BIND 9.2.0 Release Notes

HP-UX 11i v1

invent

Manufacturing Part Number: 5991-0757

December 2004

United States

Legal Notices

Printed in the US

TradeMark Notices

Contents

1 New and Changed Features

BIND 9.2.0 is available on HP-UX 11i v1 platform as a Web upgrade. Most of the features available in previous versions of BIND are supported in BIND 9.2.0 with additional functionality.

Summary of BIND 9.1.3 Features Supported in BIND 9.2.0

This section lists the BIND 9.1.3 features that are supported in BIND 9.2.0.

- RFC 1995 (*Incremental Zone Transfer*)
- DNS Security (DNSSEC)
- Dynamic DNS Update
- TSIG-based Transaction Security
- Lightweight Resolver Library and Daemon
- Extended Configuration Syntax and Options
- Improved Logging Mechanism

NOTE

For information on the above features, refer to the BIND 9.1.3 Release Notes available at: `http://www.docs.hp.com/hpux/netcom/index.html#Internet%20Services`

New BIND 9.2.0 Features

This section describes the new features in BIND 9.2.0.

New Options in Options Statement

The following lists the new options added in the Options statement:

- dump-file

  This option is used to specify the pathname of the file to which the server dumps the database with the rndc dumpdb command. Default is named_dump.db. The syntax of dump-file option in the Options statement in the /etc/named.conf file is as shown below:

  ```
  dump-file “path_name”;
  ```

  where:

  path_name specifies the file to which the server dumps the database.

- statistics-file

  This option is used to specify the pathname of the file in which the server appends statistics using the rndc stats command. Default is named.stats in the server’s current directory. The syntax of statistics-file option in the “Options” statement in the /etc/named.conf file is as shown below:

  ```
  statstics-file “path_name”;
  ```

  The statistics file generated by BIND 9.2.0 is similar, but not identical, to that generated by BIND 8.1.2. For information on the format of the statistics file and the statistics counters, refer to the named-conf(1) man page distributed with this release.

- blackhole

  This option is used to specify a list of addresses from which the server will not accept queries or and does not use them to resolve a query. Default is none. The syntax of blackhole option in the “Options” statement in the /etc/named.conf file is as shown below:

  ```
  [ blackhole {address_match_list {; ]
  ```

- coresize

This option is used to specify the maximum size of a core dump. Default is `default`. The syntax of `coresize` option in the “`Options`” statement in the `/etc/named.conf` file is as shown below:

```
[ coresize size_spec ; ]
```

- `sortlist`

  The `sortlist` statement takes an `address_match_list` and interprets it. Each top level statement in `sortlist` must be an explicit `address_match_list` with one or two elements. The first element, which may be an IP address, IP prefix, `acl` name or a nested address_match_list is checked against the source address of the query until a match is found.

  Once the source address of the query has been matched, if the top level statement contains only one element, the actual element that matched the source address is used to select the address in the response to move to the beginning of the response. Each top level statement element is assigned a distance and the address in the response with the minimum distance is moved to the beginning of the response.

  A sample `sortlist` statement usage in the `Options` statement in the `/etc/named.conf` file is as shown below:

  ```
  [ sortlist { address_match_list }];
  ```

NOTE Refer to the `named.conf(4)` man page for more information on the usage of `sortlist` statement.

- `max-cache-size`

  `max-cache-size` is used to specify the maximum amount of memory to use for the server’s cache, in bytes. When the amount of data in the cache reaches this limit, the server will cause records to expire prematurely so that the limit is not exceeded. In a server with multiple views, the limit applies separately to the cache of each view. The default is `unlimited`, meaning that records are purged from the cache only when their TTLs expire.

New Option in “Server” Statement

The bogus option can be used to prevent queries to a remote server which is giving out invalid data. The default value of bogus is no. The syntax of bogus option in the “Server” statement is as shown below:

```
[ bogus yes_or_no ; ]
```

New Options in “Zone” Statement

The following lists the new options added in “Zone” statement:

- forwarders

  This option can be used to specify the IP addresses to be used for forwarding. The forwarding facility can be used to create a large site-wide cache on a few servers, reducing traffic over links to external nameservers. This facility also allows queries by servers that do not have direct access to the Internet, but wish to look up exterior names. Forwarding occurs only on those queries for which the server is not authoritative and does not have an answer in its cache.

  The forwarders option is specified in the /etc/named.conf file as:

  ```
  [ forwarders { ip_addr [port ip_port] ;
          [ ip_addr [port ip_port] ; ... ] }; ]
  ```

- allow-update

  This option can be used to specify which hosts are allowed to submit Dynamic DNS updates for master zones. By default, updates from all hosts are denied.

NOTE allow-update option is not applicable for slave zones. Refer to the named.conf(4) man page for more information.

rndc-confgen

rndc-confgen can be used to generate rndc.conf, the configuration file for rndc. Alternatively, it can also be run with the -a option to set up a rndc.key file thus avoiding the need for a rndc.conf file and a control statement.

rndc-confgen is run on the command line as:

```
rndc-confgen [-a] [-b keysize] [-c keyfile] [-h] [-k keyname]
[-p port] [-r randomfile] [-s address] [-t chrootdir] [-u use]
```

Where

"-a" option is used to configure rndc automatically. This creates a file rndc.key in /etc which is read by both rndc and named on start-up.

"-b keysize" is used to specify the size of the authentication key in bits. The value must range between 1 and 512. Default is 128 bits.

"-c keyfile" is used with the -a option to specify an alternate location for the rndc.key file.

"-h" is used to print a short summary of the options and arguments to rndc-confgen utility.

"-k keyname" is used to specify the key name of the rndc authentication key. This must be a valid domain name. Default is rndc-key.

"-p port" is used to specify the command channel port where named listens for connections from rndc. Default is 953.

"-r random file" is used to specify a source file of random data for generating the authorization. Default is the /dev/random file, otherwise the input from the keyboard is accepted.

"-s address" is used to specify the IP address where named listens for command channel connections from rndc. Default is the loopback address 127.0.0.1.

"-t chrootdir" is used with the -a option to specify a directory where named will run chrooted. An additional copy of the rndc.key will be written relative to this directory so that it will be found by the chrooted named.

"-u user" is used with the -a option to set the owner of the generated rndc.key file. If -t is also specified, the owner of the file in chroot area will be changed.

NOTE Refer to the rndc-confgen(1) man page for more information.

New Command Line Options

Table 1-1 lists the new command line options that have been added for the various binaries and tools in BIND 9.2.0.

Table 1-1 New Command Line Options

Binaries/Tools	Options	Usage
`dig`	`-b`	Set the source IP address of the query to address. This must be a valid address on one of the host's network interfaces.
`dig`	`-k`	Sign the DNS queries sent by `dig` and their responses using transaction signatures (TSIG).
`dig`	`-y`	Specify the TSIG key on the command line.
dnssec-makekeyset & dnssec-signkey	`-a`	Verify all generated signatures.
dnssec-signkey	`-c class`	Specify the DNS class of the key sets. Currently only `IN` class is supported.
dnssec-signkey	`-e end-time`	Specify the date and time when the generated SIG records become invalid. If no end-time is specified, 30 days from the start time will be used as a default.
`dnssec-signkey`	`-s start-time`	Specify the data and time when the generated SIG records become valid. This can be either an absolute or relative time. If no start-time is specified, the current time will be used.

Table 1-1 New Command Line Options (Continued)

Binaries/Tools	Options	Usage
`dnssec-signzone`	`-d directory`	Look for `signedkey` files in `directory` as the directory.
dnssec-signzone	`-h`	Print a short summary of the options and arguments to `dnssec-signzone`.
dnssec-signzone	`-i interval`	Specify the cycle interval as an offset from the current time (in seconds). If a SIG record expires after the cycle interval, it is retained. Else, it is considered to be expiring soon and will be replaced. The default cycle interval is one quarter of the difference between signature end and start times. If neither end-time nor start-time is specified, dnssec-signzone generates signatures that are valid for 30 days and with a cycle interval of 7.5 days. If any existing SIG record expires in less than 7.5 days, they would be replaced.
`dnssec-signzone`	`-n ncpus`	Specify the number of threads to use. By default, one thread is started for each CPU.
dnssec-signzone	`-o origin`	Specify the zone origin. If no zone origin is specified, the name of the zone file will be considered as the `origin`.
dnssec-signzone	`-t`	Print the performance statistics at the time of completion.

Table 1-1 New Command Line Options (Continued)

Binaries/Tools	Options	Usage
named	`-v`	Report the version number and exit.
named-checkconf	`-t`	`chroot` to directory to process `include` directives in the configuration file as if it is run by a similarly chrooted named.
named-checkconf	`-v`	Print the version number of `named-checkconf` and exit.
named-checkzone	`-v`	Print the version number of `named-checkzone` and exit.
nsupdate	`key {name} [secret]`	Specify that all updates need to be TSIG signed using the keyname keysecret pair. The `key` command overrides any key specified on the command line via -y or -k.
nsupdate	`local {address} [port]`	Send all dynamic update requests using the local address. If no local statement is provided, nsupdate will send updates using an address and port chosen by the system. port can also be used to set a specific port from where requests are sent. If port number is not specified, the system will assign one.
`nsupdate`	`send`	Send the current message. This is equivalent to entering a blank line.

Table 1-1 **New Command Line Options (Continued)**

Binaries/Tools	Options	Usage
nsupdate	show	Display the current message, containing all the pre-requisites and updates specified since the last send operation.
rndc	-k keyname	This option is used to specify the key name of the rndc authentication key. This must be a valid domain name. Default is rndc-key.

New Commands in rndc

The remote name daemon control (rndc) program allows the system administrators to control the operations of a name server.

The following lists the new commands added in rndc:

- reconfig
- trace
- trace level
- notrace
- flush
- flush [view]
- status

rndc is run on the command line as:

```
rndc [-c config] [-s server] [-p port] [-y key] command [comma
nd...]
```

Where

-c config file is used to specify an alternate configuration file. The default configuration file is /etc/rndc.conf.

-s server is used to specify the server whose operation needs to be controlled.

`-p port` is used to instruct `rndc` that it should send commands to TCP port number `port` on the system running the name server instead of BIND 9.2.0's default control channel port, 953.

`-y key` identifies the key-id to use from the configuration file and `command` is one of the following:

Table 1-2 rndc commands

Command	Description
`reload`	reload configuration file and zones
`reload zone [class [view]]`	reload the given zone
`refresh zone [class [view]]`	schedule zone maintenance for the given zone
`stats`	write serve statistics to the statistics file
`querylog`	toggle query logging
`dumpdb`	dump the current contents of the cache into the file specified by the dump-file option in named.conf.
`stop`	stop the server after saving any recent changes into the master files of the updated zones.
`halt`	stop the server immediately without saving any recent changes into the master files.
reconfig	reload configuration file and new zones only.
trace	increment debugging level by 1
trace level	change the debugging level
notrace	set debugging level to 0
flush	flush all the server's caches

Table 1-2 rndc commands (Continued)

Command	Description
flush [view]	flush the server's cache for a view
status	display the status of the server

NOTE

Refer to the `rndc(1)` man page for more information.

A sample `rndc.conf` file is distributed with this release of BIND. This file can be generated automatically by the `rndc-confgen` utility, which is distributed with BIND 9.2.0. For more information on `rndc-confgen`, read the `rndc-confgen` section above.

Changed Features

This section describes the changed features in BIND 9.2.0.

HP-specific Features

The following lists the HP-specific features incorporated in BIND 9.2.0:

- noforward

  This option cannot be specified in `Options` statement in BIND 9.2.0. Instead forwarding can be suppressed by including an empty `forwarders` sub-statement as shown in the following example:

  ```
  options {
      forwarders {192.249.249.1; };
          }
  zone “hp.com” {
      type slave;
      masters { 192.249.249.4; };
      file “db.hp”;
      forwarders { };
  }
  ```

  This will suppress queries like “foo.india.hp.com” from being forwarded to nameservers at 192.249.249.1.

NOTE

Forwarding to the nameservers available in the delegation information cannot be suppressed using an empty `forwarders` sub-statement.

- alias-ip

  This option is now no longer supported. Use the `“listen-on”` option of the `“Options”` statement to implement the `alias-ip` option.

- auth-nxdomain yes/no

  If this option is specified as `yes`, then the AA bit is always set on NX domain responses, even if the server is not actually authoritative. The default value for this option has been changed from “`yes`” to “`no`”.

Unsupported Features

The following BIND 8.1.2 options are not supported in BIND 9.2.0:

- no-round-robin

  This option was used in BIND 8.1.2 to turn off the default round robin, which cycles returned IP addresses for multi-homed hosts.

- named-xfer

  This option is obsolete because it is part of the `named` binary.

- deallocate-on-exit

  This option is no longer in use as the server now always checks for memory leaks.

- fake-iquery

  This option is obsolete and is always set to “no”, thus not allowing to simulate DNS IQUERY, which is not used in BIND 9.2.0.

- statistics-interval

  This option was used in BIND 8.1.2 to log statistics of the nameserver at regular intervals. The logging consumes a lot of memory and degrades the response time.

- multiple-cnames

  This option was used in BIND 8.1.2 to allow multiple CNAME records in violation of the DNS standards. BIND 9.2.0 strictly enforces the CNAME rules both in master files and dynamic updates.

- has-old-clients

  This option is now implemented through the “`auth-nxdomain yes`” and “`rfc2308-type1 no`” options.

- treat-cr-as-space

  This option was used in BIND 8.1.2 to make the server treat carriage return `\r` characters, the same way as a space or tab character, or to facilitate loading of zone files on a Unix system that were generated on an NT or DOS machine. In BIND 9.2.0, both Unix “`\n`” and NT/DOS “`\r\n`” newlines are always accepted.

- use-id-pool

This option is now obsolete as BIND 9.2.0 always allocated query IDs from a pool.

- fetch-glue

  This option was used in BIND 8.1.2 to cause the server to fetch glue resource records it does not have when constructing the additional data section of a response.

- serial-queries

  This option was used in BIND 8.1.2 to set the maximum number of concurrent serial number queries allowed to be outstanding at any given time. BIND 9.2.0 does not limit the number of outstanding serial queries and ignores the `serial-queries` option.

- check-names

  This option was used in BIND 8.1.2 to check the hostnames as per standards.

- topology

  The topology statement takes an address_match_list and interprets it in a special way. Each top-level list element is assigned a distance.

- rfc2308-type1 yes_or_no

  If this option is set to `yes`, the server sends NS records along with the SOA record for negative answers. The default is `no`.

- min-roots

  This option specifies the minimum number of root servers that is required for a request for the root servers to be accepted. Default is 2.

- unix

  This option in `controls` statement is not supported in BIND 9.2.0.

Options not Supported in “View” and “Zone” Statements

The following lists the options in `View` and `Zone` statement that are not supported in BIND 9.2.0:

- ixfr-base

This option was used in BIND 8.1.2 to specify the name of the transaction log (journal) file for dynamic update and IXFR. BIND 9.2.0 ignores the option and constructs the name of the journal file by appending `.jnl` to the name of the zone file.

- pubkey

  This option was used in BIND 8.1.2 to specify a public zone key for verification of signatures in DNSSEC signed zones when they are loaded from disk. BIND 9.2.0 does not verify signatures on loading and ignores the option.

- max-ixfr-log-size

  This option was used in BIND 8.1.2 to set limits on server's resource consumption. This option is obsolete; it is accepted and ignored for BIND 8.1.2 compatibility.

2 Installation Information

Read this chapter before installing BIND 9.2.0.

System Requirements

The following lists the system requirements to install BIND 9.2.0:

- Hewlett-Packard 9000 System
- HP-UX 11i v2 operating system

Migrating from Previous Versions of BIND

The following sections describe how to migrate from previous versions of BIND to BIND 9.2.0.

From BIND 4.9.7 to BIND 9.2.0

A shell script, "`named-bootconf.sh`" is provided with BIND 9.2.0 in the `/usr/bin` directory to convert the BIND 4.9.7 configuration file to BIND 9.2.0-compliant configuration file.

The following steps describe how to convert the existing `/etc/named.boot` file to the BIND 9.2.0-compliant `/etc/named.conf` configuration file:

1. Execute `/usr/bin/named-bootconf.sh` with the existing /etc/named.boot file as input and redirect the output to `/etc/named.conf`.

   ```
   # /usr/bin/named-bootconf.sh < /etc/named.boot > /etc/name
   d.conf
   ```

A shell script "`change2v9db.sh`" is provided with BIND 9.2.0 in the `/usr/bin` directory to convert the existing db files to BIND 9.2.0-compliant db files.

The following steps describe how to convert the BIND 4.9.7 db files to BINDv9.1.3-compliant db files:

1. `cd` to the directory where the db files exist.
2. Execute the script as specified below with all the db files as arguments.

   ```
   # /usr/bin/change2v9db.sh dbfile1 dbfile2 ...
   ```

   After successful execution, all existing db files will be converted to BIND 9.2.0-compliant db files.

NOTE It is highly recommend that BIND 4.9.7 users read the BIND 8.1.2 optional web upgrade release notes available at http://www.software.hp.com/products/DNS_BIND/index.html.

From BIND 8.1.2 to BIND 9.2.0

BIND 9.2.0 expects the db files in a slightly different format compared to the previous versions.

A shell script "change2v9db.sh" is provided with BIND 9.2.0 to convert the existing db files to BIND 9.2.0-compliant db files. The shell script is installed in the /usr/bin directory.

The following steps describe how to convert the db files to BIND 9.2.0-compliant db files:

1. cd to the directory where the db files exist.
2. Execute the script as specified below with all the db files as arguments.

```
# /usr/bin/change2v9db.sh dbfile1 dbfile2 ...
```

From BIND 9.0 to BIND 9.2.0

Customers currently using BIND 9.0 need not modify the configuration file and db files. They are compatible with BIND 9.2.0.

From BIND 9.1.3 to BIND 9.2.0

Customers currently using BIND 9.1.3 need not modify the configuration file and db files. They are compatible with BIND 9.2.0.

Compatibility with Previous Versions of BIND

This section provides the BIND 9.2.0 compatibility information.

BIND 4.9.7 Compatibility

This section discusses the BIND 9.2.0-BIND 4.9.7 compatibility.

- BIND 9.2.0 uses a system assigned port for the UDP queries it makes rather than port 53 that BIND 4.9.7 uses. This may conflict with some firewalls.

  To specify a port, edit the /etc/named.conf file as follows:

  ```
  query-source address * port 53;
           transfer-source * port 53;
           notify-source * port 53;
  ```

- BIND 9.2.0 no longer uses the minimum field to specify the TTL of records without a explicit TTL.

  Use the $TTL directive to specify a default TTL before the first record without an explicit TTL. The `hosts_to_named` script will create TTL value in the db files.

- BIND 9.2.0 does not support multiple CNAMEs with the same owner name. For example:

  ```
  www.example.com. CNAME host1.example.com.
        www.example.com. CNAME host2.example.com.
  ```

  In the above example, multiple records with the same owner name “www.example.com” are not supported.

  The `named-checkzone` program can be used to check the correctness of the database files.

- BIND 9.2.0 does not support "CNAMEs with other data" with the same owner name, ignoring the DNSSEC records (SIG, NXT, KEY) that BIND 4.9.7 did not support. For example:

  ```
  www.example.com. CNAME host1.example.com.
  www.example.com. MX 10 host2.example.com.
  ```

- BIND 9.2.0 is less tolerant of errors in master files, so check your logs and fix any errors reported. The `named-checkzone` program can also be to check master files.

- Outgoing zone transfers now use the "`many-answers`" format by default.This format is not understood by certain old versions of BIND 4.9.7.This problem can be resolved by using the option "`transfer-format one-answer;`", but HP recommends upgrading the slave servers.

BIND 8.1.2 Compatibility

This section discusses the BIND 9.2.0-BIND 8.1.2 compatibility.

- Configuration file compatibility
  - BIND 9.2.0 supports most of the options in `named.conf` file of BIND 8.1.2. BIND 9.2.0 issues a log message if the specified option is not implemented. It also logs the information if the default value is changed.
  - In BIND 9.2.0, `named` refuses to start if it detects an error in `named.conf`. Earlier versions would start despite errors, causing the server to run with a partial configuration.
  - In BIND 9.2.0, the "`logging`" statement only takes effect after the entire `named.conf` file has been read. In BIND 8.1.2, the new logging configuration took effect immediately after a "`logging`" statement was read.
  - The source address and port for notify messages and refresh queries is now controlled by "`notify-source`" and "`transfer-source`", respectively, as against `query-source` in BIND 8.1.2.
- Zone file compatibility
  - BIND 9.2.0 does not support serial numbers of SOA record with an embedded period, like "3.002". Serial numbers should be integers.
  - TXT records with unbalanced quotes, like ‘host TXT "foo’, were not treated as errors in previous versions of BIND. If the zone files contain such records, then error messages like "unexpected end of file"will be displayed because BIND 9.2.0 will interpret everything up to the next quote character as a literal string.
  - Previous versions of BIND accept RRs containing line breaks that are not properly quoted with parentheses. This is not legal master file syntax and will be treated as an error by BIND 9.2.0.

Installing BIND 9.2.0

BIND 9.2.0 is available as a web release on HP-UX 11i v1 platform at HP's software depot at http://www.software.hp.com. The latest version of BIND 9.2.0 is Version 6.0 released in December 2004. After downloading the software package, use the `swinstall` command to install the package on your system. Detailed information on how to use BIND 9.2.0 can be found in the respective man pages.

Step1 If you have installed BIND 9.1.3 on your system, use `swremove` command to remove the old web upgrade.

Step2 Type: swinstall -s <destination path> on the command line

Where <destination path> is the absolute path where you downloaded the BIND 9.2.0 web upgrade depot to.

(Refer to the `swinstall.1m` man page for more information on `swinstall` command)

Execution of the above command would display a GUI screen.

Step3 Select the BIND 9.2.0 product in the GUI screen

Step4 Invoke `Action` menu and select `Install` option

BIND 9.2.0 on HP-UX 11i is now available for use.

If you install the current version of BIND 9.2.0 on a system where a previous version of BIND 9.2.0 is installed, the previous version of BIND 9.2.0 is overwritten. Now, if you try removing the current version of BIND 9.2.0, both the current version and previous version of BIND 9.2.0 are removed, and the system will revert back to the base version of BIND, that is 8.1.2, delivered with the HP-UX 11i v1 operating system.

The BIND 9.2.0 files are installed into the `/usr/contrib/bind` directory. During installation, the `/usr/bin/enable_inet` script backs up the existing BIND 8.1.2 files into `/usr/contrib/bind/save_custom/backup` directory and activates the higher version of BIND by linking the new files to existing file locations.

The `enable_inet -r bind` command allows reverting back to the older version of BIND. `enable_inet status bind` shows the currently active version of BIND. If you want to install a GR patch, you need to disable

BIND 9.2.0 by running the command "`/usr/bin/enable_inet -r bind`" in the command line to revert back to the base version delivered with HP-UX 11i (BIND 8.1.2) prior to patching.

3 Documentation

This chapter discusses the product documentation that is distributed with BIND 9.2.0.

Man Pages

BIND 9.2.0 documentation is available through its man pages. Table 3-1 lists and describes the man pages distributed with BIND 9.2.0.

Table 3-1 **Man Pages**

Man Page	Description
`named.1m`	Internet domain name server
`dnssec-keygen.1`	Key generation tool for DNSSEC
`dnssec-makekeyset.1`	Program used to produce a set of DNS keys.
`dnssec-signkey.1`	DNSSEC keyset signing tool
`host.1`	DNS lookup utility
`nslookup.1`	Program used to query nameservers interactively.
`nsupdate.1`	Dynamic DNS update utility
`lwresd.1m`	Lightweight resolver daemon
`rndc.1`	Name server control utility
`rndc.conf.4`	`rndc` configuration file
`sig-named.1m`	Program used to send signals to the nameserver.
`named-checkconf.1`	`named` configuration file syntax checking tool
`named-checkzone.1`	Zone validity checking tool
`hosts_to_named.1m`	Program used to translate host table to name server file format.
`dig.1m`	Domain information groper
`rndc-confgen.1`	`rndc` key generation tool

Table 3-1 Man Pages (Continued)

Man Page	Description
named-conf.4	Configuration file for name daemon

nslookup, dig, and host can be used to troubleshoot BIND 9.2.0.

NOTE Please refer to the respective man pages for detailed information and examples.

4 Known Problems and Limitations

This chapter discusses the known problems and limitations in BIND 9.2.0.

Known Problems

The following are the known problems in BIND 9.2.0:

- In BIND 9.2.0, if duplicate data is available for a query, the duplicate data will not be dropped.
- Use of wildcard address "*" in "query-source address * port 53;" may not work as expected. Instead of the wildcard address "*", you need to use an explicit source IP address.
- In IPv4 environments, DNS can listen on any specified addresses, whereas if you want to listen on IPv6 the flexibility of specifying the chosen addresses is not available. If you wish to accept DNS queries over IPv6, you need to specify "listen-on-v6 { any; };" in the `named.conf` `Options` statement.
- The `hosts_to_named` configuration file migration script does not add the `listen-on-v6` option to the `named.conf` file on a dual stack machine.
- SAM NNC over IPv6 cannot set the DNS listen-on-any IPv6 socket option.
- The DNS resolvers (res_*()) implement only RFC 1886 i.e., AAAA-based lookups.
- `nslookup` recognizes only AAAA records and support for A6 records is not available.

NOTE

HP recommends using `dig` instead of `nslookup`, as it may be obsoleted in the future releases.

Refer to the `dig(1m)` man page for information about the `dig` utility.

Limitations

The following lists the limitations in BIND 9.2.0:

- Specific IPv6 addresses cannot be specified with the `listen-on-v6` option.
- The `rndc dump.db` command dumps only the cache information. You can run `dig axfr <domain>` command to obtain the db file information.
- In IPv6 systems, the `notify` directive in the `Options` statement in `named.conf` will be successful only if there is an IPv4-mapped-IPv6 address in the `masters` clause of the slave zone.
- To set up forwarding nameservers, `db.<prefix>.IP6.INT` files need to be created manually. Currently, `db.<prefix>.IP6.INT` files are not being created. For example: for IPv6 address fe80::1/16, the db file `db.0.8.e.f.IP6.INT`, should be created and `named.conf` should be changed accordingly.
- In IPv6 systems, the ACLs may not produce desired results if an IPv4 address is specified in the ACL entry.

  An IPv4-mapped-IPv6 address needs to be specified instead of the IPv4 address in the ACL entry as follows:

  ```
  acl egacl { ::ffff:15.70.128.34:};
  ```
- In `nslookup`, the ‘`ls`’ command is used to list the information available for domain, optionally creating or appending to filename. The output of this command contains host names and their Internet addresses. The AAAA records are not shown in this output.
- The “`server`” option in nslookup does not work for IPv6 addresses if the name server specified in `/etc/resolv.conf` is an IPv4 server. This option will not work for IPv4 addresses if the name server is specified in `/etc/resolv.conf` is an IPv6 server.
- The command used to revert back to the previous version of BIND (i.e., 9.2.0), “`/usr/bin/enable_inet -r bind`” must not be executed in the directory “`/usr/contrib/bind/save_custom/`” or in any of its sub-directories.

Defects Closed in this Release

Table 4-1 and Table 4-2 describe the defects closed in the previous releases and the current release of BIND 9.2, respectively.

Table 4-1 Defects Closed in the Previous Releases

Defect	Description
JAGad95074	Porting of BIND9.2.0 on HPUX 11.11.
JAGae38578	Problem with nslookup in BIND.
JAGae37800	Openssl not working properly
JAGae33084	A buffer-length based computational error exits in the nslookup.
JAGae33027	`named` is not handling ENOSR error when writing to the internal control pipe.
JAGae32214	Potential memory leak in `named`.
JAGae31999	`named` is not logging the unexpected error.
JAGae31407	`named` fails to exit after `rndc` is invoked with incorrect zone.
JAGae30189	A name server configured as a cache only server fails to process the queries under certain circumstances.
JAGae16049	`named(1M)` does not close socket with `blackhole` configuration.
JAGae16048	named does not close socket with `controls` configuration.
JAGae08966	`accept()` fails with an error message `No buffer space available`.

Table 4-1 Defects Closed in the Previous Releases (Continued)

Defect	Description
JAGae32958	The `hosts_to_named` command takes considerable amount of time to process the host table.
JAGae95793	The `rndc dumpdb` command does not dump the address database cache.
JAGae93621	Certain openssl certificates do not work properly.
JAGae72605	In an IPv6 system, if the `listen-on-v6 ( none };` option is specified in the named.conf file named does not listen on an IPv4 interface.
JAGae51696	Adding the `edns` option in the `options` statement in `named.conf` file for BIND9.
JAGae69740	`named` does not handle large domain names properly.
JAGae69742	`named` handles certain valid octal bit labels incorrectly.
JAGae69743	Openssl gives error while parsing tokens.
JAGae70323	`named` hangs during certain circumstances.

Table 4-2 Defects Closed in this Release

<table>
<tr><th>Defect</th><th>Description</th></tr>
<tr><td>JAGaf06536</td><td>In multithreaded environment, named aborts with an assertion failure <code>REQUIRE</code>. The following error message is logged in the syslog file:
<pre>
lib/dns/resolver.c:5065: REQUIRE((((fetch)
!= 0L) &&(((constisc__magic_t *
)(fetch))->magic == (((’F’) << 24 | (’t’)
<< 16 | (’c’) << 8 | (’h’)))))) failed
Nov 04 00:30:00.459 general: critical:
exiting (due to assertion failure)
</pre></td></tr>
<tr><td>JAGae97983</td><td>In multithreaded environment, named aborts with an assertion failure. The error reported in the syslog file is as follows:
<pre>
critical: lib/dns/name.c:3200:
REQUIRE((((name) != 0L) && (((const
isc__magic_t *)(name))->magic == (((’D’) <<
24 | (’N’) << 16 | (’S’) << 8 | (’n’))))))
failed
Sep 11 15:54:09.269 general: critical:
exiting (due to assertion failure)
</pre></td></tr>
<tr><td>JAGaf11223</td><td>Data in the files created by <code>hosts_to_named</code> is inconsistent between the <code>named.conf</code> and the secondary files.</td></tr>
<tr><td>JAGaf09745</td><td>named aborts with assertion failure <code>REQUIRE</code> in <code>task.c</code>. The following error message is logged in the syslog file:
<pre>
named[9203]: lib/isc/task.c:395:
REQUIRE((((task) != 0L) &&(((const
isc__magic_t *)(task))->magic == (((’T’) <<
24 | (’A’) << 16 | (’S’) << 8 | (’K’))))))
failed
</pre></td></tr>
<tr><td>JAGaf35663</td><td>The <code>dnssec-keygen</code> utility does not use the <code>/dev/random</code> file, by default, as a source of entropy.</td></tr>
</table>

Table 4-2 Defects Closed in this Release (Continued)

Defect	Description
JAGaf40799	The `rndc stop` command does not flush data into the db files.
JAGaf45348	named aborts with assertion failure `INSIST` in `name.c`.

Table 4-3 lists the defects fixed in BIND 9.2.0 that are ported back from the new versions of BIND.

Table 4-3 Backported Defects

New BIND Version	Defect Number
BIND 9.2.4	JAGaf06536 JAGaf09745
BIND 9.2.3	JAGae70323 JAGae97983
BIND 9.2.2	JAGae08966 JAGae69740 JAGaf40799
BIND 9.2.1	JAGaf45348 JAGae16048 JAGae33027 JAGae32214 JAGae31999 JAGae31407 JAGae69742 JAGae30189 JAGae16049