Knot DNS Documentation

Release 2.3.3

Jan 19, 2017

CHAPTER

ONE

INTRODUCTION

1.1 What is Knot DNS

Knot DNS is a high-performance open-source DNS server. It implements only the authoritative domain name service. Knot DNS is best suited for use on TLD domains but it can reliably serve any other zones as well.

Knot DNS benefits from its multi-threaded and mostly lock-free implementation which allows it to scale well on SMP systems and operate non-stop even when adding or removing zones.

1.2 Knot DNS features

DNS features:

- IN class and partially CH class
- TCP/UDP protocols
- AXFR, IXFR – master, slave
- TSIG
- EDNS0
- DNSSEC, including NSEC3
- NSID
- Dynamic updates
- Response Rate Limiting
- RR types A, NS, CNAME, SOA, PTR, HINFO, MINFO, MX, TXT, RP, AFSDB, RT, KEY, AAAA, LOC, SRV, NAPTR, KX, CERT, DNAME, APL, DS, SSHFP, IPSECKEY, RRSIG, NSEC, DNSKEY, DHCID, NSEC3, NSEC3PARAM, TLSA, CDS, CDNSKEY, SPF, NID, L32, L64, LP, EUI48, EUI64, URI, CAA and Unknown

Server features:

- Adding/removing/editing zones on-the-fly
- Reconfiguring server instance on-the-fly
- Dynamic configuration
- IPv4 and IPv6 support
- Semantic checks of zones
- DDNS support
- Persistent zone timers
- Automatic DNSSEC signing

- PKCS #11 interface
- Forward and reverse records synthesis

For more info and downloads see www.knot-dns.cz.

Git repository: git://git.nic.cz/knot-dns.git

Knot DNS issue tracker: gitlab.labs.nic.cz/labs/knot/issues

Knot DNS users mailing list: knot-dns-users@lists.nic.cz

1.3 License

Knot DNS is licensed under the GNU General Public License version 3 or (at your option) any later version. The full text of the license is available in the `COPYING` file distributed with source code.

CHAPTER

TWO

REQUIREMENTS

2.1 Hardware

Knot DNS requirements are not very demanding for typical installations, and a commodity server or a virtual solution will be sufficient in most cases.

However, please note that there are some scenarios that will require administrator's attention and a testing of exact requirements before deploying Knot DNS to a production environment. These cases include deployment for a large number of zones (DNS hosting), large number of records in one or more zones (TLD) or large number of requests.

2.1.1 CPU requirements

Knot DNS scales with processing power and also with the number of available cores/CPUs.

There is no lower bound on the CPU requirements, but it should support memory barriers and CAS (i586 and newer).

2.1.2 Memory requirements

Knot DNS implementation focuses on performance and thus can be quite memory demanding. The rough estimate for memory requirements is 3 times the size of the zone in text format. Again this is only an estimate and you are advised to do your own measurements before deploying Knot DNS to production.

Note: To ensure uninterrupted serving of the zone, Knot DNS employs the Read-Copy-Update mechanism instead of locking and thus requires twice the amount of memory for the duration of incoming transfers.

2.2 Operating system

Knot DNS itself is written in a portable way, but it depends on several libraries. Namely userspace-rcu, which could be a constraint when it comes to the operating system support. Knot DNS can be compiled and run on most UNIX-like systems, such as Linux, *BSD, and OS X.

CHAPTER

THREE

INSTALLATION

3.1 Required build environment

GCC at least 4.1 is strictly required for atomic built-ins, but the latest available version is recommended. Another requirement is `_GNU_SOURCE` support, otherwise it adapts to the compiler available features.

LLVM clang compiler can be used as well. However, the compilation with enabled optimizations will take a long time, unless the `--disable-fastparser` configure option is given.

Knot DNS build system relies on these standard tools:

- make
- libtool
- autoconf >= 2.65

3.2 Required libraries

Knot DNS requires few libraries to be compiled:

- GnuTLS, at least 3.3
- Jansson, at least 2.3
- Userspace RCU, at least 0.5.4
- libedit
- lmdb (included)
- libcap-ng, at least 0.6.4 (optional)
- libidn (optional)
- libsystemd (optional)
- protobuf-c and fstrm (optional)

The LMDB library is required. It is included with the Knot DNS source code, however linking with the system library is preferred.

If the libcap-ng library is available, Knot DNS will take advantage of the POSIX 1003.1e *capabilites(7)* by sandboxing the exposed threads. Most rights are stripped from the exposed threads for security reasons.

The libidn library is a prerequisite for IDNA2003 (International Domain Names) support in Knot DNS utilities.

If the libsystemd library is available, the server will use systemd's startup notifications mechanism and journald for logging.

If the protobuf-c and fstrm libraries are available, the support for logging in Dnstap format will be included.

3.3 Installation from source code

You can find the source code for the latest release on www.knot-dns.cz. Alternatively, you can fetch the whole project from the git repository git://git.nic.cz/knot-dns.git.

After obtaining the source code, the compilation and installation is a quite straightforward process using autotools.

3.3.1 Configuring and generating Makefiles

If compiling from the git source, you need to bootstrap the `./configure` file first:

```
$ autoreconf -i -f
```

In most cases, you can just run configure without any options:

```
$ ./configure
```

For all available configure options run:

```
$ ./configure --help
```

3.3.2 Compilation

After running `./configure` you can compile Knot DNS by running `make` command, which will produce binaries and other related files:

```
$ make
```

3.3.3 Installation

When you have finished building Knot DNS, it's time to install the binaries and configuration files into the operation system hierarchy. You can do so by executing:

```
$ make install
```

When installing as a non-root user, you might have to gain elevated privileges by switching to root user, e.g. `sudo make install` or `su -c 'make install'`.

3.4 OS specific installation

Knot DNS might already be available in the destination operating system repository.

3.4.1 Debian Linux

Knot DNS is already available from Debian 7 (Wheezy) upwards. In addition to the official packages we also provide custom repository, which can be used by adding:

```
deb     http://deb.knot-dns.cz/debian/ <codename> main
deb-src http://deb.knot-dns.cz/debian/ <codename> main
```

to your `/etc/apt/sources.list` or into separate file in `/etc/apt/sources.list.d/`.

As an example, for Debian 8 (Jessie) the Knot DNS packages can be added by executing following command as the root user:

```
# cat >/etc/apt/sources.list.d/knot.list <<EOF
deb     http://deb.knot-dns.cz/debian/ jessie main
deb-src http://deb.knot-dns.cz/debian/ jessie main
EOF
# apt-get update
# apt-get install knot
```

3.4.2 Ubuntu Linux

Prepackaged version of Knot DNS can be found in Ubuntu from version 12.10 (Quantal Quetzal). In addition to the package included in the main archive, we provide Personal Package Archive (PPA) as an option in order to upgrade to the last stable version of Knot DNS or to install it on older versions of Ubuntu Linux.

Adding official PPA repository for Knot DNS

To start installing and using software from a Personal Package Archive, you first need to tell Ubuntu where to find the PPA:

```
$ sudo add-apt-repository ppa:cz.nic-labs/knot-dns
$ sudo apt-get update
$ sudo apt-get install knot
```

Running this sequence of commands will ensure that you will install Knot DNS on your system and keep it up-to-date in the future, when new versions are released.

3.4.3 Fedora Linux

The RPM packages for Knot DNS are available in official Fedora repositories since Fedora 18 (Spherical Cow). Search for the `knot` package in your package manager. To install the package using Yum, run the following command as the root user:

```
# yum install knot
```

3.4.4 Arch Linux

Knot DNS is available in the official package repository (AUR). To install the package, run:

```
# pacman -S knot
```

3.4.5 Gentoo Linux

Knot DNS is also available in the Gentoo package repository. However, you will probably need to unmask the package prior to starting the installation:

```
# emerge -a knot
```

3.4.6 FreeBSD

Knot DNS is in ports tree under `dns/knot`. To install the port, run:

```
# cd /usr/ports/dns/knot
# make install
```

CHAPTER

FOUR

CONFIGURATION

4.1 Simple configuration

The following example presents a simple configuration file which can be used as a base for your Knot DNS setup:

```
# Example of a very simple Knot DNS configuration.

server:
    listen: 0.0.0.0@53
    listen: ::@53

zone:
  - domain: example.com
    storage: /var/lib/knot/zones/
    file: example.com.zone

log:
  - target: syslog
    any: info
```

Now let's walk through this configuration step by step:

- The *listen* statement in the *server section* defines where the server will listen for incoming connections. We have defined the server to listen on all available IPv4 and IPv6 addresses, all on port 53.
- The *zone section* defines the zones that the server will serve. In this case, we defined one zone named *example.com* which is stored in the zone file `/var/lib/knot/zones/example.com.zone`.
- The *log section* defines the log facilities for the server. In this example, we told Knot DNS to send its log messages with the severity `info` or more serious to the syslog.

For detailed description of all configuration items see *Configuration Reference*.

4.2 Zone templates

A zone template allows a single zone configuration to be shared among several zones. The `default` template identifier is reserved for the default template:

```
template:
  - id: default
    storage: /var/lib/knot/master
    semantic-checks: on

  - id: signed
    storage: /var/lib/knot/signed
    dnssec-signing: on
    semantic-checks: on
    master: [master1, master2]
```

```
  - id: slave
    storage: /var/lib/knot/slave

zone:
  - domain: example1.com     # Uses default template

  - domain: example2.com     # Uses default template
    semantic-checks: off     # Override default settings

  - domain: example.cz
    template: signed
    master: master3          # Override masters to just master3

  - domain: example1.eu
    template: slave
    master: master1

  - domain: example2.eu
    template: slave
    master: master2
```

Note: Each template option can be explicitly overridden in zone-specific configuration.

4.3 Access control list (ACL)

An ACL list specifies which remotes are allowed to send the server a specific request. A remote can be a single IP address or a network subnet. Also a TSIG key can be assigned (see *keymgr* how to generate a TSIG key):

```
key:
  - id: key1
    algorithm: hmac-md5
    secret: Wg==

acl:
  - id: address_rule
    address: [2001:db8::1, 192.168.2.0/24] # Allowed IP address list
    action: [transfer, update]  # Allow zone transfers and updates

  - id: deny_rule              # Negative match rule
    address: 192.168.2.100
    action: transfer
    deny: on                   # The request is denied

  - id: key_rule
    key: key1                  # Access based just on TSIG key
    action: transfer
```

These rules can then be referenced from a zone *acl*:

```
zone:
  - domain: example.com
    acl: [address_rule, deny_rule, key_rule]
```

4.4 Slave zone

Knot DNS doesn't strictly differ between master and slave zones. The only requirement is to have a *master* statement set for the given zone. Also note that you need to explicitly allow incoming zone changed notifications via `notify` *action* through zone's *acl* list, otherwise the update will be rejected by the server. If the zone file doesn't exist it will be bootstrapped over AXFR:

```
remote:
  - id: master
    address: 192.168.1.1@53

acl:
  - id: notify_from_master
    address: 192.168.1.1
    action: notify

zone:
  - domain: example.com
    storage: /var/lib/knot/zones/
    # file: example.com.zone   # Default value
    master: master
    acl: notify_from_master
```

Note that the *master* option accepts a list of multiple remotes. The remotes should be listed according to their preference. The first remote has the highest preference, the other remotes are used for failover. When the server receives a zone update notification from a listed remote, that remote will be the most preferred one for the subsequent transfer.

To use TSIG for transfers and notification messages authentication, configure a TSIG key and assign the key both to the remote and the ACL rule. Notice that the *remote* and *ACL* definitions are independent:

```
key:
  - id: slave1_key
    algorithm: hmac-md5
    secret: Wg==

remote:
  - id: master
    address: 192.168.1.1@53
    key: slave1_key

acl:
  - id: notify_from_master
    address: 192.168.1.1
    key: slave1_key
    action: notify
```

Note: When transferring a lot of zones, the server may easily get into a state when all available ports are in the TIME_WAIT state, thus the transfers seize until the operating system closes the ports for good. There are several ways to work around this:

- Allow reusing of ports in TIME_WAIT (sysctl -w net.ipv4.tcp_tw_reuse=1)
- Shorten TIME_WAIT timeout (tcp_fin_timeout)
- Increase available local port count

4.5 Master zone

An ACL with the `transfer` action must be configured to allow outgoing zone transfers. An ACL rule consists of a single address or a network subnet:

```
remote:
  - id: slave1
    address: 192.168.2.1@53

acl:
  - id: slave1_acl
    address: 192.168.2.1
    action: transfer

  - id: others_acl
    address: 192.168.3.0/24
    action: transfer

zone:
  - domain: example.com
    storage: /var/lib/knot/zones/
    file: example.com.zone
    notify: slave1
    acl: [slave1_acl, others_acl]
```

Optionally, a TSIG key can be specified:

```
key:
  - id: slave1_key
    algorithm: hmac-md5
    secret: Wg==

remote:
  - id: slave1
    address: 192.168.2.1@53
    key: slave1_key

acl:
  - id: slave1_acl
    address: 192.168.2.1
    key: slave1_key
    action: transfer

  - id: others_acl
    address: 192.168.3.0/24
    action: transfer
```

4.6 Dynamic updates

Dynamic updates for the zone are allowed via proper ACL rule with the `update` action. If the zone is configured as a slave and a DNS update message is accepted, the server forwards the message to its primary master. The master's response is then forwarded back to the originator.

However, if the zone is configured as a master, the update is accepted and processed:

```
acl:
  - id: update_acl
    address: 192.168.3.0/24
    action: update
```

```
zone:
  - domain: example.com
    file: example.com.zone
    acl: update_acl
```

4.7 Response rate limiting

Response rate limiting (RRL) is a method to combat DNS reflection amplification attacks. These attacks rely on the fact that source address of a UDP query can be forged, and without a worldwide deployment of BCP38, such a forgery cannot be prevented. An attacker can use a DNS server (or multiple servers) as an amplification source and can flood a victim with a large number of unsolicited DNS responses.

The RRL lowers the amplification factor of these attacks by sending some of the responses as truncated or by dropping them altogether.

You can enable RRL by setting the *rate-limit* option in the *server section*. The option controls how many responses per second are permitted for each flow. Responses exceeding this rate are limited. The option *rate-limit-slip* then configures how many limited responses are sent as truncated (slip) instead of being dropped.

```
server:
    rate-limit: 200     # Allow 200 resp/s for each flow
    rate-limit-slip: 2  # Every other response slips
```

4.8 Automatic DNSSEC signing

Knot DNS supports automatic DNSSEC signing for static zones. The signing can operate in two modes:

1. *Automatic key management*. In this mode, the server maintains signing keys. New keys are generated according to assigned policy and are rolled automatically in a safe manner. No zone operator intervention is necessary.
2. *Manual key management*. In this mode, the server maintains zone signatures only. The signatures are kept up-to-date and signing keys are rolled according to timing parameters assigned to the keys. The keys must be generated and timing parameters must be assigned by the zone operator.

The DNSSEC signing process maintains some metadata which is stored in the KASP (Key And Signature Policy) database. This database is simply a directory in the file-system containing files in the JSON format.

Warning: Make sure to set the KASP database permissions correctly. For manual key management, the database must be *readable* by the server process. For automatic key management, it must be *writeable*. If no HSM is used, the database also contains private key material – don't set the permissions too week.

4.8.1 Automatic key management

For automatic key management, a signing policy has to be configured and assigned to the zone. The policy specifies how the zone is signed (i.e. signing algorithm, key size, key lifetime, signature lifetime, etc.). The policy can be configured in the *policy section*, or a `default` policy with the default parameters can be used.

A minimal zone configuration may look as follows:

```
zone:
  - domain: myzone.test
    dnssec-signing: on
    dnssec-policy: default
```

With custom signing policy, the policy section will be added:

```
policy:
  - id: rsa
    algorithm: RSASHA256
    ksk-size: 2048
    zsk-size: 1024

zone:
  - domain: myzone.test
    dnssec-signing: on
    dnssec-policy: rsa
```

After configuring the server, reload the changes:

```
$ knotc reload
```

The server will generate initial signing keys and sign the zone properly. Check the server logs to see whether everything went well.

Warning: This guide assumes that the zone *myzone.test* was not signed prior to enabling the automatic key management. If the zone was already signed, all existing keys must be imported using `keymgr zone key import` command before enabling the automatic signing. Also the algorithm in the policy must match the algorithm of all imported keys. Otherwise the zone will be resigned at all.

4.8.2 Manual key management

For automatic DNSSEC signing with manual key management, a signing policy with manual key management flag has to be set:

```
policy:
  - id: manual
    manual: on

zone:
  - domain: myzone.test
    dnssec-signing: on
    dnssec-policy: manual
```

To generate signing keys, use the *keymgr* utility. Let's use the Single-Type Signing scheme with two algorithms, which is a scheme currently not supported by the automatic key management. Run:

```
$ keymgr zone key generate myzone.test algorithm RSASHA256 size 1024
$ keymgr zone key generate myzone.test algorithm ECDSAP256SHA256 size 256
```

And reload the server. The zone will be signed.

To perform a manual rollover of a key, the timing parameters of the key need to be set. Let's roll the RSA key. Generate a new RSA key, but do not activate it yet:

```
$ keymgr zone key generate myzone.test algorithm RSASHA256 size 1024 active +1d
```

Take the key ID (or key tag) of the old RSA key and disable it the same time the new key gets activated:

```
$ keymgr zone key set myzone.test <old_key_id> retire +1d remove +1d
```

Reload the server again. The new key will be published (i.e. the DNSKEY record will be added into the zone). Do not forget to update the DS record in the parent zone to include a reference to the new RSA key. This must happen in one day (in this case) including a delay required to propagate the new DS to caches.

Note that as the `+1d` time specification is computed from the current time, the key replacement will not happen at once. First, a new key will be activated. A few moments later, the old key will be deactivated and removed. You can use exact time specification to make these two actions happen in one go.

4.8.3 Zone signing

The signing process consists of the following steps:

1. Processing KASP database events. (e.g. performing a step of a rollover).
2. Fixing the NSEC or NSEC3 chain.
3. Updating the DNSKEY records. The whole DNSKEY set in zone apex is replaced by the keys from the KASP database. Note that keys added into the zone file manually will be removed. To add an extra DNSKEY record into the set, the key must be imported into the KASP database (possibly deactivated).
4. Removing expired signatures, invalid signatures, signatures expiring in a short time, and signatures issued by an unknown key.
5. Creating missing signatures. Unless the Single-Type Signing Scheme is used, DNSKEY records in a zone apex are signed by KSK keys and all other records are signed by ZSK keys.
6. Updating and resigning SOA record.

The signing is initiated on the following occasions:

- Start of the server
- Zone reload
- Reaching the signature refresh period
- Received DDNS update
- Forced zone resign via server control interface

On a forced zone resign, all signatures in the zone are dropped and recreated.

The `knotc zone-status` command can be used to see when the next scheduled DNSSEC resign will happen.

4.8.4 Limitations

The current DNSSEC implementation in Knot DNS has some limitations. Most of the limitations will be hopefully removed in the near future.

- Automatic key management:
  - Only one DNSSEC algorithm can be used per zone.
  - Single-Type Signing scheme is not supported.
  - ZSK rollover always uses key pre-publish method (actually a feature).
  - KSK rollover is not implemented.
- Signing:
  - Signature expiration jitter is not implemented.
  - Signature expiration skew is not implemented.
- Utilities:
  - Legacy key import requires a private key.
  - Legacy key export is not implemented.
  - DS record export is not implemented.

CHAPTER

FIVE

QUERY MODULES

Knot DNS supports configurable query modules that can alter the way queries are processed. The concept is quite simple – each query requires a finite number of steps to be resolved. We call this set of steps a *query plan*, an abstraction that groups these steps into several stages.

- Before-query processing
- Answer, Authority, Additional records packet sections processing
- After-query processing

For example, processing an Internet-class query needs to find an answer. Then based on the previous state, it may also append an authority SOA or provide additional records. Each of these actions represents a 'processing step'. Now, if a query module is loaded for a zone, it is provided with an implicit query plan which can be extended by the module or even changed altogether.

A module is active if its name, which includes the `mod-` prefix, is assigned to the zone/template *module* option or to the *default* template *global-module* option if activating for all queries. If the module is configurable, a corresponding module section with an identifier must be created and then referenced in the form of `module_name/module_id`.

Note: Query modules are processed in the order they are specified in the zone/template configuration.

5.1 `dnstap` – dnstap-enabled query logging

A module for query and response logging based on dnstap library. You can capture either all or zone-specific queries and responses; usually you want to do the former. The configuration comprises only a *sink* path parameter, which can be either a file or a UNIX socket:

```
mod-dnstap:
  - id: capture_all
    sink: /tmp/capture.tap

template:
  - id: default
    global-module: mod-dnstap/capture_all
```

Note: To be able to use a Unix socket you need an external program to create it. Knot DNS connects to it as a client using the libfstrm library. It operates exactly like syslog. See here for more details.

Note: Dnstap log files can also be created or read using `kdig`.

5.2 synth-record – Automatic forward/reverse records

This module is able to synthesize either forward or reverse records for a given prefix and subnet.

Records are synthesized only if the query can't be satisfied from the zone. Both IPv4 and IPv6 are supported.

5.3 Automatic forward records

Example:

```
mod-synth-record:
  - id: test1
    type: forward
    prefix: dynamic-
    ttl: 400
    network: 2620:0:b61::/52

zone:
  - domain: test.
    file: test.zone # Must exist
    module: mod-synth-record/test1
```

Result:

```
$ kdig AAAA dynamic-2620-0000-0b61-0100-0000-0000-0000-0001.test.
...
;; QUESTION SECTION:
;; dynamic-2620-0000-0b61-0100-0000-0000-0000-0001.test. IN AAAA

;; ANSWER SECTION:
dynamic-2620-0000-0b61-0100-0000-0000-0000-0001.test. 400 IN AAAA 2620:0:b61:100::1
```

You can also have CNAME aliases to the dynamic records, which are going to be further resolved:

```
$ kdig AAAA alias.test.
...
;; QUESTION SECTION:
;; alias.test. IN AAAA

;; ANSWER SECTION:
alias.test. 3600 IN CNAME dynamic-2620-0000-0b61-0100-0000-0000-0000-0002.test.
dynamic-2620-0000-0b61-0100-0000-0000-0000-0002.test. 400 IN AAAA 2620:0:b61:100::2
```

5.4 Automatic reverse records

Example:

```
mod-synth-record:
  - id: test2
    type: reverse
    prefix: dynamic-
    origin: test
    ttl: 400
    network: 2620:0:b61::/52

zone:
  - domain: 1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa.
```

```
    file: 1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa.zone # Must exist
    module: mod-synth-record/test2
```

Result:

```
$ kdig -x 2620:0:b61::1
...
;; QUESTION SECTION:
;; 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.6.b.0.0.0.0.0.2.6.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.6.b.0.0.0.0.0.2.6.2.ip6.arpa. 400 IN␣
↪PTR
                                dynamic-2620-0000-0b61-0000-0000-0000-0000-0001.
↪test.
```

5.5 `dnsproxy` – Tiny DNS proxy

The module catches all unsatisfied queries and forwards them to the indicated server for resolution, i.e. a tiny DNS proxy. There are several uses of this feature:

- A substitute public-facing server in front of the real one
- Local zones (poor man's "views"), rest is forwarded to the public-facing server
- etc.

Note: The module does not alter the query/response as the resolver would, and the original transport protocol is kept as well.

The configuration is straightforward and just a single remote server is required:

```
remote:
  - id: hidden
    address: 10.0.1.1

mod-dnsproxy:
  - id: default
    remote: hidden

template:
  - id: default
    global-module: mod-dnsproxy/default

zone:
  - domain: local.zone
```

When clients query for anything in the `local.zone`, they will be responded to locally. The rest of the requests will be forwarded to the specified server (`10.0.1.1` in this case).

5.6 `rosedb` – Static resource records

The module provides a mean to override responses for certain queries before the record is searched in the available zones. The module comes with the `rosedb_tool` tool used to manipulate the database of static records. Neither the tool nor the module are enabled by default, recompile with the `--enable-rosedb` configuration flag to enable them.

For example, let's suppose we have a database of following records:

```
myrecord.com.      3600 IN A 127.0.0.1
www.myrecord.com.  3600 IN A 127.0.0.2
ipv6.myrecord.com. 3600 IN AAAA ::1
```

And we query the nameserver with the following:

```
$ kdig IN A myrecord.com
  ... returns NOERROR, 127.0.0.1
$ kdig IN A www.myrecord.com
  ... returns NOERROR, 127.0.0.2
$ kdig IN A stuff.myrecord.com
  ... returns NOERROR, 127.0.0.1
$ kdig IN AAAA myrecord.com
  ... returns NOERROR, NODATA
$ kdig IN AAAA ipv6.myrecord.com
  ... returns NOERROR, ::1
```

An entry in the database matches anything at the same or a lower domain level, i.e. 'myrecord.com' matches 'a.a.myrecord.com' as well. This can be utilized to create catch-all entries.

You can also add authority information for the entries, provided you create SOA + NS records for a name, like so:

```
myrecord.com.      3600 IN SOA master host 1 3600 60 3600 3600
myrecord.com.      3600 IN NS ns1.myrecord.com.
myrecord.com.      3600 IN NS ns2.myrecord.com.
ns1.myrecord.com. 3600 IN A 127.0.0.1
ns2.myrecord.com. 3600 IN A 127.0.0.2
```

In this case, the responses will:

1. Be authoritative (AA flag set)
2. Provide an authority section (SOA + NS)
3. Be NXDOMAIN if the name is found *(i.e. the 'IN AAAA myrecord.com' from the example)*, but not the RR type *(this is to allow the synthesis of negative responses)*

The SOA record applies only to the 'myrecord.com.', not to any other record (not even those of its subdomains). From this point of view, all records in the database are unrelated and not hierarchical. The idea is to provide subtree isolation for each entry.*

In addition, the module is able to log matching queries via remote syslog if you specify a syslog address endpoint and an optional string code.

Here is an example on how to use the module:

- Create the entries in the database:

```
$ mkdir /tmp/static_rrdb
$ # No logging
$ rosedb_tool /tmp/static_rrdb add myrecord.com. A 3600 "127.0.0.1" "-" "-"
$ # Logging as 'www_query' to Syslog at 10.0.0.1
$ rosedb_tool /tmp/static_rrdb add www.myrecord.com. A 3600 "127.0.0.1" \
                                                   "www_query" "10.0.0.1"
$ # Logging as 'ipv6_query' to Syslog at 10.0.0.1
$ rosedb_tool /tmp/static_rrdb add ipv6.myrecord.com. AAAA 3600 "::1" \
                                                 "ipv6_query" "10.0.0.1"
$ # Verify settings
$ rosedb_tool /tmp/static_rrdb list
www.myrecord.com.       A RDATA=10B     www_query       10.0.0.1
ipv6.myrecord.com.      AAAA RDATA=22B  ipv6_query      10.0.0.1
myrecord.com.           A RDATA=10B     -               -
```

Note: The database may be modified later on while the server is running.

- Configure the query module:

```
mod-rosedb:
  - id: default
    dbdir: /tmp/static_rrdb

template:
  - id: default
    global-module: mod-rosedb/default
```

The module accepts just one parameter – the path to the directory where the database will be stored.

- Start the server:

```
$ knotd -c knot.conf
```

- Verify the running instance:

```
$ kdig @127.0.0.1#6667 A myrecord.com
```

5.7 `online-sign` — Online DNSSEC signing

The module provides online DNSSEC signing. Instead of pre-computing the zone signatures when the zone is loaded into the server or instead of loading an externally signed zone, the signatures are computed on-the-fly during answering.

The main purpose of the module is to enable authenticated responses with zones which use other dynamic module (e.g., automatic reverse record synthesis) because these zones cannot be pre-signed. However, it can be also used as a simple signing solution for zones with low traffic and also as a protection against zone content enumeration (zone walking).

In order to minimize the number of computed signatures per query, the module produces a bit different responses from the responses that would be sent if the zone was pre-signed. Still, the responses should be perfectly valid for a DNSSEC validating resolver.

Differences from statically signed zones:

- The NSEC records are constructed as Minimally Covering NSEC Records (see Appendix A in **RFC 7129**). Therefore the generated domain names cover the complete domain name space in the zone's authority.
- NXDOMAIN responses are promoted to NODATA responses. The module proves that the query type does not exist rather than that the domain name does not exist.
- Domain names matching a wildcard are expanded. The module pretends and proves that the domain name exists rather than proving a presence of the wildcard.

Records synthesized by the module:

- DNSKEY record is synthesized in the zone apex and includes public key material for the active signing key.
- NSEC records are synthesized as needed.
- RRSIG records are synthesized for authoritative content of the zone.

How to use the online signing module:

- First add the zone into the server's KASP database and generate a key to be used for signing:

```
$ keymgr -d /path/to/kasp -l init
$ keymgr -d /path/to/kasp -l zone add example.com
$ keymgr -d /path/to/kasp -l zone key generate example.com algorithm␣
↪ecdsap256sha256 size 256
```

```
```

- Enable the module in server configuration and hook it to the zone:

```
zone:
  - domain: example.com
    module: mod-online-sign
    dnssec-signing: false
```

Note: This module is not configurable.

- Make sure the zone is not signed and also that the automatic signing is disabled. All is set, you are good to go. Reload (or start) the server:

```
$ knotc reload
```

The following example stacks the online signing with reverse record synthesis module:

```
mod-synth-record:
  - id: lan-forward
    type: forward
    prefix: ip-
    ttl: 1200
    network: 192.168.100.0/24

template:
  - id: default
    dnssec-signing: false

zone:
  - domain: corp.example.net
    module: [mod-synth-record/lan-forward, mod-online-sign]
```

Known issues:

- The delegations are not signed correctly.
- Some CNAME records are not signed correctly.

Limitations:

- Only a Single-Type Signing scheme is supported.
- Only one active signing key can be used.
- Key rollover is not possible.
- The NSEC records may differ for one domain name if queried for different types. This is an implementation shortcoming as the dynamic modules cooperate loosely. Possible synthesis of a type by other module cannot be predicted. This dissimilarity should not affect response validation, even with validators performing aggressive negative caching.
- The NSEC proofs will work well with other dynamic modules only if the modules synthesize only A and AAAA records. If synthesis of other type is required, please, report this information to Knot DNS developers.

5.8 `whoami` — whoami module

The module synthesizes an A or AAAA record containing the query source IP address, at the apex of the zone being served. It makes sure to allow Knot DNS to generate cacheable negative responses, and to allow fallback to extra records defined in the underlying zone file. The TTL of the synthesized record is copied from the TTL of the SOA record in the zone file.

Because a DNS query for type A or AAAA has nothing to do with whether the query occurs over IPv4 or IPv6, this module requires a special zone configuration to support both address families. For A queries, the underlying zone must have a set of nameservers that only have IPv4 addresses, and for AAAA queries, the underlying zone must have a set of nameservers that only have IPv6 addresses.

To enable this module, you need to add something like the following to the Knot DNS configuration file:

```
zone:
  - domain: whoami.domain.example
    file: "/path/to/whoami.domain.example"
    module: mod-whoami

zone:
  - domain: whoami6.domain.example
    file: "/path/to/whoami6.domain.example"
    module: mod-whoami
```

Note: This module is not configurable.

The whoami.domain.example zone file example:

```
$TTL 1

@       SOA     (
                        whoami.domain.example.          ; MNAME
                        hostmaster.domain.example.      ; RNAME
                        2016051300                      ; SERIAL
                        86400                           ; REFRESH
                        86400                           ; RETRY
                        86400                           ; EXPIRE
                        1                               ; MINIMUM
                )

$TTL 86400

@       NS      ns1.whoami.domain.example.
@       NS      ns2.whoami.domain.example.
@       NS      ns3.whoami.domain.example.
@       NS      ns4.whoami.domain.example.

ns1     A       198.51.100.53
ns2     A       192.0.2.53
ns3     A       203.0.113.53
ns4     A       198.19.123.53
```

The whoami6.domain.example zone file example:

```
$TTL 1

@       SOA     (
                        whoami6.domain.example.         ; MNAME
                        hostmaster.domain.example.      ; RNAME
                        2016051300                      ; SERIAL
                        86400                           ; REFRESH
                        86400                           ; RETRY
                        86400                           ; EXPIRE
                        1                               ; MINIMUM
                )

$TTL 86400
```

```
@       NS      ns1.whoami6.domain.example.
@       NS      ns2.whoami6.domain.example.
@       NS      ns3.whoami6.domain.example.
@       NS      ns4.whoami6.domain.example.

ns1     AAAA    2001:db8:100::53
ns2     AAAA    2001:db8:200::53
ns3     AAAA    2001:db8:300::53
ns4     AAAA    2001:db8:400::53
```

The parent domain would then delegate whoami.domain.example to ns[1-4].whoami.domain.example and whoami6.domain.example to ns[1-4].whoami6.domain.example, and include the corresponding A-only or AAAA-only glue records.

5.9 noudp — noudp module

The module sends empty truncated response to any UDP query. This is similar to a slipped answer in *response rate limiting*. TCP queries are not affected.

To enable this module globally, you need to add something like the following to the configuration file:

```
template:
  - id: default
    global-module: mod-noudp
```

Note: This module is not configurable.

CHAPTER

SIX

OPERATION

The Knot DNS server part `knotd` can run either in the foreground, or in the background using the `-d` option. When run in the foreground, it doesn't create a PID file. Other than that, there are no differences and you can control both the same way.

The tool `knotc` is designed as a user front-end, making it easier to control running server daemon. If you want to control the daemon directly, use `SIGINT` to quit the process or `SIGHUP` to reload the configuration.

If you pass neither configuration file (`-c` parameter) nor configuration database (`-C` parameter), the server will first attempt to use the default configuration database stored in `/var/lib/knot/confdb` or the default configuration file stored in `/etc/knot/knot.conf`. Both the default paths can be reconfigured with `--with-storage=path` or `--with-configdir=path` respectively.

Example of server start as a daemon:

```
$ knotd -d -c knot.conf
```

Example of server shutdown:

```
$ knotc -c knot.conf stop
```

For a complete list of actions refer to the program help (`-h` parameter) or to the corresponding manual page.

Also, the server needs to create *rundir* and *storage* directories in order to run properly.

6.1 Configuration database

In the case of a huge configuration file, the configuration can be stored in a binary database. Such a database can be simply initialized:

```
$ knotc conf-init
```

or preloaded from a file:

```
$ knotc conf-import input.conf
```

Also the configuration database can be exported into a textual file:

```
$ knotc conf-export output.conf
```

Warning: The import and export commands access the configuration database directly, without any interaction with the server. So it is strictly recommended to perform these operations when the server is not running.

6.2 Dynamic configuration

The configuration database can be accessed using the server control interface during the running server. To get the full power of the dynamic configuration, the server must be started with a specified configuration database location or with the default database initialized. Otherwise all the changes to the configuration will be temporary (until the server stop).

Note: The database can be *imported* in advance.

Most of the commands get an item name and value parameters. The item name is in the form of `section[identifier].name`. If the item is multivalued, more values can be specified as individual (command line) arguments. Beware of the possibility of pathname expansion by the shell. For this reason, slashed square brackets or quoted parameters is advisable.

To get the list of configuration sections or to get the list of section items:

```
$ knotc conf-list
$ knotc conf-list 'server'
```

To get the whole configuration or to get the whole configuration section or to get all section identifiers or to get a specific configuration item:

```
$ knotc conf-read
$ knotc conf-read 'remote'
$ knotc conf-read 'zone.domain'
$ knotc conf-read 'zone[example.com].master'
```

Warning: The following operations don't work on OpenBSD!

Modifying operations require an active configuration database transaction. Just one transaction can be active at a time. Such a transaction then can be aborted or committed. A semantic check is executed automatically before every commit:

```
$ knotc conf-begin
$ knotc conf-abort
$ knotc conf-commit
```

To set a configuration item value or to add more values or to add a new section identifier or to add a value to all identified sections:

```
$ knotc conf-set 'server.identity' 'Knot DNS'
$ knotc conf-set 'server.listen' '0.0.0.0@53' '::@53'
$ knotc conf-set 'zone[example.com]'
$ knotc conf-set 'zone.slave' 'slave2'
```

Note: Also the include operation can be performed. A non-absolute file location is relative to the server binary path, not to the control binary path!:

```
$ knotc conf-set 'include' '/tmp/new_zones.conf'
```

To unset the whole configuration or to unset the whole configuration section or to unset an identified section or to unset an item or to unset a specific item value:

```
$ knotc conf-unset
$ knotc conf-unset 'zone'
```

```
$ knotc conf-unset 'zone[example.com]'
$ knotc conf-unset 'zone[example.com].master'
$ knotc conf-unset 'zone[example.com].master' 'remote2' 'remote5'
```

To get the change between the current configuration and the active transaction for the whole configuration or for a specific section or for a specific identified section or for a specific item:

```
$ knotc conf-diff
$ knotc conf-diff 'zone'
$ knotc conf-diff 'zone[example.com]'
$ knotc conf-diff 'zone[example.com].master'
```

An example of possible configuration initialization:

```
$ knotc conf-begin
$ knotc conf-set 'server.listen' '0.0.0.0@53' '::@53'
$ knotc conf-set 'remote[master_server]'
$ knotc conf-set 'remote[master_server].address' '192.168.1.1'
$ knotc conf-set 'template[default]'
$ knotc conf-set 'template[default].storage' '/var/lib/knot/zones/'
$ knotc conf-set 'template[default].master' 'master_server'
$ knotc conf-set 'zone[example.com]'
$ knotc conf-diff
$ knotc conf-commit
```

6.3 Slave mode

Running the server as a slave is very straightforward as you usually bootstrap zones over AXFR and thus avoid any manual zone operations. In contrast to AXFR, when the incremental transfer finishes, it stores the differences in the journal file and doesn't update the zone file immediately but after the *zonefile-sync* period elapses.

6.4 Master mode

If you just want to check the zone files before starting, you can use:

```
$ knotc zone-check example.com
```

For an approximate estimation of server's memory consumption, you can use:

```
$ knotc zone-memstats example.com
```

This action prints the count of resource records, percentage of signed records and finally estimation of memory consumption for each zone, unless specified otherwise. Please note that the estimated values may differ from the actual consumption. Also, for slave servers with incoming transfers enabled, be aware that the actual memory consumption might be double or higher during transfers.

6.5 Reading and editing zones

Knot DNS allows you to read or change zone contents online using server control interface.

Warning: Avoid concurrent zone file modification, and/or dynamic updates, and/or zone changing over control interface. Otherwise, the zone could be inconsistent.

To get contents of all configured zones, or a specific zone contents, or zone records with a specific owner, or even with a specific record type:

```
$ knotc zone-read --
$ knotc zone-read example.com
$ knotc zone-read example.com ns1
$ knotc zone-read example.com ns1 NS
```

Note: If the record owner is not a fully qualified domain name, then it is considered as a relative name to the zone name.

To start a writing transaction on all zones or on specific zones:

```
$ knotc zone-begin --
$ knotc zone-begin example.com example.net
```

Now you can list all nodes within the transaction using the `zone-get` command, which always returns current data with all changes included. The command has the same syntax as `zone-read`.

Within the transaction, you can add a record to a specific zone or to all zones with an open transaction:

```
$ knotc zone-set example.com ns1 3600 A 192.168.0.1
$ knotc zone-set -- ns1 3600 A 192.168.0.1
```

To remove all records with a specific owner, or a specific rrset, or a specific record data:

```
$ knotc zone-unset example.com ns1
$ knotc zone-unset example.com ns1 A
$ knotc zone-unset example.com ns1 A 192.168.0.2
```

To see the difference between the original zone and the current version:

```
$ knotc zone-diff example.com
```

Finally, either commit or abort your transaction:

```
$ knotc zone-commit example.com
$ knotc zone-abort example.com
```

A full example of setting up a completely new zone from scratch:

```
$ knotc conf-begin
$ knotc conf-set zone.domain example.com
$ knotc conf-commit
$ knotc zone-begin example.com
$ knotc zone-set example.com @ 7200 SOA ns hostmaster 1 86400 900 691200 3600
$ knotc zone-set example.com ns 3600 A 192.168.0.1
$ knotc zone-set example.com www 3600 A 192.168.0.100
$ knotc zone-commit example.com
```

6.6 Daemon controls

Knot DNS was designed to allow server reconfiguration on-the-fly without interrupting its operation. Thus it is possible to change both configuration and zone files and also add or remove zones without restarting the server. This can be done with:

```
$ knotc reload
```

If you want to enable ixfr differences creation from changes you make to a zone file, enable *ixfr-from-differences* in the zone configuration and reload your server as seen above. If *SOA*'s *serial* is not changed, no differences will be created.

If you want to refresh the slave zones, you can do this with:

```
$ knotc zone-refresh
```

CHAPTER

SEVEN

TROUBLESHOOTING

First of all, check the logs. Enabling at least the `warning` message severity may help you to identify some problems. See the *Logging section* for details.

7.1 Reporting bugs

If you are unable to solve the problem by yourself, you can submit a bugreport to the Knot DNS developers. For security or sensitive issues contact the developers directly on knot-dns@labs.nic.cz. All other bugs and questions may be directed to the public Knot DNS users mailing list (knot-dns-users@lists.nic.cz) or may be entered into the issue tracking system.

Before anything else, please try to answer the following questions:

- Has it been working?
- What has changed? System configuration, software updates, network configuration, firewall rules modification, hardware replacement, etc.

The bugreport should contain the answers for the previous questions and in addition at least the following information:

- Knot DNS version and type of installation (distribution package, from source, etc.)
- Operating system, platform, kernel version
- Relevant basic hardware information (processor, amount of memory, available network devices, etc.)
- Description of the bug
- Log output with the highest verbosity (category `any`, severity `debug`)
- Steps to reproduce the bug (if known)
- Backtrace (if the bug caused a crash or a hang; see the next section)

If possible, please provide a minimal configuration file and zone files which can be used to reproduce the bug.

7.2 Generating backtrace

Backtrace carries basic information about the state of the program and how the program got where it is. It helps determining the location of the bug in the source code.

If you run Knot DNS from distribution packages, make sure the debugging symbols for the package are installed. The symbols are usually distributed in a separate package.

There are several ways to get the backtrace. One possible way is to extract the backtrace from a core dump file. Core dump is a memory snapshot generated by the operating system when a process crashes. The generating of core dumps must be usually enabled:

```
$ ulimit -c unlimited                    # Enable unlimited core dump size
$ knotd ...                              # Reproduce the crash
...
$ gdb knotd <core-dump-file>             # Start gdb on the core dump
(gdb) info threads                       # Get a summary of all threads
(gdb) thread apply all bt full           # Extract backtrace from all threads
(gdb) quit
```

To save the backtrace into a file, the following GDB commands can be used:

```
(gdb) set pagination off
(gdb) set logging file backtrace.txt
(gdb) set logging on
(gdb) info threads
(gdb) thread apply all bt full
(gdb) set logging off
```

To generate a core dump of a running process, the *gcore* utility can be used:

```
$ gcore -o <output-file> $(pidof knotd)
```

Please note that core dumps can be intercepted by an error-collecting system service (systemd-coredump, ABRT, Apport, etc.). If you are using such a service, consult its documentation about core dump retrieval.

If the error is reproducible, it is also possible to start and inspect the server directly in the debugger:

```
$ gdb --args knotd -c /etc/knot.conf
(gdb) run
...
```

Alternatively, the debugger can be attached to a running server process. This is generally useful when troubleshooting a stuck process:

```
$ knotd ...
$ gdb --pid $(pidof knotd)
(gdb) continue
...
```

If you fail to get a backtrace of a running process using the previous method, you may try the single-purpose `pstack` utility:

```
$ pstack $(pidof knotd) > backtrace.txt
```

CHAPTER

EIGHT

CONFIGURATION REFERENCE

8.1 Description

Configuration files for Knot DNS use simplified YAML format. Simplified means that not all of the features are supported.

For the description of configuration items, we have to declare a meaning of the following symbols:

- *INT* – Integer
- *STR* – Textual string
- *HEXSTR* – Hexadecimal string (with `0x` prefix)
- *BOOL* – Boolean value (`on`/`off` or `true`/`false`)
- *TIME* – Number of seconds, an integer with possible time multiplier suffix (`s` ~ 1, `m` ~ 60, `h` ~ 3600 or `d` ~ 24 * 3600)
- *SIZE* – Number of bytes, an integer with possible size multiplier suffix (`B` ~ 1, `K` ~ 1024, `M` ~ 1024^2 or `G` ~ 1024^3)
- *BASE64* – Base64 encoded string
- *ADDR* – IPv4 or IPv6 address
- *DNAME* – Domain name
- ... – Multi-valued item, order of the values is preserved
- [ ] – Optional value
- | – Choice

There are 10 main sections (`server`, `control`, `log`, `keystore`, `policy`, `key`, `acl`, `remote`, `template`, and `zone`) and module sections with the `mod-` prefix. Most of the sections (excluding `server` and `control`) are sequences of settings blocks. Each settings block begins with a unique identifier, which can be used as a reference from other sections (such identifier must be defined in advance).

A multi-valued item can be specified either as a YAML sequence:

```
address: [10.0.0.1, 10.0.0.2]
```

or as more single-valued items each on an extra line:

```
address: 10.0.0.1
address: 10.0.0.2
```

If an item value contains spaces or other special characters, it is necessary to enclose such value within double quotes `" "`.

8.2 Comments

A comment begins with a # character and is ignored during processing. Also each configuration section or sequence block allows a permanent comment using the `comment` item which is stored in the server beside the configuration.

8.3 Includes

Another configuration file or files, matching a pattern, can be included at the top level in the current file. If the path is not absolute, then it is considered to be relative to the current file. The pattern can be an arbitrary string meeting POSIX *glob* requirements, e.g. dir/*.conf. Matching files are processed in sorted order.

```
include: STR
```

8.4 Server section

General options related to the server.

```
server:
    identity: [STR]
    version: [STR]
    nsid: [STR|HEXSTR]
    rundir: STR
    user: STR[:STR]
    pidfile: STR
    udp-workers: INT
    tcp-workers: INT
    background-workers: INT
    async-start: BOOL
    tcp-handshake-timeout: TIME
    tcp-idle-timeout: TIME
    tcp-reply-timeout: TIME
    max-tcp-clients: INT
    max-udp-payload: SIZE
    max-ipv4-udp-payload: SIZE
    max-ipv6-udp-payload: SIZE
    rate-limit: INT
    rate-limit-slip: INT
    rate-limit-table-size: INT
    rate-limit-whitelist: ADDR[/INT] | ADDR-ADDR ...
    listen: ADDR[@INT] ...
```

8.4.1 identity

An identity of the server returned in the response to the query for TXT record `id.server.` or `hostname.bind.` in the CHAOS class (see RFC 4892). Set empty value to disable.

Default: FQDN hostname

8.4.2 version

A version of the server software returned in the response to the query for TXT record `version.server.` or `version.bind.` in the CHAOS class (see RFC 4892). Set empty value to disable.

Default: server version

8.4.3 nsid

A DNS name server identifier (see RFC 5001). Set empty value to disable.

Default: FQDN hostname

8.4.4 rundir

A path for storing run-time data (PID file, unix sockets, etc.).

Default: `${localstatedir}/run/knot` (configured with `--with-rundir=path`)

8.4.5 user

A system user with an optional system group (`user:group`) under which the server is run after starting and binding to interfaces. Linux capabilities are employed if supported.

Default: root:root

8.4.6 pidfile

A PID file location.

Default: *rundir*/knot.pid

8.4.7 udp-workers

A number of UDP workers (threads) used to process incoming queries over UDP.

Default: auto-estimated optimal value based on the number of online CPUs

8.4.8 tcp-workers

A number of TCP workers (threads) used to process incoming queries over TCP.

Default: auto-estimated optimal value based on the number of online CPUs

8.4.9 background-workers

A number of workers (threads) used to execute background operations (zone loading, zone updates, etc.).

Default: auto-estimated optimal value based on the number of online CPUs

8.4.10 async-start

If enabled, server doesn't wait for the zones to be loaded and starts responding immediately with SERVFAIL answers until the zone loads.

Default: off

8.4.11 tcp-handshake-timeout

Maximum time between newly accepted TCP connection and the first query. This is useful to disconnect inactive connections faster than connections that already made at least 1 meaningful query.

Default: 5

8.4.12 tcp-idle-timeout

Maximum idle time between requests on a TCP connection. This also limits receiving of a single query, each query must be received in this time limit.

Default: 20

8.4.13 tcp-reply-timeout

Maximum time to wait for an outgoing connection or for a reply to an issued request (SOA, NOTIFY, AXFR...).

Default: 10

8.4.14 max-tcp-clients

A maximum number of TCP clients connected in parallel, set this below the file descriptor limit to avoid resource exhaustion.

Default: 100

8.4.15 rate-limit

Rate limiting is based on the token bucket scheme. A rate basically represents a number of tokens available each second. Each response is processed and classified (based on several discriminators, e.g. source netblock, query type, zone name, rcode, etc.). Classified responses are then hashed and assigned to a bucket containing number of available tokens, timestamp and metadata. When available tokens are exhausted, response is dropped or sent as truncated (see *rate-limit-slip*). Number of available tokens is recalculated each second.

Default: 0 (disabled)

8.4.16 rate-limit-table-size

Size of the hash table in a number of buckets. The larger the hash table, the lesser the probability of a hash collision, but at the expense of additional memory costs. Each bucket is estimated roughly to 32 bytes. The size should be selected as a reasonably large prime due to better hash function distribution properties. Hash table is internally chained and works well up to a fill rate of 90 %, general rule of thumb is to select a prime near 1.2 * maximum_qps.

Default: 393241

8.4.17 rate-limit-slip

As attacks using DNS/UDP are usually based on a forged source address, an attacker could deny services to the victim's netblock if all responses would be completely blocked. The idea behind SLIP mechanism is to send each N^{th} response as truncated, thus allowing client to reconnect via TCP for at least some degree of service. It is worth noting, that some responses can't be truncated (e.g. SERVFAIL).

- Setting the value to **0** will cause that all rate-limited responses will be dropped. The outbound bandwidth and packet rate will be strictly capped by the *rate-limit* option. All legitimate requestors affected by the limit will face denial of service and will observe excessive timeouts. Therefore this setting is not recommended.
- Setting the value to **1** will cause that all rate-limited responses will be sent as truncated. The amplification factor of the attack will be reduced, but the outbound data bandwidth won't be lower than the incoming bandwidth. Also the outbound packet rate will be the same as without RRL.

- Setting the value to **2** will cause that half of the rate-limited responses will be dropped, the other half will be sent as truncated. With this configuration, both outbound bandwidth and packet rate will be lower than the inbound. On the other hand, the dropped responses enlarge the time window for possible cache poisoning attack on the resolver.
- Setting the value to anything **larger than 2** will keep on decreasing the outgoing rate-limited bandwidth, packet rate, and chances to notify legitimate requestors to reconnect using TCP. These attributes are inversely proportional to the configured value. Setting the value high is not advisable.

Default: 1

8.4.18 rate-limit-whitelist

A list of IP addresses, network subnets, or network ranges to exempt from rate limiting. Empty list means that no incoming connection will be white-listed.

Default: not set

8.4.19 max-udp-payload

Maximum EDNS0 UDP payload size default for both IPv4 and IPv6.

Default: 4096

8.4.20 max-ipv4-udp-payload

Maximum EDNS0 UDP payload size for IPv4.

Default: 4096

8.4.21 max-ipv6-udp-payload

Maximum EDNS0 UDP payload size for IPv6.

Default: 4096

8.4.22 listen

One or more IP addresses where the server listens for incoming queries. Optional port specification (default is 53) can be appended to each address using `@` separator. Use `0.0.0.0` for all configured IPv4 addresses or `::` for all configured IPv6 addresses.

Default: not set

8.5 Key section

Shared TSIG keys used to authenticate communication with the server.

```
key:
  - id: DNAME
    algorithm: hmac-md5 | hmac-sha1 | hmac-sha224 | hmac-sha256 | hmac-sha384 |␣
↪hmac-sha512
    secret: BASE64
```

8.5.1 id

A key name identifier.

8.5.2 algorithm

A key algorithm.

Default: not set

8.5.3 secret

Shared key secret.

Default: not set

8.6 ACL section

Access control list rule definitions. The ACLs are used to match incoming connections to allow or deny requested operation (zone transfer request, DDNS update, etc.).

```
acl:
  - id: STR
    address: ADDR[/INT] | ADDR-ADDR ...
    key: key_id ...
    action: notify | transfer | update ...
    deny: BOOL
```

8.6.1 id

An ACL rule identifier.

8.6.2 address

An ordered list of IP addresses, network subnets, or network ranges. The query must match one of them. Empty value means that address match is not required.

Default: not set

8.6.3 key

An ordered list of *reference*s to TSIG keys. The query must match one of them. Empty value means that TSIG key is not required.

Default: not set

8.6.4 action

An ordered list of allowed actions. Empty action list is only allowed if *deny* is set.

Possible values:

- `transfer` – Allow zone transfer
- `notify` – Allow incoming notify

- `update` – Allow zone updates

Default: not set

8.6.5 deny

Deny if *address*, *key* and *action* match.

Default: off

8.7 Control section

Configuration of the server control interface.

```
control:
    listen: STR
    timeout: TIME
```

8.7.1 listen

A UNIX socket path where the server listens for control commands.

Default: *rundir*/knot.sock

8.7.2 timeout

Maximum time the control socket operations can take. Set 0 for infinity.

Default: 5

8.8 Keystore section

DNSSEC keystore configuration.

```
keystore:
  - id: STR
    backend: pem | pkcs11
    config: STR
```

8.8.1 id

A keystore identifier.

8.8.2 backend

A key storage backend type. A directory with PEM files or a PKCS #11 storage.

Default: pem

8.8.3 config

A backend specific configuration. A directory with PEM files (the path can be specified as a relative path to *kasp-db*) or a configuration string for PKCS #11 storage.

Note: Example configuration string for PKCS #11:

```
"pkcs11:token=knot;pin-value=1234 /usr/lib64/pkcs11/libsofthsm2.so"
```

Default: *kasp-db*/keys

8.9 Policy section

DNSSEC policy configuration.

```
policy:
  - id: STR
    keystore: STR
    manual: BOOL
    algorithm: dsa | rsasha1 | dsa-nsec3-sha1 | rsasha1-nsec3-sha1 | rsasha256 |␣
↪rsasha512 | ecdsap256sha256 | ecdsap384sha384
    ksk-size: SIZE
    zsk-size: SIZE
    dnskey-ttl: TIME
    zsk-lifetime: TIME
    propagation-delay: TIME
    rrsig-lifetime: TIME
    rrsig-refresh: TIME
    nsec3: BOOL
    nsec3-iterations: INT
    nsec3-salt-length: INT
    nsec3-salt-lifetime: TIME
```

8.9.1 id

A policy identifier.

8.9.2 keystore

A *reference* to a keystore holding private key material for zones. A special *default* value can be used for the default keystore settings.

Default: default

8.9.3 manual

If enabled, automatic key management is not used.

Default: off

8.9.4 algorithm

An algorithm of signing keys and issued signatures.

Default: ecdsap256sha256

8.9.5 ksk-size

A length of newly generated KSK (Key Signing Key) keys.

Default: 1024 (dsa*), 2048 (rsa*), 256 (ecdsap256*), 384 (ecdsap384*)

8.9.6 zsk-size

A length of newly generated ZSK (Zone Signing Key) keys.

Default: see default for *ksk-size*

8.9.7 dnskey-ttl

A TTL value for DNSKEY records added into zone apex.

Default: zone SOA TTL

Note: has infuence over ZSK key lifetime

8.9.8 zsk-lifetime

A period between ZSK publication and the next rollover initiation.

Default: 30 days

Note: ZSK key lifetime is also infuenced by propagation-delay and dnskey-ttl

8.9.9 propagation-delay

An extra delay added for each key rollover step. This value should be high enough to cover propagation of data from the master server to all slaves.

Default: 1 day

Note: has infuence over ZSK key lifetime

8.9.10 rrsig-lifetime

A validity period of newly issued signatures.

Default: 14 days

8.9.11 rrsig-refresh

A period how long before a signature expiration the signature will be refreshed.

Default: 7 days

8.9.12 nsec3

Specifies if NSEC3 will be used instead of NSEC.

Default: off

8.9.13 nsec3-iterations

A number of additional times the hashing is performed.

Default: 5

8.9.14 nsec3-salt-length

A length of a salt field in octets, which is appended to the original owner name before hashing.

Default: 8

8.9.15 nsec3-salt-lifetime

A validity period of newly issued salt field.

Default: 30 days

8.10 Remote section

Definitions of remote servers for outgoing connections (source of a zone transfer, target for a notification, etc.).

```
remote:
  - id: STR
    address: ADDR[@INT] ...
    via: ADDR[@INT] ...
    key: key_id
```

8.10.1 id

A remote identifier.

8.10.2 address

An ordered list of destination IP addresses which are used for communication with the remote server. The addresses are tried in sequence unless the operation is successful. Optional destination port (default is 53) can be appended to the address using `@` separator.

Default: not set

8.10.3 via

An ordered list of source IP addresses. The first address with the same family as the destination address is used. Optional source port (default is random) can be appended to the address using `@` separator.

Default: not set

8.10.4 key

A *reference* to the TSIG key which ise used to authenticate the communication with the remote server.

Default: not set

8.11 Template section

A template is a shareable zone setting which can be used for configuration of many zones in one place. A special default template (with the *default* identifier) can be used for global querying configuration or as an implicit configuration if a zone doesn't have another template specified.

```
template:
  - id: STR
    timer-db: STR
    global-module: STR/STR ...
    # All zone options (excluding 'template' item)
```

8.11.1 id

A template identifier.

8.11.2 timer-db

Specifies a path of the persistent timer database. The path can be specified as a relative path to the *default* template *storage*.

Note: This option is only available in the *default* template.

Default: *storage*/timers

8.11.3 global-module

An ordered list of references to query modules in the form of *module_name* or *module_name/module_id*. These modules apply to all queries.

Note: This option is only available in the *default* template.

Default: not set

8.12 Zone section

Definition of zones served by the server.

```
zone:
  - domain: DNAME
    template: template_id
    storage: STR
    file: STR
    journal: STR
    master: remote_id ...
```

```
    ddns-master: remote_id
    notify: remote_id ...
    acl: acl_id ...
    semantic-checks: BOOL
    disable-any: BOOL
    zonefile-sync: TIME
    ixfr-from-differences: BOOL
    max-journal-size: SIZE
    max-zone-size : SIZE
    dnssec-signing: BOOL
    dnssec-policy: STR
    kasp-db: STR
    request-edns-option: INT:[HEXSTR]
    serial-policy: increment | unixtime
    module: STR/STR ...
```

8.12.1 domain

A zone name identifier.

8.12.2 template

A *reference* to a configuration template.

Default: not set or *default* (if the template exists)

8.12.3 storage

A data directory for storing zone files, journal files and timers database.

Default: `${localstatedir}/lib/knot` (configured with `--with-storage=path`)

8.12.4 file

A path to the zone file. Non absolute path is relative to *storage*. It is also possible to use the following formatters:

- `%c[N]` or `%c[N-M]` – means the *N*th character or a sequence of characters beginning from the *N*th and ending with the *M*th character of the textual zone name (see `%s`). The indexes are counted from 0 from the left. All dots (including the terminal one) are considered. If the character is not available, the formatter has no effect.
- `%l[N]` – means the *N*th label of the textual zone name (see `%s`). The index is counted from 0 from the right (0 ~ TLD). If the label is not available, the formatter has no effect.
- `%s` – means the current zone name in the textual representation (beware of special characters which are escaped or encoded in the \DDD form where DDD is corresponding decimal ASCII code). The zone name doesn't include the terminating dot (the result for the root zone is the empty string!).
- `%%` – means the `%` character

Default: *storage*/`%s`.zone

8.12.5 journal

A path to the zone journal. Non absolute path is relative to *storage*. The same set of formatters as for *file* is supported.

Default: *storage*/`%s`.db

8.12.6 master

An ordered list of *references* to zone master servers.

Default: not set

8.12.7 ddns-master

A *reference* to zone primary master server. If not specified, the first *master* server is used.

Default: not set

8.12.8 notify

An ordered list of *references* to remotes to which notify message is sent if the zone changes.

Default: not set

8.12.9 acl

An ordered list of *references* to ACL rules which can allow or disallow zone transfers, updates or incoming notifies.

Default: not set

8.12.10 semantic-checks

If enabled, extra zone file semantic checks are turned on.

Several checks are enabled by default and cannot be turned off. An error in mandatory checks causes zone not to be loaded. An error in extra checks is logged only.

Mandatory checks:

- An extra record together with CNAME record (except for RRSIG and DS)
- SOA record missing in the zone (RFC 1034)
- DNAME records having records under it (DNAME children) (RFC 2672)

Extra checks:

- Missing NS record at the zone apex
- Missing glue A or AAAA records
- Broken or non-cyclic NSEC(3) chain
- Wrong NSEC(3) type bitmap
- Multiple NSEC records at the same node
- Missing NSEC records at authoritative nodes
- NSEC3 insecure delegation that is not part of Opt-out span
- Wrong original TTL value in NSEC3 records
- Wrong RDATA TTL value in RRSIG record
- Signer name in RRSIG RR not the same as in DNSKEY
- Signed RRSIG
- Wrong key flags or wrong key in RRSIG record (not the same as ZSK)

Default: off

8.12.11 disable-any

If enabled, all authoritative ANY queries sent over UDP will be answered with an empty response and with the TC bit set. Use this option to minimize the risk of DNS reflection attack.

Default: off

8.12.12 zonefile-sync

The time after which the current zone in memory will be synced with a zone file on the disk (see *file*). The server will serve the latest zone even after a restart using zone journal, but the zone file on the disk will only be synced after `zonefile-sync` time has expired (or after manual zone flush). This is applicable when the zone is updated via IXFR, DDNS or automatic DNSSEC signing. In order to disable automatic zonefile synchronization, -1 value can be used (manual zone flush is still possible).

Note: If you are serving large zones with frequent updates where the immediate sync with a zone file is not desirable, increase the value.

Warning: If the zone file is not up-to-date, the zone should be flushed before its zone file editation or the SOA record must be untouched after editation. Otherwise the journal can't be applied.

Default: 0 (immediate)

8.12.13 ixfr-from-differences

If enabled, the server creates zone differences from changes you made to the zone file upon server reload. This option is relevant only if the server is a master server for the zone.

Note: This option has no effect with enabled *dnssec-signing*.

Default: off

8.12.14 max-journal-size

Maximum size of the zone journal file.

Default: 2^64

8.12.15 max-zone-size

Maximum size of the zone. The size is measured as size of the zone records in wire format without compression. The limit is enforced for incoming zone transfers and dynamic updates.

For incremental transfers (IXFR), the effective limit for the total size of the records in the transfer is twice the configured value. However the final size of the zone must satisfy the configured value.

Default: 2^64

8.12.16 dnssec-signing

If enabled, automatic DNSSEC signing for the zone is turned on.

Note: Cannot be enabled on a slave zone.

Default: off

8.12.17 dnssec-policy

A *reference* to DNSSEC signing policy. A special *default* value can be used for the default policy settings.

Required

8.12.18 kasp-db

A KASP database path. Non absolute path is relative to *storage*.

Default: *storage*/keys

8.12.19 request-edns-option

An arbitrary EDNS0 option which is included into a server request (AXFR, IXFR, SOA, or NOTIFY). The value is in the option_code:option_data format.

Default: not set

8.12.20 serial-policy

Specifies how the zone serial is updated after a dynamic update or automatic DNSSEC signing. If the serial is changed by the dynamic update, no change is made.

Possible values:

- `increment` – The serial is incremented according to serial number arithmetic
- `unixtime` – The serial is set to the current unix time

Note: If your serial was in other than unix time format, be careful with the transition to unix time. It may happen that the new serial will be 'lower' than the old one. If this is the case, the transition should be done by hand (see RFC 1982).

Default: increment

8.12.21 module

An ordered list of references to query modules in the form of *module_name* or *module_name/module_id*. These modules apply only to the current zone queries.

Default: not set

8.13 Logging section

Server can be configured to log to the standard output, standard error output, syslog (or systemd journal if systemd is enabled) or into an arbitrary file.

There are 6 logging severity levels:

- `critical` – Non-recoverable error resulting in server shutdown
- `error` – Recoverable error, action should be taken
- `warning` – Warning that might require user action
- `notice` – Server notice or hint
- `info` – Informational message
- `debug` – Debug messages (must be turned on at compile time)

In the case of missing log section, `warning` or more serious messages will be logged to both standard error output and syslog. The `info` and `notice` messages will be logged to standard output.

```
log:
  - target: stdout | stderr | syslog | STR
    server: critical | error | warning | notice | info | debug
    zone: critical | error | warning | notice | info | debug
    any: critical | error | warning | notice | info | debug
```

8.13.1 target

A logging output.

Possible values:

- `stdout` – Standard output
- `stderr` – Standard error output
- `syslog` – Syslog
- *file_name* – File

8.13.2 server

Minimum severity level for messages related to general operation of the server that are logged.

Default: not set

8.13.3 zone

Minimum severity level for messages related to zones that are logged.

Default: not set

8.13.4 any

Minimum severity level for all message types that are logged.

Default: not set

8.14 Module dnstap

The module dnstap allows query and response logging.

For all queries logging, use this module in the *default* template. For zone-specific logging, use this module in the proper zone configuration.

```
mod-dnstap:
  - id: STR
    sink: STR
    identity: STR
    version: STR
    log-queries: BOOL
    log-responses: BOOL
```

8.14.1 id

A module identifier.

8.14.2 sink

A sink path, which can be either a file or a UNIX socket when prefixed with `unix:`.

Required

8.14.3 identity

A DNS server identity. Set empty value to disable.

Default: FQDN hostname

8.14.4 version

A DNS server version. Set empty value to disable.

Default: server version

8.14.5 log-queries

If enabled, query messages will be logged.

Default: on

8.14.6 log-responses

If enabled, response messages will be logged.

Default: on

8.15 Module synth-record

This module is able to synthesize either forward or reverse records for the given prefix and subnet.

```
mod-synth-record:
  - id: STR
    type: forward | reverse
    prefix: STR
    origin: DNAME
    ttl: INT
    network: ADDR[/INT] | ADDR-ADDR
```

8.15.1 id

A module identifier.

8.15.2 type

The type of generated records.

Possible values:

- `forward` – Forward records
- `reverse` – Reverse records

Required

8.15.3 prefix

A record owner prefix.

Note: The value doesn't allow dots, address parts in the synthetic names are separated with a dash.

Default: empty

8.15.4 origin

A zone origin (only valid for the *reverse type*).

Required

8.15.5 ttl

Time to live of the generated records.

Default: 3600

8.15.6 network

An IP address, a network subnet, or a network range the query must match.

Required

8.16 Module dnsproxy

The module catches all unsatisfied queries and forwards them to the indicated server for resolution.

```
mod-dnsproxy:
  - id: STR
    remote: remote_id
    timeout: INT
    catch-nxdomain: BOOL
```

8.16.1 id

A module identifier.

8.16.2 remote

A *reference* to a remote server where the queries are forwarded to.

Required

8.16.3 timeout

A remote response timeout in milliseconds.

Default: 500

8.16.4 catch-nxdomain

If enabled, all unsatisfied queries (also applies to local zone lookups) are forwarded.

Default: off

8.17 Module rosedb

The module provides a mean to override responses for certain queries before the available zones are searched for the record.

```
mod-rosedb:
  - id: STR
    dbdir: STR
```

8.17.1 id

A module identifier.

8.17.2 dbdir

A path to the directory where the database is stored.

Required

CHAPTER

NINE

UTILITIES

Knot DNS comes with a few DNS client utilities and a few utilities to control the server. This section collects manual pages for all provided binaries:

9.1 kdig – Advanced DNS lookup utility

9.1.1 Synopsis

kdig [*common-settings*] [*query* [*settings*]]...

kdig -h

9.1.2 Description

This utility sends one or more DNS queries to a nameserver. Each query can have individual *settings*, or it can be specified globally via *common-settings*, which must precede *query* specification.

Parameters

query *name* | **-q** *name* | **-x** *address* | **-G** *tapfile*

common-settings, ***settings*** [*class*] [*type*] [@*server*]... [*options*]

name Is a domain name that is to be looked up.

server Is a domain name or an IPv4 or IPv6 address of the nameserver to send a query to. An additional port can be specified using address:port ([address]:port for IPv6 address), address@port, or address#port notation. If no server is specified, the servers from `/etc/resolv.conf` are used.

If no arguments are provided, **kdig** sends NS query for the root zone.

Options

-4 Use the IPv4 protocol only.

-6 Use the IPv6 protocol only.

-b *address* Set the source IP address of the query to *address*. The address must be a valid address for local interface or :: or 0.0.0.0. An optional port can be specified in the same format as the *server* value.

-c *class* Set the query class (e.g. CH, CLASS4). An explicit variant of *class* specification. The default class is IN.

-d Enable debug messages.

-h, –help Print the program help.

-k *keyfile* Use the TSIG key stored in a file *keyfile* to authenticate the request. The file must contain the key in the same format as accepted by the **-y** option.

-p *port* Set the nameserver port number or service name to send a query to. The default port is 53.

-q *name* Set the query name. An explicit variant of *name* specification.

-t *type* Set the query type (e.g. NS, IXFR=12345, TYPE65535, NOTIFY). An explicit variant of *type* specification. The default type is A. IXFR type requires SOA serial parameter. NOTIFY type without SOA serial parameter causes pure NOTIFY message without any SOA hint.

-V, –version Print the program version.

-x *address* Send a reverse (PTR) query for IPv4 or IPv6 *address*. The correct name, class and type is set automatically.

-y [*alg*:]*name*:*key* Use the TSIG key named *name* to authenticate the request. The *alg* part specifies the algorithm (the default is hmac-md5) and *key* specifies the shared secret encoded in Base64.

-E *tapfile* Export a dnstap trace of the query and response messages received to the file *tapfile*.

-G *tapfile* Generate message output from a previously saved dnstap file *tapfile*.

+[no]multiline Wrap long records to more lines and improve human readability.

+[no]short Show record data only.

+[no]generic Use the generic representation format when printing resource record types and data.

+[no]aaflag Set the AA flag.

+[no]tcflag Set the TC flag.

+[no]rdflag Set the RD flag.

+[no]recurse Same as **+[no]rdflag**

+[no]raflag Set the RA flag.

+[no]zflag Set the zero flag bit.

+[no]adflag Set the AD flag.

+[no]cdflag Set the CD flag.

+[no]dnssec Set the DO flag.

+[no]all Show all packet sections.

+[no]qr Show the query packet.

+[no]header Show the packet header.

+[no]opt Show the EDNS pseudosection.

+[no]question Show the question section.

+[no]answer Show the answer section.

+[no]authority Show the authority section.

+[no]additional Show the additional section.

+[no]tsig Show the TSIG pseudosection.

+[no]stats Show trailing packet statistics.

+[no]class Show the DNS class.

+[no]ttl Show the TTL value.

+[no]tcp Use the TCP protocol (default is UDP for standard query and TCP for AXFR/IXFR).

+[no]ignore Don't use TCP automatically if a truncated reply is received.

+[no]tls Use TLS with the Opportunistic privacy profile.

+[no]tls-ca[=*FILE*] Use TLS with the Out-Of-Band privacy profile, use a specified PEM file (default is system certificate storage if no argument is provided). Can be specified multiple times.

+[no]tls-pin=*BASE64* Use TLS with a pinned certificate check. The PIN must be a Base64 encoded SHA-256 hash of the X.509 SubjectPublicKeyInfo. Can be specified multiple times.

+[no]tls-hostname=*STR* Use TLS with a remote server hostname check.

+[no]nsid Request the nameserver identifier (NSID).

+[no]bufsize=*B* Set EDNS buffer size in bytes (default is 512 bytes).

+[no]padding=*B* Set EDNS(0) padding option data length (default is no).

+[no]alignment[=*B*] Align the query to B-byte-block message using the EDNS(0) padding option (default is no or 128 if no argument is specified).

+[no]subnet=*SUBN* Set EDNS(0) client subnet SUBN=addr/prefix.

+[no]edns[=*N*] Use EDNS version (default is 0).

+[no]time=*T* Set the wait-for-reply interval in seconds (default is 5 seconds). This timeout applies to each query attempt.

+[no]retry=*N* Set the number (>=0) of UDP retries (default is 2). This doesn't apply to AXFR/IXFR.

+noidn Disable the IDN transformation to ASCII and vice versa. IDNA2003 support depends on libidn availability during project building!

9.1.3 Notes

Options **-k** and **-y** can not be used simultaneously.

Dnssec-keygen keyfile format is not supported. Use *keymgr(8)* instead.

9.1.4 Examples

1. Get A records for example.com:

```
$ kdig example.com A
```

2. Perform AXFR for zone example.com from the server 192.0.2.1:

```
$ kdig example.com -t AXFR @192.0.2.1
```

3. Get A records for example.com from 192.0.2.1 and reverse lookup for address 2001:DB8::1 from 192.0.2.2. Both using the TCP protocol:

```
$ kdig +tcp example.com -t A @192.0.2.1 -x 2001:DB8::1 @192.0.2.2
```

4. Get SOA record for example.com, use TLS, use system certificates, check for specified hostname, check for certificate pin, and print additional debug info:

```
$ kdig -d @185.49.141.38 +tls-ca +tls-host=getdnsapi.net \
  +tls-pin=foxZRnIh9gZpWnl+zEiKa0EJ2rdCGroMWm02gaxSc9S= soa example.com
```

9.1.5 Files

`/etc/resolv.conf`

9.1.6 See Also

khost(1), *knsupdate(1)*, *keymgr(8)*.

9.2 keymgr – Key management utility

9.2.1 Synopsis

keymgr [*global-options*] [*command...*] [*arguments...*]

keymgr [*global-options*] [*command...*] **help**

9.2.2 Description

The **keymgr** utility serves for key management in Knot DNS server.

Primarily functions for DNSSEC keys and KASP (Key And Signature Policy) management are provided. However the utility also provides functions for TSIG key generation.

The DNSSEC and KASP configuration is stored in a so called KASP database. The database is simply a directory in the file-system containing files in the JSON format.

The operations are organized into commands and subcommands. A command specifies the operation to be performed with the KASP database. It is usually followed by named arguments. The special command **help** can be used to list available subcommands in that area. The listing of available command arguments is not supported yet.

Command and argument names are parsed in a smart way. Only a beginning of a name can be entered and it will be recognized. The specified part of a name must be unique amongst the other names.

Global options

-c, –config *file* Use a textual configuration file to get the KASP database location.

-C, –confdb *directory* Use a binary configuration database directory to get the KASP database location.

-d, –dir *path* Use a specified KASP database path to work with.

-h, –help Print the program help.

-l, –legacy Enable legacy mode. Zone, policy, and keystore configuration is stored in KASP database (not in server configuration).

-V, –version Print the program version.

KASP database location

The location of the KASP database is determined as follows:

1. The path specified with **–dir**.
2. The path read from the server configuration specified with **–confdb** or **–config**.
3. The path read from the server default configuration database.
4. The path read from the server default configuration file.

In legacy mode, the path is determined as follows:

1. The path specified with **–dir**.
2. The path specified in the `KEYMGR_DIR` environment variable.
3. The current working dir.

Main commands

tsig ... Operations with TSIG keys.

zone ... Operations with zones in the database. A zone holds assigned signing configuration and signing metadata.

Main commands (legacy)

init Initialize new KASP database or upgrade existing one. The command is idempotent and therefore it is safe to be run multiple times.

The command creates a default policy and default key store (both named *default*). In case of upgrade, existing objects are checked and any missing attributes are filled in.

policy ... Operations with KASP policies. A policy holds parameters that define the way how a zone is signed.

keystore ... Operations with key stores configured for the KASP database. A private key store holds private key material for zone signing separately from the zone metadata.

tsig commands

tsig generate *name* [algorithm *id*] [size *bits*] Generate new TSIG key and print it on the standard output. The algorithm defaults to *hmac-sha256*. The default key size is determined optimally based on the selected algorithm.

The generated key is printed out in the server configuration format to allow direct inclusion into the server configuration. The first line of the output contains a comment with the key in the one-line key format accepted by client utilities.

zone commands

zone key list *zone-name* [filter] List key IDs and tags of zone keys.

zone key show *zone-name key* Show zone key details. The *key* can be a key tag or a key ID prefix.

zone key ds *zone-name key* Show DS records for a zone key. The *key* can be a key tag or a key ID prefix.

zone key generate *zone-name* [*key-parameter*...] Generate a new key for a zone.

zone key import *zone-name key-file* Import an existing key in the legacy format. The *key-file* suffix `.private` or `.key` is not required. A public key without a matching private key cannot be imported.

zone key set *zone-name key* [*key-parameter*...] Change a key parameter. Only key timing parameters can be changed.

Available *key-parameter*s:

algorithm *id* Algorithm number or IANA mnemonic.

size *bits* Size of the key in bits.

ksk Set the DNSKEY SEP (Secure Entry Point) flag.

publish *time* The time the key is published as a DNSKEY record.

active *time* The time the key is started to be used for signing.

retire *time* The time the key is stopped to be used for signing.

remove *time* The time the key's DNSKEY is removed from the zone.

The *time* accepts YYYYMMDDHHMMSS format, unix timestamp, or offset from the current time. For the offset, add **+** or **-** prefix and optionally a suffix **mi**, **h**, **d**, **w**, **mo**, or **y**. If no suffix is specified, the offset is in seconds.

zone commands (legacy)

zone add ***zone-name*** **[policy** ***policy-name*****]** Add a zone into the database. The policy defaults to 'default'.

zone list [*pattern***]** List zones in the database matching the *pattern* as a substring.

zone remove ***zone-name*** **[force]** Remove a zone from the database. If some keys are currently active, the **force** argument must be specified.

zone set ***zone-name*** **[policy** ***policy-name*****]** Change zone configuration. At the moment, only a policy can be changed.

zone show ***zone-name*** Show zone details.

policy commands (legacy)

policy list List policies in the database.

policy show ***policy-name*** Show policy details.

policy add ***policy-name*** **[***policy-parameter***...]** Add a new policy into the database.

policy set ***policy-name*** **[***policy-parameter***...]** Change policy configuration.

policy remove ***policy-name*** Remove a policy from the database. **Note**, the utility does not check if the policy is used.

Available *policy-parameter*s:

algorithm ***id*** DNSKEY algorithm number or IANA mnemonic.

dnskey-ttl ***seconds*** TTL value for DNSKEY records.

ksk-size ***bits*** Size of the KSK.

zsk-size ***bits*** Size of the ZSK.

zsk-lifetime ***seconds*** Period between ZSK publication and the next rollover initiation.

rrsig-lifetime ***seconds*** Validity period of issued signatures.

rrsig-refresh ***seconds*** Period before signature expiration when the signature will be refreshed.

nsec3 ***enable*** Specifies if NSEC3 will be used instead of NSEC.

nsec3-iterations ***iterations*** Specifies the number of additional iterations in NSEC3 computation.

nsec3-salt-length ***bytes*** Specifies salt length for NSEC3 computation.

nsec3-salt-lifetime ***seconds*** Period after which a new NSEC3 salt is generated.

soa-min-ttl ***seconds*** SOA Minimum TTL field. **Note**, Knot DNS overwrites the value with the real used value.

zone-max-ttl ***seconds*** Max TTL in the zone. **Note**, Knot DNS will determine the value automatically in the future.

delay ***seconds*** Zone signing and data propagation delay. The value is added for safety to timing of all rollover steps.

manual ***enable*** Enable manual key management. If enabled, no keys will be generated or rolled automatically.

keystore ***name*** Name of the key store to be used for private key material.

keystore commands (legacy)

keystore list List names of configured key stores.

keystore show *name* Show configuration of a key store named *name* and list key IDs of private key material present in that key store.

keystore add *name* [backend *backend*] [config *config*] Configure new key store. The *name* is a unique key store identifier. The *backend* and backend-specific configuration string *config* determine where the private key material will be physically stored.

Supported key store backends:

pkcs8 (default) The backend stores private key material in unencrypted X.509 PEM files in a directory specified as the backend configuration string. The path can be specified relatively to the KASP database location.

pkcs11 The backend stores private key material in a cryptographic token accessible via the PKCS #11 interface. The configuration string consists of a token PKCS #11 URL and PKCS #11 module path separated by the space character.

The format of the PKCS #11 URL is described in RFC 7512. If the token is protected by a PIN, make sure to include *pin-value* or *pin-source* attribute in the URL.

The PKCS #11 module path can be an absolute path or just a module name. In the later case, the module is looked up in the default modules location.

9.2.3 Examples

1. Generate two RSA-SHA-256 signing keys. The first key will be used as a KSK, the second one as a ZSK:

```
$ keymgr zone key generate example.com algorithm rsasha256 size 2048 ksk
$ keymgr zone key generate example.com algorithm rsasha256 size 1024
```

2. Import a key in legacy format. The used algorithm must match with the one configured in the policy:

```
$ keymgr zone key import example.com Kexample.com+010+12345.private
```

3. Generate a TSIG key named *operator.key*:

```
$ keymgr tsig generate operator.key algorithm hmac-sha512
```

9.2.4 See Also

RFC 6781 - DNSSEC Operational Practices.

knot.conf(5), *knotc(8)*, *knotd(8)*.

9.3 khost – Simple DNS lookup utility

9.3.1 Synopsis

khost [*options*] *name* [*server*]

9.3.2 Description

This utility sends a DNS query for the *name* to the *server* and prints a reply in more user-readable form. For more advanced DNS queries use **kdig** instead.

Parameters

name Is a domain name that is to be looked up. If the *name* is IPv4 or IPv6 address the PTR query type is used.

server Is a name or an address of the nameserver to send a query to. The address can be specified using [address]:port notation. If no server is specified, the servers from `/etc/resolv.conf` are used.

If no arguments are provided, **`khost`** prints a short help.

Options

-4 Use the IPv4 protocol only.

-6 Use the IPv6 protocol only.

-a Send ANY query with verbose mode.

-d Enable debug messages.

-h, –help Print the program help.

-r Disable recursion.

-T Use the TCP protocol.

-v Enable verbose output.

-V, –version Print the program version.

-w Wait forever for the reply.

-c *class* Set the query class (e.g. CH, CLASS4). The default class is IN.

-t *type* Set the query type (e.g. NS, IXFR=12345, TYPE65535). The default is to send 3 queries (A, AAAA and MX).

-R *retries* The number (>=0) of UDP retries to query a nameserver. The default is 1.

-W *wait* The time to wait for a reply in seconds. This timeout applies to each query try. The default is 2 seconds.

9.3.3 Examples

1. Get the A, AAAA and MX records for example.com:

```
$ khost example.com
```

2. Get the reverse record for address 192.0.2.1:

```
$ khost 192.0.2.1
```

3. Perform a verbose zone transfer for zone example.com:

```
$ khost -t AXFR -v example.com
```

9.3.4 Files

`/etc/resolv.conf`

9.3.5 See Also

`kdig(1)`, *`knsupdate(1)`*.

9.4 kjournalprint – Knot DNS journal print utility

9.4.1 Synopsis

kjournalprint [*parameters*] *journal zone_name*

9.4.2 Description

Program requires journal. As default, changes are colored for terminal.

Parameters

-n, –no-color Removes changes coloring.

-l, –limit *limit* Limits the number of displayed changes.

-h, –help Print the program help.

-V, –version Print the program version.

Journal

Requires journal in the form of path/zone-name.db

Zone name

Requires name of the zone contained in the journal.

9.4.3 Examples

Last (*most recent*) 5 changes without colors

```
$ kjournalprint -nl 5 example.com.db example.com.
```

9.4.4 See Also

knotd(8), *knot.conf(5)*.

9.5 knot1to2 – Knot DNS configuration conversion utility

9.5.1 Synopsis

knot1to2 [*options*] -i *file* -o *file*

9.5.2 Description

This utility generates Knot DNS configuration file version 2.x from configuration file version 1.x.

Parameters

-i, –in *file* Input configuration file (Knot version 1.x).

-o, –out *file* Output configuration file (Knot version 2.x).

Options

-r, –raw Raw output, do not reformat via **knotc**.

-p, –path *directory* Path to **knotc** utility.

-h, –help Print the program help.

-V, –version Print the program version.

9.5.3 See Also

knotc(8), *knotd(8)*, *knot.conf(5)*.

9.6 knotc – Knot DNS control utility

9.6.1 Synopsis

knotc [*parameters*] *action* [*action_args*]

9.6.2 Description

If no *action* is specified, the program is executed in interactive mode.

Parameters

-c, –config *file* Use a textual configuration file (default is `@config_dir@/knot.conf`).

-C, –confdb *directory* Use a binary configuration database directory (default is `@storage_dir@/confdb`). The default configuration database, if exists, has a preference to the default configuration file.

-s, –socket *path* Use a control UNIX socket path (default is `@run_dir@/knot.sock`).

-t, –timeout *seconds* Use a control timeout in seconds. Set 0 for infinity (default is 5).

-f, –force Forced operation. Overrides some checks.

-v, –verbose Enable debug output.

-h, –help Print the program help.

-V, –version Print the program version.

Actions

status Check if the server is running.

stop Stop the server if running.

reload Reload the server configuration and modified zone files. All open zone transactions will be aborted!

zone-check [*zone*...] Test if the server can load the zone. Semantic checks are executed if enabled in the configuration. (*)

zone-memstats [*zone*...] Estimate memory use for the zone. (*)

zone-status [*zone*...] Show the zone status. (*)

zone-reload [*zone*...] Trigger a zone reload from a disk without checking its modification time. For slave zone, the refresh from a master server is scheduled; for master zone, the notification of slave servers is scheduled. An open zone transaction will be aborted!

zone-refresh [*zone*...] Trigger a check for the zone serial on the zone's master. If the master has a newer zone, a transfer is scheduled. This command is valid for slave zones.

zone-retransfer [*zone*...] Trigger a zone transfer from the zone's master. The server doesn't check the serial of the master's zone. This command is valid for slave zones.

zone-flush [*zone*...] Trigger a zone journal flush into the zone file.

zone-sign [*zone*...] Trigger a DNSSEC re-sign of the zone. Existing signatures will be dropped. This command is valid for zones with automatic DNSSEC signing.

zone-read *zone* [*owner* [*type*]] Get zone data that are currently being presented.

zone-begin *zone*... Begin a zone transaction.

zone-commit *zone*... Commit the zone transaction. All changes are applied to the zone.

zone-abort *zone*... Abort the zone transaction. All changes are discarded.

zone-diff *zone* Get zone changes within the transaction.

zone-get *zone* [*owner* [*type*]] Get zone data within the transaction.

zone-set *zone owner* [*ttl*] *type rdata* Add zone record within the transaction. The first record in a rrset requires a ttl value specified.

zone-unset *zone owner* [*type* [*rdata*]] Remove zone data within the transaction.

zone-purge *zone*... Purge zone data, file, journal, and timers.

conf-init Initialize the configuration database. (*)

conf-check Check the server configuration. (*)

conf-import *filename* Import a configuration file into the configuration database. Ensure the server is not using the configuration database! (*)

conf-export *filename* Export the configuration database into a config file. (*)

conf-list [*item*] List the configuration database sections or section items.

conf-read [*item*] Read the item from the active configuration database.

conf-begin Begin a writing configuration database transaction. Only one transaction can be opened at a time.

conf-commit Commit the configuration database transaction.

conf-abort Rollback the configuration database transaction.

conf-diff [*item*] Get the item difference in the transaction.

conf-get [*item*] Get the item data from the transaction.

conf-set *item* [*data*...] Set the item data in the transaction.

conf-unset [*item*] [*data*...] Unset the item data in the transaction.

Note

Empty or **–** *zone* parameter means all zones or all zones with a transaction.

Use @ *owner* to denote the zone name.

Type *item* parameter in the form of *section*[[*id*]][**.***name*].

(*) indicates a local operation which requires a configuration.

Interactive mode

The utility provides interactive mode with basic line editing functionality, command completion, and command history.

Interactive mode behavior can be customized in *~/.editrc*. Refer to `editrc(5)` for details.

Command history is saved in *~/.knotc_history*.

9.6.3 Examples

Reload the whole server configuration

```
$ knotc reload
```

Flush the example.com and example.org zones

```
$ knotc zone-flush example.com example.org
```

Get the current server configuration

```
$ knotc conf-read server
```

Get the list of the current zones

```
$ knotc conf-read zone.domain
```

Get the master remotes for the example.com zone

```
$ knotc conf-read 'zone[example.com].master'
```

Add example.org zone with a zonefile location

```
$ knotc conf-begin
$ knotc conf-set 'zone[example.org]'
$ knotc conf-set 'zone[example.org].file' '/var/zones/example.org.zone'
$ knotc conf-commit
```

Get the SOA record for each configured zone

```
$ knotc zone-read -- @ SOA
```

9.6.4 See Also

`knotd(8)`, `knot.conf(5)`, `editrc(5)`.

9.7 knotd – Knot DNS server daemon

9.7.1 Synopsis

knotd [*parameters*]

9.7.2 Description

Parameters

-c, –config *file* Use a textual configuration file (default is `@config_dir@/knot.conf`).

-C, –confdb *directory* Use a binary configuration database directory (default is `@storage_dir@/confdb`). The default configuration database, if exists, has a preference to the default configuration file.

-s, –socket *path* Use a remote control UNIX socket path (default is `@run_dir@/knot.sock`).

-d, –daemonize [*directory*] Run the server as a daemon. New root directory may be specified (default is `/`).

-v, –verbose Enable debug output.

-h, –help Print the program help.

-V, –version Print the program version.

9.7.3 See Also

knotc(8), *knot.conf(5)*.

9.8 knsec3hash – NSEC hash computation utility

9.8.1 Synopsis

knsec3hash *salt algorithm iterations name*

9.8.2 Description

This utility generates a NSEC3 hash for a given domain name and parameters of NSEC3 hash.

Parameters

salt Specifies a binary salt encoded as a hexadecimal string.

algorithm Specifies a hashing algorithm by number. Currently, the only supported algorithm is SHA-1 (number 1).

iterations Specifies the number of additional iterations of the hashing algorithm.

name Specifies the domain name to be hashed.

9.8.3 Examples

```
$ knsec3hash c01dcafe 1 10 knot-dns.cz
7PTVGE7QV67EM61ROS9238P5RAKR2DM7 (salt=c01dcafe, hash=1, iterations=10)
```

```
$ knsec3hash - 1 0 net
A1RT98BS5QGC9NFI51S9HCI47ULJG6JH (salt=-, hash=1, iterations=0)
```

9.8.4 See Also

RFC 5155 – DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.

knotc(8), *knotd(8)*.

9.9 knsupdate – Dynamic DNS update utility

9.9.1 Synopsis

knsupdate [*options*] [*filename*]

9.9.2 Description

This utility sends Dynamic DNS update messages to a DNS server. Update content is read from a file (if the parameter *filename* is given) or from the standard input.

The format of updates is textual and is made up of commands. Every command is placed on the separate line of the input. Lines starting with a semicolon are comments and are not processed.

Options

-d Enable debug messages.

-h, –help Print the program help.

-k *keyfile* Use the TSIG key stored in a file *keyfile* to authenticate the request. The file should contain the key in the same format, which is accepted by the **-y** option.

-p *port* Set the port to use for connections to the server (if not explicitly specified in the update). The default is 53.

-r *retries* The number of retries for UDP requests. The default is 3.

-t *timeout* The total timeout (for all UDP update tries) of the update request in seconds. The default is 12. If set to zero, the timeout is infinite.

-v Use a TCP connection.

-V, –version Print the program version.

-y [*alg*:]*name*:*key* Use the TSIG key with a name *name* to authenticate the request. The *alg* part specifies the algorithm (the default is hmac-md5) and *key* specifies the shared secret encoded in Base64.

Commands

server *name* [*port*] Specifies a receiving server of the dynamic update message. The *name* parameter can be either a host name or an IP address. If the *port* is not specified, the default port is used. The default port value can be controlled using the **-p** program option.

local *address* [*port*] Specifies outgoing *address* and *port*. If no local is specified, the address and port are set by the system automatically. The default port number is 0.

zone *name* Specifies that all updates are done within a zone *name*. If not used, the default zone is the root zone.

origin *name* Specifies fully qualified domain name suffix which is appended to non-fqd owners in update commands. The default origin is the root zone.

class *name* Sets *name* as the default class for all updates. If not used, the default class is IN.

ttl *value* Sets *value* as the default TTL (in seconds). If not used, the default value is 0.

key [*alg*:]*name key* Specifies the TSIG *key* named *name* to authenticate the request. An optional *alg* algorithm can be specified. This command has the same effect as the program option **-y**.

[prereq] nxdomain *name* Adds a prerequisite for a non-existing record owned by *name*.

[prereq] yxdomain *name* Adds a prerequisite for an existing record owned by *name*.

[prereq] nxrrset *name* [*class*] *type* Adds a prerequisite for a non-existing record of the *type* owned by *name*. Internet *class* is expected.

[prereq] yxrrset *name* [*class*] *type* [*data*] Adds a prerequisite for an existing record of the *type* owned by *name* with optional *data*. Internet *class* is expected.

[update] add *name* [*ttl*] [*class*] *type data* Adds a request to add a new resource record into the zone. Please note that if the *name* is not fully qualified domain name, the current origin name is appended to it.

[update] del[ete] *name* [*ttl*] [*class*] [*type*] [*data*] Adds a request to remove all (or matching *class*, *type* or *data*) resource records from the zone. There is the same requirement for the *name* parameter as in **update add** command. The *ttl* item is ignored.

show Displays current content of the update message.

send Sends the current update message and cleans the list of updates.

answer Displays the last answer from the server.

debug Enable debugging. This command has the same meaning as the **-d** program option.

quit Quit the program.

9.9.3 Notes

Options **-k** and **-y** can not be used simultaneously.

Dnssec-keygen keyfile format is not supported. Use *keymgr(8)* instead.

Zone name/server guessing is not supported if the zone name/server is not specified.

Empty line doesn't send the update.

9.9.4 Examples

1. Send one update of the zone example.com to the server 192.168.1.1. The update contains two new records:

```
$ knsupdate
> server 192.168.1.1
> zone example.com.
> origin example.com.
> ttl 3600
> add test1.example.com. 7200 A 192.168.2.2
> add test2 TXT "hello"
> show
> send
> answer
> quit
```

9.9.5 See Also

kdig(1), *khost(1)*, *keymgr(8)*.

9.10 kzonecheck – Knot DNS zone file checking tool

9.10.1 Synopsis

kzonecheck [*options*] *filename*

9.10.2 Description

The utility checks zone file syntax and runs semantic checks on the zone content. The executed checks are the same as the checks run by the Knot DNS server.

Please, refer to the `semantic-checks` configuration option in *knot.conf(5)* for the full list of available semantic checks.

Options

-o, –origin *origin* Zone origin. If not specified, the origin is determined from the file name (possibly removing the `.zone` suffix).

-v, –verbose Enable debug output.

-h, –help Print the program help.

-V, –version Print the program version.

9.10.3 See Also

knotd(8), *knot.conf(5)*.

CHAPTER

TEN

MIGRATION FROM OTHER DNS SERVERS

10.1 Knot DNS for BIND users

10.1.1 Automatic DNSSEC signing

Migrating automatically signed zones from BIND to Knot DNS requires copying up-to-date zone files from BIND, importing existing private keys, and updating server configuration:

1. To obtain current content of the zone which is being migrated, request BIND to flush the zone into the zone file: `rndc flush example.com`.

   Note: If dynamic updates (DDNS) are enabled for the given zone, you might need to freeze the zone before flushing it. That can be done similarly:

   ```
   $ rndc freeze example.com
   ```

2. Copy the fresh zone file into the zones *storage* directory of Knot DNS.

3. Import all existing zone keys into the KASP database. Make sure that all the keys were imported correctly:

   ```
   $ keymgr zone key import example.com path/to/Kexample.com.+013+11111
   $ keymgr zone key import example.com path/to/Kexample.com.+013+22222
   $ ...
   $ keymgr zone key list example.com
   ```

   Note: The server can be run under a dedicated user account, usually `knot`. As the server requires read-write access to the KASP database, the permissions must be set correctly. This can be achieved for instance by executing all KASP database management commands under sudo:

   ```
   $ sudo -u knot keymgr ...
   ```

4. Follow *Automatic DNSSEC signing* steps to configure DNSSEC signing.

CHAPTER

ELEVEN

APPENDICES

11.1 Compatible PKCS #11 Devices

This section has informative character. Knot DNS has been tested with several devices which claim to support PKCS #11 interface. The following table indicates which algorithms and operations have been observed to work. Please notice minimal GnuTLS library version required for particular algorithm support.

	Key generate	Key import	ECDSA 256-bit	ECDSA 384-bit	RSA 1024-bit	RSA 2048-bit	RSA 4096-bit	DSA 512-bit	DSA 1024-bit
Feitian ePass 2003	**yes**	no	no	no	**yes**	**yes**	no	no	no
SafeNet Network HSM (Luna SA 4)	**yes**	no	no	no	**yes**	**yes**	**yes**	no	no
SoftHSM 2.0	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**	**yes**
Trustway Proteccio NetHSM	**yes**	ECDSA only	**yes**	**yes**	**yes**	**yes**	**yes**	no	no

The following table summarizes supported DNSSEC algorithm numbers and minimal GnuTLS library version required. Any algorithm may work with older library, however the supported operations may be limited (e.g. private key import).

	Numbers	GnuTLS version
ECDSA	13, 14	3.4.8 or newer
RSA	5, 7, 8, 10	3.4.6 or newer
DSA	3, 6	3.4.10 or newer

R