NUST Cyber Security Team 2020

How to Install and Configure Fail2ban on Ubuntu

Fail2ban is a tool that helps protect your Linux machine from brute-force and other automated attacks by monitoring the services logs for malicious activity. It uses regular expressions to scan log files. All entries matching the patterns are counted, and when their number reaches a certain predefined threshold, Fail2ban bans the offending IP using the system firewall for a specific length of time. When the ban period expires, the IP address is removed from the ban list.

Installing Fail2ban on Ubuntu

sudo apt update

sudo apt install fail2ban

Once the installation is completed, the Fail2ban service will start automatically. You can verify it by checking the status of the service:

sudo systemctl status fail2ban

Fail2ban Configuration

The default Fail2ban installation comes with two configuration files, /etc/fail2ban/jail.conf and /etc/fail2ban/jail.d/defaults-debian.conf. It is not recommended to modify these files as they may be overwritten when the package is updated.

Fail2ban reads the configuration files in the following order. Each .local file overrides the settings from the .conf file:

- `/etc/fail2ban/jail.conf`
- `/etc/fail2ban/jail.d/*.conf`
- `/etc/fail2ban/jail.local`
- `/etc/fail2ban/jail.d/*.local`

For most users, the easiest way to configure Fail2ban is to copy the jail.conf to jail.local and modify the .local file. More advanced users can build a .local configuration file from scratch. The .local file doesn't have to include all settings from the corresponding .conf file, only those you want to override.

Create a .local configuration file from the default jail.conf file:

sudo cp /etc/fail2ban/jail.{conf,local}

To start configuring the Fail2ban server open, the jail.local file with your text editor :

sudo nano /etc/fail2ban/jail.local

The file includes comments describing what each configuration option does. In this example, we'll change the basic settings.

Whitelist IP Addresses

IP addresses, IP ranges, or hosts that you want to exclude from banning can be added to the ignoreip directive. Here you should add your local PC IP address and all other machines that you want to whitelist.

Uncomment the line starting with ignoreip and add your IP addresses separated by space:

e.g ignoreip = 127.0.0.1/8 ::1 123.123.123.123 192.168.1.0/24

Ban Settings

The values of bantime, findtime, and maxretry options define the ban time and ban conditions.

bantime is the duration for which the IP is banned. When no suffix is specified, it defaults to seconds. By default, the bantime value is set to 10 minutes. Generally, most users will want to set a longer ban time. Change the value to your liking:

e.g bantime = 1d

To permanently ban the IP use a negative number.

findtime is the duration between the number of failures before a ban is set. For example, if Fail2ban is set to ban an IP after five failures (maxretry, see below), those failures must occur within the findtime duration.

e.g findtime = 10m

Fail2ban Jails

Fail2ban uses a concept of jails. A jail describes a service and includes filters and actions. Log entries matching the search pattern are counted, and when a predefined condition is met, the corresponding actions are executed.

Fail2ban ships with a number of jail for different services. You can also create your own jail configurations.

By default, only the ssh jail is enabled. To enable a jail, you need to add enabled = true after the jail title. The following example shows how to enable the proftpd jail:

/etc/fail2ban/jail.local

```
[proftpd]

port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(proftpd_log)s
backend  = %(proftpd_backend)s
```

/etc/fail2ban/jail.local

```
[sshd]
enabled   = true
maxretry  = 3
findtime  = 1d
bantime   = 4w
ignoreip  = 127.0.0.1/8 23.34.45.56
```

Each time you edit a configuration file, you need to restart the Fail2ban service for changes to take effect:

sudo systemctl restart fail2ban

Fail2ban Client

Fail2ban ships with a command-line tool named fail2ban-client that you can use to interact with the Fail2ban service.

To view all available options, invoke the command with the -h option:

fail2ban-client -h

This tool can be used to ban/unban IP addresses, change settings, restart the service, and more. Here are a few examples:

Check the jail status:

sudo fail2ban-client status sshd

Unban an IP:

sudo fail2ban-client set sshd unbanip 23.34.45.56

Ban an IP:

sudo fail2ban-client set sshd banip 23.34.45.56