fail2ban add custom filters

i love fail2ban and i think it should be enabled and configured by default in any linux server (and maybe even workstations) .. if you don't know it: fail2ban checks your logs and blocks ip's who repeatedly do something stupid on your system.. in more detail: fail2ban has a set of **filters** which contain regular expressions that are matched against a specific log file. In addition to that, fail2ban has **jails** which you define for each filter. A jail defines, how many times a filter's regex may match within what time frame for the same IP address. It also defines, how long that IP should be blocked and how exactly this should be achieved once it exceeds the allowed thresholds of regex matches.

usually your favorite distribution comes packed with filters and all you may have to do is enable them.. however, sometimes you might want to write your own rule, be it for your own application or for some case which is simply not covered by the default rules..

here is an example of how I added a new rule for postfix which filters out some bots who try to brute-force smtpd accounts. most of those are covered by the default filter in ubuntu, however, i had a case of a bot which tried to authenticate on a smtpd which only allowed TLS but it did not use TLS.. so the bot will honestly never suceed with this method of course, but it still was flooding my logs, so i decided to do something against that..

first let's look a the log entries which identify that sucker:

```
Dec  6 07:22:10 mail postfix/submission/smtpd[24962]: connect from unknown[170.106.11.80]
Dec  6 07:22:11 mail postfix/submission/smtpd[24962]: lost connection after EHLO from unknown[170.106.11.80]
Dec  6 07:22:11 mail postfix/submission/smtpd[24962]: disconnect from unknown[170.106.11.80] ehlo=1 auth=0/1 commands=1/2
```

we certainly don't want to block lline 1, as this would limit the number of connections per given timeframe you are allowed to make.. i don't want to limit that generally.. I also don't want to scan for line 2 as EHLO does not seem very harmful and you never know, maybe some appliatons will use that extensively for whatever reason.. but line 3 looks specific enough that I think it probably should not match any “normal” operations too often.. so let's go for that one

first we create a new filter in `/etc/fail2ban/filter.d/postfix-ehlo.conf`

/etc/fail2ban/filter.d/postfix-ehlo.conf

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = postfix/smtpd
failregex = ^%(__prefix_line)spostfix/submission/smtpd.*disconnect from unknown\[<HOST>\] ehlo=1 auth=0/1 commands=1/2$
ignoreregex =
```

HINT to figure out the regex, you can use `grep -P “my regex..” /var/log/mail.log` for example and then replace the `Dec 6 07:22:11 mail` part with `%(prefix_line)s`

now we can test this filter against our log file using `fail2ban-client`:

```
fail2ban-regex /var/log/mail.log /etc/fail2ban/filter.d/postfix-ehlo.conf
```

the important line we are looking for is this one:

```
Lines: 27233 lines, 0 ignored, 9005 matched, 18228 missed
```

s so you can see, the regex matched 9005 lines, that seems about right..