

Filters

You can customize, improve the filters Fail2Ban uses. You can find the filters in `/etc/fail2ban/filter.d/`. Below is a **small** collection of filters for the services, I have already covered.

nginx-http-auth.conf

[Definition]

```
failregex = ^ \[error\] \d+#\d+: \*\d+ user "\S+":? (password mismatch|was not found in ".*"), client: <HOST>,
server: \S+, request: "\S+ \S+ HTTP/\d+\.\d+", host: "\S+"$
^ \[error\] \d+#\d+: \*\d+ no user/password was provided for basic authentication, client: <HOST>,
server: \S+, request: "\S+ \S+ HTTP/\d+\.\d+", host: "\S+"$
```

```
ignoreregex =
```

nginx-badbots.conf

```
sudo cp apache-badbots.conf nginx-badbots.conf
```

nginx-noscript

[Definition]

```
failregex = ^<HOST> -.*GET.*(\.php|\.asp|\.exe|\.pl|\.cgi|\.scgi)
```

```
ignoreregex =
```

nginx-noproxy

[Definition]

```
failregex = ^<HOST> -.*GET http.*
```

```
ignoreregex =
```

MongoDB

mongo-auth.conf

[INCLUDES]

before = common.conf

[Definition]

_daemon = mongod

failregex = ^.*[aA]uthentication [fF]ail(ed|ure) for \w+ on \w+ from client <HOST>:[0-9].*|

ignoreregex =

Author: luisseok (<https://github.com/luisseok>)

Revision #1

Created 24 November 2024 17:13:20 by Nicolas

Updated 16 December 2024 10:42:28 by Nicolas