Fail2Ban einstellen

Bitte stellen Sie sicher, dass Sie bevor Sie dieser Anleitung folgen, sudo und nano auf Ihrem Server installiert haben.

Zunächst müssen Sie die Muster Konfigurationsdatei als neue Datei speichern. Das können Sie mit folgendem Befehl erreichen.

Code

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

Die Konfigurationsdatei von Fail2Ban können Sie mit folgendem Befehl öffnen.

Code

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

Jetzt haben Sie eine endlos lange Konfigurationsdatei.

Hier ist eine Übersicht mit den wichtigsten Zeilen.

Alle Zeilen mit einem # werden von dem Programm ignoriert und werden Kommentare genannt.

Mit "ignoreip = 127.0.0.1/8" können Sie festlegen, welche IPs nicht gebannt werden sollen. Dies ist aber nur mit einer Festen IP sinnvoll.

Mit "bantime = 600" können Sie festlegen, wie lange ein Benutzer gebannt werden soll. Die Zeit wird hier in Sekunden gemessen.

Mit "findtime = 600" können Sie festlegen, wie lange die fehlgeschlagenen Login Versuche in der Vergangenheit zählen.

Mit "maxretry = 5" können Sie festlegen, wie viele fehlgeschlagene Login versuche erfolgen, bis es zu einem Ban kommt.

Anwendungen werden mit 2 eckigen Klammern gegenzeichnet z.B. "[sshd]".

Um einen Schutz für eine Anwendung zu aktivieren, fügen Sie "enabled = true".

Sollten Sie den Port einer Anwendung geändert haben können Sie diesen einfach mit einem "," an den schon vorhandenen Port anhängen.

Hier ist ein Beispiel für SSH.

Code

```
1. [sshd]
2. enabled = true
3. port = ssh,9876
4. logpath = %(sshd_log)s
5. backend = %(sshd_backend)s
```

Wenn man alles Fertig eingestellt hat, muss man die Datei mit "STRG+X" schließen und mit "Y" und "ENTER" bestätigen.

Jetzt muss man Fail2Ban noch Neustarten werden, um die Änderungen zu übernehmen. Das kann mit folgendem Befehl gemacht werden.

Code

```
1. sudo /etc/init.d/fail2ban restart
```

Sollte Fail2Ban nicht starten so ist ein Fehler in der Konfiguration oder ein Aktivierter Servers läuft nicht.