



CindLine-Tech

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

Céline FERRIERES / CindLine-Tech

Sommaire

1) Reformulation du besoin	3
2) Analyse de l'existant.....	4
3) Proposition de solution.....	5
3.1) Description	5
3.2) Planification.....	5
4) Mise en place	6
4.1) Mise en place du serveur Linux (Ubuntu)	6
4.2) Création des utilisateurs, du compte badge et des groupes "info" et "tech"	7
4.3) Création des dossier "LOG" et "SCRIPT" et attribution des droits	9
4.4) Installation et configuration du SSH	10
4.5) installation et configuration du fail2ban.....	11
5) Tests de fin	15
6) Problèmes rencontrés / solutions apporté / Bibliographie	17
7) Annexes (si besoin).....	18

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

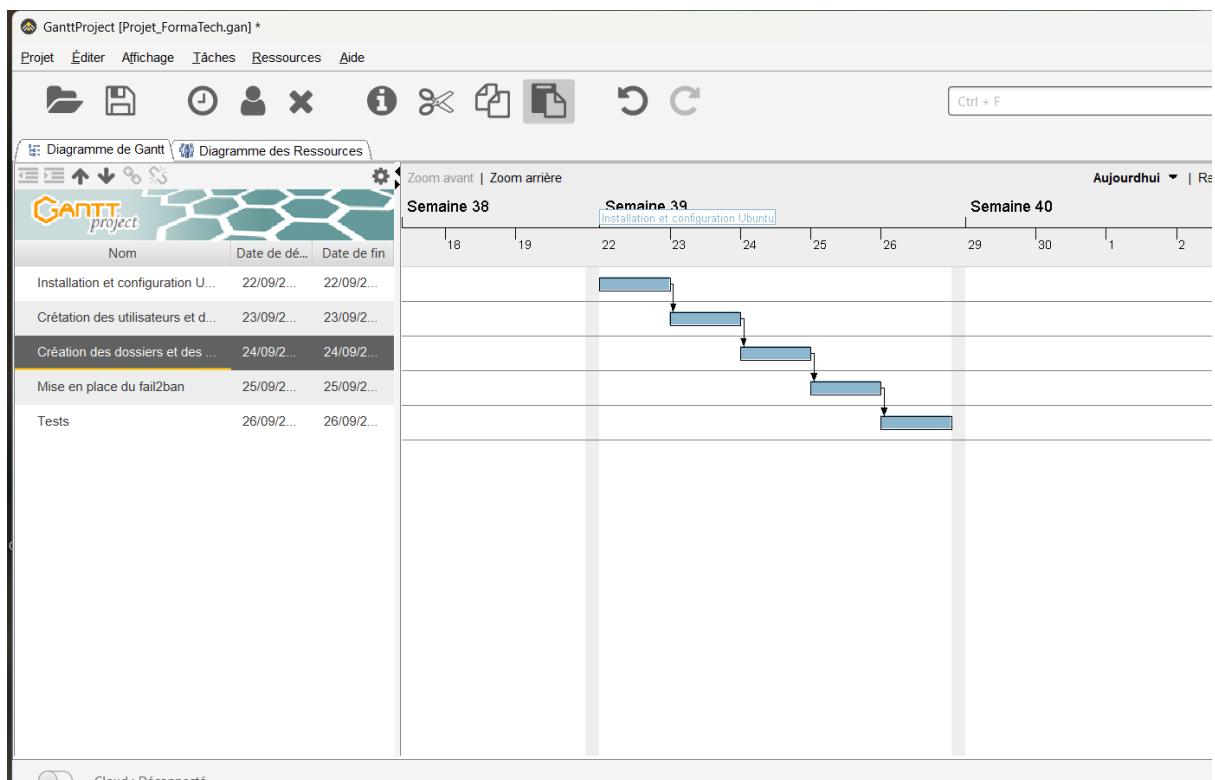
3) Proposition de solution

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 Its
- 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

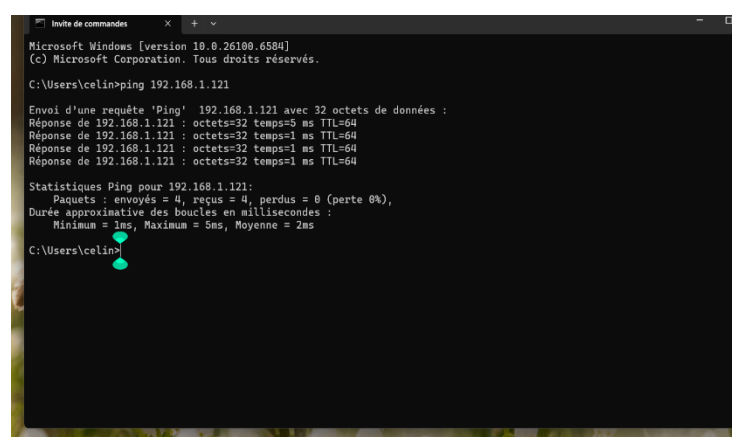
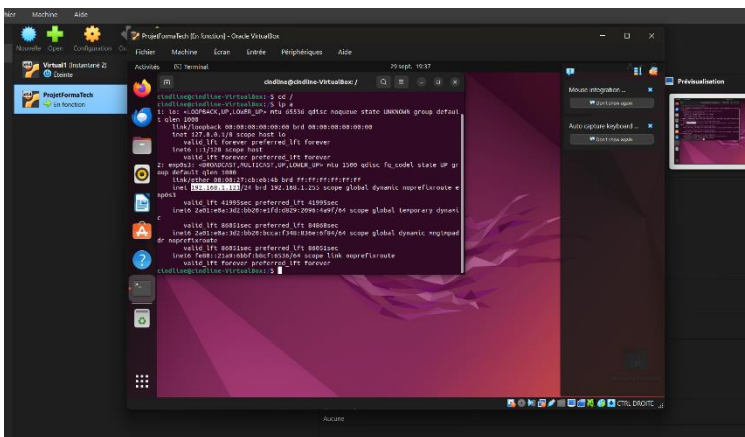
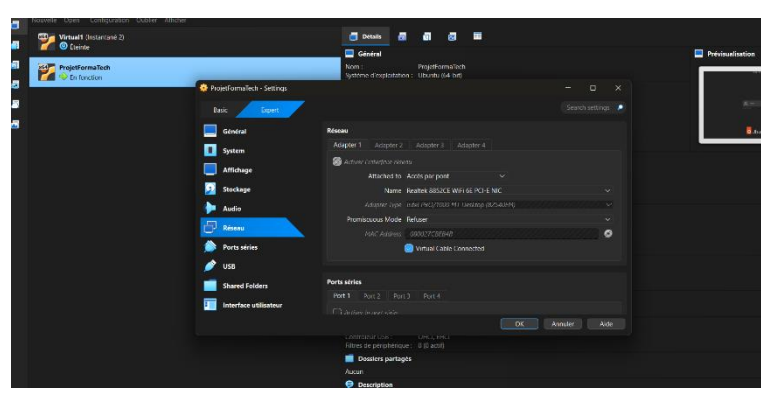
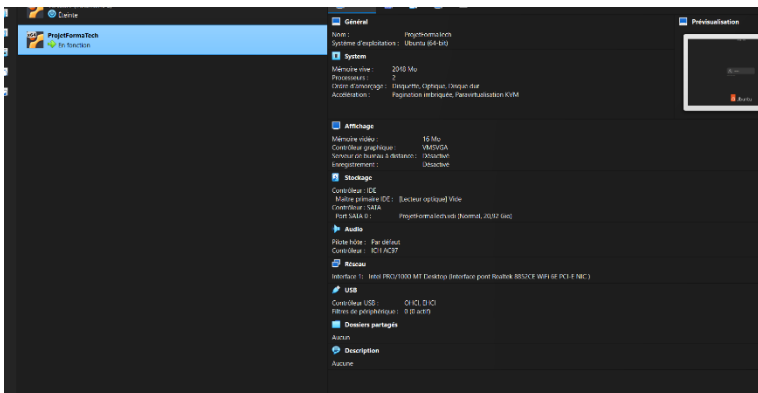
Passage à la racine avec la commande: `cd /`

Recherche et installation des mises à jour: `sudo apt update`

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 faite.
- 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`

```
Téléphone personnel []:
Autre []:
Ces informations sont-elles correctes ? [0/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 ? [0/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 ? [0/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 ? [0/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`

```

telephone personnel []:
Autre []:
Ces informations sont-elles correctes ? [0/n] o
cindline@cindline-VirtualBox:/$ sudo usermod -ag info uninfo
cindline@cindline-VirtualBox:/$ sudo usermod -ag info deuxinfo
cindline@cindline-VirtualBox:/$ sudo usermod -ag info troisinfo
cindline@cindline-VirtualBox:/$ sudo getent groupe info
Base de données inconnue : « groupe »
Pour en savoir davantage, faites : «getent --help » ou «getent --usage».
cindline@cindline-VirtualBox:/$ sudo getent info
sudo: getent : commande introuvable
cindline@cindline-VirtualBox:/$ sudo getent group info
sudo: getent : commande introuvable
cindline@cindline-VirtualBox:/$ sudo getent group info
info:x:1001:uninfo,deuxinfo,troisinfo
cindline@cindline-VirtualBox:/$ sudo usermod -ag tech untech
cindline@cindline-VirtualBox:/$ sudo usermod -ag tech deuxtech
cindline@cindline-VirtualBox:/$ sudo usermod -ag tech troistech
cindline@cindline-VirtualBox:/$ sudo getent group tech
tech:x:1002:untech,deuxtech,troistech
cindline@cindline-VirtualBox:/$

```

Test :

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

```

cindline@cindline-VirtualBox:/$ sudo su badge
[sudo] Mot de passe de cindline :
badge@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su uninfo
uninfo@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su deuxinfo
deuxinfo@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su troisinfo
troisinfo@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su untech
untech@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su deuxtech
deuxtech@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su troistech
troistech@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ sudo su autre
autre@cindline-VirtualBox:/$ exit
exit
cindline@cindline-VirtualBox:/$ █

```

- 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
ne@cindline-VirtualBox:/$ sudo su badge
```

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

Tests :

- Affichage des droits avec la commande ls -ld dossier

```
cindline@cindline-VirtualBox:/$ sudo chmod -R 750 /log
cindline@cindline-VirtualBox:/$ sudo chown badge /script
cindline@cindline-VirtualBox:/$ sudo chgrp info /script
cindline@cindline-VirtualBox:/$ sudo chmod -R 770 /script
cindline@cindline-VirtualBox:/$ ls -ld log
drwxr-x--- 2 badge formatech 4096 sept. 29 21:40 log
cindline@cindline-VirtualBox:/$ ls -ld script
drwxrwx--- 2 badge info 4096 sept. 29 21:40 script
cindline@cindline-VirtualBox:/$
```

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

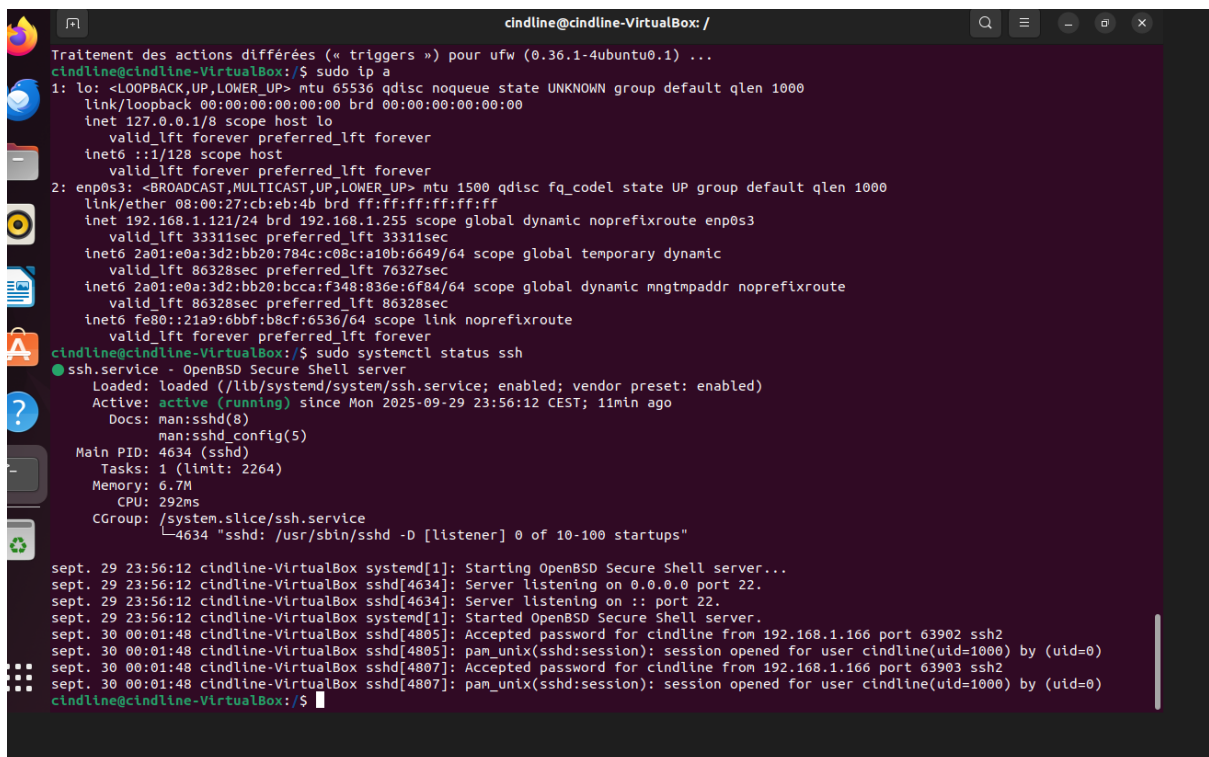
Installation du ssh

Commande : sudo apt install openssh-server

```
cindline@cindline-VirtualBox:/$ sudo apt install openssh-server
[sudo] Mot de passe de cindline :
Lecture de la base de données... Fait
MessagerieThunderbird : 3 paquets... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  ncurses-term openssh-sftp-server ssh-import-id
Paquets suggérés :
  molly-guard monkeysphere ssh-askpass
Les NOUVEAUX paquets suivants seront installés :
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 751 ko dans les archives.
Après cette opération, 6 050 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.13 [38,7 kB]
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.13 [435 kB]
Réception de :3 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Réception de :4 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10,1 kB]
751 ko réceptionnés en 15s (51,1 ko/s)
Préconfiguration des paquets...
Sélection du paquet openssh-sftp-server précédemment désélectionné.
(Lecture de la base de données... 206758 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../openssh-sftp-server_1%3a8.9p1-3ubuntu0.13_amd64.deb ...
Dépaquetage de openssh-sftp-server (1:8.9p1-3ubuntu0.13) ...
Sélection du paquet openssh-server précédemment désélectionné.
Préparation du dépaquetage de .../openssh-server_1%3a8.9p1-3ubuntu0.13_amd64.deb ...
Dépaquetage de openssh-server (1:8.9p1-3ubuntu0.13) ...
Sélection du paquet ncurses-term précédemment désélectionné.
Préparation du dépaquetage de .../ncurses-term_6.3-2ubuntu0.1_all.deb ...
Dépaquetage de ncurses-term (6.3-2ubuntu0.1) ...
Sélection du paquet ssh-import-id précédemment désélectionné.
Préparation du dépaquetage de .../ssh-import-id_5.11-0ubuntu1_all.deb ...
Dépaquetage de ssh-import-id (5.11-0ubuntu1) ...
Paramétrage de openssh-sftp-server (1:8.9p1-3ubuntu0.13) ...
Paramétrage de openssh-server (1:8.9p1-3ubuntu0.13) ...
```

Test du statut actif du ssh

Commande sudo systemctl status ssh



```
Traitement des actions différées (« triggers ») pour ufw (0.36.1-4ubuntu0.1) ...
cindline@cindline-VirtualBox:/$ sudo ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:eb:4b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.121/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 33311sec preferred_lft 33311sec
    inet6 2a01:e0a:3d2:bb20:784c:c08c:a10b:6649/64 scope global temporary dynamic
        valid_lft 86328sec preferred_lft 76327sec
    inet6 2a01:e0a:3d2:bb20:bcca:f348:836e:6f84/64 scope global dynamic mngtppaddr noprefixroute
        valid_lft 86328sec preferred_lft 86328sec
    inet6 fe80::21a9:6bbf:b8cf:6536/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
cindline@cindline-VirtualBox:/$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-09-29 23:56:12 CEST; 11min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 4634 (sshd)
     Tasks: 1 (limit: 2264)
    Memory: 6.7M
       CPU: 292ms
    CGroup: /system.slice/ssh.service
           └─4634 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

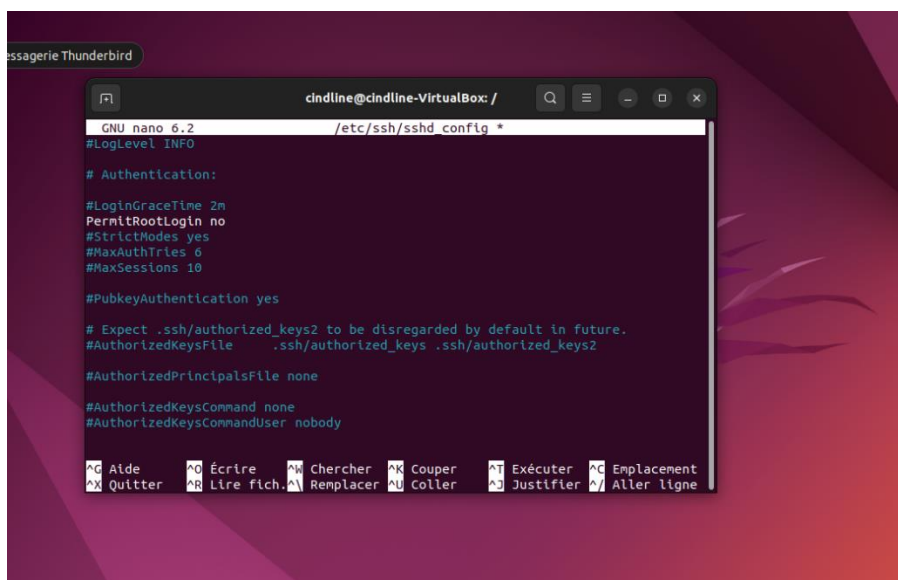
sept. 29 23:56:12 cindline-VirtualBox systemd[1]: Starting OpenBSD Secure Shell server...
sept. 29 23:56:12 cindline-VirtualBox sshd[4634]: Server listening on 0.0.0.0 port 22.
sept. 29 23:56:12 cindline-VirtualBox sshd[4634]: Server listening on :: port 22.
sept. 29 23:56:12 cindline-VirtualBox systemd[1]: Started OpenBSD Secure Shell server.
sept. 30 00:01:48 cindline-VirtualBox sshd[4805]: Accepted password for cindline from 192.168.1.166 port 63902 ssh2
sept. 30 00:01:48 cindline-VirtualBox sshd[4805]: pam_unix(sshd:session): session opened for user cindline(uid=1000) by (uid=0)
sept. 30 00:01:48 cindline-VirtualBox sshd[4807]: Accepted password for cindline from 192.168.1.166 port 63903 ssh2
sept. 30 00:01:48 cindline-VirtualBox sshd[4807]: pam_unix(sshd:session): session opened for user cindline(uid=1000) by (uid=0)
cindline@cindline-VirtualBox:/$
```

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



```
sshagerie Thunderbird
cindline@cindline-VirtualBox: /
GNU nano 6.2 /etc/ssh/sshd_config *
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

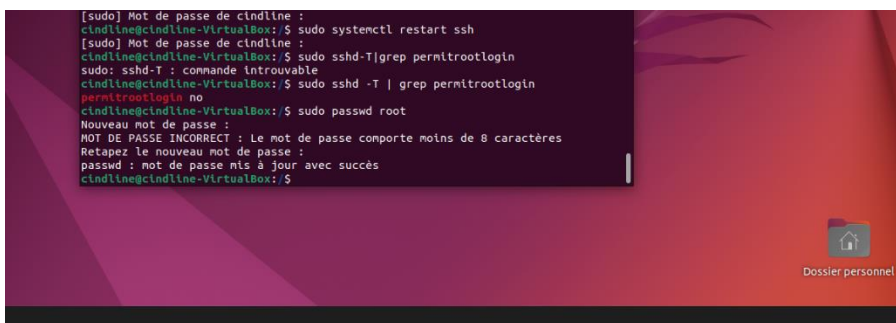
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

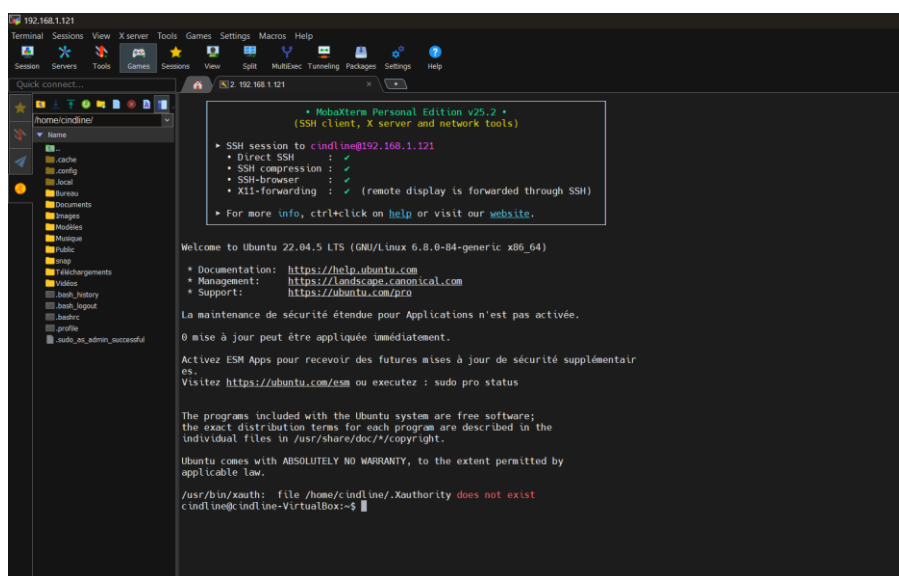
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

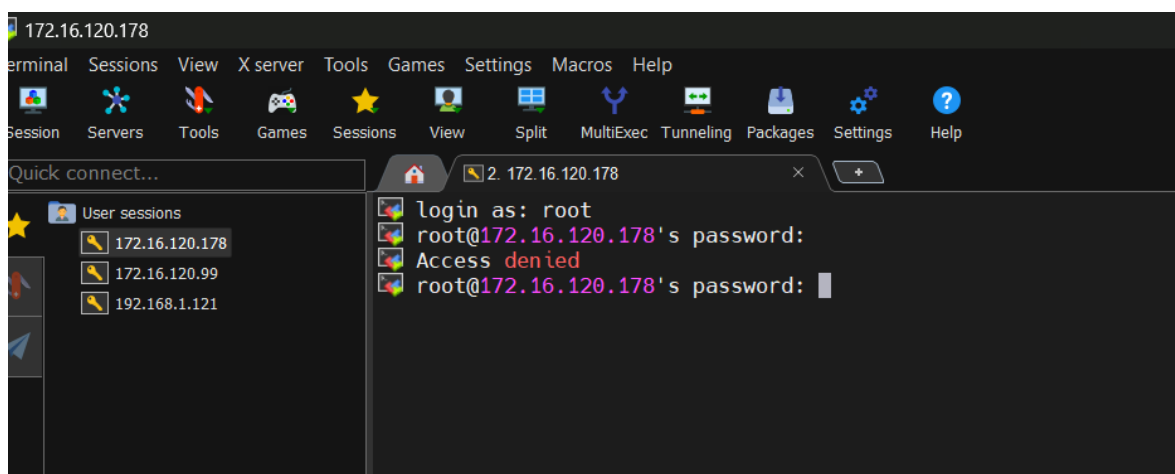
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^A Remplacer ^U Coller ^J Justifier ^_ Aller ligne
```



Connexion sur moba

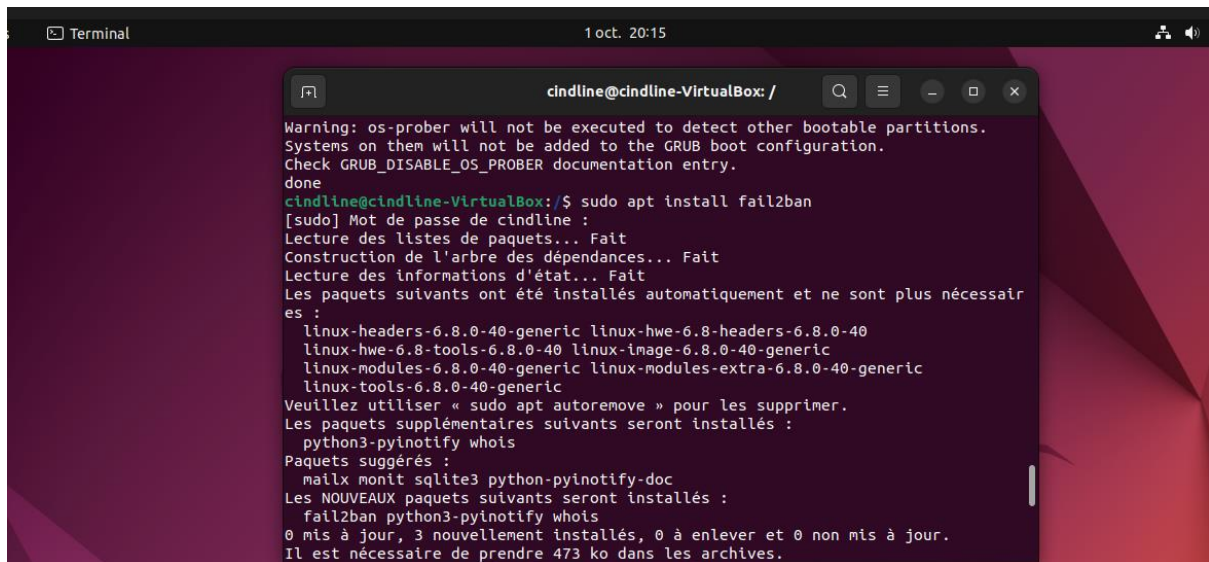


Accès root refusé



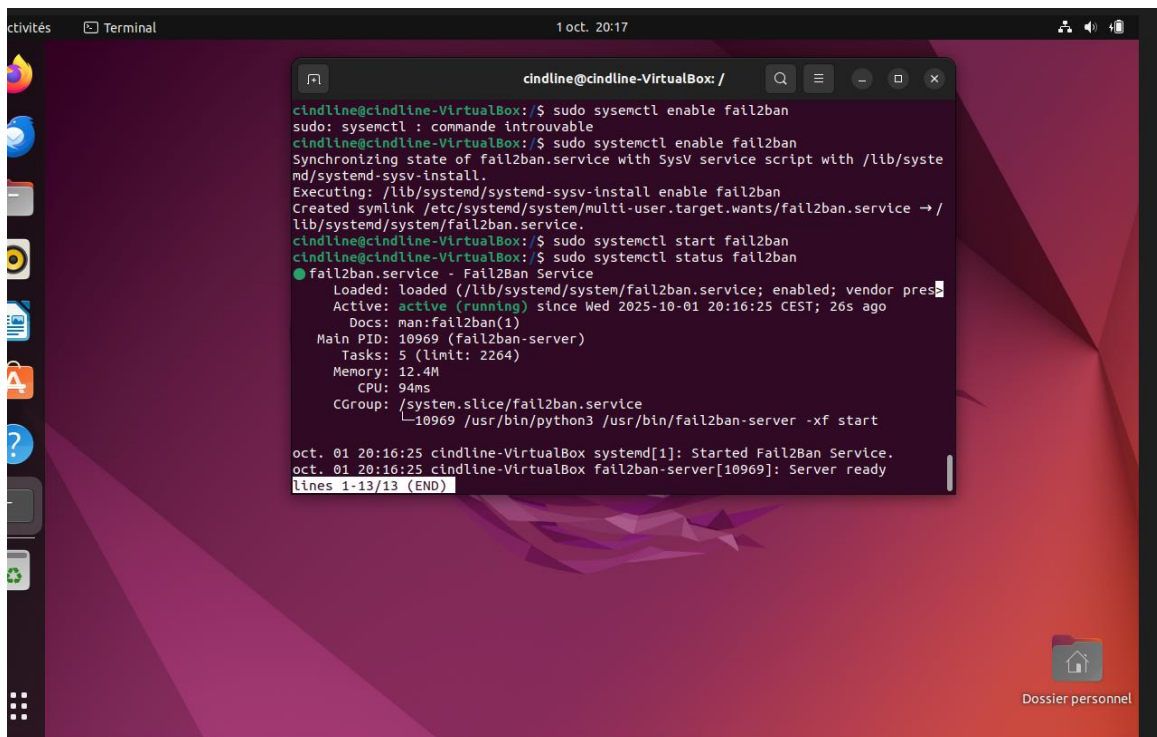
4.5) Installation et configuration du Fail2Ban

Installation fail2ban : `sudo apt install fail2ban`



```
Terminal 1 oct. 20:15
cindline@cindline-VirtualBox: /
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
cindline@cindline-VirtualBox:/$ sudo apt install fail2ban
[sudo] Mot de passe de cindline :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  linux-headers-6.8.0-40-generic linux-hwe-6.8-headers-6.8.0-40
  linux-hwe-6.8-tools-6.8.0-40 linux-image-6.8.0-40-generic
  linux-modules-6.8.0-40-generic linux-modules-extra-6.8.0-40-generic
  linux-tools-6.8.0-40-generic
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  python3-pyinotify whois
Paquets suggérés :
  mailx monit sqlite3 python-pyinotify-doc
Les NOUVEAUX paquets suivants seront installés :
  fail2ban python3-pyinotify whois
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 473 ko dans les archives.
```

Vérification du statuts de fail2ban :



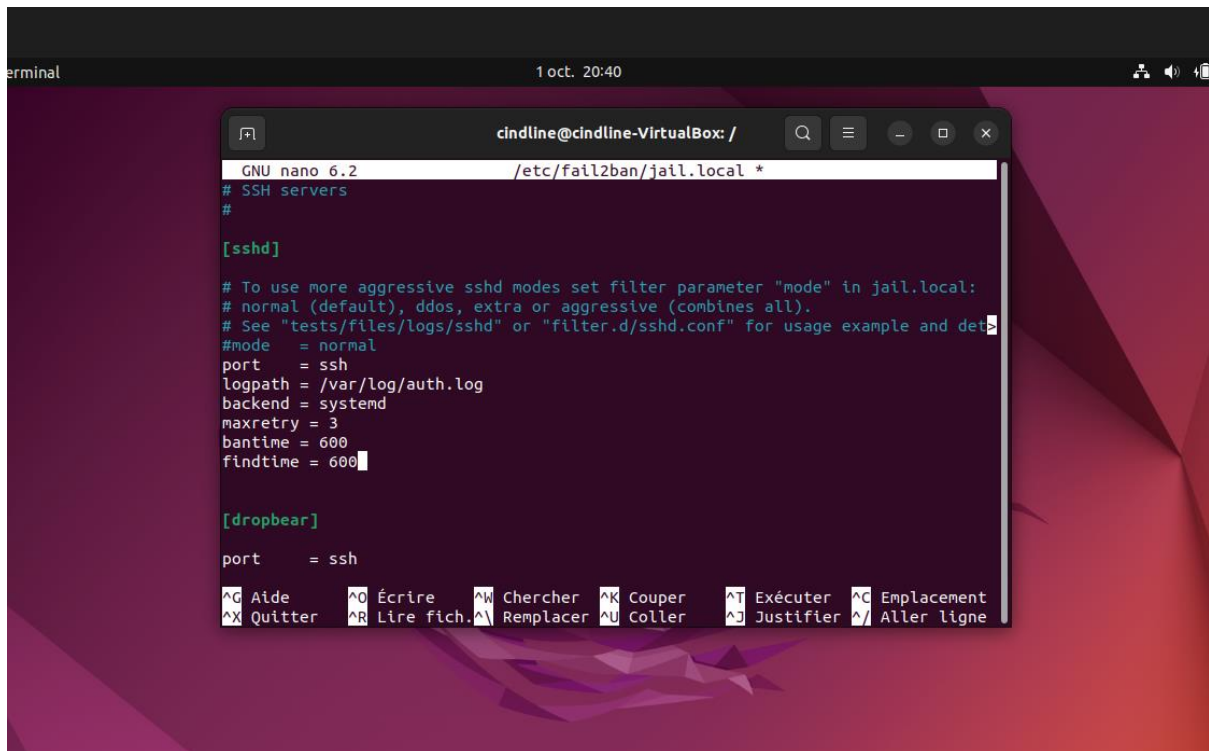
```
Terminal 1 oct. 20:17
cindline@cindline-VirtualBox: /
cindline@cindline-VirtualBox:/$ sudo systemctl enable fail2ban
sudo: systemctl : commande introuvable
cindline@cindline-VirtualBox:/$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/syste
md/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /
lib/systemd/system/fail2ban.service.
cindline@cindline-VirtualBox:/$ sudo systemctl start fail2ban
cindline@cindline-VirtualBox:/$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pres
   Active: active (running) since Wed 2025-10-01 20:16:25 CEST; 26s ago
     Docs: man:fail2ban(1)
    Main PID: 10969 (fail2ban-server)
       Tasks: 5 (limit: 2264)
      Memory: 12.4M
         CPU: 94ms
    CGroup: /system.slice/fail2ban.service
            └─10969 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

oct. 01 20:16:25 cindline-VirtualBox systemd[1]: Started Fail2Ban Service.
oct. 01 20:16:25 cindline-VirtualBox fail2ban-server[10969]: Server ready
lines 1-13/13 (END)
```

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`

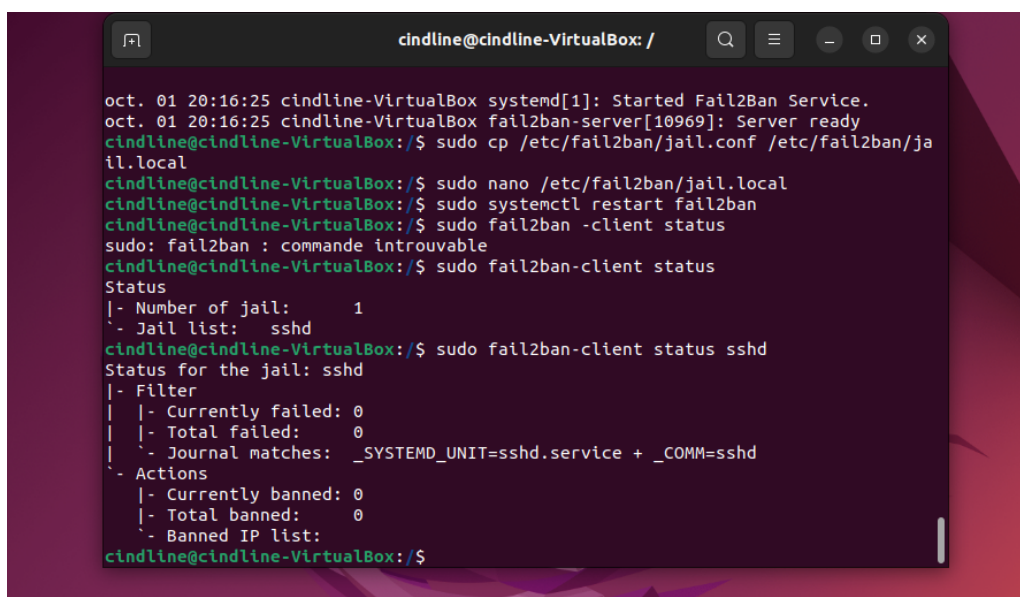


```
terminal 1 oct. 20:40
cindline@cindline-VirtualBox: /
GNU nano 6.2 /etc/fail2ban/jail.local *
# SSH servers
#
[sshd]
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and det
#mode = normal
port = ssh
logpath = /var/log/auth.log
backend = systemd
maxretry = 3
bantime = 600
findtime = 600
[dropbear]
port = ssh
Aide Écrire Chercher Couper Exécuter Emplacement
Quitter Lire fich. Remplacer Coller Justifier Aller ligne
```

Redémarrer fail2ban : `sudo systemctl restart fail2ban`

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

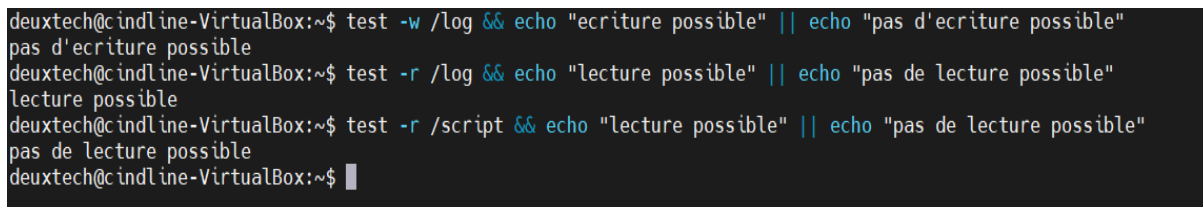
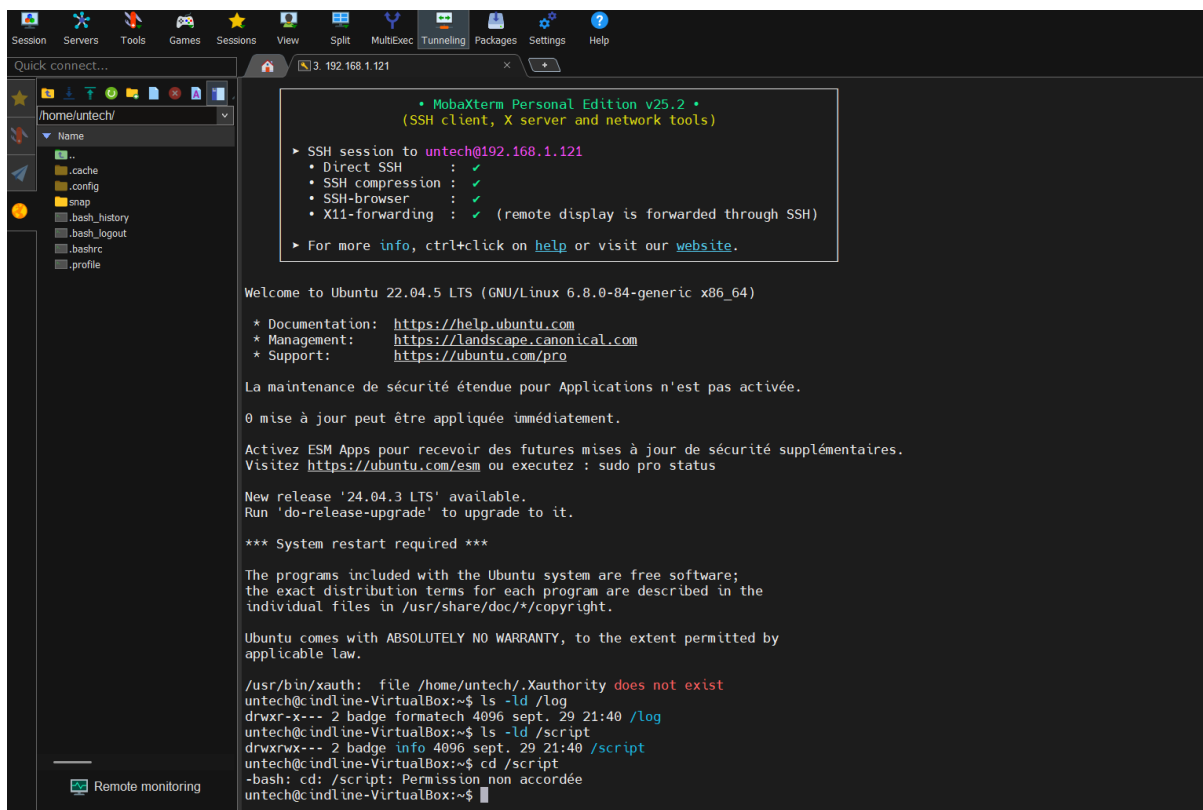
Etat détaillé de la jail ssh : `sudo fail2ban-client status sshd`



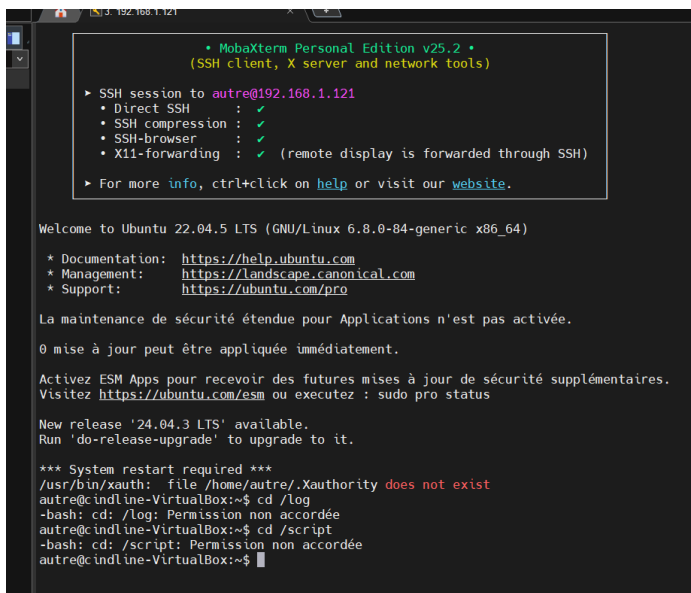
```
cindline@cindline-VirtualBox: /
oct. 01 20:16:25 cindline-VirtualBox systemd[1]: Started Fail2Ban Service.
oct. 01 20:16:25 cindline-VirtualBox fail2ban-server[10969]: Server ready
cindline@cindline-VirtualBox:/$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
cindline@cindline-VirtualBox:/$ sudo nano /etc/fail2ban/jail.local
cindline@cindline-VirtualBox:/$ sudo systemctl restart fail2ban
cindline@cindline-VirtualBox:/$ sudo fail2ban -client status
sudo: fail2ban : commande introuvable
cindline@cindline-VirtualBox:/$ sudo fail2ban-client status
Status
|- Number of jail: 1
  |-- Jail list: sshd
cindline@cindline-VirtualBox:/$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |-- Currently failed: 0
| |-- Total failed: 0
| |-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
  |-- Actions
  |-- Currently banned: 0
  |-- Total banned: 0
  |-- Banned IP list:
cindline@cindline-VirtualBox:/$
```

5) Tests de fin

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



Pas d'accès pour l'utilisateur autre



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

```
login as: badge
badge@192.168.1.121's password:
Access denied
badge@192.168.1.121's password:
Access denied
badge@192.168.1.121's password:
Access denied
badge@192.168.1.121's password:
Network error: Software caused connection abort

Session stopped
- Press <Return> to exit tab
- Press R to restart session
- Press S to save terminal output to file
```

```
cindline@cindline-VirtualBox:/$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned: 1
   `-- Banned IP list: 192.168.1.166
cindline@cindline-VirtualBox:/$
```

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)