

# 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
```

## action

[action.d/telegram.conf](#)

```
[Definition]
actionstart = /usr/local/bin/telegram-send -g --format markdown "`uname
-n`: [Fail2Ban] jail <name> è stata avviata"
actionstop = /usr/local/bin/telegram-send -g --format markdown "`uname
-n`: [Fail2Ban] jail <name> è stata fermata"
actioncheck =
actionban = /usr/local/bin/telegram-send -g --format markdown "`uname -
n`: [Fail2Ban] IP <ip> è stato bannato dopo <failures> tentativi
falliti dalla jail <name>"
actionunban =

[Init]
init = 'Fail2Ban Telegram plugins activated'
```

# 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
action = %(action_)s
        telegram[name=GIANO]
```

## 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
```

## telegram action

```
pip install telegram-send
```

create configuration file with token and chat id

[/etc/telegram-send.conf](#)

```
[telegram]  
chat_id =  
token =
```

test (-g option to use /etc/telegram-send.conf)

```
telegram-send -g "hello, world"
```

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

Permanent link:  
<https://wiki.csgalileo.org/tips/fail2ban>

Last update: **2019/04/15 09:04**

