RED HAT SYSTEM-CONFIG-BIND
BIND (BERKELEY INTERNET NAME DOMAIN)
DNS (DOMAIN NAME SYSTEM)
CONFIGURATION TOOL
– USER GUIDE AND MANUAL –

Jason Vas Dias <jvdias@redhat.com>

Copyright (©) Red Hat Inc. 2005

Table of Contents

1 Introduction....3
  1.1 Prerequisites....3
  1.2 Files managed by system-config-bind....3
  1.3 Starting system-config-bind....3
  1.4 Installing The Initial Default BIND Configuration:....4
  1.5 Modifying an Existing BIND Configuration:....4
  1.6 Backup Files created by system-config-bind....4
  1.7 The system-config-bind BIND Configuration Display:....5
2 Importing hosts(5) files....6
  2.1 Accessing the Import Facility:....6
  2.2 Using the Import Filter Facility....6
3 The Default “Primary Master” name server....8
4 Creating New Zones....9
  4.1 Accessing the New Zone Dialog....9
    4.1.1 Zone Types, Classes and Origin Types....9
    4.1.2 master Zone Start of Authority (SOA) and Name Server (NS) Record Parameters....11
    4.1.3 Cache Time To Live (TTL) Values....11
    4.1.4 Other SOA Record Timing Parameters....12
    4.1.5 The “Authoritative Name Server” SOA parameter....12
    4.1.6 The “Responsible Person” email address SOA parameter....12
  4.2 Creating the New Zone....12
  4.3 Creating a New Slave Zone....13
  4.4 Creating a New Forward Zone....15
  4.5 Creating a new root cache hint Zone....16
  4.6 Creating a new Stub Zone:....16
  4.7 Creating a new “delegation-only” Zone....16
5 Deleting Zones....16
6 Previewing the BIND Configuration Files....17
7 Saving the modified BIND Configuration....18
  7.1 Saving the Configuration at Exit....18
  7.2 The Save Configuration dialog:....18
8 Adding Zone Database Records....19
  8.1 Automatic Generation of Corresponding PTR / (A / AAAA) records....20
9 Editing or Deletion of Zone Records....21
10 Editing Name Server and Zone Configuration Options:....21
  10.1 Editing the DNS Server Global Options....21
  10.2 Adding a New DNS Server or Zone Configuration Option:....22
  10.3 Removing an Existing DNS Server or Zone Configuration Option....23
  10.4 Editing Zone or View Configuration Options....24
11 Access Control Lists (ACLs)....25
  11.1 Creating a new Global ACL....25
12 Including a Global ACL in a Configuration Option....27
  12.1 Editing Global ACLs....28
  12.2 Deleting Global ACLs:....28
  12.3 Embedded ACLs....28
13 Transaction Signature (TSIG) Key Management....30
  13.1 Creating new TSIG Keys....30
  13.2 Referencing TSIG keys in an ACL....31
  13.3 Edit and Deletion of TSIG Keys:....32
14 Managing Zone Access Control and Options with Views....33
  14.1 Creating a View....33

- 14.2 Editing View Options:....34
- 14.3 Editing view “From” and “To” ACLs....35
- 14.4 Creating “split DNS” Views....35
- 14.5 Copying or Moving Zones between Views....36

15 Enabling Zone Authentication Security (DNSSEC)....39

- 15.1 Signing Zones....39
- 15.2 Importing Keys to Trust from another DNS server....41

16 Controlling DNS Server Logging....43

- 16.1 Creating a new Logging Channel....44
  - 16.1.1 Setting the Logging Channel Destination....44
  - 16.1.2 Specifying the File Logging Destination....45
  - 16.1.3 Specifying the syslog Channel Destination 45
  - 16.1.4 Selecting the Severity of Messages to be logged to the Channel....46
  - 16.1.5 Selecting the Message Header fields to be Printed for the Channel....46
- 16.2 Defining Logging Categories to be Output on certain Channels....46

17 Configuring DNS Server Controls....47

- 17.1 Adding a New DNS Server Control Channel....47

18 Specifying Options for Remote DNS Servers....50

- 18.1 Creating a Server object....50
- 18.2 Editing Remote Server Options....50

19 Starting, Stopping and Restarting the DNS Server....51

20 Using the Search Facility....52

21 APPENDIX A : Bug Reporting....53

1 Introduction

This document explains how to use the Red Hat **Bind Configuration Tool** (`system-config-bind`) to configure the ISC (Internet Software Consortium) BIND (Berkeley Internet Name Domain) DNS (Domain Name System) server, `named`. The Bind Configuration Tool manages `named.conf` server configuration files and zone database files.

This document assumes that you have rudimentary understanding of BIND and DNS; it does not attempt to explain the basic concepts of BIND and DNS; for this purpose, the reader is directed to the book "DNS and BIND, 4th Ed.", by Paul Albitz and Cricket Liu, O'Reilly (ISBN-596-000158-4). Nor does it attempt to be a BIND configuration reference manual; for this purpose, consult the ISC BIND Administrator's Reference Manual (ARM), installed with your Red Hat Linux BIND distribution in : /usr/share/doc/bind-${VERSION}/arm/Bv9ARM.html .

1.1 Prerequisites

Before you begin, ensure that the `bind` RPM is installed on your system:

```
# rpm -q bind
bind-9.3.1
```

The string "9.3.1" is the version of BIND you are using and the value of `${VERSION}` in the ARM link above.

Without these packages installed: `bind`, `bind-libs`, `bind-utils` – `system-config-bind` will not run.

Once the bind packages are installed, you are ready to start `system-config-bind`.

You are advised to run `system-config-bind` on a machine connected to the internet – it may need to do DNS lookups.

1.2 Files managed by `system-config-bind`

`system-config-bind` manages BIND configuration files: it provides facilities to Create, Edit and Remove them.

The BIND configuration files managed by `system-config-bind` are:

a. `named` Configuration Files:

```
$ROOTDIR/etc/named.conf
$ROOTDIR/etc/rndc.conf
```

and any named configuration files included in the above by use of the '`include`' statement;

b. Zone Database Files referenced in `named` Configuration '`zone`' statements:

```
$ROOTDIR/var/named/*
```

and any zone database files included by use of the '`$include`' zone file directive.

`$ROOTDIR` may be set (or not) in `/etc/sysconfig/named`, for example by the `bind-chroot` package, which sets it to `/var/named/chroot` .

1.3 Starting `system-config-bind`

To start the Bind Configuration Tool, ensure that the X-Window system and the GNOME or KDE Window Manager are running (the GUI Desktop is displayed on your monitor). Go to the Main Menu Button (on the Panel) and select:

```
 System Settings => Server Settings => Domain Name Service
```

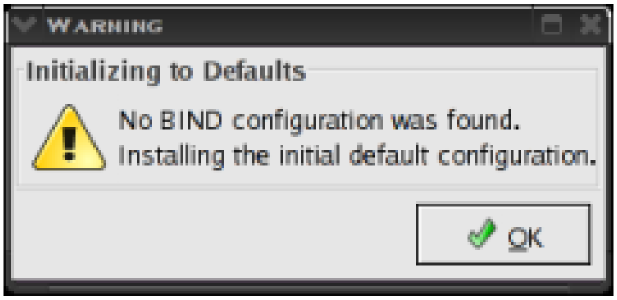
or type this command at a shell prompt (for example, in an XTerm or GNOME-terminal):

```
# system-config-bind
```

If you do not run this command as the '`root`' user, you will be prompted for the root user password - `system-config-bind` can only be run as `root` .

1.4 Installing The Initial Default BIND Configuration:

If you do not have any BIND configuration files setup when `system-config-bind` runs, you will be prompted to allow installation of an initial BIND configuration:



Initializing to Defaults

No BIND configuration was found.
Installing the initial default configuration.

Click <OK> to enable installation of the default BIND configuration. This is very similar to the BIND configuration obtained by installation of the `caching-nameserver` package, and configures `named` to be a Caching Only nameserver .

1.5 Modifying an Existing BIND Configuration:

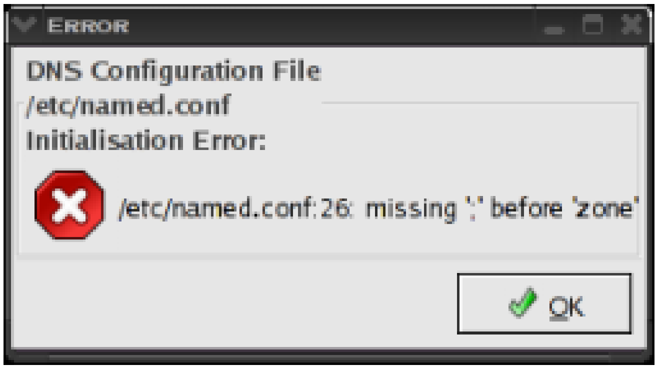
Valid BIND configuration files existing when `system-config-bind` is started up are read into the configuration.

`system-config-bind` will preserve formatting and comments in existing BIND configuration files after it is used to modify and save them .

If existing BIND configuration files contain syntax errors that would not allow `named` to use them, `system-config-bind` will not read in the configuration and will prompt you to correct the errors before continuing. For example, if your existing named.conf file contains the erroneous zone declarations:

```
zone “example1.com” { file “example1.com.db”; }
zone “example2.com” { file “example2.com.db”; }
```

`system-config-bind` will present a dialog informing you of the error and will not proceed further:



DNS Configuration File
/etc/named.conf
Initialisation Error:

/etc/named.conf:26: missing ';' before 'zone'

If you are presented with a dialog like this when `system-config-bind` starts, you must either correct the errors or remove the existing configuration files to proceed.

1.6 Backup Files created by `system-config-bind`

When you modify BIND configuration files with `system-config-bind` and save them, it will create backups of the files before the modification whose names will end with the date and time the modification was made, for example:

```
named.conf.2005-1-1_12.0.0
```

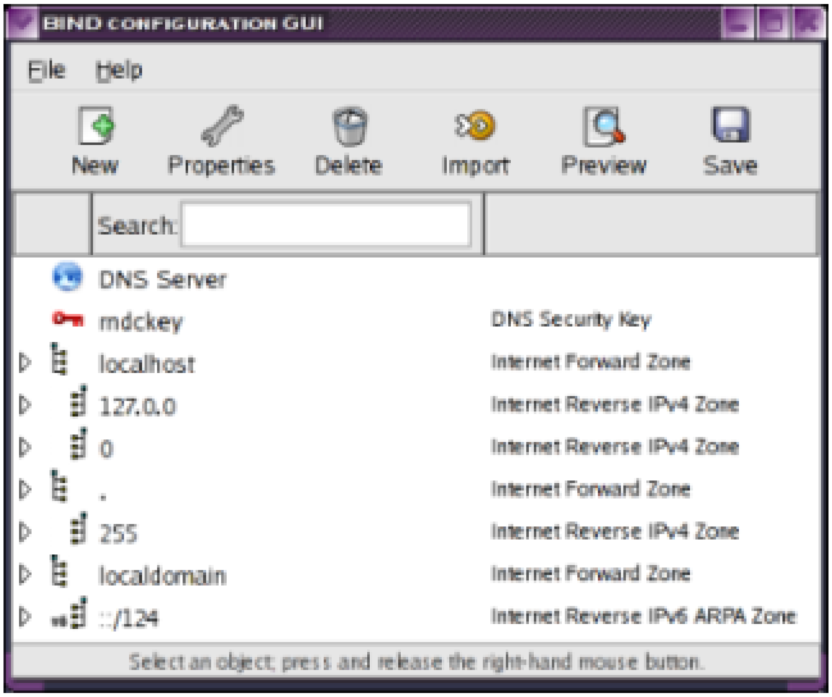
Before `system-config-bind` saves any modified configuration file, it will perform the same checks it does at startup; if for any reason those checks should fail (and they should not!), it will NOT modify the original file, but will save the erroneous file in a backup whose name will end in '`.REJECT.`' followed by the timestamp, as in:

```
named.conf.REJECT.2005-1-1_12.0.0
```

If you ever get any of these files generated please report them as a bug as described in the “Bug Reporting” section below.

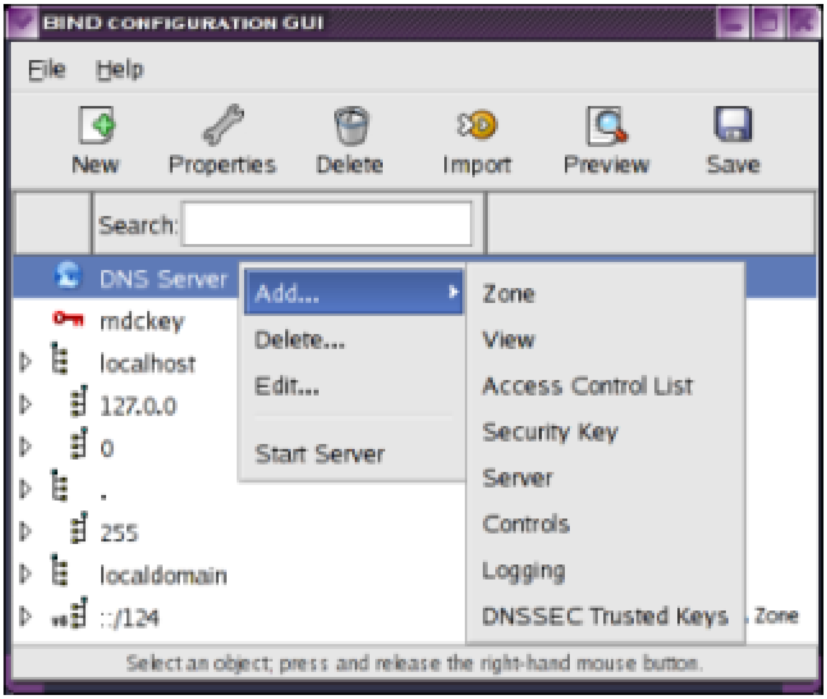
1.7 The system-config-bind BIND Configuration Display:

Once `system-config-bind` starts up, you are then presented with the `system-config-bind` main window, here showing the default initial configuration:


BIND CONFIGURATION GUI
File
Help
New
Properties
Delete
Import
Preview
Save
Search:
DNS Server
mdckey DNS Security Key
localhost Internet Forward Zone
127.0.0 Internet Reverse IPv4 Zone
0 Internet Reverse IPv4 Zone
. Internet Forward Zone
255 Internet Reverse IPv4 Zone
localdomain Internet Forward Zone
::/124 Internet Reverse IPv6 ARPA Zone
Select an object; press and release the right-hand mouse button.

You can access Menus for appropriate functionality by selecting any object in the list, then pressing and releasing the right–hand mouse button.

For example, to access functionality pertinent to global DNS server configuration, click and release the right–hand mouse button on the "DNS Server" icon:

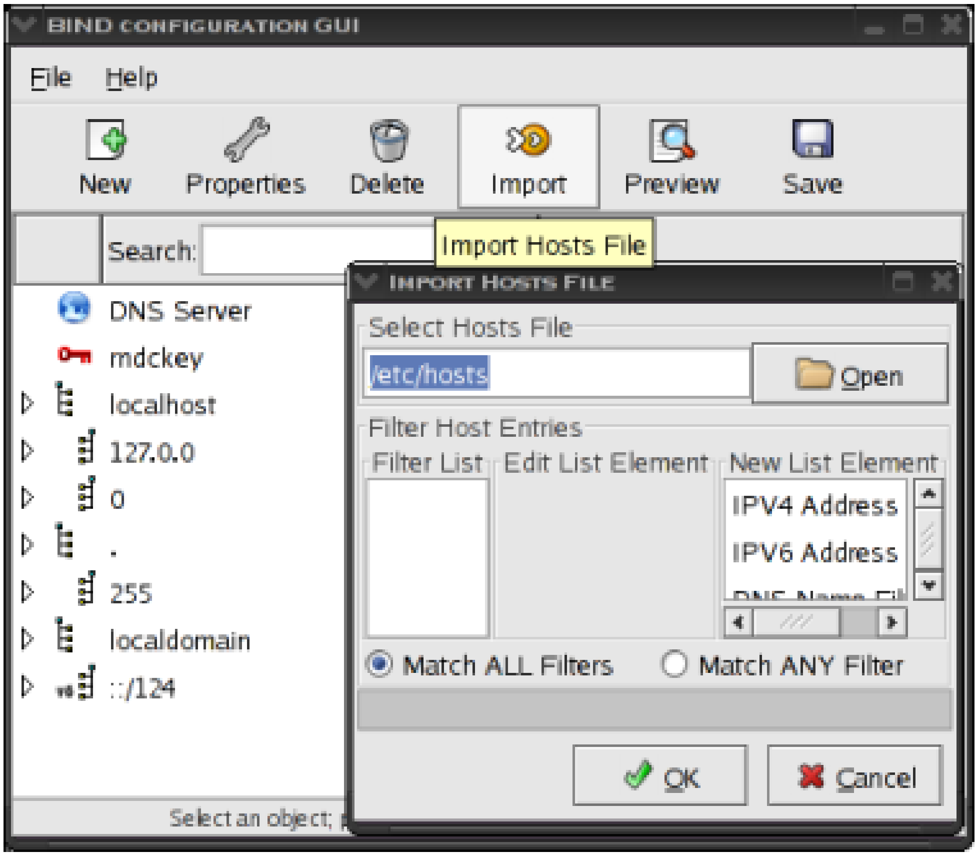


2 Importing `hosts(5)` files

You can use `system-config-bind` to import `hosts(5)` database text files formatted as documented in the `hosts(5)` manual page, to transfer your file based host name to address mappings into the DNS .

2.1 Accessing the Import Facility:

Click on the "Import" button in the Tool Bar. You are then presented with the Import Dialog:



Select Hosts File: /etc/hosts
Open

● Match ALL Filters ○ Match ANY Filter

2.2 Using the Import Filter Facility

Suppose the `hosts` file you want to import looks like this:

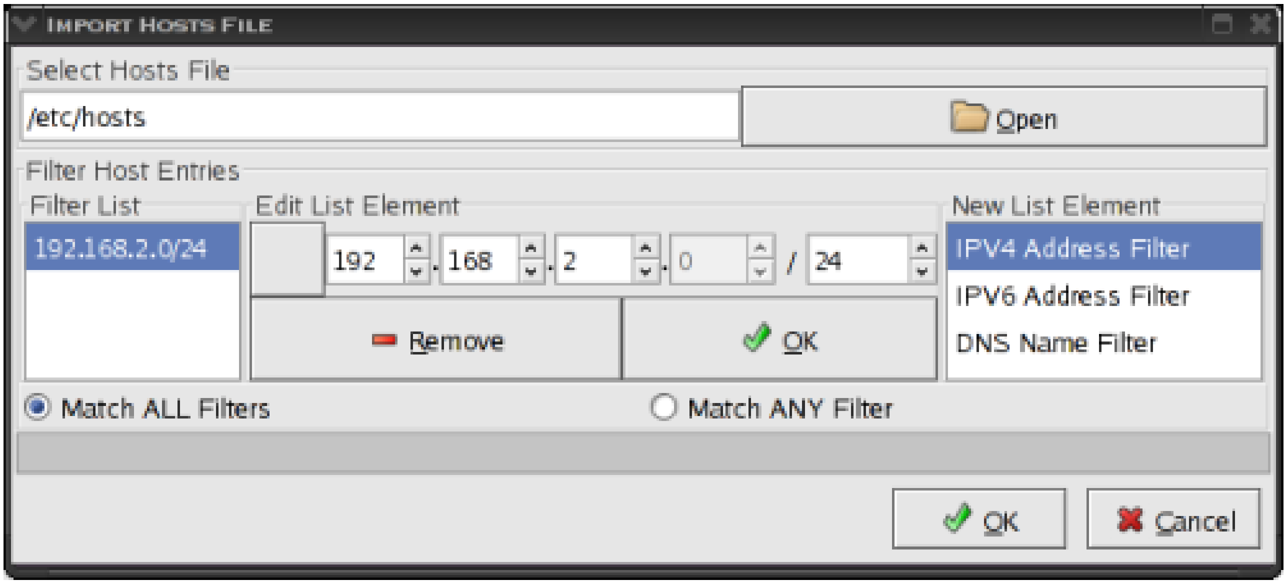
```
127.0.0.1       localhost.localdomain   localhost
192.168.2.1     hosta.example.com       hosta
192.168.2.2     hostb.example.com       hostb
192.168.2.3     hostc.example.com       hostc
192.168.2.4     hostd.example.com       hostd
192.168.2.5     hoste.example.com       hoste
192.168.2.6     hostf.example.com       hostf
192.168.2.7     hostg.example.com       hostg
192.168.2.8     hosth.example.com       hosth
66.187.224.20   download.fedora.redhat.com   fedora
209.132.176.20  download.fedora.redhat.com   fedora
2001:503:231d::2:30 b.gtld-servers.net       root-b
192.33.14.30    b.gtld-servers.net           root-b
```

and you want to import only the hosts in the "example.com" domain . Use the Filter facility in the Import Dialog to select only the hosts with addresses in subnet 192.168.2/24, or which end with example.com:

1 Select the "IPV4 Address" element in the "New List Element" list of the "Filter Host Entries" frame

2 Enter the IPv4 subnet prefix 192.168.2/24

3 Click on the "OK" button in the "Edit List Frame", then on the dialog "OK" button .



Select Hosts File: /etc/hosts

Filter List: 192.168.2.0/24

Edit List Element: 192 . 168 . 2 . 0 / 24

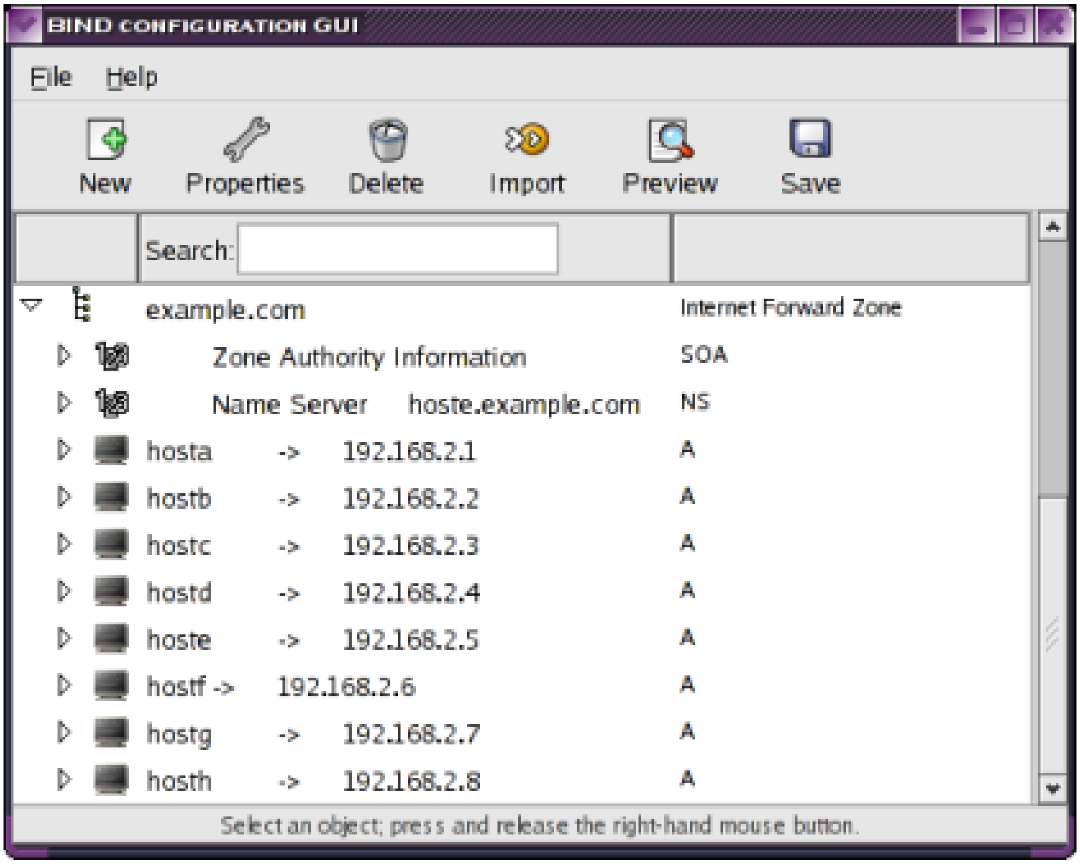
● Match ALL Filters ○ Match ANY Filter

To use a hosts file that is not “/etc/hosts”, you can type in a path in the entry or select a different hosts file by clicking the “Open” button and completing the file selection dialog in the “Select Hosts File” frame .

The button just before the '192' entry above is the “Not” button – if pressed, it will display the “!” character and the Filter will be negated – it will select the complement of the set of entries selected without the “Not” button having been pressed.

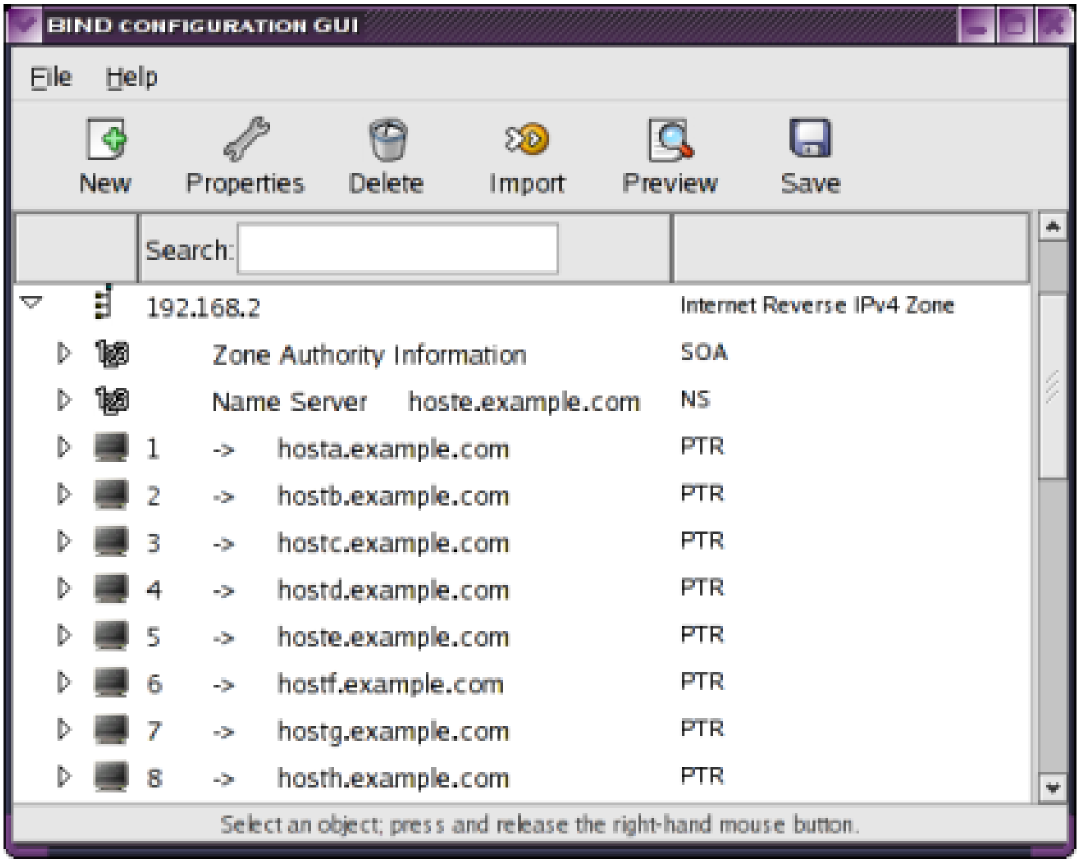
By default, ALL filters in the list must match an entry for that entry to be included in the selected set; select the “Match Any Filter” radio button to specify that a match of an entry against ANY filter will include it in the selected set .

If you then click on OK, the following Zones will be imported:



```
example.com                                    Internet Forward Zone
    Zone Authority Information                 SOA
    Name Server     hoste.example.com          NS
    hosta    ->    192.168.2.1                 A
    hostb    ->    192.168.2.2                 A
    hostc    ->    192.168.2.3                 A
    hostd    ->    192.168.2.4                 A
    hoste    ->    192.168.2.5                 A
    hostf -> 192.168.2.6                       A
    hostg    ->    192.168.2.7                 A
    hosth    ->    192.168.2.8                 A
```

Select an object; press and release the right-hand mouse button.



192.168.2			Internet Reverse IPv4 Zone
Zone Authority Information			SOA
Name Server		hoste.example.com	NS
1	->	hosta.example.com	PTR
2	->	hostb.example.com	PTR
3	->	hostc.example.com	PTR
4	->	hostd.example.com	PTR
5	->	hoste.example.com	PTR
6	->	hostf.example.com	PTR
7	->	hostg.example.com	PTR
8	->	hosth.example.com	PTR

Select an object; press and release the right-hand mouse button.

In this case, the same import would have resulted from a "Filter List" consisting of the "DNS Name Filter" of "example.com", or from a "Filter List" of:

```
!127.0.0.0/8   ( IPV4 Address Filter )
!66.0.0.0/8    ( IPV4 Address Filter )
!209/8         ( IPV4 Address Filter )
!192.33/16     ( IPV4 Address Filter )
!2001::/16     ( IPV6 Address Filter )
```

3 The Default "Primary Master" name server

Because the local host on which `system-config-bind` is running in the example above had an active interface address of "192.168.2.5" , the "primary master" nameserver, ie. the **authoritative** name server, of the new zones was set to "hoste.example.com", which has this IPv4 address configured on an active interface.

`system-config-bind` will always try to find the default primary master nameserver to use for new zones as follows:

1 If the output of the `hostname(1)` command resolves to a fully-qualified domain name, that name will be used

2 The first active ("UP") IP interface (as listed by the `ifconfig(8)` command) which has an IPv4 address with an associated DNS PTR record, looked up according to the rules described in `resolver(5)` .

3 If none of the above can be found, then "`localhost.localdomain`" (127.0.0.1) .

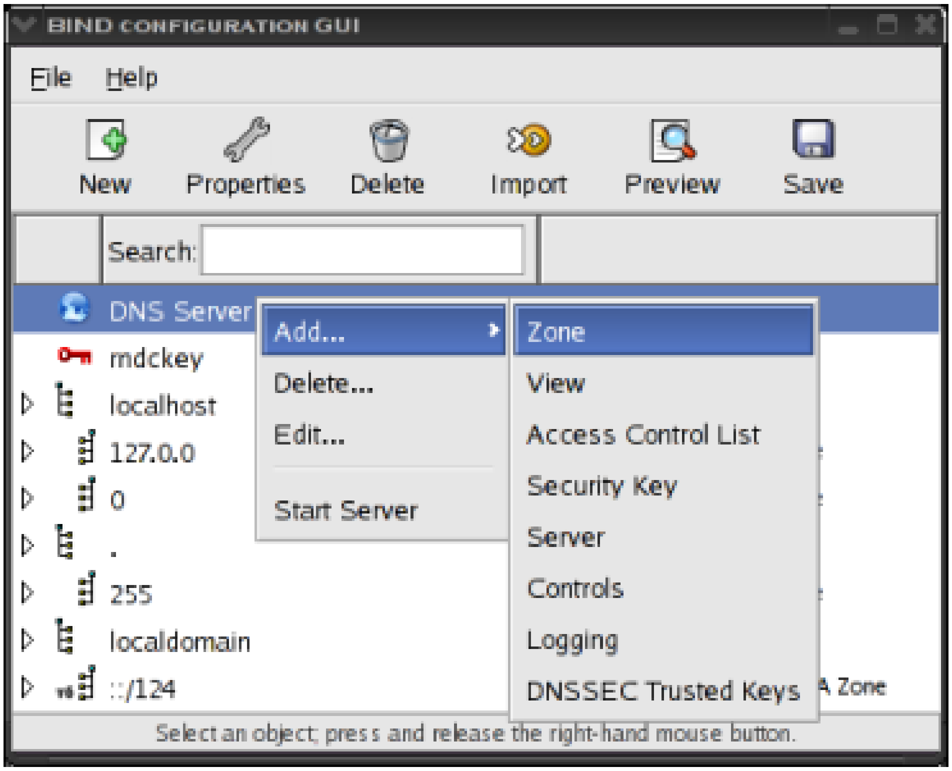
If you wish to use a primary master nameserver other than the default for new zones, you can change the value when creating new zones, or by editing the "Start of Authority" (SOA) and "Nameserver" (NS) records of existing zones, as described below – or set the hostname of the machine so it resolves with DNS by the procedure above .

Note that for DNS to work properly, the authoritative nameserver name for a zone must resolve in DNS to the address of the nameserver serving that zone.

4 Creating New Zones

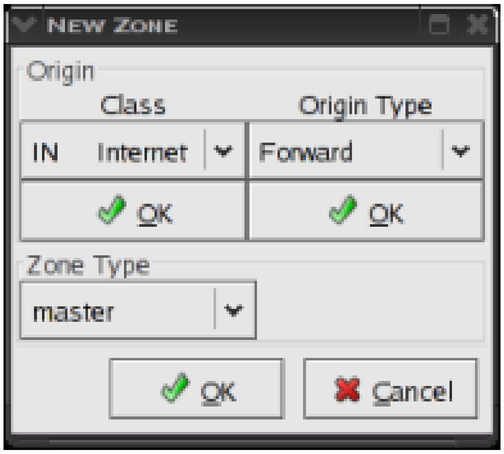
4.1 Accessing the New Zone Dialog

To create a new zone, either ensure no object is selected or select the 'DNS Server' object in the list, and click on the "New" button or press and release the right-hand mouse button and select the "Add" option of the popup menu:



Select an object; press and release the right-hand mouse button.

The "New Zone" dialog is displayed:



Origin

Class: IN Internet

Origin Type: Forward

Zone Type: master

4.1.1 Zone Types, Classes and Origin Types

`System-config-bind` supports creation of these zone and origin types:

Zone Origin Types:

Forward	The Zone Origin is a DNS Name and the Zone maps Names to Addresses
IPV4 Reverse	The Zone Origin is an IPv4 class A, B or C subnet prefix and the Zone maps IPv4 Addresses to Names
IPV6 Reverse	The Zone Origin is an IPv6 subnet prefix of hexadecimal (hex) 4-bit numbers (nibbles)
NSAP Reverse	The Zone Origin is an OSI NSAP subnet prefix of hex nibbles

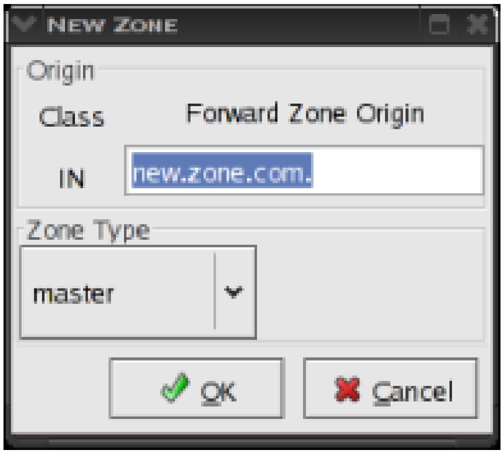
Zone Types:

master	This DNS server is authoritative for this zone and the zone file database is created locally
slave	This DNS server is authoritative for this zone, but the zone database resides on another DNS server which has the “master” type set for this zone; this server must perform Zone Transfers to access it.
stub	A slave zone which replicates only the Name Server records from the master
forward	All queries for this zone are to be forwarded to other DNS servers specified in a list of DNS servers
hint	The contents of this database specify the initial contents of `named`'s cache, usually the '.' domain servers
delegation-only	This zone may contain only SOA and NS records for sub zone servers

Zone Classes:

IN	Internet: the default zone class for Internet Data
HS	Hesiod : the zone class for Hesiod data
CH	ChaosNet: the zone class for ChaosNet data

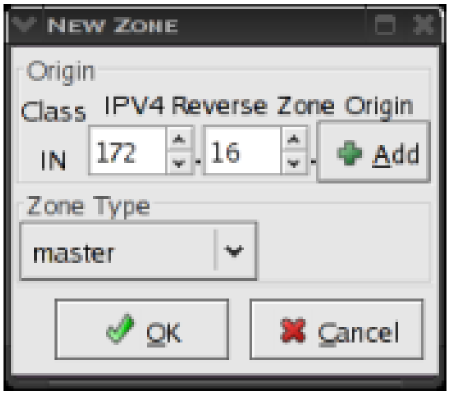
Select the Zone Class and Origin Type by choosing option values from the option lists and pressing the OK buttons beneath them. Select the Zone Type from the Zone Type option list. Type in the new zone origin in the Zone Origin entry field that appears:



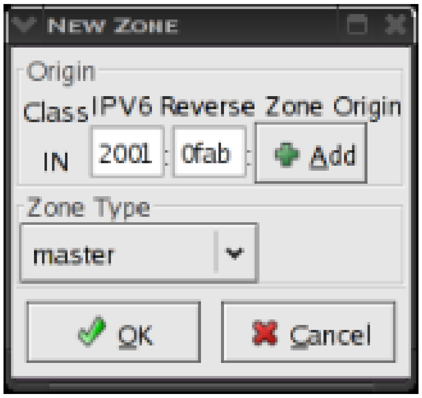
Class: IN
Forward Zone Origin: new.zone.com.
Zone Type: master

If you are creating a Forward zone, the zone origin must be absolute – it must end with a “.” – you will be prompted to allow the addition of a “.” if the zone origin you entered is not absolute.

For Reverse zones, enter only the address prefix common to all names in the zone, composed of decimal octets (8-bit numbers) for IPv4 addresses, and hexadecimal nibbles for IPv6 addresses – click the “Add” button to add more octets or nibbles to the origin:



Class: IN
IPV4 Reverse Zone Origin: 172 . 16
Zone Type: master

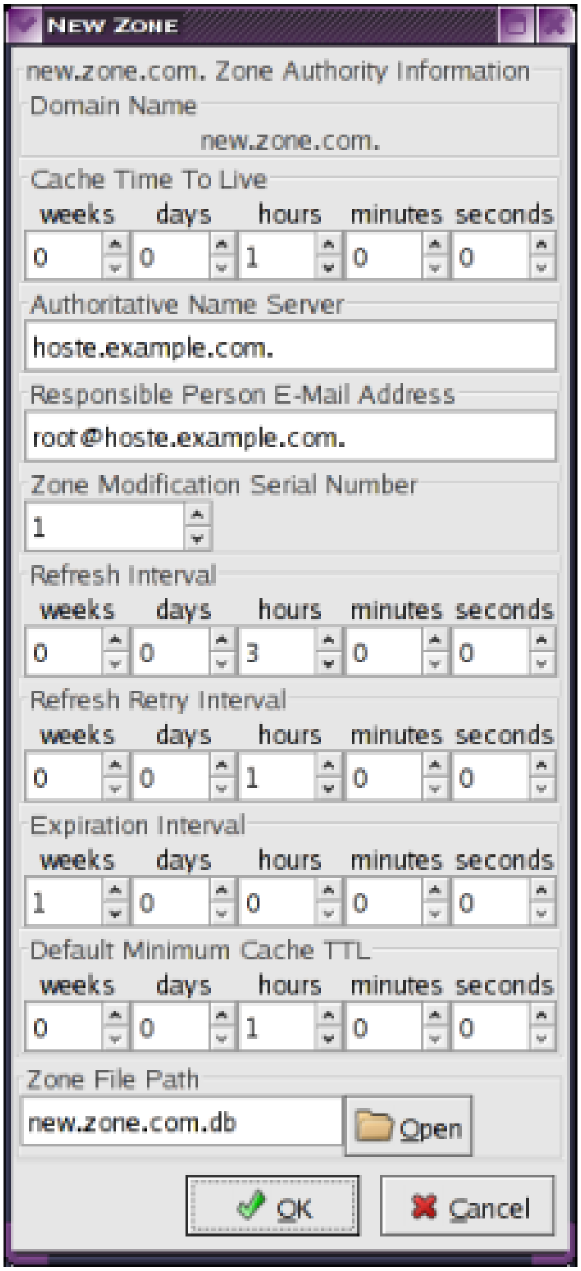


Class: IN
IPV6 Reverse Zone Origin: 2001 : 0fab
Zone Type: master

You do not always need to create corresponding Forward or Reverse zones – using the Automatic Generation feature when creating A or AAAA Name to Address mapping record in a Forward Zone will automatically create the Reverse Zone and PTR record, or when creating a PTR address to Name mapping record in a Reverse Zone, it will automatically create the corresponding Forward Zone A or AAAA record , as described below .

4.1.2 master Zone Start of Authority (SOA) and Name Server (NS) Record Parameters

Having filled in the Zone Class, Origin and Type as above, and pressing the "OK" button, you will be presented with the Zone Creation dialog for your new Zone, filled out with default parameters as shown :



new.zone.com. Zone Authority Information

Domain Name: new.zone.com.

	weeks	days	hours	minutes	seconds
Cache Time To Live	0	0	1	0	0

Authoritative Name Server: hoste.example.com.

Responsible Person E-Mail Address: root@hoste.example.com.

Zone Modification Serial Number: 1

	weeks	days	hours	minutes	seconds
Refresh Interval	0	0	3	0	0
Refresh Retry Interval	0	0	1	0	0
Expiration Interval	1	0	0	0	0
Default Minimum Cache TTL	0	0	1	0	0

Zone File Path: new.zone.com.db

4.1.3 Cache Time To Live (TTL) Values

Each record in a BIND Zone database has an associated Time To Live (TTL) : the maximum time that the record will reside in a querying name server's cache before it can be flushed from the cache and the next query for the record will go to the authoritative nameserver, not be served from the cache. The TTL values for each record can be set individually or from defaults configured at Zone creation time in the Zone Start of Authority (SOA) record, which specifies the "MINIMUM" "Default Minimum Cache TTL" record TTL value.

BIND differs slightly from RFC 1035 in this respect: it interprets the SOA "MINIMUM" value not as being the default TTL for records that do not specify a TTL, but as being the "Negative Caching TTL", the length of time querying servers are to cache NXDOMAIN responses from this server. It also enforces that each zone file must begin with a $TTL directive that specifies the default TTL for records that do not specify a TTL.

`system-config-bind` creates the $TTL directive beginning each new zone file specifying the TTL value from the "Default Minimum Cache TTL" field in the SOA record.

The initial Zone SOA “MINIMUM” value thus becomes the default TTL value for every record that does not explicitly specify a TTL value.

By default, `system-config-bind` sets the default minimum TTL to be 1 hour . This also specifies the limit on how fast data in the zone can change: servers which have zone data in their cache will not pick up new zone data until data in the zone has expired. You can explicitly flush the cache using the ‘`rndc flush`’ command .

The SOA record itself has a TTL value that can be specified; by default, this is set to the default $TTL value.

4.1.4 Other SOA Record Timing Parameters

Refresh Interval : The maximum time that must elapse before all TTLs in cached zone data are considered expired and the zone must be refreshed by querying the authoritative server.

Refresh Retry Interval: The minimum time that must elapse before a failed refresh attempt should be retried

Expiration Interval: The maximum time that must elapse before the cached zone data is no longer considered authoritative.

4.1.5 The “Authoritative Name Server” SOA parameter

This specifies the DNS name of the DNS server serving the zone . By default, this is set to the DNS name of the local host, determined as described in Section 3 above . A Nameserver (NS) record will be created in the new zone for this server.

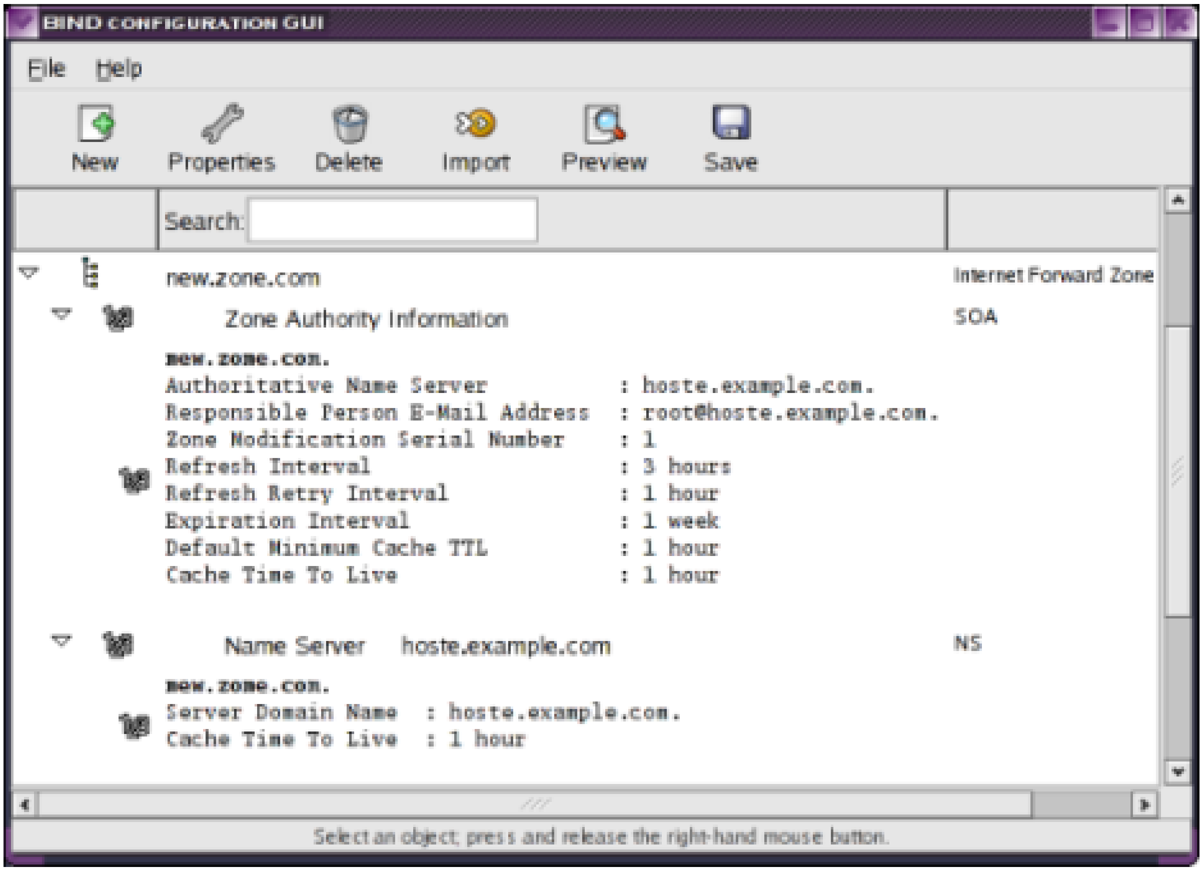
4.1.6 The “Responsible Person” email address SOA parameter

Each SOA record must specify an administrative contact to which mail regarding the Zone can be directed by DNS users .

By default, this is set to “root@<name server>”, where <name server> is the authoritative nameserver for the new zone.

4.2 Creating the New Zone

Once you are satisfied with the values of the Zone SOA and primary nameserver parameters, Click on the “OK” button to create the zone. It will then appear in the Zone List:



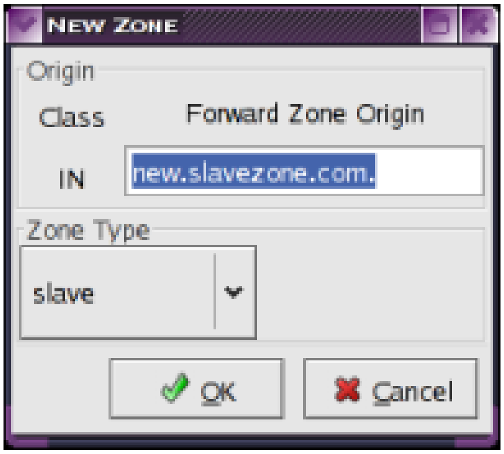
```
new.zone.com                                      Internet Forward Zone
    Zone Authority Information                    SOA
    new.zone.com.
    Authoritative Name Server          : hoste.example.com.
    Responsible Person E-Mail Address  : root@hoste.example.com.
    Zone Modification Serial Number    : 1
    Refresh Interval                   : 3 hours
    Refresh Retry Interval             : 1 hour
    Expiration Interval                : 1 week
    Default Minimum Cache TTL          : 1 hour
    Cache Time To Live                 : 1 hour

    Name Server    hoste.example.com                NS
    new.zone.com.
    Server Domain Name  : hoste.example.com.
    Cache Time To Live  : 1 hour
```

4.3 Creating a New Slave Zone

To create a slave zone, there must be a DNS server with the “master” copy of the zone which has the “allow-transfer” option for the zone set to an Access Control List (ACL) that includes the DNS server on which you want to add the slave zone – see the section on “Editing Zone Options” below .

Access the “New Zone” dialog as described in section 4.1 above. Choose the “slave” zone type:

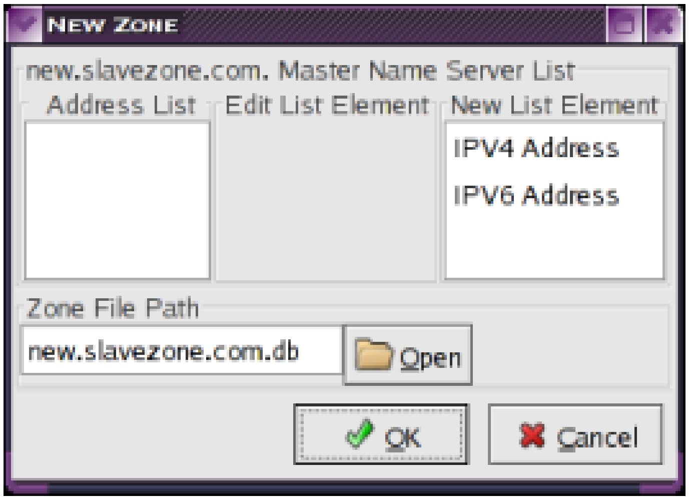


Class: IN

Forward Zone Origin: new.slavezone.com.

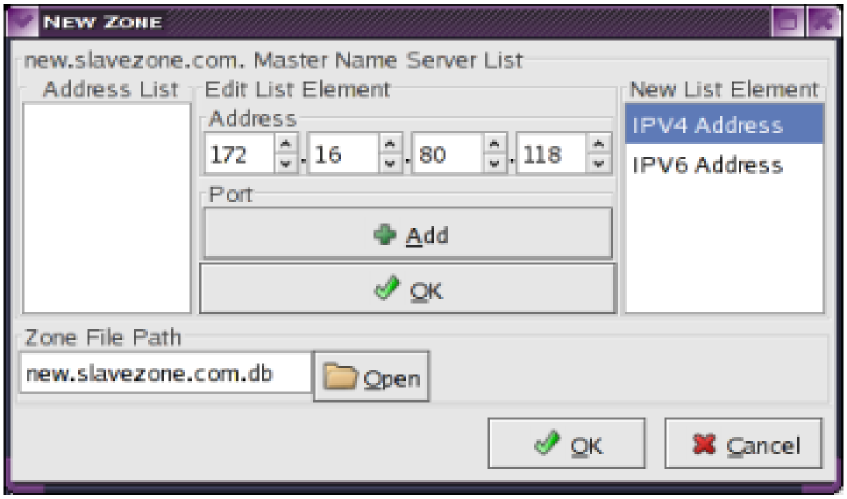
Zone Type: slave

Choose the appropriate zone Class, and type in the Origin of the slave zone; then click on the “OK” button . The New Slave Zone dialog is displayed:



Zone File Path: new.slavezone.com.db

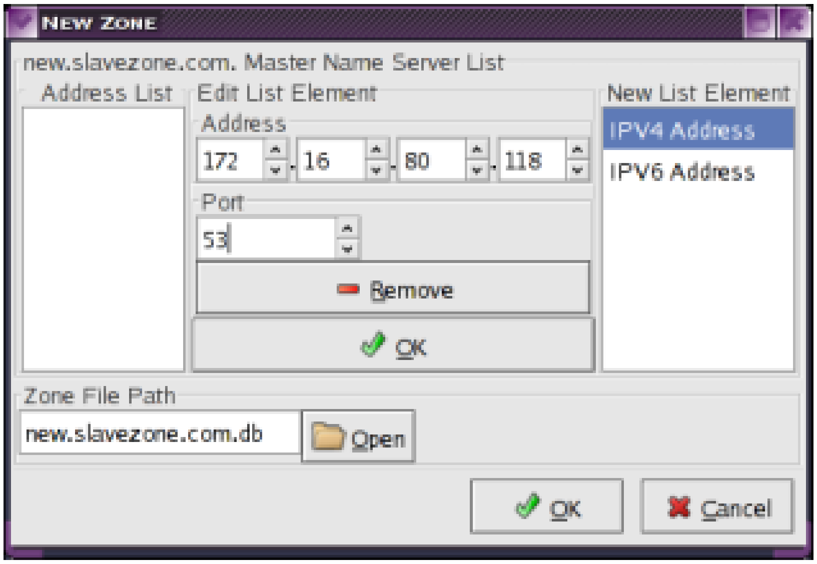
You must enter a non-empty list of master DNS servers for the zone. Select the type of address (IPV4 or IPV6) of your master server in the right hand list and enter the address details in the “Edit List Element” frame;



Address: 172 . 16 . 80 . 118

Zone File Path: new.slavezone.com.db

If your master name server listens on a different port other than the default "domain" port (53) you'll need to specify it by clicking on the "Add" button in the Port frame:



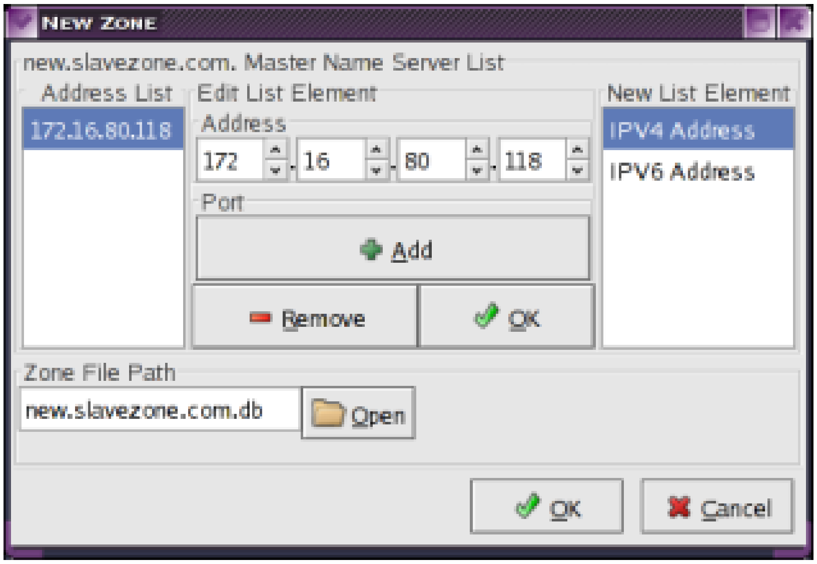
new.slavezone.com. Master Name Server List

Address: 172 . 16 . 80 . 118

Port: 53

Zone File Path: new.slavezone.com.db

Once you are satisfied with the address and Port settings, click on the "OK" button in the "Edit List Element" frame to add the master server to the Address List:



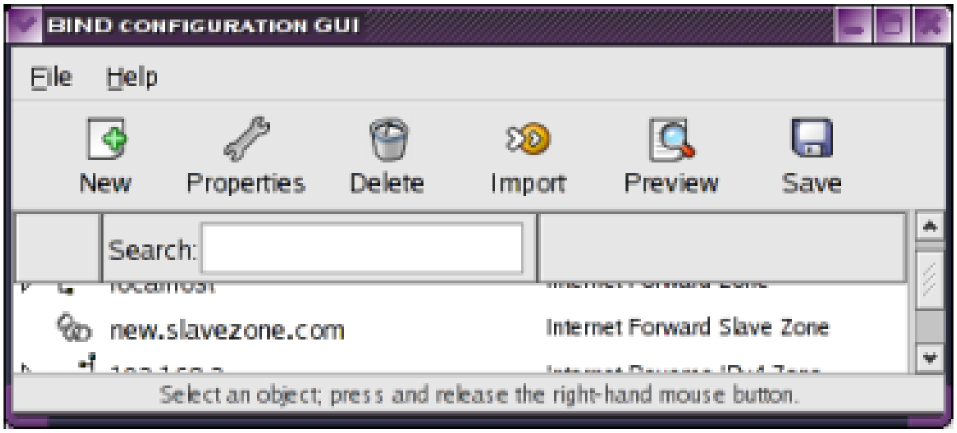
new.slavezone.com. Master Name Server List

Address List: 172.16.80.118

Address: 172 . 16 . 80 . 118

Zone File Path: new.slavezone.com.db

Once you are satisfied with the last of master servers, click on the main dialog "OK" button. The new slave zone will then be added to the configuration:



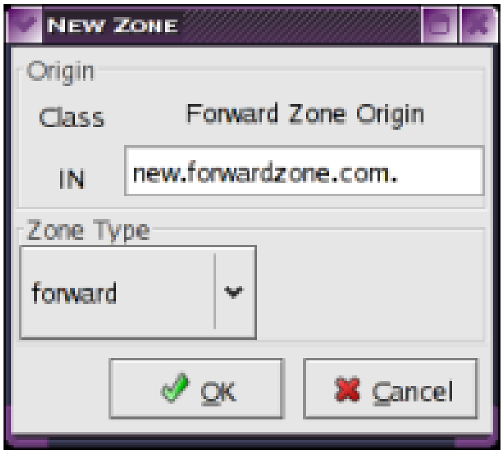
new.slavezone.com Internet Forward Slave Zone

Select an object; press and release the right-hand mouse button.

4.4 Creating a New Forward Zone

You can create Forward zones to specify that all queries for those zones received by this DNS server are to be forwarded to a list of "forwarder" DNS servers as follows.

Access the "New Zone" dialog as described in section 4.1 above . Choose the "forward" zone type:



New Zone

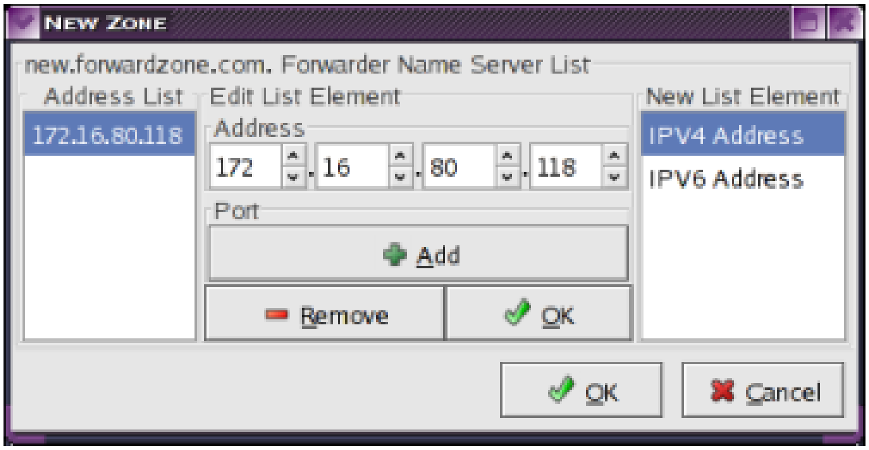
Origin

Class: IN

Forward Zone Origin: new.forwardzone.com.

Zone Type: forward

Choose the appropriate Class and enter the Origin name for the new zone. Then click on the "OK" button . The New Forward Zone dialog is displayed:



New Zone

new.forwardzone.com. Forwarder Name Server List

Address List: 172.16.80.118

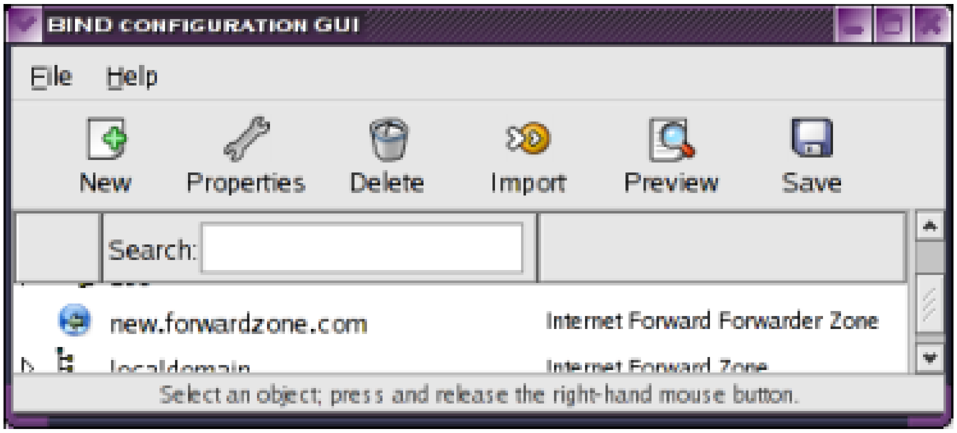
Edit List Element

Address: 172 . 16 . 80 . 118

Port

New List Element: IPV4 Address, IPV6 Address

Create the Forwarder Name Server Addess List of addresses and optional ports of the forwarder name servers as for the Master Name Server List described in section 4.5 above . When you are satisfied with the Forwarder Name Server list, click on the main Dialog "OK" button – the new Forward zone will be created and displayed in the Zone List :



BIND Configuration GUI

Search:

new.forwardzone.com Internet Forward Forwarder Zone

localdomain Internet Forward Zone

Select an object; press and release the right-hand mouse button.

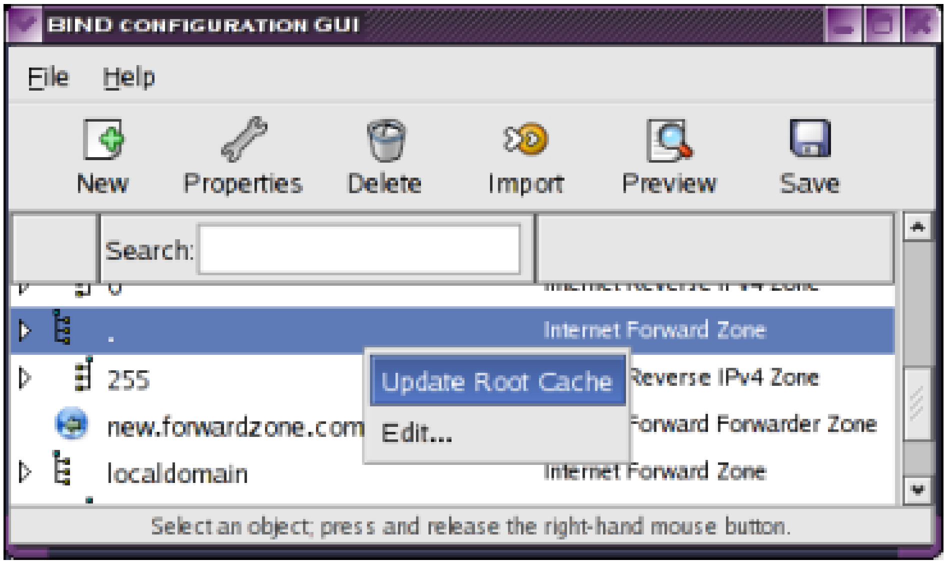
4.5 Creating a new root cache hint Zone

If you did not start with the system-config-bind default initial configuration, you may not have a root cache hint zone, (a zone of type “hint” with origin “.”), without which named will be unable to function properly as it needs to know the addresses of the root name servers.

If you do not have a zone with origin “.” and type 'hint', access the New Zone dialog as described in section 4.1 and create a Forward zone with Origin “.” and type 'hint'.

The root hints zone will be downloaded and stored in the 'named.root' zone database file.

You can download a fresh copy of the root cache hints zone database file by removing the 'named.root' file from the zone database file directory before you start system-config-bind – it will be downloaded automatically for you – or by selecting “Update Root Cache” from the “.” zone Popup Menu:



Select an object; press and release the right-hand mouse button.

4.6 Creating a new Stub Zone:

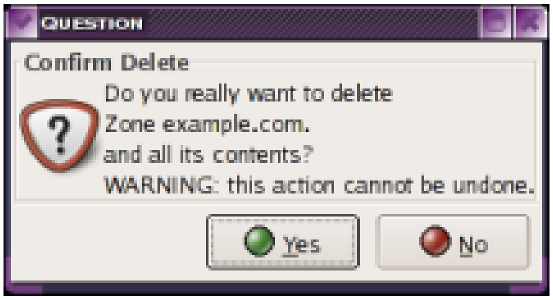
A stub zone may be created in the same way as a slave zone, as described in section 4.5 above, except that a Zone Type of 'stub' should be entered.

4.7 Creating a new “delegation-only” Zone

These may be created in the same way as other zones, except that the Zone Type should be set to delegation-only.

5 Deleting Zones

To delete a zone, select the zone from the Zone List and click on the “Delete” button or press and release the right-hand mouse button and select “Delete” from the pop-up menu. You will be prompted to confirm deletion of the zone and all of its contents :



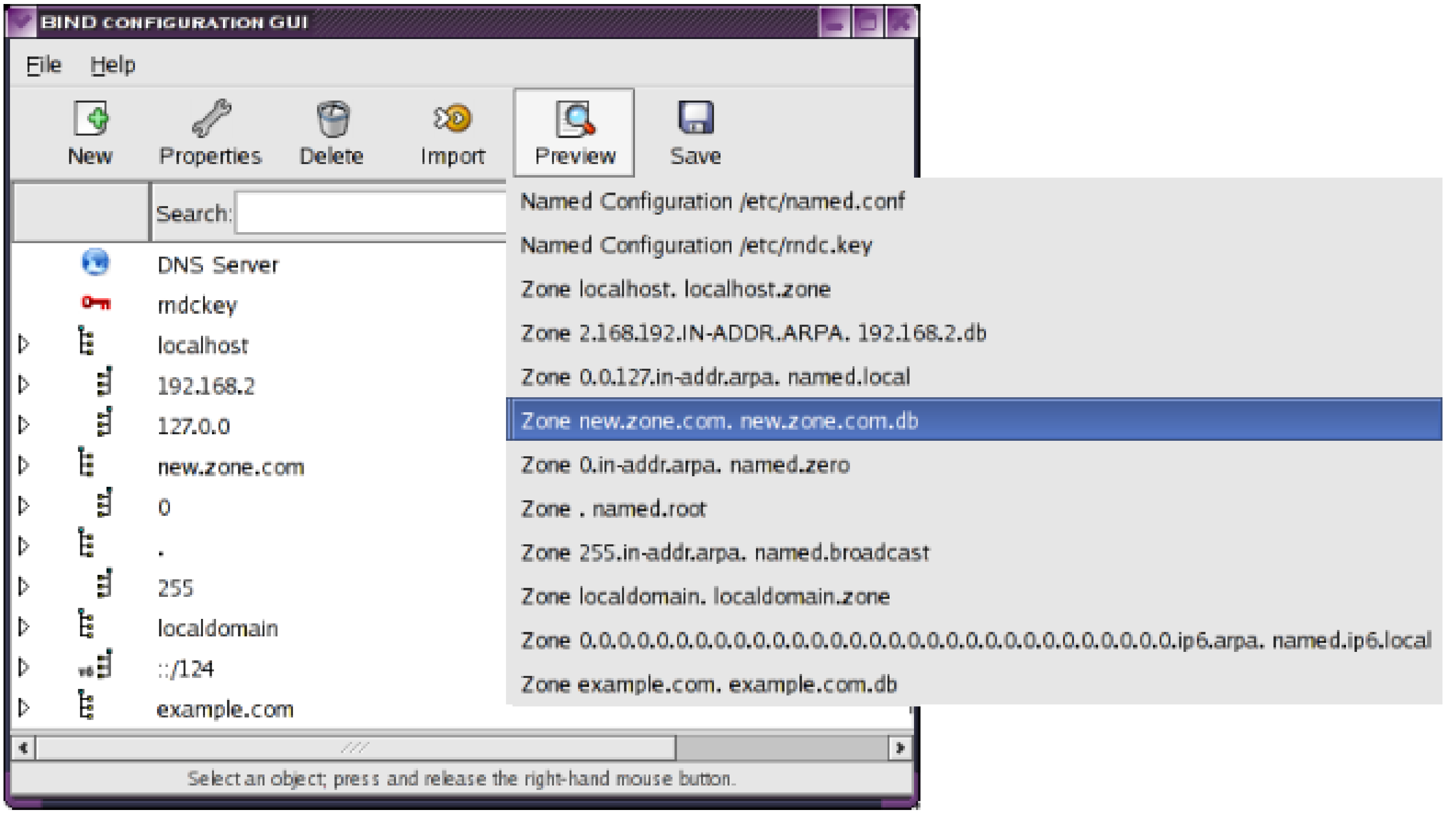
Confirm Delete

Do you really want to delete
Zone example.com.
and all its contents?
WARNING: this action cannot be undone.

Click on the “Yes” button to confirm deletion of the zone . The Zone File database is NOT deleted when the zone is removed from the configuration.

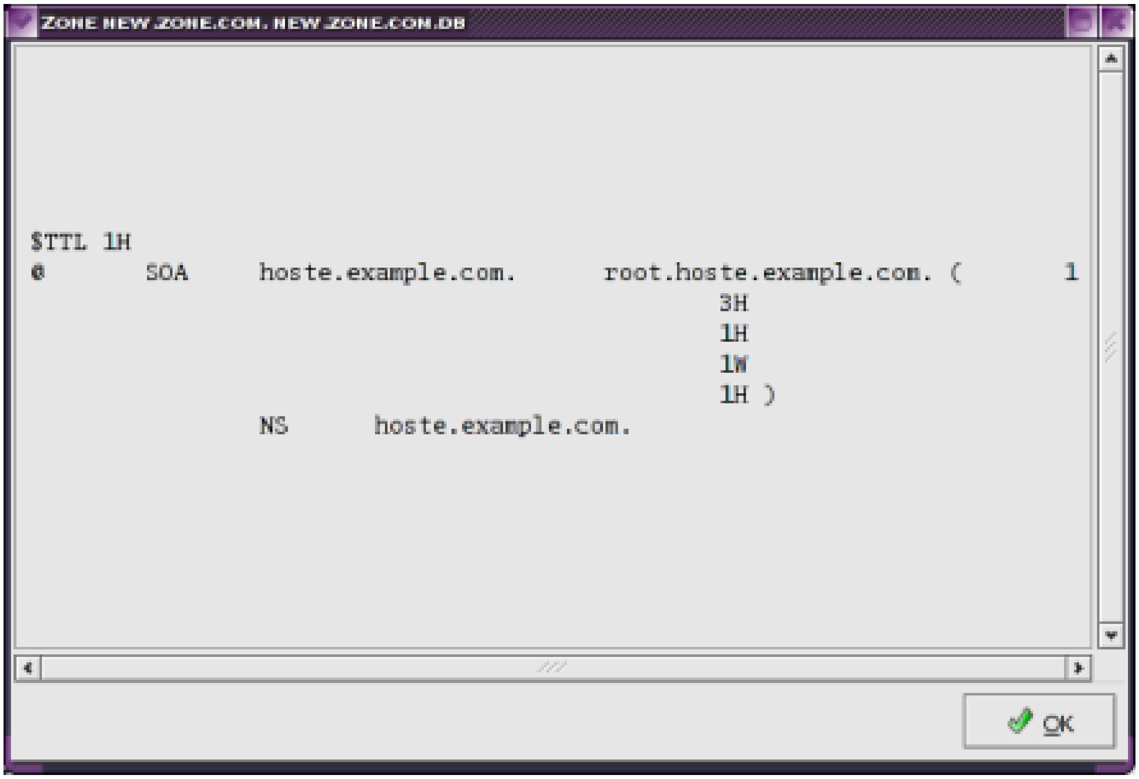
6 Previewing the BIND Configuration Files

You can preview the text that will be written to the BIND configuration files by clicking on the “Preview” button and selecting the configuration file to view:


BIND CONFIGURATION GUI
File
Help
New
Properties
Delete
Import
Preview
Save
Search:
DNS Server
rndckey
localhost
192.168.2
127.0.0
new.zone.com
0
.
255
localdomain
::/124
example.com
Named Configuration /etc/named.conf
Named Configuration /etc/rndc.key
Zone localhost. localhost.zone
Zone 2.168.192.IN-ADDR.ARPA. 192.168.2.db
Zone 0.0.127.in-addr.arpa. named.local
Zone new.zone.com. new.zone.com.db
Zone 0.in-addr.arpa. named.zero
Zone . named.root
Zone 255.in-addr.arpa. named.broadcast
Zone localdomain. localdomain.zone
Zone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa. named.ip6.local
Zone example.com. example.com.db

Select an object; press and release the right-hand mouse button.

The “new.zone.com.db” zone file will then be displayed:

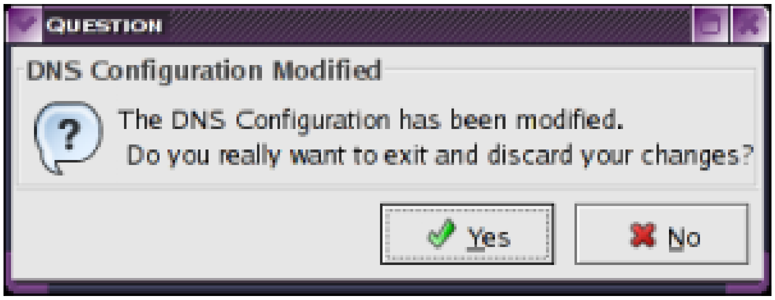


```
$TTL 1H
@       SOA     hoste.example.com.      root.hoste.example.com. (       1
                                                3H
                                                1H
                                                1W
                                                1H )
                NS      hoste.example.com.
```

7 Saving the modified BIND Configuration

7.1 Saving the Configuration at Exit

Having made modifications to the BIND configuration, if you then attempt to exit the `system-config-bind`, either by choosing the "Exit" menu option or by clicking on the Window Manager's "X" top-right-hand button on the window frame, you will be prompted to save the configuration files :



DNS Configuration Modified

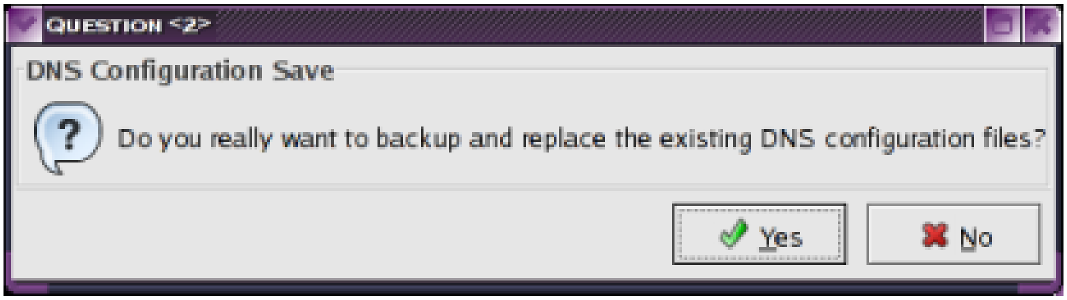
The DNS Configuration has been modified.
Do you really want to exit and discard your changes?

If you press "Yes" in answer to this dialog, your modifications will be discarded and `system-config-bind` will exit.

If you press "No" in answer to this dialog, the "Save Configuration" dialog will be entered (see below).

7.2 The Save Configuration dialog:

To save the BIND configuration, click on the "Save" button in the toolbar or choose the "Save" option from the menu, or modify the configuration and attempt to exit `system-config-bind` . The "Save Configuration" dialog is displayed:



DNS Configuration Save

Do you really want to backup and replace the existing DNS configuration files?

Click "Yes" to save the configuration.

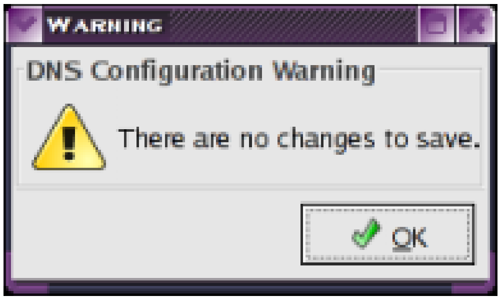
ONLY files that were modified will be saved.

If Zone Database files were modified, their Serial Number(s) will be incremented.

The previous versions of modified configuration files are backed up as described in Section 1.6 above .

If the DNS server was running before the Save , it will be restarted when the Save has completed successfully .

If no configuration files have been modified when the Save dialog is invoked, an error message will be displayed:

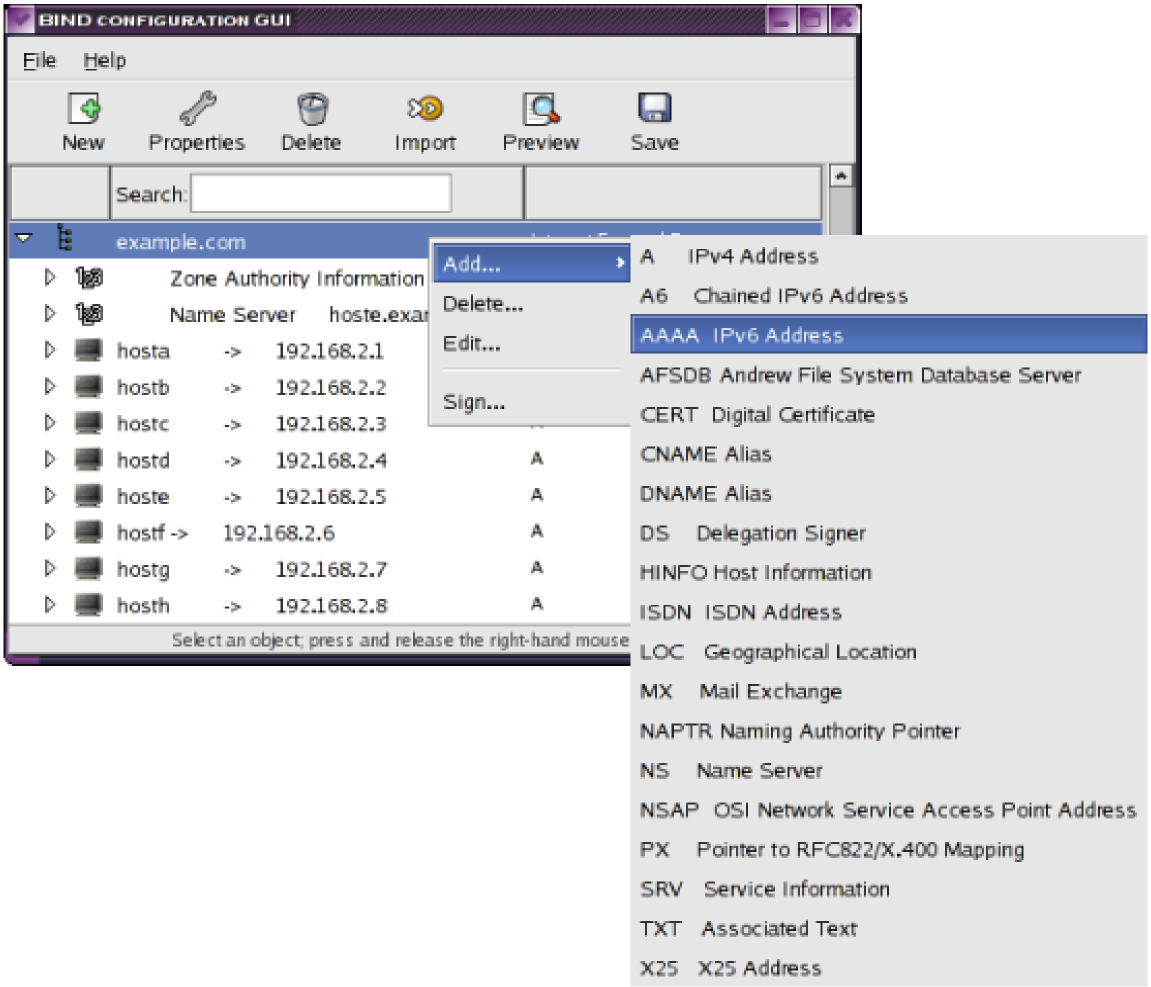


DNS Configuration Warning

There are no changes to save.

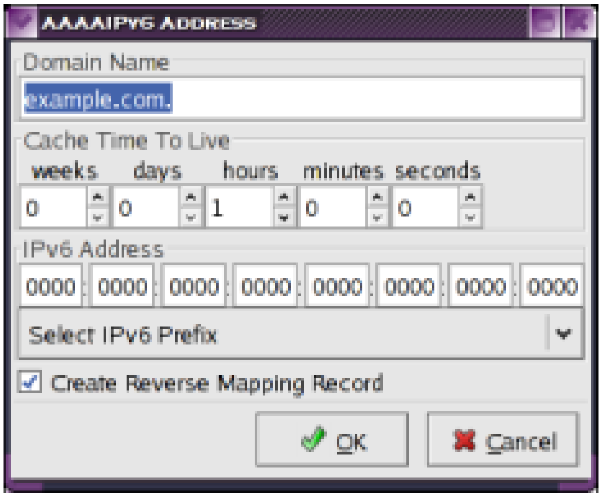
8 Adding Zone Database Records

To add new records to a Zone, select the zone to which you want to add records in the Zone List, and then press and release the right-hand mouse button and select the Add item on the popup menu or press the “New” button . A menu of appropriate record types is the displayed. Select the type of record you want to create:



example.com
Zone Authority Information
Name Server hoste.exa
hosta -> 192.168.2.1
hostb -> 192.168.2.2
hostc -> 192.168.2.3
hostd -> 192.168.2.4 A
hoste -> 192.168.2.5 A
hostf -> 192.168.2.6 A
hostg -> 192.168.2.7 A
hosth -> 192.168.2.8 A

The Record Edit dialog for the chosen type is then displayed:



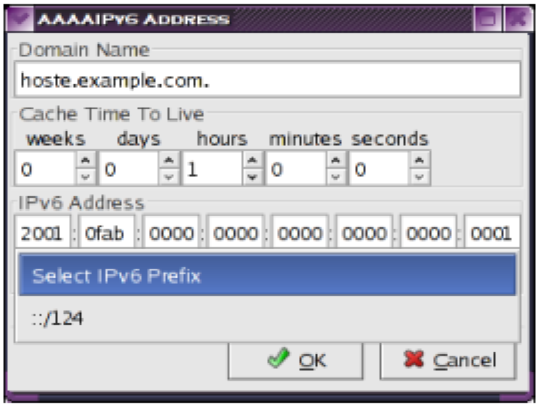
Domain Name: example.com.

Cache Time To Live: weeks 0, days 0, hours 1, minutes 0, seconds 0

IPv6 Address: 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

☑ Create Reverse Mapping Record

Type in the details of the record you want to create:



Domain Name: hoste.example.com.

Cache Time To Live: weeks 0, days 0, hours 1, minutes 0, seconds 0

IPv6 Address: 2001 : 0fab : 0000 : 0000 : 0000 : 0000 : 0000 : 0001

Select IPv6 Prefix

::/124

You can use the “Select Prefix” option list to select a prefix for the address of an existing IPV6 zone origin when creating an AAAA record (as above) or of an existing IPV4 zone origin when creating an A record.

When you are satisfied with the record details, click on the “OK” button .

8.1 Automatic Generation of Corresponding PTR / (A / AAAA) records

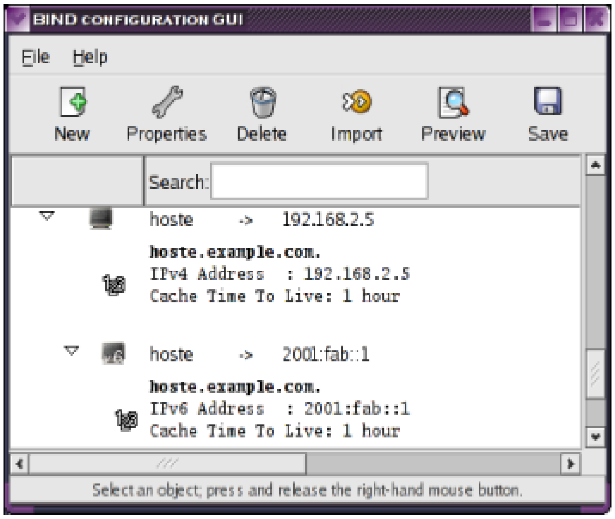
Because the “Create Reverse Mapping Record” checkbox was checked, when the AAAA record shown above is created by pressing the “OK” button, a reverse mapping PTR record will be created from the address `2001:0fab::1` to the name `hoste.example.com`.

In the case above, because no existing zone has an origin that prefixes the address `2001:0fab::1`, a new zone will also be created to contain the reverse mapping record.

If a zone had existed whose origin was a prefix of the address, the reverse mapping record would have been created in the zone with the longest matching origin; ie. in this case, if both zones '2.ip6.arpa' and '1.0.0.2.ip6.arpa' had existed, the new PTR record would have been created in 1.0.0.2.ip6.arpa.

So for the example above, the 'AAAA' record for 'hoste.example.com -> 2001:0fab::1' is added to zone example.com, and because the 'Create Reverse Mapping' checkbox was checked, the “0.0.0.0.0.0.0.b.a.f.0.1.0.0.2.ip6.arpa” zone was created with default parameters, and a 'PTR' record for '2001:0fab::1 -> hoste.example.com' is was added to the newly created zone.

The “Create Forward Mapping” Checkbox on the “PTR” record creation dialog operates in a similar way, only it creates A or AAAA records and possibly Forward zones as appropriate .



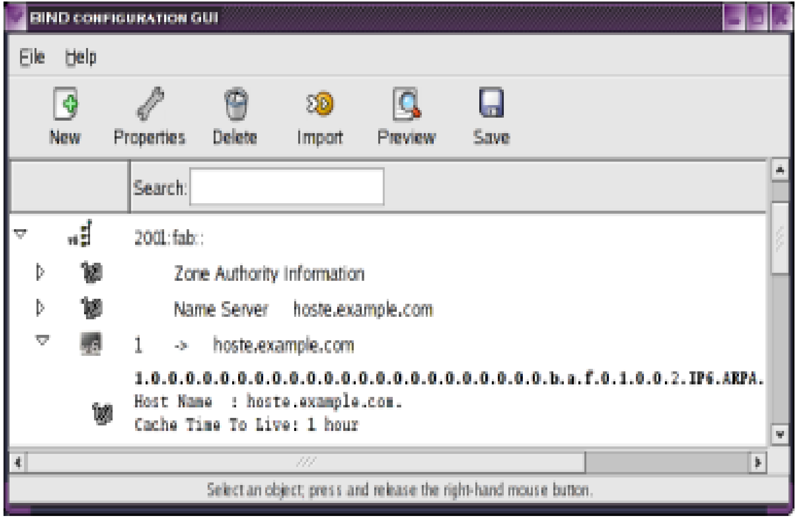
hoste -> 192.168.2.5

```
hoste.example.com.
IPv4 Address  : 192.168.2.5
Cache Time To Live: 1 hour
```

hoste -> 2001:fab::1

```
hoste.example.com.
IPv6 Address  : 2001:fab::1
Cache Time To Live: 1 hour
```

Select an object; press and release the right-hand mouse button.



2001:fab::

Zone Authority Information

Name Server hoste.example.com

1 -> hoste.example.com

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.a.f.0.1.0.0.2.IP6.ARPA.
Host Name  : hoste.example.com.
Cache Time To Live: 1 hour
```

Select an object; press and release the right-hand mouse button.

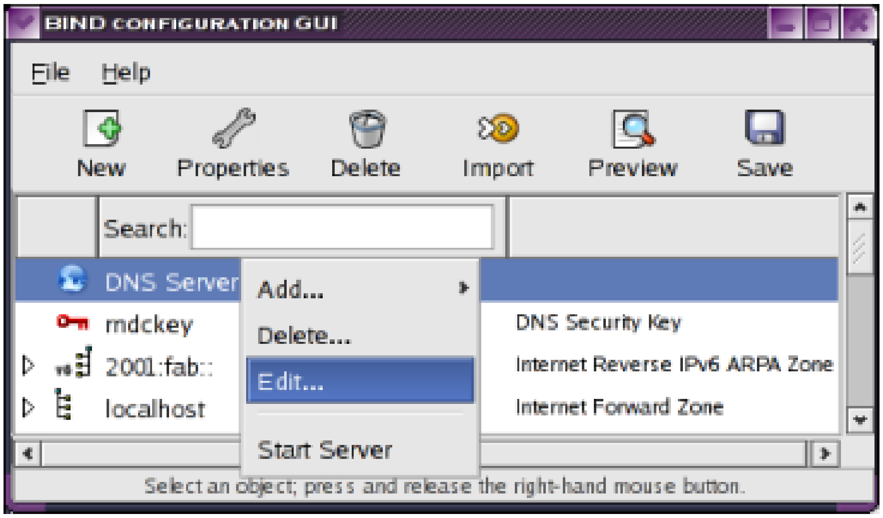
9 Editing or Deletion of Zone Records

To Delete a Zone Record, select it in the Zone List and double click or click on the “Properties” button edit or the “Delete button to delete, or press and release the right-hand mouse button and select the “Delete” or “Edit” option from the popup menu. For Editing, the same record edit dialog as described above for addition is displayed.

10 Editing Name Server and Zone Configuration Options:

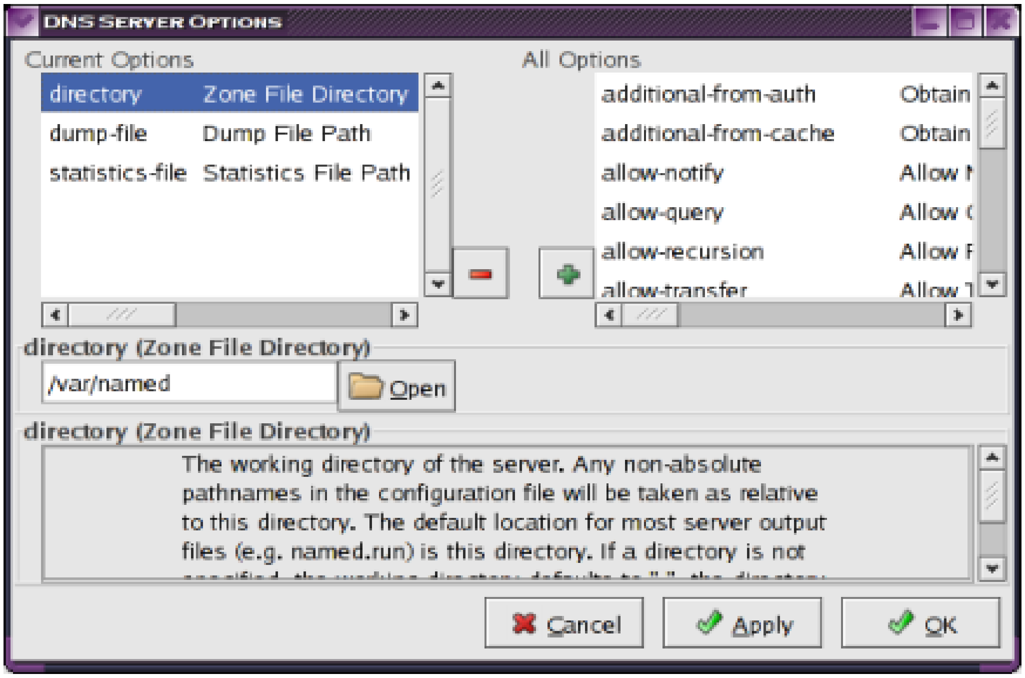
10.1 Editing the DNS Server Global Options

The name server as a whole and each zone has configuration options. You can view and edit these options by double-clicking on the “DNS Server” or zone row in the Zone List or by selecting the row, pressing and releasing the right-hand mouse button, and selecting the “Edit...” option from the popup menu, or by clicking on the “Properties” button on the tool bar when the row is selected.



Select an object; press and release the right-hand mouse button.

Selecting “Edit” or pressing “Properties” for the DNS Server row presents the global configuration options to be edited:



directory	Zone File Directory
dump-file	Dump File Path
statistics-file	Statistics File Path

/var/named

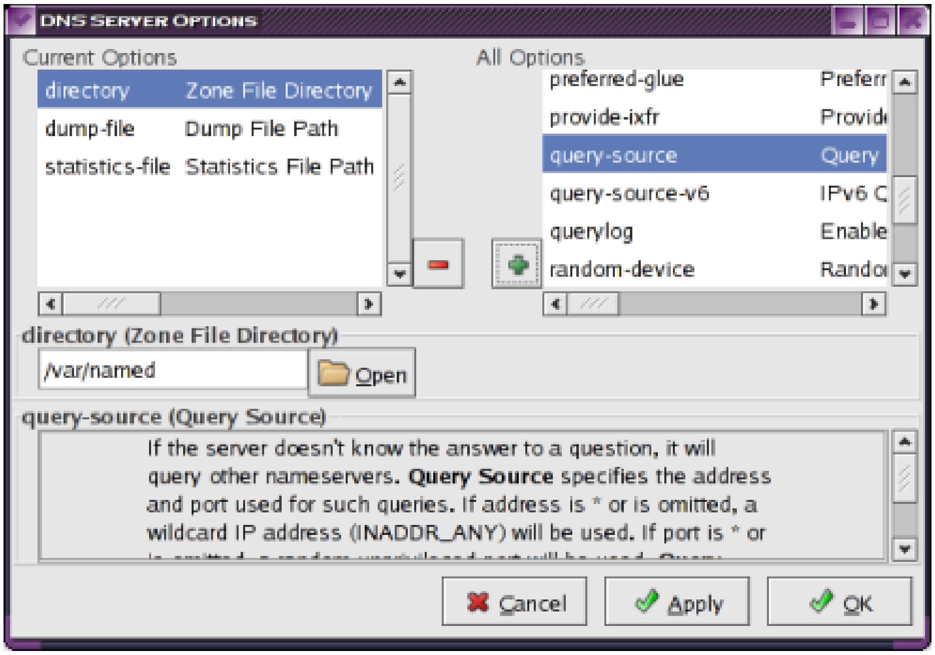
The working directory of the server. Any non-absolute pathnames in the configuration file will be taken as relative to this directory. The default location for most server output files (e.g. named.run) is this directory. If a directory is not

The options currently in effect are displayed in the left-hand “Current Options” list. Selecting an item from the “Current Options” list presents an edit dialog for the current value of the option in the middle frame . Above, the “directory” option is selected and can be edited in the middle frame. Documentation for the selected option is displayed in the bottom frame. If you modify an option, and then select a different option, your modifications are saved but are not applied to the configuration until the “Apply” or “OK” button is pressed.

10.2 Adding a New DNS Server or Zone Configuration Option:

The right-hand “All Options” list displays options that may be added to the list of current options. To add an option, select the option you want to add in the “All Options” list – its documentation is displayed in the bottom frame, but the middle editing frame remains editing the currently selected option from the “Current Options” list.

To Add a new option, click on the “+” button to the left of the “All Options” list :



Current Options:

directory	Zone File Directory
dump-file	Dump File Path
statistics-file	Statistics File Path

All Options:

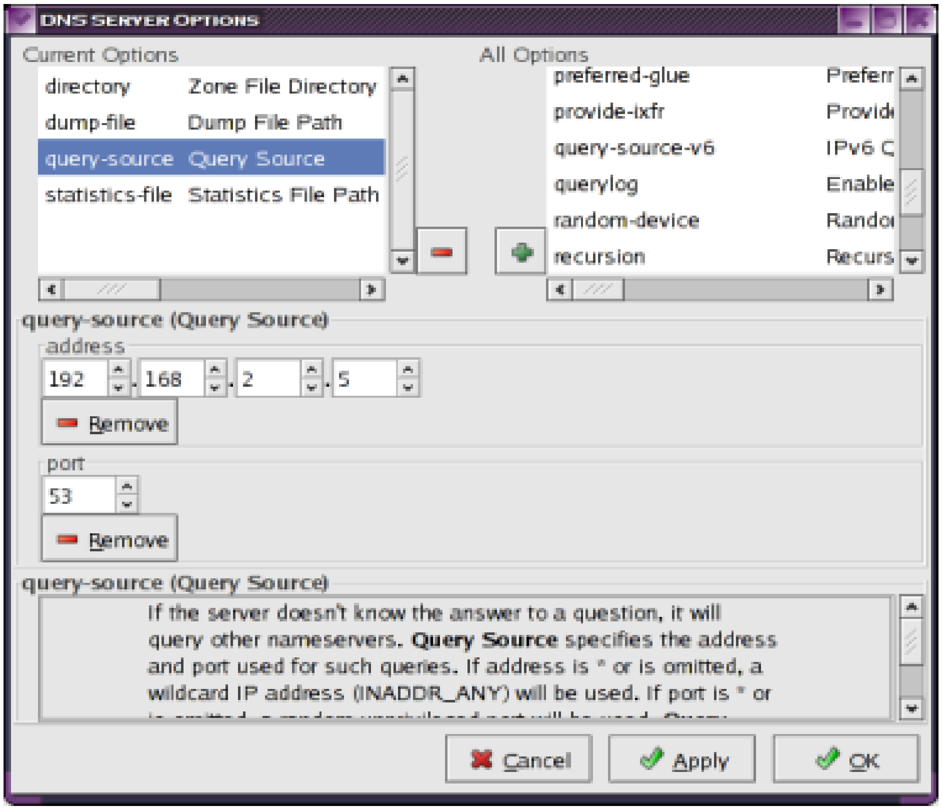
preferred-glue	Preferr
provide-ixfr	Provid
query-source	Query
query-source-v6	IPv6 C
querylog	Enable
random-device	Rando

directory (Zone File Directory)

/var/named

query-source (Query Source)

If the server doesn't know the answer to a question, it will query other nameservers. **Query Source** specifies the address and port used for such queries. If address is * or is omitted, a wildcard IP address (INADDR_ANY) will be used. If port is * or



Current Options:

directory	Zone File Directory
dump-file	Dump File Path
query-source	Query Source
statistics-file	Statistics File Path

All Options:

preferred-glue	Preferr
provide-ixfr	Provid
query-source-v6	IPv6 C
querylog	Enable
random-device	Rando
recursion	Recurs

query-source (Query Source)

address

192 . 168 . 2 . 5

port

53

query-source (Query Source)

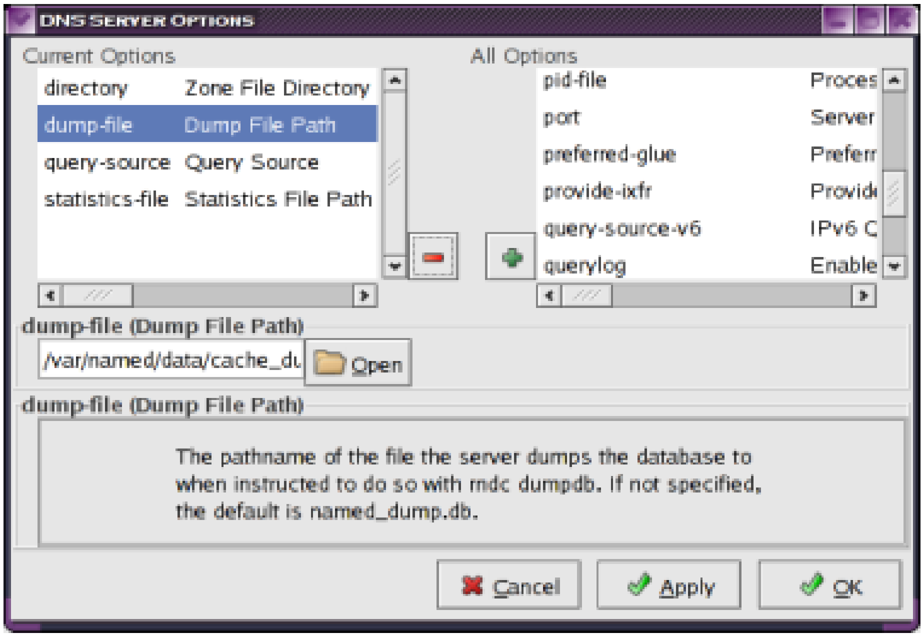
If the server doesn't know the answer to a question, it will query other nameservers. **Query Source** specifies the address and port used for such queries. If address is * or is omitted, a wildcard IP address (INADDR_ANY) will be used. If port is * or

Above, the “Query Source” option was added to the “Current Options” list by clicking on the green “**+**” (Add) button . It then became the currently selected row of the “Current Options” list and its edit dialog was displayed in the middle frame.

Since the “Query Source” option consists of two optional components, the “Address” and “Port” , the “**-** Remove” button for each component is displayed; you can specify only an Address by clicking on the “Port” component's “**-** Remove” button, or only a Port by clicking on the “Address” component's “- Remove” button. Once you click on a “**-** Remove” button for a component, an “**+** Add” button is displayed for it – clicking on a component's “**+** Add” button will add the component value to the Option .

10.3 Removing an Existing DNS Server or Zone Configuration Option

To remove an Option from the “Current Options” list, select the option you want to remove in the list, and then click on the red “**–**” (Remove) button to the right of the “Current Options” list :



Current Options	
directory	Zone File Directory
dump-file	Dump File Path
query-source	Query Source
statistics-file	Statistics File Path

All Options	
pid-file	Proces
port	Server
preferred-glue	Preferr
provide-ixfr	Provid
query-source-v6	IPv6 C
querylog	Enable

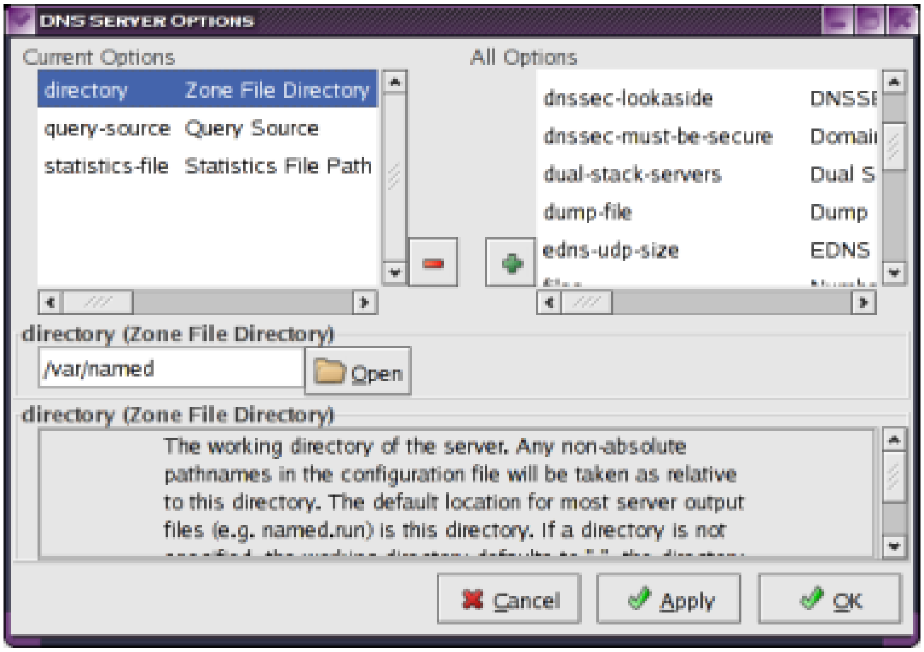
dump-file (Dump File Path)

/var/named/data/cache_du

dump-file (Dump File Path)

The pathname of the file the server dumps the database to when instructed to do so with rndc dumpdb. If not specified, the default is named_dump.db.

The selected option is then removed from the “Current Options” list and added to the “All Options” list :



Current Options	
directory	Zone File Directory
query-source	Query Source
statistics-file	Statistics File Path

All Options	
dnssec-lookaside	DNSSE
dnssec-must-be-secure	Domai
dual-stack-servers	Dual S
dump-file	Dump
edns-udp-size	EDNS

directory (Zone File Directory)

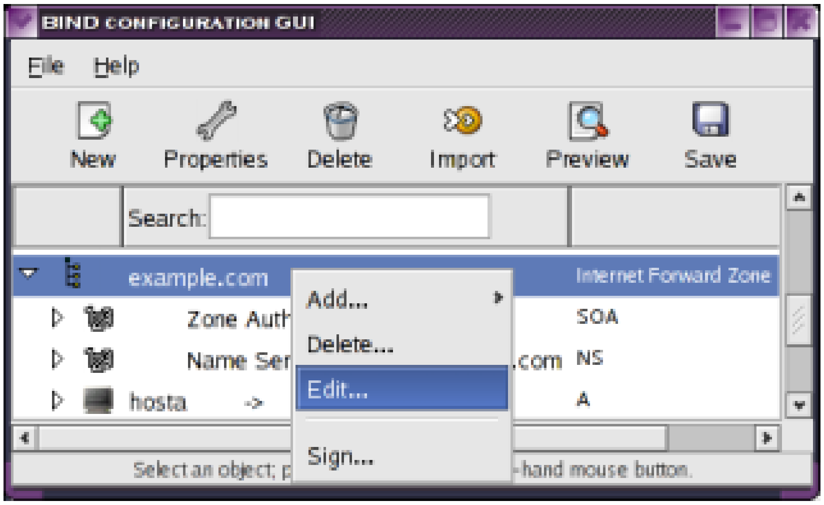
/var/named

directory (Zone File Directory)

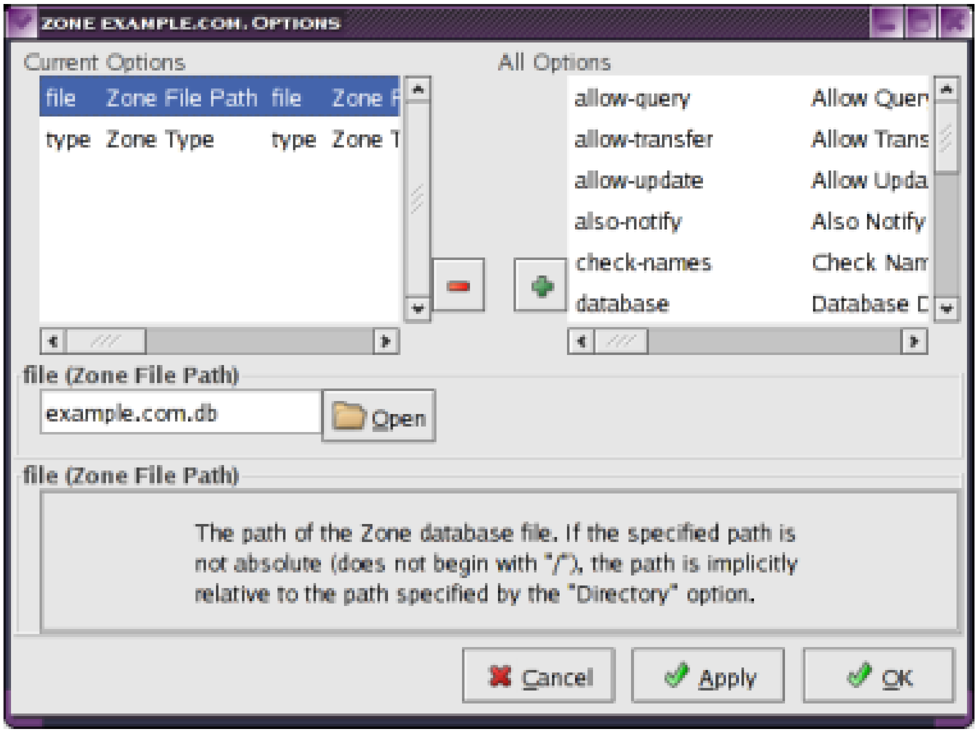
The working directory of the server. Any non-absolute pathnames in the configuration file will be taken as relative to this directory. The default location for most server output files (e.g. named.run) is this directory. If a directory is not

10.4 Editing Zone or View Configuration Options

To edit configuration options for a Zone or View, select the Zone or View in the Zone List, and either double-click on it, click on the “Properties” button on the toolbar, or press and release the right-hand mouse button and select the “Edit...” option:



The Edit Options dialog is displayed for the Zone options:



file (Zone File Path)

example.com.db

file (Zone File Path)

The path of the Zone database file. If the specified path is not absolute (does not begin with "/"), the path is implicitly relative to the path specified by the "Directory" option.

The list of “ALL Options” displayed will depend on the object type (View or Zone) and the “type” of the Zone (master, slave, or forward).

Zone or View options can be Edited, Added or Removed in the same manner as for DNS Server global options as described above.

11 Access Control Lists (ACLs)

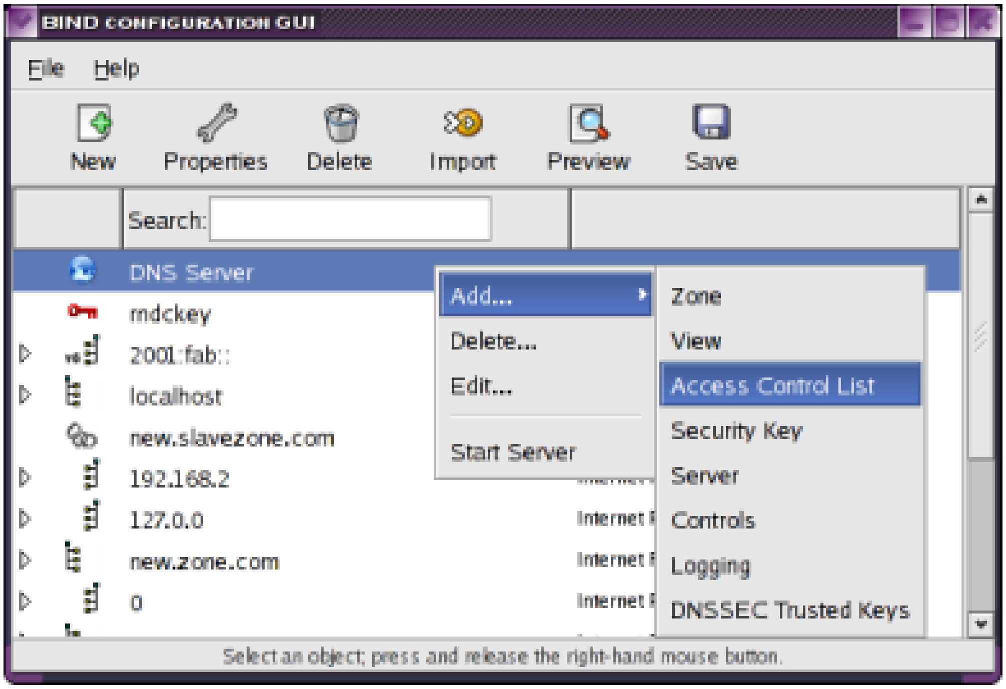
You can restrict access to DNS Server services with Access Control Lists, which specify sets of hosts that can be allowed or denied access to services .

The configuration can contain global named ACLs, which can be referenced in any other ACL.

Many configuration options contain ACL components; these are all specified using the same ACL editing dialogs described here, and may contain names of global ACLs in the configuration.

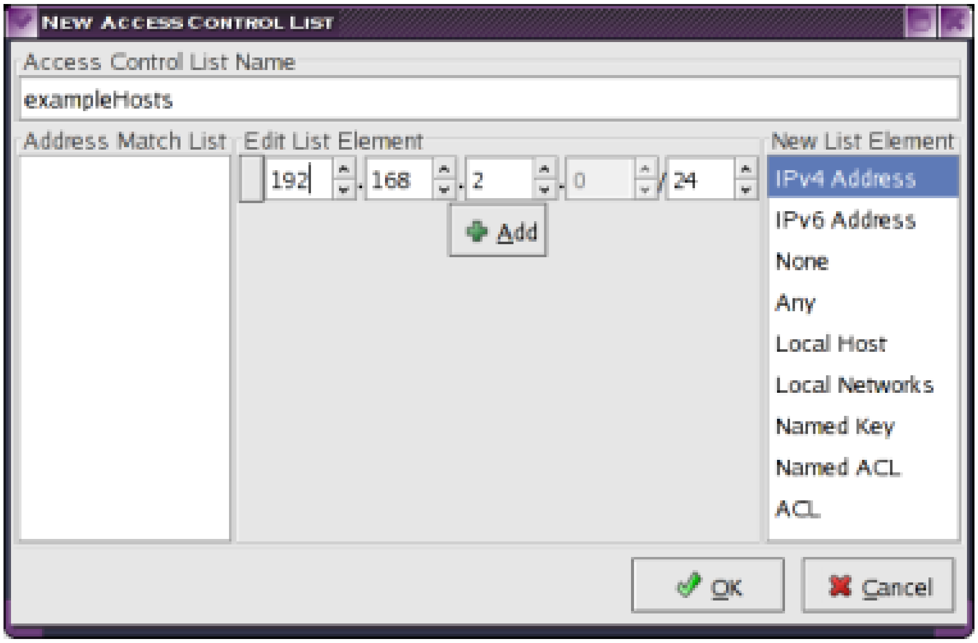
11.1 Creating a new Global ACL

Select the “DNS Server” row and click on the “New” button in the Toolbar or press and release the right-hand mouse button over the “DNS Server” row and select the “Add” option in the popup menu; then select the “Access Control List” option:



Select an object; press and release the right-hand mouse button.

The Access Control List dialog is displayed:



Access Control List Name: exampleHosts

Edit List Element: 192 . 168 . 2 . 0 / 24

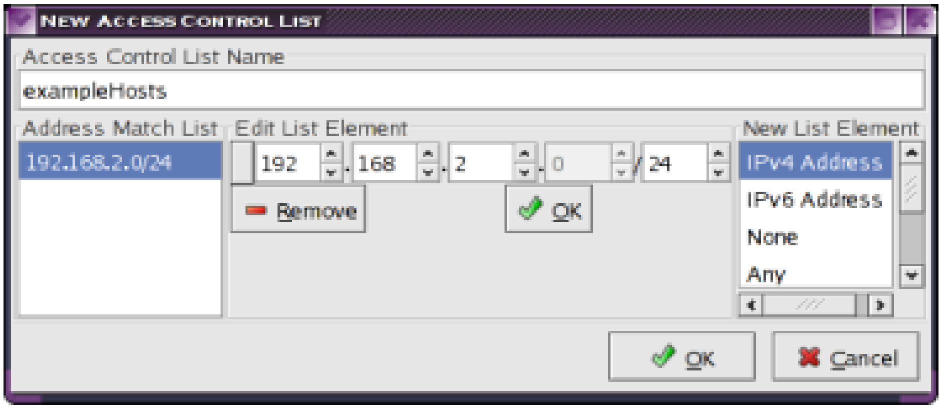
New List Element: IPv4 Address

ACLs consists of an “Address Match List”, which is a list of addresses, address prefixes, keys, or other ACLs that together must all match a given address for that address to be included in the set that the ACL selects.

The “Address Match List” is shown in the list on the left of the dialog, and the list of possible component types is shown in the “New List Element” list on the right of the dialog. The currently selected member of the “Address Match List” or “New List Element” list can be edited in the “Edit List Element” frame in the middle of the dialog.

To add a new component of the Address Match List, select the desired component type in the “New List Elements” list . A dialog for specifying the value of the new component is shown in the “Edit List Element” frame as shown above.

When you are satisfied with the component's value, click the “**+** Add” button in the “Edit List Element” frame to to add it to the Address Match List:



Access Control List Name: exampleHosts

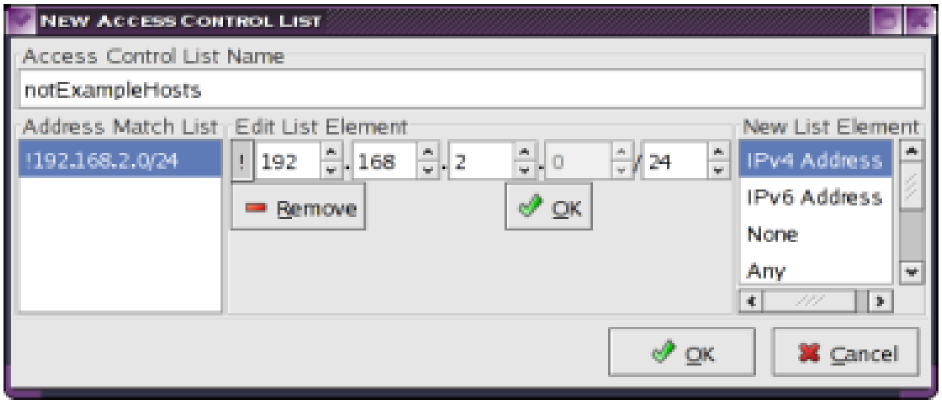
Address Match List: 192.168.2.0/24

Edit List Element: 192 . 168 . 2 . 0 / 24

The new Address Match List component is then displayed in the “Address Match List”, and in edit mode in the “Edit List Element” frame, and you can click on the “- Remove” button to remove it from the Address Match List, or make changes to its value and save it with the “OK” button .

The Address Match List above will select all hosts with addresses matching 192.168.2.0 with subnet mask 255.255.255.0 .

To select the complement of that set, ie. all hosts with addresses that do not match 192.168.2/24 , then click on the “Not” button which is just to the left of the “Edit List Element” entry :

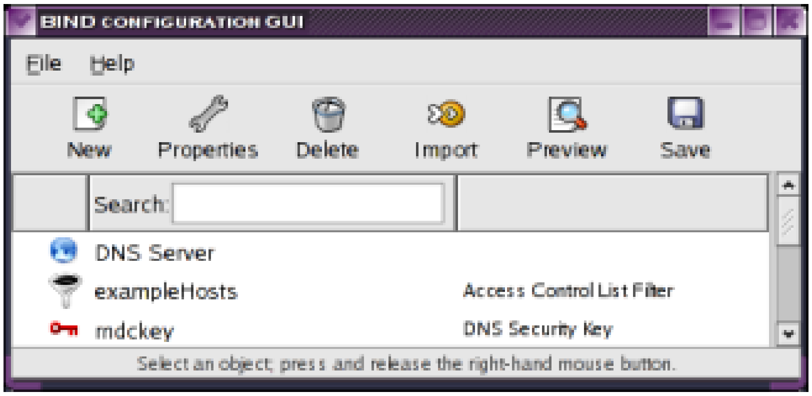


Access Control List Name: notExampleHosts

Address Match List: !192.168.2.0/24

Edit List Element: ! 192 . 168 . 2 . 0 / 24

Once you are satisfied with the “Address Match List” contents, click on the “OK” button to save the ACL.

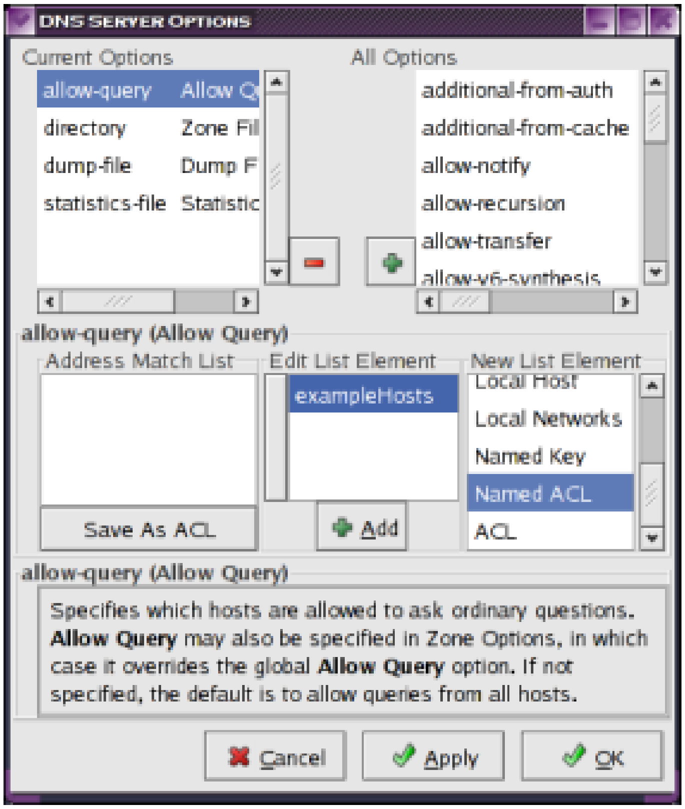


DNS Server
exampleHosts Access Control List Filter
rndckey DNS Security Key

Select an object; press and release the right-hand mouse button.

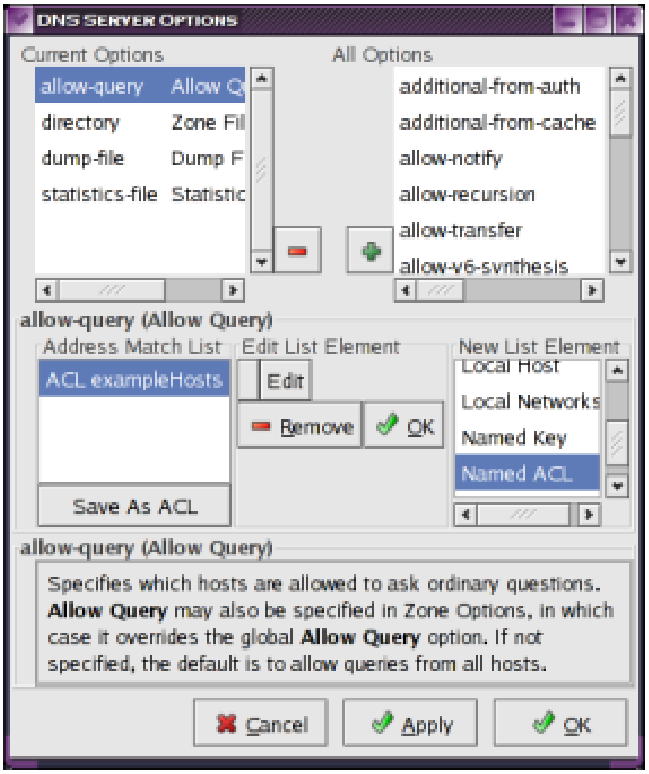
12 Including a Global ACL in a Configuration Option

Once you have created a global ACL, it can be included in any other ACL, such as ACL configuration option components, by selecting the “Named ACL” row in the “New List Element” list and then the name of the ACL you want to add to the ACL being edited. For example, to restrict the DNS Server to provide answers only to members of the set of hosts defined by the “exampleHosts” ACL, add the “exampleHosts” ACL to the “Allow Queries” DNS Server global option:



Specifies which hosts are allowed to ask ordinary questions. **Allow Query** may also be specified in Zone Options, in which case it overrides the global **Allow Query** option. If not specified, the default is to allow queries from all hosts.

Clicking on the “+Add” button then adds the “exampleHosts” ACL to the “allow-query” ACL, and you can then Edit the “exampleHosts” ACL from this dialog by pressing the “Edit” button or remove it from the “allow-query” ACL “Address Match List” by pressing the “- Remove” button:



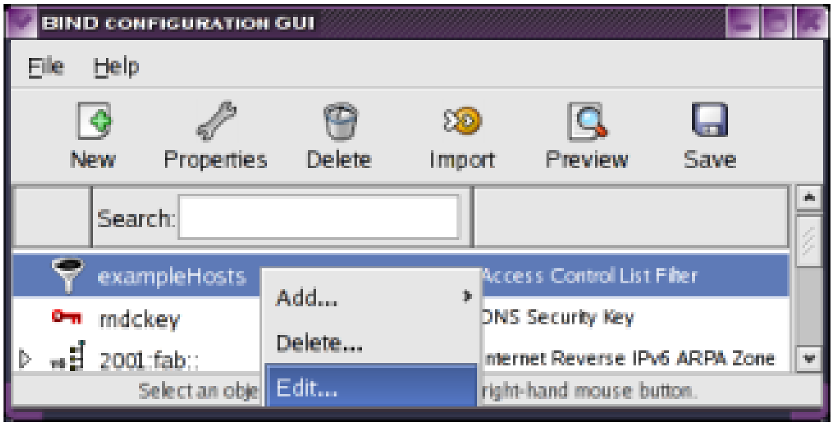
Specifies which hosts are allowed to ask ordinary questions. **Allow Query** may also be specified in Zone Options, in which case it overrides the global **Allow Query** option. If not specified, the default is to allow queries from all hosts.

Pressing the “Edit” button for the “ACL exampleHosts” member of the “allow-query” ACL would pop-up the ACL Edit dialog for the global “exampleHosts” ACL .

You could also use the “Not” button directly to the left of the “Edit” button to negate the exampleHosts ACL and cause the complement of the set to be selected by the “allow-query” ACL – this does not affect the global exampleHosts ACL .

12.1 Editing Global ACLs

You can edit a global ACL by selecting it in the Zone List, and either double-clicking the mouse on it, or clicking on the Properties button, or pressing and releasing the right-hand mouse button and selecting the edit option:



exampleHosts Access Control List Filter
mdckey DNS Security Key
2001:fab:: nternet Reverse IPv6 ARPA Zone
Select an obje right-hand mouse button.

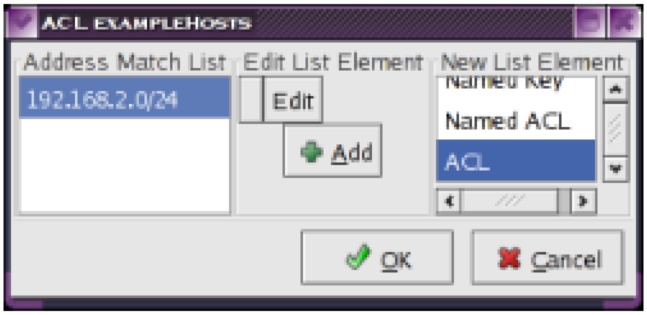
The ACL Edit dialog will then pop up as shown below.

12.2 Deleting Global ACLs:

You can delete a global ACL by selecting it as shown above for edit and selecting the “Delete” option from the popup menu or pressing the “Delete” button in the tool bar. Deletion of global ACLs is not allowed if they are referenced by other ACLs.

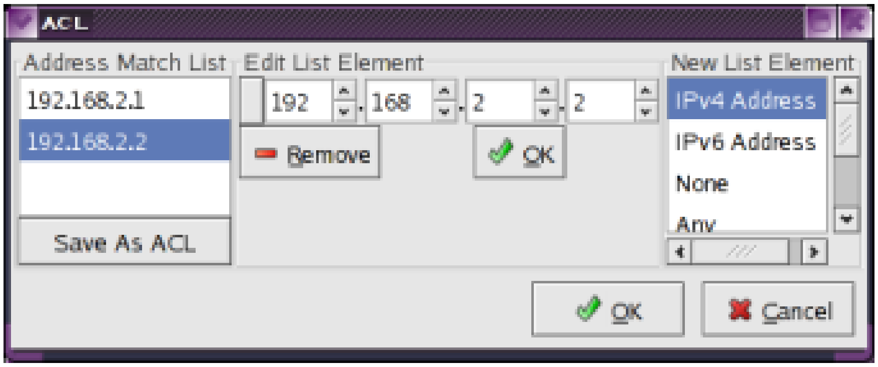
12.3 Embedded ACLs

ACLs may also contain other un-named ACLs, or embedded ACLs . To embed an ACL in another ACL, edit the ACL and select the “ACL” option in the “New List Element” list:



192.168.2.0/24

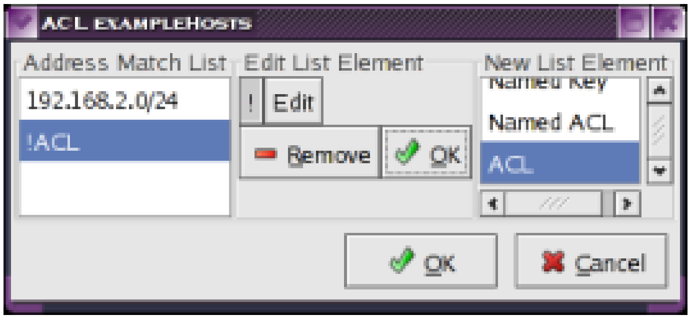
Click on the “Edit” button and a new ACL Edit Dialog will pop-up :



192.168.2.1
192.168.2.2
192 . 168 . 2 . 2

Create the address match list you require, and click on the “OK” button. The pop-up dialog disappears, and the embedded ACL is added to the “exampleHosts” ACL's Address Match List by clicking the 'OK' button.

The "Not" button to the left of the "Edit" button can be clicked to select the complement of the set selected by the embedded ACL :

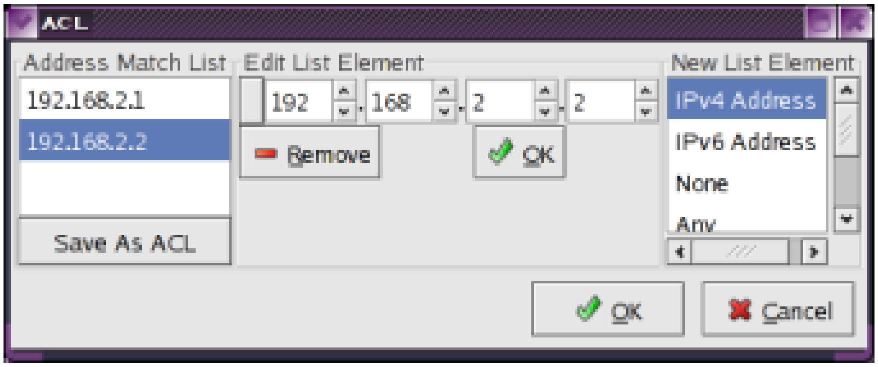


Address Match List:
192.168.2.0/24
!ACL

The exampleHosts ACL now selects all hosts on subnet 192.168.2/24 EXCEPT hosts 192.168.2.1 or 192.168.2.2 .

You can now edit this embedded ACL only by selecting it in the exampleHosts ACL edit dialog and pressing the Edit button in the "Edit List Element" frame – the ACL Edit dialog for the embedded ACL will pop-up .

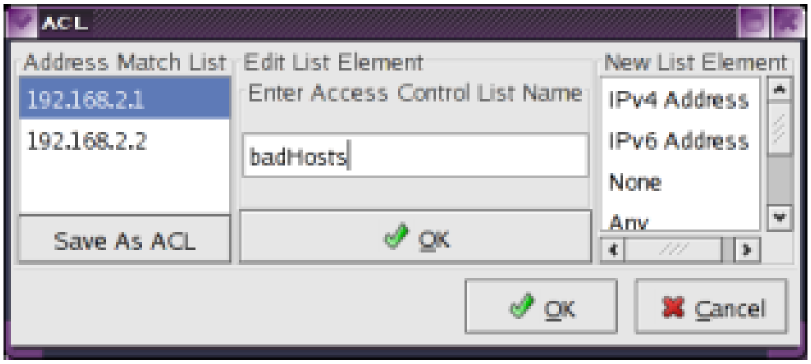
Having entered the edit dialog for an embedded ACL, you then have the option of saving this embedded (un-named) ACL as a global (named) ACL by clicking on the "Save As ACL" button directly underneath the Address Match List:



Address Match List:
192.168.2.1
192.168.2.2

Edit List Element: 192 . 168 . 2 . 2

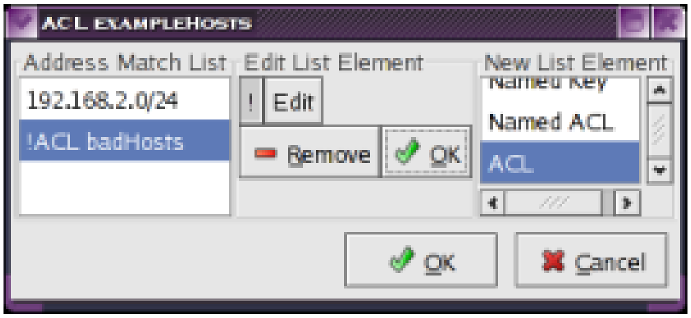
Pressing the "Save As ACL" button will prompt you for a name to call the new global ACL :



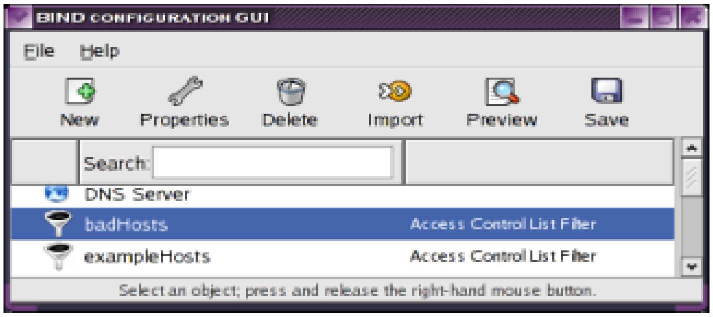
Address Match List:
192.168.2.1
192.168.2.2

Enter Access Control List Name: badHosts

Pressing the "OK" button in the "Edit List Element" frame would then create a global ACL called "badHosts", and change the embedded ACL edit dialog into the edit dialog for the global "badHosts" ACL. Pressing the "OK" button on this dialog then converts the embedded ACL in the "exampleHosts" ACL into a reference to the global "badHosts" ACL :



Address Match List:
192.168.2.0/24
!ACL badHosts



DNS Server
badHosts Access Control List Filter
exampleHosts Access Control List Filter

Select an object; press and release the right-hand mouse button.

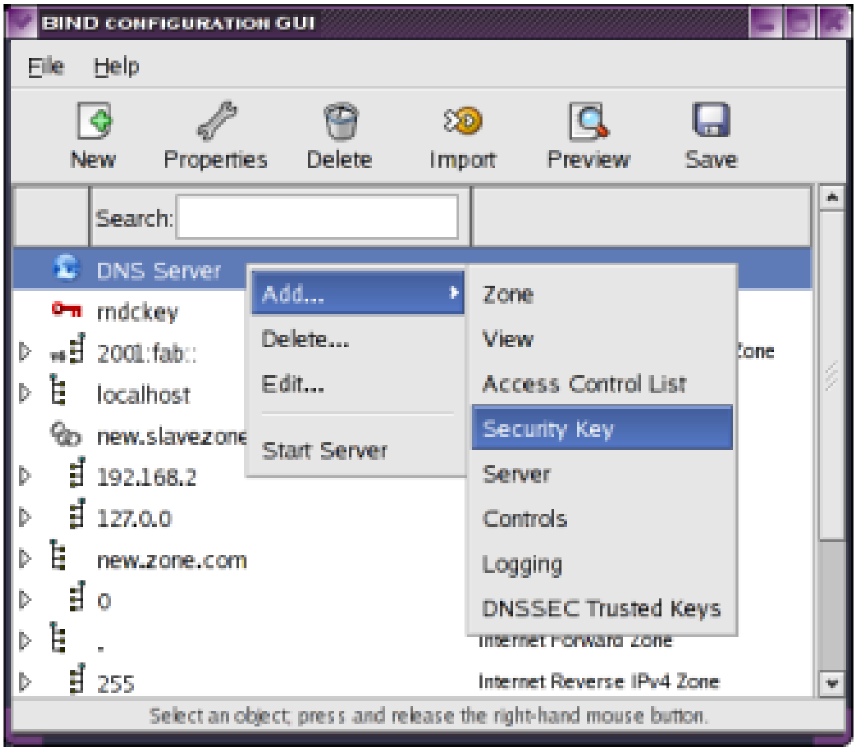
13 Transaction Signature (TSIG) Key Management

Transactions between DNS Servers such as Dynamic DNS (DDNS), Zone Transfers, Notify and Recursive Queries and the control of DNS servers on their Control Channels by applications such as `rndc`, can be securely authenticated using transaction signature (TSIG) keys .

One such TSIG key must exist by default in all DNS servers to allow server control by the `rndc` application ; by convention this key is named `rndckey` .

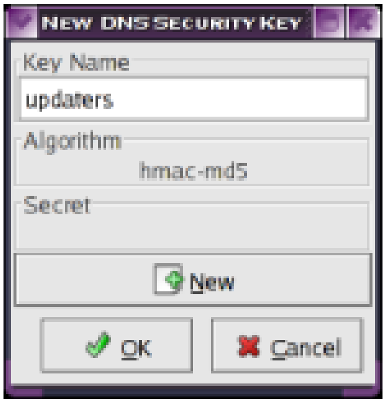
13.1 Creating new TSIG Keys

To create a TSIG key, select the DNS Server row in the Zone List, and click on the "New" button or press and release the right-hand mouse button and select the "Add" option from the popup menu:



Select an object; press and release the right-hand mouse button.

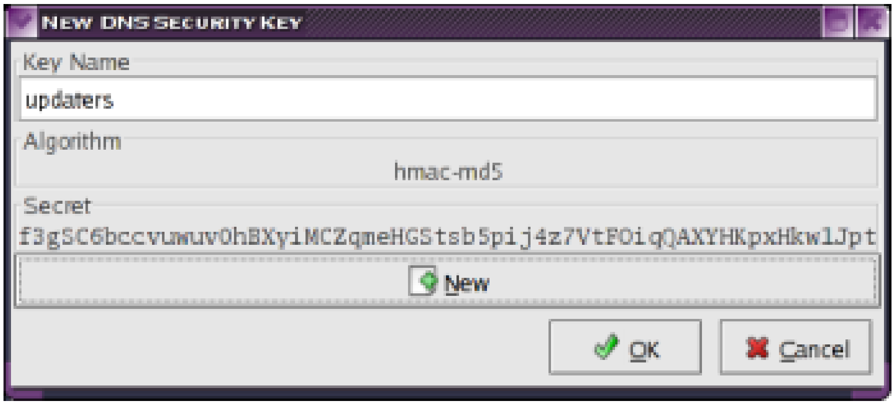
The New Key dialog will be displayed. Type in the "Key Name" for the new key and click on the "New" button to create a new key:



Key Name: updaters

Algorithm: hmac-md5

Secret:

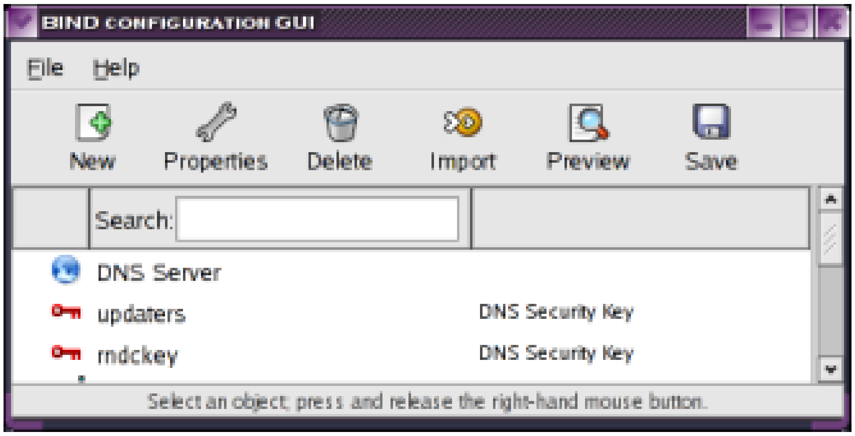


Key Name: updaters

Algorithm: hmac-md5

Secret: f3gSC6bccvuwuv0hBXyiMCZqmeHGStsb5pij4z7VtFOiqQAXYHKpxHkw1Jpt

Pressing the "OK" button then adds the new key to the configuration:



DNS Server
updaters DNS Security Key
rndckey DNS Security Key

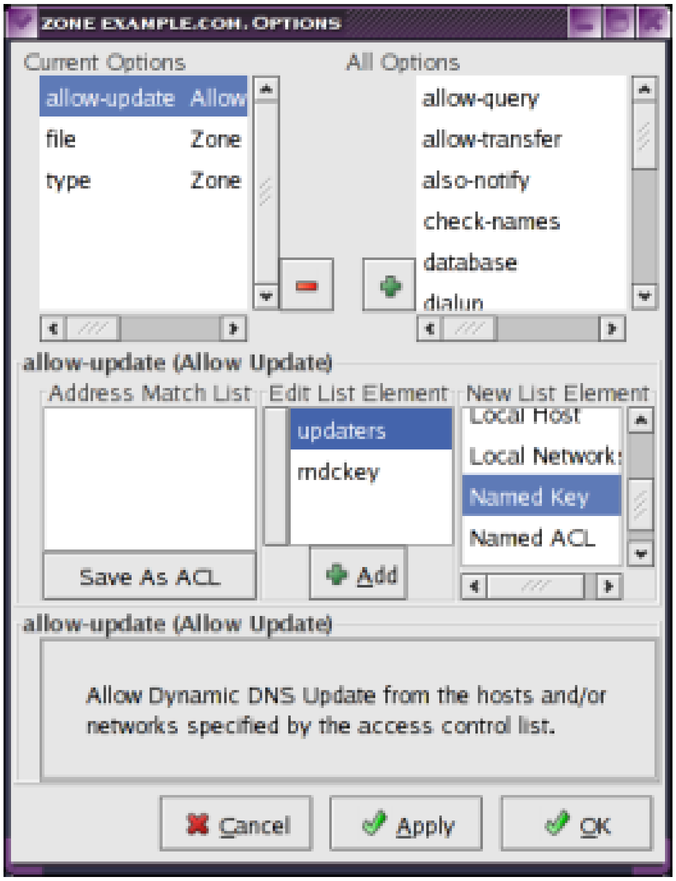
Select an object, press and release the right-hand mouse button.

13.2 Referencing TSIG keys in an ACL

TSIG keys can be referenced in any ACL, such as in the “allow-update” or “allow-transfer” Zone Configuration Options.

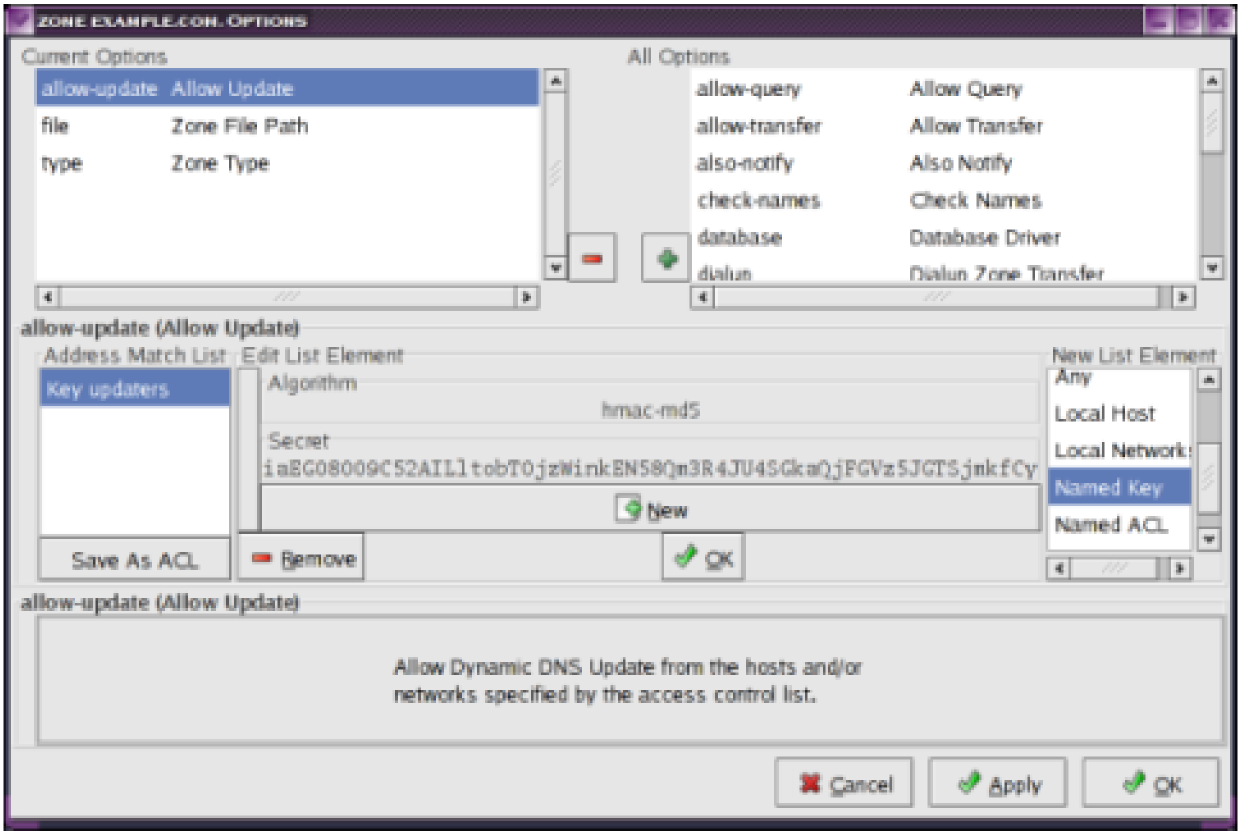
A reference to a TSIG key in an ACL specifies the set of hosts that sign transactions using this key .

So we could allow Dynamic DNS Update of zone “example.com.” only by hosts that use the “updaters” key by specifying an “allow-update” option that references the “updaters” key:



Allow Dynamic DNS Update from the hosts and/or networks specified by the access control list.

To add a TSIG key to an ACL, select the “Named Key” option from the “New List Element” list and choose the key you want to add by selecting its name in the “Edit List Element” list; then press the “Add” button in the “Edit List Element” frame. The Key name then appears in the Address Match List, and the key is displayed in the “Edit List Element” frame.



Current Options	
allow-update	Allow Update
file	Zone File Path
type	Zone Type

All Options	
allow-query	Allow Query
allow-transfer	Allow Transfer
also-notify	Also Notify
check-names	Check Names
database	Database Driver
dialup	Dialup Zone Transfer

allow-update (Allow Update)

Algorithm: hmac-md5

Secret: iaEG08009C52AILltobT0jzWinkEN58Qm3R4JU4SGkaQjFGVz5JGTSjmkfCy

allow-update (Allow Update)

Allow Dynamic DNS Update from the hosts and/or networks specified by the access control list.

Click on the “OK” button to save the “allow-update” ACL option containing the named key to the Zone “example.com” options, so that only hosts that sign their packets with this key are allowed to perform DDNS updates.

13.3 Edit and Deletion of TSIG Keys:

You can edit a TSIG key by selecting it in the Zone List and double-clicking it, clicking on the “Properties” toolbar button, or by pressing and releasing the the right-hand mouse button and selecting the “Edit “ option from the popup menu. The same dialog as for addition is displayed.

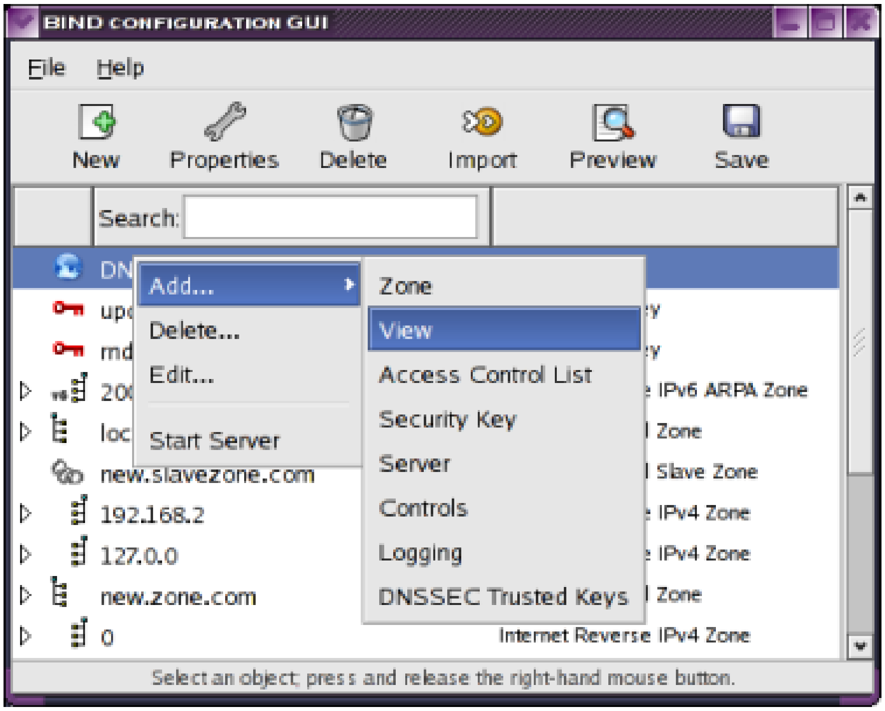
To delete a TSIG key, select as described above for Editing, and click on the “Delete” toolbar button or select the “Delete” option from the popup menu.

14 Managing Zone Access Control and Options with Views

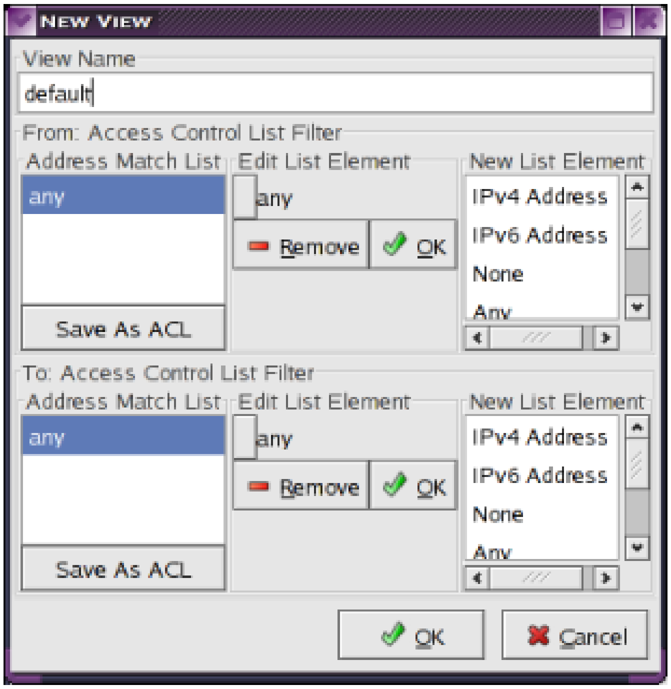
Views are a feature of BIND 9 that allow you to specify common access control and options for groups of zones without having to specify duplicate options for each zone . Each view presents a different set of zones and options based on clients' source address (the "From:" ACL) and destination address (the "To:" ACL) so different clients see different DNS "views".

14.1 Creating a View

Select the "DNS Server" row, and either click on the "New" button, or press and release the right-hand mouse button and select the Add option from the popup menu. Select the "View" option from the popup menu:

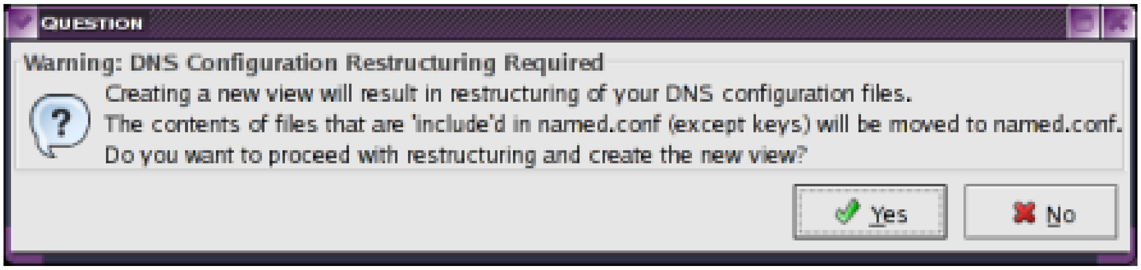


The "New View" dialog is displayed:



The ACLs for matching client sources (the "From:" filter) and destinations (the "To:" filter) and the view name must be specified. Once you are satisfied with the ACL contents and view name, click the "OK" button to create the view.

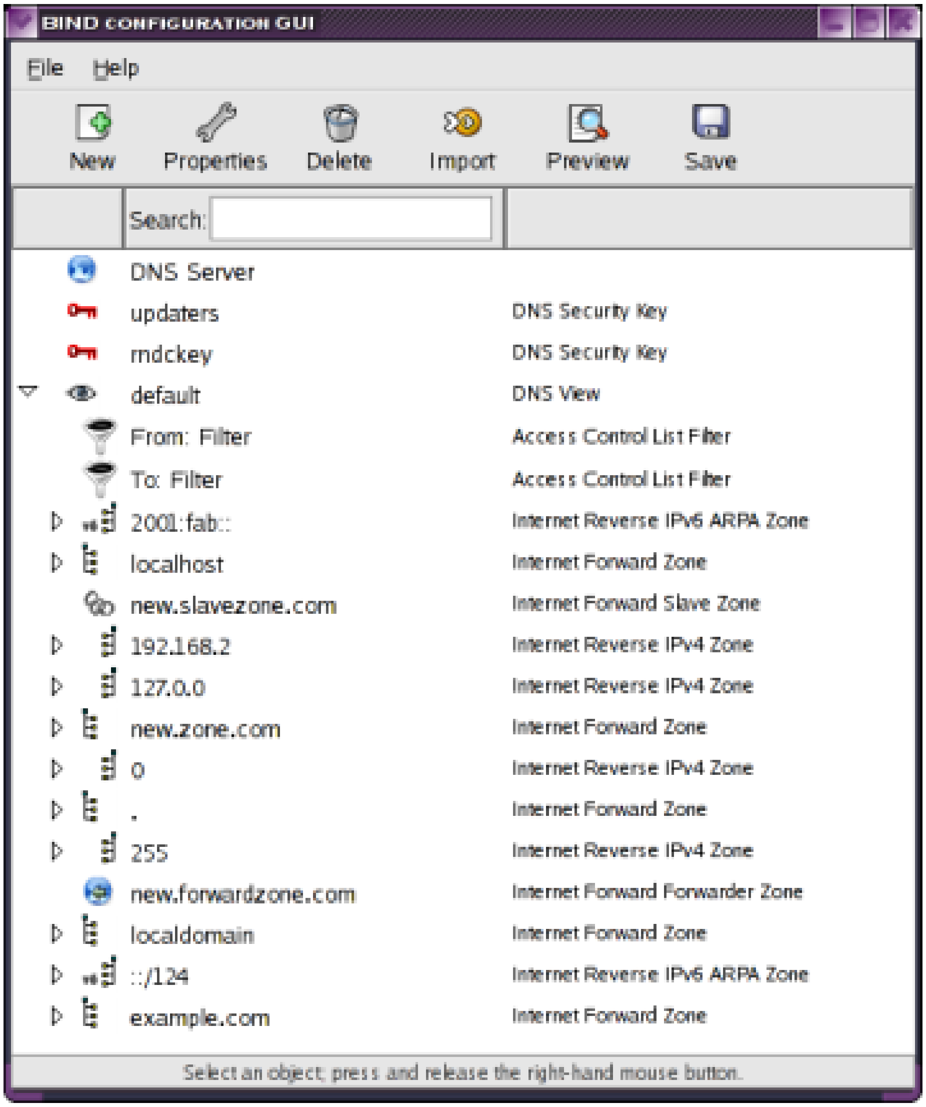
Because the current configuration contains no views, it must be restructured to support views; any zones that are defined in "include" files will be moved to the main `named` configuration file. You will be prompted to allow restructuring:



Warning: DNS Configuration Restructuring Required

Creating a new view will result in restructuring of your DNS configuration files.
The contents of files that are 'include'd in named.conf (except keys) will be moved to named.conf.
Do you want to proceed with restructuring and create the new view?

Click "OK" to allow restructuring and create the view. All current zones are then moved into the new view (BIND requires that if a view exists in the configuration, all zones must be defined within a view) :



DNS Server	
updaters	DNS Security Key
rndckey	DNS Security Key
default	DNS View
From: Filter	Access Control List Filter
To: Filter	Access Control List Filter
2001:fab::	Internet Reverse IPv6 ARPA Zone
localhost	Internet Forward Zone
new.slavezone.com	Internet Forward Slave Zone
192.168.2	Internet Reverse IPv4 Zone
127.0.0	Internet Reverse IPv4 Zone
new.zone.com	Internet Forward Zone
0	Internet Reverse IPv4 Zone
.	Internet Forward Zone
255	Internet Reverse IPv4 Zone
new.forwardzone.com	Internet Forward Forwarder Zone
localdomain	Internet Forward Zone
::/124	Internet Reverse IPv6 ARPA Zone
example.com	Internet Forward Zone

Select an object, press and release the right-hand mouse button.

14.2 Editing View Options:

You can edit view options by double clicking on the view row, or by selecting the view row and clicking on the "Properties" button, or by pressing and releasing the right-hand mouse button over the view row and selecting the "Edit..." option, Options that apply to zones can be specified in the view options, and then would apply to all zones contained in the view.

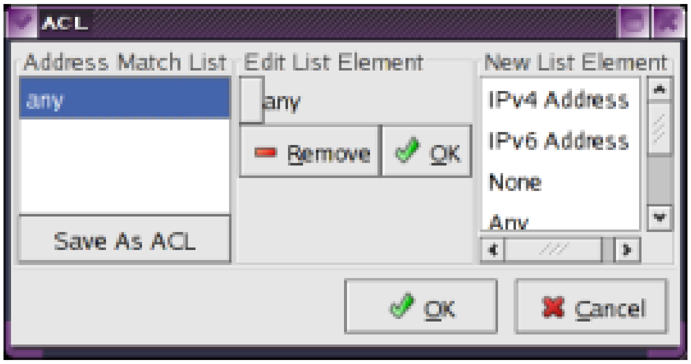
14.3 Editing view “From” and “To” ACLs

The “From:” and “To:” ACLs are displayed and can be edited separately, by double-clicking on the ACL row, or selecting the ACL row a pressing the “Properties” , or by pressing and releasing the right-hand mouse button over the ACL row and and selecting the “Edit...” option, or from the “View Options” edit dialog as the “match-clients” and “match-destinations” options.

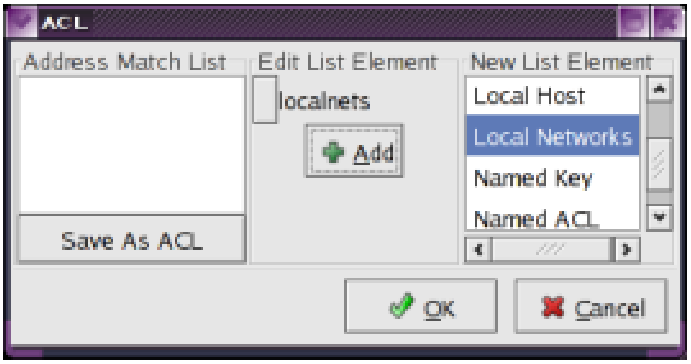
14.4 Creating “split DNS” Views

A typical use of Views is to split the DNS, by presenting different views to internal and external clients. To do this, we’ll specify that the new “default” view can be shown only to clients from the local area network (LAN), by setting the “From:” and “To:” ACLs to be “localnets”, meaning an address on one of the subnets that are configured on the local interfaces:

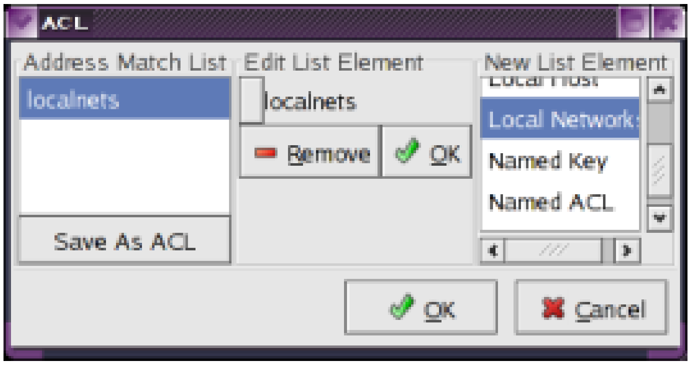
For both the “From:” and “To:” ACLs, edit the ACLs to remove the “any” address match list element and add the “localnets” address match list element:



Click on the “Remove” button to remove the “any” element.

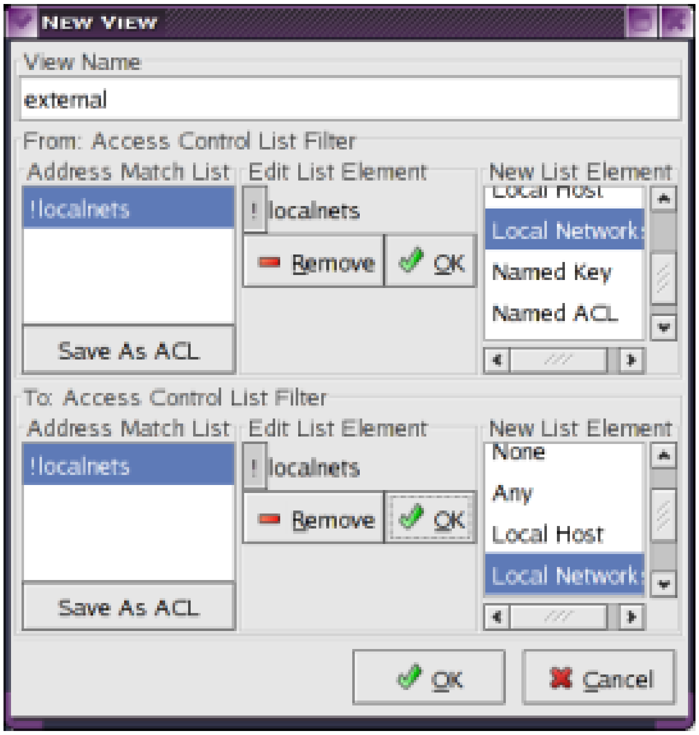


Select the “Local Networks” element and click the “Add” button.



Repeat for the “To:” ACL .

Then create a new view for external clients, with “From:” and “To:” ACLs set to the complement of “localnets” :

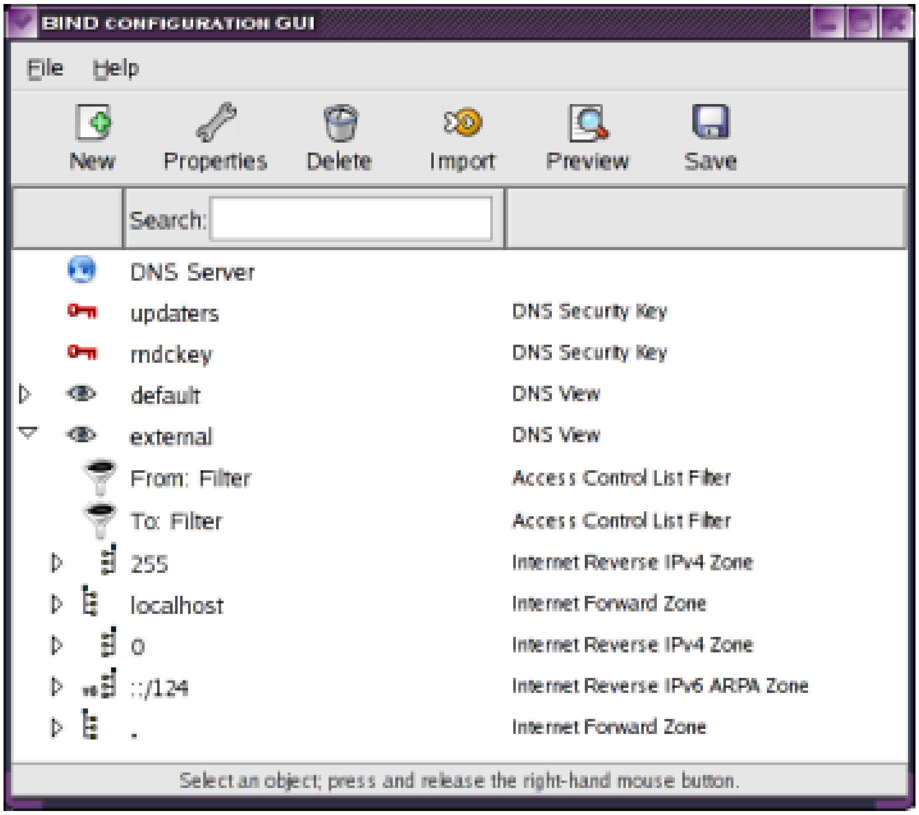


View Name: external

From: Address Match List: !localnets

To: Address Match List: !localnets

Clicking the “OK” button will create a new “external” view:



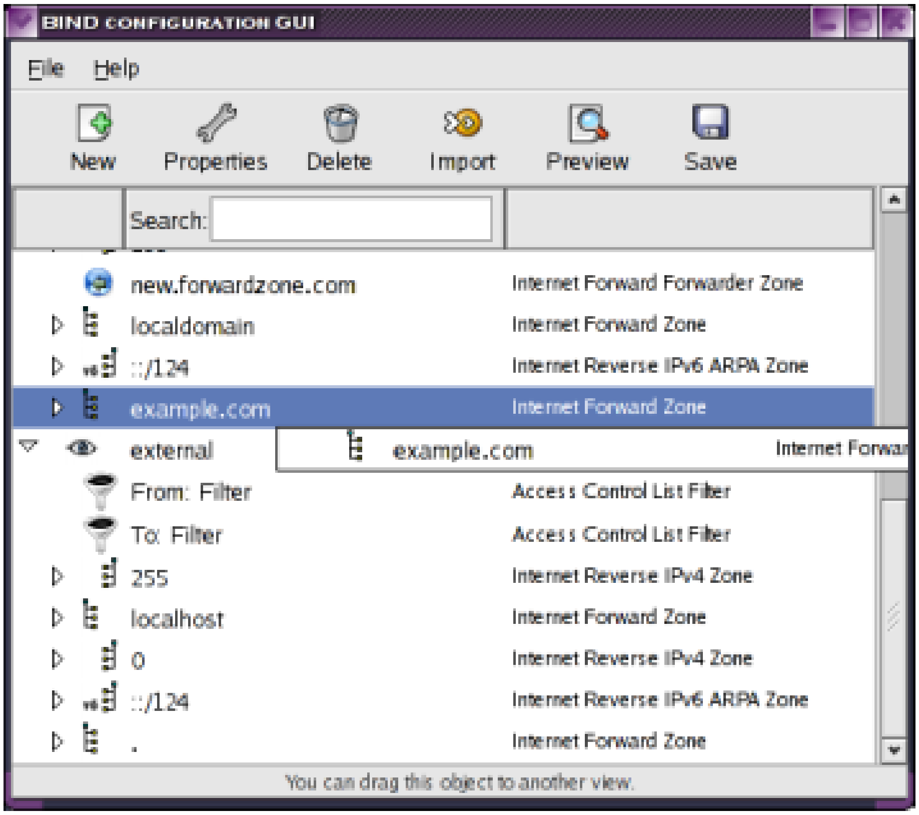
DNS Server	
updaters	DNS Security Key
rndckey	DNS Security Key
default	DNS View
external	DNS View
From: Filter	Access Control List Filter
To: Filter	Access Control List Filter
255	Internet Reverse IPv4 Zone
localhost	Internet Forward Zone
0	Internet Reverse IPv4 Zone
::/124	Internet Reverse IPv6 ARPA Zone
.	Internet Forward Zone

The mandatory top-level domains as defined in RFC 1912 are copied into the new view by default . Now only hosts from the LAN will see zones “example.com” and “2.168.192.in-addr.arpa” .

14.5 Copying or Moving Zones between Views

Having more than one view, you can drag zones from one view to another.

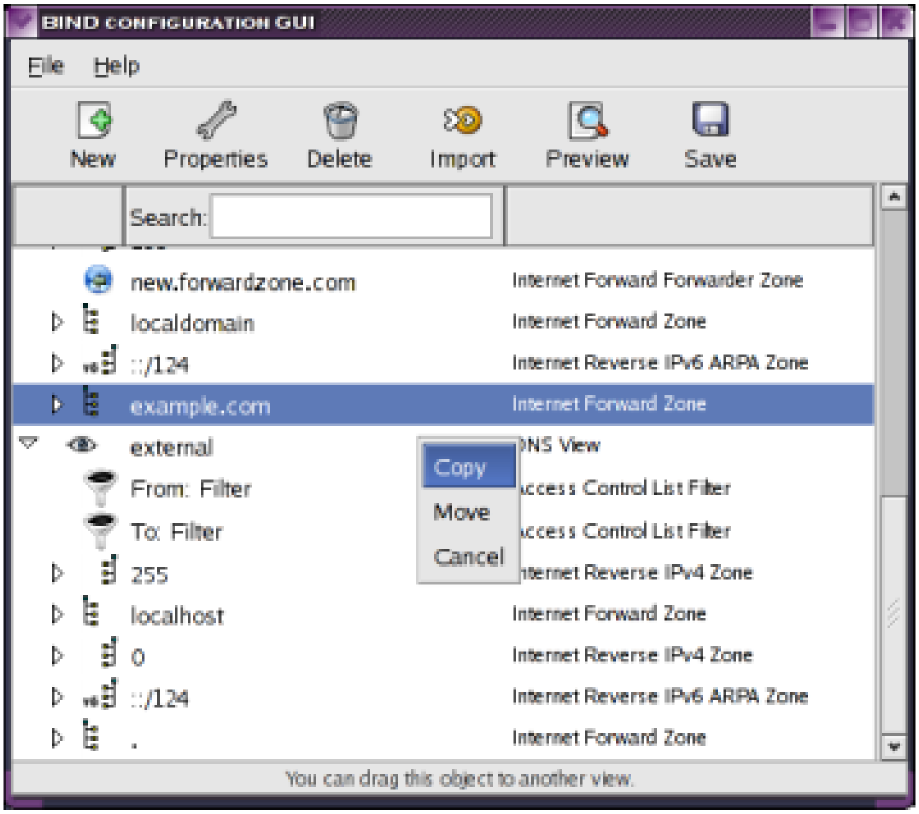
Select the zone you want to drag by pressing and holding (NOT releasing) the left-hand mouse button:



new.forwardzone.com	Internet Forward Forwarder Zone
localdomain	Internet Forward Zone
::/124	Internet Reverse IPv6 ARPA Zone
example.com	Internet Forward Zone
external	
From: Filter	Access Control List Filter
To: Filter	Access Control List Filter
255	Internet Reverse IPv4 Zone
localhost	Internet Forward Zone
0	Internet Reverse IPv4 Zone
::/124	Internet Reverse IPv6 ARPA Zone
.	Internet Forward Zone

You can drag this object to another view.

Then, without releasing the left-hand mouse button, drag the zone to the destination view and release the mouse button; the drag options menu pops up:

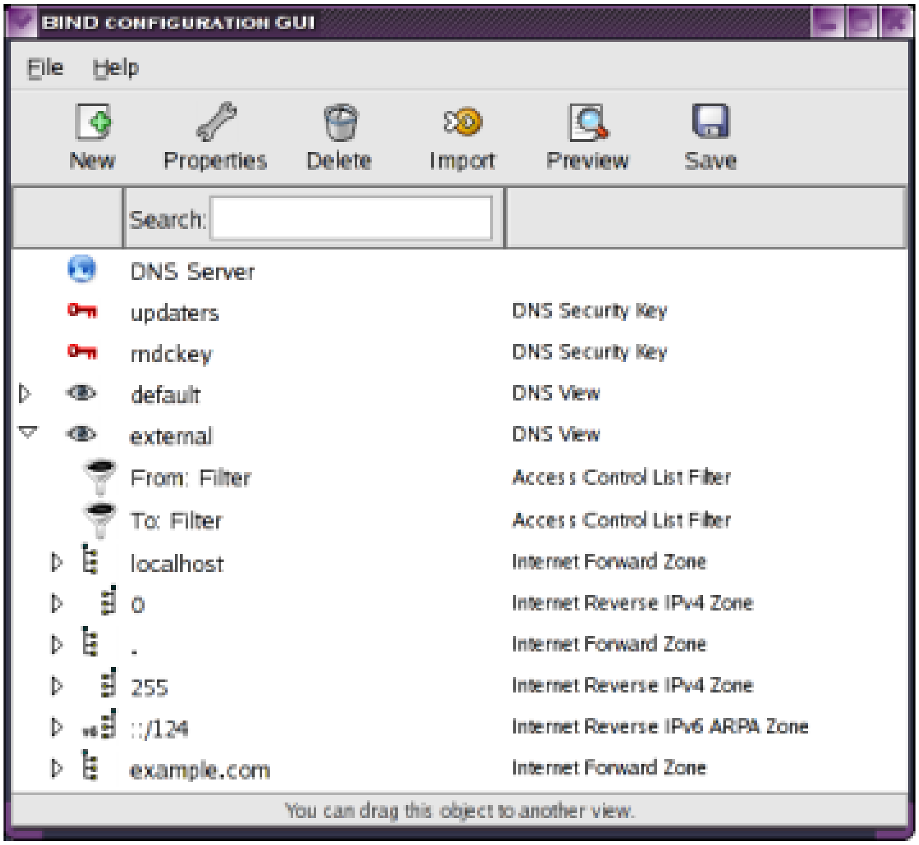


new.forwardzone.com	Internet Forward Forwarder Zone
localdomain	Internet Forward Zone
::/124	Internet Reverse IPv6 ARPA Zone
example.com	Internet Forward Zone
external	NS View
From: Filter	ccess Control List Filter
To: Filter	ccess Control List Filter
255	nternet Reverse IPv4 Zone
localhost	Internet Forward Zone
0	Internet Reverse IPv4 Zone
::/124	Internet Reverse IPv6 ARPA Zone
.	Internet Forward Zone

You can drag this object to another view.

Select “Copy” to copy the zone to the destination view; select “Move” to move the zone to the destination view.

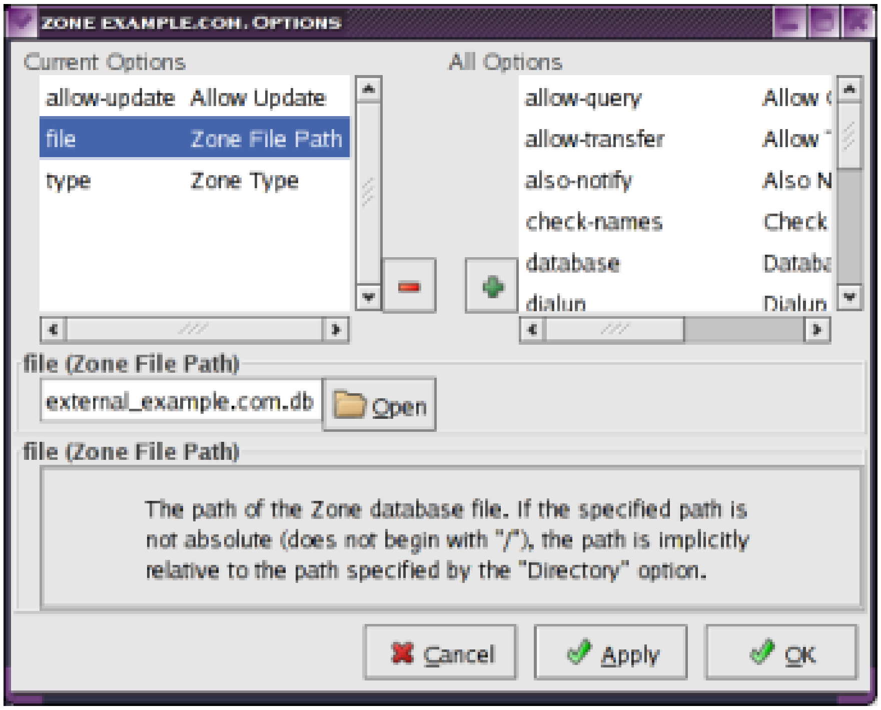
The “example.com” zone is now in the destination view:



DNS Server	
updaters	DNS Security Key
rndckey	DNS Security Key
default	DNS View
external	DNS View
From: Filter	Access Control List Filter
To: Filter	Access Control List Filter
localhost	Internet Forward Zone
0	Internet Reverse IPv4 Zone
.	Internet Forward Zone
255	Internet Reverse IPv4 Zone
::/124	Internet Reverse IPv6 ARPA Zone
example.com	Internet Forward Zone

You can drag this object to another view.

If the “Copy” option was chosen, the zone file for the zone in the destination view will be copied to a file named with a prefix of the view name:



Current Options:

allow-update	Allow Update
file	Zone File Path
type	Zone Type

All Options:

allow-query	Allow (
allow-transfer	Allow '
also-notify	Also N
check-names	Check
database	Databa
dialup	Dialup

file (Zone File Path): external_example.com.db

file (Zone File Path)

The path of the Zone database file. If the specified path is not absolute (does not begin with "/"), the path is implicitly relative to the path specified by the "Directory" option.

15 Enabling Zone Authentication Security (DNSSEC)

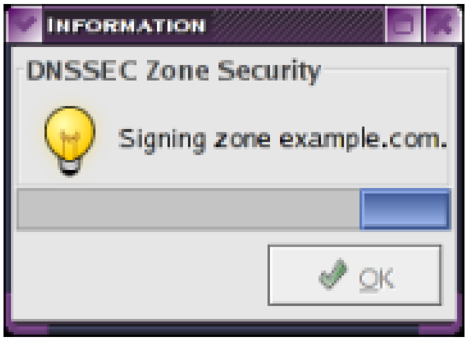
You can enable clients of your DNS Server to verify that query responses come from a trusted source (your DNS server) using DNSSEC – zones can be "Signed" with public keys distributed to clients.

15.1 Signing Zones

To enable DNSSEC zone signing, select a zone, press and release the right-hand mouse button, and select the "Sign..." option.

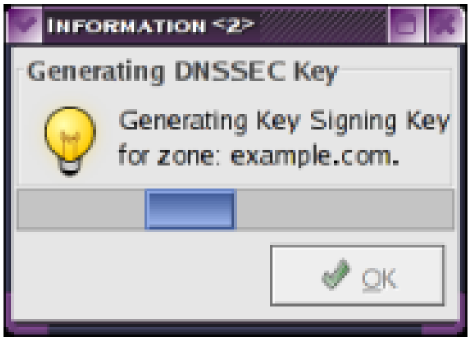
Zone signing involves generating public and private keys for signing the zone records (the Zone Signing Key or ZSK) and for signing the Zone Key records (the Key Signing Key or KSK) . The public keys must be distributed to clients.

If there are existing pubic and private keys both for Zone and Key signing, they will be used to sign the zone. If zone keys have not been generated for the zone, the Zone Key Generation dialog will be displayed:



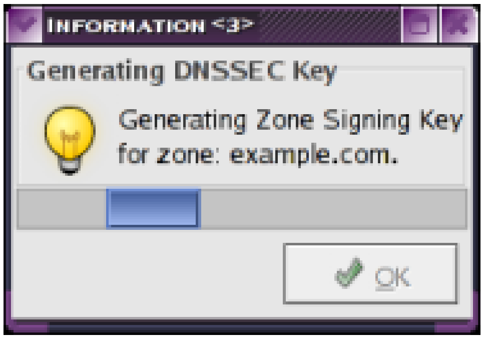
DNSSEC Zone Security

Signing zone example.com.



Generating DNSSEC Key

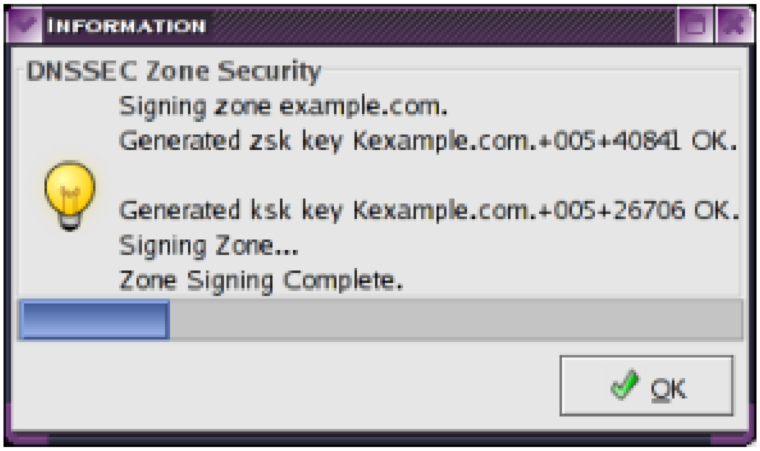
Generating Key Signing Key for zone: example.com.



Generating DNSSEC Key

Generating Zone Signing Key for zone: example.com.

The key generation processes can take some time (a few minutes) . When they are complete, the zone will be signed using the generated keys:



DNSSEC Zone Security

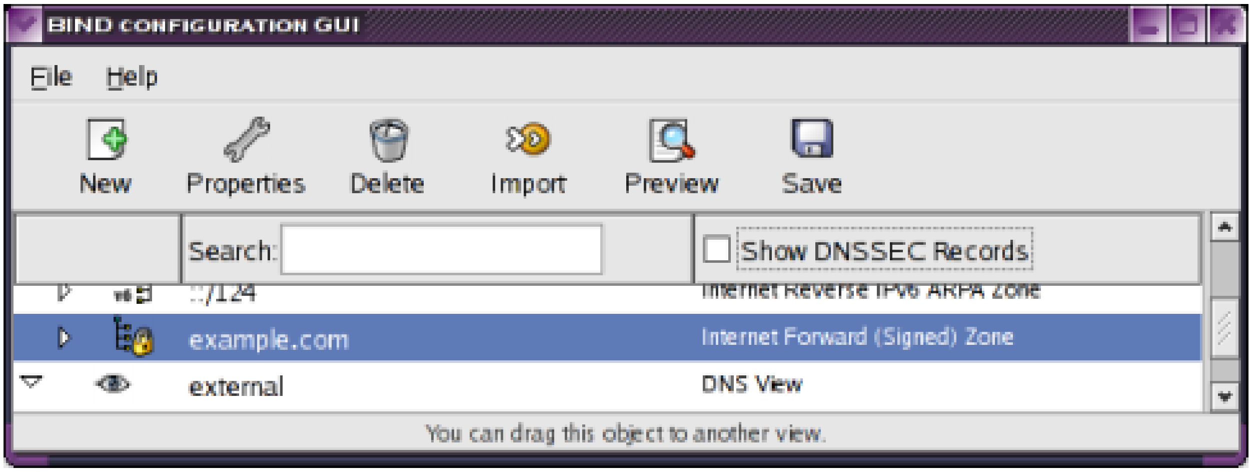
Signing zone example.com.
Generated zsk key Kexample.com.+005+40841 OK.

Generated ksk key Kexample.com.+005+26706 OK.
Signing Zone...
Zone Signing Complete.

These files will be created in the zone database file directory :

`Kexample.com+005+40841.key`	(the public zone signing key)
`Kexample.com+005+40841.private`	(the private zone signing key)
`Kexample.com+005+26706.key`	(the public key signing key)
`Kexample.com+005+26706.private`	(the private zone signing key)

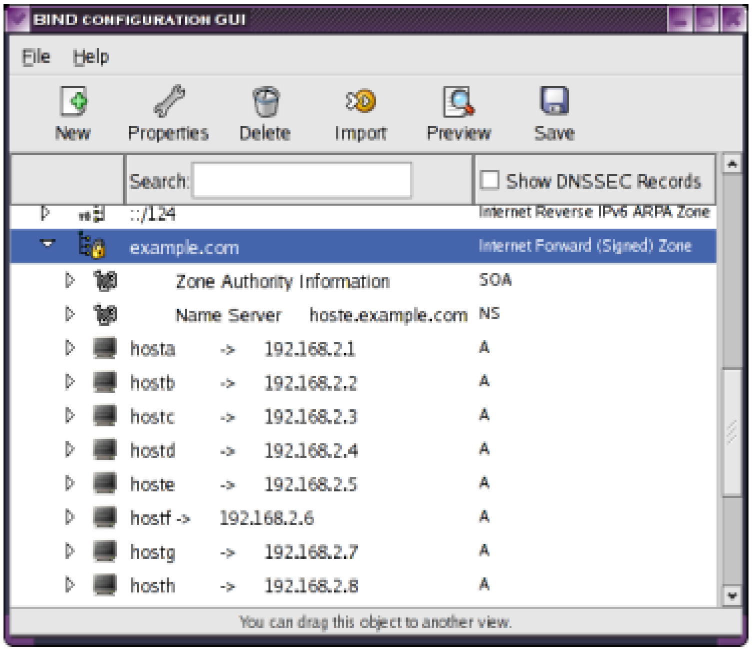
And the signed zone will be displayed :



::/124 Internet Reverse IPv6 ARPA Zone
example.com Internet Forward (Signed) Zone
external DNS View

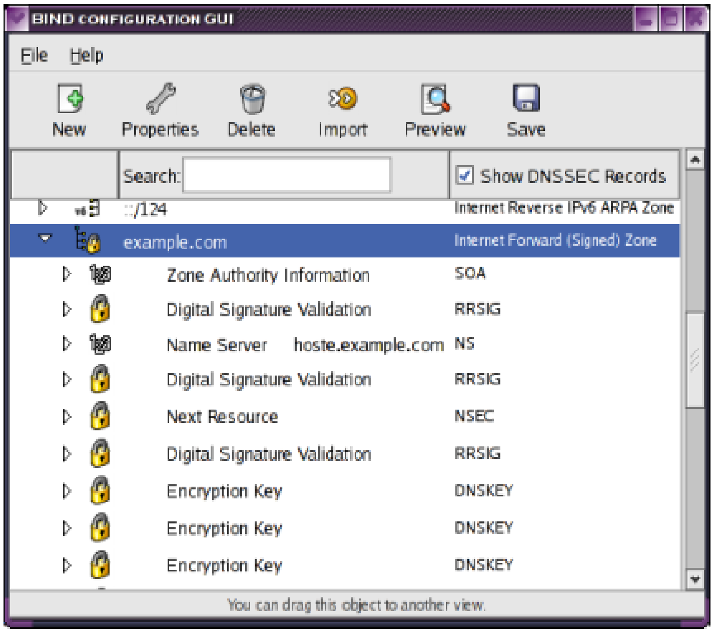
You can drag this object to another view.

By clicking the “Show DNSSEC Records” checkbox you can control whether or not to display DNSSEC records:



::/124 Internet Reverse IPv6 ARPA Zone
example.com Internet Forward (Signed) Zone
Zone Authority Information SOA
Name Server hoste.example.com NS
hosta -> 192.168.2.1 A
hostb -> 192.168.2.2 A
hostc -> 192.168.2.3 A
hostd -> 192.168.2.4 A
hoste -> 192.168.2.5 A
hostf -> 192.168.2.6 A
hostg -> 192.168.2.7 A
hosth -> 192.168.2.8 A

You can drag this object to another view.



::/124 Internet Reverse IPv6 ARPA Zone
example.com Internet Forward (Signed) Zone
Zone Authority Information SOA
Digital Signature Validation RRSIG
Name Server hoste.example.com NS
Digital Signature Validation RRSIG
Next Resource NSEC
Digital Signature Validation RRSIG
Encryption Key DNSKEY
Encryption Key DNSKEY
Encryption Key DNSKEY

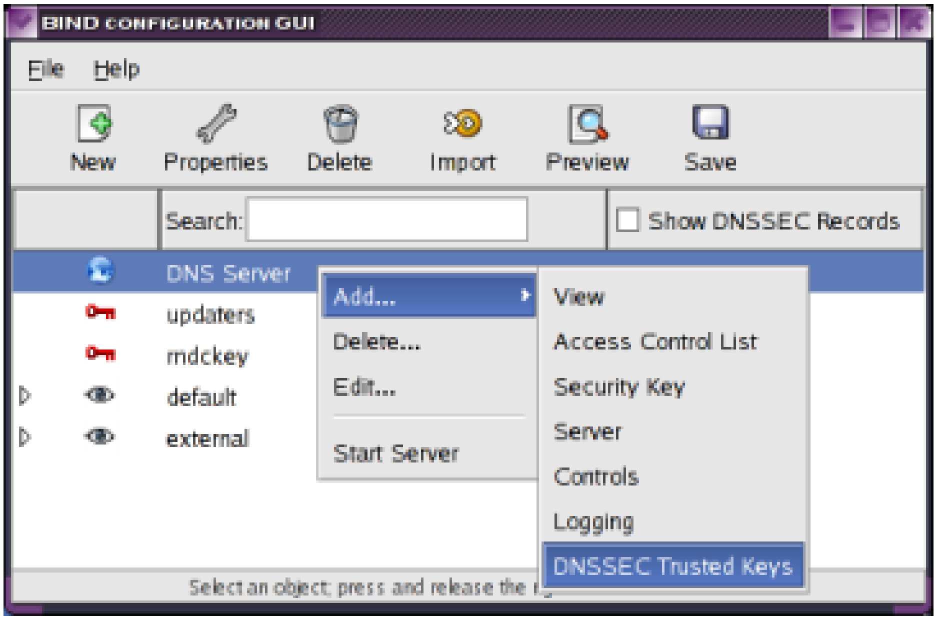
You can drag this object to another view.

Once a zone has been signed, if any zone contents are modified, or if the signature expires (it will be valid for one month) the zone will be automatically resigned when the zone is saved .

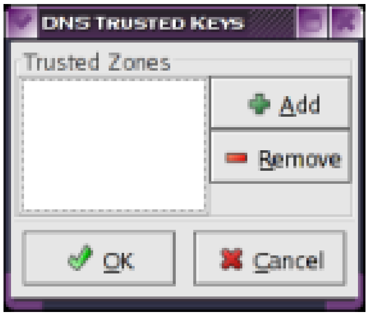
15.2 Importing Keys to Trust from another DNS server

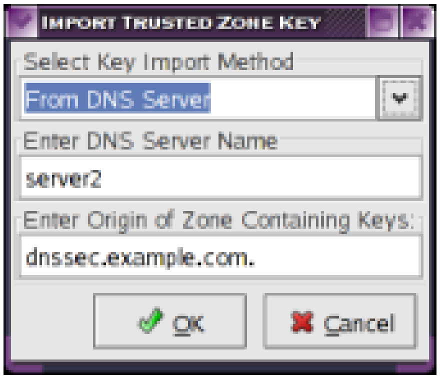
In order for DNSSEC signed zones to be validated by clients, every zone in the path from the root "." zone to the leaf zone must be signed with DNSSEC keys in each zone, or client DNS Servers must have the public DNSSEC keys installed in "trusted-keys" statements. For example, for a querying client DNS Server to validate the zone "host.example.com" using DNSSEC, the servers for zones ".", "com.", and "example.com." must all be signed with DNSSEC keys, and the "." zone must contain a "DS" (Delegation Signer) record for "com.", and the "com." server must contain a DS record for "example.com.", or the client must have a a key for "example.com." installed in its trusted keys. Because most public DNS servers of the top-level domains such as "." and "com." are not signed with DNSSEC yet, in order to provide a DNSSEC security "island" for "example.com.", validating clients must install "example.com."'s keys in their set of trusted keys.

To import keys for a zone into the server's trusted key set with `system-config-bind`, select the "DNS Server" row and either click on the "New" button or press and release the right-hand mouse button and select the "Add..." option, and then select the "DNSSEC Trusted Keys" option .



The "DNS Trusted Keys" dialog will be displayed. Click on the "Add" button to add a Trusted Zone:

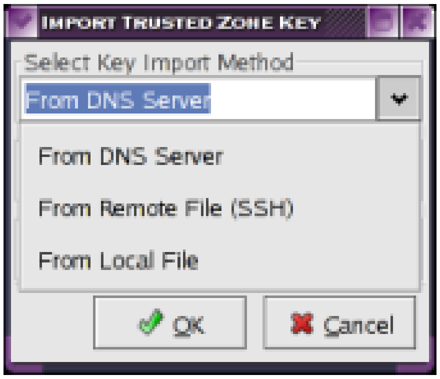




Select Key Import Method: From DNS Server

Enter DNS Server Name: server2

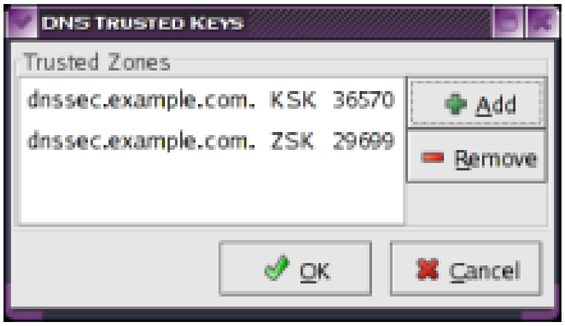
Enter Origin of Zone Containing Keys: dnssec.example.com.



As shown in the drop-down list in the third image above, three "Key Import Method"s are supported:

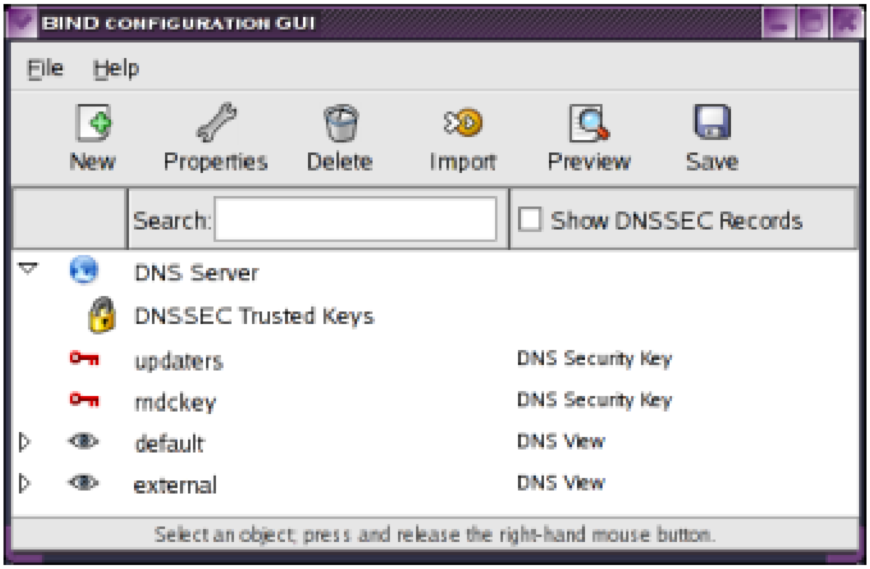
- "From DNS Server" : the remote DNS server is queried with DNS for the Zone's DNSKEY or KEY records (you must already trust that all DNS responses from the remote server will be authentic)
- "From Remote File": the key files are copied from remote DNS server with SSH (Secure Shell) . You will be prompted to enter your password on the remote server (passwords are sent encrypted and are not saved to disk). The Key files must be in the DNS Server Zone Database directory (`$ROOTDIR/var/named`) on the remote server.
- "From Local File" - The Key files must be in `$ROOTDIR/var/named` on the local server.

Once you are satisfied with the Import Method, DNS Server, and Zone Origin settings, click OK . The keys for the zone are then imported:



dnssec.example.com. KSK 36570
dnssec.example.com. ZSK 29699

You can then "Remove" some of the imported keys or "Add" more imported keys. Once you are satisfied with the list of trusted keys, click the "OK" button. The keys are then saved in the configuration:



DNS Server
DNSSEC Trusted Keys
updaters DNS Security Key
rndckey DNS Security Key
default DNS View
external DNS View

Select an object, press and release the right-hand mouse button.

The DNS server will now attempt DNSSEC validation of all records in the 'dnssec.example.com.' zone using the trusted keys we just installed. If a subzone of dnssec.example.com is created, say 'sub.dnssec.example.com.', all that is necessary is to sign the sub.dnssec.example.com using the same keys, or create a 'DS' record pointing to the new keys; it is not necessary to add new keys to the trusted key set for subzones of zones whose keys are already in the trusted key set.

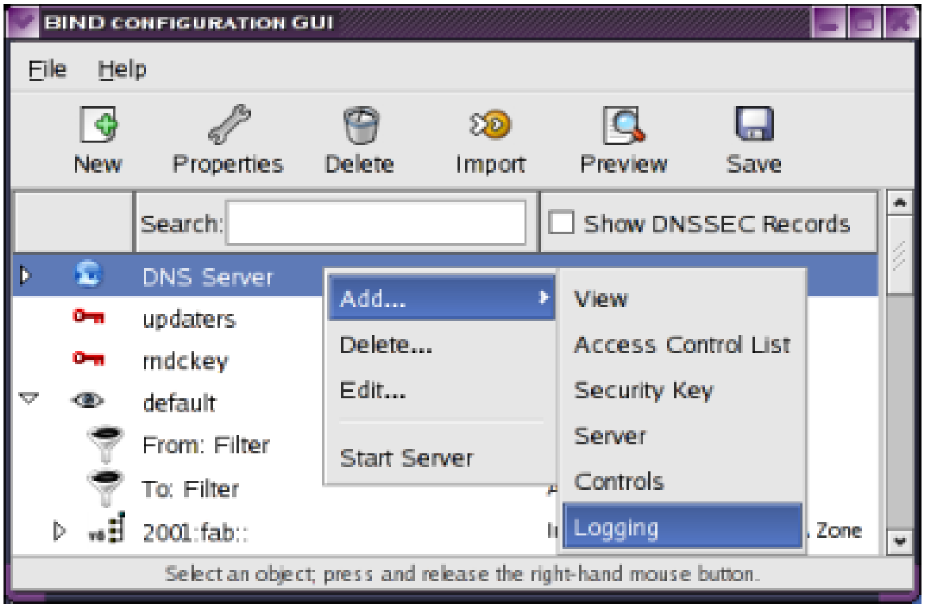
16 Controlling DNS Server Logging

By default, the `named` DNS server logs a minimal set of “info” messages during startup and shutdown and for error conditions to the system log using the `daemon syslogd(8)` facility, as controlled by `syslog.conf(5)`.

`named` can potentially log many other types of useful information, if instructed to do so with a custom Logging configuration.

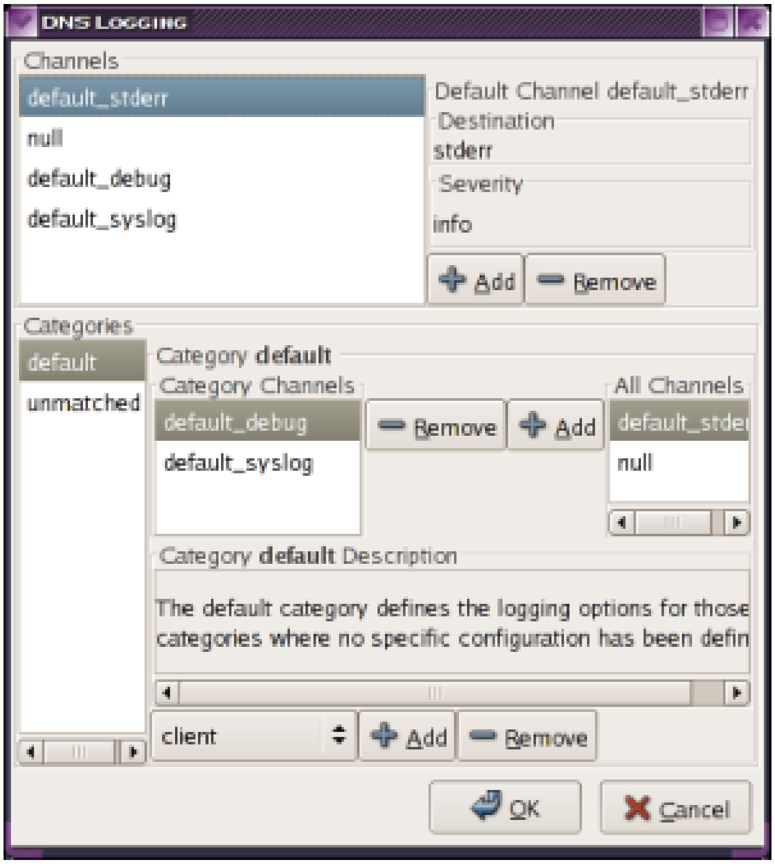
You can use system-config-bind to generate custom Logging configurations for `named` as follows.

Select the DNS server, and click on the “New” button, or press and release the right-hand mouse button and select the “Add...” and “Logging...” options from the popup menu:



Select an object; press and release the right-hand mouse button.

The DNS Logging Dialog is displayed:



The default category defines the logging options for those categories where no specific configuration has been defin `named`'s logging is controlled with Channels and Categories . Channels specify a logging destination and the severity of messages to be directed to it, while categories specify which types of message are to be directed to which Channels .

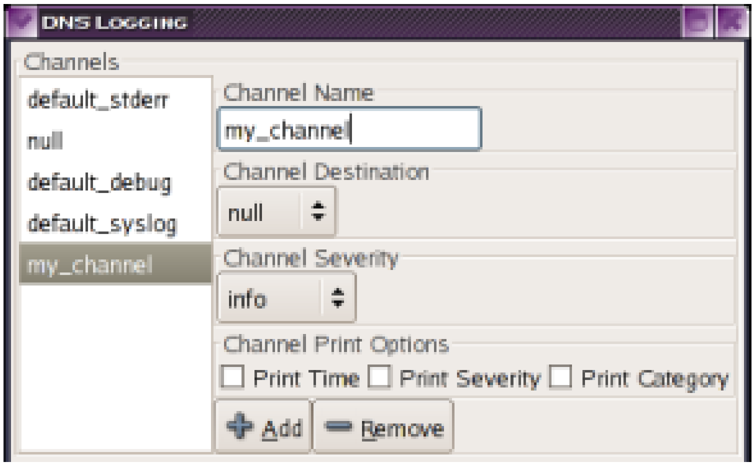
By default, named directs messages of a certain severity to the system log, the `default_syslog` channel, and debugging messages to the `default_debug` channel, which can be enabled by use of `named`'s `-d` option or by the '`rndc trace`' command. There are also the `default_stderr` channel, which directs messages to named's `stderr` output file descriptor (`/dev/null` by default), and `null`, a message sink to which messages to be discarded can be directed ; by default, no message Categories are directed to these channels .

You cannot modify the default channels, but you can modify which messages are directed to them , and create new channels to which any message category may be directed .

The two default Categories are the "catch all" categories `default` , which matches messages which are directed to the default syslog and debug channels by default, and `unmatched` , which matches messages which match no other category, which is directed to null by default.

16.1 Creating a new Logging Channel

You can create new logging Channels to specify new logging destinations for messages of certain severities . To create a logging channel, click on the Add ('**+**') button in the Channels frame:

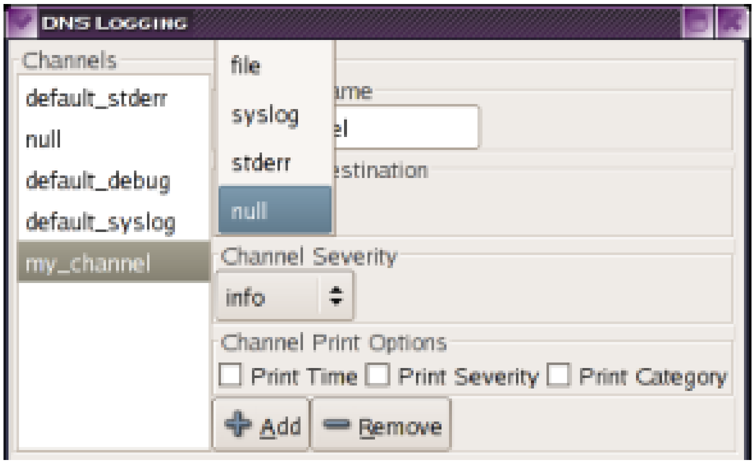


Channel Name: my_channel
Channel Destination: null
Channel Severity: info

Type a name for the new channel in the "Channel Name" entry.

16.1.1 Setting the Logging Channel Destination

Select a destination type from the "Channel Destination" list:



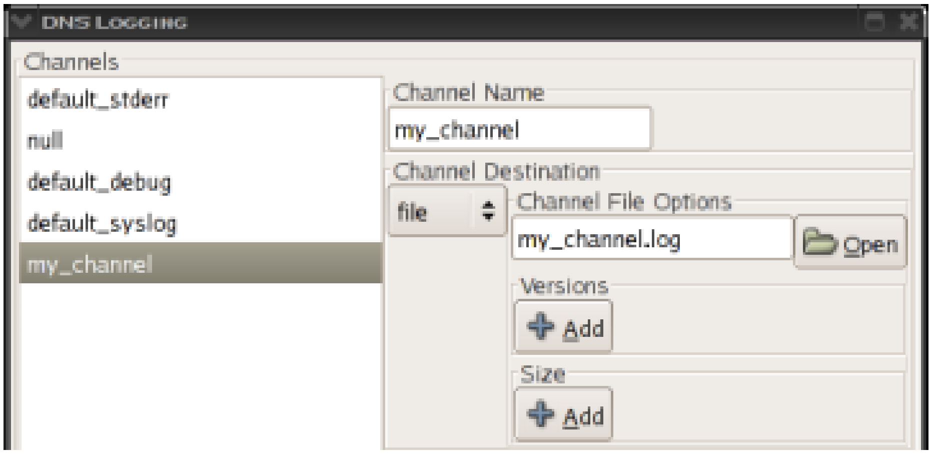
Channel Severity: info

Destination Types:

file : The log messages will be stored in the named file, and you can specify maximum file size and versions to retain
syslog: The log messages will be sent to the system logging daemon `syslogd(8)`, and you can choose the priority
stderr: The log messages will be written to named's process output, which is closed unless stderr channels are defined
null : The log messages will be discarded

16.1.2 Specifying the File Logging Destination

Choose the "file" destination from the "Channel Destination" list.

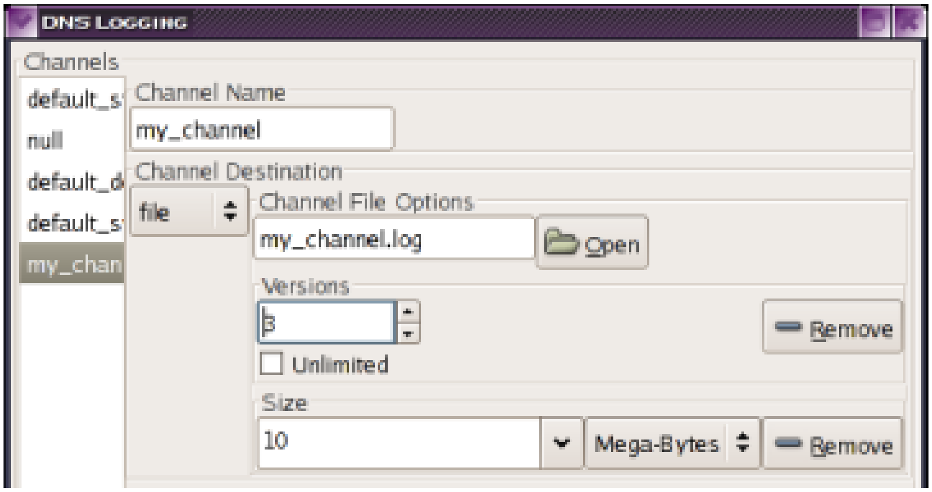


Channel Name: my_channel
Channel Destination: file
Channel File Options: my_channel.log

Type the name of a file in the Entry box in the Channel File Options frame. By default, the file name will be relative to the `$ROOTDIR/var/named` directory . Absolute file names (beginning with '/') are also allowed. You can select an new location for the file by clicking on the "Open" button and completing the File Selection dialog .

NOTE: The `named:named` user must have write access to the log file location .

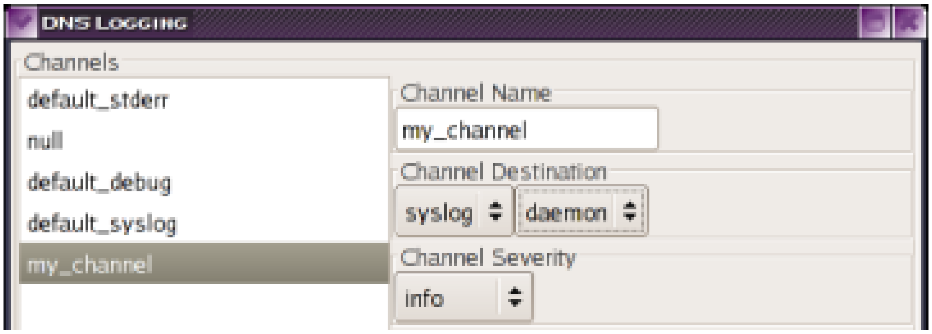
You can specify the maximum file size of the log file by clicking on the "Add" ('**+**') button in the "Size" frame, and the number of Versions of the file to keep by clicking on the "Add" ('**+**') button in the "Versions" frame:



Channel Name: my_channel
Channel Destination: file
Channel File Options: my_channel.log
Versions: 3
☐ Unlimited
Size: 10 Mega-Bytes

Check the "Unlimited" check box to not limit the number of versions of the file that will be retained .

16.1.3 Specifying the `syslog` Channel Destination



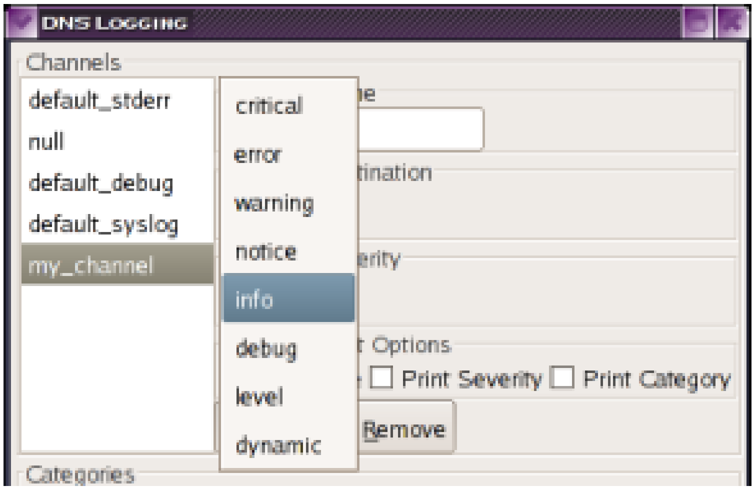
Channel Name: my_channel
Channel Destination: syslog daemon
Channel Severity: info

Choose the "syslog" destination from the "Channel Name" destination list . Select the syslog facility to use from the option list – see `man syslog.conf(5)` for details of available facilities.

16.1.4 Selecting the Severity of Messages to be logged to the Channel

You can select the Severity of the messages to be logged to the Channel by using the “Channel Severity” option list.

Only messages of the selected Severity or higher will be logged .



16.1.5 Selecting the Message Header fields to be Printed for the Channel

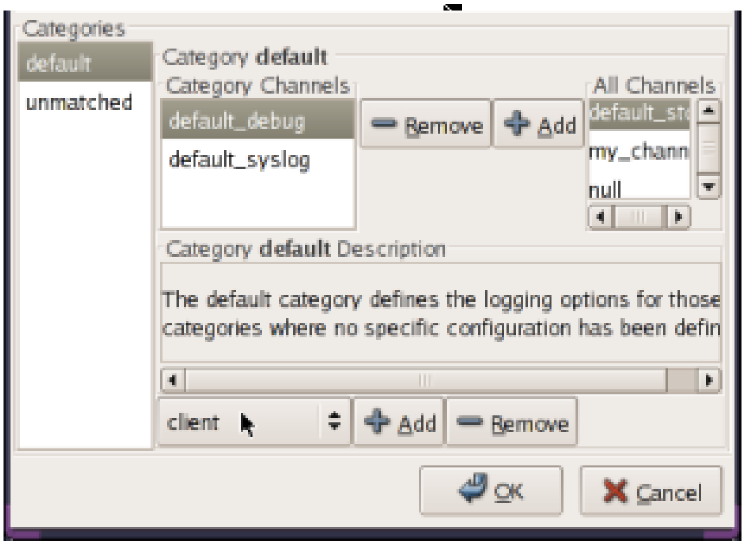
Using the “Print Time”, “Print Severity” and “Print Category” you can select what fields are printed in the header of each message on the channel. For instance , with the message :

```
01-Apr-2005 12:00:01 general : info   : starting BIND 9.3.1
     TIME          CATEGORY  SEVERITY
```

would be printed as above if all the “Print” check boxes were checked .

16.2 Defining Logging Categories to be Output on certain Channels

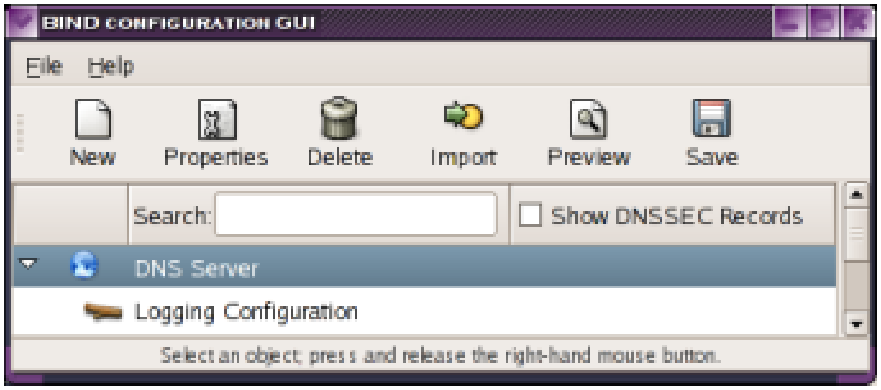
You can direct log message Categories to be output on certain channels using the “Categories” frame of the Logging dialog:



The default category defines the logging options for those categories where no specific configuration has been defin

Select a Category to Edit in the “Categories” list – the “Category” frame allows you to edit it by Adding or Removing Channels to the “Category Channels” list. You can remove the selected Channel from the “Category Channels” list by clicking on the “**-** Remove” button to the left of the “Category Channels” list. You can add a Channel to the “Category Channels list by selecting a channel in the “All Channels” list and clicking on the “**+** Add” button to its left . You can Add a new Category to the “Categories” list by choosing a Category from the popup list (showing “client” with an arrow above) and clicking on the “**+** Add” button to its right. You can remove a Category by selecting it in the Categories list and clicking the lower right “**-** Remove” button. See the ARM about logging Categories.

You can Save the modified logging configuration by clicking on the “OK” button. The Logging configuration is displayed under the “DNS Server” entry in the Zone List:



You can re-edit the Logging Configuration by double-clicking on it, by selecting it and pressing the Properties button, or by pressing and releasing the right-hand mouse button over it and selecting “Edit” from the popup menu.

You can delete the Logging Configuration by selecting it and pressing the Delete button or by pressing and releasing the right-hand mouse button over it and selecting “Delete” from the popup menu.

17 Configuring DNS Server Controls

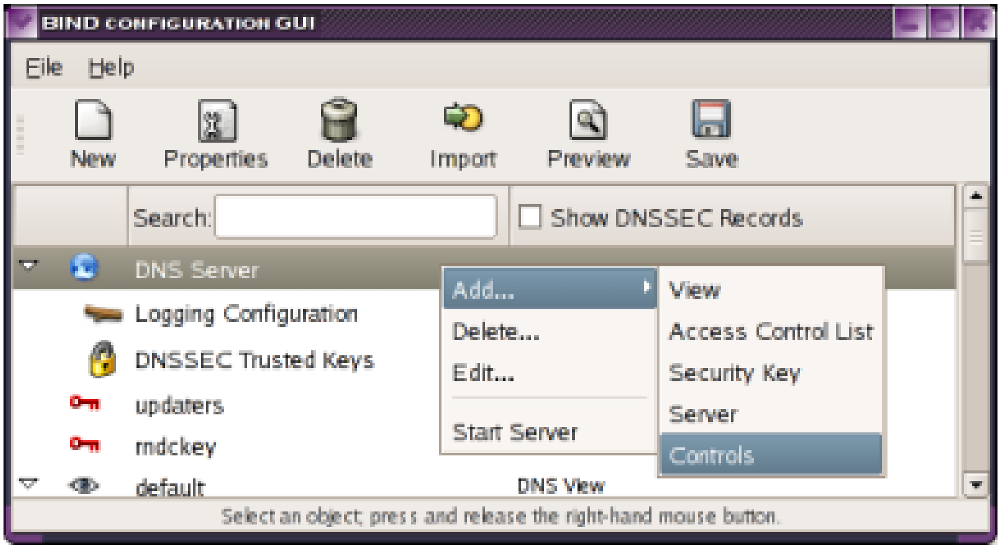
You can configure `named`’s control channels and authentication for applications such as `rndc(8)` which send commands to the server to shut down, reload, or perform maintenance and diagnostic functions with DNS server controls.

By default, `named` allows ONLY the `rndc(8)` application using the control channel on IPv4 address 127.0.0.1 , port 953, using the TSIG key “`rndckey`” defined in the `rndc.key` file, to control it.

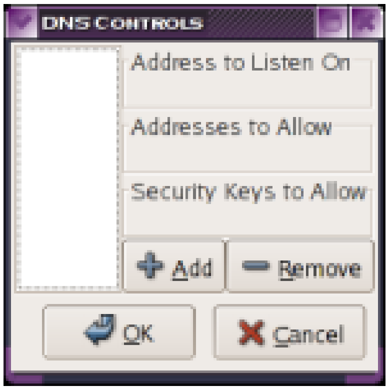
You can direct `named` to listen to other control channels and accept other TSIG keys using DNS Server Controls .

17.1 Adding a New DNS Server Control Channel

Select the “DNS Server” row, and click on the “New” toolbar button or press and release the right-hand mouse button and select “Controls” from the “Add” sub-menu:

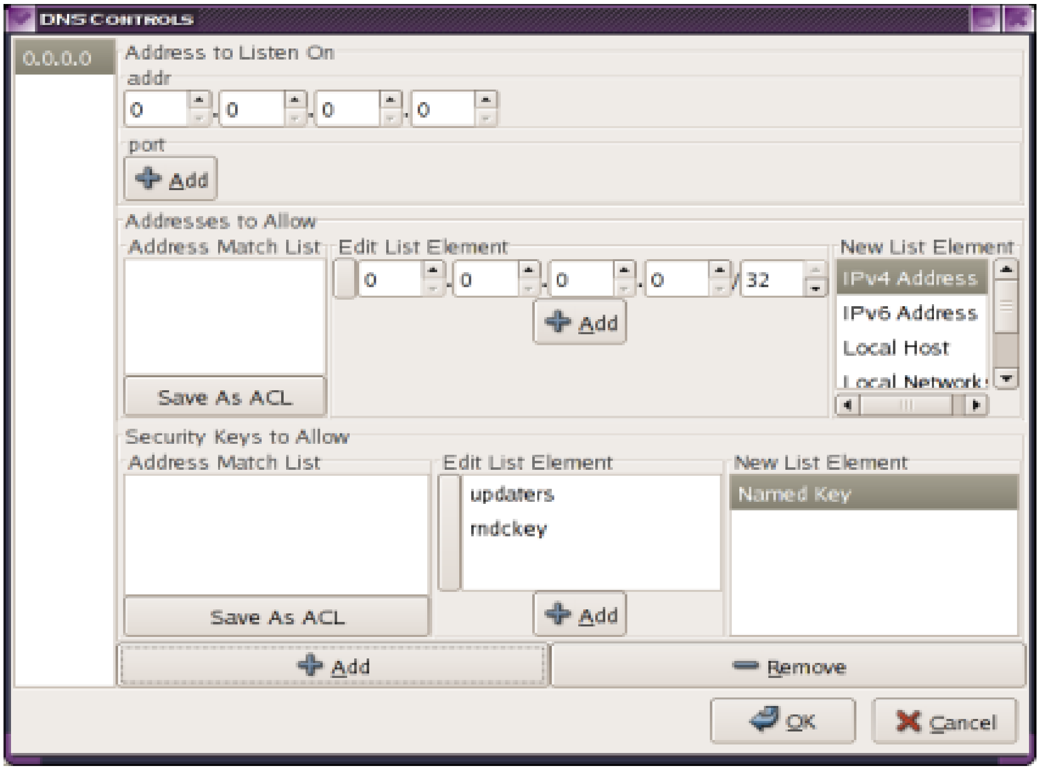


The “DNS Controls” dialog is displayed :



You cannot edit or delete the default “rndc” control channel, so it is not displayed .

Click on the “**+**Add” button to add a control channel. The “DNS Control” dialog is displayed:



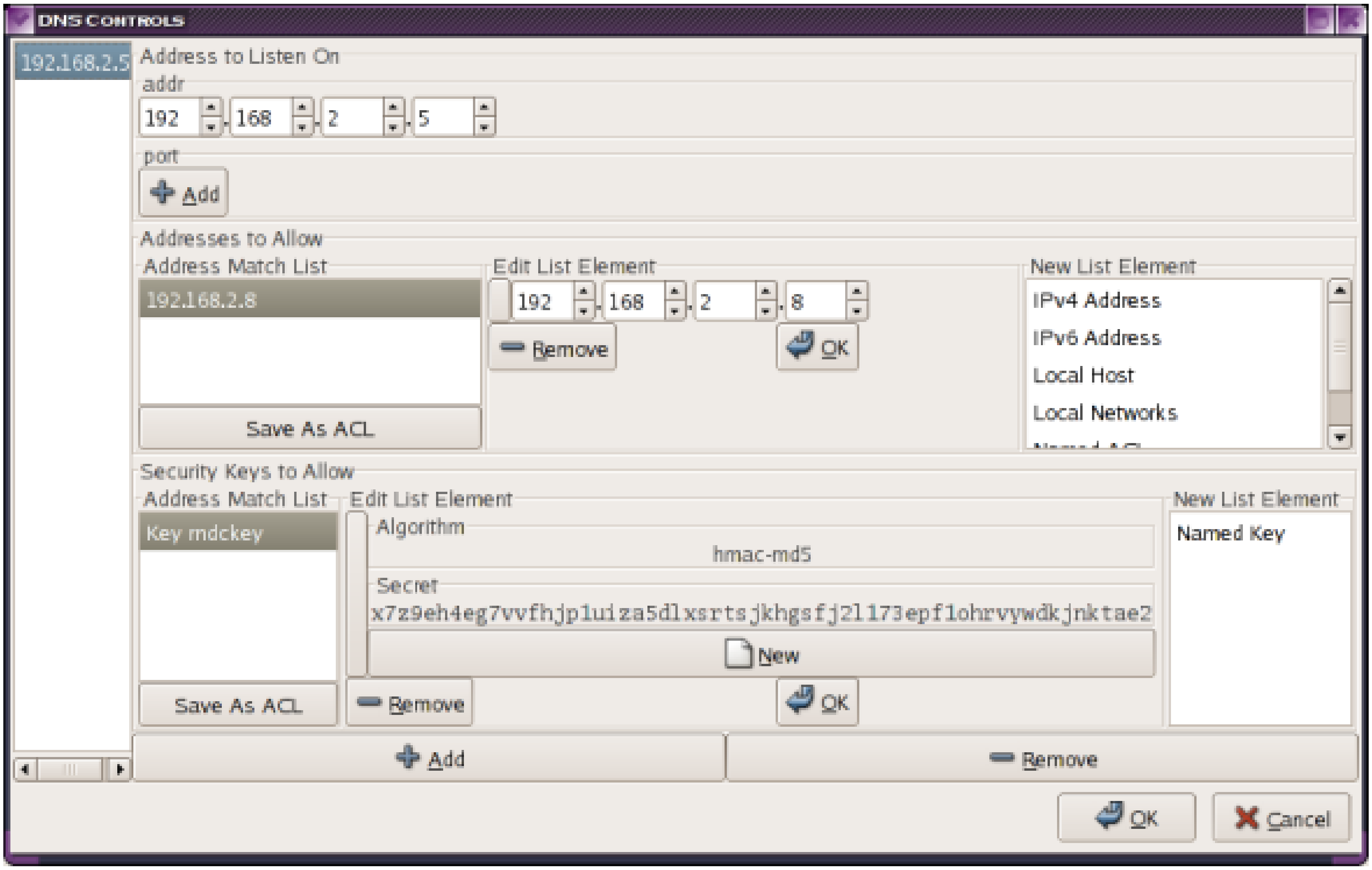
In the List on the Left, the Addresses to Listen On are displayed. You can add a new address to listen on by filling out the address in the “Address” frame.

You can Allow control connections only from certain addresses by filling out the optional “Addresses To Allow” ACL as for ACLs described above.

You can select control connections only signed with a certain named key by filling out the “Security Keys To Allow” ACL as for ACLs described above.

Click OK to save the Control Channel or Cancel to discard it.

An example showing a control channel listening on the 192.168.2.5 interface for control connections only from 192.168.2.8 with key “rndckey” is shown below.



192.168.2.5

addr: 192 . 168 . 2 . 5

192.168.2.8

Edit List Element: 192 . 168 . 2 . 8

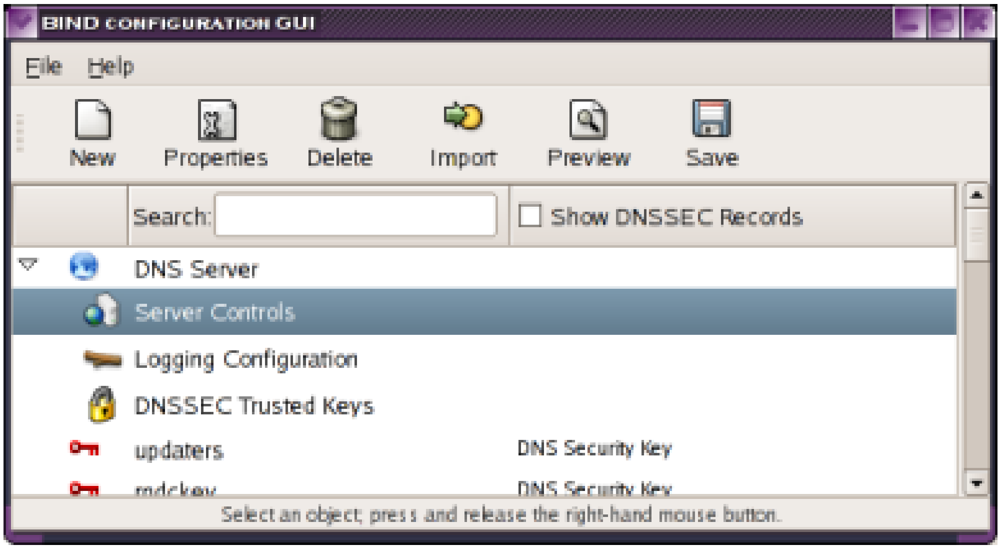
Key rndckey

Algorithm: hmac-md5

Secret: x7z9eh4eg7vvfhjp1uiza5dlxsrtsjkhgsfj21173epf1ohrvywdkjnktae2

Click “OK” to save the control channel.

The new controls are then shown under the “DNS Server” in the Zone List:



DNS Server
Server Controls
Logging Configuration
DNSSEC Trusted Keys
updaters DNS Security Key
rndckey DNS Security Key

Select an object, press and release the right-hand mouse button.

You can re-edit the Controls by double clicking on it, selecting it and clicking on the “Properties” tool-bar button, or pressing and releasing the right-hand mouse button over it and selecting “Edit” .

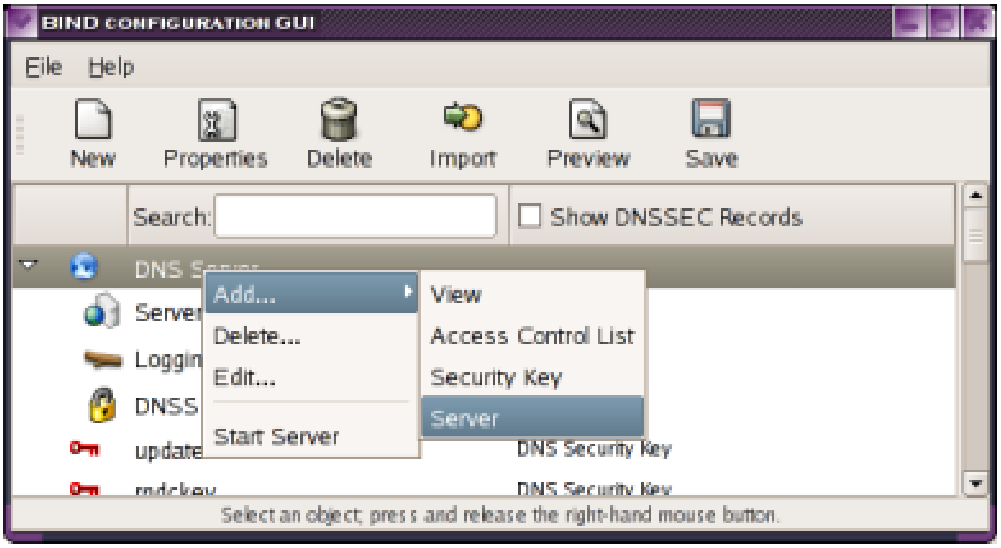
You can delete the Controls by selecting it and clicking on the “Delete” tool-bar button, or pressing and releasing the right-hand mouse button over it and selecting “Delete” .

18 Specifying Options for Remote DNS Servers

You can specify options for remote DNS Servers that your DNS Server will communicate with by creating Server objects and specifying Options for them .

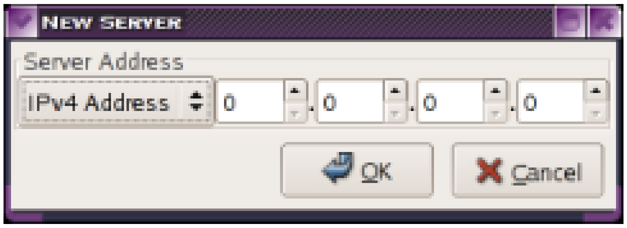
18.1 Creating a Server object

Select the DNS Server row in the Zone List and press on the "New" toolbar button and select "Server" or press and release the right-hand mouse button over it and select "Server" from the "Add" sub-menu:



Select an object; press and release the right-hand mouse button.

The "New Server" dialog is displayed:

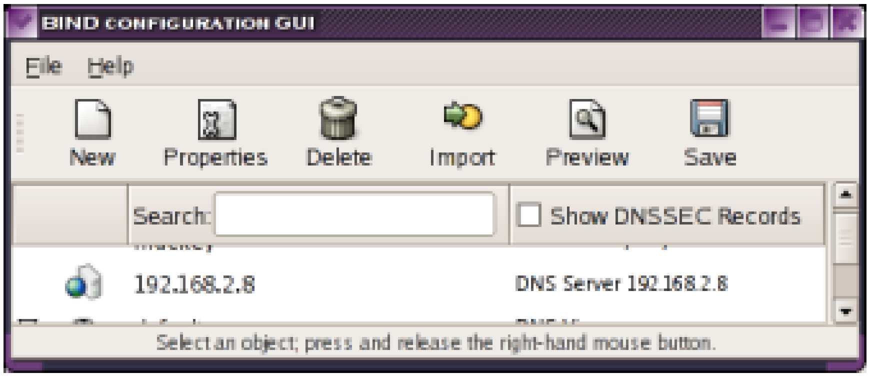


0 . 0 . 0 . 0

Type in the IPv4 address of the remote DNS Server, or select "IPv6 Address" from the "Server Address" option list and type in the server address.

Click on the "OK" button to create the Server object.

The Server object is displayed in the Zone List:



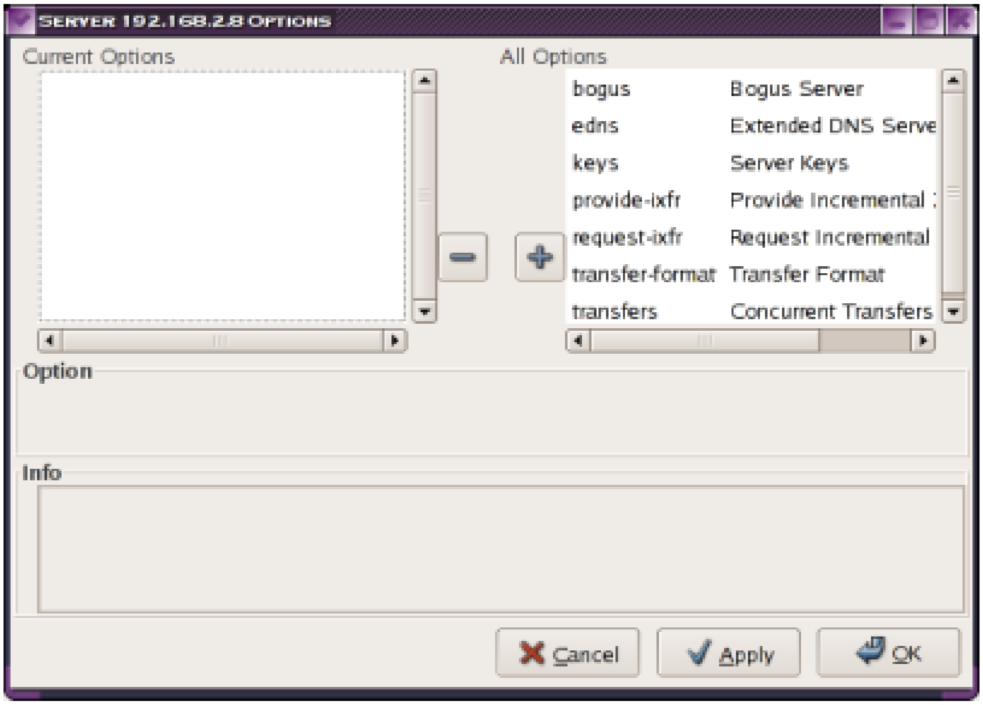
192.168.2.8 DNS Server 192.168.2.8

Select an object; press and release the right-hand mouse button.

18.2 Editing Remote Server Options

You can edit the Options for the server in the same way as DNS Server, Zone or View options by double-clicking on it, or by selecting it and pressing the properties button , or by pressing and releasing the right-hand mouse button over it and selecting "Edit" from the popup menu.

The “Server Options” dialog is displayed :

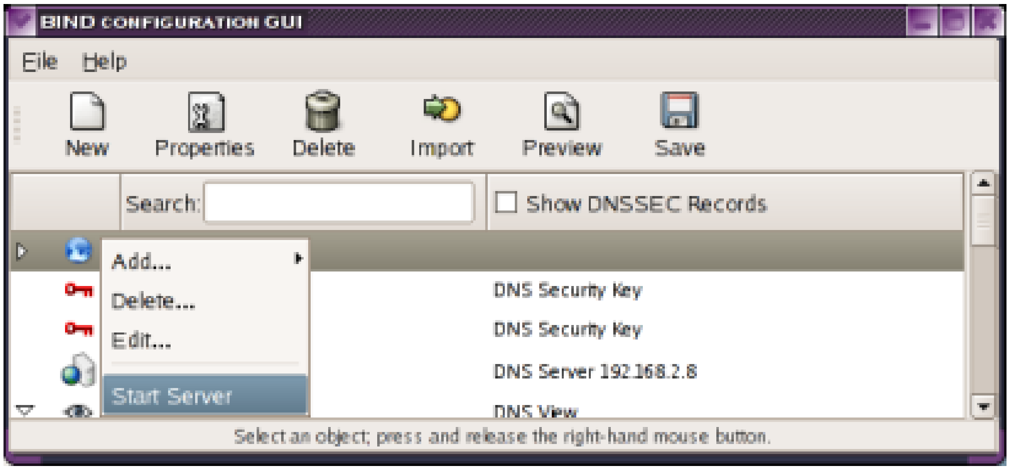


bogus	Bogus Server
edns	Extended DNS Serve
keys	Server Keys
provide-ixfr	Provide Incremental :
request-ixfr	Request Incremental
transfer-format	Transfer Format
transfers	Concurrent Transfers

You can edit these options in the same way as described in the sections on editing DNS Server and Zone options above.

19 Starting, Stopping and Restarting the DNS Server

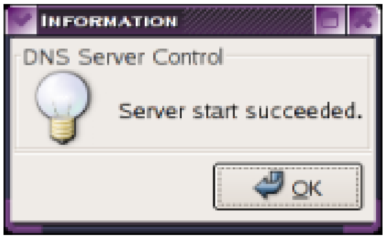
You can Start, Stop or Restart the DNS Server by selecting the “DNS Server” row in the Zone List, pressing and releasing the right hand mouse button, and selecting the required option :



DNS Security Key
DNS Security Key
DNS Server 192.168.2.8
DNS View

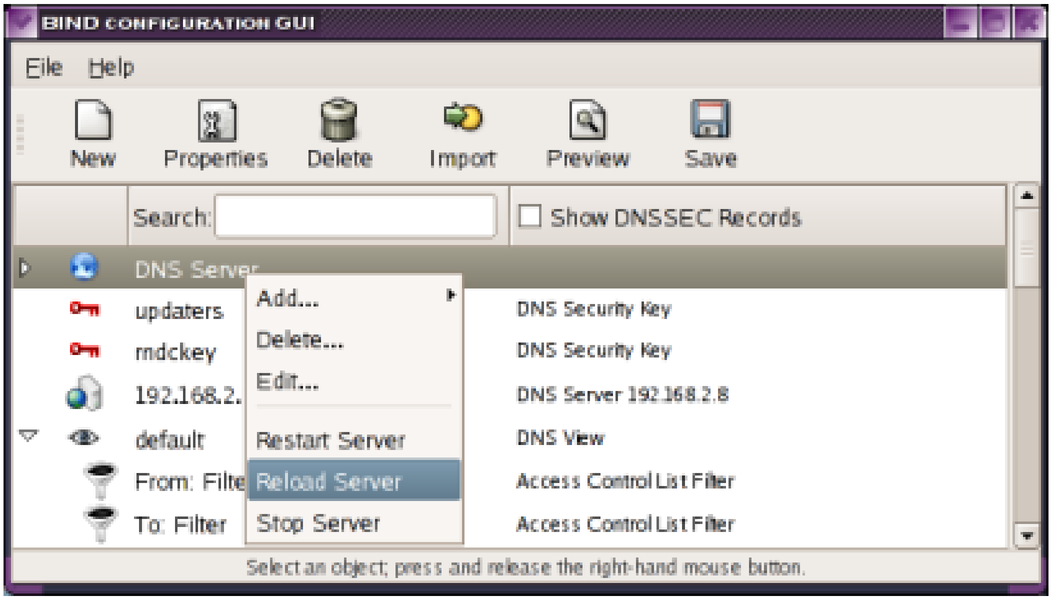
Select an object; press and release the right-hand mouse button.

The server start status dialog is displayed:



Server start succeeded.

Once the server is started, or if it was already running, you will be presented with options to stop or restart the server in the same manner:

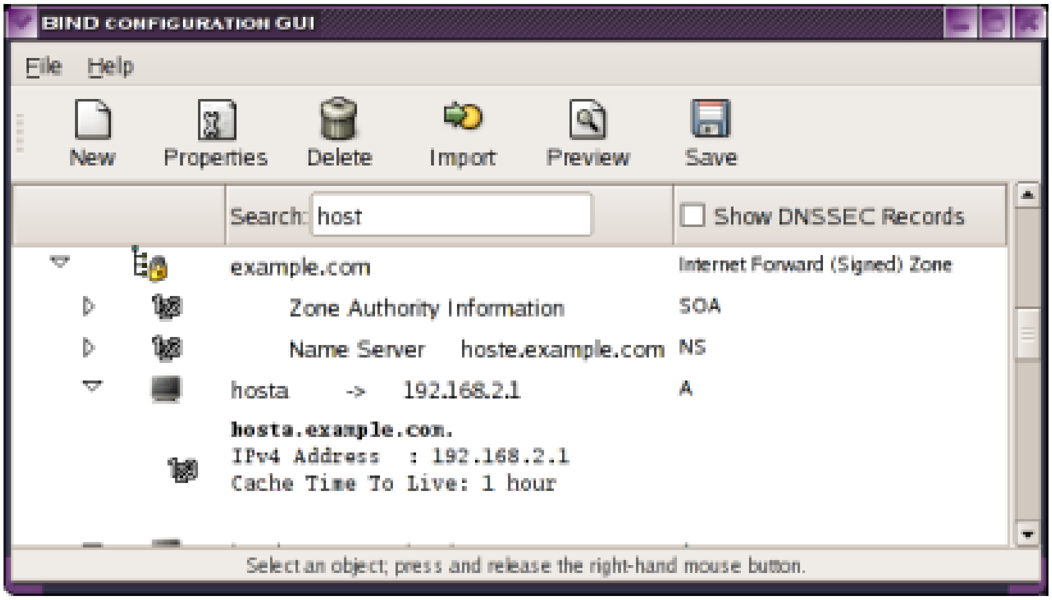


Select an object; press and release the right-hand mouse button.

If the server is currently running when the configuration is saved, it will be automatically restarted and you will be notified of the success or failure of the restart .

20 Using the Search Facility

You can quickly scroll to and highlight any object in the DNS configuration containing a search string by typing into the "Search" entry . All entries whose DNS names are prefixed by the search string are expanded and the Zone List scrolls to the first occurrence of a search string prefix:



Search: host

```
hosta.example.com.
IPv4 Address   : 192.168.2.1
Cache Time To Live: 1 hour
```

Select an object; press and release the right-hand mouse button.

21 APPENDIX A : Bug Reporting

Please report any bugs found, appending any occurences of files matching `$ROOTDIR/var/named/*.REJECT*`, to

https://bugzilla.redhat.com/bugzilla/enter_bug.cgi?component=system-config-bind