# CachingNameserver

- Installing
  - Unbound
  - PowerDNS Recursor
  - BIND
  - rbldnsd
- Using
- Testing

# Installing

SpamAssassin will perform many DNS lookups for NetworkTests to significantly improve scoring of messages primarily by DNSBlocklists like Spamhaus, SORBS, etc. This information needs to be cached locally to improve performance and limit the number of external DNS queries since some DNSBlockLists have limits on free usage.

NOTE: A local DNS caching server should not forward to other DNS servers to ensure your queries are not combined with others. Forwarding to other DNS servers often results in URIBL_BLOCKED or similar rule hits meaning you have gone over their free usage limit. More info about this can be found in FAQ.

Wikipedia DNS Server feature matrix

Dnsmasq should not be used by SpamAssassin since it can only forward to other DNS servers.

An advanced setup is possible atleast with Unbound and BIND, where queries are forwarded by default to another DNS servers, *but exceptions like Spamhaus can be made to go direct*. Using global forwarders like Cloudflare (1.1.1.1) or Google (8.8.8.8) can actually improve performance, since their huge caches help with all the common stuff like DKIM, SPF, PTR/MX lookups etc.

## Unbound

Packaging varies slightly between distributions so refer Internet articles for details and current information for your OS version. The default configuration files should give us a desired caching non-forwarding DNS server listening locally only.

Debian/Ubuntu:

```
apt-get update
apt-get install unbound
```

RHEL/CentOS:

```
yum install unbound
chkconfig unbound on
service unbound start
```

Fedora:

```
dnf install unbound
systemctl enable unbound
systemctl start unbound
```

## PowerDNS Recursor

Default PowerDNS Recursor installs should be the desired non-forwarding caching only DNS server listening only on localhost. Refer to other online articles for details about the config files and settings specific to your OS version.

Debian/Ubuntu:

```
apt-get update
apt-get install pdns-recursor
```

RHEL/CentOS:

```
# EPEL repository required
yum install epel-release
yum install pdns-recursor
chkconfig pdns-recursor on
service pdns-recursor start
```

Fedora:

```
dnf install pdns-recursor
systemctl enable pdns-recursor
systemctl start pdns-recursor
```

## BIND

Debian/Ubuntu:

```
apt-get update
apt-get install bind9
```

RHEL/CentOS:

```
yum install bind bind-utils
chkconfig named on
service named start
```

Fedora:

```
dnf install bind bind-utils
systemctl enable named
systemctl start named
```

## rbldnsd

Rbldnsd is not a recursive caching DNS server. It is an authoritative DNS server primarily used to host private/internal zones from feeds like Spamhaus, Invaluement, SORBS, etc. Typically rbldnsd will listen on an alternate port then the primary DNS server setup above would forward specific zones to rbldnsd.

Rbldnsd is a little tricky to get setup but once you do it is rock solid. You simply wget, curl, rsync the feed files and rbldnsd can detect changes then automatically reload them.

Search the Internet for current articles for your specific OS. Here's the basic setup on a systemctl-based OS taken from CentOS 7:

1. Rsync the feed files into /var/lib/rbldnsd
2. List the feed files in /etc/systemd/system/rbldnsd-dsbl.service

   ```
   .include /etc/systemd/rbldnsd.conf

   [Unit]
   Description=DNSBL (rbldnsd) dsbl instance

   [Service]
   ExecStart=/sbin/rbldnsd -n -f -r /var/lib/rbldnsd -b 127.0.0.1/530 dul.dnsbl.sorbs.net:ip4set:dul.dnsbl.
   sorbs.net http.dnsbl.sorbs.net:dnset:http.dnsbl.sorbs.net smtp.dnsbl.sorbs.net:ip4set:smtp.dnsbl.sorbs.
   net new.spam.dnsbl.sorbs.net:ip4set:new.spam.dnsbl.sorbs.net dnsbl-1.uceprotect.net:ip4set:dnsbl-1.
   uceprotect.net
   ```

3. Enable and start the service

```
systemctl enable rbldnsd-dsbl
systemctl start rbldnsd-dsbl
```

4. rbldnsd should now be listening on port 530

   ```
   # netstat -tunlap | grep rbldns
   udp        0      0 127.0.0.1:530           0.0.0.0:*                           901/rbldnsd
   ```

5. Setup your main DNS caching server to forward to rbldnsd. This is an example for PowerDNS recursor:
   - /etc/pdns-recursor/recursor.conf

     ```
     forward-zones-file=/etc/pdns-recursor/forward-zones
     ```

   - /etc/pdns-recursor/forward-zones

     ```
     dul.dnsbl.sorbs.net=127.0.0.1:530
     http.dnsbl.sorbs.net=127.0.0.1:530
     smtp.dnsbl.sorbs.net=127.0.0.1:530
     new.spam.dnsbl.sorbs.net=127.0.0.1:530
     dnsbl-1.uceprotect.net=127.0.0.1:530
     ```

# Using

SpamAssassin local.cf

```
dns_available yes
```

/etc/resolv.conf

```
search example.com
nameserver 127.0.0.1
```

NOTE: If something like NetworkManager is reverting your changes in /etc/resolv.conf or you don't have permission to update the /etc/resolv.conf, you may specify a DNS server in the local.cf:

```
dns_server 127.0.0.1
```

# Testing

Use *dig* to test DNS queries. If you don't get a response then the local DNS server could:

1. not have proper connectivity outbound to the Internet - a firewall could be blocking UDP/TCP 53
2. have reached the free usage limit of the DNSBlockList - remove the "+short" to see more detail in the ANSWER section
3. may not be configured correctly - search for articles on how to setup your specific DNS caching server on your specific OS

Spamhaus Zen:

```
dig +short 2.0.0.127.zen.spamhaus.org
127.0.0.10
127.0.0.4
127.0.0.2
```

SORBS DUL:

```
# dig 2.0.0.127.dul.dnsbl.sorbs.net +short
127.0.0.10
```

URIBL:

```
dig test.uribl.com.multi.uribl.com txt +short
"permanent testpoint"
```

If you don't get the *permanent testpoint* response above, then you are most likely also hitting the URIBL_BLOCKED rule. Check your mail logs. If you are a major mail filtering provider with high volume, then you may have to disable the following rules in the local.cf or you might just get an email from them with pricing information:

```
score URIBL_BLACK 0
score URIBL_GREY 0
score URIBL_RED 0
```