How to Install and configure Fail2ban

What is Fail2ban

Fail2ban is an open-source intrusion prevention software that helps protect Linux servers from **malicious attacks** by monitoring log files for suspicious activity and implementing various countermeasures. It works by analyzing log entries generated by system services and applications, such as SSH, Apache, Nginx, or any other service with configurable logs.

The primary purpose of Fail2ban is to detect and block **repeated failed login attempts**, **brute-force attacks**, or **any other suspicious activity that could indicate a potential security breach**. It achieves this by dynamically modifying firewall rules to block the IP addresses associated with the detected malicious behavior.

To install and configure Fail2ban, you can follow these general steps

1. Update your system

Ensure your system is up to date by running the following commands:

```
sudo apt update
sudo apt upgrade
```

or

```
apt update && apt upgrade -y && apt autoremove -y && apt autoclean
```

2. Install Fail2ban

Use the package manager of your distribution to install Fail2ban.
For Ubuntu or Debian-based systems, run:

```
sudo apt install fail2ban
```

or

```
apt install -y fail2ban
```

3. Configure Fail2ban

The main configuration file for Fail2ban is typically located at `/etc/fail2ban/jail.conf`. However, it's recommended to create an override configuration file to make future updates easier. Run the following command to create the override file:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

or

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

4. Edit the configuration file

Open the jail.local file in a text editor:

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

or

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

In this file, you'll find various configuration options. Some important options to consider are:
Locate the [DEFAULT] section, which contains the following global options:

- **ignoreip**: This option enables you to specify **IP addresses** or **hostnames** that fail2ban will ignore. For example, you could add your home or office IP address so fail2ban does not prevent you from accessing your own server. To specify multiple addresses, separate them with a space. For example:

  ```
  ignoreip = 127.0.0.1/8 93.184.216.34
  ```

- **bantime**: This option defines in seconds how long an IP address or host is banned. The default is 600 seconds (10 minutes).
- **maxretry**: This option defines the number of failures a host is allowed before it is banned.
- **findtime**: This option is used together with the maxretry option. If a host exceeds the maxretry setting within the time period specified by the findtime option, it is banned for the length of time specified by the bantime option.
- **destemail**: The email address where notifications will be sent.
- **action**: The action to be taken when a rule is triggered (e.g., banning the IP, sending an email).

Some important options to consider are:

- **enabled**: Set to true to enable the jail.

- **port**: The service's port you want to protect.
- **filter**: The name of the filter to use (usually corresponds to the service, e.g., sshd for SSH).
- **logpath**: The log file Fail2ban should monitor.

Adjust these options based on your needs. You can also enable/disable specific jail sections depending on which services you want to protect.

In this file, you can define custom jails (rules) and configure their behavior. Here's an example of a basic configuration for SSH protection:

```
[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1/8 123.45.67.89
# The bantime parameter sets the length of time that a client will be banned
# when they have failed to authenticate correctly. This is measured in seconds.
# By default, this is set to 30 days.
bantime = 30d
# The next two parameters are findtime and maxretry. These work together to
# establish the conditions under which a client is found to be an illegitimate
# user that should be banned.
# The maxretry variable sets the number of tries a client has to authenticate
# within a window of time defined by findtime, before being banned. With the
# default settings, the fail2ban service will ban a client that unsuccessfully
# attempts to log in 5 times within a 1 day window. Time units 1s 1m 1h 1d 1w
findtime = 1d
backend = auto
usedns = warn

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
```

You can add more jails for other services you want to protect, such as Apache, Nginx, or any other application running on your server.

5. Create Custom Filters (if necessary)

Filters define patterns Fail2ban looks for in log files. Default filters are located in `/etc/fail2ban/filter.d/`. If you need to create custom filters, you can do so by creating .conf files in this directory.

6. Enable and start Fail2ban

Once the configuration is complete, enable and start the Fail2ban service:

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

or

```
systemctl enable fail2ban
systemctl start fail2ban
```

Fail2ban should now be running and actively monitoring log files for suspicious activity.

?7. Check Fail2ban status

To check the status of Fail2ban and view any banned IP addresses, use the following command:

```
sudo fail2ban-client status
```

or

```
fail2ban-client status
```

This will display information about the active jails and any banned IPs.

To view detailed information about a specific jail:

```
sudo fail2ban-client status <jail-name>
```

or

```
fail2ban-client status <jail-name>
```

8. Testing Fail2ban

You can test Fail2ban by intentionally triggering a ban, like repeatedly failing to log in to your SSH server. After reaching the maxretry limit, your IP address should be banned.

That's it! You have installed and configured Fail2ban on your system. It will now monitor log files and take actions against suspicious activity based on your defined rules. Make sure to review the Fail2ban documentation for advanced configuration options and additional customization.

Ins0mniA

Revision #11
Created 2025-03-03 20:57:48 EET by Green
Updated 2025-09-04 02:03:24 EEST by Green