

plateflop_ftp

installer proftpd:

```
apt install proftpd
```

installer proftpd-mod-crypto:

```
apt install proftpd-mod-crypto
```

Désactivez l'accès SSH pour `root`. Modifiez `/etc/ssh/sshd_config`:
et mettre `PermitRootLogin no`

création de l'utilisateur '`monitor`' :

```
useradd monitor
```

privilege sudo:

```
usermod -aG sudo monitor
```

1. Créer le répertoire `.ssh` pour l'utilisateur `monitor`

```
mkdir -p /home/monitor/.ssh
```

2. Définir les permissions appropriées:

```
chown -R monitor:monitor /home/monitor/.ssh
```

```
chmod 700 /home/monitor/.ssh
```

3. Générer la paire de clés SSH

générer la clé SSH et de la sauvegarder dans le répertoire
`~monitor/.ssh` :

```
ssh-keygen -t rsa -b 4096 -C "monitor" -f /home/monitor/.ssh/id_rsa
```

Cette commande générera une clé privée (`id_rsa`) et une clé publique (`id_rsa.pub`) dans le répertoire `/home/monitor/.ssh/`.

4. Définir les permissions pour les fichiers de clé

```
chown monitor:monitor /home/monitor/.ssh/id_rsa
```

```
/home/monitor/.ssh/id_rsa.pub
```

```
chmod 600 /home/monitor/.ssh/id_rsa
```

```
chmod 644 /home/monitor/.ssh/id_rsa.pub
```

5. Copier la clé publique dans `authorized_keys`

```
cat /home/monitor/.ssh/id_rsa.pub >>
/home/monitor/.ssh/authorized_keys
chmod 600 /home/monitor/.ssh/authorized_keys
```

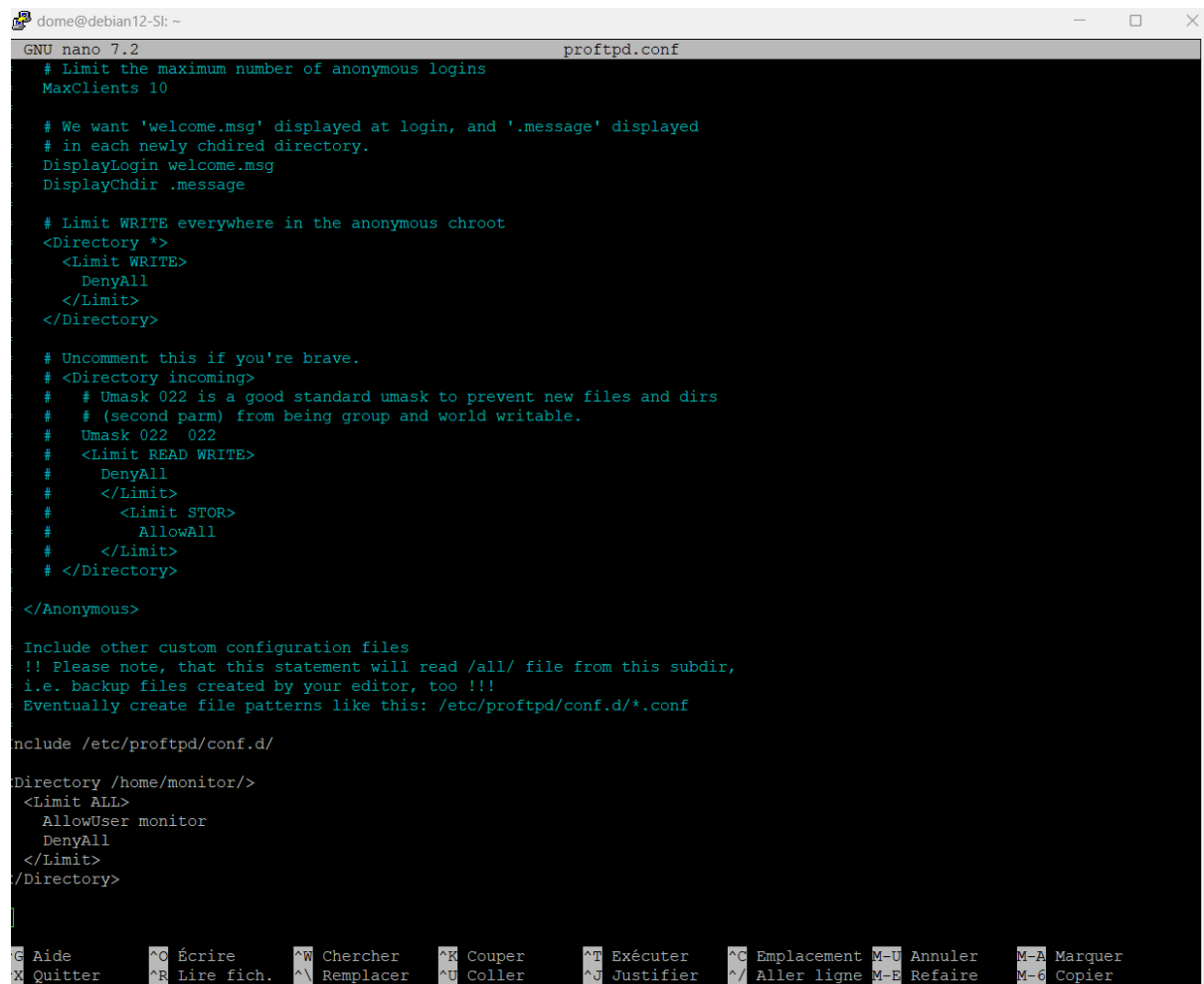
6. Tester la connexion SSH

```
C:\Users\satin>ssh monitor@192.168.52.137
The authenticity of host '192.168.52.137 (192.168.52.137)' can't be established.
ED25519 key fingerprint is SHA256:b1ZpqM/P0tZ5TaIGSQSoI+qrtumq97D9hy/BdTxA9Hc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.52.137' (ED25519) to the list of known hosts.
monitor@192.168.52.137's password:
Linux debian12-SI 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
monitor@debian12-SI:~$
```

ajout de l'user 'monitor' dans proftpd.conf



```
GNU nano 7.2 proftpd.conf
# Limit the maximum number of anonymous logins
MaxClients 10

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdir'd directory.
DisplayLogin welcome.msg
DisplayChdir .message

# Limit WRITE everywhere in the anonymous chroot
<Directory *>
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>

# Uncomment this if you're brave.
# <Directory incoming>
#   # Umask 022 is a good standard umask to prevent new files and dirs
#   # (second parm) from being group and world writable.
#   Umask 022 022
#   <Limit READ WRITE>
#     DenyAll
#   </Limit>
#   <Limit STOR>
#     AllowAll
#   </Limit>
# </Directory>

</Anonymous>

Include other custom configuration files
!! Please note, that this statement will read /all/ file from this subdir,
i.e. backup files created by your editor, too !!!
Eventually create file patterns like this: /etc/proftpd/conf.d/*.conf

include /etc/proftpd/conf.d/

Directory /home/monitor/>
  <Limit ALL>
    AllowUser monitor
    DenyAll
  </Limit>
</Directory>
```

Copier la clé publique avec **ssh-copy-id** :

bash

Copier le code

ssh-copy-id monitor@adresse_ip_du_serveur

script ssh_login1.py

```
root@cli-amandine:/home/amandine# python3 ssh_login1.py
Entrez le mot de passe SSH :
Résultat de la commande 'df':
Sys. de fichiers blocs de 1K Utilisé Disponible Uti% Monté sur
udev                984000      0    984000   0% /dev
tmpfs               201444    592    200852   1% /run
/dev/sda1          15421320 2611940 12004212 18% /
tmpfs              1007204      0    1007204   0% /dev/shm
tmpfs               5120       0     5120    0% /run/lock
tmpfs              201440      0    201440   0% /run/user/1000
```

script ssh_login_sudo.py

```
root@cli-amandine:/home/amandine# python3 ssh_login_sudo.py
Entrez le mot de passe SSH :
Entrez le mot de passe sudo :
Résultat de la commande 'apt update' avec sudo:
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Réception de :2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Réception de :3 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 DEP-11 Metadata [4 492 kB]
Réception de :5 http://deb.debian.org/debian bookworm/non-free-firmware amd64 DEP-11 Metadata [15,5 kB]
Réception de :6 http://deb.debian.org/debian bookworm/non-free amd64 DEP-11 Metadata [4 428 B]
Réception de :7 http://deb.debian.org/debian bookworm/contrib amd64 DEP-11 Metadata [16,5 kB]
4 632 ko réceptionnés en 1s (3 181 ko/s)
Lecture des listes de paquets...
Construction de l'arbre des dépendances...
Lecture des informations d'état...
Tous les paquets sont à jour.
```

Donner des droits de lecture à l'utilisateur **monitor** (ou celui utilisé pour SSH) :

Vous pouvez soit changer les permissions du fichier, soit donner temporairement les droits de lecture à l'utilisateur.

Option 1 : Ajouter **monitor au groupe **root**** C'est la méthode la plus simple, mais elle peut potentiellement poser des risques de sécurité si vous ajoutez trop de privilèges à l'utilisateur **monitor**.

bash

Copier le code

sudo usermod -aG root monitor

1. Ensuite, reconnectez-vous pour que les changements de groupe prennent effet.
2. **Option 2 : Modifier les permissions pour permettre à tout le monde de lire le fichier** Si vous préférez éviter de modifier les groupes, vous pouvez temporairement rendre le fichier lisible par tous (en général, cela est moins recommandé car cela pourrait exposer des informations sensibles).

bash

Copier le code

```
sudo chmod 644 /var/log/proftpd/proftpd.log
```

Cependant, cette approche nécessite que `monitor` soit configuré pour exécuter `sudo` sans demander de mot de passe, ce qui peut être fait en modifiant le fichier `sudoers` :

bash

Copier le code

```
sudo visudo
```

Ajoutez une ligne comme celle-ci :

bash

Copier le code

```
monitor ALL=(ALL) NOPASSWD: /bin/cat /var/log/proftpd/proftpd.log
```

Cela permettra à l'utilisateur `monitor` d'exécuter la commande `cat` sur ce fichier sans avoir à entrer un mot de passe.

```
script_ftp_error.py
```

```
root@cli-amandine:/home/amandine# ./ssh_ftp_error4.py
2024-09-25 07:55:43,324 - INFO - Connected (version 2.0, client OpenSSH_9.2p1)
2024-09-25 07:55:43,415 - INFO - Authentication (password) successful!
2024-09-25 07:55:43,503 - INFO - Les logs ont été récupérés et sauvegardés dans proftpd.log
2024-09-25 07:55:43,503 - WARNING - Erreur détectée : 2024-09-24 10:40:28,152 srv-ftp proftpd[20189] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password
2024-09-25 07:55:43,504 - WARNING - Erreur détectée : 2024-09-24 10:41:27,948 srv-ftp proftpd[20226] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER x: no such user found from cli-amandine.homelab.lan [192.168.10.101] to ::ffff:192.168.10.185:21
2024-09-25 07:55:43,505 - WARNING - Erreur détectée : 2024-09-24 10:49:32,191 srv-ftp proftpd[20547] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password
2024-09-25 07:55:43,505 - WARNING - Erreur détectée : 2024-09-25 07:55:32,083 srv-ftp proftpd[63802] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password
2024-09-25 07:55:43,505 - INFO - 4 erreur(s) détectée(s) dans les logs.
```

script ssh_serveur_mail

```
root@cli-amandine:/home/amandine# ./ssh_serveur_mail.py
2024-09-25 08:48:59,142 - INFO - Connected (version 2.0, client OpenSSH_9.2p1)
2024-09-25 08:48:59,267 - INFO - Authentication (password) successful!
2024-09-25 08:49:00,304 - INFO - Email envoyé à satin.amandine@gmail.com
root@cli-amandine:/home/amandine#
```

compte gmail :activer authentication à 2 étapes , ensuite générer une clé d'accès et mot de passe d' application

Rapport de tentatives de connexion échouées - 2024-09-24

Boîte de réception x

satin.amandine@gmail.com

À moi ▾

08:48 (il y a 0 minute) ☆ 😊 ↶ ⋮

Tentatives de connexion échouées du 2024-09-24:

2024-09-24 10:40:28,152 srv-ftp proftpd[20189] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password

2024-09-24 10:41:27,948 srv-ftp proftpd[20226] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER x: no such user found from cli-amandine.homelab.lan [192.168.10.101] to ::ffff:192.168.10.185:21

2024-09-24 10:49:32,191 srv-ftp proftpd[20547] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password

↶ Répondre

↷ Transférer

😊

script ssh_cron_backup

```
root@cli-amandine:/home/amandine# ./ssh_cron-backup.py
2024-09-25 11:30:49,258 - INFO - Connected (version 2.0, client OpenSSH_9.2p1)
2024-09-25 11:30:49,347 - INFO - Authentication (password) successful!
2024-09-25 11:30:49,428 - INFO - [chan 0] Opened sftp connection (server version 3)
2024-09-25 11:30:49,436 - INFO - Erreurs insérées avec succès dans la table error_log.
```

```
MariaDB [plateflop]> SELECT * FROM error_log;
```

-----+-----			
id	error_type	error_message	timestamp
		-----+-----	
-----+-----			
1	SSH Connection Error	Authentication failed.	2024-09-25 11:04:47
2	SSH Connection Error	Authentication failed.	2024-09-25 11:06:47
3	SSH Connection Error	[Errno 2] No such file or directory: '/.ssh/id_rsa.pub'	2024-09-25 11:20:09
4	SSH Connection Error	Authentication failed.	2024-09-25 11:22:52
5	SSH Connection Error	Authentication failed.	2024-09-25 11:28:38
6	FTP Error	2024-09-24 10:40:28,152 srv-ftp proftpd[20189] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password	2024-09-25 11:30:49
7	FTP Error	2024-09-24 10:49:32,191 srv-ftp proftpd[20547] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password	2024-09-25 11:30:49
8	FTP Error	2024-09-25 07:55:32,083 srv-ftp proftpd[63802] srv-ftp (cli-amandine.homelab.lan[192.168.10.101]): USER monitor (Login failed): Incorrect password	2024-09-25 11:30:49
-----+-----			

script ssh_system_status

```
oot@cli-amandine:/home/amandine# nano ssh_system_status.py
oot@cli-amandine:/home/amandine# ./ssh_system_status.py
024-09-25 11:56:55,396 - INFO - Connected (version 2.0, client OpenSSH_9.2p1)
024-09-25 11:56:55,483 - INFO - Authentication (password) successful!
024-09-25 11:56:55,837 - INFO - Statut système inséré avec succès dans la base de données.
oot@cli-amandine:/home/amandine# mysql -h 192.168.10.152 -u amandine -p
```

```
oot@cli-amandine:/home/amandine# mysql -h 192.168.10.152 -u amandine -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 70
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use plateflop;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [plateflop]> SELECT * FROM system_status;
+-----+-----+-----+-----+-----+-----+
id | timestamp          | cpu_usage | ram_total | ram_used | disk_usage |
+-----+-----+-----+-----+-----+-----+
1 | 2024-09-25 11:56:55 | 0         | 1967     | 564      | 0%         |
+-----+-----+-----+-----+-----+-----+
1 row in set (0,001 sec)
```

script ssh_system_mail

```
root@cli-amandine:/home/amandine# ./ssh_system_mail.py
2024-09-25 12:27:17,585 - INFO - Connected (version 2.0, client OpenSSH_9.2p1)
2024-09-25 12:27:17,675 - INFO - Authentication (password) successful!
2024-09-25 12:27:18,021 - INFO - Statut système inséré avec succès dans la base de données.
2024-09-25 12:27:18,872 - INFO - E-mail d'alerte envoyé avec succès.
```



Alerte : Utilisation des ressources système élevée Boîte de réception x



satin.amandine@gmail.com

À satin.amandine ▾

Alerte ! Les seuils d'utilisation des ressources ont été dépassés :

- Utilisation CPU : 0.0%

- Utilisation RAM : 29.994916115912556%

- Utilisation Disque : 0.0%



Mail Delivery Subsystem <mailer-daemon@googlemail.com>

À moi ▾


```
Database changed
MariaDB [plateflop]> SELECT * FROM system_status;
+-----+-----+-----+-----+-----+-----+
| id | timestamp                | cpu_usage | ram_total | ram_used | disk_usage |
+-----+-----+-----+-----+-----+-----+
| 5 | 2024-09-30 09:05:01 | 0 | 1967 | 401 | 0.0 |
| 6 | 2024-09-30 09:10:02 | 0 | 1967 | 405 | 0.0 |
| 7 | 2024-09-30 09:13:46 | 0 | 1967 | 409 | 0.0 |
| 8 | 2024-09-30 09:15:01 | 0 | 1967 | 417 | 0.0 |
| 9 | 2024-09-30 09:15:01 | 0 | 1967 | 417 | 0.0 |
| 10 | 2024-09-30 09:20:02 | 0 | 1967 | 417 | 0.0 |
| 11 | 2024-09-30 09:22:39 | 0 | 1967 | 417 | 0.0 |
| 12 | 2024-09-30 09:25:01 | 50 | 1967 | 433 | 0.0 |
| 13 | 2024-09-30 09:25:01 | 0 | 1967 | 433 | 0.0 |
| 14 | 2024-09-30 09:30:02 | 0 | 1967 | 438 | 0.0 |
| 15 | 2024-09-30 09:30:02 | 0 | 1967 | 438 | 0.0 |
+-----+-----+-----+-----+-----+-----+
11 rows in set (0,001 sec)

MariaDB [plateflop]> exit
```

script google_chat

créer un espace et aller dans **applis ert integration** ,webhook et
créer un liens et le mettre dans le script

```
root@cli-amandine:/home/amandine# ./google_tchat.py
2024-10-01 08:51:39,398 - INFO - Message envoyé à Google Chat avec succès.
```

← **plateflop** 4 membres • Privé

Chat Partagés Tâches

Aujourd'hui

Amandine, bienvenue dans votre nouvel espace de collaboration. C'est parti :

[Ajouter des me...](#) [Partager un fi...](#) [Attribuer des t...](#)

Vous avez créé cet espace aujourd'hui

Amandine SATIN a créé un webhook appelé plateflop

1 non lue(s)

Aujourd'hui

Message supprimé par son auteur 1 min

Amandine SATIN a ajouté Dylan Capron, Thierry RAMI, Domenico MANDOLINO

plateflop Application À l'instant

****État du serveur au 2024-10-01 08:51:38****
CPU Utilisation : 0.0%
RAM Utilisation : 21.1%
Disque Utilisation : 21.8%