

Install And Configure Fail2Ban

Installation

1. Run the command below to install Fail2Ban

```
yum install fail2ban fail2ban-systemd
```

Configuration

1. Copy the “jail.conf” file and re-save it with the name “jail.local”

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

2. Edit the jail.local and add your local IP address onto the ***ignoreip*** line

[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
```

```
# Override /etc/fail2ban/jail.d/00-firewalld.conf:
```

```
banaction = iptables-multiport
```

```
# "bantime" is the number of seconds that a host is banned.
```

```
bantime = 600
```

```
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
```

```
findtime = 600
```

```
# "maxretry" is the number of failures before a host get banned.
```

```
maxretry = 5
```

Add a jail file to protect SSH access

1. Create a new file called sshd.local

```
| touch /etc/fail2ban/jail.d/sshd.local && chmod +x /etc/fail2ban/jail.d/sshd.local |
```

2. Edit the file and add the lines below

```
vi /etc/fail2ban/jail.d/sshd.local
```

Add these lines to the file

```
=====
```

```
[sshd]
enabled = true
port = ssh
#action = firewallcmd-ipset
logpath = %(sshd_log)s
maxretry = 5
bantime = 86400
```

Enable and start the FAIL2BAN service

1. Run the following commands to enable and start the Fail2Ban service

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

Revision #1

Created 16 April 2020 01:39:27 by Admin

Updated 16 April 2020 02:20:00 by Admin