 Documentation – Sécurisation du serveur BackupPC avec Fail2Ban

Installation de Fail2Ban

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

2. Activation du service

```
sudo systemctl start fail2ban
sudo systemctl enable fail2ban
```

3. Structure de configuration Ne jamais modifier directement /etc/fail2ban/jail.conf.

Créer un fichier de configuration local

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

4. ⚙ Configuration des jails dans /etc/fail2ban/jail.local

Édite le fichier : c'est dans ce fichier qu'il faut ces jails ajiouter

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

5. Création du filtre pour l’interface BackupPC

nano /etc/fail2ban/filter.d/backuppc-auth.conf

```
[Definition]
failregex = ^<HOST> - .* "GET /backuppc/ HTTP/1\.1" 401
ignoreregex =
```

 Redémarrage de Fail2Ban

```
sudo systemctl restart fail2ban
```

7. Vérification de l’état des jails

```

```

```
sudo fail2ban-client status
sudo fail2ban-client status backuppc-apache
```

comment faire pour debannir ..? Si tu es banni en SSH (et que tu n’as plus accès au serveur)
Connecte-toi à ton serveur via SSH avec une autre IP.

Liste les IP bannies dans la jail

```
sudo fail2ban-client status backuppc-apache
```

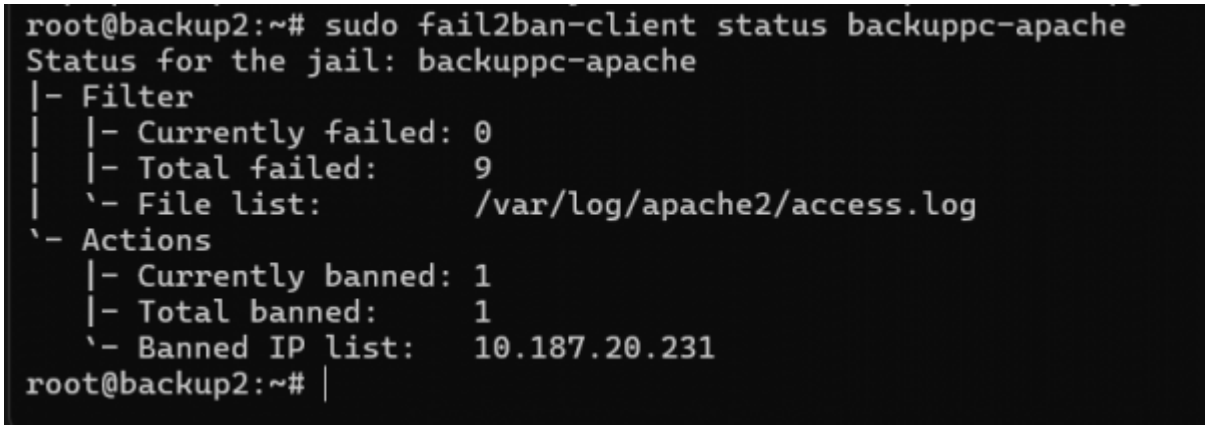
Débannis ton IP :

```
fail2ban-client set backuppc-apache unbanip <<IP.ICI à debanne>
```

faire la même chose pour la jail SSH :

```
 fail2ban-client set sshd unbanip TON.IP.ICI
```

TEST DE FONCTIONNALITE



```
root@backup2:~# sudo fail2ban-client status backuppc-apache
Status for the jail: backuppc-apache
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     9
|  `- File list:        /var/log/apache2/access.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   10.187.20.231
root@backup2:~#  fail2ban-client set backuppc-apache unbanip 10.187.20.231
1
root@backup2:~# sudo fail2ban-client status backuppc-apache
Status for the jail: backuppc-apache
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     9
|  `- File list:        /var/log/apache2/access.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
root@backup2:~#
```

BACKUPPC ... http://10.31.240.74/backuppc , c'est l'accès a l'interface

⚙ Installation de BackupPC Sur le serveur BackupPC :

```
sudo apt update
sudo apt install backuppc
```

3. Configuration de l'accès web Changer le mot de passe web :

```
sudo htpasswd /etc/backuppc/htpasswd backuppc
```

Activer l'accès web :

```
sudo cp /etc/backuppc/apache.conf /etc/apache2/sites-available/backuppc.conf
sudo a2ensite backuppc.conf
sudo systemctl reload apache2
```

 Accès : (http://10.31.240.74/backuppc)

4. Création d’un utilisateur avec accès SSH sans mot de passe 4.1 Sur le serveur BackupPC :

1. Aller dans le compte backuppc :

```
sudo su - backuppc
```

2. Générer une clé SSH :

```
cd ~/.ssh
ssh-keygen -t rsa -b 4096 -f id_rsa
Laisse vide (pas de passphrase)
```

La clé publique : ~/.ssh/id_rsa.pub

 4.2 Sur chaque machine cible à sauvegarder 1. Créer un utilisateur de sauvegarde : sudo adduser backup 2. Préparer le dossier SSH :

```
sudo mkdir -p /home/backup/.ssh
sudo chown backup:backup /home/backup/.ssh
```

3. Copier la clé publique : # Depuis le serveur BackupPC :

```
ssh-copy-id -i /var/lib/backuppc/.ssh/id_rsa.pub backup@IP_MACHINES_CIBLE
```

OU manuellement : copier le contenu de id_rsa.pub dans :

```
/home/backup/.ssh/authorized_keys
```

Puis :

```
sudo chown backup:backup ~/.ssh/authorized_keys
sudo chmod 600 ~/.ssh/authorized_keys
```

5. Interface Web Accessible via navigateur :

```
http://10.31.240.74/backuppc
```

Dans l’interface : Edit Hosts → Ajouter les hôtes à sauvegarder, ex :

Copier Modifier stp1dess backup rsync smb-pr backup smb webserver backup rsync Edit Config > Xfer :

Choisir rsync

Remplacer root par backup

Ajouter sudo devant la commande

6. Vérification de la connexion Depuis le serveur BackupPC :

```
sudo su - backuppc
ssh backup@<IP_MACHINE_CIBLE>
```

✔ Si tu es connecté sans mot de passe → tout est bon.