

Compte rendu complet Fail2ban + ProFTPD + test ssh

1. Installation de Fail2ban Commande d'installation :

```
sudo apt update
sudo apt install fail2ban
```

Vérifie que Fail2ban est installé :

```
fail2ban-client --version
```

2. Démarrage et vérification du service

Démarre le service Fail2ban :

```
sudo systemctl start fail2ban
```

Vérifie que Fail2ban tourne :

```
sudo systemctl status fail2ban
```

En cas d'erreur (ex: exit-code failed), lire les logs :

```
sudo journalctl -u fail2ban.service --since "5 minutes ago"
sudo tail -n 30 /var/log/fail2ban.log
```

3. Configuration Fail2ban pour ProFTPD

Ne jamais modifier /etc/fail2ban/jail.conf directement, créer/modifier /etc/fail2ban/jail.local.

Exemple minimal pour ProFTPD (création/édition du fichier) :

```
sudo nano /etc/fail2ban/jail.local
```

Coller dedans :

```
[DEFAULT]
bantime = 600
findtime = 600
maxretry = 3

[proftpd]
enabled = true
port = ftp,ftp-data,ftps,ftps-data
filter = proftpd
logpath = /var/log/proftpd/proftpd.log
maxretry = 3
```

```
bantime = 600
```

Enregistre puis quitte l'éditeur

3.2 Fichier filter (proftpd.conf)

Editer ou créer le fichier /etc/fail2ban/filter.d/proftpd.conf :

```
sudo nano /etc/fail2ban/filter.d/proftpd.conf
```

Coller le contenu fusionné corrigé (sans doublon de [Definition]) :

```
[Definition]

_daemon = proftpd

failregex = ^%(__prefix_line)s%(__hostname)s \S+\[<HOST>\][[: -]]+ <F-CONTENT>(?:USER|SECURITY|Maximum) .+</F-CONTENT>$
^USER <F-USER>\S+|.?.?</F-USER>(?: LoginfailedLoginfailed)??: ([Uu]ser not
authorized for login|[Nn]o such user found|[Ii]ncorrect password|[Pp]assword
expired|[Aa]ccount disabled|[Ii]nvalid shell: '\S+'|[Uu]ser in \S+|[Ll]imit
(access|configuration) denies login|[Nn]ot a >)$
^SECURITY VIOLATION: <F-USER>\S+|.?.?</F-USER> login attempted
^Maximum login attempts \d+\d+ exceeded
.* no such user found from <HOST> .*.* to .*
.* USER .* LoginfailedLoginfailed: .* <HOST><HOST>
.* authentication failed from <HOST>

ignoreregex =

[Init]
journalmatch = _SYSTEMD_UNIT=proftpd.service
```

Enregistre et quitte

4. Démarrage et rechargement de Fail2ban

Redémarre Fail2ban pour appliquer les configs :

```
sudo systemctl restart fail2ban
```

Vérifie le statut :

```
sudo systemctl status fail2ban
```

Liste des jails activés :

```
sudo fail2ban-client status
```

Vérifie la jail proftpd spécifiquement :

```
sudo fail2ban-client status proftpd
```

5 Tester fail2ban.

Il faut au minimum avoir les commandes iptables dans le conteneur pour que Fail2ban puisse appliquer les règles. Tu peux l'installer via :

```
sudo apt install iptables
```

Étapes de test :

Depuis un terminal, connecte-toi au serveur FTP avec un mauvais utilisateur ou mot de passe.

Répète 3 fois la tentative de connexion erronée rapidement.

Si Fail2ban fonctionne, la connexion sera bloquée après les échecs (ton IP sera bannie).

Vérifie sur le serveur :

```
sudo fail2ban-client status proftpd
```

Tu dois voir ta propre IP dans la liste des bannissements.

6. Commandes utiles pour gérer Fail2ban

Voir les logs en temps réel :

```
sudo tail -f /var/log/fail2ban.log
```

Lister toutes les jails actives :

```
sudo fail2ban-client status
```

Voir le détail d'une jail :

```
sudo fail2ban-client status proftpd
```

Bannir une IP manuellement :

```
sudo fail2ban-client set proftpd banip IP_ADDRESS
```

Débannir une IP manuellement :

```
sudo fail2ban-client set proftpd unbanip IP_ADDRESS
```

7. Résumé des erreurs fréquentes et solutions

Problème	Cause fréquente	Solution
Fail2ban ne démarre pas (exit-code)	Doublon ou erreur dans filtre ou jail	Vérifier filtres et jail.local, corriger
"Failed to access socket path"	Fail2ban non démarré	Démarrer Fail2ban, vérifier logs
Jail ne bannit pas	Mauvais chemin log ou filtre mal écrit	Vérifier logpath et filtres regex
IP bannie trop longtemps ou jamais levée	Mauvaise configuration bantime ou maxretry	Ajuster dans jail.local
Fichier filter avec		

doublon [Definition] Provoque crash Fail2ban Ne garder qu'une seule section [Definition]

From:

<https://sisr2.beaupeyrat.com/> - **Documentations SIO2 option SISR**

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr1-g5:fail2ban>

Last update: **2025/05/23 14:33**

