

Fail2ban pour Nextcloud sur Debian10 (Turnkey16)

Difficulté



Moyen

https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html#setup-fail2ban

HAProxy

- Régler pour obtenir les IPs de connexion tout en étant derrière le proxy: [HAProxy](#)

Fail2ban

source: <https://linuxize.com/post/install-configure-fail2ban-on-debian-10/>

- fail2ban est configuré d'origine sur ct Turnkey.

```
#systemctl status fail2ban
```

le confirme

- installer whois pour des infos plus détaillées sur les IPs bloquées

```
# apt-get install whois
```

- copier le fichier de configuration d'origine qui ne doit pas être modifié

```
# cp /etc/fail2ban/jail.{conf,local}
```

- paramétrer dans cette copie

```
# nano /etc/fail2ban/jail.{conf,local}
...
ignoreip = 127.0.0.1/8 IPs.reseau.lan.local/24 si besoin
...
bantime = 60m
...
findtime = 10m
...
maxretry = 5
...
destemail = admin@domain.tld
...
action = %(action_mw)s
...
```

```
# systemctl restart fail2ban
```

- Activer les jails:
Le plus simple est de faire ça dans webmin. Activer toutes les jails apache et SSL.

Pour Nextcloud

Malheureusement les jails de fail2ban ne suffisent pas car ce n'est pas Apache qui logge pas les tentatives d'identification mais Nextcloud!

- créer le filtre:

```
# nano /etc/fail2ban/filter.d/nextcloud.conf

[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": "
Trusted domain error.
datepattern = ,?\s*"time"\s*:\s*"%%Y-%%m-%%d[T ]%%H:%%M:%%S(%%Z)?"
```

- créer la jail:

```
# nano /etc/fail2ban/jail.d/nextcloud.local

[nextcloud]
backend = auto
enabled = true
port = 80,443
protocol = tcp
filter = nextcloud
maxretry = 3
bantime = 86400
findtime = 43200
logpath = /path/to/data/directory/nextcloud.log
```

- # systemctl restart fail2ban

Restreindre l'accès au répertoire

d'administration

- Dans la config d'Apache:

```
# nano /etc/apache2/sites-available/joomla.conf
```

et ajouter:

```
<Directory /var/www/joomla/administrator>  
    Order Deny,Allow  
    Deny from all  
    Allow from ip1.ou.bien.réseau1/24 ip2.ou.bien.réseau.2/24  
</Directory>
```

- # systemctl restart apache2

From:
<https://wiki.guedel.eu/> - Wiki-Guedel

Permanent link:
https://wiki.guedel.eu/doku.php?id=welcome:linux_usually:secure_nextcloud&rev=1638900339

Last update: **2021/12/07 18:05**

