# Fail2ban en CentOS7

Fail2ban logotipo
https://en.wikipedia.org/wiki/File:Fail2ban_logo.png

## Fail2ban es poderoso. Punto.

Desde el año 2015 lo utilizo y solo en unas cuantas ocasiones he tenido que revisarlo. En mi servidor principal tengo más de 22 mil direcciones IP que han osado de conectar por SSH **sin mi permiso ni autorización. Son demasiado abusadores.**

## Introducción

Para aquel año de 2015 escribimos un artículo, ni siquiera totalmente dedicado a Fail2ban sino como complemento a las conexiones SSH.

- Aquel artículo está escrito para Ubuntu 16.
- Aquel artículo está escrito para proteger SSH.
- Muchas de las cosas de ese artículo aún son válidas, otras no.

Aunque me gusta escribir artículos largos como aquel, pues que con tanto trabajo pues debo ahorrar tiempo.

**La razón importante para este nuevo artículo es mostrar que Fail2ban sirve para mucho, mucho más... ¿Qué?** Lean y sabrán.

## Añadir repositorio

## Instalar fail2ban

## Configurar fail2ban

Fail2ban lee su propia configuración de dos ficheros y todos los archivos contenidos en dos directorios (con extensiones .conf y .local)

```
/etc/fail2ban/jail.conf
/etc/fail2ban/jail.d/*.conf
/etc/fail2ban/jail.local
/etc/fail2ban/jail.d/*.local
```

En el caso de las carpetas, los archivos son procesados en orden alfabético. **La última instrucción que sea leída por Fail2ban será la que quede vigente (para ese parámetro o comando correspondiente).**

Lo de la extensión .local aún se mantiene por retrocompatibilidad, así que solamente usaremos la extensión .conf no más.

Haremos un fichero nuevo en el directorio jail:

```
sudo nano /etc/fail2ban/jail.d/mi_fail2ban.conf
```

En introducimos lo siguiente:

- Las líneas que comienzan con # son comentarios.
- Bloqueo por 3600 segundos (1 hora).
- Que utilice **iptables** para bloquear (banaction).
- Que se encargue de las conexiones SSH.

```
[DEFAULT]
# Bloquea por una hora:
bantime = 3600
# Sobreescribe /etc/fail2ban/jail.d/00-firewalld.conf:
banaction = iptables-multiport

[sshd]
enabled = true
```

Pulsamos CTRL+X, luego la tecla Y pulsamos Intro para guardar con el mismo nombre de archivo.

Y reiniciamos Fail2ban:

Confirmamos con:

```
sudo fail2ban-client status
```

O podemos ver solamente esa "jaula" que habilitamos, allí veremos las direcciones IP que han

sido bloqueadas por haber realizado intentos fallidos y no autorizados:

```
sudo fail2ban-client status sshd
```

## Configuración general

Ahora tocaremos algo más importante: la configuración para **todas las "jaulas" que tengamos** (por ahora una sola...)

Editamos:

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

Y buscamos los siguientes parámetros y lo modificamos a nuestro gusto:

```
# Para que ignore nuestras propias equivocaciones (IPv4 e IPv6)
ignoreip = 127.0.0.1/8 ::1

# Tiempo de bloqueo: un año (365 días)
bantime = 365d

# Bloqueo al primer intento
maxretry = 1
```

Pulsamos CTRL+X, luego la tecla Y pulsamos Intro para guardar con el mismo nombre de archivo.

Y reiniciamos Fail2ban:

```
systemctl restart fail2ban
```

## Configurando para Postfix

Ahora protegeremos nuestros servidor de correo electrónico **Postfix**, el cual solicita contraseña para poder atender el envío de cartas por correo electrónico.

Para ello buscaremos esta sección en /etc/fail2ban/jail.conf:

```
[postfix-sasl]
# Habilitamos esta jaula
enabled = true
# Le indicamos cuál puerto proteger
port = smtp
# Le obligamos a usar un filtro (ver más adelante)
filter = postfix-sasl
# De aquí de este registro de eventos (log) sacaremos
# los intentos fallidos y sus direcciones IP a bloquear
logpath = /var/log/mail.log
# Bloquea al primer intento
maxretry = 1
```

Para editar al filtro:

```
sudo nano /etc/fail2ban/filter.d/postfix-sasl.conf
```

E introducimos lo siguiente:

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = postfix/smtpd
failregex = warning: unknown\[\]: SASL (?:LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5
) authentication failed

[Init]
journalmatch = _SYSTEMD_UNIT=postfix.service
```

Esencialmente le estamos indicando a Fail2ban con el parámetro failregex que busque dentro de /var/log/mail.log los intentos fallidos como los siguientes:

```
May 12 19:31:06 aristarcos postfix/submission/smtpd[12212]: warning: unkn
own[141.98.10.27]: SASL PLAIN authentication failed:
May 12 19:33:43 aristarcos dovecot: auth-worker(16267): Error: pam(docume
nt,141.98.10.203): pam_authenticate() failed: Authentication failure (/et
c/pam.d/smtp missing?)
May 12 19:33:45 aristarcos postfix/submission/smtpd[16205]: warning: unkn
own[141.98.10.203]: SASL PLAIN authentication failed:
May 12 19:36:05 aristarcos dovecot: auth-worker(19281): Error: pam(anton,
141.98.10.81): pam_authenticate() failed: Authentication failure (/etc/pa
m.d/smtp missing?)
May 12 19:36:07 aristarcos postfix/submission/smtpd[19219]: warning: unkn
own[141.98.10.81]: SASL PLAIN authentication failed:
May 12 19:40:32 aristarcos dovecot: auth-worker(24447): Error: pam(tommy,
45.125.66.24): pam_authenticate() failed: Authentication failure (/etc/pa
m.d/smtp missing?)
May 12 19:40:34 aristarcos postfix/submission/smtpd[24408]: warning: unkn
own[45.125.66.24]: SASL PLAIN authentication failed:
May 12 19:43:19 aristarcos dovecot: auth-worker(27696): Error: pam(marian
ne,141.98.10.82): pam_authenticate() failed: Authentication failure (/etc
/pam.d/smtp missing?)
May 12 19:43:21 aristarcos postfix/submission/smtpd[27640]: warning: unkn
own[141.98.10.82]: SASL PLAIN authentication failed:
May 12 19:47:30 aristarcos dovecot: auth-worker(321): Error: pam(fred,141
.98.10.70): pam_authenticate() failed: Authentication failure (/etc/pam.d
/smtp missing?)
May 12 19:47:32 aristarcos postfix/submission/smtpd[32724]: warning: unkn
own[141.98.10.70]: SASL PLAIN authentication failed:
May 12 19:48:28 aristarcos postfix/submission/smtpd[32724]: warning: unkn
own[141.98.10.84]: SASL PLAIN authentication failed:
May 12 19:49:18 aristarcos postfix/submission/smtpd[32724]: warning: unkn
own[45.125.65.159]: SASL PLAIN authentication failed:
May 12 19:50:03 aristarcos postfix/submission/smtpd[32724]: warning: unkn
own[141.98.11.19]: SASL PLAIN authentication failed:
May 12 19:50:47 aristarcos postfix/submission/smtpd[32724]: warning: unkn
own[185.36.81.192]: SASL PLAIN authentication failed:
```

Guardar y reiniciar Fail2ban y confirmamos de nuevo cada "jaula" (ver secciones anteriores).

## Consultando iptables

Fail2ban utiliza a **iptables** para que se encargue del trabajo sucio, si consultamos con:

```
sudo iptables -L INPUT -v -n
```

Veremos los nombres de las "jaulas" y estas a su vez tendrán las direcciones IP bloqueadas.

## Fuentes consultadas

- https://www.digitalocean.com/community/tutorials/how-fail2ban-works-to-protect-services-on-a-linux-server
- https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-centos-7
- https://github.com/fail2ban/fail2ban/issues/2036
- https://fail2ban.readthedocs.io/en/latest/filters.html
- https://bobcares.com/blog/fail2ban-postfix-sasl/
- http://enricorossi.org/blog/2022/fail2ban_postfix_sasl/