Unbound DNS Resolver

Unbound is a fast, secure, validating, recursive, and caching DNS resolver. It's commonly used for privacy (no third-party logs), DNSSEC validation, and performance via local caching.

Installation

```
apt update && apt dist-upgrade -y
apt install sudo vim unbound unbound-anchor dns-root-data
```

Basic Configuration

Create or edit a config file. Common location:

`/etc/unbound/unbound.conf` (main file, often includes other files)

```
vim /etc/unbound/unbound.conf
```

Minimal recommended config (for home use):

```
server:
    # DNSSEC trust anchor (auto-updates)
    auto-trust-anchor-file: "/var/lib/unbound/root.key"

    # Privacy: minimal information sent upstream
    qname-minimisation: yes

    # Listen on all interfaces (or 127.0.0.1 for local-only)
    interface: 0.0.0.0
    # interface: ::0   # IPv6

    # Allow queries from your local network
    access-control: 127.0.0.0/8 allow
```

```
    access-control: 192.168.178.0/16 allow   # Adjust to your subnet (e.g. 10.0.0.0/8)
    # access-control: 172.16.0.0/12 allow

    # Security & performance
    harden-glue: yes
    harden-dnssec-stripped: yes
    use-caps-for-id: no
    edns-buffer-size: 1232
    prefetch: yes
    num-threads: 1   # Increase on powerful hardware

    # Hide private addresses
    private-address: 192.168.178.0/16
    private-address: 10.0.0.0/8
    private-address: 172.16.0.0/12

    # Logging
    verbosity: 0
```

Root Hints & DNSSEC

Most package installs handle this automatically via `dns-root-data`. To update manually:

```
wget https://www.internic.net/domain/named.root -qO- | sudo tee /var/lib/unbound/root.hints

# Initialize DNSSEC trust anchor
sudo unbound-anchor -a /var/lib/unbound/root.key
```

Start and Enable the Service

```
sudo systemctl enable --now unbound
sudo systemctl restart unbound
```

Check status:

```
sudo systemctl status unbound
```

Validate config:

```
unbound-checkconf
```

Test It

```
# Local test
dig example.com @192.168.178.118


# Should show SERVER: 127.0.0.1#53
```

Configure your client to DNS Server

which is in my case 192.168.178.118

```
vim /etc/resolv.conf
```

```
nameserver 192.168.178.118
```

Validate DNSSEC

to validate your DNSSEC you can got to this page:

https://wander.science/projects/dns/dnssec-resolver-test/

Revision #1
Created 2026-06-01 21:39:57 UTC by tinfoil-hat
Updated 2026-06-01 21:40:17 UTC by tinfoil-hat