Version : **2026.01**

Dernière mise-à-jour : 2025/11/27 14:03

LDF403 - Authentification

Contenu du Module

- Ajouter un Prison

Le Problématique

Un pirate peut utiliser un logiciel de **crackage** pour tenter de découvrir un mot de passe. Le plus connu est **John The Ripper**.

Le principe de ces logiciels est simples - le logiciel utilise des dictionnaires de mots de passe qui sont utilisés le uns après les autres à une vitesse qui peut atteindre des milliers par seconde.

Surveillance Sécuritaire

La commande last

Cette commande indique les dates et heures des connexions des utilisateurs à partir du contenu du fichier **/var/log/wtmp** :

```
root@debian12:~# last
trainee  pts/2        10.0.2.1         Thu Nov 27 12:08   still logged in
trainee  pts/2        10.0.2.1         Wed Nov 26 15:35 - 17:26  (01:50)
trainee  pts/1        10.0.2.1         Tue Nov 25 14:58   still logged in
trainee  pts/0        10.0.2.1         Tue Nov 25 12:26   still logged in
trainee  pts/0        10.0.2.1         Tue Nov 25 09:23 - 11:29  (02:06)
reboot   system boot  6.1.0-41-amd64   Tue Nov 25 09:10   still running
trainee  pts/0        10.0.2.1         Mon Nov 24 17:41 - 17:41  (00:00)
trainee  pts/0        10.0.2.1         Mon Nov 24 17:38 - 17:41  (00:02)
reboot   system boot  6.1.0-41-amd64   Mon Nov 24 17:36   still running
trainee  pts/0        10.0.2.1         Mon Nov 24 16:29 - 17:36  (01:06)
reboot   system boot  5.10.0-36-amd64  Mon Nov 24 16:25 - 17:36  (01:10)
trainee  pts/0        10.0.2.1         Mon Nov 24 15:27 - 16:25  (00:57)
reboot   system boot  5.10.0-26-amd64  Mon Nov 24 15:27 - 16:25  (00:57)
trainee  pts/0        10.0.2.1         Mon Oct 16 12:26 - crash (770+04:00)
```

```
reboot   system boot  5.10.0-26-amd64  Mon Oct 16 08:43 - 16:25 (770+08:41)
trainee  pts/0        10.0.2.1         Sat Oct 14 07:48 - crash (2+00:55)
reboot   system boot  5.10.0-13-amd64  Thu Oct 12 12:53 - 16:25 (774+04:31)
reboot   system boot  5.10.0-13-amd64  Sun Jul 10 12:40 - 16:25 (1233+04:45)
trainee  tty7         :0               Sun Jul 10 12:29 - crash  (00:10)
reboot   system boot  5.10.0-13-amd64  Sun Jul 10 12:29 - 16:25 (1233+04:55)
trainee  tty7         :0               Sun Jul 10 12:27 - 12:29  (00:01)
reboot   system boot  5.10.0-13-amd64  Sun Jul 10 12:26 - 12:29  (00:02)
trainee  tty7         :0               Mon Jul  4 13:32 - crash (5+22:54)
reboot   system boot  5.10.0-13-amd64  Mon Jul  4 13:31 - 12:29 (5+22:57)
reboot   system boot  5.10.0-13-amd64  Sat Jun 18 08:54 - 09:04  (00:10)
trainee  pts/0        10.0.2.1         Sat Jun 18 08:48 - 08:54  (00:05)
reboot   system boot  5.10.0-13-amd64  Sat Jun 18 08:48 - 08:54  (00:05)
trainee  pts/1        10.0.2.1         Sat Jun 18 08:11 - crash  (00:36)
trainee  tty7         :0               Sat Jun 18 07:58 - crash  (00:50)
reboot   system boot  5.10.0-13-amd64  Sat Jun 18 07:56 - 08:54  (00:57)
trainee  pts/0        10.0.2.1         Sun May  1 10:38 - 10:39  (00:01)
reboot   system boot  5.10.0-13-amd64  Sun May  1 10:38 - 08:54 (47+22:15)
trainee  pts/1        10.0.2.1         Mon Apr 25 07:05 - 07:05  (00:00)
trainee  tty7         :0               Mon Apr 25 07:03 - crash (6+03:34)
reboot   system boot  5.10.0-13-amd64  Mon Apr 25 07:01 - 08:54 (54+01:52)

wtmp begins Mon Apr 25 07:01:57 2022
```

La commande lastlog

Cette commande indique les dates et heures de la connexion au système la plus récente des utilisateurs :

```
root@debian12:~# lastlog
Username         Port     From                                       Latest
root                                                               **Never logged in**
daemon                                                             **Never logged in**
bin                                                                **Never logged in**
```

```
sys                                                     **Never logged in**
sync                                                    **Never logged in**
games                                                   **Never logged in**
man                                                     **Never logged in**
lp                                                      **Never logged in**
mail                                                    **Never logged in**
news                                                    **Never logged in**
uucp                                                    **Never logged in**
proxy                                                   **Never logged in**
www-data                                                **Never logged in**
backup                                                  **Never logged in**
list                                                    **Never logged in**
irc                                                     **Never logged in**
gnats                                                   **Never logged in**
nobody                                                  **Never logged in**
_apt                                                    **Never logged in**
systemd-network                                         **Never logged in**
systemd-resolve                                         **Never logged in**
messagebus                                              **Never logged in**
systemd-timesync                                        **Never logged in**
usbmux                                                  **Never logged in**
rtkit                                                   **Never logged in**
dnsmasq                                                 **Never logged in**
avahi                                                   **Never logged in**
speech-dispatcher                                        **Never logged in**
pulse                                                   **Never logged in**
saned                                                   **Never logged in**
colord                                                  **Never logged in**
lightdm                                                 **Never logged in**
trainee          pts/2    10.0.2.1                      Thu Nov 27 12:08:14 +0100 2025
systemd-coredump                                        **Never logged in**
sshd                                                    **Never logged in**
polkitd                                                 **Never logged in**
```

La Commande lastb

Cette commande indique les dates et heures des connexions infructueueses des utilisateurs à partir du contenu du fichier **/var/log/btmp** :

```
root@debian12:~# lastb

btmp begins Mon Nov 24 15:27:36 2025

root@debian12:~# exit
logout

trainee@debian12:~$ su -
Password: stagiaire
su: Authentication failure

trainee@debian12:~$ su -
Password: fenestros

root@debian12:~# lastb
root     pts/2                         Thu Nov 27 14:10 - 14:10  (00:00)

btmp begins Thu Nov 27 14:10:38 2025
```

/var/log/auth.log

Sous Debian ce fichier contient la journalisation des opérations de gestion des authentifications :

```
root@debian12:~# tail -n 15 /var/log/auth.log
2025-11-27T12:24:16.056759+01:00 debian12 systemd-logind[587]: Watching system buttons on /dev/input/event0 (AT
Translated Set 2 keyboard)
2025-11-27T12:25:31.173844+01:00 debian12 su[4281]: pam_unix(su-l:session): session closed for user root
2025-11-27T12:25:38.248068+01:00 debian12 su[5663]: (to root) trainee on pts/2
```

```
2025-11-27T12:25:38.248250+01:00 debian12 su[5663]: pam_unix(su-l:session): session opened for user root(uid=0)
by trainee(uid=1000)
2025-11-27T12:30:01.905701+01:00 debian12 CRON[6574]: pam_unix(cron:session): session opened for user root(uid=0)
by (uid=0)
2025-11-27T12:30:01.936039+01:00 debian12 CRON[6574]: pam_unix(cron:session): session closed for user root
2025-11-27T13:17:01.948466+01:00 debian12 CRON[6602]: pam_unix(cron:session): session opened for user root(uid=0)
by (uid=0)
2025-11-27T13:17:02.019129+01:00 debian12 CRON[6602]: pam_unix(cron:session): session closed for user root
2025-11-27T13:30:01.958236+01:00 debian12 CRON[6611]: pam_unix(cron:session): session opened for user root(uid=0)
by (uid=0)
2025-11-27T13:30:02.027208+01:00 debian12 CRON[6611]: pam_unix(cron:session): session closed for user root
2025-11-27T14:10:21.963600+01:00 debian12 su[5663]: pam_unix(su-l:session): session closed for user root
2025-11-27T14:10:36.377777+01:00 debian12 su: pam_unix(su-l:auth): authentication failure; logname=trainee
uid=1000 euid=0 tty=/dev/pts/2 ruser=trainee rhost=  user=root
2025-11-27T14:10:38.301943+01:00 debian12 su[8296]: FAILED SU (to root) trainee on pts/2
2025-11-27T14:10:49.456601+01:00 debian12 su[8297]: (to root) trainee on pts/2
2025-11-27T14:10:49.456783+01:00 debian12 su[8297]: pam_unix(su-l:session): session opened for user root(uid=0)
by trainee(uid=1000)
```

Important - Sous Red Hat, consultez le fichier **/var/log/secure**.

Les Contre-Mesures

Les contre-mesures incluent le renforcement de la sécurité des comptes et l'utilisation des mots de passe complexes.

LAB #1 - Renforcer la sécurité des comptes

Passez en revue le fichier **/etc/passwd** :

```
root@debian12:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:106:113:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:114:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:109:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:110:116:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:111:119::/var/lib/saned:/usr/sbin/nologin
colord:x:112:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
lightdm:x:113:121:Light Display Manager:/var/lib/lightdm:/bin/false
trainee:x:1000:1000:trainee,,,:/home/trainee:/bin/bash
```

```
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:114:65534::/run/sshd:/usr/sbin/nologin
polkitd:x:998:998:polkit:/nonexistent:/usr/sbin/nologin
prison:x:501:502:chroot_user:/home/prison:/bin/chroot
```

Important : Notez que la valeur de l'UID de root est toujours de 0. Notez cependant que sous RHEL 5 et 6 les UID des utilisateurs normaux commencent à **500** et les UID des comptes système sont inclus entre 1 et 99 par convention. Sous RHEL 7, 8 et 9, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 201 et 999. Sous Debian 6, 7 et 8 les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 999 par convention. Sous openSUSE, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 499. Sous Ubuntu, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 999.

Chaque ligne est constituée de 7 champs :

- Le nom d'utilisateur
- Le mot de passe. Une valeur de **x** dans ce champs indique que le système utilise le fichier **/etc/shadow** pour stocker les mots de passe.
- L'UID. Une valeur unique qui est utilisée pour déterminée les droits aux fichiers et aux répertoires.
- Le GID. Une valeur indiquant le groupe **principal** de l'utilisateur
- Le nom complet. Ce champs optionnel est aussi appelé **GECOS**
- Le répertoire personnel de l'utilisateur
- Le shell de l'utilisateur.

Notez d'abord les utilisateurs inutiles. Par exemple, dans le cas ci-dessus, l'utilisateur suivant est inutile si vous ne souhaitez par imprimer a partir du serveur:

```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

Supprimez donc les utilisateurs et groupes inutiles en utilisant des commandes telles:

```
# userdel -r lp [Entree]
```

```
# groupdel lp [Entree]
```

Pour les utilisateurs restants, utilisez le système de shadowing :

```
root@debian12:~# cat /etc/shadow
root:$y$j9T$3oULwcP4KCW0crXb9zLB90$Tqr6eSITrKaEnKecir1vRGXpa1OdRRi3/Q.gLwLPph/:19107:0:99999:7:::
daemon:*:19107:0:99999:7:::
bin:*:19107:0:99999:7:::
sys:*:19107:0:99999:7:::
sync:*:19107:0:99999:7:::
games:*:19107:0:99999:7:::
man:*:19107:0:99999:7:::
lp:*:19107:0:99999:7:::
mail:*:19107:0:99999:7:::
news:*:19107:0:99999:7:::
uucp:*:19107:0:99999:7:::
proxy:*:19107:0:99999:7:::
www-data:*:19107:0:99999:7:::
backup:*:19107:0:99999:7:::
list:*:19107:0:99999:7:::
irc:*:19107:0:99999:7:::
gnats:*:19107:0:99999:7:::
nobody:*:19107:0:99999:7:::
_apt:*:19107:0:99999:7:::
systemd-network:*:19107:0:99999:7:::
systemd-resolve:*:19107:0:99999:7:::
messagebus:*:19107:0:99999:7:::
systemd-timesync:*:19107:0:99999:7:::
usbmux:*:19107:0:99999:7:::
rtkit:*:19107:0:99999:7:::
```

```
dnsmasq:*:19107:0:99999:7:::
avahi:*:19107:0:99999:7:::
speech-dispatcher:!:19107:0:99999:7:::
pulse:*:19107:0:99999:7:::
saned:*:19107:0:99999:7:::
colord:*:19107:0:99999:7:::
lightdm:*:19107:0:99999:7:::
trainee:$y$j9T$iKJ5MC8LmULY.yq58DCjw1$WsIdItQEonaSeCFZil61bk4YPxSp1.5aFg0uDhwIbZC:19107:0:99999:7:::
systemd-coredump:!*:19107::::::
sshd:*:19107:0:99999:7:::
polkitd:!*:20416::::::
```

Chaque ligne est constituée de 8 champs :

- Le nom de l'utilisateur. Ce champs est utilisé pour faire le lien avec le fichier **/etc/passwd**,
- Le mot de passe **crypté** de l'utilisateur. Le cryptage est à sens **unique**. Ce champ peut aussi contenir une des trois valeurs suivantes :
  - **!!** - Le mot de passe n'a pas encore été défini et l'utilisateur ne peut pas se connecter,
  - * - L'utilisateur ne peut pas se connecter,
  - **vide** - aucun mot de passe sera demandé pour l'utilisateur concerné,
- Le nombre de jours entre le **01/01/1970** et le dernier changement du mot de passe,
- Le nombre de jours que le mot de passe est encore valide. Une valeur de **0** dans ce champs indique sue le mot de passe n'expire jamais,
- Le nombre de jours après lequel le mot de passe doit être changé,
- Le nombre de jours avant la date de modification forcée que l'utilisateur recevra un avertissement,
- Le nombre de jours après l'expiration du mot de passe que le compte sera désactivé,
- Le **numéro** du jour après le **01/01/1970** que le compte a été désactivé.

LAB #2 - PAM

PAM (*Pluggable Authentification Modules* ou Modules d'Authentification Enfichables) est une architecture modulaire permettant à l'administrateur système de définir une politique d'authentification pour les logiciels prenant en charge PAM.

Les fichiers de configuration se trouvent dans le répertoire **/etc/pam.d** :

```
root@debian12:~# ls -l /etc/pam.d
total 104
-rw-r--r-- 1 root root  384 Feb  7  2020 chfn
-rw-r--r-- 1 root root   92 Feb  7  2020 chpasswd
-rw-r--r-- 1 root root  581 Feb  7  2020 chsh
-rw-r--r-- 1 root root 1208 Nov 24 17:27 common-account
-rw-r--r-- 1 root root 1214 Nov 24 17:27 common-auth
-rw-r--r-- 1 root root 1660 Nov 24 17:27 common-password
-rw-r--r-- 1 root root 1146 Nov 24 17:27 common-session
-rw-r--r-- 1 root root 1154 Nov 24 17:27 common-session-noninteractive
-rw-r--r-- 1 root root  606 Feb 22  2021 cron
-rw-r--r-- 1 root root   69 May 27  2021 cups
-rw-r--r-- 1 root root 1354 Feb  3  2020 lightdm
-rw-r--r-- 1 root root 1428 Feb  3  2020 lightdm-autologin
-rw-r--r-- 1 root root  493 Feb  3  2020 lightdm-greeter
-rw-r--r-- 1 root root 4126 Feb  7  2020 login
-rw-r--r-- 1 root root   92 Feb  7  2020 newusers
-rw-r--r-- 1 root root  520 Jan 30  2021 other
-rw-r--r-- 1 root root   92 Feb  7  2020 passwd
-rw-r--r-- 1 root root  168 Jan  7  2021 ppp
-rw-r--r-- 1 root root  143 Jan 20  2022 runuser
-rw-r--r-- 1 root root  138 Jan 20  2022 runuser-l
-rw-r--r-- 1 root root 2133 Mar 13  2021 sshd
-rw-r--r-- 1 root root 2259 Jan 20  2022 su
-rw-r--r-- 1 root root  185 Jun 24 09:22 sudo
-rw-r--r-- 1 root root  170 Jun 24 09:22 sudo-i
-rw-r--r-- 1 root root  137 Jan 20  2022 su-l
```

Ces fichiers ont une structure spécifique et sont nommés d'après le service ou l'application qu'ils contrôlent. Leur contenu fait appel à des modules qui se trouvent dans le répertoire **/lib/x86_64-linux-gnu/security** :

```
root@debian12:~# ls /lib/x86_64-linux-gnu/security
pam_access.so         pam_issue.so      pam_permit.so      pam_time.so
pam_debug.so          pam_keyinit.so    pam_pwhistory.so   pam_timestamp.so
```

```
pam_deny.so            pam_lastlog.so    pam_rhosts.so      pam_tty_audit.so
pam_echo.so            pam_limits.so     pam_rootok.so      pam_umask.so
pam_env.so             pam_listfile.so   pam_securetty.so   pam_unix.so
pam_exec.so            pam_localuser.so  pam_selinux.so     pam_userdb.so
pam_faildelay.so       pam_loginuid.so   pam_sepermit.so    pam_usertype.so
pam_faillock.so        pam_mail.so       pam_setquota.so    pam_warn.so
pam_filter.so          pam_mkhomedir.so  pam_shells.so      pam_wheel.so
pam_ftp.so             pam_motd.so       pam_stress.so      pam_xauth.so
pam_gnome_keyring.so   pam_namespace.so  pam_succeed_if.so
pam_group.so           pam_nologin.so    pam_systemd.so
```

Les modules les plus importants sont :

Module	**Description**
pam_access.so	Ce module est utilisé pour interdire l'accès aux services sécurisés par des hôtes non-autorisés.
pam_echo.so	Ce module présente le contenu du fichier passé en argument à tout utilisateur lors de sa connexion.
pam_limits.so	Ce module implémente les limites des ressources détaillées dans le fichier **/etc/security/limits.conf** et dans les fichiers ***.conf** trouvés dans le répertoire **/etc/security/limits.d/**.
pam_listfile.so	Ce module est utilisé pour consulter un fichier spécifique pour vérifier les authiorisations. Par exemple, le service ftp utilise ce module pour consulter le fichier **/etc/ftpusers** qui contient une liste d'utilisateurs qui ne sont **pas** autorisés à se connecter au serveur ftp.
pam_nologin.so	Ce module interdit les connexions d'utilisteurs, autre que root, dans le cas où le fichier **/etc/nologin** est présent.
pam_securetty.so	Ce module interdit des connexions de root à partir des périphériques tty qui ne sont pas listés dans le fichier **/etc/securetty**.
pam_unix.so	Ce module est utilisé pour vérifier les informations suivantes ; expire, last_change, max_change, min_change, warn_change.

Chaque fichier dans /etc/pam.d contient les règles PAM utilisées pendant l'authentification. Ouvrez le fichier **login** :

```
root@debian12:~# cat /etc/pam.d/login
#
# The PAM configuration file for the Shadow `login' service
#

# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
```

```
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth       optional   pam_faildelay.so  delay=3000000

# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth       required   pam_issue.so issue=/etc/issue

# Disallows other than root logins when /etc/nologin exists
# (Replaces the `NOLOGINS_FILE' option from login.defs)
auth       requisite  pam_nologin.so

# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible
# that a module could execute code in the wrong domain.
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close

# Sets the loginuid process attribute
session    required     pam_loginuid.so

# Prints the message of the day upon successful login.
# (Replaces the `MOTD_FILE' option in login.defs)
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional   pam_motd.so motd=/run/motd.dynamic
session    optional   pam_motd.so noupdate

# SELinux needs to intervene at login time to ensure that the process
# starts in the proper default security context. Only sessions which are
# intended to run in the user's context should be run after this.
# pam_selinux.so changes the SELinux context of the used TTY and configures
# SELinux in order to transition to the user context with the next execve()
```

```
# call.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so open
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)

# This module parses environment configuration file(s)
# and also allows you to use an extended config
# file /etc/security/pam_env.conf.
#
# parsing /etc/environment needs "readenv=1"
session       required   pam_env.so readenv=1
# locale variables are also kept into /etc/default/locale in etch
# reading this file *in addition to /etc/environment* does not hurt
session       required   pam_env.so readenv=1 envfile=/etc/default/locale

# Standard Un*x authentication.
@include common-auth

# This allows certain extra groups to be granted to a user
# based on things like time of day, tty, service, and user.
# Please edit /etc/security/group.conf to fit your needs
# (Replaces the `CONSOLE_GROUPS' option in login.defs)
auth       optional   pam_group.so

# Uncomment and edit /etc/security/time.conf if you need to set
# time restraint on logins.
# (Replaces the `PORTTIME_CHECKS_ENAB' option from login.defs
# as well as /etc/porttime)
# account    requisite  pam_time.so

# Uncomment and edit /etc/security/access.conf if you need to
# set access limits.
# (Replaces /etc/login.access file)
# account  required       pam_access.so
```

```
# Sets up user limits according to /etc/security/limits.conf
# (Replaces the use of /etc/limits in old login)
session    required   pam_limits.so

# Prints the last login info upon successful login
# (Replaces the `LASTLOG_ENAB' option from login.defs)
session    optional   pam_lastlog.so

# Prints the status of the user's mailbox upon successful login
# (Replaces the `MAIL_CHECK_ENAB' option from login.defs).
#
# This also defines the MAIL environment variable
# However, userdel also needs MAIL_DIR and MAIL_FILE variables
# in /etc/login.defs to make sure that removing a user
# also removes the user's mail spool file.
# See comments in /etc/login.defs
session    optional   pam_mail.so standard

# Create a new session keyring.
session    optional   pam_keyinit.so force revoke

# Standard Un*x account and session
@include common-account
@include common-session
@include common-password
```

La première ligne de ce fichier est un commentaire qui spécifie que le fichier est conforme à la spécification PAM 1.0.

Ce fichier, tout comme les autres, est ensuite structuré de la façon suivante :

- Une module par ligne,
- Quatre champs séparés par un espace dans chaque règle dont les trois premières sont obligatoires.

Le **premier champs** est le ***type de module***. Il en existe quatre :

Type	Description
auth	Utilisé pour authentifier un utilisateur ou les pré-requis système (par exemple /etc/nologin)
account	Utilisé pour vérifier si l'utilisateur peut s'authentifier (par exemple la validité du compte)
password	Utilisé pour vérifier si l'utilisateur dispose des droits pour mettre le mécanisme d'authentification à jour
session	Utilisé pour gérer la session après l'authentification (par exemple monter un répertoire)

Le **deuxième champs** est le ***Control-flag***. Il en existe quatre :

Control-flag	Description
required	La réussite de ce module est indispensable. L'échec d'un module *required* n'est communiqué à l'application qu'après la vérification de tous les modules ayant un *control-flag* de **required**
requisite	La réussite de ce module est indispensable. L'échec d'un module *requisite* est immédiatement communiqué à l'application
sufficient	La réussite de ce module est suffisant pour authoriser l'authentification. Si aucun test *required* précédent est en échec, la vérification s'arrête. Si un test *required* précédent était en échec, le test *sufficient* est ignoré. L'échec d'un test *sufficient* n'a pas de conséquence si tous les tests *required* réussissent.
optional	La réussite ou l'échec de ce module est sans importance, **sauf** s'il s'agit du seul module à exécuter
@include	Ce control-flag permet d'inclure toutes les lignes du même *type de module* se trouvant dans le fichier spécifié en argument

Le **troisième champs** stipule le ***module*** associé à la règle. Sans chemin absolu, le fichier est supposé être dans le répertoire **/lib/x86_64-linux-gnu/security**. Pour inclure un module en dehors de ce répertoire il convient donc de stipuler son chemin absolu.

Le **quatrième champs** contient éventuellement les **arguments**.

Dernièrement, PAM propose une solution pour toutes les applications ne disposant pas de leurs propres fichiers de configuration PAM. Cette solution prend la forme du fichier **/etc/pam.d/other** :

```
root@debian12:~# cat /etc/pam.d/other
#
# /etc/pam.d/other - specify the PAM fallback behaviour
#
# Note that this file is used for any unspecified service; for example
#if /etc/pam.d/cron  specifies no session modules but cron calls
#pam_open_session, the session module out of /etc/pam.d/other is
#used.  If you really want nothing to happen then use pam_permit.so or
```

```
#pam_deny.so as appropriate.

# We fall back to the system default in /etc/pam.d/common-*
#

@include common-auth
@include common-account
@include common-password
@include common-session
```

2.1 - Configuration des modules

Certains modules de PAM peuvent être configurés grâce aux fichiers présents dans le répertoire **/etc/security** :

```
root@debian12:~# ls -l /etc/security
total 48
-rw-r--r-- 1 root root 4564 Aug 26  2021 access.conf
-rw-r--r-- 1 root root 2234 Aug 26  2021 faillock.conf
-rw-r--r-- 1 root root 3635 Aug 26  2021 group.conf
-rw-r--r-- 1 root root 2752 Sep 21  2023 limits.conf
drwxr-xr-x 2 root root 4096 Nov 24 17:26 limits.d
-rw-r--r-- 1 root root 1637 Aug 26  2021 namespace.conf
drwxr-xr-x 2 root root 4096 Aug 26  2021 namespace.d
-rwxr-xr-x 1 root root 1016 Sep 21  2023 namespace.init
-rw------- 1 root root    0 Apr 25  2022 opasswd
-rw-r--r-- 1 root root 2971 Aug 26  2021 pam_env.conf
-rw-r--r-- 1 root root  418 Sep 21  2023 sepermit.conf
-rw-r--r-- 1 root root 2179 Aug 26  2021 time.conf
```

Parmi les fichiers cités on note ceux qui peuvent être utilisés pour configurer les modules suivants :

Fichier/*Répertoire*	**Module**

Fichier/*Répertoire*	**Module**
access.conf	pam_access.so
faillock.conf	pam_faillock.so
group.conf	pam_group.so
limits.conf	pam_limits.so
namespace.conf	pam_namespace.so
pam_env.conf	pam_env.so
sepermit.conf	pam_sepermit.so
time.conf	pam_time.so

2.2 - Utiliser des Mots de Passe Complexes

La complexité des mots de passe est gérée par le module **pam_pwquality.so**. Commencez par installer **libpam-pwquality** :

```
root@debian12:~# apt-get -y install libpam-pwquality
```

Vérifiez la présence du module :

```
root@debian12:~# ls /lib/x86_64-linux-gnu/security | grep quality
pam_pwquality.so
```

L'installation du module a aussi installé un fichier de configuration :

```
root@debian12:~# ls -l /etc/security/pwquality.conf
-rw-r--r-- 1 root root 2674 Dec 15  2022 /etc/security/pwquality.conf
```

Afin de mettre en place une politique de mots de passe complexe, il convient de modifier le fichier **/etc/security/pwquality.conf** :

```
root@debian12:~# vi /etc/security/pwquality.conf
root@debian12:~# cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
```

```
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -2
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
minclass = 4
#
# The maximum number of allowed consecutive same characters in the new password.
```

```
# The check is disabled if the value is 0.
# maxrepeat = 0
#
# The maximum number of allowed consecutive characters of the same class in the
# new password.
# The check is disabled if the value is 0.
# maxclassrepeat = 0
#
# Whether to check for the words from the passwd entry GECOS string of the user.
# The check is enabled if the value is not 0.
gecoscheck = 1
#
# Whether to check for the words from the cracklib dictionary.
# The check is enabled if the value is not 0.
dictcheck = 1
#
# Whether to check if it contains the user name in some form.
# The check is enabled if the value is not 0.
usercheck = 1
#
# Length of substrings from the username to check for in the password
# The check is enabled if the value is greater than 0 and usercheck is enabled.
# usersubstr = 0
#
# Whether the check is enforced by the PAM module and possibly other
# applications.
# The new password is rejected if it fails the check and the value is not 0.
enforcing = 1
#
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
#
# Prompt user at most N times before returning with error. The default is 1.
# retry = 3
```

```
#
# Enforces pwquality checks on the root user password.
# Enabled if the option is present.
# enforce_for_root
#
# Skip testing the password quality for users that are not present in the
# /etc/passwd file.
# Enabled if the option is present.
# local_users_only
```

LAB #3 - Mise en place du Système de Prévention d'Intrusion Fail2Ban

Fail2Ban est un **S**ystème de **P**révention d'**I**ntrusion. Fail2Ban lit les logs de divers services (SSH, Apache, FTP...) à la recherche d'erreurs d'authentification répétées et ajoute une règle à iptables pour bannir l'adresse IP de la source.

3.1 - Installation

Utilisez APT pour installer fail2ban :

```
root@debian12:~# apt install fail2ban
```

3.2 - Configuration

La configuration de Fail2Ban se trouve dans le fichier **/etc/fail2ban/jail.conf** :

```
root@debian12:~# more /etc/fail2ban/jail.conf
#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
```

```
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information



# Comments: use '#' for comment lines and ';' (following a space) for inline comments


[INCLUDES]

#before = paths-distro.conf
before = paths-debian.conf
```

```
# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.

[DEFAULT]

#
# MISCELLANEOUS OPTIONS
#

# "bantime.increment" allows to use database for searching of previously banned ip's to increase a
# default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
#bantime.increment = true

# "bantime.rndtime" is the max number of seconds using for mixing with random time
# to prevent "clever" botnets calculate exact time IP can be unbanned again:
#bantime.rndtime =

# "bantime.maxtime" is the max number of seconds using the ban time can reach (doesn't grow further)
--More--(6%)
```

Dans ce fichier se trouvent des sections pour configurer l'action de Fail2Ban pour chaque service :

```
...
[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 details.
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

Ces sections, appelées des Prisons (*Jails* en anglais), peuvent contenir des directives telles que :

Directive	Description
enabled	Indique si oui (true) ou non (false) le prison est activé.
port	Le port à bloquer dans iptables.
filter	Le nom du filtre, une expression régulière, associé au prison et utilisé pour trouver une activité suspect. Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire **/etc/fail2ban/filter.d/**. Par exemple la valeur **sshd** fait reférence au fichier **/etc/fail2ban/filter.d/sshd.conf**.
logpath	Le nom et le chemin du journal à examiner.
maxretry	Le nombre maximal de tentatives.
action	Spécifie l'action à entreprendre lors d'une corréspondance du **filter**. Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire **/etc/fail2ban/action.d/**. Par exemple la valeur **iptables** fait reférence au fichier **/etc/fail2ban/action.d/iptables.conf**.
mode	Spécifie un comportement spécifique pour le filtre, annulant ses paramètres par défaut. Les modes disponibles offrent différents niveaux de sensibilité de détection, tels que normal, rbl (Real-time Blackhole List), aggressive (qui combine les paramètres normaux et agressifs), et ddos. En spécifiant un mode, vous pouvez ajuster la sensibilité du filtre pour un service ou une jail particulier, lui demandant d'utiliser des critères différents pour faire correspondre les entrées de journal.

Il n'est pas recommendé de modifier ce fichier afin de ne pas voir ses modifications ecrasées lors de la prochaine mise-à-jour de Fail2Ban. Fail2Ban nous donne la possibilité de créer le fichier **/etc/fail2ban/jail.local** pour contenir nos modifications. Créez donc ce fichier avec le contenu ci-dessous :

```
root@debian12:~# vi /etc/fail2ban/jail.local

root@debian12:~# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 172.YY+20.0.3
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true
```

Il est à noter que les directives dans le fichier **jail.conf** sont surchargées par celles dans les fichiers suivantes et dans l'ordre suivant :

- **/etc/fail2ban/jail.d/*.conf** dans l'ordre alphabétique,

- **/etc/fail2ban/jail.local**,
- **/etc/fail2ban/jail.d/*.local** dans l'ordre alphabétique.

Important - Notez que la définition des variables dans la section **[DEFAULT]** du fichier **/etc/fail2ban/jail.local** s'appliquent à toutes les sections de prisons actives dans les fichiers **/etc/fail2ban/jail.local** et **/etc/fail2ban/jail.conf** sauf si dans la section du prison elle-même, la variable est redéfinie.

Dans ce fichier, les directives sont donc :

Directive	Description
ignoreip	Liste des adresses IP, séparées par un **espace**, qui ne sont pas concernées par l'action de Fail2Ban ou une liste d'adresses de réseaux, exprimées au format CIDR.
findtime	L'intervale de temps en secondes, avant l'heure actuelle, pendant laquelle des authentifications infructueueses sont prises en compte pour le calcul de banir l'adresse IP ou non.
bantime	La durée de vie des règles, en secondes, inscrites dans le pare-feu iptables.
maxretry	Le nombre maximal de tentatives. La règle sera donc inscrite dans le pare-feu lors de la sixième tentative.

Le répertoire /etc/fail2ban

Le répertoire **/etc/fail2ban/** contient des fichiers et répertoires importants pour le fonctionnement de Fail2Ban :

```
root@debian12:~# ls -l /etc/fail2ban/
total 68
drwxr-xr-x 2 root root  4096 Nov 27 14:37 action.d
-rw-r--r-- 1 root root  3017 Nov  9  2022 fail2ban.conf
drwxr-xr-x 2 root root  4096 Apr 21  2023 fail2ban.d
drwxr-xr-x 3 root root  4096 Nov 27 14:37 filter.d
-rw-r--r-- 1 root root 25607 Nov  9  2022 jail.conf
drwxr-xr-x 2 root root  4096 Nov 27 14:37 jail.d
```

```
-rw-r--r-- 1 root root   114 Nov 27 14:44 jail.local
-rw-r--r-- 1 root root   645 Nov  9  2022 paths-arch.conf
-rw-r--r-- 1 root root  2728 Nov  9  2022 paths-common.conf
-rw-r--r-- 1 root root   627 Nov  9  2022 paths-debian.conf
-rw-r--r-- 1 root root   738 Nov  9  2022 paths-opensuse.conf
```

Le fichier fail2ban.conf

Ce fichier définit les configurations globales de Fail2Ban, telles le **pidfile**, le **socket** et le niveau syslog de journalisation :

```
root@debian12:~# cat /etc/fail2ban/fail2ban.conf
# Fail2Ban main configuration file
#
# Comments: use '#' for comment lines and ';' (following a space) for inline comments
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in fail2ban.local file, e.g.:
#
# [DEFAULT]
# loglevel = DEBUG
#

[DEFAULT]

# Option: loglevel
# Notes.: Set the log level output.
#         CRITICAL
#         ERROR
#         WARNING
#         NOTICE
#         INFO
#         DEBUG
# Values: [ LEVEL ]  Default: INFO
```

```
#
loglevel = INFO

# Option: logtarget
# Notes.: Set the log target. This could be a file, SYSTEMD-JOURNAL, SYSLOG, STDERR or STDOUT.
#         Only one log target can be specified.
#         If you change logtarget from the default value and you are
#         using logrotate -- also adjust or disable rotation in the
#         corresponding configuration file
#         (e.g. /etc/logrotate.d/fail2ban on Debian systems)
# Values: [ STDOUT | STDERR | SYSLOG | SYSOUT | SYSTEMD-JOURNAL | FILE ]  Default: STDERR
#
logtarget = /var/log/fail2ban.log

# Option: syslogsocket
# Notes: Set the syslog socket file. Only used when logtarget is SYSLOG
#        auto uses platform.system() to determine predefined paths
# Values: [ auto | FILE ]  Default: auto
syslogsocket = auto

# Option: socket
# Notes.: Set the socket file. This is used to communicate with the daemon. Do
#         not remove this file when Fail2ban runs. It will not be possible to
#         communicate with the server afterwards.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.sock
#
socket = /var/run/fail2ban/fail2ban.sock

# Option: pidfile
# Notes.: Set the PID file. This is used to store the process ID of the
#         fail2ban server.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.pid
#
pidfile = /var/run/fail2ban/fail2ban.pid
```

```
# Option: allowipv6
# Notes.: Allows IPv6 interface:
#         Default: auto
# Values: [ auto yes (on, true, 1) no (off, false, 0) ] Default: auto
#allowipv6 = auto

# Options: dbfile
# Notes.: Set the file for the fail2ban persistent data to be stored.
#         A value of ":memory:" means database is only stored in memory
#         and data is lost when fail2ban is stopped.
#         A value of "None" disables the database.
# Values: [ None :memory: FILE ] Default: /var/lib/fail2ban/fail2ban.sqlite3
dbfile = /var/lib/fail2ban/fail2ban.sqlite3

# Options: dbpurgeage
# Notes.: Sets age at which bans should be purged from the database
# Values: [ SECONDS ] Default: 86400 (24hours)
dbpurgeage = 1d

# Options: dbmaxmatches
# Notes.: Number of matches stored in database per ticket (resolvable via
#         tags <ipmatches>/<ipjailmatches> in actions)
# Values: [ INT ] Default: 10
dbmaxmatches = 10

[Definition]


[Thread]

# Options: stacksize
# Notes.: Specifies the stack size (in KiB) to be used for subsequently created threads,
#         and must be 0 or a positive integer value of at least 32.
# Values: [ SIZE ] Default: 0 (use platform or configured default)
```

```
#stacksize = 0
```

Le répertoire /etc/fail2ban/filter.d/

Ce répertoire contient les fichiers appelés par les directives **filter** dans les sections des prisons :

```
root@debian12:~# ls -l /etc/fail2ban/filter.d/
total 384
-rw-r--r-- 1 root root  467 Nov  9  2022 3proxy.conf
-rw-r--r-- 1 root root 3228 Nov  9  2022 apache-auth.conf
-rw-r--r-- 1 root root 2831 Nov  9  2022 apache-badbots.conf
-rw-r--r-- 1 root root 1265 Nov  9  2022 apache-botsearch.conf
-rw-r--r-- 1 root root 1619 Nov  9  2022 apache-common.conf
-rw-r--r-- 1 root root  403 Nov  9  2022 apache-fakegooglebot.conf
-rw-r--r-- 1 root root  511 Nov  9  2022 apache-modsecurity.conf
-rw-r--r-- 1 root root  596 Nov  9  2022 apache-nohome.conf
-rw-r--r-- 1 root root 1246 Nov  9  2022 apache-noscript.conf
-rw-r--r-- 1 root root 2187 Nov  9  2022 apache-overflows.conf
-rw-r--r-- 1 root root  362 Nov  9  2022 apache-pass.conf
-rw-r--r-- 1 root root 1020 Nov  9  2022 apache-shellshock.conf
-rw-r--r-- 1 root root 3492 Nov  9  2022 assp.conf
-rw-r--r-- 1 root root 2386 Nov  9  2022 asterisk.conf
-rw-r--r-- 1 root root  427 Nov  9  2022 bitwarden.conf
-rw-r--r-- 1 root root  522 Nov  9  2022 botsearch-common.conf
-rw-r--r-- 1 root root  307 Nov  9  2022 centreon.conf
-rw-r--r-- 1 root root 2776 Nov  9  2022 common.conf
-rw-r--r-- 1 root root  244 Nov  9  2022 counter-strike.conf
-rw-r--r-- 1 root root  463 Nov  9  2022 courier-auth.conf
-rw-r--r-- 1 root root  512 Nov  9  2022 courier-smtp.conf
-rw-r--r-- 1 root root  444 Nov  9  2022 cyrus-imap.conf
-rw-r--r-- 1 root root  338 Nov  9  2022 directadmin.conf
-rw-r--r-- 1 root root 2107 Nov  9  2022 domino-smtp.conf
-rw-r--r-- 1 root root 2647 Nov  9  2022 dovecot.conf
```

```
-rw-r--r-- 1 root root 1730 Nov  9  2022 dropbear.conf
-rw-r--r-- 1 root root  547 Nov  9  2022 drupal-auth.conf
-rw-r--r-- 1 root root 1572 Nov  9  2022 ejabberd-auth.conf
-rw-r--r-- 1 root root  534 Nov  9  2022 exim-common.conf
-rw-r--r-- 1 root root 2875 Nov  9  2022 exim.conf
-rw-r--r-- 1 root root 2158 Nov  9  2022 exim-spam.conf
-rw-r--r-- 1 root root 1922 Nov  9  2022 freeswitch.conf
-rw-r--r-- 1 root root 1210 Nov  9  2022 froxlor-auth.conf
-rw-r--r-- 1 root root  236 Nov  9  2022 gitlab.conf
-rw-r--r-- 1 root root  388 Nov  9  2022 grafana.conf
-rw-r--r-- 1 root root  236 Nov  9  2022 groupoffice.conf
-rw-r--r-- 1 root root  322 Nov  9  2022 gssftpd.conf
-rw-r--r-- 1 root root 1447 Nov  9  2022 guacamole.conf
-rw-r--r-- 1 root root 1170 Nov  9  2022 haproxy-http-auth.conf
-rw-r--r-- 1 root root  404 Nov  9  2022 horde.conf
drwxr-xr-x 2 root root 4096 Nov 27 14:37 ignorecommands
-rw-r--r-- 1 root root  938 Nov  9  2022 kerio.conf
-rw-r--r-- 1 root root  459 Nov  9  2022 lighttpd-auth.conf
-rw-r--r-- 1 root root 2279 Nov  9  2022 mongodb-auth.conf
-rw-r--r-- 1 root root  787 Nov  9  2022 monit.conf
-rw-r--r-- 1 root root  640 Nov  9  2022 monitorix.conf
-rw-r--r-- 1 root root  441 Nov  9  2022 mssql-auth.conf
-rw-r--r-- 1 root root  927 Nov  9  2022 murmur.conf
-rw-r--r-- 1 root root  953 Nov  9  2022 mysqld-auth.conf
-rw-r--r-- 1 root root  400 Nov  9  2022 nagios.conf
-rw-r--r-- 1 root root 1600 Nov  9  2022 named-refused.conf
-rw-r--r-- 1 root root  474 Nov  9  2022 nginx-bad-request.conf
-rw-r--r-- 1 root root  740 Nov  9  2022 nginx-botsearch.conf
-rw-r--r-- 1 root root 1048 Nov  9  2022 nginx-http-auth.conf
-rw-r--r-- 1 root root 1513 Nov  9  2022 nginx-limit-req.conf
-rw-r--r-- 1 root root  779 Nov  9  2022 nsd.conf
-rw-r--r-- 1 root root  452 Nov  9  2022 openhab.conf
-rw-r--r-- 1 root root  495 Nov  9  2022 openwebmail.conf
-rw-r--r-- 1 root root 1937 Nov  9  2022 oracleims.conf
```

```
-rw-r--r-- 1 root root  947 Nov  9  2022 pam-generic.conf
-rw-r--r-- 1 root root  568 Nov  9  2022 perdition.conf
-rw-r--r-- 1 root root  278 Nov  9  2022 phpmyadmin-syslog.conf
-rw-r--r-- 1 root root  891 Nov  9  2022 php-url-fopen.conf
-rw-r--r-- 1 root root  242 Nov  9  2022 portsentry.conf
-rw-r--r-- 1 root root 3222 Nov  9  2022 postfix.conf
-rw-r--r-- 1 root root 1163 Nov  9  2022 proftpd.conf
-rw-r--r-- 1 root root 2409 Nov  9  2022 pure-ftpd.conf
-rw-r--r-- 1 root root  795 Nov  9  2022 qmail.conf
-rw-r--r-- 1 root root 1374 Nov  9  2022 recidive.conf
-rw-r--r-- 1 root root 1541 Apr 21  2023 roundcube-auth.conf
-rw-r--r-- 1 root root  354 Nov  9  2022 scanlogd.conf
-rw-r--r-- 1 root root  821 Nov  9  2022 screensharingd.conf
-rw-r--r-- 1 root root  538 Nov  9  2022 selinux-common.conf
-rw-r--r-- 1 root root  570 Nov  9  2022 selinux-ssh.conf
-rw-r--r-- 1 root root  790 Nov  9  2022 sendmail-auth.conf
-rw-r--r-- 1 root root 2970 Nov  9  2022 sendmail-reject.conf
-rw-r--r-- 1 root root  371 Nov  9  2022 sieve.conf
-rw-r--r-- 1 root root  706 Nov  9  2022 slapd.conf
-rw-r--r-- 1 root root  451 Nov  9  2022 softethervpn.conf
-rw-r--r-- 1 root root  722 Nov  9  2022 sogo-auth.conf
-rw-r--r-- 1 root root 1094 Nov  9  2022 solid-pop3d.conf
-rw-r--r-- 1 root root  260 Nov  9  2022 squid.conf
-rw-r--r-- 1 root root  191 Nov  9  2022 squirrelmail.conf
-rw-r--r-- 1 root root 7879 Nov  9  2022 sshd.conf
-rw-r--r-- 1 root root  363 Nov  9  2022 stunnel.conf
-rw-r--r-- 1 root root  649 Nov  9  2022 suhosin.conf
-rw-r--r-- 1 root root  890 Nov  9  2022 tine20.conf
-rw-r--r-- 1 root root 2390 Nov  9  2022 traefik-auth.conf
-rw-r--r-- 1 root root  374 Nov  9  2022 uwimap-auth.conf
-rw-r--r-- 1 root root  637 Nov  9  2022 vsftpd.conf
-rw-r--r-- 1 root root  444 Nov  9  2022 webmin-auth.conf
-rw-r--r-- 1 root root  520 Nov  9  2022 wuftpd.conf
-rw-r--r-- 1 root root  521 Nov  9  2022 xinetd-fail.conf
```

```
-rw-r--r-- 1 root root  912 Nov  9  2022 znc-adminlog.conf
-rw-r--r-- 1 root root 1146 Nov  9  2022 zoneminder.conf
```

Le répertoire /etc/fail2ban/action.d/

Ce répertoire contient les fichiers appelés par les directives **action** dans les sections des prisons :

```
root@debian12:~# ls -l /etc/fail2ban/action.d/
total 288
-rw-r--r-- 1 root root 3748 Nov  9  2022 abuseipdb.conf
-rw-r--r-- 1 root root  587 Nov  9  2022 apf.conf
-rw-r--r-- 1 root root 1413 Nov  9  2022 apprise.conf
-rw-r--r-- 1 root root 2715 Nov  9  2022 blocklist_de.conf
-rw-r--r-- 1 root root 3226 Nov  9  2022 bsd-ipfw.conf
-rw-r--r-- 1 root root 3037 Nov  9  2022 cloudflare.conf
-rw-r--r-- 1 root root 3004 Nov  9  2022 cloudflare-token.conf
-rw-r--r-- 1 root root 4773 Nov  9  2022 complain.conf
-rw-r--r-- 1 root root 7684 Nov  9  2022 dshield.conf
-rw-r--r-- 1 root root 1717 Nov  9  2022 dummy.conf
-rw-r--r-- 1 root root 1501 Nov  9  2022 firewallcmd-allports.conf
-rw-r--r-- 1 root root 2649 Nov  9  2022 firewallcmd-common.conf
-rw-r--r-- 1 root root 3669 Nov  9  2022 firewallcmd-ipset.conf
-rw-r--r-- 1 root root 1270 Nov  9  2022 firewallcmd-multiport.conf
-rw-r--r-- 1 root root 1898 Nov  9  2022 firewallcmd-new.conf
-rw-r--r-- 1 root root 1021 Nov  9  2022 firewallcmd-rich-logging.conf
-rw-r--r-- 1 root root 1753 Nov  9  2022 firewallcmd-rich-rules.conf
-rw-r--r-- 1 root root  592 Nov  9  2022 helpers-common.conf
-rw-r--r-- 1 root root 1657 Nov  9  2022 hostsdeny.conf
-rw-r--r-- 1 root root 1573 Nov  9  2022 ipfilter.conf
-rw-r--r-- 1 root root 1505 Nov  9  2022 ipfw.conf
-rw-r--r-- 1 root root  291 Nov  9  2022 iptables-allports.conf
-rw-r--r-- 1 root root 4790 Nov  9  2022 iptables.conf
-rw-r--r-- 1 root root 2576 Nov  9  2022 iptables-ipset.conf
```

```
-rw-r--r-- 1 root root 1980 Nov  9  2022 iptables-ipset-proto4.conf
-rw-r--r-- 1 root root  814 Nov  9  2022 iptables-ipset-proto6-allports.conf
-rw-r--r-- 1 root root  773 Nov  9  2022 iptables-ipset-proto6.conf
-rw-r--r-- 1 root root  232 Nov  9  2022 iptables-multiport.conf
-rw-r--r-- 1 root root 2163 Nov  9  2022 iptables-multiport-log.conf
-rw-r--r-- 1 root root  332 Nov  9  2022 iptables-new.conf
-rw-r--r-- 1 root root 2842 Nov  9  2022 iptables-xt_recent-echo.conf
-rw-r--r-- 1 root root 4292 Nov  9  2022 ipthreat.conf
-rw-r--r-- 1 root root 2495 Nov  9  2022 mail-buffered.conf
-rw-r--r-- 1 root root 1757 Nov  9  2022 mail.conf
-rw-r--r-- 1 root root 1051 Nov  9  2022 mail-whois-common.conf
-rw-r--r-- 1 root root 1890 Nov  9  2022 mail-whois.conf
-rw-r--r-- 1 root root 2459 Nov  9  2022 mail-whois-lines.conf
-rw-r--r-- 1 root root 5321 Nov  9  2022 mynetwatchman.conf
-rw-r--r-- 1 root root 1493 Nov  9  2022 netscaler.conf
-rw-r--r-- 1 root root  383 Nov  9  2022 nftables-allports.conf
-rw-r--r-- 1 root root 6318 Nov  9  2022 nftables.conf
-rw-r--r-- 1 root root  384 Nov  9  2022 nftables-multiport.conf
-rw-r--r-- 1 root root 4010 Nov  9  2022 nginx-block-map.conf
-rw-r--r-- 1 root root 1524 Nov  9  2022 npf.conf
-rw-r--r-- 1 root root 3234 Nov  9  2022 nsupdate.conf
-rw-r--r-- 1 root root  497 Nov  9  2022 osx-afctl.conf
-rw-r--r-- 1 root root 2302 Nov  9  2022 osx-ipfw.conf
-rw-r--r-- 1 root root 3750 Nov  9  2022 pf.conf
-rw-r--r-- 1 root root 1023 Nov  9  2022 route.conf
-rw-r--r-- 1 root root 2806 Nov  9  2022 sendmail-buffered.conf
-rw-r--r-- 1 root root 1938 Nov  9  2022 sendmail-common.conf
-rw-r--r-- 1 root root  829 Nov  9  2022 sendmail.conf
-rw-r--r-- 1 root root 1761 Nov  9  2022 sendmail-geoip-lines.conf
-rw-r--r-- 1 root root  950 Nov  9  2022 sendmail-whois.conf
-rw-r--r-- 1 root root 1055 Nov  9  2022 sendmail-whois-ipjailmatches.conf
-rw-r--r-- 1 root root 1036 Nov  9  2022 sendmail-whois-ipmatches.conf
-rw-r--r-- 1 root root 1299 Nov  9  2022 sendmail-whois-lines.conf
-rw-r--r-- 1 root root 1000 Nov  9  2022 sendmail-whois-matches.conf
```

```
-rw-r--r-- 1 root root 2156 Nov  9  2022 shorewall.conf
-rw-r--r-- 1 root root 3521 Nov  9  2022 shorewall-ipset-proto6.conf
-rw-r--r-- 1 root root 6277 Nov  9  2022 smtp.py
-rw-r--r-- 1 root root 1503 Nov  9  2022 symbiosis-blacklist-allports.conf
-rw-r--r-- 1 root root 2379 Nov  9  2022 ufw.conf
-rw-r--r-- 1 root root 6443 Nov  9  2022 xarf-login-attack.conf
```

3.3 - Commandes

Fail2Ban est constitué de deux commandes :

```
root@debian12:~# which fail2ban-server
/usr/bin/fail2ban-server

root@debian12:~# which fail2ban-client
/usr/bin/fail2ban-client
```

L'exécutable **fail2ban-server** est responsable de l'examen des fichiers de journalisation ainsi que les commandes de blocage/déblocage. La commande fail2ban-client est utilisée pour configurer le **fail2ban-server**.

Les options de la commande **fail2ban-server** sont :

```
root@debian12:~# fail2ban-server --help
Usage: fail2ban-server [OPTIONS]

Fail2Ban v1.0.2 reads log file that contains password failure report
and bans the corresponding IP addresses using firewall rules.

Options:
    -c, --conf <DIR>        configuration directory
    -s, --socket <FILE>     socket path
    -p, --pidfile <FILE>    pidfile path
    --pname <NAME>          name of the process (main thread) to identify instance (default fail2ban-server)
```

```
    --loglevel <LEVEL>      logging level
    --logtarget <TARGET>    logging target, use file-name or stdout, stderr, syslog or sysout.
    --syslogsocket auto|<FILE>
    -d                      dump configuration. For debugging
    --dp, --dump-pretty     dump the configuration using more human readable representation
    -t, --test              test configuration (can be also specified with start parameters)
    -i                      interactive mode
    -v                      increase verbosity
    -q                      decrease verbosity
    -x                      force execution of the server (remove socket file)
    -b                      start server in background (default)
    -f                      start server in foreground
    --async                 start server in async mode (for internal usage only, don't read configuration)
    --timeout               timeout to wait for the server (for internal usage only, don't read configuration)
    --str2sec <STRING>      convert time abbreviation format to seconds
    -h, --help              display this help message
    -V, --version           print the version (-V returns machine-readable short format)

Report bugs to https://github.com/fail2ban/fail2ban/issues
```

Les options de la commande **fail2ban-client** sont :

```
root@debian12:~# fail2ban-client --help
Usage: fail2ban-client [OPTIONS] <COMMAND>

Fail2Ban v1.0.2 reads log file that contains password failure report
and bans the corresponding IP addresses using firewall rules.

Options:
    -c, --conf <DIR>        configuration directory
    -s, --socket <FILE>     socket path
    -p, --pidfile <FILE>    pidfile path
    --pname <NAME>          name of the process (main thread) to identify instance (default fail2ban-server)
    --loglevel <LEVEL>      logging level
```

```
    --logtarget <TARGET>    logging target, use file-name or stdout, stderr, syslog or sysout.
    --syslogsocket auto|<FILE>
    -d                      dump configuration. For debugging
    --dp, --dump-pretty     dump the configuration using more human readable representation
    -t, --test              test configuration (can be also specified with start parameters)
    -i                      interactive mode
    -v                      increase verbosity
    -q                      decrease verbosity
    -x                      force execution of the server (remove socket file)
    -b                      start server in background (default)
    -f                      start server in foreground
    --async                 start server in async mode (for internal usage only, don't read configuration)
    --timeout               timeout to wait for the server (for internal usage only, don't read configuration)
    --str2sec <STRING>      convert time abbreviation format to seconds
    -h, --help              display this help message
    -V, --version           print the version (-V returns machine-readable short format)

Command:
                                          BASIC
    start                                 starts the server and the jails
    restart                               restarts the server
    restart [--unban] [--if-exists] <JAIL>   restarts the jail <JAIL> (alias
                                          for 'reload --restart ... <JAIL>')
    reload [--restart] [--unban] [--all]     reloads the configuration without
                                          restarting of the server, the
                                          option '--restart' activates
                                          completely restarting of affected
                                          jails, thereby can unban IP
                                          addresses (if option '--unban'
                                          specified)
    reload [--restart] [--unban] [--if-exists] <JAIL>
                                          reloads the jail <JAIL>, or
                                          restarts it (if option '--restart'
                                          specified)
```

```
    stop                                stops all jails and terminate the
                                        server
    unban --all                         unbans all IP addresses (in all
                                        jails and database)
    unban <IP> ... <IP>                 unbans <IP> (in all jails and
                                        database)
    banned                              return jails with banned IPs as
                                        dictionary
    banned <IP> ... <IP>]               return list(s) of jails where
                                        given IP(s) are banned
    status                              gets the current status of the
                                        server
    ping                                tests if the server is alive
    echo                                for internal usage, returns back
                                        and outputs a given string
    help                                return this output
    version                             return the server version

                                        LOGGING
    set loglevel <LEVEL>                sets logging level to <LEVEL>.
                                        Levels: CRITICAL, ERROR, WARNING,
                                        NOTICE, INFO, DEBUG, TRACEDEBUG,
                                        HEAVYDEBUG or corresponding
                                        numeric value (50-5)
    get loglevel                        gets the logging level
    set logtarget <TARGET>              sets logging target to <TARGET>.
                                        Can be STDOUT, STDERR, SYSLOG,
                                        SYSTEMD-JOURNAL or a file
    get logtarget                       gets logging target
    set syslogsocket auto|<SOCKET>      sets the syslog socket path to
                                        auto or <SOCKET>. Only used if
                                        logtarget is SYSLOG
    get syslogsocket                    gets syslog socket path
    flushlogs                           flushes the logtarget if a file
```

```
                                        and reopens it. For log rotation.

                                        DATABASE
set dbfile <FILE>                       set the location of fail2ban
                                        persistent datastore. Set to
                                        "None" to disable
get dbfile                              get the location of fail2ban
                                        persistent datastore
set dbmaxmatches <INT>                  sets the max number of matches
                                        stored in database per ticket
get dbmaxmatches                        gets the max number of matches
                                        stored in database per ticket
set dbpurgeage <SECONDS>                sets the max age in <SECONDS> that
                                        history of bans will be kept
get dbpurgeage                          gets the max age in seconds that
                                        history of bans will be kept

                                        JAIL CONTROL
add <JAIL> <BACKEND>                    creates <JAIL> using <BACKEND>
start <JAIL>                            starts the jail <JAIL>
stop <JAIL>                             stops the jail <JAIL>. The jail is
                                        removed
status <JAIL> [FLAVOR]                  gets the current status of <JAIL>,
                                        with optional flavor or extended
                                        info

                                        JAIL CONFIGURATION
set <JAIL> idle on|off                  sets the idle state of <JAIL>
set <JAIL> ignoreself true|false        allows the ignoring of own IP
                                        addresses
set <JAIL> addignoreip <IP>             adds <IP> to the ignore list of
                                        <JAIL>
set <JAIL> delignoreip <IP>             removes <IP> from the ignore list
                                        of <JAIL>
```

```
    set <JAIL> ignorecommand <VALUE>          sets ignorecommand of <JAIL>
    set <JAIL> ignorecache <VALUE>            sets ignorecache of <JAIL>
    set <JAIL> addlogpath <FILE> ['tail']     adds <FILE> to the monitoring list
                                              of <JAIL>, optionally starting at
                                              the 'tail' of the file (default
                                              'head').
    set <JAIL> dellogpath <FILE>              removes <FILE> from the monitoring
                                              list of <JAIL>
    set <JAIL> logencoding <ENCODING>         sets the <ENCODING> of the log
                                              files for <JAIL>
    set <JAIL> addjournalmatch <MATCH>        adds <MATCH> to the journal filter
                                              of <JAIL>
    set <JAIL> deljournalmatch <MATCH>        removes <MATCH> from the journal
                                              filter of <JAIL>
    set <JAIL> addfailregex <REGEX>           adds the regular expression
                                              <REGEX> which must match failures
                                              for <JAIL>
    set <JAIL> delfailregex <INDEX>           removes the regular expression at
                                              <INDEX> for failregex
    set <JAIL> addignoreregex <REGEX>         adds the regular expression
                                              <REGEX> which should match pattern
                                              to exclude for <JAIL>
    set <JAIL> delignoreregex <INDEX>         removes the regular expression at
                                              <INDEX> for ignoreregex
    set <JAIL> findtime <TIME>                sets the number of seconds <TIME>
                                              for which the filter will look
                                              back for <JAIL>
    set <JAIL> bantime <TIME>                 sets the number of seconds <TIME>
                                              a host will be banned for <JAIL>
    set <JAIL> datepattern <PATTERN>          sets the <PATTERN> used to match
                                              date/times for <JAIL>
    set <JAIL> usedns <VALUE>                 sets the usedns mode for <JAIL>
    set <JAIL> attempt <IP> [<failure1> ... <failureN>]
                                              manually notify about <IP> failure
```

```
    set <JAIL> banip <IP> ... <IP>           manually Ban <IP> for <JAIL>
    set <JAIL> unbanip [--report-absent] <IP> ... <IP>
                                             manually Unban <IP> in <JAIL>
    set <JAIL> maxretry <RETRY>              sets the number of failures
                                             <RETRY> before banning the host
                                             for <JAIL>
    set <JAIL> maxmatches <INT>              sets the max number of matches
                                             stored in memory per ticket in
                                             <JAIL>
    set <JAIL> maxlines <LINES>              sets the number of <LINES> to
                                             buffer for regex search for <JAIL>
    set <JAIL> addaction <ACT>[ <PYTHONFILE> <JSONKWARGS>]
                                             adds a new action named <ACT> for
                                             <JAIL>. Optionally for a Python
                                             based action, a <PYTHONFILE> and
                                             <JSONKWARGS> can be specified,
                                             else will be a Command Action
    set <JAIL> delaction <ACT>               removes the action <ACT> from
                                             <JAIL>

                                             COMMAND ACTION CONFIGURATION
    set <JAIL> action <ACT> actionstart <CMD>
                                             sets the start command <CMD> of
                                             the action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionstop <CMD> sets the stop command <CMD> of the
                                             action <ACT> for <JAIL>
    set <JAIL> action <ACT> actioncheck <CMD>
                                             sets the check command <CMD> of
                                             the action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionban <CMD>  sets the ban command <CMD> of the
                                             action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionunban <CMD>
                                             sets the unban command <CMD> of
                                             the action <ACT> for <JAIL>
```

```
    set <JAIL> action <ACT> timeout <TIMEOUT>
                                            sets <TIMEOUT> as the command
                                            timeout in seconds for the action
                                            <ACT> for <JAIL>

                                            GENERAL ACTION CONFIGURATION
    set <JAIL> action <ACT> <PROPERTY> <VALUE>
                                            sets the <VALUE> of <PROPERTY> for
                                            the action <ACT> for <JAIL>
    set <JAIL> action <ACT> <METHOD>[ <JSONKWARGS>]
                                            calls the <METHOD> with
                                            <JSONKWARGS> for the action <ACT>
                                            for <JAIL>

                                            JAIL INFORMATION
    get <JAIL> banned                       return banned IPs of <JAIL>
    get <JAIL> banned <IP> ... <IP>]        return 1 if IP is banned in <JAIL>
                                            otherwise 0, or a list of 1/0 for
                                            multiple IPs
    get <JAIL> logpath                      gets the list of the monitored
                                            files for <JAIL>
    get <JAIL> logencoding                  gets the encoding of the log files
                                            for <JAIL>
    get <JAIL> journalmatch                 gets the journal filter match for
                                            <JAIL>
    get <JAIL> ignoreself                   gets the current value of the
                                            ignoring the own IP addresses
    get <JAIL> ignoreip                     gets the list of ignored IP
                                            addresses for <JAIL>
    get <JAIL> ignorecommand                gets ignorecommand of <JAIL>
    get <JAIL> failregex                    gets the list of regular
                                            expressions which matches the
                                            failures for <JAIL>
    get <JAIL> ignoreregex                  gets the list of regular
```

```
                                        expressions which matches patterns
                                        to ignore for <JAIL>
    get <JAIL> findtime                 gets the time for which the filter
                                        will look back for failures for
                                        <JAIL>
    get <JAIL> bantime                  gets the time a host is banned for
                                        <JAIL>
    get <JAIL> datepattern              gets the pattern used to match
                                        date/times for <JAIL>
    get <JAIL> usedns                   gets the usedns setting for <JAIL>
    get <JAIL> banip [<SEP>|--with-time]    gets the list of of banned IP
                                        addresses for <JAIL>. Optionally
                                        the separator character ('<SEP>',
                                        default is space) or the option '
                                        --with-time' (printing the times
                                        of ban) may be specified. The IPs
                                        are ordered by end of ban.
    get <JAIL> maxretry                 gets the number of failures
                                        allowed for <JAIL>
    get <JAIL> maxmatches               gets the max number of matches
                                        stored in memory per ticket in
                                        <JAIL>
    get <JAIL> maxlines                 gets the number of lines to buffer
                                        for <JAIL>
    get <JAIL> actions                  gets a list of actions for <JAIL>

                                        COMMAND ACTION INFORMATION
    get <JAIL> action <ACT> actionstart     gets the start command for the
                                        action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionstop      gets the stop command for the
                                        action <ACT> for <JAIL>
    get <JAIL> action <ACT> actioncheck     gets the check command for the
                                        action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionban       gets the ban command for the
```

```
                                            action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionunban     gets the unban command for the
                                            action <ACT> for <JAIL>
    get <JAIL> action <ACT> timeout         gets the command timeout in
                                            seconds for the action <ACT> for
                                            <JAIL>

                                            GENERAL ACTION INFORMATION
    get <JAIL> actionproperties <ACT>       gets a list of properties for the
                                            action <ACT> for <JAIL>
    get <JAIL> actionmethods <ACT>          gets a list of methods for the
                                            action <ACT> for <JAIL>
    get <JAIL> action <ACT> <PROPERTY>      gets the value of <PROPERTY> for
                                            the action <ACT> for <JAIL>

Report bugs to https://github.com/fail2ban/fail2ban/issues
```

Activer et Démarrer le Serveur

Pour prendre en compte la configuration dans le fichier **/etc/fail2ban/jail.local**, re-démarrez le server :

```
root@debian12:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-11-27 14:37:44 CET; 12min ago
       Docs: man:fail2ban(1)
   Main PID: 8709 (fail2ban-server)
      Tasks: 5 (limit: 19123)
     Memory: 19.2M
        CPU: 416ms
     CGroup: /system.slice/fail2ban.service
             └─8709 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

```
Nov 27 14:37:44 debian12 systemd[1]: Started fail2ban.service - Fail2Ban Service.
Nov 27 14:37:45 debian12 fail2ban-server[8709]: 2025-11-27 14:37:45,255 fail2ban.configreader   [8709]: WARNING
'allowipv6' not defined in 'Definition'. Using default one: 'auto'
Nov 27 14:37:45 debian12 fail2ban-server[8709]: Server ready

root@debian12:~# systemctl restart fail2ban

root@debian12:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-11-27 14:51:13 CET; 2s ago
       Docs: man:fail2ban(1)
   Main PID: 8768 (fail2ban-server)
      Tasks: 5 (limit: 19123)
     Memory: 12.3M
        CPU: 135ms
     CGroup: /system.slice/fail2ban.service
             └─8768 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Nov 27 14:51:13 debian12 systemd[1]: Started fail2ban.service - Fail2Ban Service.
Nov 27 14:51:13 debian12 fail2ban-server[8768]: 2025-11-27 14:51:13,578 fail2ban.configreader   [8768]: WARNING
'allowipv6' not defined in 'Definition'. Using default one: 'auto'
Nov 27 14:51:13 debian12 fail2ban-server[8768]: Server ready
```

Utiliser la Commande Fail2Ban-server

Pour connaître le status de Fail2Ban-server, saisissez la commande suivante :

```
root@debian12:~# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Il est aussi possible de se renseigner sur le statut d'un prison particulier :

```
root@debian12:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

La commande **fail2ban-client** peut être utilisée pour contrôler un prison :

```
root@debian12:~# fail2ban-client stop sshd
Jail stopped

root@debian12:~# fail2ban-client status sshd
2025-11-27 14:52:41,173 fail2ban                [8782]: ERROR   NOK: ('sshd',)
Sorry but the jail 'sshd' does not exist

root@debian12:~# fail2ban-client reload
2025-11-27 14:52:51,975 fail2ban.configreader   [8783]: WARNING 'allowipv6' not defined in 'Definition'. Using
default one: 'auto'
OK

root@debian12:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
```

```
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

Ajouter un Prison

Installez maintenant le serveur Apache si ce n'est pas déjà fait :

```
root@debian12:~# apt install apache2
```

Vérifiez que le service Apache est lancé et activé :

```
root@debian12:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-11-27 14:54:20 CET; 31s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 9233 (apache2)
      Tasks: 55 (limit: 19123)
     Memory: 17.5M
        CPU: 54ms
     CGroup: /system.slice/apache2.service
             ├─9233 /usr/sbin/apache2 -k start
             ├─9235 /usr/sbin/apache2 -k start
             └─9236 /usr/sbin/apache2 -k start

Nov 27 14:54:19 debian12 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 27 14:54:20 debian12 apachectl[9232]: AH00557: apache2: apr_sockaddr_info_get() failed for debian12
Nov 27 14:54:20 debian12 apachectl[9232]: AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this mess>
Nov 27 14:54:20 debian12 systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Modifiez maintenant votre fichier **/etc/fail2ban/jail.local** :

```
root@debian12:~# vi /etc/fail2ban/jail.local

root@debian12:~# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 172.YY+20.0.3
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true

[apache-auth]
enabled = true
```

Appliquez la nouvelle configuration et constatez le résultat :

```
root@debian12:~# fail2ban-client reload
2025-11-27 14:56:34,440 fail2ban.configreader   [9386]: WARNING 'allowipv6' not defined in 'Definition'. Using
default one: 'auto'
OK

root@debian12:~# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:   apache-auth, sshd
```
