

Fail2Ban

```
apt install fail2ban -y
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
sudo fail2ban-client reload
sudo fail2ban-client status  sshd
systemctl enable fail2ban
```

```
banaction = nftables-multiport
banaction_allports = nftables-allports
```

Налаштування Fail2Ban для запуску/зупинки за допомогою nftables

Ми намагаємося досягти наступного:

- під час завантаження сервер запускає спочатку nftables.service, а потім fail2ban.service;
- якщо ми запускаємо nftables.service, він також повинен запускати fail2ban.service;
- якщо ми зупинимо nftables.service, він також має зупинити fail2ban.service;
- якщо ми перезапустимо nftables.service, він також має перезапустити fail2ban.service;
- якщо ми запускаємо fail2ban.service, він також повинен запускати nftables.service;
- зупинка та перезавантаження дій на fail2ban.service не повинні впливати на nftables.service.

Ми можемо зробити все це, створивши файл перевизначення для fail2ban, вказавши йому, що він залежить від nftables, а потім nftables хоче, щоб він запусився:

```
mkdir -p /etc/systemd/system/fail2ban.service.d/
```

```
nano /etc/systemd/system/fail2ban.service.d/override.conf
```

```
[Unit]
Requires=nftables.service
PartOf=nftables.service

[Install]
WantedBy=multi-user.target nftables.service
```

Оскільки ми змінили розділ [Install], нам потрібно повторно ввімкнути відповідну службу, щоб створити відповідні символічні посилання. Ми також переконуємося, що nftables спочатку встановлено як сервісний блок:

```
# systemctl enable nftables.service
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib/systemd/system/nftables.service.
# systemctl enable fail2ban.service
Created symlink /etc/systemd/system/nftables.service.wants/fail2ban.service →
/lib/systemd/system/fail2ban.service.
# systemctl daemon-reload
```

Як саме це працює?

У нашому файлі заміни або повному файлі конфігурації (див. нижче) ми включаємо такі параметри:

```
[Unit]
Requires=nftables.service "запуск цієї служби спочатку запустить nftables.service."
PartOf=nftables.service "змушує цю службу зупинятися або перезапуститися (але не запускатися) за допомогою
nftables.service."

[Install]
WantedBy=multi-user.target nftables.service "змушує цю службу запускатися, коли запускається будь-яка з перелічених служб."
```

Як бачите, нам потрібно встановити Requires , PartOf і WantedBy , щоб отримати бажану поведінку.

From:
<https://ndp.pp.ua/> - **my NoDeny Wiki**

Permanent link:
<https://ndp.pp.ua/doku.php/debian/fail2ban?rev=1665184419>

Last update: **2022/10/08 02:13**

