BIND 9 Administrator Reference Manual

BIND Version 9.10.3-P2

Chapter 1

Introduction

The Internet Domain Name System (DNS) consists of the syntax to specify the names of entities in the Internet in a hierarchical manner, the rules used for delegating authority over names, and the system

Chapter 3

Name Server Configuration

In this chapter we provide some suggested configurations along with guidelines for their use. We suggest reasonable values for certain option settings.

3.1 Sample Configurations

```
     // This is the default
     allow-query { any; };
     // Do not provide recursive service
     recursion no;
};

// Provide a reverse mapping for the loopback
// address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
     type master;
     file "localhost.rev";
     notify no;
};
// We are the master server for example.com
zone "example.com" {
     type master;
     file "example.com.db";
     // IP addresses of slave servers allowed to
     // transfer example.com
     allow-transfer {
          192.168.4.14;
          192.168.5.53;
     };
};
// We are a slave server for eng.example.com
zone "eng.example.com" {
     type slave;
     file "eng.example.com.bk";
     // IP address of eng.example.com master server
     masters { 192.168.4.12; };
};
```

3.2 Load Balancing

A primitive form of load balancing can be achieved in the DNS by using multiple records (such as multiple A records) for one name.

For example, if you have three WWW servers with network addresses of 10.0.0.1, 10.0.0.2 and 10.0.0.3,

3.3 Name Server Operations

3.3.1 Tools for Use With the Name Server Daemon

This section describes several indispensable diagnostic, administrative and monitoring tools available to the system administrator for controlling and debugging the name server daemon.

3.3.1.1 Diagnostic Tools

The **dig**, **host**, and **nslookup** programs are all command line tools for manually querying name servers. They differ in style and output format.

dig The domain information groper (**dig**) is the most versatile and complete of these lookup tools. It has two modes: simple interactive mode for a single query, and batch mode which executes a query for each in a list of several query lines. All query options are accessible from the command line.

```
};
options {
     default-server 127.0.0.1;
     default-key    rndc_key;
};
```

This file, if installed as `/etc/rndc.conf`, would allow the command:

```
$rndc reload
```

Chapter 4

Advanced DNS Features

4.1 Notify

DNS NOTIFY is a mechanism that allows master servers to notify their slave servers of changes to a zone's data. In response to a **NOTIFY** from a master server, the slave will check to see that its version of the zone is the current version and, if not, initiate a zone transfer.

For more information about DNS **NOTIFY**, see the description of the **notify** option in Section 6.2.16.1 and the description of the zone option **also-notify** in Section 6.2.16.7. The **NOTIFY** protocol is specified in RFC 1996.

NOTE

4.9.2 Dynamic DNS update method

To insert the keys via dynamic update:

```
% nsupdate
> ttl 3600
```

4.9.13 NSEC3 and OPTOUT

named only supports creating new NSEC3 chains where all the NSEC3 records in the zone have the same OPTOUT state. **named** supports UPDATES to zones where the NSEC3 records in the chain have mixed OPTOUT state. **named** does not support changing the OPTOUT state of an individual NSEC3 record, the entire chain needs to be changed if the OPTOUT state of an individual NSEC3 needs to be changed.

4.10 Dynamic Trust Anchor Management

BIND 9.7.0 introduces support for RFC 5011, dynamic trust anchor management. Using this feature

4.11.3.1 Patching OpenSSL

```
    (pkcs11) PKCS #11 engine support (crypto accelerator)
```

Next, run ”**apps/openssl engine pkcs11 -t**”. This will attempt to initialize the PKCS#11 engine. If it is

If you wish to generate a second key in the HSM for use as a zone-signing key, follow the same procedure above, using a different keylabel, a smaller key size, and omitting ”-f KSK” from the dnssec-keyfromlabel arguments:

(Note: When using OpenSSL-based PKCS#11 the label is an arbitrary string which identifies the key. With native PKCS#11, the label is a PKCS#11 URI string which may include other details about the key and the HSM, including its PIN. See dnssec-keyfromlabel(8) for details.)

```
$ pkcs11-keygen -b 1024 -l sample-zsk
$ dnssec-keyfromlabel -l sample-zsk example.net
```

Alternatively, you may prefer to generate a conventional on-disk key, using dnssec-keygen:

```
$ dnssec-keygen example.net
```

This provides less security than an HSM key, but since HSMs can be slow or cumbersome to use for security reasons, it may be more efficient to reserve HSM keys for use in the less frequent key-signing operation. The zone-signing key can be rolled more frequently, if you wish, to compensate for a reduction in key security. (Note: When using native PKCS#11, there is no speed advantage to using on-disk keys, as cryptographic operations will be done by the HSM regardless.)

Now you can sign the zone. (Note: If not using the -S option to **dnssec-signzone** accomplished by placing the PIN into the openssl.cnf file (in the above examples, `/opt/pkcs11/usr/ssl/openssl.cnf`).

4.12.1 Configuring DLZ

A DLZ database is configured with a **dlz** statement in named.conf:

```
    dlz example {
        database "dlopen driver.so args";
        search yes;
    };
```

This specifies a DLZ module to search when answering queries; the module is implemented in driver.so

Chapter 5

The BIND 9 Lightweight Resolver

5.1 The Lightweight Resolver Library

Traditionally applications have been linked with a stub resolver library that sends recursive DNS queries to a local caching name server.

```
ip
```

6.1.2.1 Syntax

```
/* This is a BIND comment as in C */
```

```
// This is a BIND comment as in C++
```

```
# This is a BIND comment as in common UNIX shells
# and perl
```

6.1.2.2 Definition and Usage

Comments may appear anywhere that whitespace may appear in a BIND configuration file.

C-style comments start with the two characters `/*` (slash, star) and end with `*/` (star, slash). Because they are completely delimited with these characters, they can be used to comment only a portion of a line or to span multiple lines.

acl	defines a named IP address matching list, for access control and other uses.
controls	declares control channels to be used by the **rndc** utility.
include	

6.2.8 key Statement Definition and Usage

The **key** statement defines a shared secret key for use with TSIG (see Section 4.5) or the command channel (see Section 6.2.4).

The **key**

update	Dynamic updates.
update-security	Approval and denial of update requests.
queries	Specify where queries should be logged to. At startup, specifying the category **queries** will also enable query logging unless **querylog** option has been specified. The query log entry reports the client's IP address and

`qrysent`	The number of queries the resolver sent at the `domain` zone.
`timeout`	The number of timeouts since the resolver received the last response.
`lame`	

The **listen-on** statement specifies a list of IPv4 addresses (and ports) that this instance of a lightweight

```
    [ coresize size_spec ; ]
    [ datasize size_spec ; ]
    [ files size_spec ; ]
    [ stacksize size_spec ; ]
    [ cleaning-interval number; ]
    [ heartbeatng-interval number; ]
    [number; ]
    [ acache-cleaning-interval number; ]
    [ max-acache-size size_spec ; ]
    [ max-recursion-depth number ; ]
    [ max-recursion-queries number ; ]
    [ masterfile-format
            (text|raw|map) ; ]
    [ empty-server name ; ]
    [ empty-contact name ; ]
    [ empty-zones-enable yes_or_no ; ]
    [ disable-empty-zone zone_name ; ]
    [ zero-no-soa-ttl yes_or_no ; ]
    [ zero-no-soa-ttl-cache yes_or_no ; ]
    [ resolver-query-timeout number ; ]
    [ deny-answer-addresses { address_match_list } [ except-from { namelist } ];]
    [ deny-answer-aliases { namelist } [ except-from { namelist } ];]
    [ prefetch number [number] ; ]

    [ rate-limit {
        [ responses-per-second number ; ]
        [ referrals-per-second number ; ]
        [ nodata-per-second number ; ]
        [ nxdomains-per-second number ; ]
        [ errors-per-second number ; ]
        [ all-per-second number ; ]
        [ window number ; ]
        [ log-only yes_or_no ; ]
        [ qps-scale number ; ]
        [ ipv4-prefix-length number ; ]
        [ ipv6-prefix-length number ; ]
        [ slip number ; ]
        [ exempt-clients  { address_match_list } ; ]
        [ max-table-size number ; ]
        [ min-table-size number ; ]
    } ; ]
    [ response-policy {
        zone zone_name
        [ policy (given | disabled | passthru | drop |
                  nxdomain | nodata | cname domain) ]
        [ recursive-only yes_or_no ]
        [ max-policy-ttl number ]
        ; [...]
    } [ recursive-only yes_or_no ]
      [ max-policy-ttl number ]
      [ break-dnssec yes_or_no ]
      [ min-ns-dots number ]
      [ qname-wait-recurse yes_or_no ]
    ; ]
};
```

6.2.16 options Statement Definition and Usage

The **options** statement sets up global options to be used by BIND. This statement may appear only once in a configuration file. If there is no **options** statement, an options block with each option set to its default will be used.

attach-cache Allows multiple views to share a single cache database. Each view has its own cache

6.2.16.3 Dual-stack Servers

Dual-stack servers are used as servers of last resort to work around problems in reachability due the lack of support for either IPv4 or IPv6 on the host machine.

dual-stack-servers Specifies host names or addresses of machines with access to both IPv4 and IPv6 transports. If a hostname is used, the server must be able to resolve the name using only the transport it has. If the machine is dual stacked, then the **dual-stack-servers** have no effect unless access to a transport has been disabled on the command line (e.g. **named -4**).

allow-query-cache-on Specifies which local addresses can give answers from the cache. If not specified, the default is to allow cache queries on any address, **localnets**

There are circumstances in which **named** will not preserve the case of owner names of records: if a zone file defines records of different types with the same name, but the capitalization of the name is different (e.g., "www.example.com / A" and "WWW.EXAMPLE.COM / AAAA"), then all responses for that name will use the *first* version of the name that was used in the zone file. This

NOTE

The address specified in the

alt-transfer-source An alternate transfer source if the one listed in **transfer-source** fails and **use-alt-transfer-source** is set.

> NOTE
>
> If you do not wish the alternate transfer source to be used, you should set **use-alt-transfer-source** appropriately and you should not depend upon getting an answer back to the first refresh query.

tcp-clients The maximum number of simultaneous client TCP connections that the server will accept. The default is `100`.

clients-per-query, max-clients-per-query

interface-interval The server will scan the network interface list every **interface-interval** minutes. The default is 60 minutes. The maximum value is 28 days (40320 minutes). If set to 0, interface scanning will only occur when the configuration file is loaded. After the scan, the server will begin listening for queries on any newly discovered interfaces (provided they are allowed by the **listen-on** configuration), and will stop listening on interfaces that have gone away.

- 72.100.IN-ADDR.ARPA
- 73.100.IN-ADDR.ARPA
- 74.100.IN-ADDR.ARPA
- 75.100.IN-ADDR.ARPA
- 76.100.IN-ADDR.ARPA
- 77.100.IN-ADDR.ARPA
- 78.100.IN-ADDR.ARPA
- 79.100.IN-ADDR.ARPA
- 80.100.IN-ADDR.ARPA
- 81.100.IN-ADDR.ARPA
- 82.100.IN-ADDR.ARPA
- 83.100.IN-ADDR.ARPA
- 84.100.IN-ADDR.ARPA
- 85.100.IN-ADDR.ARPA
- 86.100.IN-ADDR.ARPA
- 87.100.IN-ADDR.ARPA
- 88.100.IN-ADDR.ARPA
- 89.100.IN-ADDR.ARPA
- 90.100.IN-ADDR.ARPA
- 91.100.IN-ADDR.ARPA
- 92.100.IN-ADDR.ARPA
- 93.100.IN-ADDR.ARPA
- 94.100.IN-ADDR.ARPA
- 95.100.IN-ADDR.ARPA
- 96.100.IN-ADDR.ARPA
- 97.100.IN-ADDR.ARPA
- 98.100.IN-ADDR.ARPA
- 99.100.IN-ADDR.ARPA
- 100.100.IN-ADDR.ARPA
- 101.100.IN-ADDR.ARPA
- 102.100.IN-ADDR.ARPA
- 103.100.IN-ADDR.ARPA
- 104.100.IN-ADDR.ARPA
- 105.100.IN-ADDR.ARPA
- 106.100.IN-ADDR.ARPA
- 107.100.IN-ADDR.ARPA
- 108.100.IN-ADDR.ARPA
- 109.100.IN-ADDR.ARPA
- 110.100.IN-ADDR.ARPA

-

NOTE

max-acache-size

the mapping is legitimate or not within the DNS. The ”rebinding” attack must primarily be protected at the application that uses the DNS. For a large site, however, it may be difficult to protect all possible applications at once. This filtering feature is provided only to help such an operational environment; it is generally discouraged to turn it on unless you are very sure you have no other choice and the attack is a real threat for your applications.

Care should be particularly taken if you want to use this option for addresses within 127.0.0.0/8. These

zones should appear first, because they will often not be logged if a higher precedence trigger is found first.

PASSTHRU, DROP, TCP-Only, NXDOMAIN, NODATA override with the corresponding per-record policy.

CNAME domain causes all RPZ policy records to act as if they were ”cname domain” records.

```
; redirect x.bzone.domain.com to x.bzone.domain.com.garden.example.com
*.bzone.domain.com      CNAME   *.garden.example.com.
```

6.2.27 zone Statement Grammar

```
zone zone_name [class] {
    type master;
    [ allow-query { address_match_list }; ]
    [ allow-query-on { address_match_list }; ]
    [ allow-transfer { address_match_list }; ]
    [ allow-update { address_match_list }; ]
    [ update-check-ksk yes_or_no; ]
    [ dnssec-dnskey-kskonly yes_or_no; ]
    [ dnssec-loadkeys-interval number; ]
    [ update-policy local | { update_policy_rule [...] }; ]
    [ also-notify { ip_addr [port ip_port] [dscp ip_dscp] ;
                  [ ip_addr [port ip_port] [dscp ip_dscp] ; ... ] }; ]
    [ check-names (warn|fail|ignore) ; ]
    [ check-mx (warn|fail|ignore) ; ]
    [ check-wildcard yes_or_no; ]
    [ check-spf ( warn | ignore ); ]
    [ check-integrity yes_or_no ; ]
    [ dialup dialup_option ; ]
    [ file string ; ]
    [ masterfile-format (text|raw|map) ; ]
    [ journal string ; ]
    [ max-journal-size size_spec; ]
    [ forward (only|first) ; ]
    [ forwarders { [ ip_addr [port ip_port] [dscp ip_dscp] ; ... ] }; ]
    [ ixfr-base string ; ]
    [ ixfr-from-differences yes_or_no; ]
    [ ixfr-tmp-file string ; ]
    [ request-ixfr yes_or_no ; ]
    [ maintain-ixfr-base yes_or_no ; ]
    [ max-ixfr-log-size number ; ]
    [ max-.3985wt1isia; 0onds ]
```

```
zone zone_name [class] {
```

`hint`	The initial set of root name servers is specified using a ”hint zone”. When the server starts up, it uses the root hints to find a root name server and get the most recent list of root name servers. If no hint zone is specified for class IN, the server uses a compiled-in default set of root servers hints. Classes other than IN have no built-in defaults hints.
`redirect`	

The default is `"rbt"`, BIND 9's native in-memory red-black-tree database. This database does not take arguments.

Other values are possible if additional database drivers have been linked into the server. Some sample drivers are included with the distribution but none are linked in by default.

dialup See the description of **dialup** in Section 6.2.16.1.

delegation-only

notify-source-v6 See the description of **notify-source-v6** in Section 6.2.16.7.

min-refresh-time, max-refresh-time, min-retry-time, max-retry-time See the description in Section 6.2.16.15.

ixfr-from-differences See the description of **ixfr-from-differences** in Section 6.2.16.1. (Note that the **ixfr-from-differences** `master` and

zonesub	This rule is similar to subdomain, except that it matches when the name being updated is a subdomain of the zone in which the **update-policy** statement appears. This obviates the need to type the zone name twice, and enables the use of a standard **update-policy** statement in multiple zones without modification. When this rule is used, the *name*

`6to4-self` Allow the 6to4 prefix to be update by any TCP connection from the 6to4 network or from the corresponding IPv4 address. This is intended to allow NS or DNAME RRsets to be added to the reverse tree.

NOTE

It is theoretically possible to spoof these TCP sessions.

`external` This rule allows **named** to defer the decision of whether to allow a given update to an external daemon.
The method of communicating with the daemon is specified in the *`identity`* field, the format of which is "`local:`*`path`*", where *`path`*

```
    };
};

view external {
    match-clients { any; };

    zone example.com {
        in-view internal;
    };
};
```

An **in-view** option cannot refer to a view that is configured later in the configuration file.

A **zone** statement which uses the **in-view** option may not use any other options with the exception of **forward**

A	A host address. In the IN class, this is a 32-bit IP address.

TLSA	Transport Layer Security Certificate Association. Described in RFC 6698.
TXT	Text records. Described in RFC 1035.
UID	Reserved.
UINFO	Reserved.
UNSPEC	Reserved. Historical.
URI	Holds a URI. Described in RFC 7553.
WKS	Information about which well known network services, such as SMTP, that a domain supports. Historical.
X25	Representation of X.25 network addresses. Experimental. Described in RFC 1183.

The following *classes* of resource records are currently valid in the DNS:

IN	The Internet.
CH	Chaosnet, a LAN protocol created at MIT in the mid-1970s. Rarely used for its historical purpose, but reused for BIND's built-in server information zones, e.g.,

```
2.0.0.192.IN-ADDR.ARPA. CNAME 2.0.0.0.192.IN-ADDR.ARPA.
...
127.0.0.192.IN-ADDR.ARPA. CNAME 127.0.0.0.192.IN-ADDR.ARPA.
```

6.3.7 Additional File Formats

In addition to the standard textual format, BIND 9 supports the ability to read or dump to zone files in other formats.

The `raw`

RecQryRej	**RURQ**	Recursive queries rejected.
XfrRej	**RUXFR**	Zone transfer requests rejected.
UpdateRej	**RUUpd**	Dynamic update requests rejected.
Response	**SAns**	

6.4.1.2 Zone Maintenance Statistics Counters

Symbol	*Description*
NotifyOutv4	IPv4 notifies sent.
NotifyOutv6	IPv6 notifies sent.
NotifyInv4	IPv4 notifies received.
NotifyInv6	IPv6 notifies received.
NotifyRej	Incoming notifies rejected.
SOAOutv4	IPv4 SOA queries sent.

QryRTTnn

Frequency table on round trip times (RTTs) of queries. Each **nn** specifies the corresponding frequency. In the sequence of **nn_1**, **nn_2**, ..., **nn_m**, the value of

ROpts This counter is not supported because **BIND** 9 does not care about IP options in the first place.

Chapter 7

BIND 9 Security Considerations

7.1 Access Control Lists

Some sites choose to keep all dynamically-updated DNS data in a subdomain and delegate that subdomain to a separate zone. This way, the top-level zone containing critical data such as the IP addresses of

Appendix A

Release Notes

A.1 Release Notes for BIND Version 9.10.3-P2

A.1.1 Introduction

This document summarizes changes since BIND 9.10.3:

A.1.6 Bug Fixes

- None.

A.1.7 End of Life

References

Standards

[RFC1034] *Domain Names — Concepts and Facilities*, P.V. Mockapetris, November 1987.

[RFC1035] *Domain Names — Implementation and Specification*, P. V. Mockapetris, November 1987.

[RFC974] *Mail Routing and the Domain System*, C. Partridge, January 1986.

Proposed Standards

[RFC4074] *Common Misbehaviour Against DNS Queries for IPv6 Addresses*, Y. Morishita and T. Jinmei, May 2005.

Resource Record Types

[RFC1183] *New DNS RR Definitions*, C.F. Everhart, L. A. Mamakos, R. Ullmann, and P. Mockapetris, October 1990.

[RFC1706]

DNS Operations

[RFC1033] *Domain administrators operations guide.*, M. Lottor, November 1987.

[RFC1537] *Common DNS Data File Configuration Errors*, P. Beertema, October 1993.

[RFC1912] *Common DNS Operational and Configuration Errors*, D. Barr, February 1996.

[RFC2010] *Operational Criteria for Root Name Servers.*, B. Manning and P. Vixie, October 1996.

[RFC2219] *Use of DNS Aliases for Network Services.*, M. Hamilton and R. Wright, October 1997.

Internationalized Domain Names

[RFC2825] *A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols*,

Appendix D

D.1.3 Installation

```
$ cd lib/export
$ make install
```

This will install library object files under the directory specified by the –with-export-libdir configure option (default: EPREFIX/lib/bind9), and header files under the directory specified by the –with-export-includedir configure option (default: PREFIX/include/bind9). Root privilege is normally required. "**make install**" at the top directory will do the same.

D.1.6.1 sample: a simple stub resolver utility

It sends a query of a given name (of a given optional RR type) to a specified recursive server, and prints the result as a list of RRs. It can also act as a validating stub resolver if a trust anchor is given via a set of command line options.

Usage: sample [options] server_address hostname

Options and Arguments:

-t RRtype specify the RR type of the query. The default is the A RR.

[-a algorithm] [-e] -k keyname -K keystring specify a command-line DNS key to validate the answer. For example, to specify the following-t RRtype

Appendix E

Manual pages

E.1 dig

Name

dig — DNS lookup utility

Synopsis

`+[no]rrcomments` Toggle the display of per-record comments in the output (for example, human-readable key information about DNSKEY records). The default is not to print record comments unless multiline mode is active.

`+[no]search` Use [do not use] the search list defined by the searchlist or domain directive in `resolv.conf` (if any). The search list is not used by default.

’ndots’ from `resolv.conf` (default 1) which may be overridden by *+ndots* determines if the

-a *`anchor-file`* Specifies a file from which to read DNSSEC trust anchors. The default is `/etc/bind.keys`, which is included with BIND 9 and contains trust anchors for the root zone (”`.`”) and for the ISC DNSSEC lookaside validation zone (”dlv.isc.org”).

Keys that do not match the root or DLV trust-anchor names are ignored; these key names can be overridden using the `+dlv=NAME` or `+root=NAME` options.

Note: When reading the trust anchor file, **delv** treats

`10.in-addr.arpa` and sets the query type to PTR. IPv6 addresses are looked up using nibble format under the IP6.ARPA domain.

-4 Forces **delv** to only use IPv4.

-6 Forces **delv** to only use IPv6.

QUERY OPTIONS

delv

E.4 dnssec-checkds

Name

dnssec-checkds — A DNSSEC delegation consistency checking tool.

Synopsis

This option is mandatory unless the `-f` has been used to specify a zone file, or a default key TTL was set with the `-L` to **dnssec-keygen**

When BIND 9 is built with native PKCS#11 support, the label is a PKCS#11 URI string in the format ”pkcs11:keyword=*value*[;keyword=*value*;...]” Keywords include ”token”, which identifies the

Both `.key` and `.private` files are generated for symmetric encryption algorithms such as HMAC-MD5, even though the public and private key are equivalent.

EXAMPLE

-V Prints version information.

-E *engine* Specifies the cryptographic hardware to use, when applicable.

When BIND is built with OpenSSL PKCS#11 support, this defaults to the string ”pkcs11”, which identifies an OpenSSL engine that can drive a cryptographic accelerator or hardware service module. When BIND is built with native PKCS#11 cryptography (–enable-native-pkcs11), it defaults

OPTIONS

-f Force an update of an old-format key with no metadata fields. Without this option, **dnssec-settime**

`[-R] [-r` *`randomdev`*`] [-S] [-s` *`start-time`*`] [-T` *`ttl`*`] [-t] [-u] [-v` *`level`*`]`
`[-V] [-X` *`extended end-time`*`] [-x] [-z] [-3` *`salt`*`] [-H` *`iterations`*`] [-A]`
`zonefile [key...]`

DESCRIPTION

dnssec-signzone signs a zone. It generates NSEC and RRSIG records and produces a signed version of

-H *`iterations`* When generating an NSEC3 chain, use this many iterations. The default is 10.

-A When generating an NSEC3 chain set the OPTOUT flag on all NSEC3 records and do not generate NSEC3 records for insecure delegations.

Using this option twice (i.e., `-AA`) turns the OPTOUT flag off for all records. This is useful when

Synopsis

```
dnssec-verify [-c class] [-E engine] [-I input-format] [-o origin] [-v
    level] [-V] [-x] [-z] zonefile
```

DESCRIPTION

dnssec-verify

AUTHOR

Internet Systems Consortium

E.14 named-checkconf

Name

named-checkconf — named configuration file syntax checking tool

Synopsis

-v Print the version of the **named-checkzone** program and exit.

-j When loading a zone file, read the journal if it exists. The journal file name is assumed to be the zone

-n *`mode`* Specify whether NS records should be checked to see if they are addresses. Possible modes are **"fail"** (default for **named-compilezone**), **"warn"** (default for **named-checkzone**) and **"ignore"**.

-o *`filename`* Write zone output to `filename`. If `filename` is `-` then write to standard out. This is mandatory for **named-compilezone**.

-r *`mode`*

AUTHOR

Internet Systems Consortium

E.18 named-rrchecker

Name

named-rrchecker — A syntax checker for individual DNS resource records

Synopsis

`named-rrchecker [-h] [-o` *`origin`*`] [-p] [-u] [-C] [-T] [-P]`

DESCRIPTION

named-rrchecker

DESCRIPTION

nsupdate is used to submit Dynamic DNS Update requests as defined in RFC 2136 to a name server. This allows resource records to be added or removed from a zone without manually editing the zone

server servername [port] Sends all dynamic update requests to the name server `servername`. When no server statement is provided, **nsupdate** will send updates to the master server of the correct

[update] add domain-name ttl [class] type data... Adds a new resource record with the specified *ttl*, *class* and *data*.

show Displays the current message, containing all of the prerequisites and updates specified since the last send.

send Sends the current message. This is equivalent to entering a blank line.

answer Displays the answer.

debug Turn on debugging.

version Print version number.

help Print a list of commands.

```
K{name}.+157.+{random}.key
```

`dumpdb [-all|-cache|-zone|-adb|-bad] [`*`view ...`*`]` Dump the server's caches (default) and / or zones to the dump file for the specified views. If no view is specified, all views are dumped. (See the **dump-file** option in the BIND 9 Administrator Reference Manual.)

`flush` Flushes the server's cache.

`flushname`

rently active for the given domain, and how many have been passed or dropped because of the `fetches-per-zone` option.)

`stats` Write server statistics to the statistics file. (See the **statistics-file** option in the BIND 9 Adminis-

SEE ALSO

rndc.conf(5), rndc-confgen(8), named(8), named.conf(5), ndc(8), *BIND 9 Administrator Reference Manual*.

AUTHOR

Internet Systems Consortium

E.21 `rndc.conf`

Name

`rndc.conf` — rndc configuration file

Synopsis

`rndc.conf`

DESCRIPTION

`rndc.conf` is the configuration file for **rndc**, the BIND 9 name server control utility. This file has a and HMAC-SHA512 are supported. This is followed by a secret clause which contains the base-64 en-

NAME SERVER CONFIGURATION

The name server must be configured to accept rndc connections and to recognize the key specified in the `rndc.conf` file, using the controls statement in `named.conf`

-b *`keysize`* Specifies the size of the authentication key in bits. Must be between 1 and 512 bits; the default is the hash size.

-c *`keyfile`*

-s