fail2ban

install

```
apt install fail2ban
```

filter

define new filter

/etc/fail2ban/filter.d/giano-login.conf

```
[Definition]
failregex = ^<HOST> .+ /auth/token/v2 HTTP/1.[0-9]" 401
ignoreregex =
```

test filter

```
fail2ban-regex /var/log/nginx/access.log /etc/fail2ban/filter.d/giano-login.conf --print-all-matched
```

jail

/etc/fail2ban/jail.d/giano-login.conf

```
[giano-login]
enabled = true
filter = giano-login
port = http,https
logpath = /var/log/nginx/*access*.log
findtime = 60
bantime = 6000
maxretry = 3
```

test

test

```
fail2ban-client -d
```

restart service to apply filter and jail

```
systemctl restart fail2ban
```

status

```
fail2ban-client status giano-login
```

unban

```
fail2ban-client set giano-login unbanip IPADDRESS
```

From:
https://wiki.csgalileo.org/ - **Galileo Labs**

Permanent link:
https://wiki.csgalileo.org/tips/fail2ban?rev=1555308405

Last update: **2019/04/15 08:06**