

# Linux

## RockyLinux8 nftablesをDDNS対応(自宅のグローバルIPが動的の場合など)にしたい

nftablesでは、IPアドレスやポート等の指定でアクセスコントロールを行う。  
FQDNでは登録が出来ない。しかしながら、githubを巡回している際に、まさに欲しかった機能を  
開発されているソースを見かけたので実装した。

### ○ プログラム azlux / nft-dns

<https://github.com/azlux/nft-dns>

### ○ 動作

動作は至ってシンプルで、通常通りnftablesを動作させておき、  
nft-dnsが起動時に設定ファイルから、ホスト名(FQDN)を名前解決。  
nftコマンドで、予め定義されているテーブルへIPアドレスで登録。

nft-dns 初回動作後はデーモンとして常駐。デフォルト300秒 スリープして再度名前解決。  
IPアドレスが変更されていれば、nftコマンドで再登録される。

### ○ 注意

アクセスコントロール(ACL)において、ホスト名(FQDN)で名前解決での登録は脆弱であるという考えもあると思  
う。  
代表されるものに、「DNSキャッシュポイズニング(キャッシュ汚染)」があるが、nft-dnsの設定ファイルで、  
名前解決するDNSサーバを指定出来る。信頼のおけるDNSサーバを指定すれば、精神的に楽になるだろう。

### ○ インストール

debianではパッケージが用意されているようだが、RockyLinux用は無いので手動インストールを行う。

```
# dnf install python3.11.x86_64 python3.11-pip.noarch python3.11-pip-wheel.noarch
    デフォルトの3.6, 試しにインストールした3.9では動作せず。
    3.11 で動作確認
```

```
# dnf install python3.11-dns.noarch
# pip3.11 install pydantic
```

```
# git clone https://github.com/azlux/nft-dns.git
# cd nft-dns
# install -d /opt/nft-dns/{bin,etc,systemd}
# install -m 0755 nft-dns.py /opt/nft-dns/bin
# install -m 0644 entry.py /opt/nft-dns/bin
# install -m 0644 nft-dns.conf /opt/nft-dns/etc
# install -m 0644 nft-dns.service /opt/nft-dns/systemd
# ln -s /opt/nft-dns/systemd/nft-dns.service /lib/systemd/system
```

```
# vi /opt/nft-dns/systemd/nft-dns.service
    ExecStart行を変更
```

```
*** nft-dns.service.org 2024-04-30 20:05:42.087115770 +0900
--- nft-dns.service 2024-04-30 20:41:19.788540171 +0900
*****
*** 6,12 ****
[Service]
Type=simple
! ExecStart=/opt/nft-dns/nft-dns.py
Restart=on-failure
[Install]
--- 6,12 ----
```

# Linux

```
[Service]
Type=simple
! ExecStart=/opt/nft-dns/bin/nft-dns.py -c /opt/nft-dns/etc/nft-dns.conf
Restart=on-failure
[Install]
```

```
# vi /opt/nft-dns/bin/nft-dns.py
```

```
*** nft-dns.py.org 2024-04-30 15:51:26.107111494 +0900
--- nft-dns.py 2024-04-30 20:42:30.588258802 +0900
*****
```

```
*** 1,4 ****
```

```
! #!/usr/bin/env python3
```

```
from datetime import datetime, timedelta
import signal
from pathlib import Path
```

```
--- 1,4 ----
```

```
! #!/usr/bin/env python3.11
```

```
from datetime import datetime, timedelta
import signal
from pathlib import Path
```

```
# vi /opt/nft-dns/etc/nft-dns.conf
```

```
[GLOBAL]
```

```
#maxttl = 86400
#minttl = 300
#mode = capture
#custom_resolver = "1.1.1.1"
#dryrun = False
#verbose = False
includeconfdir = /opt/nft-dns/etc/nft-dns.d
```

```
[myddnsip]
```

```
setname = ALLOW-DNS
enable = true
family=ip
table=filter
domains = hoge.mydnsxxxxxx.mydns.jp
```

```
# systemctl enable nft-dns.service
# systemctl start nft-dns.service
# systemctl status nft-dns.service
```

```
nft-dns.service - NFTABLES DNS support
```

```
Loaded: loaded (/opt/nft-dns/systemd/nft-dns.service; enabled; vendor preset: disabled)
```

```
Active: active (running) since Thu 2024-11-21 05:30:08 JST; 3 days ago
```

```
Main PID: 264877 (python3.11)
```

```
Tasks: 1 (limit: 4408)
```

```
Memory: 21.7M
```

```
CGroup: /system.slice/nft-dns.service
```

```
mq264877 python3.11 /opt/nft-dns/bin/nft-dns.py -c /opt/nft-dns/etc/nft-dns.conf
```

```
11月 24 15:38:40 test.example.jp nft-dns.py[264877]: 2024-11-24 15:38:40,814 INFO:Sleeping for 302s
```

```
11月 24 15:43:42 test.example.jp nft-dns.py[264877]: 2024-11-24 15:43:42,855 INFO:Sleeping for 302s
```

```
11月 24 15:48:44 test.example.jp nft-dns.py[264877]: 2024-11-24 15:48:44,899 INFO:Sleeping for 302s
```

```
11月 24 15:53:46 test.example.jp nft-dns.py[264877]: 2024-11-24 15:53:46,941 INFO:Sleeping for 302s
```

```
11月 24 15:58:48 test.example.jp nft-dns.py[264877]: 2024-11-24 15:58:48,982 INFO:Sleeping for 302s
```

```
11月 24 16:03:51 test.example.jp nft-dns.py[264877]: 2024-11-24 16:03:51,024 INFO:Sleeping for 302s
```

ページ 2 / 3

© 2026 netstaff <netstaff@chovits.net> | 2026-05-14 16:11

URL: <https://www.chovits.jp/phpmyfaq/content/0cat=1/58/ja/rockylinux8-nftablesをddns対応自宅のグローバルipが動的の場合などにしたい.html>

# Linux

```
11月 24 16:08:53 test.example.jp nft-dns.py[264877]: 2024-11-24 16:08:53,064 INFO:Sleeping for 302s
11月 24 16:13:55 test.example.jp nft-dns.py[264877]: 2024-11-24 16:13:55,105 INFO:Sleeping for 302s
11月 24 16:18:57 test.example.jp nft-dns.py[264877]: 2024-11-24 16:18:57,144 INFO:Sleeping for 302s
11月 24 16:23:59 test.example.jp nft-dns.py[264877]: 2024-11-24 16:23:59,185 INFO:Sleeping for 302s
```

```
# nft list ruleset
```

(抜粋)

```
set ALLOW-DNS {
  type ipv4addr
  flags interval
  elements = { 203.0.113.100 }
}

chain INPUT {
  type filter hook input priority filter; policy drop;
  ct state new tcp dport 22 ip saddr @ALLOW-DNS accept
}
```

「ALLOW-DNS」リストに、hoge.mydnsxxxxx.mydns.jpのIPアドレス 203.0.113.100 が登録され、  
「INPUT」チェーンで、ソースIPが@ALLOW-DNS  
に登録されているリストを参照。かつ、destポートは、22/TCPはacceptする

このnft-dns.serviceでは、300秒おきにチェックしているが、  
自宅RouterのグローバルIPが変更されているかをチェックするスクリプト。  
変更された場合、DDNSサーバー(ここではMyDNS)へ変更を通知し、反映タイミング。キャッシュ時間待ち等を含めると、  
トータルで数十分は待たされる事にはなるが、有効活用したい。

添付ファイル::

一意的なソリューション ID: #1057

製作者: n/a

最終更新: 2024-11-24 16:48