

Testování DNS serveru, kompletní příkazy

1. Test lokálního resolveru (Pi-hole)

```
# Otestujte základní dotaz přes Pi-hole
dig @127.0.0.1 example.com

# Test rekurze + DNSSEC
dig @127.0.0.1 example.com +dnssec +multiline

# Test blokování reklam (mělo vrátit 0.0.0.0)
dig @127.0.0.1 doubleclick.net
```

2. Test Unbound (lokální cache)

```
# Dotaz přímo na Unbound (port 5053)
dig @127.0.0.1 -p 5053 example.com

# Zkontrolujte cache (TTL by se měl snižovat)
dig @127.0.0.1 -p 5053 example.com +short
```

3. Test DNSCrypt-proxy (šifrovaný DNS)

```
# Dotaz přímo na DNSCrypt (port 5300)
dig @127.0.0.1 -p 5300 example.com

# Test DoH (DNS-over-HTTPS)
curl -H 'accept: application/dns-json' 'http://127.0.0.1:5300/dns-query?name=example.com&type=A'
```

4. Test z externích zařízení

```
# Z Synology (IP 192.168.54.254)
nslookup example.com 192.168.54.X # (IP Pi-hole)

# Z jiného zařízení v síti
```

```
dig @192.168.54.X example.com # (IP Pi-hole)
```

5. Pokročilé testy

```
# Test rychlosti (měří odezvu)
time dig @127.0.0.1 example.com
# Test DNSSEC (mělo být "ad" flag)
dig @127.0.0.1 sigok.verteiltesysteme.net +dnssec
# Test netestovaného doménového jména (mělo selhat)
dig @127.0.0.1 test.dnssec-failed.org
```

Ideální výsledek

- Všechny dotazy by měly vracet **rychlé odpovědi** (pod 50 ms)
- DNSSEC dotazy by měly mít **"ad" flag** (ověřené)
- Blokované domény by měly vracet **0.0.0.0**
- V logách by neměly být **chyby "ignoring query"**

Revision #1

Created 19 April 2025 23:24:30 by Admin

Updated 19 April 2025 23:28:48 by Admin