~$ getent group compta
compta:x:1004:jhon,tex
amine@debian:~$
```

Nous attribuons le fichier au groupe jhon, qui reste propriétaire du fichier, tandis que compta devient le groupe dont les utilisateurs peuvent lire et écrire via la commande chmod 770.

```
amine@debian:/$ sudo chown jhon dcompta
amine@debian:/$ sudo chgrp compta dcompta
amine@debian:/$ chmod 770 dcompta
```

7 (pour jhon (le propriétaire) → Peut lire, écrire et exécuter.

7 pour le groupe compta → Tous les membres du groupe compta peuvent aussi lire, écrire et exécuter.

0 (---) pour les autres utilisateurs → Aucun accès.)

Nous débutons les tests en nous connectant au profil tex, qui dispose des autorisations nécessaires pour accéder au fichier.

```
amine@debian:/$ su - tex
Mot de passe :
tex@debian:~$ cd /
tex@debian:/$ cd dcompta
tex@debian:/dcompta$ cd
```

Nous vérifions si l'user2 a accès au fichier.

```
tex@debian:~$ su - user2
Mot de passe :
user2@debian:~$ cd /
user2@debian:/$ cd dcompta
-bash: cd: dcompta: Permission non accordée
```

Comme indiqué dans la ligne de commande ci-dessous, l'autorisation n'a pas été accordée à user2.

Étape 3 : Gestion avancée des permissions sur plusieurs dossiers

Nous créons d'abord le dossier "laumor" à la racine.

```
amine@debian:/$ sudo mkdir laumor
[sudo] Mot de passe de amine :
amine@debian:/$ ls
bin      dev   initrd.img      lib         media  proc  sbin  tmp  vmlinuz
boot     etc   initrd.img.old  lib64       mnt    root  srv   usr  vmlinuz.old
dcompta  home  laumor          lost+found  opt    run   sys   var
```

Ensuite, nous ajoutons les fichiers tech, compta et direction dans le dossier Laumor et vérifions s'ils ont été correctement créés.

```
amine@debian:/laumor$ sudo mkdir tech
amine@debian:/laumor$ sudo mkdir compta
amine@debian:/laumor$ sudo mkdir direction
amine@debian:/laumor$ ls -l
total 12
drwxr-xr-x 2 root root 4096 11 mars  14:47 compta
drwxr-xr-x 2 root root 4096 11 mars  14:48 direction
drwxr-xr-x 2 root root 4096 11 mars  14:47 tech
```

Nous créerons 6 utilisateurs pour approfondir le test.

```
amine@debian:/$ sudo adduser pierre
amine@debian:/$ sudo adduser luc
amine@debian:/$ sudo adduser yassine
amine@debian:/$ sudo adduser bilal
amine@debian:/$ sudo adduser sandrine
amine@debian:/$ sudo adduser jules
```

Nous créons le groupe Glaumor pour accéder au dossier laumor et ajoutons tous nos utilisateurs avec la commande `gpasswd -M`. Puis, nous intégrons le groupe au fichier laumor via les commandes `chown` et `chgrp`.

Une erreur est apparue car la commande n'a pas été exécutée avec `sudo`, ce qui est nécessaire.

Ensuite, nous attribuons la règle `chmod 770` pour que seuls les utilisateurs du groupe puissent y accéder.

```
amine@debian:~$ sudo groupadd Glaumor
amine@debian:~$ sudo gpasswd -M pierre,luc,yassine,bilal,sandrine,jules Glaumor
amine@debian:~$ cd /
amine@debian:/$ sudo chown root:Glaumor laumor
amine@debian:/$ chgrp Glaumor laumor
chgrp: modification du groupe de 'laumor': Opération non permise
amine@debian:/$ sudo chgrp Glaumor laumor
amine@debian:/$ sudo chmod 770 laumor
```

Nous créerons des groupes pour accéder aux fichiers. Le fichier tech sera accessible à tous, tandis que seule la direction et la compta auront accès à leurs fichiers via leur groupe respectif.

```
amine@debian:/$ sudo groupadd direction
sudo groupadd compta
```

Nous ajoutons les utilisateurs à leur groupe respectif. La consigne donnée était :

- Pierre et Luc ont accès à tous les dossiers.
- Yassine et Bilal ont accès au dossier direction.
- Sandrine et Jules ont accès au dossier compta.

```
amine@debian:/$ sudo usermod -aG direction yassine
amine@debian:/$ sudo usermod -aG direction bilal
amine@debian:/$ sudo usermod -aG compta sandrine
amine@debian:/$ sudo usermod -aG compta jules
amine@debian:/$ sudo usermod -aG compta luc
amine@debian:/$ sudo usermod -aG direction luc
amine@debian:/$ sudo usermod -aG direction pierre
```

Nous attribuons les groupes aux utilisateurs

Nous ajoutons chaque groupe à son dossier et activons les règles avec la commande chmod 770.

```
amine@debian:/$ su
Mot de passe :
root@debian:/# cd /
root@debian:/# cd laumor
root@debian:/laumor# chown root:compta compta
root@debian:/laumor# chgrp compta compta
root@debian:/laumor# chmod 770 compta
root@debian:/laumor# chown root:direction direction
root@debian:/laumor# chgrp direction direction
root@debian:/laumor# chmod 770 direction
root@debian:/laumor# exit
```

Étape 4 : Vérification des autorisations d'accès au fichier

Yassine ne dispose pas des autorisations nécessaires pour accéder au fichier comptable.

```
yassine@debian:/laumor$ cd compta
bash: cd: compta: Permission non accordée
```

Toutefois, il dispose de l'accès au dossier de la direction.

```
yassine@debian:/laumor/direction$
```

Sandrine a accès à la compta.

```
sandrine@debian:/laumor$ cd compta
sandrine@debian:/laumor/compta$
```

Cependant elle n'a pas accès au fichier direction.

```
sandrine@debian:/laumor$ cd direction/
bash: cd: direction/: Permission non accordée
sandrine@debian:/laumor$
```

Luc a accès à tous les fichiers.

```
luc@debian:/laumor$ cd compta
luc@debian:/laumor/compta$
luc@debian:/laumor$ cd direction/
luc@debian:/laumor/direction$
```

Problèmes rencontrés et solutions :

Constat :

Après avoir utilisé chmod 770 et chown pour attribuer des permissions, certains utilisateurs n'avaient toujours pas accès aux fichiers.

Solution :

- **Vérifier que les utilisateurs appartiennent bien au groupe en utilisant : « Groups utilisateur »**
- **Rafraîchir la session de l'utilisateur pour appliquer les changements : « newgrp groupe »**

Constat :

Certaines commandes comme chown ou gpasswd renvoyaient une erreur d'autorisation.

Solution :

- **Exécuter les commandes en mode super-utilisateur :**

  « sudo chown utilisateur:dcompta dossier »
- **Vérifier que l'utilisateur a bien les droits sudo :**

  « sudo usermod -aG sudo utilisateur »

Constat :

La commande usermod -AddGroup a retourné une erreur.

Solution :

- **La bonne syntaxe est :**

  « sudo usermod -aG groupe utilisateur »
- **Vérifier que le groupe existe avec :**

  « cat /etc/group | grep nom_du_groupe »

Conclusion

Synthèse du Projet :

Grâce à ce projet, nous avons mis en place **une gestion avancée des permissions** permettant de **sécuriser les accès aux fichiers** selon les rôles des utilisateurs. Chaque utilisateur a été affecté à un groupe spécifique avec des **droits strictement définis**, garantissant ainsi un **meilleur contrôle des accès**.

Impact en Entreprise :

- **Sécurisation accrue des données sensibles**
- **Meilleure gestion des droits d'accès**
- **Maintenance facilitée grâce à une gestion centralisée des groupes**
- **Conformité aux normes de sécurité (ISO 27001, RGPD, etc.)**

Évolutions possibles :

- **Automatisation des permissions avec des scripts Shell**
- **Supervision des accès via un journal des connexions**
- **Comparaison avec les systèmes Windows et les solutions Active Directory**