FAIL2BAN

Fail2ban est un outil de sécurité utilisé principalement pour protéger les serveurs contre les attaques par **brute force** et les tentatives de connexion malveillantes en bloquant automatiquement les adresses IP sources qui tentent de se connecter de manière excessive sans succès.

Comment Fail2ban fonctionne :
1. **Surveillance des journaux** : Fail2ban fonctionne en analysant les fichiers de journaux (logs) d'un serveur. Ces journaux contiennent des informations sur les tentatives de connexion, y compris les connexions réussies et échouées. Par exemple, lorsqu'un utilisateur tente de se connecter à un service comme SSH, FTP, ou une application web, une entrée est ajoutée au fichier de journalisation du serveur, indiquant si la tentative a échoué ou réussi.

2. **Détection des échecs de connexion** : Fail2ban détecte les motifs indiquant des échecs de connexion. Lorsqu'un utilisateur entre un mot de passe incorrect plusieurs fois, Fail2ban remarque ces tentatives et les enregistre comme échecs. Cela peut concerner des services comme SSH, FTP, HTTP, etc.

3. **Blocage des IP malveillantes** : Après avoir détecté plusieurs tentatives de connexion échouées en provenance d'une même adresse IP, Fail2ban prend une mesure. Par défaut, il **bloque temporairement** cette adresse IP pour une période définie, comme 10 minutes, 1 heure, ou plus. Cela empêche l'attaquant d'effectuer d'autres tentatives de connexion sur le serveur.

4. **Utilisation de pare-feu pour bloquer l'IP** : Fail2ban utilise généralement des outils comme **iptables** ou **firewalld** pour bloquer l'adresse IP malveillante. Ces outils ajoutent une règle au pare-feu du serveur, empêchant l'IP d'accéder à certains services ou à tout le serveur pendant une période donnée.

Pourquoi utiliser Fail2ban ?
- **Protection contre les attaques par brute force** : Une attaque par brute force consiste à essayer différentes combinaisons de noms d'utilisateur et de mots de passe jusqu'à ce que la bonne combinaison soit trouvée. Fail2ban bloque ces tentatives en empêchant les attaquants de continuer leurs essais.

- **Réduction des risques d'intrusion** : En bloquant les IP après un certain nombre de tentatives échouées, Fail2ban réduit les chances d'accès non autorisé à un serveur ou à un service.
- **Automatisation de la sécurité** : Fail2ban fonctionne de manière autonome, en surveillant constamment les journaux et en appliquant les règles de sécurité sans intervention manuelle.
- **Alerte et prévention** : Lorsqu'une adresse IP est bloquée, Fail2ban peut envoyer une alerte (par email ou autre) à l'administrateur du serveur, ce qui permet de suivre les tentatives d'attaque.

Fail2ban FTP

```
On installe fail2ban sur le serveur FTP (proftpd)
apt update && sudo apt upgrade -y
```

```
apt install fail2ban
```

On ajoute la jail de proftpd

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

```
[proftpd]
enabled  = true          # Active la jail pour ProFTPd
port     = ftp,ftp-data   # Surveille les ports FTP (21) et FTP data (20)
filter   = proftpd        # Utilise le filtre 'proftpd' pour détecter les échecs de connexion
logpath  = /var/log/proftpd/proftpd.log  # Surveille le fichier de log de ProFTPd
maxretry = 3             # Nombre maximal de tentatives échouées avant bannissement
bantime  = 600           # Durée du bannissement (en secondes, ici 10 minutes)
findtime = 300           # Fenêtre de temps (en secondes) dans laquelle les tentatives sont comptées (ici 5 minutes)
```

Le fichier jail.local permet de personnaliser la configuration de Fail2ban pour activer, désactiver ou ajuster les règles de surveillance des services (FTP pour nous ici) sans modifier le fichier par défaut jail.conf. Il définit des paramètres spécifiques pour chaque service, tels que le chemin des logs, le nombre de tentatives échouées avant un bannissement, la durée du bannissement, et plus. Cela permet de maintenir une configuration stable et facilement personnalisable tout en protégeant les services contre les attaques par brute-force.

Puis nous passons au filtre FTP, de base Fail2ban créer un filtre pour proftpd, Les filtres de Fail2ban servent à définir des expressions régulières (regex) permettant d'analyser les fichiers de logs à la recherche de comportements suspects, comme des tentatives de connexion échouées, pour ensuite appliquer des actions de sécurité (comme bannir une IP).

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

```
# Fail2Ban filter for the Proftpd FTP daemon
#
# Set "UseReverseDNS off" in proftpd.conf to avoid the need for DNS.
# See: http://www.proftpd.org/docs/howto/DNS.html
# When the default locale for your system is not en_US.UTF-8
# on Debian-based systems be sure to add this to /etc/default/proftpd
# export LC_TIME="en_US.UTF-8"

[INCLUDES]

before = common.conf

[Definition]
```

```
_daemon = proftpd

__suffix_failed_login = ([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 UserAlias|[mM]aximum login
length exceeded)


prefregex = ^%(__prefix_line)s%(__hostname)s \(\S+\[<HOST>\]\)[: -]+ <F-
CONTENT>(?:USER|SECURITY|Maximum) .+</F-CONTENT>$


failregex = ^USER <F-USER>\S+|.*?</F-USER>(?: \(Login failed\))?:
%(__suffix_failed_login)s
            ^SECURITY VIOLATION: <F-USER>\S+|.*?</F-USER> login attempted
            ^Maximum login attempts \(\d+\) exceeded

ignoreregex =

[Init]
journalmatch = _SYSTEMD_UNIT=proftpd.service

# Author: Yaroslav Halchenko
#         Daniel Black - hardening of regex
```

Après avoir configuré Fail2ban pour ProFTPd, redémarrez le service Fail2ban pour appliquer les changements :

```
systemctl restart fail2ban
```

Assurez-vous que Fail2ban est bien actif :

```
sudo systemctl status fail2ban
```

Vérifier les jails actifs Utilisez la commande suivante pour voir si la jail proftpd est bien active :

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

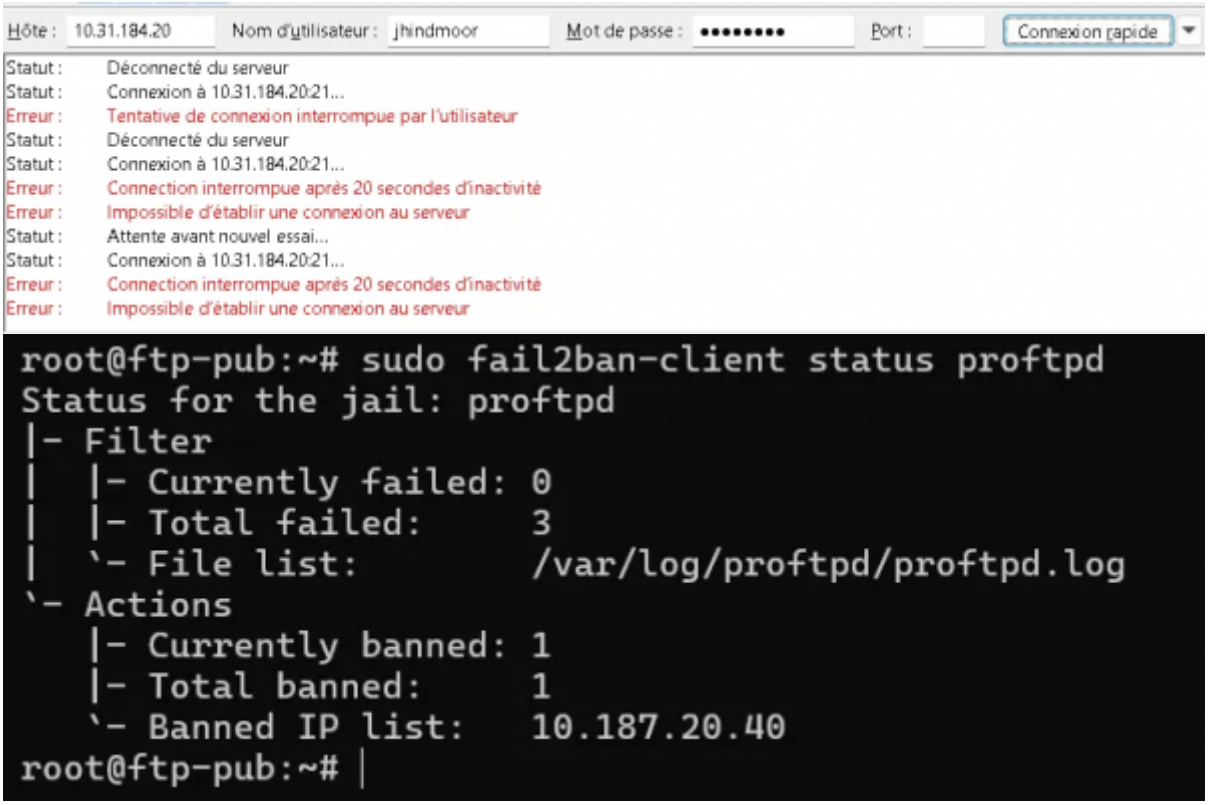
Test avec FileZilla

Pour tester le bannissement, essayez de vous connecter plusieurs fois à votre serveur FTP via FileZilla avec un mauvais mot de passe.

1. Lancez plusieurs tentatives infructueuses.

2. Après avoir dépassé le nombre de tentatives (`maxretry = 3` dans la configuration), Fail2ban devrait bloquer l'IP de la machine source.

Vérifiez si votre IP est maintenant bannie en utilisant :



Fail2ban SSH

Pour ssh, installer fail2ban sur une machine, nous on va faire Fail2ban SSH sur notre serveur FTP aussi :

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

La configuration pour **SSH** est généralement déjà incluse dans le fichier de configuration de Fail2ban, mais vérifions-le.

- **Ouvrir ou créer** le fichier `jail.local` si ce n'est pas déjà fait :

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

```
[sshd]  # Définit une jail pour le service SSH (sshd)
enabled = true  # Active la jail pour SSH (vrai signifie que la jail est activée)
port    = ssh  # Indique que cette jail surveille le port SSH (par défaut, le port 22)
filter  = sshd  # Utilise le filtre "sshd" pour détecter les tentatives de connexion échouées
logpath = /var/log/auth.log  # Spécifie le chemin vers le fichier de log où Fail2ban recherche les erreurs de connexion
```

```
maxretry = 3  # Définit le nombre maximum de tentatives échouées avant de bannir l'IP (ici, 3 tentatives)
bantime  = 600  # Le temps pendant lequel l'IP est bannie (en secondes) - ici, 10 minutes (600 secondes)
findtime = 300  # Période de temps (en secondes) pendant laquelle les tentatives échouées sont comptées - ici, 5 minutes (300 secondes)
```

Après avoir configuré la jail pour SSH, redémarrez Fail2ban pour appliquer les changements :

```
systemctl restart fail2ban
fail2ban-client status sshd
```

```
root@ftp-pub:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
```

Pour tester. Il faut spam la connexion SSH sur le serveur :

```
C:\Users\mazab>ssh root@10.31.184.20
Enter passphrase for key 'C:\Users\mazab/.ssh/id_rsa':
Enter passphrase for key 'C:\Users\mazab/.ssh/id_rsa':
Enter passphrase for key 'C:\Users\mazab/.ssh/id_rsa':
root@10.31.184.20's password:
Permission denied, please try again.
root@10.31.184.20's password:
Permission denied, please try again.
root@10.31.184.20's password:
root@10.31.184.20: Permission denied (publickey,password).
```

Puis verifier avec la commande :

```
root@ftp-pub:~# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   10.187.20.45
root@ftp-pub:~#
```

Portsentry

nmap (The famous Network MAPper) est un scanner de port open-source qui a pour but de détecter les ports ouverts, identifier les services qui tournent (et leur version éventuellement) et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Installation sur un serveur (web ici) :

```
apt update
apt install portsentry
```

Exemple de scan avant portsentry :

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@ftp-pub:~# nmap -sS 10.31.184.80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-06 07:37 UTC
Nmap scan report for 10.31.184.80
Host is up (0.0000070s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: BC:24:11:FC:62:6C (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Portsentry ne sert à rien après installation (il ne bloque rien). Il faudra quelques étapes simples pour qu'il soit fonctionnel. Mais avant ça, comme pour Fail2ban (ci-dessous), il est assez facile, en testant le fonctionnement de tels outils, de se bloquer sa propre machine... Pour éviter cela il existe 2 fichiers de configuration spéciaux :

```
root@web-publique:/etc/portsentry# tree
.
|-- portsentry.conf
|-- portsentry.ignore
`-- portsentry.ignore.static
```

Vous devez ajouter les IP des machines à ne pas « bloquer » dans le fichier portsentry.ignore.static (nous : 10.31.184.80/22). Au démarrage du service, le contenu de ce fichier est copié dans portsentry.ignore

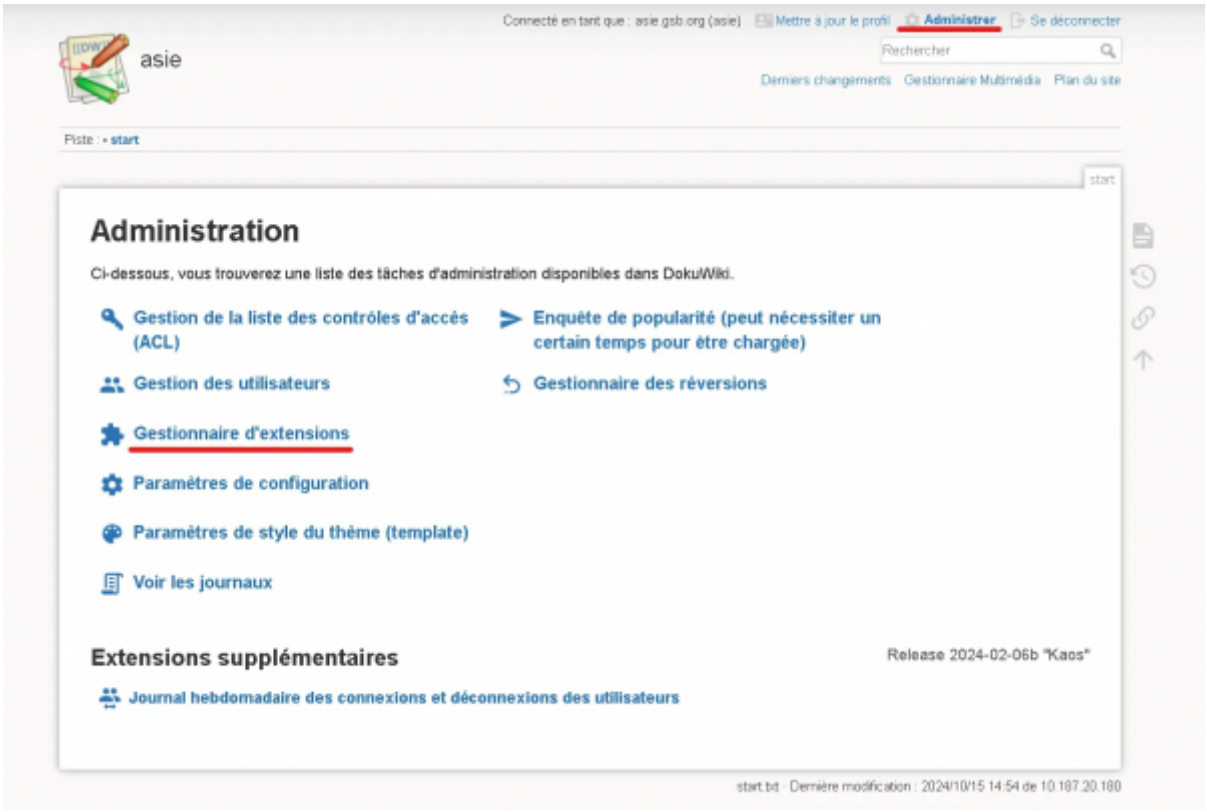
```
root@web-publique:/etc/portsentry# cat /etc/default/portsentry
# /etc/default/portsentry
#
# This file is read by /etc/init.d/portsentry. See the portsentry.8
# manpage for details.
#
# The options in this file refer to commandline arguments (all in lowercase)
# of portsentry. Use only one tcp and udp mode at a time.
#
TCP_MODE="tcp"
UDP_MODE="udp"
```

Après installation de Portsentry :

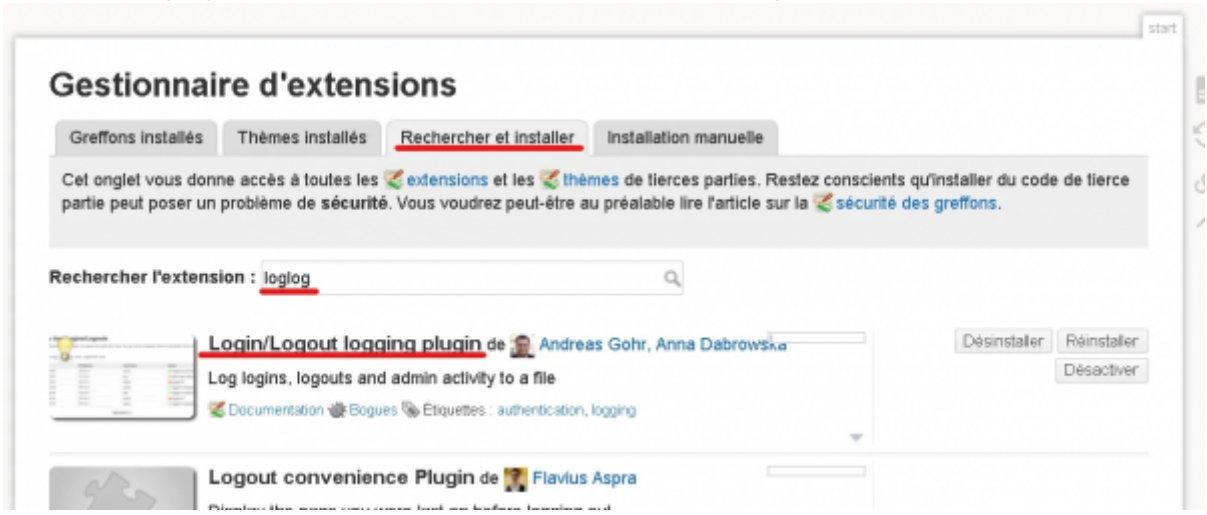
```
root@ftp-pub:~# nmap -sS 10.31.184.80
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-06 07:36 UTC
Nmap scan report for 10.31.184.80
Host is up (0.0000070s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  tcpmux
22/tcp    open  ssh
79/tcp    open  finger
80/tcp    open  http
111/tcp   open  rpcbind
119/tcp   open  nntp
143/tcp   open  imap
443/tcp   open  https
1080/tcp  open  socks
1524/tcp  open  ingreslock
2000/tcp  open  cisco-sccp
6667/tcp  open  irc
12345/tcp open  netbus
31337/tcp open  Elite
32771/tcp open  sometimes-rpc5
32772/tcp open  sometimes-rpc7
32773/tcp open  sometimes-rpc9
32774/tcp open  sometimes-rpc11
MAC Address: BC:24:11:FC:62:6C (Unknown)
```

Fail2Ban Dokuwiki

- Aller sur ‘docs.asie.gsb.org’, puis se connecter à un compte administrateur - Aller ensuite dans Administrer et Gestionnaire d’extensions :



Puis rechercher loglog dans la barre de recherche et installer le premier de Andreas Gohr



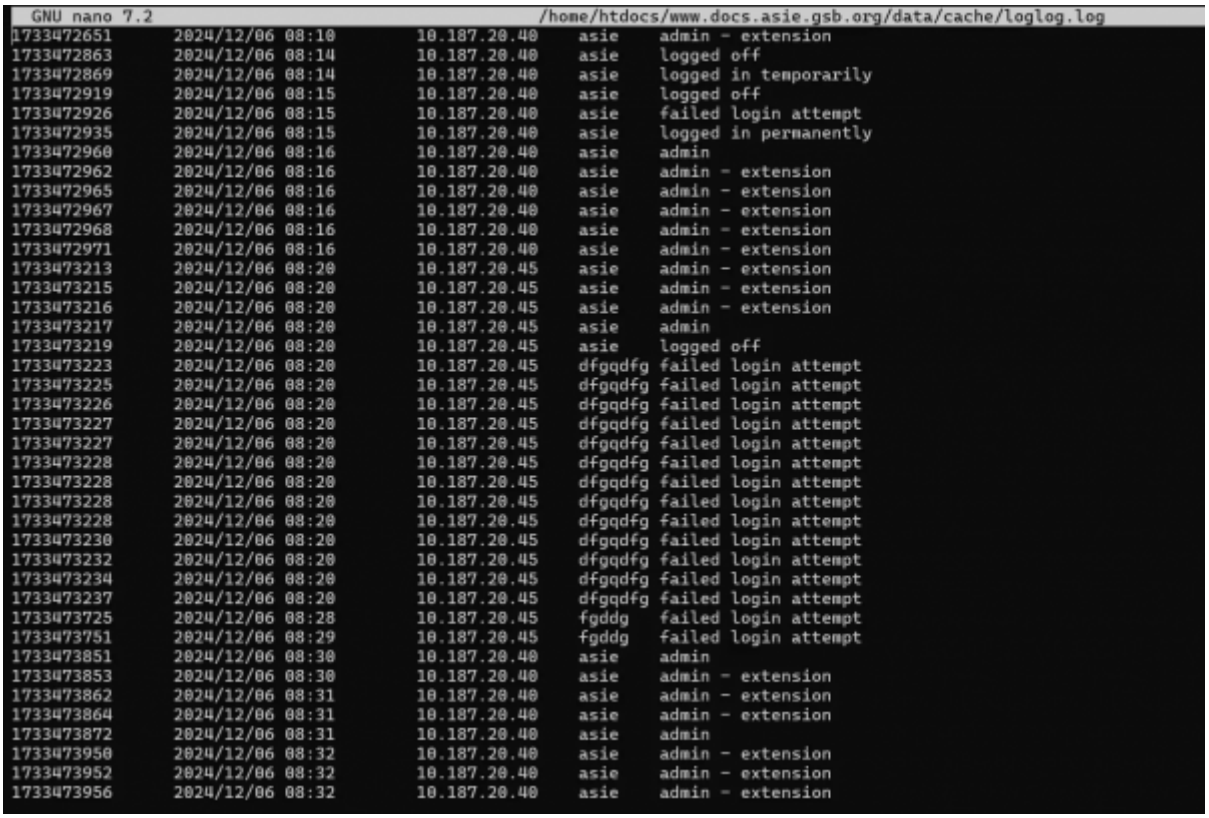
Si vous avez pas le bouton Installer, il faut modifier les droits du répertoire plugins

Une fois installé, il faut configurer. - Aller dans '/etc/fail2ban/jail.d/dokuwiki.local' et ajouter cette conf :

```
[dokuwiki]
# To use more aggressive 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.
enabled = true
mode = aggressive
port = http,https
filter = dokuwiki
action = iptables-allports
maxretry = 2
```

```
bantime = -1
logpath = /home/htdocs/www.docs.asie.gsb.org/data/cache/loglog.log
```

Aller dans '/etc/fail2ban/fil



```
  GNU nano 7.2                                  /home/htdocs/www.docs.asie.gsb.org/data/cache/loglog.log
1733472651      2024/12/06 08:10        10.187.20.40    asie    admin - extension
1733472863      2024/12/06 08:14        10.187.20.40    asie    logged off
1733472869      2024/12/06 08:14        10.187.20.40    asie    logged in temporarily
1733472919      2024/12/06 08:15        10.187.20.40    asie    logged off
1733472926      2024/12/06 08:15        10.187.20.40    asie    failed login attempt
1733472935      2024/12/06 08:15        10.187.20.40    asie    logged in permanently
1733472960      2024/12/06 08:16        10.187.20.40    asie    admin
1733472962      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472965      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472967      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472968      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472971      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733473213      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473215      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473216      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473217      2024/12/06 08:20        10.187.20.45    asie    admin
1733473219      2024/12/06 08:20        10.187.20.45    asie    logged off
1733473223      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473225      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473226      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473227      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473227      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473230      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473232      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473234      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473237      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473725      2024/12/06 08:28        10.187.20.45    fgddg   failed login attempt
1733473751      2024/12/06 08:29        10.187.20.45    fgddg   failed login attempt
1733473851      2024/12/06 08:30        10.187.20.40    asie    admin
1733473853      2024/12/06 08:30        10.187.20.40    asie    admin - extension
1733473862      2024/12/06 08:31        10.187.20.40    asie    admin - extension
1733473864      2024/12/06 08:31        10.187.20.40    asie    admin - extension
1733473872      2024/12/06 08:31        10.187.20.40    asie    admin
1733473950      2024/12/06 08:32        10.187.20.40    asie    admin - extension
1733473952      2024/12/06 08:32        10.187.20.40    asie    admin - extension
1733473956      2024/12/06 08:32        10.187.20.40    asie    admin - extension
```

ter.d/dokuwiki.conf' pour ajouter la regex :

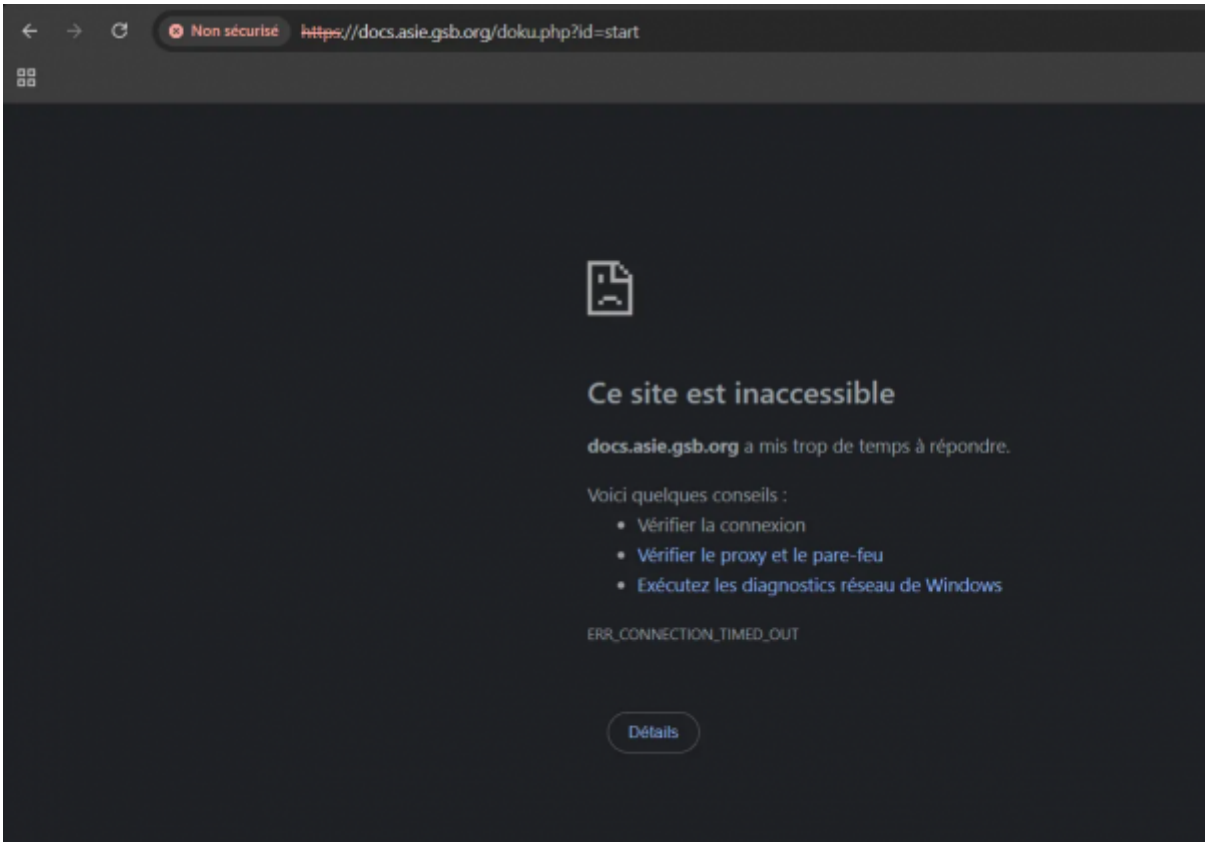
```
[Definition]
failregex = ^.*:\d{2}\s{1,}<HOST>\s.*failed
ignoreregex =
```

verifier les logs dans loglog.log

```
 GNU nano 7.2                                  /home/htdocs/www.docs.asie.gsb.org/data/cache/loglog.log
1733472651      2024/12/06 08:10        10.187.20.40    asie    admin - extension
1733472863      2024/12/06 08:14        10.187.20.40    asie    logged off
1733472869      2024/12/06 08:14        10.187.20.40    asie    logged in temporarily
1733472919      2024/12/06 08:15        10.187.20.40    asie    logged off
1733472926      2024/12/06 08:15        10.187.20.40    asie    failed login attempt
1733472935      2024/12/06 08:15        10.187.20.40    asie    logged in permanently
1733472960      2024/12/06 08:16        10.187.20.40    asie    admin
1733472962      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472965      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472967      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472968      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733472971      2024/12/06 08:16        10.187.20.40    asie    admin - extension
1733473213      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473215      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473216      2024/12/06 08:20        10.187.20.45    asie    admin - extension
1733473217      2024/12/06 08:20        10.187.20.45    asie    admin
1733473219      2024/12/06 08:20        10.187.20.45    asie    logged off
1733473223      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473225      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473226      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473227      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473227      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473228      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473230      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473232      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473234      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473237      2024/12/06 08:20        10.187.20.45    dfgqdfg failed login attempt
1733473725      2024/12/06 08:28        10.187.20.45    fgddg   failed login attempt
1733473751      2024/12/06 08:29        10.187.20.45    fgddg   failed login attempt
1733473851      2024/12/06 08:30        10.187.20.40    asie    admin
1733473853      2024/12/06 08:30        10.187.20.40    asie    admin - extension
1733473862      2024/12/06 08:31        10.187.20.40    asie    admin - extension
1733473864      2024/12/06 08:31        10.187.20.40    asie    admin - extension
1733473872      2024/12/06 08:31        10.187.20.40    asie    admin
1733473950      2024/12/06 08:32        10.187.20.40    asie    admin - extension
1733473952      2024/12/06 08:32        10.187.20.40    asie    admin - extension
1733473956      2024/12/06 08:32        10.187.20.40    asie    admin - extension
```

Puis tester :

Il faut spam un mauvais identifiant sur la page de connexion dokuwiki, puis ... BAN

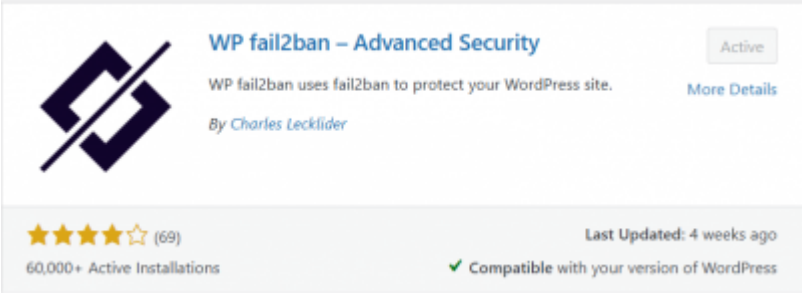


preuve :

```
root@web-priv:~# fail2ban-client status dokuwiki
Status for the jail: dokuwiki
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     18
|  `- File list:        /home/htdocs/www.docs.asie.gsb.org/data/cache/loglog.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     3
   `- Banned IP list:   10.187.20.45
root@web-priv:~#
```

Fail2Ban Wordpress

Pour commencer l'installation de fail2ban sur Wordpress, il faut se connecter sur les 2 wordpress et installer le plugin fail2ban.



Une fois l'installations du plugin fait sur Wordpress, il faut déplacer le filtre dans le bon fichier :

```
/etc/fail2ban/filter.d
```

Pour cela, il faut utiliser la commande mv et copier les 3 fichier wordpress-...-conf dans "/etc/fail2ban/filter.d/"

```
mv /home/htdocs/asie.gsb.org/wp-content/plugins/wp-
fail2ban/filters.d/wordpress-extra.conf /etc/fail2ban/filter.d/
mv /home/htdocs/asie.gsb.org/wp-content/plugins/wp-
fail2ban/filters.d/wordpress-hard.conf /etc/fail2ban/filter.d/
mv /home/htdocs/asie.gsb.org/wp-content/plugins/wp-
fail2ban/filters.d/wordpress-soft.conf /etc/fail2ban/filter.d
```

Pour la suite, il faut configurer le jail dans le dossier "/etc/fail2ban/jail.d" en créant le fichier wordpress.conf :

```
[wordpress]
enabled = true
port = http,https
filter = wordpress-soft
maxretry = 2
logpath = /var/log/auth.log
bantime = 10m
```

Une fois la configuration fini, il suffit de restart le service fail2ban avec la commande suivant puis de tester :

```
service fail2ban restart
```

Fail2Ban Nextcloud

Configurer un filtre et une jail pour Nextcloud

Un filtre définit des règles regex permettant d'identifier les échecs d'authentification des utilisateurs sur l'interface utilisateur de Nextcloud, WebDAV, ou l'utilisation d'un domaine non approuvé pour accéder au serveur.

Création d'un filtre pour Nextcloud Créez un fichier dans /etc/fail2ban/filter.d nommé nextcloud.conf avec le contenu suivant :

```
[Definition]
_groupsre = (?:(?:,?\s*"\w+":(?:"[^"]+"|\w+))*)
failregex =
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Login
failed:
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Trust
ed domain error.
datepattern = ,?\s*"time"\s*:\s*"%%Y-%%m-%%d[T ]%%H:%%M:%%S(%%z)?"
```

Création d'une prison pour Nextcloud
Le fichier de configuration de la prison définit comment gérer les tentatives d'authentification échouées détectées par le filtre Nextcloud.

Créez un fichier dans /etc/fail2ban/jail.d nommé nextcloud.local avec le contenu suivant :

```
[nextcloud]
backend = auto
enabled = true
port = 80,443
protocol = tcp
filter = nextcloud
maxretry = 3
bantime = 86400
findtime = 43200
logpath = /chemin/vers/le/dossier/data/nextcloud.log
#logpath : Remplacez cette valeur par le chemin du fichier nextcloud.log de
votre installation.
#port : Si votre serveur Web utilise des ports différents de 80 et 443,
ajustez ces valeurs.
#bantime et findtime : Ces durées sont exprimées en secondes.
```

Redémarrez le service Fail2Ban :

```
sudo systemctl restart fail2ban
```

Pour vérifier l'état de la prison Nextcloud, exécutez la commande suivante :

```
fail2ban-client status nextcloud
```

Test :

```
root@web-priv:/etc/fail2ban/jail.d# fail2ban-client status nextcloud
Status for the jail: nextcloud
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /home/htdocs/www.intranet.asie.gsb.org/nextcloud/data/nextcloud.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   10.187.20.40
```

bien ban :