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

If no type is specified, dig queries for an “A”-record. If not told to query a specific name server, dig will try each of the servers listed in the systems /etc/resolv.conf. Have a look at the manual page for more options.

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="80.147.157.18"; IPADDR="$( dig -x $IPADDR | egrep '^;.*PTR$' | cut -c 2- | awk '{print $1}' )";
dig in ns $IPADDR;
```

```
; <<>> DiG 9.18.26 <<>> in ns 18.157.147.80.in-addr.arpa.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29955
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1424
;; QUESTION SECTION:
;18.157.147.80.in-addr.arpa.    IN      NS

;; AUTHORITY SECTION:
157.147.80.in-addr.arpa. 3600   IN      SOA     pns.dtag.de. dns.telekom.de. 2024050700 86400 7200
3600000 3600

;; Query time: 39 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Tue May 07 14:55:38 CEST 2024
;; MSG SIZE  rcvd: 114
```

The **DNS server**, serving the **PTR record** for **80.147.157.18** (nanoscopic.de), is **pns.dtag.de**.

For IPv6 addresses, e.g. 2003:a:b1c:f420:be24:11ff:feb3:a94f, replace the last four hexadecimal digits with a zero: 2003:a:b1c:f420:be24:11ff:feb3:0.

Query the RDNS server of a Network Segment for current PTR data

To get current RDNS data, use @<HOSTNAME_OF_RDNS_SERVER>.

```
dig @pns.dtag.de -x 2003:a:b1c:f420:be24:11ff:feb3:a94f
```

```
; <<>> DiG 9.18.26 <<>> @pns.dtag.de -x 2003:a:b1c:f420:be24:11ff:feb3:a94f
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57046
;; 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
; COOKIE: 0df13100e908f31301000000663a234b9c80aa6cf1625885 (good)
;; QUESTION SECTION:
;f.4.9.a.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 PTR

;; ANSWER SECTION:
f.4.9.a.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. 86400 IN PTR mail.ignion.de.

;; Query time: 9 msec
;; SERVER: 2003:40:8000::100#53(pns.dtag.de) (UDP)
;; WHEN: Tue May 07 14:49:15 CEST 2024
;; MSG SIZE  rcvd: 157
```

How to inspect a SPF Record

Determine the authoritative DNS server

```
dig -t SOA mx.wiretrip.de
```

```
; <<>> DiG 9.18.26 <<>> -t soa wiretrip.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58644
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

```
;; ANSWER SECTION:
wiretrip.de.            43200   IN      SOA     a.ns14.net. domains.wiretrip.de. 2024050305 43200 14400
604800 43200

;; Query time: 139 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Tue May 07 15:08:24 CEST 2024
;; MSG SIZE  rcvd: 94
```

Then query the authoritative DNS server for current data:

```
dig @a.ns14.net -t TXT wiretrip.de
```

```
; <<>> DiG 9.18.26 <<>> @a.ns14.net -t TXT wiretrip.de
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48047
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
wiretrip.de.            43200   IN      TXT     "v=spf1 ip4:159.69.16.204 ip4:80.147.157.18
ip6:2a01:4f8:c0c:fa5c::1 ip6:2003:a:b1c:f420:f0ce:b1ff:fe08:3162 -all"
wiretrip.de.            43200   IN      TXT     "YweIdum3Gyt2qOzYU44Q"

;; Query time: 16 msec
;; SERVER: 62.116.159.231#53(a.ns14.net) (UDP)
;; WHEN: Tue May 07 15:09:38 CEST 2024
;; MSG SIZE  rcvd: 198
```

```
dig @a.ns14.net -t TXT wiretrip.de | grep spf
```

```
wiretrip.de.            43200   IN      TXT     "v=spf1 ip4:159.69.16.204 ip4:80.147.157.18
ip6:2a01:4f8:c0c:fa5c::1 ip6:2003:a:b1c:f420:f0ce:b1ff:fe08:3162 -all"
```

How to interpret DIG output

~~DISCUSSION~~