Fail2Ban Reference & Useful Commands

Category: All About Ubuntu
Last Updated: May 11, 2025
Applies To: Ubuntu Server 22.04+

Fail2Ban Jail Configuration

Fail2Ban jails control how long an IP remains banned after matching filters. To increase ban duration (e.g., to 48 hours):

Configuration File

```
sudo nano /etc/fail2ban/jail.local
```

Example Jail Settings for SSH and UFW Block:

```
[sshd]
enabled = true
port    = ssh
logpath = %(sshd_log)s
bantime = 172800
findtime = 600
maxretry = 3

[ufw-block]
enabled = true
filter  = ufw-block
logpath = /var/log/ufw.log
bantime = 172800
findtime = 600
maxretry = 3
```

[`bantime` is in seconds → `172800` equals 48 hours
[`findtime` is the window (in seconds) to detect repeated offenses
[`maxretry` is the number of failed attempts before banning

After changes:

```
sudo systemctl restart fail2ban
```

Useful Commands

Task	Command
Check fail2ban service status	`sudo systemctl status fail2ban`
Start fail2ban	`sudo systemctl start fail2ban`
Restart fail2ban	`sudo systemctl restart fail2ban`
View all jail statuses	`sudo fail2ban-client status`
View a specific jail (e.g., sshd)	`sudo fail2ban-client status sshd`
See currently banned IPs in a jail	`sudo fail2ban-client get sshd banned`
Unban an IP from a jail	`sudo fail2ban-client set sshd unbanip <IP>`
Get ignore list for a jail	`sudo fail2ban-client get sshd ignoreip`
Manually test a filter (dry run)	`fail2ban-regex /var/log/auth.log /etc/fail2ban/filter.d/sshd.conf`

Filter & Jail File Paths

File Purpose	Path
Jail configuration	`/etc/fail2ban/jail.local`
Custom filters	`/etc/fail2ban/filter.d/`
Fail2Ban main log	`/var/log/fail2ban.log`
UFW log (for ufw-block)	`/var/log/ufw.log`

Dynamically Updating `ignoreip` in Fail2Ban with DDNS

To prevent your own dynamic IP from being blocked by Fail2Ban (especially on services like `sshd` or custom UFW blocks), you can automate the injection of a DDNS-resolved IP into the `ignoreip`

configuration.

Script Overview

Location:
`/usr/local/bin/update-fail2ban-ignoreip.sh`

Purpose:
Resolves a DDNS hostname to an IPv4 address and updates the `ignoreip` line in `/etc/fail2ban/jail.local`. This helps Fail2Ban ignore your dynamic IP address automatically.

Key Script Breakdown

```
#!/bin/bash
DDNS_HOST="your-ddns.example.com"
RESOLVED_IP=$(dig +short "$DDNS_HOST" | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' | head -n 1)
```

- Resolves your DDNS hostname to a valid IPv4 address.

```
JAIL_FILE="/etc/fail2ban/jail.local"
```

- Points to the jail config you want to modify.

```
sed -i -E "s|^(ignoreip\s*=).*|\1 127.0.0.1/8 ::1 $RESOLVED_IP fe80::/10|" "$JAIL_FILE"
```

- Uses `sed` to replace the entire `ignoreip` line with:
  - localhost + loopback (`127.0.0.1/8 ::1`)
  - your **resolved** DDNS IP
  - and optional link-local IPv6 scope (`fe80::/10`)

```
systemctl restart fail2ban
```

- Restarts Fail2Ban so the updated IP takes effect immediately.

Example Output

```
Resolved IP: <your ip>
ignoreip updated in jail.local
Fail2Ban restarted successfully
```

Cron Job (Optional)

To schedule it daily or multiple times a day, add to `root`'s crontab:

```
*/15 * * * * /usr/local/bin/update-fail2ban-ignoreip.sh >> /var/log/update-fail2ban-ignoreip.log 2>&1
```

Notes

- Use `ignoreip` to exempt safe IPs (including local/DDNS).
- Consider rotating logs weekly to avoid bloated logs.
- Fail2Ban can be extended to cover other services (Apache, Postfix, etc.).

Revision #4
Created 9 May 2025 22:18:27 by Nate Nash
Updated 4 June 2025 23:32:00 by Nate Nash