Unbound

Unbound is a validating, recursive, and caching DNS resolver product from NLnet Labs. It is distributed free of charge in open-source form under the BSD license.

Package

```
sudo pacman -S unbound expat
```

Configuration

```
sudo nano /etc/unbound/unbound.conf
```

```
server:
    # If no logfile is specified, syslog is used
    # logfile: "/var/log/unbound/unbound.log"
    verbosity: 0

# Enable port if you're going to use DNSCrypt/ADGuardhome.
#    port: 5353

    do-ip4: yes
    do-udp: yes
    do-tcp: yes
    do-daemonize: no
    trust-anchor-file: /etc/unbound/trusted-key.key

    # May be set to yes if you have IPv6 connectivity
    do-ip6: no

    # Use this only when you downloaded the list of primary root servers!
    root-hints: "/etc/unbound/root.hints"

    # Trust glue only if it is within the servers authority
    harden-glue: yes

    # Require DNSSEC data for trust-anchored zones, if such data is absent,
the zone becomes BOGUS
    harden-dnssec-stripped: yes

    # Don't use Capitalization randomization as it known to cause DNSSEC
issues sometimes
    # see
https://discourse.pi-hole.net/t/unbound-stubby-or-dnscrypt-proxy/9378 for
further details
```

```
    use-caps-for-id: no

    # Reduce EDNS reassembly buffer size.
    # Suggested by the unbound man page to reduce fragmentation reassembly
problems
    edns-buffer-size: 1472

    # TTL bounds for cache
    cache-min-ttl: 3600
    cache-max-ttl: 86400

    # Perform prefetching of close to expired message cache entries
    # This only applies to domains that have been frequently queried
    prefetch: yes

    # One thread should be sufficient, can be increased on beefy machines
    num-threads: 1

    # Ensure kernel buffer is large enough to not loose messages in traffic
spikes
    so-rcvbuf: 1m

    hide-identity: yes
    hide-version: yes
```

root.hints

To recursively query a host that is not cached as an address, the resolver must start at the top of the server tree and query the root servers to learn where to find the top-level domain for the queried address. There are hints built into Unbound by default. Therefore, if the package is updated regularly, no manual intervention is required. Otherwise, it is advisable to use a root hint file, since the built-in hints may be outdated.

```
curl --output /etc/unbound/root.hints
https://www.internic.net/domain/named.cache
```

```
sudo nano /etc/systemd/system/roothints.service
```

```
[Unit]
Description=Update root hints for unbound
After=network.target

[Service]
ExecStart=/usr/bin/curl -o /etc/unbound/root.hints
https://www.internic.net/domain/named.cache
```

```
sudo nano /etc/systemd/system/roothints.timer
```

```
[Unit]
```

```
Description=Run root.hints monthly

[Timer]
OnCalendar=monthly
Persistent=true

[Install]
WantedBy=timers.target
```

Start

```
sudo systemctl enable --now unbound.service roothints.timer
```

Local DNS via NetworkManager

```
sudo nano /etc/NetworkManager/conf.d/dns-servers.conf
```

```
[global-dns-domain-*]
servers=127.0.0.1
```

```
sudo systemctl restart NetworkManager.service
```

DNSCrypt proxy

If you want to install our DNSCrypt tutorial, or you already have it, you still need to enable the port

> # Enable port if you're going to use DNSCrypt/ADGuardhome.
> port: 5353

and add the following to the bottom:

```
# dnscrypt-proxy
  do-not-query-localhost: no
forward-zone:
  name: "."
  forward-addr: 127.0.0.1@5300
```

2022/05/30 02:20 · dan

From:
http://wiki.techsaviours.org/ - **Your Digital Privacy DIY Solutions | TECH SAVIOURS .ORG**

Permanent link:
http://wiki.techsaviours.org/en/desktop/services/unbound

Last update: **2022/10/24 08:24**