NAME

drill - get (debug) information out of DNS(SEC)

SYNOPSIS

drill [*OPTIONS*] *name* [*@server*] [*type*] [*class*]

DESCRIPTION

drill is a tool to designed to get all sorts of information out of the DNS. It is specificly designed to be used with DNSSEC.

The name **drill** is a pun on **dig**. With **drill** you should be able get even more information than with **dig**.

If no arguments are given class defaults to ’IN’ and type to ’A’. The server(s) specified in /etc/resolv.conf are used to query against.

name Ask for this name.

@server Send to query to this server. If not specified use the nameservers from */etc/resolv.conf*.

type Ask for this RR type. If type is not given on the command line it defaults to ’A’. Except when doing a reverse lookup when it defaults to ’PTR’.

class Use this class when querying.

SAMPLE USAGE

drill mx miek.nl Show the MX records of the domain miek.nl

drill -S jelte.nlnetlabs.nl

Chase any signatures in the jelte.nlnetlab.nl domain. This option is only available when ldns has been compiled with openssl-support.

drill -TD www.example.com

Do a DNSSEC (-D) trace (-T) from the rootservers down to www.example.com. This option only works when ldns has been compiled with openssl support.

drill -s dnskey jelte.nlnetlabs.nl

Show the DNSKEY record(s) for jelte.nlnetlabs.nl. For each found DNSKEY record also print the DS record.

OPTIONS

-D Enable DNSSEC in the query. When querying for DNSSEC types (DNSKEY, RRSIG, DS and NSEC) this is *not* automatically enabled.

-T Trace *name* from the root down. When using this option the @server arguments is not used.

-S Chase the signature(s) of ’name’ to a known key or as high up in the tree as possible.

-I *IPv4 or IPv6 address*

Source address to query from. The source address has to be present on an interface of the host running drill.

-V *level*

Be more verbose. Set level to 5 to see the actual query that is sent.

-Q Quiet mode, this overrules -V.

-f *file*

Read the query from a file. The query must be dumped with -w.

-i *file*

read the answer from the file instead from the network. This aids in debugging and can be used to check if a query on disk is valid. If the file contains binary data it is assumed to be a query in network order.

-w *file*
Write an answer packet to file.

-q *file*
Write the query packet to file.

-v Show drill’s version.

-h Show a short help message.

QUERY OPTIONS

-4 Stay on ip4. Only send queries to ip4 enabled nameservers.

-6 Stay on ip6. Only send queries to ip6 enabled nameservers.

-a Use the resolver structure’s fallback mechanism if the answer is truncated (TC=1). If a truncated packet is received and this option is set, drill will first send a new query with EDNS0 buffer size 4096.

If the EDNS0 buffer size was already set to 512+ bytes, or the above retry also results in a truncated answer, the resolver structure will fall back to TCP.

-b *size*
Use size as the buffer size in the EDNS0 pseudo RR.

-c *file*
Use file instead of /etc/resolv.conf for nameserver configuration.

-d *domain*
When tracing (-T), start from this domain instead of the root.

-t Use TCP/IP when querying a server

-k *keyfile*

Use this file to read a (trusted) key from. When this options is given **drill** tries to validate the current answer with this key. No chasing is done. When **drill** is doing a secure trace, this key will be used as trust anchor. Can contain a DNSKEY or a DS record.

Alternatively, when DNSSEC enabled tracing (**-TD**) or signature chasing (**-S**), if **-k** is not specified, and a default trust anchor (/etc/unbound/root.key) exists and contains a valid DNSKEY or DS record, it will be used as the trust anchor.

-o *mnemonic*

Use this option to set or unset specific header bits. A bit is set by using the bit mnemonic in CAPITAL letters. A bit is unset when the mnemonic is given in lowercase. The following mnemonics are understood by **drill**:

QR, qr: set, unset QueRy (default: on)
AA, aa: set, unset Authoritative Answer (default: off)
TC, tc: set, unset TrunCated (default: off)
RD, rd: set, unset Recursion Desired (default: on)
CD, cd: set, unset Checking Disabled (default: off)
RA, ra: set, unset Recursion Available (default: off)
AD, ad: set, unset Authenticated Data (default: off)

Thus: **-o CD**, will enable Checking Disabled, which instructs the cache to not validate the answers it gives out.

-p *port*

Use this port instead of the default of 53.

-r *file*

When tracing (-T), use file as a root servers hint file.

-s When encountering a DNSKEY print the equivalent DS also.

-u Use UDP when querying a server. This is the default.

-w *file*

write the answer to a file. The file will contain a hexadecimal dump of the query. This can be used in conjunction with -f.

-x Do a reverse lookup. The type argument is not used, it is preset to PTR.

-y *<name:key[:algo]>*

specify named base64 tsig key, and optional an algorithm (defaults to hmac-md5.sig-alg.reg.int)

-z don’t randomize the nameserver list before sending queries.

EXIT STATUS

The exit status is 0 if the looked up answer is secure and trusted, or insecure. The exit status is not 0 if the looked up answer is untrusted or bogus, or an error occurred while performing the lookup.

FILES

/etc/unbound/root.key

The file from which trusted keys are loaded when no **-k** option is given.

SEE ALSO

unbound-anchor(8)

AUTHOR

Jelte Jansen and Miek Gieben. Both of NLnet Labs.

REPORTING BUGS

Report bugs to <ldns-team@nlnetlabs.nl>.

BUGS

COPYRIGHT

SEE ALSO

dig(1), *RFC403{3,4,5}*.