

PROJET IT DOCUMENTATION

Gestion des Utilisateurs et Groupes
(RBAC & Permissions)

MORGAN BURERA

JUILLET 2025

Ubuntu, Terminal

Captures d'écrans

Annotations

```
Jul 28 02:12
morgan@morganclient:~$ awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd
morgan
user1
morgan@morganclient:~$
```

- Début de projet.
- Je vérifie les utilisateurs de ma machine.
- Il devrait y en avoir beaucoup plus mais la première commande me permet d'uniquement afficher les utilisateurs humain. C'est ce qui m'intéresse ici

```
Jul 28 02:13
morgan@morganclient:~$ sudo mkdir -p /srv/{HR,Finance,IT}
morgan@morganclient:~$ ls -l /srv/
total 12
drwxr-xr-x 2 root root 4096 Jul 28 02:12 Finance
drwxr-xr-x 2 root root 4096 Jul 28 02:12 HR
drwxr-xr-x 2 root root 4096 Jul 28 02:12 IT
morgan@morganclient:~$ sudo addgroup hr
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `hr' (GID 1002) ...
morgan@morganclient:~$ sudo addgroup finance
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `finance' (GID 1003) ...
morgan@morganclient:~$ sudo addgroup it
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `it' (GID 1004) ...
morgan@morganclient:~$ Ajout des groupes selon le secteur
```

- Création des répertoires pour chaque département
- Je vérifie également qu'ils ont bien été créés
- '**sudo addgroup hr**' me permet d'ajouter le nouveau groupe

Jul 28 02:16

```
morgan@morganclient:~
```

New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jacques
Enter the new value, or press ENTER for the default
 Full Name []:
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n]
info: Adding new user `jacques' to supplemental / extra groups `users' ...
info: Adding user `jacques' to group `users' ...
morgan@morganclient:~\$ sudo adduser cesar
info: Adding user `cesar' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `cesar' (1010) ...
info: Adding new user `cesar' (1010) with group `cesar (1010)' ...
warn: The home directory `/home/cesar' already exists. Not touching this directory.
warn: Warning: The home directory `/home/cesar' does not belong to the user you
are currently creating.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for cesar
Enter the new value, or press ENTER for the default
 Full Name []:
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n]
info: Adding new user `cesar' to supplemental / extra groups `users' ...
info: Adding user `cesar' to group `users' ...
morgan@morganclient:~\$ awk -F: '\$3 >= 1000 && \$3 != 65534 {print \$1}' /etc/passwd
morgan
user1
jean
paul
lisa
emma
jacques
cesar
morgan@morganclient:~\$

- Crédation des utilisateurs nécessaires au reste du projet.
- ‘**sudo adduser “nom_utilisateur”**’

Jul 28 02:19

```
morgan@morganclient:~$ awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd
morgan
user1
jean
paul
lisa
emma
jacques
cesar
morgan@morganclient:~$ sudo usermod -aG hr lisa
morgan@morganclient:~$ sudo usermod -aG hr emma
morgan@morganclient:~$ sudo usermod -aG finance jean
morgan@morganclient:~$ sudo usermod -aG finance cesar
morgan@morganclient:~$ sudo usermod -aG it jacques
morgan@morganclient:~$ sudo usermod -aG it kevin
usermod: user 'kevin' does not exist
morgan@morganclient:~$ sudo usermod -aG it paul
morgan@morganclient:~$ Ajout de chaque employé à son département.
```

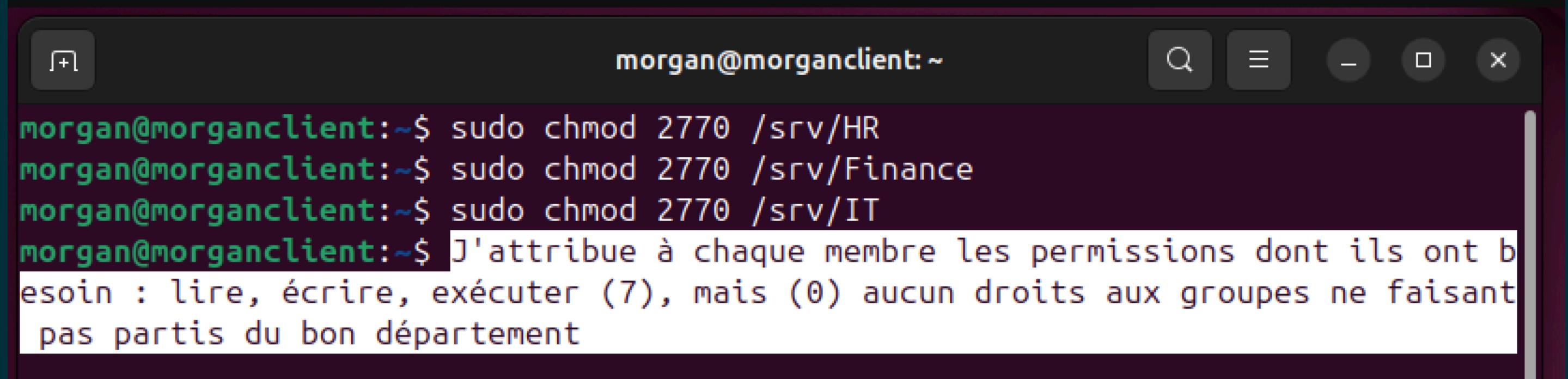
- Vérification des nouveaux utilisateurs implémenté précédemment.
- ‘**sudo usermod -aG hr lisa**’ permet d’ajouter lisa au groupe “hr”
- Ajout de chaque utilisateur à son département respectif.

Jul 28 02:21

```
morgan@morganclient:~$ sudo chown -R root:hr /srv/HR
morgan@morganclient:~$ sudo chown -R root:finance /srv/Finance
morgan@morganclient:~$ sudo chown -R root:hr /srv/IT
morgan@morganclient:~$ Ici j'ai attribué la propriété de chaque dossier au département dédié, ainsi seuls les personnes de chaque départements ne peuvent que consulter/modifier les documents qui les concernent.
```

- ‘**sudo chown -R root:hr /srv/HR**’ : J’indique à ma machine que les utilisateurs de hr sont maîtres du répertoire /HR/, en effet seulement ces utilisateurs peuvent le consulter, y écrire et le modifier.
- Idem pour le reste des groupes et répertoires

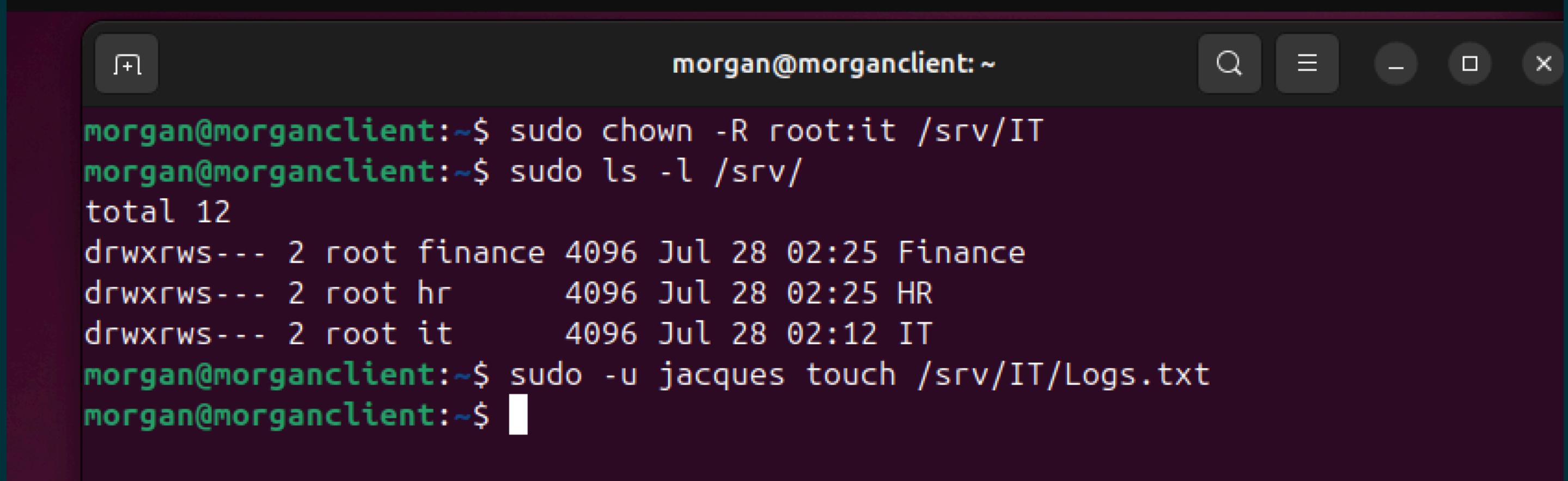
Jul 28 02:23



```
morgan@morganclient:~$ sudo chmod 2770 /srv/HR
morgan@morganclient:~$ sudo chmod 2770 /srv/Finance
morgan@morganclient:~$ sudo chmod 2770 /srv/IT
morgan@morganclient:~$ J'attribue à chaque membre les permissions dont ils ont besoin : lire, écrire, exécuter (7), mais (0) aucun droits aux groupes ne faisant pas parti du bon département
```

- Attribution des permissions des utilisateurs quant à leur département respectifs.

Jul 28 02:28



```
morgan@morganclient:~$ sudo chown -R root:it /srv/IT
morgan@morganclient:~$ sudo ls -l /srv/
total 12
drwxrws--- 2 root finance 4096 Jul 28 02:25 Finance
drwxrws--- 2 root hr      4096 Jul 28 02:25 HR
drwxrws--- 2 root it      4096 Jul 28 02:12 IT
morgan@morganclient:~$ sudo -u jacques touch /srv/IT/Logs.txt
morgan@morganclient:~$
```

- Ici j'ai voulu vérifier que les permissions ont bien été assignées.
- Pour cela j'ai utilisé 'jacques' pour créer un fichier 'Logs.txt' dans le répertoire IT.
- On peut voir que root (Moi, l'admin) possède tous' les droits sur chaque départements mais les départements également. En somme si 'jacques' est dans IT, alors 'jacques' peut y écrire, lire et exécuter chaque fichiers dans IT.

The screenshot shows a terminal window with the following content:

```
Jul 28 02:33
morgan@morganclient:~$ Vérifions les permissions accordées ^C
morgan@morganclient:~$ 
morgan@morganclient:~$ sudo ls -l /srv/HR
total 0
-rw-rw-r-- 1 lisa hr 0 Jul 28 02:25 Bienvenue.txt
morgan@morganclient:~$ sudo ls -l /srv/Finance
total 0
-rw-rw-r-- 1 jean finance 0 Jul 28 02:29 Sales.txt
morgan@morganclient:~$ sudo ls -l /srv/IT
total 0
-rw-rw-r-- 1 jacques it 0 Jul 28 02:27 Logs.txt
morgan@morganclient:~$ On a bien nos employés avec les bons droits sur les fichiers
aussi ils sont avant leur département car ils ont créer le fichiers eux mêmes. Enfin
les gens extérieur aux départements ne peuvent pas consulter ces fichiers car on ne
oit que "lisa hr 0" 0 signifiant qu'il n'y a pas d'autre groupe
```

- J'ai vérifié que les fichiers créés par les employés avaient les bonnes permissions.
- Grâce à '**sudo chmod 2700 -R root :"groupe" /srv/"Département/"**' utilisé juste avant.

Jul 28 02:34

morgan@morganclient:~

```
morgan@morganclient:~$ sudo adduser kevin
info: Adding user `kevin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `kevin' (1011) ...
info: Adding new user `kevin' (1011) with group `kevin (1011)' ...
warn: The home directory `/home/kevin' already exists. Not touching this directory.
warn: Warning: The home directory `/home/kevin' does not belong to the user you are currently creating.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for kevin
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
info: Adding new user `kevin' to supplemental / extra groups `users' ...
info: Adding user `kevin' to group `users' ...
morgan@morganclient:~$ sudo usermod -aG finance kevin
morgan@morganclient:~$ sudo -u kevin touch /srv/Finance/test_kevin.txt
morgan@morganclient:~$ sudo ls -l /srv/Finance
total 0
-rw-rw-r-- 1 jean  finance 0 Jul 28 02:29 Sales.txt
-rw-rw-r-- 1 kevin finance 0 Jul 28 02:34 test_kevin.txt
morgan@morganclient:~$
```

- Premier scénario : Arrivée d'un nouvel employé.
- Je lui attribue un groupe.
- Je créer un fichier avec fichier avec cet utilisateur.
- Puis je vérifie le contenu de son département afin de vérifier qu'il a bien hérité des permissions attribué à son groupe : Oui.
- **'sudo ls -l /srv/Finance'** Pour consulter le contenu de son répertoire.
- L'usage de sudo était mandataire ici car d'après les permissions, tout utilisateur ne faisant pas partie de Finance n'y aura pas accès.
L'utilisation du profil root (administrateur est donc requis).

Jul 28 02:38

```
morgan@morganclient:~$ awk -F: '$3 >= 1000 && $3 != 65534 {print $1}' /etc/passwd
morgan
user1
jean
paul
emma
jacques
cesar
kevin
morgan@morganclient:~$ sudo userdel -r /home/lisa
userdel: user '/home/lisa' does not exist
morgan@morganclient:~$ ls -l /home
total 56
drwxr-x--- 2 paul paul 4096 Jul 27 23:21 alice
drwxr-x--- 2 1007 1007 4096 Jul 27 23:22 bob
drwxr-x--- 2 1007 1007 4096 Jul 27 20:53 cesar
drwxr-x--- 2 emma emma 4096 Jul 27 23:22 claire
drwxr-x--- 2 jacques jacques 4096 Jul 27 23:22 david
drwxr-x--- 14 cesar cesar 4096 Jul 27 23:43 emma
drwxr-x--- 2 1004 it 4096 Jul 26 19:09 jacques
drwxr-x--- 2 paul paul 4096 Jul 27 20:51 jean
drwxr-x--- 14 1002 hr 4096 Jul 26 19:33 kevin
drwxr-x--- 2 jean jean 4096 Jul 26 19:09 lisa
drwxr-x--- 17 morgan morgan 4096 Jul 27 23:26 morgan
drwxr-x--- 2 1015 1015 4096 Jul 27 21:12 nathalie
drwxr-x--- 2 1003 finance 4096 Jul 26 19:09 paul
drwxr-x--- 2 user1 user1 4096 Jul 8 16:28 user1
morgan@morganclient:~$ id lisa
id: 'lisa': no such user
morgan@morganclient:~$ sudo rm -r /home/lisa
morgan@morganclient:~$ ls -l /home
total 52
drwxr-x--- 2 paul paul 4096 Jul 27 23:21 alice
drwxr-x--- 2 1007 1007 4096 Jul 27 23:22 bob
drwxr-x--- 2 1007 1007 4096 Jul 27 20:53 cesar
drwxr-x--- 2 emma emma 4096 Jul 27 23:22 claire
drwxr-x--- 2 jacques jacques 4096 Jul 27 23:22 david
drwxr-x--- 14 cesar cesar 4096 Jul 27 23:43 emma
drwxr-x--- 2 1004 it 4096 Jul 26 19:09 jacques
drwxr-x--- 2 paul paul 4096 Jul 27 20:51 jean
drwxr-x--- 14 1002 hr 4096 Jul 26 19:33 kevin
drwxr-x--- 17 morgan morgan 4096 Jul 27 23:26 morgan
drwxr-x--- 2 1015 1015 4096 Jul 27 21:12 nathalie
drwxr-x--- 2 1003 finance 4096 Jul 26 19:09 paul
drwxr-x--- 2 user1 user1 4096 Jul 8 16:28 user1
morgan@morganclient:~$
```

- Voici une vue plus exhaustive qui me permet de vérifier tous mes utilisateurs et leur permissions
- Scénario 2 : Un employé quitte l'entreprise : 'lisa'
• **'sudo deluser lisa'** j'ai aussi supprimé son numéro d'identification. Après actualisation 'lisa' n'existe plus et la machine a été nettoyé de sa présence.

```
Jul 28 02:40
morgan@morganclient:~$ groups emma
emma : emma users hr
morgan@morganclient:~$ sudo gpasswd -d emma hr
Removing user emma from group hr
morgan@morganclient:~$ sudo usermod -aG finance emma
morgan@morganclient:~$ sudo ls -l /srv/Finance
total 0
-rw-rw-r-- 1 jean  finance 0 Jul 28 02:29 Sales.txt
-rw-rw-r-- 1 kevin  finance 0 Jul 28 02:34 test_kevin.txt
morgan@morganclient:~$ sudo -u emma touch /srv/Finance/EmmaTest.txt
morgan@morganclient:~$ sudo ls -l /srv/Finance
total 0
-rw-rw-r-- 1 emma  finance 0 Jul 28 02:40 EmmaTest.txt
-rw-rw-r-- 1 jean  finance 0 Jul 28 02:29 Sales.txt
-rw-rw-r-- 1 kevin  finance 0 Jul 28 02:34 test_kevin.txt
morgan@morganclient:~$ groups emma
emma : emma users finance
morgan@morganclient:~$
```

- Scénario 3 : Un employé doit changer de département : emma
- '**sudo gpasswd -d emma hr**' pour retirer emma de 'hr', ensuite c'est les mêmes commandes qu'auparavant.
- Emma a créer un fichier dans Finance, les permissions attendues sont correctes.
- '**groups emma**' permet de consulter les groupes dont emma fait partie (au cas où elle était toujours présente dans 'hr'

Jul 28 02:40

morgan@morganclient: ~

Q _ x

```
input:x:995:  
sgx:x:994:  
kvm:x:993:  
render:x:992:  
messagebus:x:101:  
syslog:x:102:  
systemd-resolve:x:991:  
uuidd:x:103:  
_ssh:x:104:  
tss:x:105:  
ssl-cert:x:106:  
systemd-oom:x:990:  
bluetooth:x:107:  
rdma:x:108:  
whoopsie:x:109:  
netdev:x:110:  
avahi:x:111:  
tcpdump:x:112:  
sssd:x:113:  
lpadmin:x:114:morgan  
fwupd-refresh:x:989:  
scanner:x:115:saned  
saned:x:116:  
geoclue:x:117:  
pipewire:x:118:  
gnome-remote-desktop:x:988:  
polkitd:x:987:  
rtkit:x:119:  
colord:x:120:  
gdm:x:121:  
lxde:x:123:  
gamemode:x:986:  
gnome-initial-setup:x:985:  
morgan:x:1000:  
wireshark:x:124:  
user1:x:1001:  
hr:x:1002:  
finance:x:1003:jean,cesar,kevin,emma  
it:x:1004:jacques,paul  
jean:x:1005:  
paul:x:1006:  
emma:x:1008:  
jacques:x:1009:  
cesar:x:1010:  
kevin:x:1011:
```

morgan@morganclient:~\$

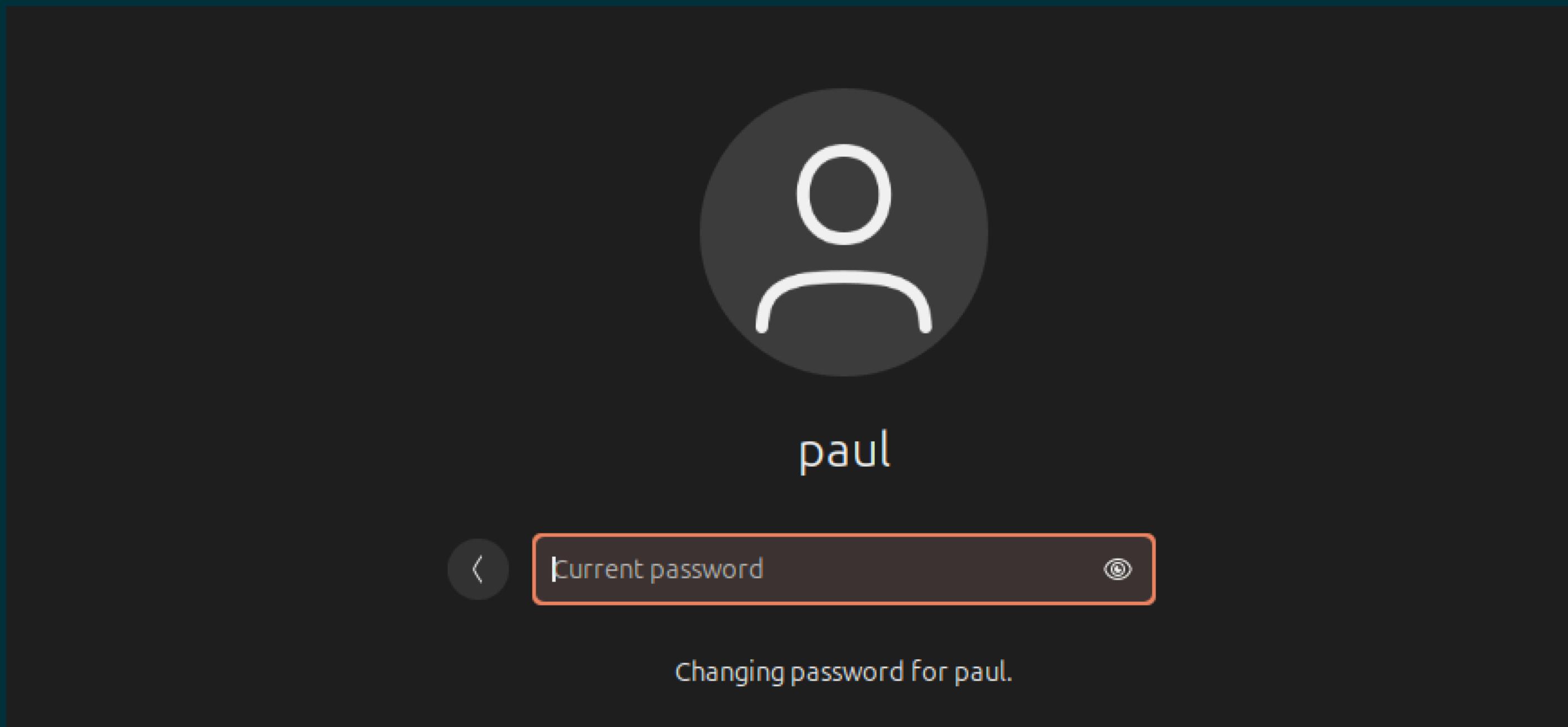
- ‘**getent group**’ afin de voir tous les groups, ici non filtré comme précédemment
- le groupe ‘finance’ contient quatre membres, dont emma qui a été récemment ajouté.

Jul 28 02:41

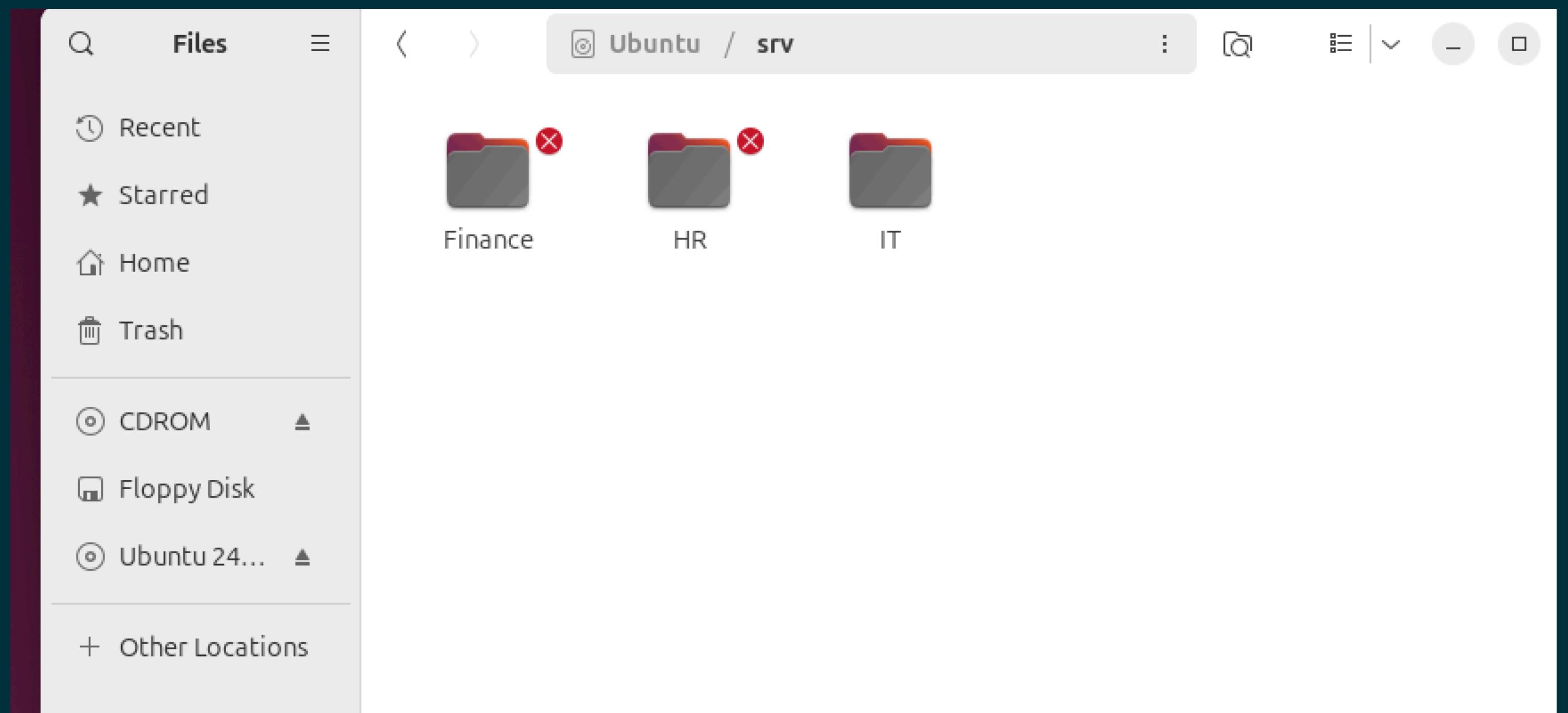
morgan@morganclient:~

```
morgan@morganclient:~$ sudo passwd paul
New password:
Retype new password:
passwd: password updated successfully
morgan@morganclient:~$ sudo chage -d 0 paul
morgan@morganclient:~$
morgan@morganclient:~$ J'ai changé le mdp de Paul, il devra le modifier à sa prochaine
connexion
```

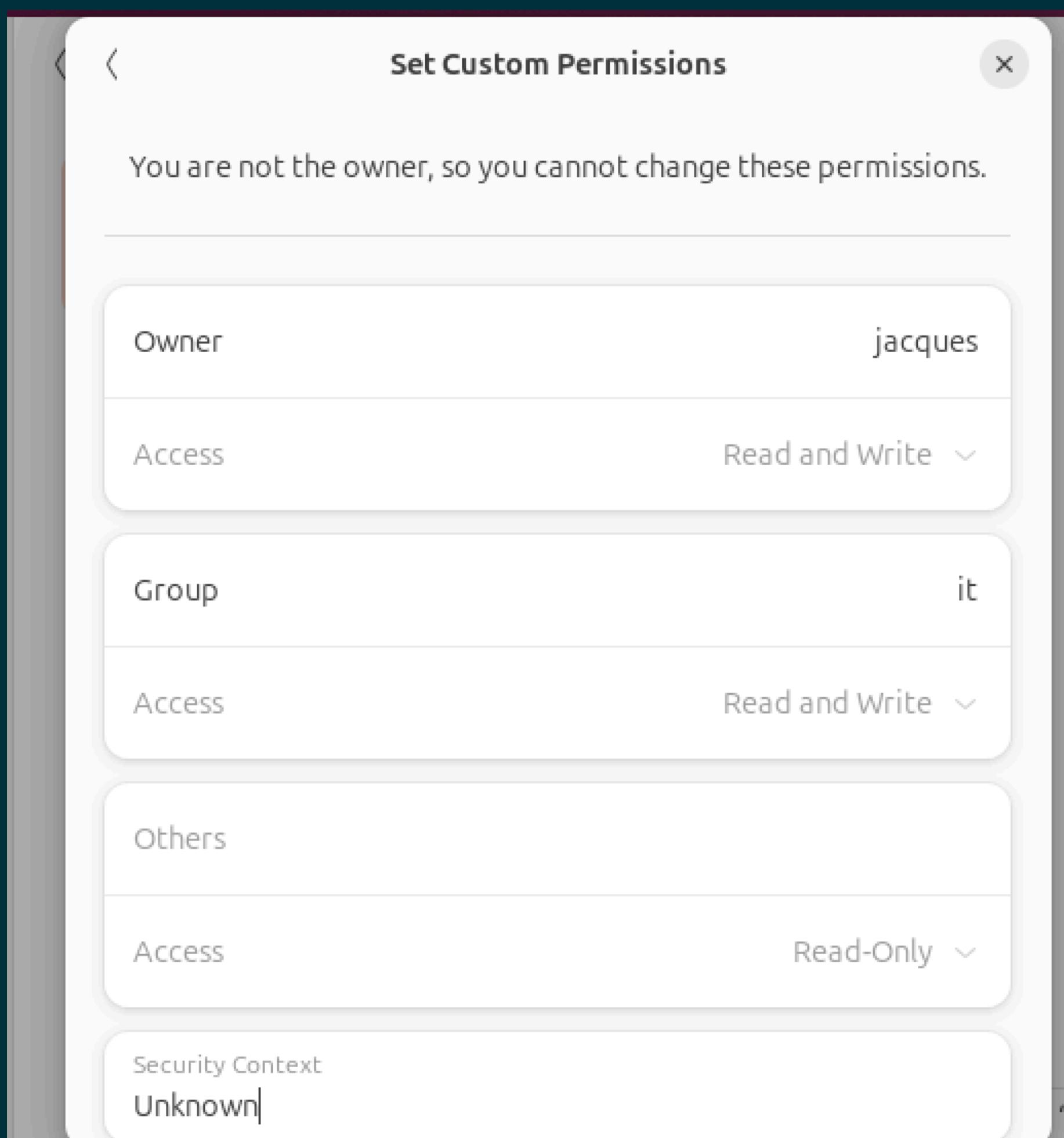
- Scénario 4 : Un employé a perdu son mot de passe.
- '**sudo passwd**' pour le modifier
- '**sudo chage -d 0 paul**' pour expirer le mot de passe de 'paul'.



- En lui donnant son nouveau mot de passe, 'paul' devra l'entrer puis insérer un nouveau mot de passe.

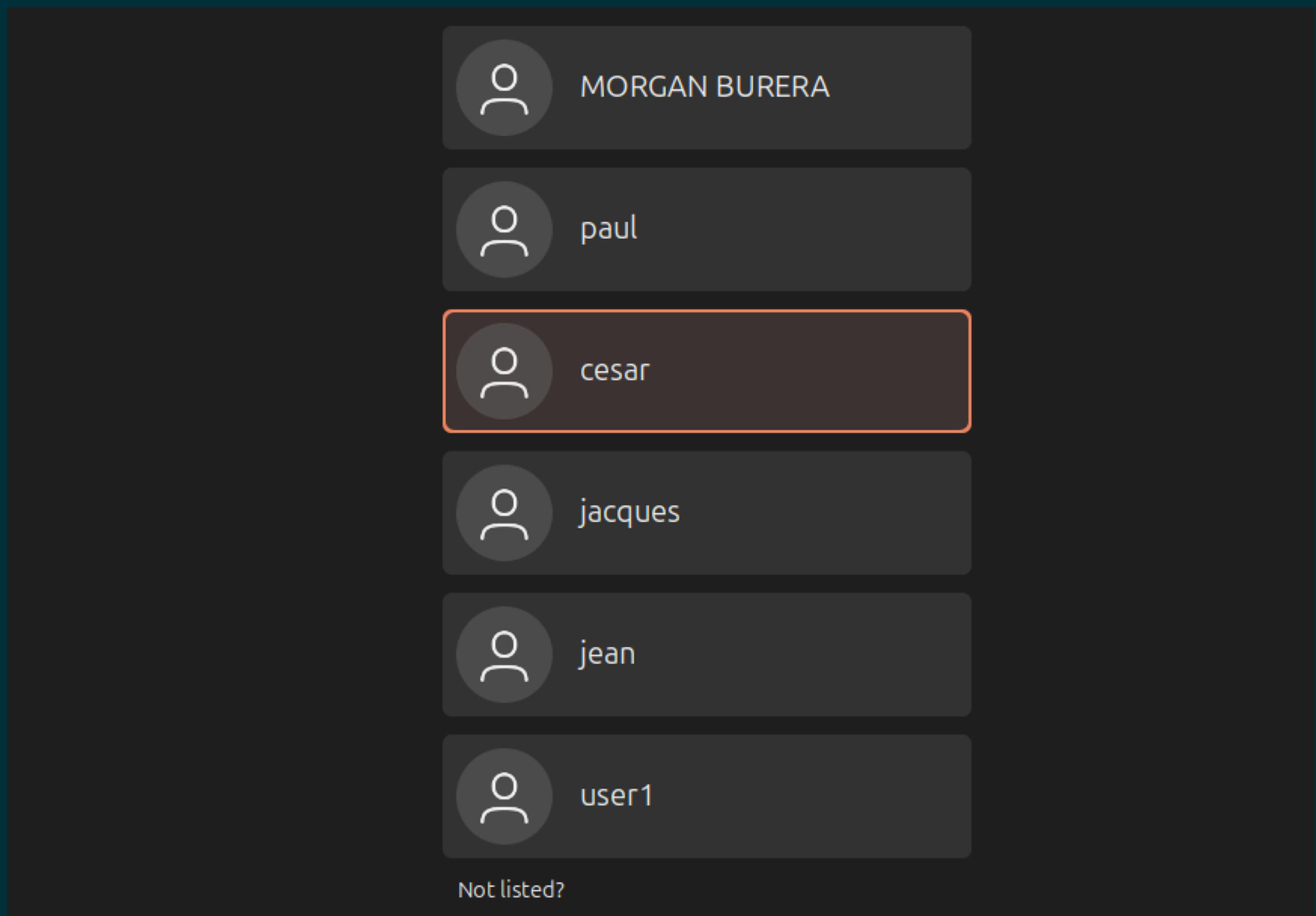


- Ici je suis connecté sur le profil 'jacques'.
- jacques ne peut consulter que le répertoire IT, son département.
- La machine me demande le mot-de-passe de l'administrateur afin de consulter les deux autres départements. Information que 'jacques' n'est pas sensé connaître.



```
Jul 28 02:48
morgan@morganclient:~$ sudo passwd -l emma
passwd: password changed.
morgan@morganclient:~$
```

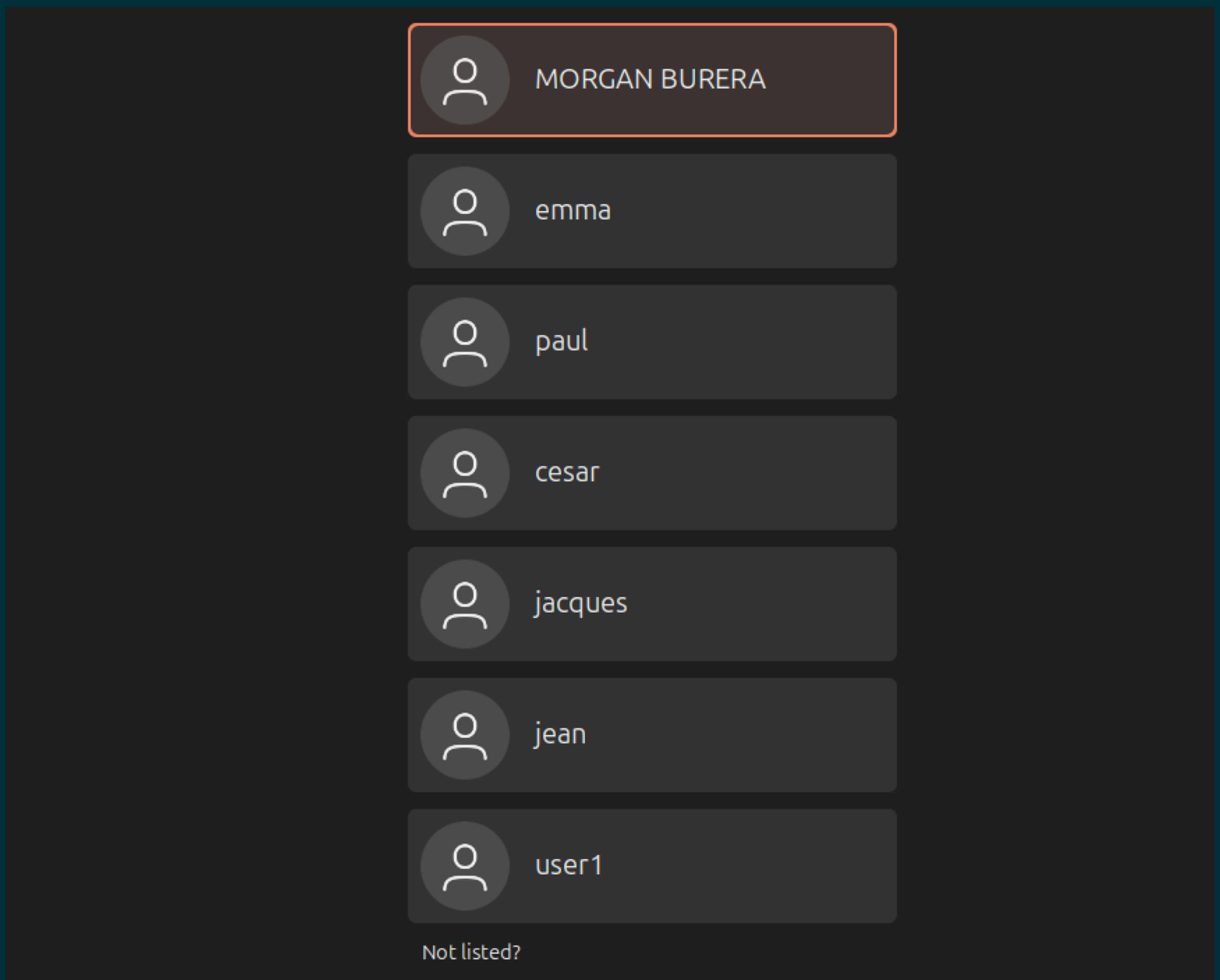
- Scénario 5 : Blocage d'un employé malveillant.
- '**sudo passwd -l emma**' bloque le profil de 'emma', elle ne pourra pas se connecter car le profil ne sera plus présent.



- Résultat attendu : OK

```
Jul 28 02:48
morgan@morganclient:~$ sudo passwd -l emma
passwd: password changed.
morgan@morganclient:~$ sudo passwd -u emma
passwd: password changed.
morgan@morganclient:~$
```

- ‘**sudo passwd -u emma**’ Débloquage du compte qui posait problème.



- Emma peut à nouveau se connecter

Jul 28 02:49

morgan@morganclient:~

```
morgan@morganclient:~$ sudo passwd -l emma
passwd: password changed.
morgan@morganclient:~$ sudo passwd -u emma
passwd: password changed.
morgan@morganclient:~$ sudo passwd -u kevin
passwd: password changed.
morgan@morganclient:~$
```

- Je change le mot-de passe afin d'éviter tout corruption.

Jul 28 02:53

morgan@morganclient:~

```
morgan@morganclient:~$ sudo addgroup stagiaires
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `stagiaires' (GID 1007) ...
morgan@morganclient:~$ sudo adduser hubert
info: Adding user `hubert' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `hubert' (1012) ...
info: Adding new user `hubert' (1012) with group `hubert (1012)' ...
info: Creating home directory `/home/hubert' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hubert
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []
Is the information correct? [Y/n] y
info: Adding new user `hubert' to supplemental / extra groups `users' ...
info: Adding user `hubert' to group `users' ...
morgan@morganclient:~$ sudo usermod -aG stagiaires hubert
morgan@morganclient:~$
```

- Scénario 6 (Bonus) : Nouvel employé, un stagiaire.

Jul 28 02:58

morgan@morganclient:~

```
morgan@morganclient:~$ groups hubert
hubert : hubert users stagiaires
morgan@morganclient:~$ sudo chown -R root:it /srv/IT
morgan@morganclient:~$ sudo chmod -R 770 /srv/IT
morgan@morganclient:~$ sudo setfacl -m g:stagiaires:rx /srv/IT
morgan@morganclient:~$ sudo setfacl -R -m g:stagiaires:rX /srv/IT
morgan@morganclient:~$ getfacl /srv/IT
getfacl: Removing leading '/' from absolute path names
# file: srv/IT
# owner: root
# group: it
# flags: -s-
user::rwx
group::rwx
group:stagiaires:r-x
mask::rwx
other::---
morgan@morganclient:~$
```

- Je souhaite que le stagiaire en IT puisse accéder au répertoire de son département mais en lecture unique, afin de consulter les documentations et d'éventuels articles. Cette mesure est prise afin d'éviter modification de documents sensibles.
- Néanmoins il appartient au groupe 'stagiaire'.
- 'hubert' aura toutes les permissions dans le répertoire Stagiaire ainsi que ses autres membres.

```
Jul 28 03:01
morgan@morganclient:~$ sudo -u hubert ls /srv/IT
Logs.txt
morgan@morganclient:~$ sudo -u hubert cat /srv/IT/Logs.txt
Logs sensibles !
morgan@morganclient:~$ sudo -u hubert touch /srv/IT/Logs.txt
touch: cannot touch '/srv/IT/Logs.txt': Permission denied
morgan@morganclient:~$ █
```

- ‘hubert’ ne peut pas créer de fichiers dans IT.
- Cette permission ne sera accordée que dans un cadre spécial.
- Je préfère utiliser la mentalité de “Accorder si besoin au fur et à mesure” plutôt que de tout accorder en avance et rencontrer des problèmes dans le futur.

```
Jul 28 03:07
morgan@morganclient:~$ getfacl /srv/IT
getfacl: Removing leading '/' from absolute path names
# file: srv/IT
# owner: root
# group: it
# flags: -s-
user::rwx
group::rwx
group:stagiaires:r-x
mask::rwx
other::---
```

```
morgan@morganclient:~$ █
```

- ‘**getfacl srv/IT**’ me permet de vérifier les permissions des utilisateurs dans coeur de IT.
- Les stagiaires ont : lire, exécuter
- les utilisateurs dans ‘it’ : lire, écrire, exécuter = modifier
- le maître est l’administrateur mais aussi les gens dans ‘it’

```
Jul 28 03:07
morgan@morganclient:~$ getfacl /srv/IT
getfacl: Removing leading '/' from absolute path names
# file: srv/IT
# owner: root
# group: it
# flags: -s-
user::rwx
group::rwx
group:stagiaires:r-x
mask::rwx
other::---
morgan@morganclient:~$ getfacl /srv/IT/Stagiaires
getfacl: /srv/IT/Stagiaires: Permission denied
morgan@morganclient:~$ sudo getfacl /srv/IT/Stagiaires
getfacl: Removing leading '/' from absolute path names
# file: srv/IT/Stagiaires
# owner: root
# group: stagiaires
# flags: -s-
user::rwx
group::rwx
other::---
morgan@morganclient:~$
```

- Comme dit précédemment les stagiaires ont néanmoins tous les droits dans leur propre répertoire. Car aucun fichier sensible pour l'entreprise n'y circule car géré par les administrateurs.

Jul 28 03:09

```
morgan@morganclient:~$ sudo -u hubert ls /srv/IT
Logs.txt  Stagiaires
morgan@morganclient:~$ sudo -u hubert cat /srv/IT/Logs.txt
Logs sensibles !
morgan@morganclient:~$ sudo -u hubert touch /srv/IT/test.txt
touch: cannot touch '/srv/IT/test.txt': Permission denied
morgan@morganclient:~$ sudo -u hubert touch /srv/IT/Stagiaires/test.txt
ls: cannot access '/srv/IT/Stagiaires': Permission denied
morgan@morganclient:~$ sudo ls -l /srv/IT/stagiaires
ls: cannot access '/srv/IT/stagiaires': No such file or directory
morgan@morganclient:~$ sudo ls -l /srv/IT/Stagiaires
total 0
-rw-rw-r-- 1 hubert stagiaires 0 Jul 28 03:08 test.txt
morgan@morganclient:~$
```

- Je tente de créer un fichier dans IT avec 'hubert' l'accès est refusé
- Le projet se termine sur la création d'un fichier 'test.txt' par 'hubert' dans le répertoire Stagiaires, les bonnes permissions sont présentes.
- Résultats globaux : OK !



Parties à ignorer contenant des erreurs de syntaxes.