Fail2ban Setup

?????

????????

/etc/fail2an/jail.conf

```
# "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
ignoreip = 127.0.0.1/8 ::1 192.168.9.0/24 192.168.31.0/24
```

????????

`fail2ban-client`

```
# set <JAIL> addignoreip <IP>
# set <JAIL> delignoreip <IP>
fail2ban-client set sshd addignoreip 123.123.123.123
fail2ban-client set sshd delignoreip 123.123.123.123
```

????

```
fail2ban-client get <JAIL> ignoreip
fail2ban-client get asterisk ignoreip
fail2ban-client get sshd ignoreip
```

???????

- Persistent Banning of IP Addresses with Fail2Ban
- Fail2Ban Blacklist JAIL for Repeat Offenders

?????

- ?????? IP? `fail2ban-client set blacklist banip xxx.xxx.xxx.xxx`

- ?????? IP? `fail2ban-client set blacklist unbanip xxx.xxx.xxx.xxx`
- ????? IP? `fail2ban-client status blacklist`

?????

`/etc/fail2ban/filter.d/blacklist.conf` :

```
# /etc/fail2ban/filter.d/blacklist.conf
# Fail2Ban Blacklist for Repeat Offenders (filter.d)

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]
# The name of the jail that this filter is used for. In jail.conf, name the
# jail using this filter 'blacklist', or change this line!
_jailname = blacklist

failregex =
ignoreregex =
```

`/etc/fail2ban/action.d/blacklist.conf` :

```
# /etc/fail2ban/action.d/blacklist.conf
# Fail2Ban Blacklist for Repeat Offenders (action.d)

[Definition]
# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#

actionstart = iptables -N f2b-<name>
              iptables -A f2b-<name> -j RETURN
              iptables -I <chain> -j f2b-<name>
              # Sort and Check for Duplicate IPs in our text file and Remove Them
              sort -u /etc/fail2ban/ip.blacklist -o /etc/fail2ban/ip.blacklist
```

```
             # Persistent banning of IPs reading from our ip.blacklist text file
             # and adding them to IPTables on our jail startup command
             cat /etc/fail2ban/ip.blacklist | while read IP; do iptables -I f2b-<name> 1 -s
$IP -j DROP; done

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#

actionstop = iptables -D <chain> -j f2b-<name>
             iptables -F f2b-<name>
             iptables -X f2b-<name>

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#

actioncheck = iptables -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#

actionban = iptables -I f2b-<name> 1 -s <ip> -j DROP
          # Add the new IP ban to our ip.blacklist file
          echo '<ip>' >> /etc/fail2ban/ip.blacklist
# I don't want reporting on any badboys service
# curl http://www.badips.com/add/badbots/<ip>/

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
```

```
actionunban = iptables -D f2b-<name> -s <ip> -j DROP
            # Remove IP from our ip.blacklist file
            sed -i -e '/<ip>/d' /etc/fail2ban/ip.blacklist

[Init]
# Chain to insert the f2b-<name> jump rule into
chain = INPUT
```

`/etc/fail2ban/jail.d/blacklist.conf` :

- bantime ? findtime ?????????????

```
# Usage:
# Add a bad IP - fail2ban-client set blacklist banip xxx.xxx.xxx.xxx
# Remove an IP - fail2ban-client set blacklist unbanip xxx.xxx.xxx.xxx

[blacklist]
enabled   = true
banaction = blacklist
bantime   = 2592000   ; 1 month
findtime  = 2592000   ; 1 month
```

DROP vs REJECT

?????

- DROP: `-j DROP`
- REJECT: `-j REJECT --reject-with icmp-port-unreachable`

? DROP ????

- Blacklist / ?? IP — ????????? IP ??????????? timeout ??
- SSH / ??????????? — ??????????????
- ????? — ?? footprint????????
- ???? (DDoS) — DROP ? REJECT ???????? ICMP ???

? REJECT ????

- ?????????? — ??? client ??????????? timeout
- ??? client ????? UX — ?????? port ??????????????? timeout
- Debug — ????????????????????
- ????????? — ????????????????? IP ???? REJECT ?? DROP

REJECT ???????

- icmp-port-unreachable?????— ??????????? port ????
- icmp-host-unreachable — ?????????????
- icmp-net-unreachable — ?????????????
- tcp-reset — ??? TCP RST?? TCP ?????????????? ICMP ???

Revision #13
Created 2022-05-30 11:46:26 CST by A-Lang (Admin)
Updated 2026-07-04 15:10:11 CST by A-Lang (Admin)