Fail2Ban

- Installation und Config
- Wichtige Befehle

Installation und Config

Auf Hetzner:

```
apt install -y fail2ban
nano /etc/fail2ban/jail.local
```

Inhalt:

```
[DEFAULT]
bantime = 3600
findtime = 600
maxretry = 5
ignoreip = 127.0.0.1/8 ::1

action = %(action_)s
         telegram

destemail = root@localhost
sendername = Fail2Ban
mta = mail

[sshd]
enabled = true
port = 9999
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 7200
```

Telegram-Action

```
nano /etc/fail2ban/action.d/telegram.conf
```

Inhalt (mit eigenen Werten)

```
[Definition]
```

```
actionstart = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="□□□Fail2Ban gestartet auf <fq-hostname>"

actionstop = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="⚠□ Fail2Ban gestoppt auf <fq-hostname>"

actioncheck =

actionban = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d parse_mode=HTML -d text="□□<b>IP gebannt!</b>%%0AServer: <fq-
hostname>%%0AJail: <name>%%0AIP: <ip>%%0AVersuche: <failures>%%0AZeit: $(date)"

actionunban = curl -s -X POST https://api.telegram.org/bot<TOKEN>/sendMessage -d
chat_id=<CHAT_ID> -d text="□ IP entsperrt: <ip> auf <fq-hostname>"

[Init]
```

Aktivieren:

```
systemctl restart fail2ban
systemctl status fail2ban
```

Wichtige Befehle

Status:

```
fail2ban-client status
fail2ban-cleint status sshd
```

Gebannte IP's:

```
fail2ban-client get sshd banned
```

IP bannen/entbannen

```
fail2ban-client set shhd banip 1.2.3.4
fail2ban-clien set shhd unbanip 1.2.3.4
```

Logs:

```
tail -f /var/log/fail2ban.log
```