Fail2Ban unter Debian installieren und konfigurieren

Inhaltsverzeichnis

- 1. 1. Fail2Ban installieren
- 2. 2. Eigene Konfigurationsdatei anlegen
- 3. 3. Grundkonfiguration für SSH
- 4. 4. SSH-Schutz aktivieren
- 5. 5. Fail2Ban neu starten
- 6. 6. Fail2Ban testen und überwachen
- 7. 7. IP-Adresse manuell entsperren
- 8. 8. Wichtige Hinweise

Fail2Ban sch??tzt deinen Server vor Brute-Force-Angriffen. Es ??berwacht Logdateien (z. B. von SSH) und sperrt IP-Adressen automatisch, wenn zu viele fehlgeschlagene Login-Versuche auftreten.

Gerade für Einsteiger ist Fail2Ban eine einfache und sehr effektive zusätzliche Sicherheitsmaßnahme.

---

1. 1. Fail2Ban installieren

Aktualisiere zuerst die Paketliste und installiere Fail2Ban:

Code

```
sudo apt update
sudo apt install fail2ban
```

Nach der Installation läuft Fail2Ban in der Regel bereits im Hintergrund.

---

2. 2. Eigene Konfigurationsdatei anlegen

Wichtig: Ändere niemals direkt die Datei `jail.conf`, da sie bei Updates überschrieben werden kann.

Erstelle stattdessen eine eigene Konfigurationsdatei:

Code

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

---

3. 3. Grundkonfiguration für SSH

Füge folgende Basis-Konfiguration ein:

Code

```
[DEFAULT]
bantime = 1h
findtime = 10m
maxretry = 5
```

Erklärung:

- `bantime` ? Wie lange eine IP gesperrt wird

- `findtime` ? Zeitraum, in dem Fehlversuche gezählt werden
- `maxretry` ? Anzahl erlaubter Fehlversuche

---

4. 4. SSH-Schutz aktivieren

Ergänze darunter die SSH-Sektion:

Code

```
[sshd]         enabled         =         true         port         =         ssh
logpath                              =                                %(sshd_log)s
backend = systemd
```

Wenn du den SSH-Port geändert hast, trage hier stattdessen deinen Port ein, z. B. `port = 2222`.

---

5. 5. Fail2Ban neu starten

Damit die Konfiguration übernommen wird, starte Fail2Ban neu:

Code

```
sudo systemctl restart fail2ban
```

Prüfe anschließend den Status:

Code

```
sudo systemctl status fail2ban
```

---

6. 6. Fail2Ban testen und überwachen

Aktive Jails anzeigen:

Code

```
sudo fail2ban-client status
```

Status speziell für SSH anzeigen:

Code

```
sudo fail2ban-client status sshd
```

Hier siehst du unter anderem:

- Anzahl gesperrter IPs
- Aktuell gebannte IP-Adressen

---

7. 7. IP-Adresse manuell entsperren

Falls du dich selbst ausgesperrt hast, kannst du eine IP manuell freigeben:

Code

```
sudo fail2ban-client set sshd unbanip <IP-Adresse>
```

Ersetze `<IP-Adresse>` durch die gesperrte IP.

8. 8. Wichtige Hinweise

- Teste Fail2Ban immer **nach der Einrichtung**, bevor du die SSH-Verbindung trennst.
- Nutze nach Möglichkeit zusätzlich **SSH-Keys**, nicht nur Passwörter.
- Fail2Ban ersetzt **keine Firewall**, sondern ergänzt sie sinnvoll.
- Bei Servern mit fester IP kannst du deine eigene IP in die Ignore-Liste aufnehmen.

Beispiel:

Code

```
ignoreip = 127.0.0.1/8 <deine-IP>
```

Mit Fail2Ban ist dein SSH-Server deutlich besser gegen automatische Angriffe geschützt und läuft komplett im Hintergrund.