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.con)

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

/etc/fail2ban/scripts/telegram.sh

```
#!/bin/bash

# Sends text messages using Telegram
# to alert webmaster of banning.

# Require one argument, one of the following
# start
# stop
# ban
# unban
# Optional second argument: Ip for ban/unband


# Display usage information
function show_usage {
  echo "Usage: $0 action <ip>"
  echo "Where action start, stop, ban, unban"
  echo "and IP is optional passed to ban, unban"
  exit
}


# Send notification
function send_msg {
  apiToken=
  chatId=
  url="https://api.telegram.org/bot$apiToken/sendMessage"

  curl -s -X POST $url -d chat_id=$chatId -d text="$1"
  exit
}

# Check for script arguments
if [ $# -lt 1 ]
then
  show_usage
fi
```

```
# Take action depending on argument
if [ "$1" = 'start' ]
then
  msg='Fail2ban+just+started.'
  send_msg $msg
elif [ "$1" = 'stop' ]
then
  msg='Fail2ban+just+stoped.'
  send_msg $msg
elif [ "$1" = 'ban' ]
then
  msg=$([ "$2" != '' ] && echo "Fail2ban+just+banned+$2" || echo
'Fail2ban+just+banned+an+ip.' )
  send_msg $msg
elif [ "$1" = 'unban' ]
then
  msg=$([ "$2" != '' ] && echo "Fail2ban+just+unbanned+$2" || echo
"Fail2ban+just+unbanned+an+ip." )
  send_msg $msg
else
  show_usage
fi
```