CindLine-Tech

Mise en place d'un serveur Linux pour la société FormaTech

Céline FERRIERES / CindLine-Tech

Sommaire

1) Reformulation du besoin

FormaTech souhaite la mise en place d'un serveur Linux (Ubuntu) pour la gestion des fichiers log de son système d'authentification par badge.

Pour la mise en place du serveur Linux la société FormaTech souhaite:

- La création de deux dossiers, LOG et SCRIPT.
- La gestion de deux groupes Info et Tech avec 3 utilisateurs par groupe et des droits propres à chaque groupe pour les dossiers.
- La création d'un compte badge avec des droits spécifiques sur les dossiers pour les besoins du système badge.
- La mise en place d'un accès SSH accessible à tous les utilisateurs sauf root.
- La mise en place d'un fail2ban pour protéger les accès.

2) Analyse de l’existant

La société FormaTech dispose de deux sites un à Paris et un à Marseille. Elle vient d'installer sur ses sites un système d'authentification par badge.

La connexion entre le serveur et le système de badge sera faite par une société extérieure.

La société FormaTech ne possède aucun serveur Linux donc tout est à mettre en place.

Ce qui existe sur le marché

- VirtualBox
- Ubuntu
- OpenSSH
- Fail2ban

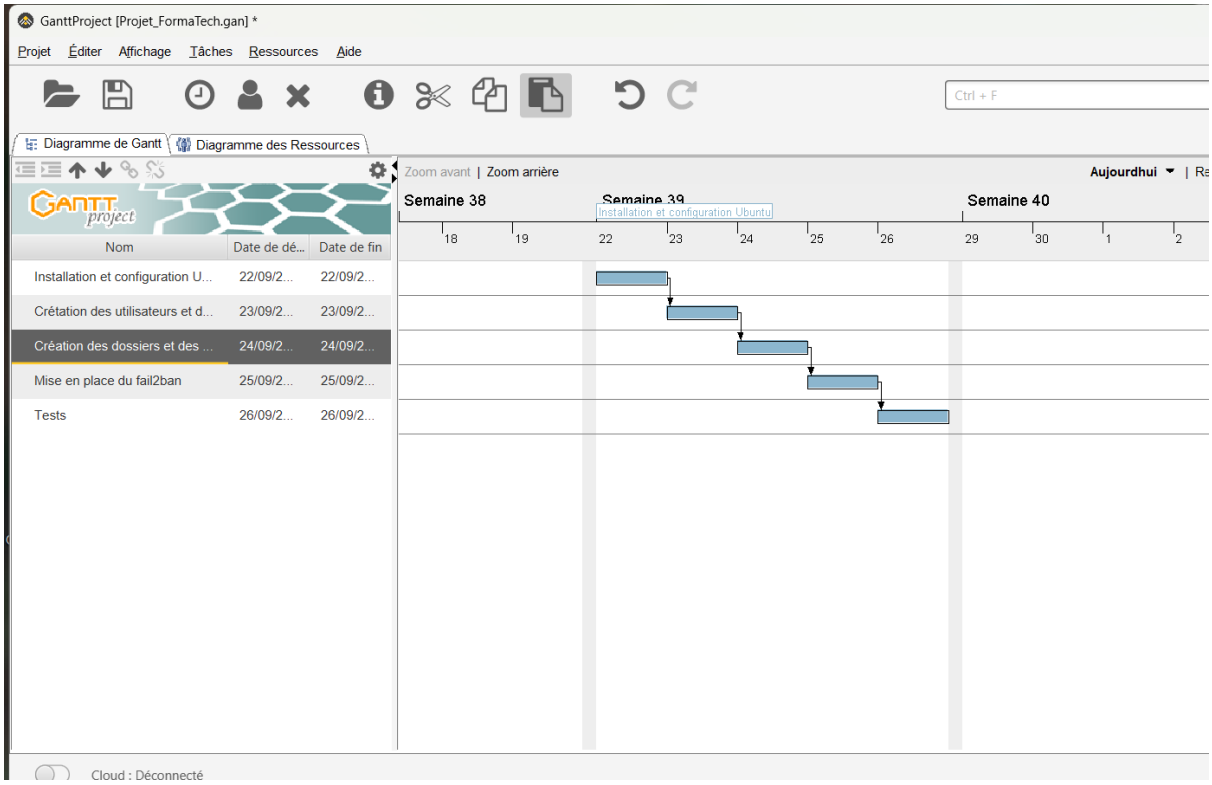
3) Proposition de solution

3.1) Description

La création et la configuration du serveur Linux seront réalisés selon les étapes suivantes:

- Création et configuration de la machine virtuelle avec VirtualBox
- Installation du système d'exploitation Ubuntu 22.04 lts
- Création des six utilisateurs et des groupes Info et Tech
- Création du compte badge
- Installation et configuration d'OpenSSH
- Création des dossiers LOG et SCRIPT et configuration des accès
- Installation et configuration de fail2ban

3.2) Planification



4) Mise en place

4.1) Mise en place du serveur Linux (Ubuntu)

Création de la machine virtuelle sur Virtual box avec

- Mémoire vive: 2048 Mo
- Processeur : 2 cœurs
- Disque dur: 25Go
- Accès au réseau par pont

Installation du système d'exploitation Ubuntu-22.04.5-desktop-amd 64 ISO

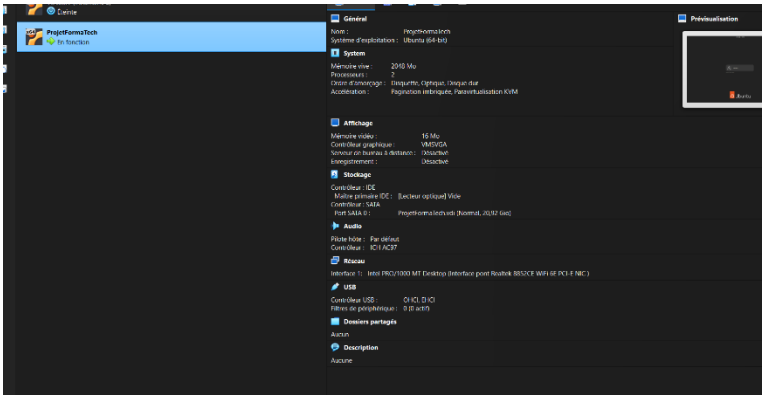
Passage à la racine avec la commande: cd /

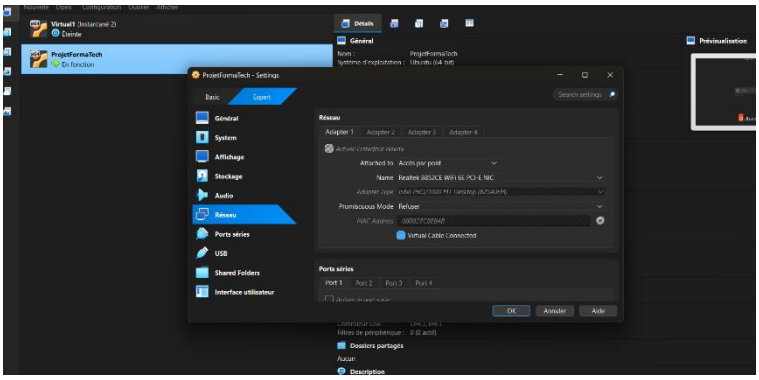
Recherche et installation des mises à jour: sudo apt uddate

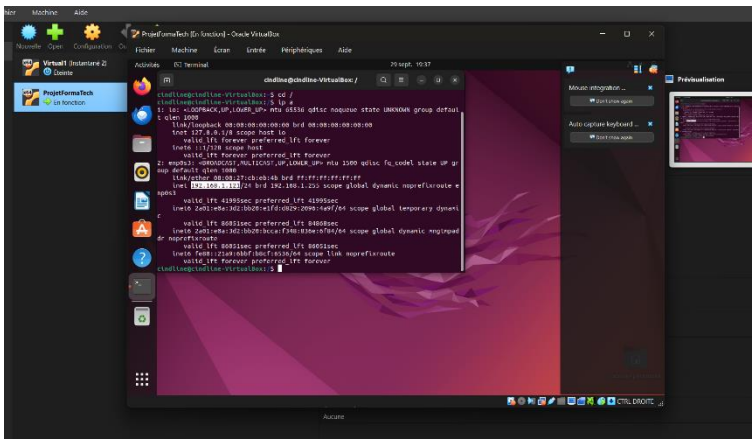
Installation des mises à jour : sudo apt upgrade

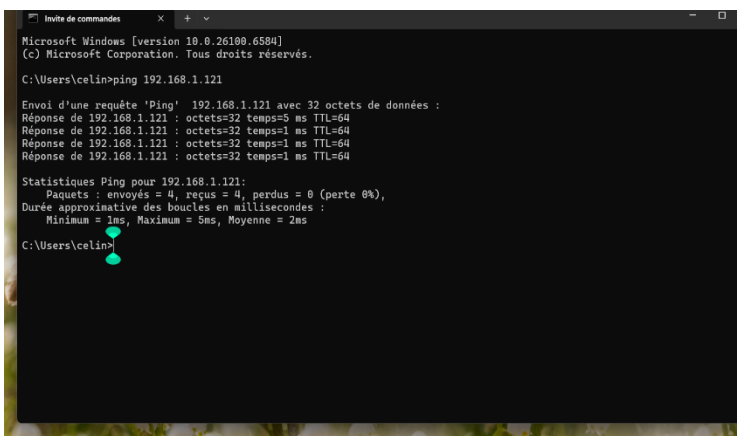
Tests:

- La VM démarre.
- Ubuntu est bien installé
- Ping via le PC hôte de l'IP de la VM. La connexion est faites.
- Mise à jour installées sans erreurs.









4.2) Création des utilisateurs, du compte badge et des groupes "info" et "tech"

- Création des groupe "info" et "tech" : sudo addgroup nomgroupe

```
Fait.
cindline@cindline-VirtualBox:/$ sudo addgroup info
Ajout du groupe « info » (GID 1001)...
Fait.
cindline@cindline-VirtualBox:/$ sudo addgroup tech
Ajout du groupe « tech » (GID 1002)...
Fait.
cindline@cindline-VirtualBox:/$
```

- Création des utilisateurs avec la commande : sudo adduser name

```
cindline@cindline-VirtualBox: /
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
cindline@cindline-VirtualBox:/$ sudo adduser deuxtech
Ajout de l'utilisateur « deuxtech » ...
Ajout du nouveau groupe « deuxtech » (1007) ...
Ajout du nouvel utilisateur « deuxtech » (1005) avec le groupe « deuxtech » ...
Le répertoire personnel « /home/deuxtech » existe déjà.  Rien n'est copié depuis « /etc/skel ».
adduser : Attention ! Le répertoire personnel « /home/deuxtech » n'appartient pas à l'utilisateur que vous êtes en train de créer.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe contient le nom d'utilisateur sous une forme
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour deuxtech
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []: deuxtech
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
cindline@cindline-VirtualBox:/$ sudo adduser troistech
Ajout de l'utilisateur « troistech » ...
Ajout du nouveau groupe « troistech » (1008) ...
Ajout du nouvel utilisateur « troistech » (1006) avec le groupe « troistech » ...
Le répertoire personnel « /home/troistech » existe déjà.  Rien n'est copié depuis « /etc/skel ».
adduser : Attention ! Le répertoire personnel « /home/troistech » n'appartient pas à l'utilisateur que vous êtes en train de créer.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe contient le nom d'utilisateur sous une forme
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour troistech
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []: troistech
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
cindline@cindline-VirtualBox:/$
```

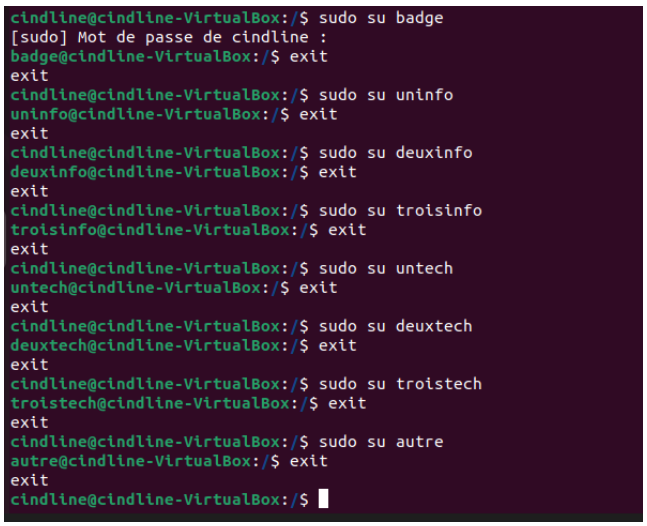
- Création du compte badge et du compte autre

```
cindline@cindline-VirtualBox:~$ cd /
cindline@cindline-VirtualBox:/$ sudo adduser badge
[sudo] Mot de passe de cindline :
Ajout de l'utilisateur « badge » ...
Ajout du nouveau groupe « badge » (1009) ...
Ajout du nouvel utilisateur « badge » (1007) avec le groupe « badge » ...
Création du répertoire personnel « /home/badge » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour badge
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
        NOM []: badge
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
cindline@cindline-VirtualBox:/$ sudo adduser autre
Ajout de l'utilisateur « autre » ...
Ajout du nouveau groupe « autre » (1010) ...
Ajout du nouvel utilisateur « autre » (1008) avec le groupe « autre » ...
```

- Ajout des utilisateurs dans leur groupe respectif: sudo usermod -ag nomgroupe nomutilisateur

Test :

- Présence de tous les utilisateurs avec la commande: sudo su utilisateur



- Affichage des utilisateurs par groupe avec la commande: sudo getent group nomgroup. (commande trouver sur malekal.com via google)

  Les utilisateurs uninfo, deuxinfo, troisinfo sont bien dans le groupe info.
  Les utilisateurs untech, deuxtech et troistech sont bien dans le groupe tech
  (voir capture ajout des utilisateurs dans leur groupe respectif)

4.3) Création des dossier "LOG" et "SCRIPT" et attribution des droits

- Création des dossier "LOG" et "SCRIPT" avec la commande: sudo mkdir nomdossier

```
ne@cindline-VirtualBox:/$ sudo mkdir log
ne@cindline-VirtualBox:/$ sudo mkdir script
```

- Attribution des droits du dossier "LOG"
  Le compte badge sera le propriétaire avec Lecture, Ecriture et Exécution soit 7.
  Création d'un groupe commun pour tous les utilisateurs des groupes "info" et "tech" qui ont les mêmes droits dans ce dossier.

```
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech uninfo
cindline@cindline-VirtualBox:/$ sudo groups uninfo
uninfo : uninfo info formatech
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech deuxinfo
cindline@cindline-VirtualBox:/$ sudo groups deuxinfo
deuxinfo : deuxinfo info formatech
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech troisinfo
cindline@cindline-VirtualBox:/$ sudo groups troisinfo
troisinfo : troisinfo info formatech
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech untech
cindline@cindline-VirtualBox:/$ sudo groups untech
untech : untech tech formatech
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech deuxtech
cindline@cindline-VirtualBox:/$ sudo groups deuxtech
deuxtech : deuxtech tech formatech
cindline@cindline-VirtualBox:/$ sudo usermod -aG formatech troistech
cindline@cindline-VirtualBox:/$ sudo groups troistech
troistech : troistech tech formatech
cindline@cindline-VirtualBox:/$
```

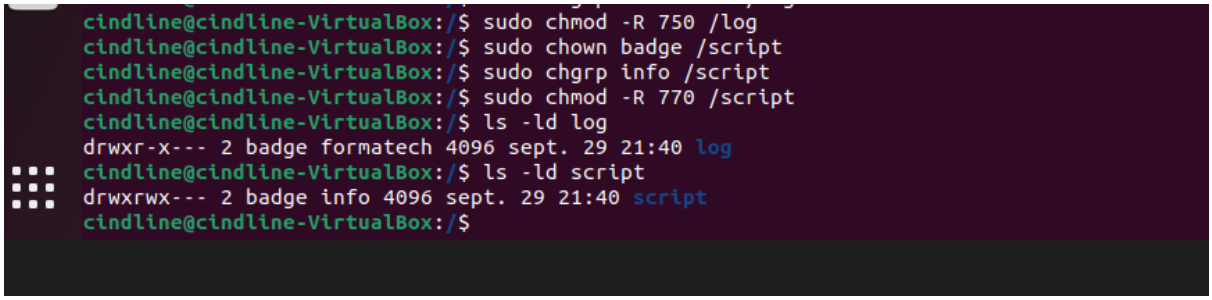
  Le groupe formatech sera le groupe propriétaire avec Lecture et Exécution soit 5.
  Les autre sans droit ont 0.

- Attribution des droits du dossier "SCRIPT"
  Le compte badge sera le propriétaire avec Lecture, Ecriture et Exécution soit 7.
  Le groupe info sera le groupe propriétaire avec Lecture, Ecriture et Exécution soit 7.
  Les autres sans droit ont 0.
  La récursive (-R) permettra que les droits soient conservés sur les futurs fichiers mis dans ces dossiers

```
ne@cindline-VirtualBox:/$ sudo chown badge /log
] Mot de passe de cindline :
ine@cindline-VirtualBox:/$ sudo chgroup formatech /log
 chgroup : commande introuvable
ine@cindline-VirtualBox:/$ sudo chgrp formatech /log
ine@cindline-VirtualBox:/$ sudo chmod -R 750 /log
ine@cindline-VirtualBox:/$ sudo chown badge /script
ne@cindline-VirtualBox:/$ sudo chgrp info /script
ne@cindline-VirtualBox:/$ sudo chmod -R 770 /script
ine@cindline-VirtualBox:/$
```

Tests :

- Affichage des droits avec la commande ls -ld dossier



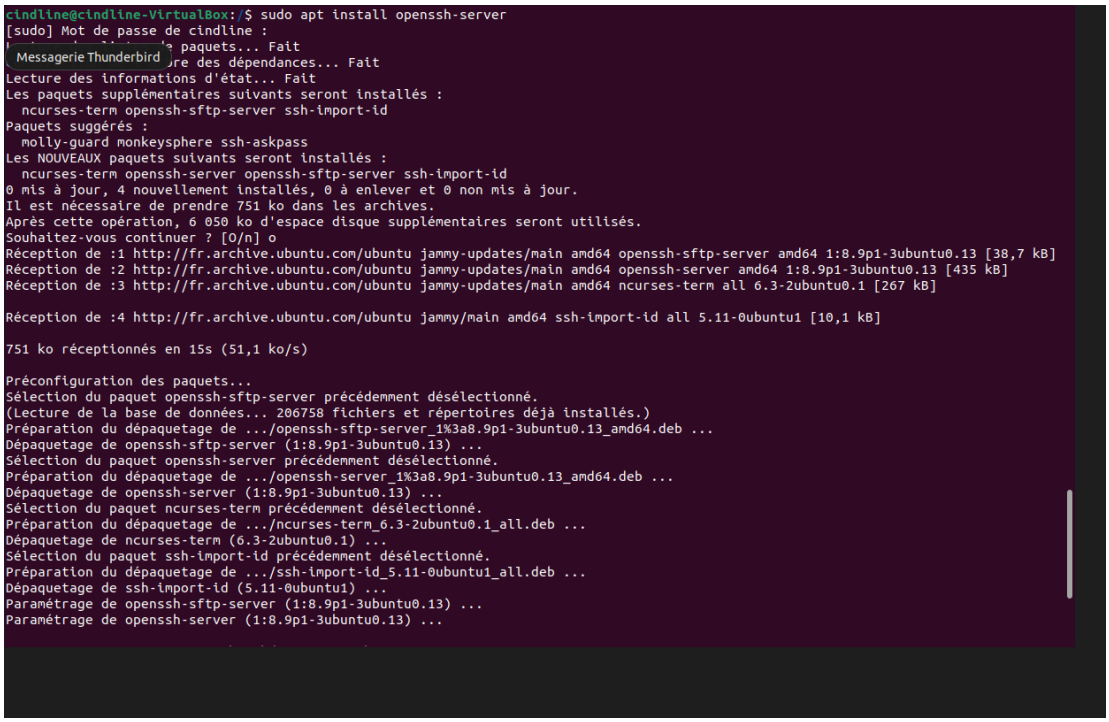
On voit sur le terminal que pour le dossier log badge est propriétaire avec lecture, écriture et exécution. Le groupe formatech a l'autorisation de lecture et d'exécution et les autres aucun droits.

Pour le dossier script on voit que badge est propriétaire avec les droits de lecture, écriture et exécution. Info est le groupe propriétaire avec lecture, écriture et exécution et les autres n'ont aucun droits.

4.4) Installation et configuration du SSH

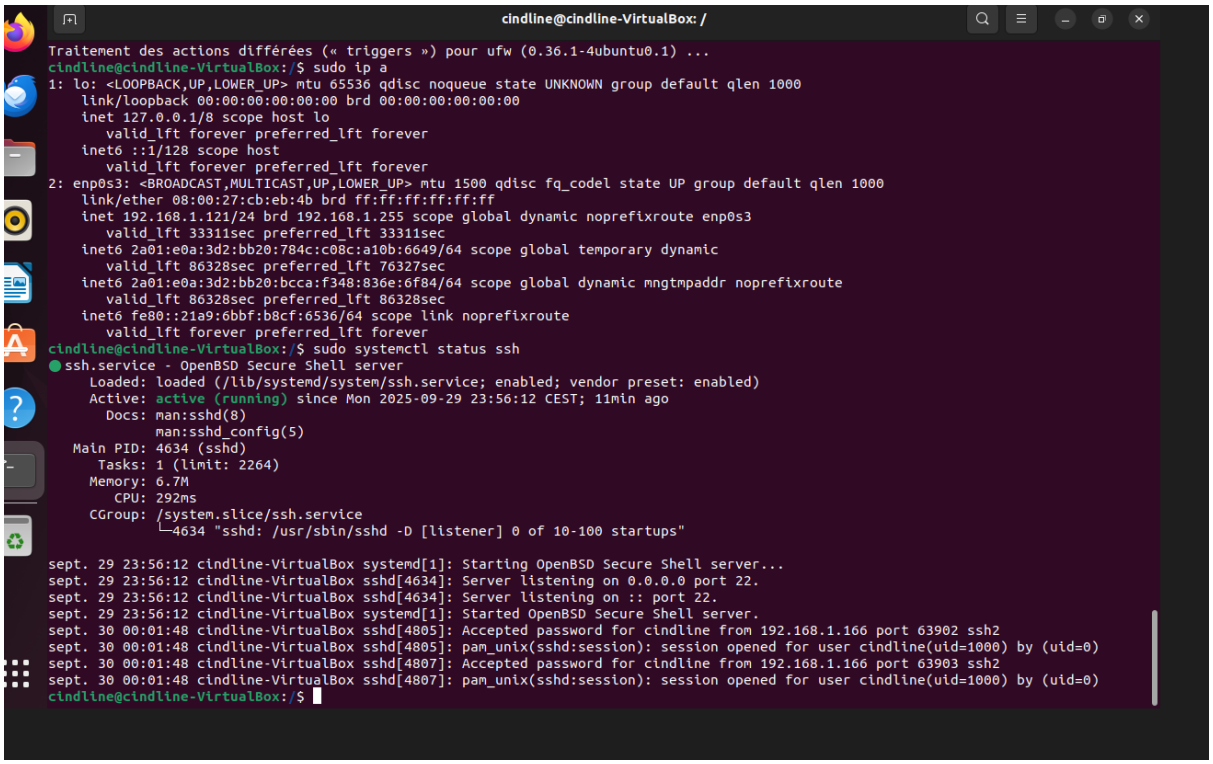
Installation du ssh

Commande : sudo apt install openssh-server



Test du statut actif du ssh

Commande sudo systemctl status ssh

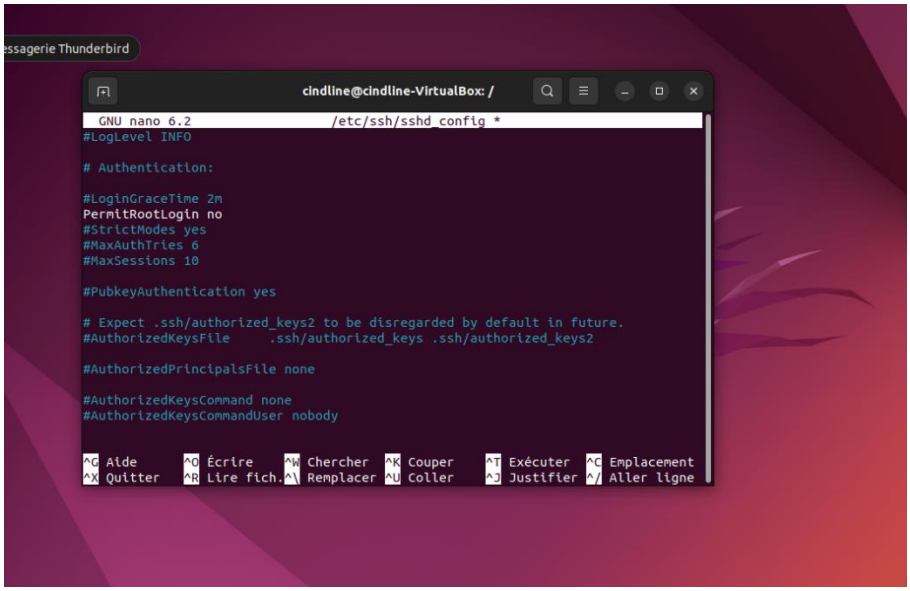


Accès à la configuration du ssh afin d'interdire l'accès du ssh à root

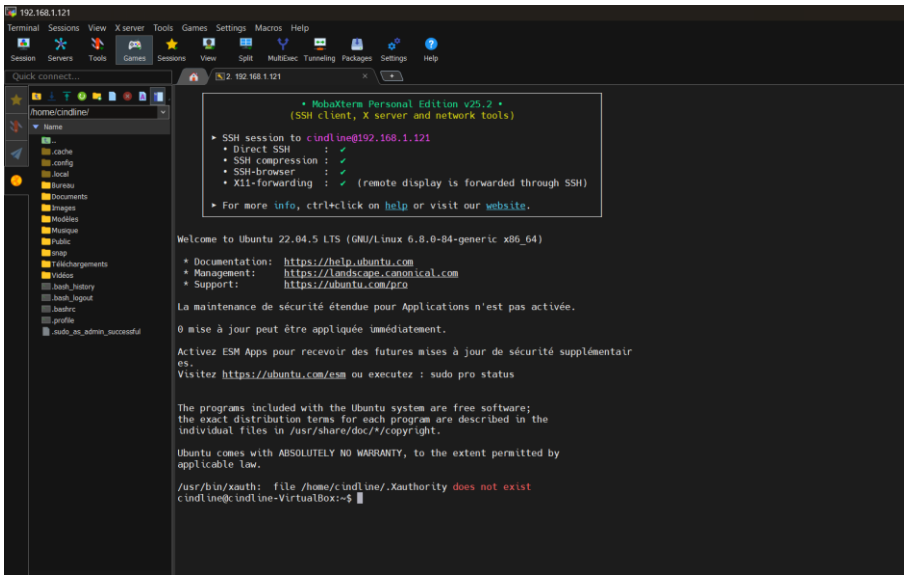
Commande: sudo nano /etc/ssh/sshd_config

Changement de l'autorisation pour root avec: PermitRootLogin no

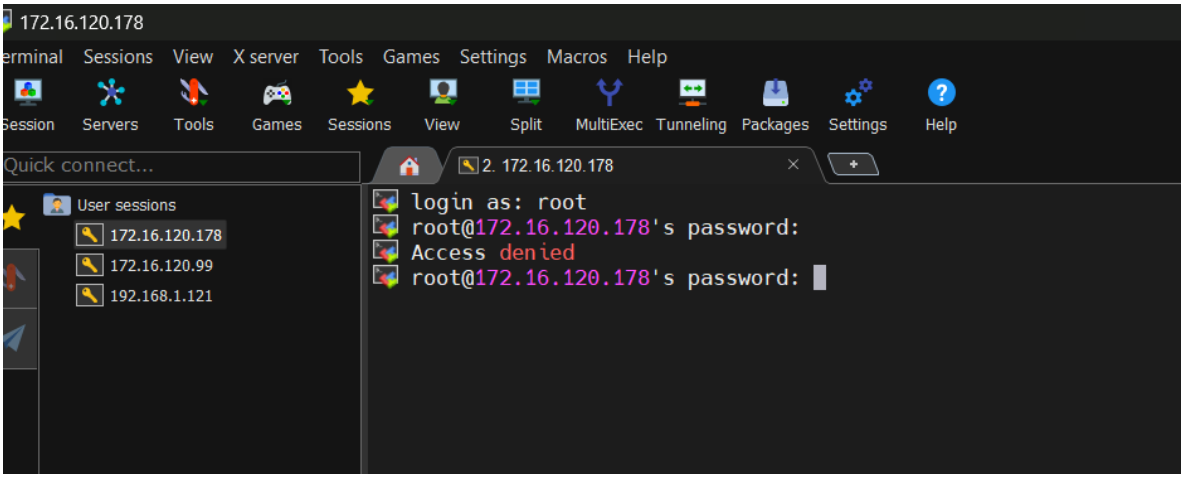
Redémarrage de ssh avec la commande sudo systemctl restart ssh



Connexion sur moba

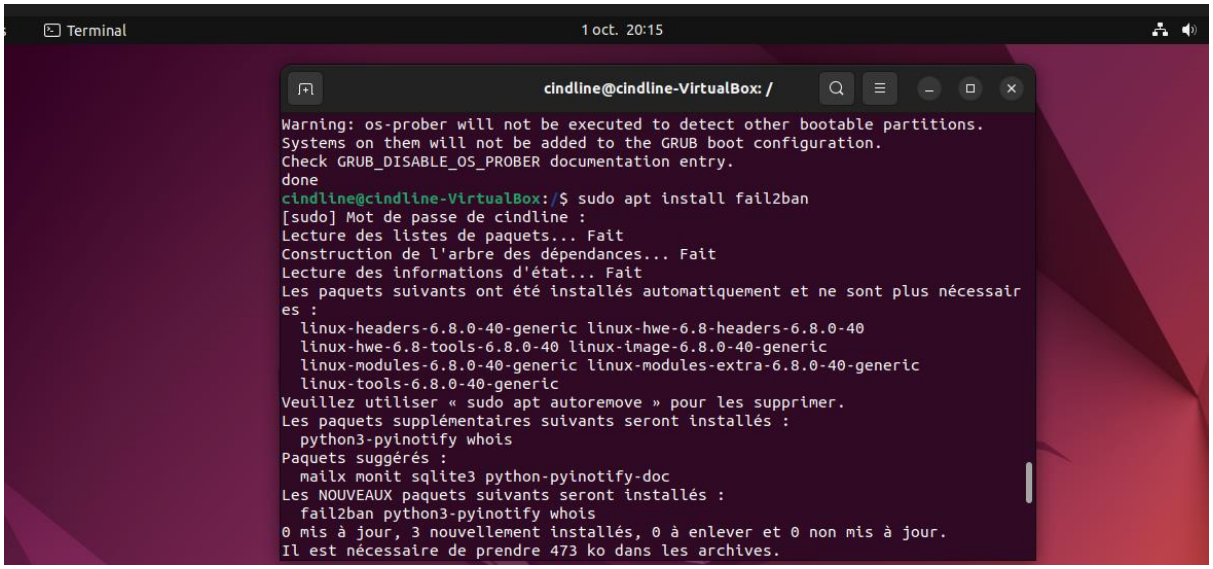


Accès root refusé

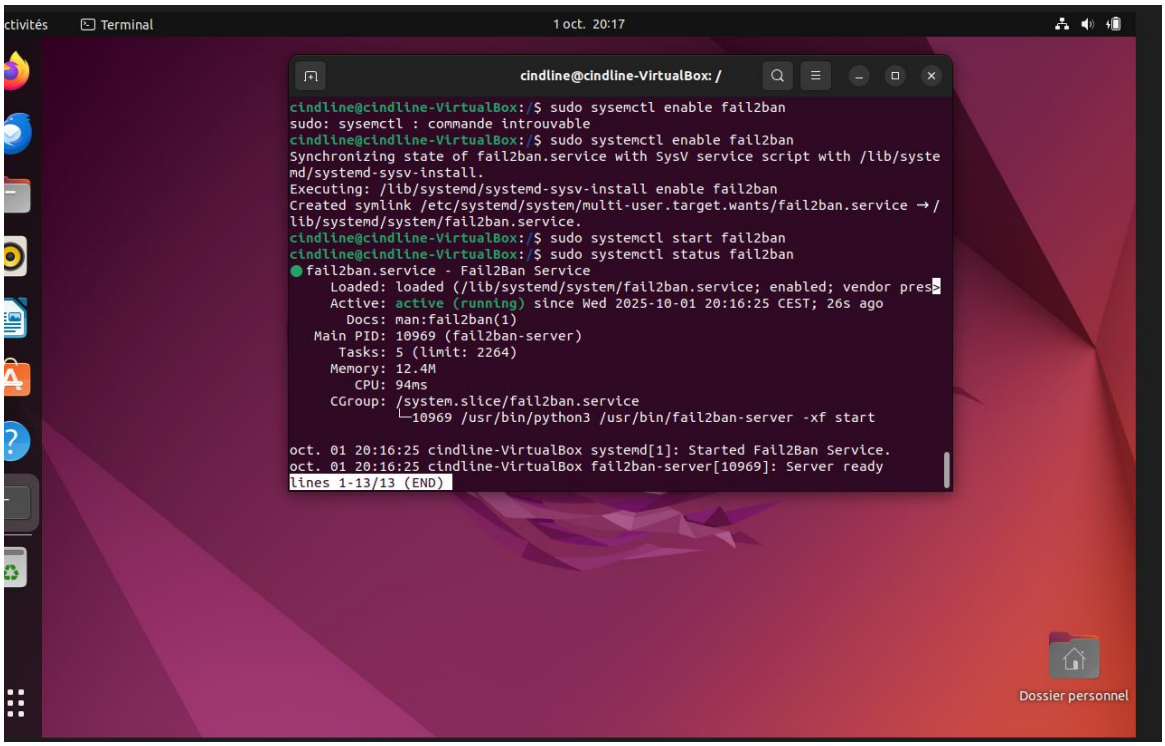


4.5) Installation et configuration du Fail2Ban

Installation fail2ban : sudo apt install fail2ban



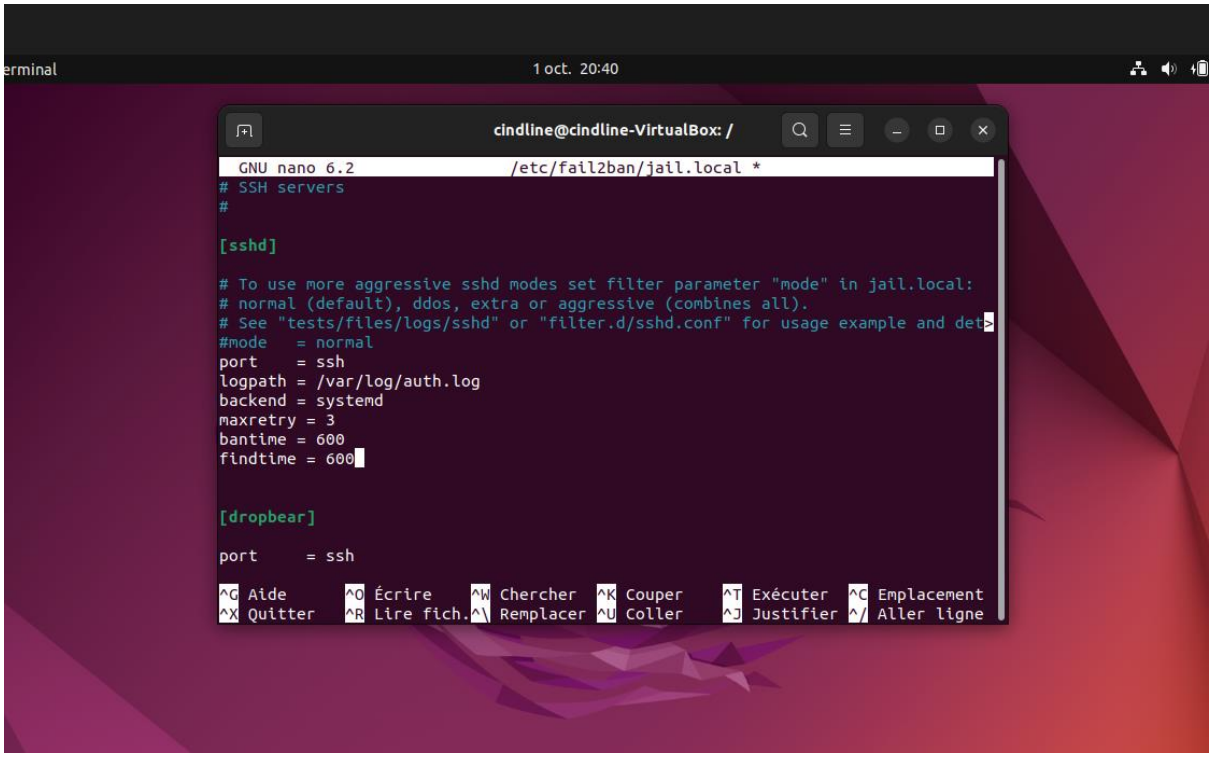
Vérification du statuts de fail2ban :



Configuration du fail2ban

Création d'un jail local : sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

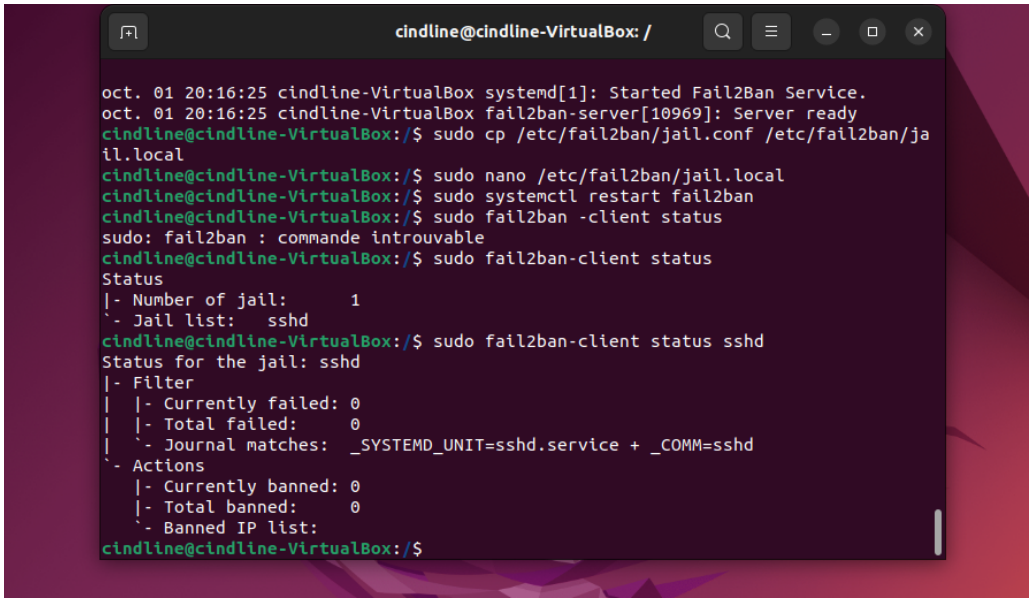
Configuration de la jail ssh : sudo nano /etc/fail2ban/jail.local



Redémarrer fail2ban : sudo systemctl restart fail2ban

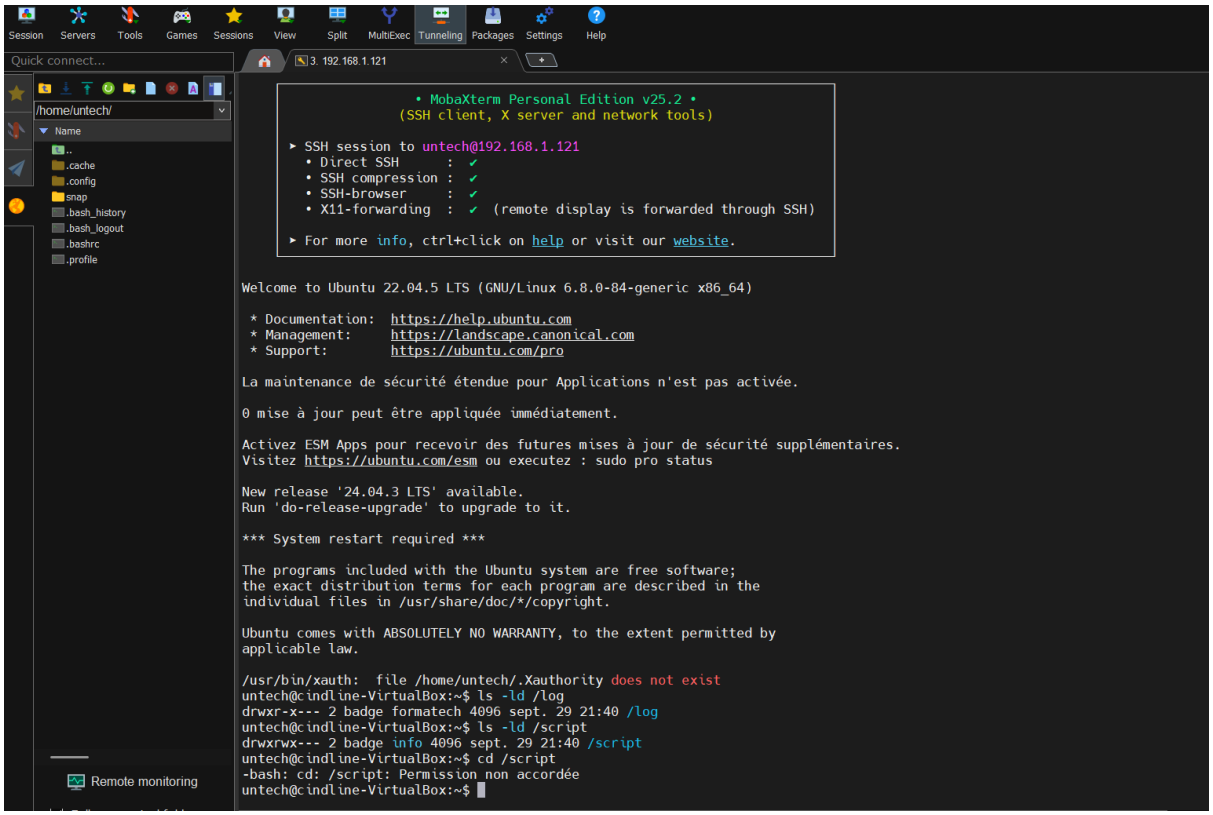
Vérifier les jail actives : sudo fail2ban-client status on voit sshd

Etat détaillé de la jail ssh : sudo fail2ban-client status sshd



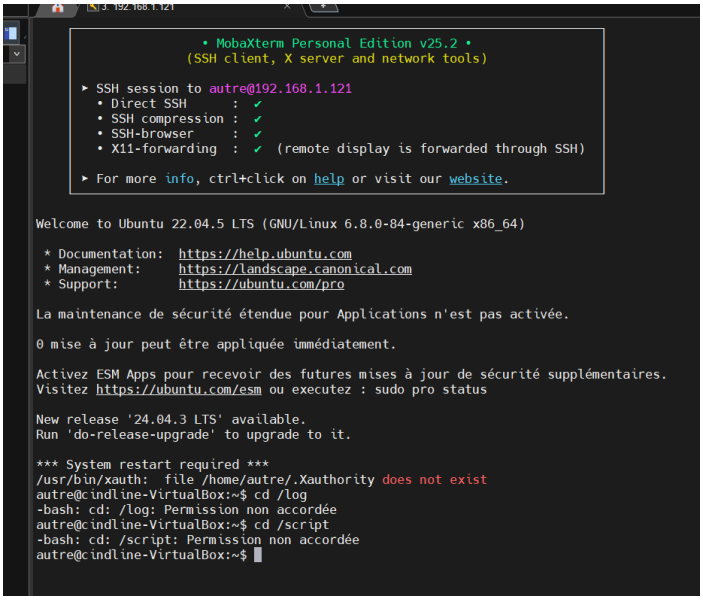
5) Tests de fin

Test d'accès au ssh et des accès dossier pour les utilisateurs

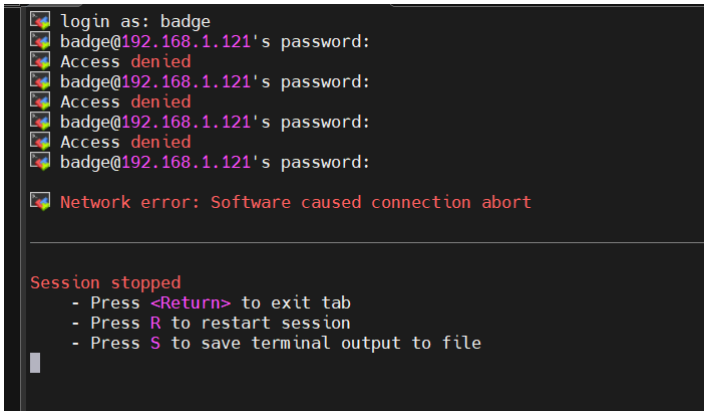



```
deuxtech@cindline-VirtualBox:~$ test -w /log && echo "ecriture possible" || echo "pas d'ecriture possible"
pas d'ecriture possible
deuxtech@cindline-VirtualBox:~$ test -r /log && echo "lecture possible" || echo "pas de lecture possible"
lecture possible
deuxtech@cindline-VirtualBox:~$ test -r /script && echo "lecture possible" || echo "pas de lecture possible"
pas de lecture possible
deuxtech@cindline-VirtualBox:~$
```

Pas d'accès pour l'utilisateur autre



Accès refusé après mot de passe erroné et mise en jail par fail2ban



6) Problèmes rencontrés / solutions apporté / Bibliographie

Je suis la seule ressource affectée au différentes tâches. Chaque tâches comportent plusieurs actions pas de possibilité sur le gantt d'affecter 2 tâches sur la même journée, j'ai essayé de mettre 0.5 ou 0.25 jour mais cela n'a pas pris.

https://www.malekal.com/lister-groupes-linux/ pour lister les groupes

https://labex.io/fr/tutorials/linux-how-to-check-if-an-ssh-server-is-running-in-linux-558785 vérification du serveur en cours d'exécution

https://forum.ubuntu-fr.org/viewtopic.php?id=336222 interdire l'accès ssh à root et wiki ubuntu. Il a fallu que je m'y reprenne à plusieurs fois car je pensais qu'au niveau du ssh l'interdiction se faisait dès le login mais il se fait après avoir taper le mot de passe.

au départ du fichier est un commentaire je ne l'ai pas trouver de suite il a fallu que je m'y reprenne à 2 fois pour que la ligne soit en exécution.

chatGPT et copilot pour l'installation et les tests du fail2ban

7) Annexes (si besoin)