Table des matières

Installer Configurer Fail2ban

Si votre trafic réseaux passe par un reverse proxy type NPM, il vous faudra faire des modification coté Apache2

Apache2 & NPM

Dans le cas ou vous passez par un reverse proxy, votre Fail2ban verra que l'ip de celui-ci et pas celle de l'internaute en face !
Du coup il déclenchera jamais !!
Pour ce faire il y a quelques modifications à faire côtés Apache2 !
Notez, que votre Fail2ban doit être sur la même machine que votre serveur Web.

- **Activer le module de réécriture de IP source**

```
sudo a2enmod remoteip
```

- **Configurer le module remoteip.conf**

```
sudo nano /etc/apache2/conf-available/remoteip.conf
```

- **Ajouter cette configuration**

```
RemoteIPHeader X-Forwarded-For
# Remplace par l'IP réelle de votre instance NPM ou autre reverse proxy
RemoteIPInternalProxy IP_DE_NPM
```

- **Activer la configuration**

```
sudo a2enconf remoteip
```

- **Modifier le format de vos log Apache**

```
sudo nano /etc/apache2/apache2.conf
```

```
# Avant
LogFormat "%h %l %u %t \"%r\" %>s %b ..." combined
```

```
# Après
LogFormat "%a %l %u %t \"%r\" %>s %b ..." combined
```

- **Redémarrer Apache2**

```
sudo systemctl restart apache2
```

Installer

Rechecher le packet fail2ban.

```
apt-cache search fail2ban
```

Résultat:

```
fail2ban - ban hosts that cause multiple authentication errors
```

Commencer par installer le packet fail2ban.

```
sudo apt-get install fail2ban
```

Configuration

Penser avant d'ouvrir le port 43 dans votre FireWall pour les résolutions WHOIS de Fail2Ban.
Dans le fichier de conf /etc/fail2ban/jail.d/defaults-debian.conf
Je vous conseil de modifier les adresses ip et de copier/coller pour gagner du temps.

```
####################################
#    My Default Configuration      #
#          Powered By Me           #
#      Feb 2020-28 at 10h30        #
#                                  #
####################################
[DEFAULT]
####################################
#DESCRIPTION DES RESEAUX A IGNORER  #
#VLAN1                             #
# 192.168.10.1/24"                 #
#VLAN2                             #
# 10.200.200.1/26                  #
#VLAN3                             #
# 10.230.200.1/27                  #
#VLAN4                             #
# 10.240.80.1/28                   #
####################################
```

```
ignoreip = 192.168.10.1/24,10.200.200.1/26,10.230.200.1/27,10.240.80.1/28
#TEMPS D'AUDIT 1h
findtime = 3600
#TEMPS DE BAN 2h
bantime = 7200
#bantime = -1 #FOREVER BAN
#RE-ESSAIS 5 fois
maxretry = 5

destemail = p.balkani@gmail.com
sender = p.balkani@gmail.com
action = %(action_mwl)s

[sshd]
enabled = true
port = 22
logpath = /var/log/auth.log
maxretry = 5

[apache-400]
enabled = true
port = http,https
filter = apache-400
logpath = /var/log/apache2/access.log
maxretry = 1

[apache-403]
enabled = true
port = http,https
filter = apache-403
logpath = /var/log/apache2/access.log
maxretry = 3

[apache-404]
enabled = true
port = http,https
filter = apache-404
logpath = /var/log/apache2/access.log
maxretry = 3

[apache-auth]
enabled = true
port = http,https
logpath = %(apache_error_log)s
maxretry = 5

[apache-botsearch]
enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 1
```

```
[squid]
enabled = true
port    = all
filter  = squid
#action = iptables[name=Squid,port=8080,protocol=tcp]
logpath  = /var/log/squid/access.log
maxretry = 5
```

La section ignoreip Permet d'ignorer vos ip ou réseaux perso afin de ne pas vous auto-bannir. 
La Section [SSHD] Permet de protéger votre serveur SSH.
La Section [SQUID] Permet de protéger votre serveur de proxy-cache.
La Section [APACHE-XXX] Permet de protéger votre serveur Web.

Dans le fichier de conf: /etc/fail2ban/fail2ban.conf
On peut aussi modifier certains paramètres globaux.
Section du fichier

```
# 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 = 3w
```

Exemple:
Le path de la BDD par défaut (**dbfile**) ou le temps avant que la BDD se purge (**dbpurgeage**) ici passé à 3 semaine.

Penser à restart le service après modification.

```
systemctl restart fail2ban.service
```

Les LOGs

Squid

```
cat /var/log/squid/access.log
```

Vous y trouverez des ligne similaire, qui correspondent à des tentatives de connexions infructueuses.

```
1582887456.777      2 83.118.199.10 TCP_DENIED/407 4192 CONNECT
push.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.026      3 83.118.199.10 TCP_DENIED/407 4320 GET
http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1582887467.031      2 83.118.199.10 TCP_DENIED/407 4232 CONNECT content-
signature-2.cdn.mozilla.net:443 - HIER_NONE/- text/html
1582887467.499      2 83.118.199.10 TCP_DENIED/407 4232 CONNECT content-
signature-2.cdn.mozilla.net:443 - HIER_NONE/- text/html
1582887467.533      2 83.118.199.10 TCP_DENIED/407 4240 CONNECT
firefox.settings.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.642      2 83.118.199.10 TCP_DENIED/407 4212 CONNECT
incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1582887467.674      2 83.118.199.10 TCP_DENIED/407 4240 CONNECT
firefox.settings.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.715      2 83.118.199.10 TCP_DENIED/407 4192 CONNECT
push.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.789      2 83.118.199.10 TCP_DENIED/407 4212 CONNECT
incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1582887467.799      2 83.118.199.10 TCP_DENIED/407 4200 CONNECT
safebrowsing.googleapis.com:443 - HIER_NONE/- text/html
1582887467.832      2 83.118.199.10 TCP_DENIED/407 4240 CONNECT
firefox.settings.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.903      2 83.118.199.10 TCP_DENIED/407 4200 CONNECT
shavar.services.mozilla.com:443 - HIER_NONE/- text/html
1582887467.939      2 83.118.199.10 TCP_DENIED/407 4212 CONNECT
incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1582887467.943      2 83.118.199.10 TCP_DENIED/407 4240 CONNECT
firefox.settings.services.mozilla.com:443 - HIER_NONE/- text/html
1582887468.050      2 83.118.199.10 TCP_DENIED/407 4212 CONNECT
incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1582887468.060      2 83.118.199.10 TCP_DENIED/407 4188 CONNECT
snippets.cdn.mozilla.net:443 - HIER_NONE/- text/html
1582887468.190      2 83.118.199.10 TCP_DENIED/407 4240 CONNECT
firefox.settings.services.mozilla.com:443 - HIER_NONE/- text/html
1582887468.297      2 83.118.199.10 TCP_DENIED/407 4212 CONNECT
incoming.telemetry.mozilla.org:443 - HIER_NONE/- text/html
1582887471.922      3 83.118.199.10 TCP_DENIED/407 4320 GET
http://detectportal.firefox.com/success.txt - HIER_NONE/- text/html
1582887472.827      2 83.118.199.10 TCP_DENIED/407 4192 CONNECT
push.services.mozilla.com:443 - HIER_NONE/- text/html
1582887473.120      4 83.118.199.10 TCP_DENIED/407 4422 GET
http://detectportal.firefox.com/success.txt qerheqj, HIER_NONE/- text
```

C'est après avoir fait des tests volontaires à travers un VPN que je me suis aperçu que Fail2ban ne les bloquaient pas.
Solution étant d'ajouter une regex sur cette erreur en particulier “407”.

- Une REGEX = Regulière Expression.

Apache2

Log d'accès

```
cat /var/log/apache2/access.log
```

```
::1 - - [07/Mar/2020:10:02:23 +0100] "OPTIONS * HTTP/1.0" 200 128 "-"
"Apache/2.4.38 (Raspbian) (internal dummy connection)"
192.241.218.203 - - [07/Mar/2020:11:04:20 +0100] "GET / HTTP/1.1" 200 3326
"-" "Mozilla/5.0 zgrab/0.x"
2.136.134.161 - - [07/Mar/2020:12:17:02 +0100] "GET / HTTP/1.1" 400 0 "-" "-
"
36.92.140.21 - - [07/Mar/2020:12:19:39 +0100] "GET / HTTP/1.1" 200 10958 "-"
"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/52.0.2743.116 Safari/537.36"
```

Log error

```
cat /var/log/apache2/error.log
```

---

filter.d

Dans des cas bien précis vos serez amené à modifier quelques regex pour le filtrage ou de créer de nouveau Jail.
*C'est le cas de **Squid Proxy Cache** afin d'améliorer la sécurité au maximum ou **Apache2** pour élargir le scope de surveillance.*

SQUID REGEX

Editer le filtre

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

Ajouter une **regex** afin de déceler l'erreur 407 DENIED qui apparrait dans /var/log/squid/access.log.

```
# Fail2Ban filter for Squid attempted proxy bypasses
#
#

[Definition]

failregex = ^\s+\d\s<HOST>\s+[A-Z_]+_DENIED/403 .*$
```

```
            ^\s+\d\s<HOST>\s+NONE/405 .*$
            ^\s+\d\s<HOST>\s+[A-Z_]+_DENIED/407 .*$
ignoreregex =

datepattern = {^LN-BEG}Epoch
              {^LN-BEG}
```

Par defaut cette regex n'éxiste pas.

```
^\s+\d\s<HOST>\s+[A-Z_]+_DENIED/407 .*$
```

Ajouter la !

ICECAST REGEX

Si tu souhaites aussi surveiller ton serveur de streaming audio !!

```
# Icecast2 filter
# POWERED By ME
# Author: Minos Corp Certified

[INCLUDES]

before = apache-common.conf

[Definition]

failregex = ^<HOST> - - \[.*\] "GET .* HTTP.*" 404 .*$
            ^<HOST> - - \[.*\] "GET .* HTTP.*" 200 .*
".*(?:scan|scanner|bot|crawler|spider).*".*$

ignoreregex =

datepattern = ^[^\[]*\[({DATE})
              {^LN-BEG}
```

cela matchera toutes les tentatives d'accès à une ressources non existante (404) et le tentative de scan les bot ou crawler

---

APACHE2 REGEX 404/400/403

Editer le filtre

```
nano /etc/fail2ban/filter.d/apache-404.conf
```

Ajouter une **regex** afin de déceler l'erreur 404 qui apparrait dans /var/log/apache2/access.log. L'erreur 404 est de type Fichier introuvable | ou n'existe pas.

```
# Fail2Ban apache-404 filter
# POWERED By ME
#
# Author: Minos Corp Certified

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# apache-common.local
before = apache-common.conf

[Definition]

failregex = ^<HOST> - - \[.*\] "(GET|POST|HEAD).*HTTP.*" 404 .*$
        ^<HOST> - .* "(GET|POST|HEAD).*HTTP.*" 404 .*$

ignoreregex =

datepattern = ^[^\[]*\[({DATE})
              {^LN-BEG}
```

NOTE: Il fortement recommandé de créer la même REGEX pour l'erreur HTTP 400 “BAD REQUEST” ou HTTP 403 “ACCESS DENIED” (souvent du Path Transversal). Souvent utilisé par des scripts pour hacker votre serveur Web Apache, NGINX etc…
Dupliquer cette conf et modifier la REGEX:
Pour du 400 bad request

```
failregex = ^<HOST> - - \[.*\] "(GET|POST|HEAD).*HTTP.*" 400 .*$
        ^<HOST> - .* "(GET|POST|HEAD).*HTTP.*" 400 .*$
```

Pour du 403 access denied

```
failregex = ^<HOST> - - \[.*\] "(GET|POST|HEAD|CONNECT).*HTTP.*" 403 .*$
        ^<HOST> - .* "(GET|POST|HEAD|CONNECT).*HTTP.*" 403 .*$
```

APACHE2 REGEX BOTSCAN Custom

Créer le filtre

```
nano /etc/fail2ban/filter.d/apache-botscan.conf
```

Ajouter cette configuration.

```
# Fail2Ban apache-BotScan filter
# POWERED By ME
# Le 26/03/2025
# Author: Minos Corp Certified

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# apache-common.local
before = apache-common.conf

[Definition]

#Expression régulière pour capturer les logs avec tentative de hack (cible
error.log)
failregex = ^.*\[core:error\] \[pid \d+(:tid \d+)?\] \[client
<HOST>(:\d{1,5})?\] .*
            ^.*\[access_compat:error\] \[pid \d+(:tid \d+)?\] \[client
<HOST>(:\d{1,5})?\] .*
            ^.*\[php7:error\] \[pid \d+(:tid \d+)?\] \[client
<HOST>(:\d{1,5})?\] .*

ignoreregex =

datepattern = ^[^\[]*\[({DATE})
              {^LN-BEG}
```

Modifier votre fichier /etc/fail2ban/jail.d/defaults-debian.conf en conséquence.

```
[apache-botscan]
enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 1
```

Explication:
Ce **Jail** matchera pour ce type de log dans /var/apache2/error.log :

```
[Tue Mar 25 06:01:10.744042 2025] [core:error] [pid 32585:tid 32585] [client
95.111.238.161:38334] AH10244: invalid URI path (/cgi-
bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh)
[Tue Mar 25 06:01:11.021936 2025] [core:error] [pid 32586:tid 32586] [client
95.111.238.161:38340] AH10244: invalid URI path (/cgi-
bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%
65/%%32%65%%32%65/%%32%65%%32%65/bin/sh)
[Tue Mar 25 19:00:14.752092 2025] [php7:error] [pid 8556:tid 8556] [client
46.101.88.140:57868] script '/var/www/html/alive.php' not found or unable to
stat
[Tue Mar 25 22:31:18.813916 2025] [php7:error] [pid 10802:tid 10802] [client
```

```
45.88.182.12:52996] script '/var/www/html/phpinfo.php' not found or unable
to stat
[Tue Mar 25 22:31:19.549716 2025] [php7:error] [pid 32586:tid 32586] [client
45.88.182.12:53012] script '/var/www/html/info.php' not found or unable to
stat
[Tue Mar 25 22:54:00.047097 2025] [access_compat:error] [pid 32584:tid
32584] [client 193.200.78.21:50616] AH01797: client denied by server
configuration: /var/www/html/
```

Contrôle Service

```
sudo systemctl restart fail2ban
```

ou

```
service fail2ban restart
service fail2ban status
```

```
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor
preset: enabled)
   Active: active (running) since Sun 2020-02-16 19:19:17 CET; 1s ago
     Docs: man:fail2ban(1)
  Process: 13410 ExecStartPre=/bin/mkdir -p /var/run/fail2ban (code=exited,
status=0/SUCCESS)
 Main PID: 13411 (fail2ban-server)
    Tasks: 2 (limit: 2200)
   Memory: 5.8M
   CGroup: /system.slice/fail2ban.service
           └─13411 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

Après avoir relancer le services fail2ban vous devez recevoir un email vous informant que votre service est OK!
Bien sur assurez vous d'avoir configurer un serveur SMTP sur votre Linux.

Status des JAILs

```
 sudo fail2ban-client status
```

```
Status
|- Number of jail:    6
`- Jail list:  apache-400, apache-404, apache-auth, apache-botsearch, squid,
sshd
```

Cela indique que tout est OK! et que vos 6 services a surveiller son bien pris en charge.

Status des JAILs Spécifique

```
 sudo fail2ban-client status apache-404
```

```
Status for the jail: apache-404
|- Filter
|  |- Currently failed:  0
|  |- Total failed:  42
|  `- File list:   /var/log/apache2/access.log
`- Actions
   |- Currently banned:   3
   |- Total banned:   12
   `- Banned IP list:  91.32.239.115 185.184.70.24 81.185.161.109
```

Cela indique la liste des ip Bannis! Les courante et le totale.

Contrôle REGEX

Voici comment tester ses REGEX avant une mise en production définitive.
Test sur apache-404.conf

```
fail2ban-regex /var/log/apache2/access.log
/etc/fail2ban/filter.d/apache-404.conf
```

```
Running tests
=============

Use   failregex filter file : apache-404, basedir: /etc/fail2ban
Use      datepattern : Default Detectors
Use         log file : /var/log/apache2/access.log
Use         encoding : UTF-8


Results
=======

Failregex: 408 total
|-  #) [# of hits] regular expression
|   1) [398] ^<HOST> - - \[.*\] "(GET|POST|HEAD).*HTTP.*" 404 .*$
|   2) [10] ^<HOST> - .* "(GET|POST|HEAD).*HTTP.*" 404 .*$
`-

Ignoreregex: 0 total

Date template hits:
```

```
|- [# of hits] date format
|  [1734] ^[^\[]*\[(Day(?P<_sep>[-/])MON(?P=_sep)ExYear[
:]?24hour:Minute:Second(?:\.Microseconds)?(?: Zone offset)?)
`-

Lines: 1734 lines, 0 ignored, 408 matched, 1326 missed
[processed in 21.39 sec]

Missed line(s): too many to print.  Use --print-all-missed to print all 1326
lines
```

Ont observe ici 408 matched, cela veux dire 408 lignes sur 1734 ont été trouvé dans les logs.

Contrôle IPTABLES

Dans un terminal sur votre PC

```
iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-apache-400  tcp  --  anywhere             anywhere             multiport
dports http,https
f2b-apache-404  tcp  --  anywhere             anywhere             multiport
dports http,https
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             state
RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-squid (0 references)
target     prot opt source               destination
REJECT     all  --  83.118.199.10        anywhere             reject-with
icmp-port-unreachable
RETURN     all  --  anywhere             anywhere

Chain f2b-apache-404 (1 references)
target     prot opt source               destination
REJECT     all  --  213.227.153.43       anywhere             reject-with
icmp-port-unreachable
REJECT     all  --  139.199.206.114      anywhere             reject-with
icmp-port-unreachable
```

```
REJECT     all  --  129.211.141.242      anywhere             reject-with
icmp-port-unreachable
REJECT     all  --  111.26.185.208       anywhere             reject-with
icmp-port-unreachable
RETURN     all  --  anywhere             anywhere

Chain f2b-apache-400 (1 references)
target     prot opt source               destination
REJECT     all  --  161.red-2-136-134.staticip.rima-tde.net  anywhere
reject-with icmp-port-unreachable
RETURN     all  --  anywhere             anywhere
```

Nous voyons clairement que fail2ban a fait son Job.

Ip BANNIS

Pour contrôler les Ip Bannis, consulter les logs dans /var/log/fail2ban.log.

```
grep " Ban " /var/log/fail2ban.log
```

```
2020-03-02 04:55:55,692 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 178.32.150.152
2020-03-02 18:01:59,450 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 78.32.231.209
2020-03-02 23:39:23,068 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 103.31.249.37
2020-03-03 04:21:54,131 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 49.232.27.19
2020-03-05 08:38:03,635 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 213.227.153.43
2020-03-05 23:48:59,196 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 111.26.185.208
2020-03-06 08:22:49,849 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 129.211.141.242
2020-03-06 23:34:40,133 fail2ban.actions        [7629]: NOTICE  [apache-404]
Ban 139.199.206.114
2020-03-07 11:00:49,668 fail2ban.actions        [7330]: NOTICE  [apache-404]
Restore Ban 111.26.185.208
2020-03-07 11:00:49,839 fail2ban.actions        [7330]: NOTICE  [apache-404]
Restore Ban 129.211.141.242
2020-03-07 11:00:49,931 fail2ban.actions        [7330]: NOTICE  [apache-404]
Restore Ban 139.199.206.114
2020-03-07 11:00:50,022 fail2ban.actions        [7330]: NOTICE  [apache-404]
Restore Ban 213.227.153.43
2020-03-07 12:17:02,980 fail2ban.actions        [7330]: NOTICE  [apache-400]
Ban 2.136.134.161
```

BAN / UNBAN

Voici comment bannir ou dé-bannir une ip proprement en commande:
dé-bannir une ip:
fail2ban-client set [nom du jail] unbanip [IP concerné]

```
fail2ban-client set apache-404 unbanip 81.185.161.109
```

bannir une ip:
fail2ban-client set [nom du jail] banip [IP à bannir]

```
fail2ban-client set apache-404 banip 81.185.161.109
```

Contrôle BDD

Pour aller plus loin, on peut aussi contrôler la bases de donnée **sqlite3** de Fail2ban.
Elle se situe dans **/var/lib/fail2ban/fail2ban.sqlite3**
Elle contient toutes les infos liées aux BAN et au temps de grâce.
Exemple je veux contrôler son poids:

```
du -h /var/lib/fail2ban/fail2ban.sqlite3
```

```
18M /var/lib/fail2ban/fail2ban.sqlite3
```

Sqlite3

Installer le paquet si pas présent sur la machine.
Contrôle:

```
dpkg -l sqlite3
```

Installation :

```
apt install sqlite3
```

Nombre d'entrée en base (ip bannis)

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite3 "select count(*) from bans"
```

Pour voir l'âge de votre entrée en base de données la plus ancienne :

```
sqlite3 /var/lib/fail2ban/fail2ban.sqlite3 "select datetime(min(timeofban),
```

```
'unixepoch') from bans"
```

Dépannage

Fail2Ban ne se lance plus ou pas
Controle du service:

```
systemctl status fail2ban.service
```

```
~# service fail2ban start
~# service fail2ban status
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor
preset: enabled)
   Active: failed (Result: exit-code) since Sat 2021-03-06 22:21:12 CET; 1s
ago
     Docs: man:fail2ban(1)
  Process: 9825 ExecStartPre=/bin/mkdir -p /var/run/fail2ban (code=exited,
status=0/SUCCESS)
  Process: 9826 ExecStart=/usr/bin/fail2ban-server -xf start (code=exited,
status=255/EXCEPTION)
 Main PID: 9826 (code=exited, status=255/EXCEPTION)

systemd[1]: Starting Fail2Ban Service...
systemd[1]: Started Fail2Ban Service.
fail2ban-server[9826]:  No file(s) found for glob /var/log/squid/access.log
fail2ban-server[9826]:  Failed during configuration: Have not found any log
file for squid jail
fail2ban-server[9826]:  Async configuration of server failed
systemd[1]: fail2ban.service: Main process exited, code=exited,
status=255/EXCEPTION
systemd[1]: fail2ban.service: Failed with result 'exit-code'.
```

L'erreur est là!
No file(s) found for glob /var/log/squid/access.log
Failed during configuration: Have not found any log file for squid jail

Ceci arrive si vous désactiver un service qui est audité par Fail2Ban .
Ici en l'occurrence, le servcie Squid !!

Référez vous à cette Procédure.
Contrôle de service locaux sous LINUX

Réactiver le service Squid et relancer Fail2Ban

```
~# service fail2ban restart
~# service fail2ban status
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor
preset: enabled)
   Active: active (running) since Sat 2021-03-06 22:27:42 CET; 2s ago
     Docs: man:fail2ban(1)
  Process: 10185 ExecStartPre=/bin/mkdir -p /var/run/fail2ban (code=exited,
status=0/SUCCESS)
 Main PID: 10187 (fail2ban-server)
    Tasks: 15 (limit: 2200)
   Memory: 10.8M
```

— *sylvain 2020/03/07 14:34*