Domain Name Server (DNS)

We use two different local DNS servers on various systems: Unbound and Dnsmasq.

Unbound vs Dnsmasq

Unbound, like Bind is a full DNS resolver which can talk directly to the DNS root servers. Dnsmasq is only a forwarder, it will ask your nearest DNS (mostly the ISP's servers or Google). Thus, a forwarders answers are an implicit trust in the DNS server chain that you are using. It's in that sense less secure that it may not return what the root servers would return. In the worst case that is an attack or unwanted advertising.

Querying DNS services

Using dig command you can query DNS name servers for your DNS lookup related tasks. Dig stands for domain information groper.

Simple query

Standard query using the default DNS server configured on your system

```
# dig oscardegroot.nl
-----------------------
; <<>> DiG 9.11.5-P4-5.1+deb10u3-Debian <<>> oscardegroot.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58194
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;oscardegroot.nl.               IN      A

;; ANSWER SECTION:
oscardegroot.nl.        13636   IN      A       83.86.60.198

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: wo mrt 24 13:06:00 CET 2021
;; MSG SIZE  rcvd: 60
```

The dig command output has the following sections:

- **Header**: This displays the dig command version number, the global options used by the dig command, and few additional header information.
- **QUESTION SECTION**: This displays the question it asked the DNS. i.e This is your input. Since we said 'dig redhat.com', and the default type dig command uses is A record, it indicates in this section that we asked for the A record of the redhat.com website
- **ANSWER SECTION**: This displays the answer it receives from the DNS. i.e This is your output. This displays the A record of redhat.com
- **AUTHORITY SECTION**: This displays the DNS name server that has the authority to respond to this query. Basically this displays available name servers of redhat.com
- **ADDITIONAL SECTION**: This displays the ip address of the name servers listed in the AUTHORITY SECTION.
- **Stats section** at the bottom displays few dig command statistics including how much time it took to execute this query

Use specific DNS server

By default dig uses the DNS servers defined in your **/etc/resolv.conf** file. If you like to use a different DNS server to perform the query, specify it in the command line as **@dnsserver**.

Short Output Using dig +short

To view just the ip-address of a web site (i.e the A record), use the short form option as shown below.

```
dig oscardegroot.nl +short
------------------------------------
83.86.60.198
```

Limit output to specific section

The response can be limited to any of the sections. E.g. the next only displays the ANSWER SECTION.

```
# dig oscardegroot.nl +noall +answer
-----------------------------------
; <<>> DiG 9.11.5-P4-5.1+deb10u3-Debian <<>> oscardegroot.nl +noall +answer
;; global options: +cmd
oscardegroot.nl.        13296   IN      A       83.86.60.198
```

Query Record types

With the -t option you can select a specific record type. This is one of: **a, any, mx, ns, soa, hinfo, axfr, txt**. The default is: a. Be aware that not all DNS servers have copies of all the records locally. So if this query return incomplete info, use a different DNS server.

```
# dig @192.168.178.1 oscardegroot.nl -t any +noall +answer
----------------------------------------------------------
```

```
; <<>> DiG 9.11.5-P4-5.1+deb10u3-Debian <<>> @192.168.178.1 oscardegroot.nl
-t any +noall +answer
; (1 server found)
;; global options: +cmd
oscardegroot.nl.        86400   IN      TXT     "v=spf1 ip4:212.54.42.1/24
~all"
oscardegroot.nl.        86400   IN      MX      10 oscardegroot.nl.
oscardegroot.nl.        86400   IN      NS      ns2.transip.eu.
oscardegroot.nl.        300     IN      NSEC3PARAM 1 0 100 7A6F6BE2671ACE93
oscardegroot.nl.        86400   IN      NS      ns1.transip.nl.
oscardegroot.nl.        300     IN      DNSKEY  257 3 7
AwEAAc4RYjNmnUu20xeaWUFNXTKF7NyceaAnUf6XSAnCWHOtNjfYCq1a
/rWQx9ewKUHZsZyzLyzW  cBDwJfVHoq0pLKXOYzgTmHcgubGAquspVVKW
5XEVK3wN1Tmn1suO8r9fo5B3d0vFsWlZLgAEfylieUL/doTIK4ZLez4O
YgEvRFPGHwjaWoTyCvCYV2jTn1qfZF4Q90Opo/p  x/RX7enfzf2kDcsPV
BWh13ghrLBdIgcflb+2JxPw9bQ8Cfmej9P5bLQsbO7sPQv/ieNChZ47V
SnkP+Pk9o6ucXNGrk7cWwx+ZP3UGx6TuQuL7CZ91gDfvdotVU1fOl+hY D  HmNMpJC7qU=
oscardegroot.nl.        300     IN      DNSKEY  256 3 7
AwEAAcVuFjB7HrAoM+qnuNb532dvTnX3Wg29wnnWIN0hlf4NAi27Z67D
WS6JbratSwuZ0ga32nQ1  6ruMh6bbDOBqrKLb/Qmp71ZLjvNP+ih7dz9G
nmqfWbSiW+mMg7H9cX0JV4+ihqw7EFxTRwyu5foJ01Il6EVr+nIKJtQM hYoorhDz
oscardegroot.nl.        86400   IN      A       83.86.60.198
oscardegroot.nl.        3600    IN      SOA     ns0.transip.net.
hostmaster.transip.nl. 2021031313 86400 1800 2419200 300
oscardegroot.nl.        86400   IN      NS      ns0.transip.net.
oscardegroot.nl.        86400   IN      RRSIG   A 7 2 86400 20210401000000
20210311000000 18644 oscardegroot.nl. scZnWng3OLaF95T8xQmB
N53oNKMCAM/c2qqViw4vvR1jx+p1XSgULMmP
xhZaxQJrKNgj3NTiQ/hUPnffxigp4Ak017+gzNwTBTSZ2YpuGEgxqSiX
ouRmLrkiZo+hiL8Cfx+1mKgq9pG1TIl6CTOY1lD  onjYW7i8Hiz04oKP9 xXg=
oscardegroot.nl.        86400   IN      RRSIG   NS 7 2 86400 20210401000000
20210311000000 18644 oscardegroot.nl. qrhwgyekbLJzHDl2bDf
oPX8BKABVxF1j7Z37CmOFxdDCJnIgj5WWnBKn
QJ/1hFgaSu4lHQ5AGaJ/H5C2rdijq+9iPeMTaieds10HUwFJHViGtb67
TOA5C7oXQVmysYnGerZ9XlOtvzBp/KJBjZFaYu  QddDxzCeRh46nn9Sm4 IG0=
oscardegroot.nl.        3600    IN      RRSIG   SOA 7 2 3600 20210401000000
20210311000000 18644 oscardegroot.nl. g11Ywidy/uu8RsfbM2r
rqUeVnTD8pJnnaL3SBFAgiRHgvCGFvnyTz8jn
4wkZdEpJL4eznJ72dZ+uvxAfhF1lTq+h4L8vIFjFRcIR1noQwlpyHBJu
4XypHmmiV+UplSnjCGf6Uz4u89GYuj+Gporeie  lfniXH+amPGBC2WkXj tGY=
oscardegroot.nl.        86400   IN      RRSIG   MX 7 2 86400 20210401000000
20210311000000 18644 oscardegroot.nl. w+HSrmvU9sKuDo/nVI8
EA/DkYRXUyG1d0q1ConEmqgGVI7H20aceMgtY
BeL204z1FfOr1yiDLJAit6W5W+U6mrH5ULpWv9xugM8qhUxtF/d6YPtk
4aJChyxSIGDa1pTdUoTx3XuEx0PVHDfopoNeF5  PZIHnMtDJkOLHT2l64 s4E=
oscardegroot.nl.        86400   IN      RRSIG   TXT 7 2 86400 20210401000000
20210311000000 18644 oscardegroot.nl. rQr5aZWPoDZub9Tm8Z
gnBXfwoJjJ54FyjlUPqQy+h3/PV5Yp/rlBaU+k
jgNnxN6ovnG6KV5b9994JTZpQRpdguv4MayDK9lQbd8NeO990FU6mXD4
V7Klo6vILRDNBMcTcaeiS49mWq/vyxIRaOnXs  s26bfvjfh6BLovzMPPC Avc=
oscardegroot.nl.        300     IN      RRSIG   DNSKEY 7 2 300
```

```
20210401000000 20210311000000 55374 oscardegroot.nl. JNRayjaaztppv35i+
uHbY587OTwMp4EW9ShHAJB9avz69pCXWAI69NFv
3O42TPId1vujND7RuDWiGKAn6vVXBzSe27bKcWbXGKGulQT24qsZKgNR
XVzjeOGxGD7bkhqx6VkMoy0qQLANjf3I2nyU  TziW1BGuvFiFXM53K8iC
ic43oP+wo/oopyy2HHAji1DBm9Y1CARA8Bm0YxVpXoJAF5M24kx5JtzF
DNImag+4U02LM96PqNFtgntXRGNbejOjjA1XQ75zJyyHhUgRiK1G7aL  0
B/As0SRzFXIUftbAdtYaTD60rc1OFEAjcfdem6aPckwqDcynR7TQJUWa huWgcA==
oscardegroot.nl.        300     IN      RRSIG   NSEC3PARAM 7 2 300
20210401000000 20210311000000 18644 oscardegroot.nl. acpYiIwzeUyrL
AsXeTYejnwOmFaDzW6ArA+OZUMbUZrQB9N/Mb5TB03I
8tUSa3wowD/noOepnAbE3A0Q+/gfsDNxZ4wuYmaPRPQ96OD9GJSJbhcS
5Bbd+QX0UOMKvRyEAQWPmbyXcOyLxx6a  3xgIjboeecAfb3oFZiPUdHT+ RyM=
```

DNS Reverse Look-up

To perform a DNS reverse look up using the ip-address using dig -x as shown below. For example, if you just have an external ip-address and would like to know the website that belongs to it, do the following.

```
# dig -x 209.132.183.81 +short
www.redhat.com.
```

or

```
nslookup 209.132.183.81
81.183.132.209.in-addr.arpa name = www.redhat.com.
```

Monitor DNS requests

```
script -q -c "sudo tcpdump -l port 53 2>/dev/null | grep --line-buffered ' A? ' | cut -d' ' -f8" | tee dns.log
```