

Zabezpečení Mailcow file2ban, přihlášení jen z CZ

- [Zabezpečení Mailcow file2ban, přihlášení jen z CZ](#)

Zabezpečení Mailcow fail2ban, p řihlášení jen z CZ

1. Nainstalovat geoip databázi:

```
apt install fail2ban
apt install geoip-database
apt install fail2ban geoip-database geoip-bin
```

Vytvoříme složku pro filtry, pokud neexistuje:

```
mkdir -p /etc/fail2ban/filter.d
```

2. Vytvořit nový filter pro fail2ban:

```
nano /etc/fail2ban/filter.d/non-cz.conf
```

S obsahem:

```
[Definition]
failregex = <HOST> .* [client .* ".*"$ !country=CZ
ignoreregex =
```

3. Vytvořit jail konfiguraci:

```
mkdir -p /etc/fail2ban/jail.d
nano /etc/fail2ban/jail.d/non-cz.conf
```

S obsahem:

```
[non-cz]
enabled = true
filter = non-cz
logpath = /var/log/auth.log
bantime = 86400
findtime = 600
maxretry = 1
```

4. Restartovat fail2ban:

```
systemctl restart fail2ban
```

Pravda, pojďme to udělat jednodušeji. Vytvořím vám jednoduchý skript, který uložíte do /root/check-ssh.sh a budete moci kdykoli spustit, abyste viděl, kdo se snažil připojit:

bash

```
cat > /root/check-ssh.sh << 'EOF'
#!/bin/bash
echo "=== Pokusy o SSH přihlášení ==="
journalctl | grep sshd | grep -i "failed\|invalid\|error" | tail -n 20
echo ""
echo "=== Blokované IP adresy ==="
iptables -L INPUT -n -v | grep DROP
EOF
```

Pak ho uděláte spustitelným:

bash

```
chmod +x /root/check-ssh.sh
```

A kdykoli budete chtít zkontrolovat pokusy o přihlášení, stačí napsat:

bash

```
/root/check-ssh.sh
```