howto, dig, diagnose, dns, rdns, spf

How to Diagnose DNS and RDNS with DIG

Sources:

- IBM NS1 - Decoding DIG Output
- serverfault - How to determine which DNS server has the authority to set rDNS (PTR records)?
- linux.die.net - dig(1) - Linux man page

DIG Basic Usage

```
dig -t ANY @a.ns14.net nanoscopic.de
```

- dig: calling the command dig
- -t ANY: specifying the query type
- @a.ns14.net: specifying the DNS server to query
- nanoscopic.de: the name to query for

Find Authoritative DNS Server

```
dig -t SOA nanoscopic.de
```

```
; <<>> DiG 9.18.26 <<>> -t SOA nanoscopic.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22729
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;nanoscopic.de.                 IN      SOA

;; ANSWER SECTION:
nanoscopic.de.          3600    IN      SOA     a.ns14.net. domains.wiretrip.de. 2024031401 43200 7200
1209600 3600

;; Query time: 26 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon May 06 17:50:07 CEST 2024
;; MSG SIZE  rcvd: 105
```

The **authoritative DNS server** for **nanoscopic.de** is **a.ns14.net**.

Query the authoritative DNS server (or a specific DNS server) for current data

To get current DNS data, use @<HOSTNAME_OF_AUTHORITATIVE_DNS_SERVER>.

IPv4

```
dig @a.ns14.net -t A nanoscopic.de
```

```
; <<>> DiG 9.18.26 <<>> @a.ns14.net -t A nanoscopic.de
; (2 servers found)
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32234
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nanoscopic.de.                 IN      A

;; ANSWER SECTION:
nanoscopic.de.          3600    IN      A       159.69.16.204

;; Query time: 16 msec
;; SERVER: 62.116.159.231#53(a.ns14.net) (UDP)
;; WHEN: Mon May 06 17:56:47 CEST 2024
;; MSG SIZE  rcvd: 58
```

IPv6

```
dig @a.ns14.net -t AAAA nanoscopic.de
```

```
; <<>> DiG 9.18.26 <<>> @a.ns14.net -t AAAA nanoscopic.de
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21488
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;nanoscopic.de.                 IN      AAAA

;; ANSWER SECTION:
nanoscopic.de.          3600    IN      AAAA    2a01:4f8:c0c:fa5c::1

;; Query time: 16 msec
;; SERVER: 62.116.159.231#53(a.ns14.net) (UDP)
;; WHEN: Mon May 06 17:58:31 CEST 2024
;; MSG SIZE  rcvd: 70
```

Determine the DNS Server holding a RDNS (PTR) Record

Works for IPv4 and IPV6 addresses

```
IPADDR="2a01:4f8:c0c:fa5c::1"; IPADDR="$( dig -x $IPADDR | egrep '^;.*PTR$' | cut -c 2- | awk '{print
$1}' )"; dig in ns $IPADDR;
```

```
; <<>> DiG 9.18.26 <<>> in ns 1.0.0.0.0.0.0.0.0.0.0.0.0.0.c.5.a.f.c.0.c.0.8.f.4.0.1.0.a.2.ip6.arpa.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50675
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;1.0.0.0.0.0.0.0.0.0.0.0.0.0.c.5.a.f.c.0.c.0.8.f.4.0.1.0.a.2.ip6.arpa. IN NS
```

```
;; AUTHORITY SECTION:
c.5.a.f.c.0.c.0.8.f.4.0.1.0.a.2.ip6.arpa. 3540 IN SOA ns1.your-server.de. dns.hetzner.com. 2020062010
14400 1800 604800 86400

;; Query time: 3 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Mon May 06 19:49:14 CEST 2024
;; MSG SIZE  rcvd: 170
```

The **DNS server**, serving the **PTR record** for **2a01:4f8:c0c:fa5c::1** (nanoscopic.de), is **ns1.your-server.de**.

For one of my Telekom addresses (2003:a:b1c:f420:be24:11ff:feb3:a94f), I can use:

```
IPADDR="2003:a:b1c:f420:be24:11ff:feb3:0"; IPADDR="$( dig -x $IPADDR | egrep '^;.*PTR$' | cut -c 2- |
awk '{print $1}' )"; dig in ns $IPADDR;
```

```
; <<>> DiG 9.18.26 <<>> in ns 0.0.0.0.3.b.e.f.f.f.1.1.4.2.e.b.0.2.4.f.c.1.b.0.a.0.0.0.3.0.0.2.ip6.arpa.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 21795
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;0.0.0.0.3.b.e.f.f.f.1.1.4.2.e.b.0.2.4.f.c.1.b.0.a.0.0.0.3.0.0.2.ip6.arpa. IN NS

;; AUTHORITY SECTION:
c.1.b.0.a.0.0.0.3.0.0.2.ip6.arpa. 3600 IN SOA   pns.dtag.de. dns.telekom.de. 2024050700 10800 3600
2419200 172800

;; Query time: 23 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Tue May 07 14:41:33 CEST 2024
;; MSG SIZE  rcvd: 160
```

The **DNS server**, serving the **PTR record** for **2003:a:b1c:f420:be24:11ff:feb3:a94f** (mail.ignion.de), is **pns.dtag.de.

How to interpret DIG output

~~DISCUSSION~~