Hewlett Packard
Enterprise

BIND (HP-UX NameServer) Release Notes v9.11.1.2.0

Part Number: P01081-002
Published: September 2017
Edition: 3

Notices

Acknowledgments

Contents

BIND (HP-UX NameServer) release notes for 9.11.x

About this document

This document discusses the most recent product information, pertaining to Berkeley Internet Name Domain or BIND (HP-UX NameServer). BIND is also referred to as Name Server or HP-UX NameServer, supported on HP-UX 11i v3 operating systems.

Table 1: Documentation Support for BIND (HP-UX NameServer)

Operating system	Version
HP-UX 11i v3	9.11.1.2.0

This document provides details about installing BIND (HP-UX NameServer) 9.11.1 on HP-UX 11i v3 operating systems.

Announcement

BIND (HP-UX NameServer) is a Berkeley implementation of the Domain Name System (DNS). It is a distributed network information lookup service, that maps host names to Internet addresses, and Internet addresses to host names. It also facilitates Internet mail routing by providing a list of hosts that accept mail for other hosts.

BIND (HP-UX NameServer) 9.11.1.mm.nn is the latest version of BIND (HP-UX NameServer), which is based on the open source BIND 9.11.1. It is available for download at: Software Depot Home.

License Information

BIND 9.11.1.mm is subject to the terms of the Mozilla Public License, v. 2.0 **http://mozilla.org/MPL/2.0/**.

License file is also available at `/usr/examples/bind/BIND.LICENSE`, which is delivered as part of Software Depot.

What is new in this version?

This version of BIND (HP-UX NameServer) 9.11.1 for HP-UX 11i v3 operating system includes various new features, change in behavior of legacy features and various defect fixes.

See **New features** on page 6 for details on the new features in Bind 9.11.1 and **Feature changes** on page 10 for the feature changes between BIND 9.9.4 and BIND 9.11.1.

For a complete list of changes and details about the defect fixes in the open source, see Release Notes of BIND 9.11.x available at **http://www.isc.org**.

Features of BIND (HP-UX NameServer) 9.11.x

New utilities

The following new utilities are available in BIND 9.11.1. See the corresponding man pages for more details:

Table 2: New utilities in BIND 9.11.1 (HP-UX NameServer)

Utility	Description
`delv(1)`	DNS lookup and validation utility.
`mdig(1)`	DNS pipelined lookup utility.
`named-rrchecker(1)`	Syntax checker for individual DNS resource records.
`dnssec-importkey(8)`	Utility to import DNSKEY records from external systems so they can be managed.
`dnssec-keyfromlabel(8)`	DNSSEC key generation tool.

New features

This version of BIND (HP-UX NameServer) for HP-UX 11i v3 operating systems includes the following new features and enhancements.

named (8)

- Minimal Response to ANY Queries
  - The new `minimal-any` option reduces the size of answers to UDP queries for type ANY by implementing one of the strategies in `draft-ietf-dnsop-refuse-any`: returning a single arbitrarily-selected RRset that matches the query name rather than returning all of the matching RRsets.
- `named -L filename` causes named to send log messages to the specified file by default instead of to the system log.
- A new zone file format, *map*, stores zone data in a format that can be mapped directly into memory, allowing significantly faster zone loading.
- The new `prefetch` option can improve recursive resolver performance. When it is in use, cache records are requested by clients are automatically refreshed from the authoritative server before they expire, reducing or eliminating the time window in which no answer is available in the cache.
- RPZ now allows response policies to be triggered on the basis of the client IP address.
- The new `in-view zone` option allows zone data to be shared between views, so that multiple views can serve the same zones authoritatively without storing multiple copies in memory.
- The new `max-zone-ttl` option enforces maximum TTLs for zones. If loading a zone containing a higher TTL, the load fails. DDNS updates with higher TTLs are accepted but the TTL is truncated.
- `named` now listens on IPv6 as well as IPv4 interfaces by default.
- `named` will now check to see whether other name server processes are running before starting up. This is implemented in two ways:

1. By refusing to start if the configured network interfaces all return address in use.
2. By attempting to acquire a lock on a file specified by the lock-file option or the -X command line option. The default lock file is /var/run/named/named.lock. Specifying none will disable the lock file check.

- A new `tcp-only` option can be specified in server statements to force named to connect to the specified server via TCP.
- When loading a signed zone, named will now check whether an RRSIG inception time is in the future, and if so, it will regenerate the RRSIG immediately. This helps when a system clock needs to be reset backwards.
- `named` now provides feedback to the owners of zones which have trust anchors configured (trusted-keys, managed-keys, dnssec-validation auto; and dnssec-lookaside auto;) by sending a daily query which encodes the keyids of the configured trust anchors for the zone. This is controlled by trust-anchor-telemetry and defaults to yes.
- A new masterfile-style zone option controls the formatting of text zone files: When set to full, the zone file will dumped in single-line-per-record format.
- serial-update-method can now be set to date. On update, the serial number will be set to the current date in YYYYMMDDNN format.
- Log output to files can now be buffered by specifying **buffered yes**; when creating a channel.
- The rate limiter configured by the serial-query-rate option no longer covers NOTIFY messages; those are now separately controlled by notify-rate and startup-notify-rate (the latter of which controls the rate of NOTIFY messages sent when the server is first started up or reconfigured).
- When answering recursive queries, SERVFAIL responses can be cached by the server for a limited time. Subsequent queries for the same query name and type will return another SERVFAIL until the cache times out. This reduces the frequency of retries when a query is persistently failing, which can be a burden on recursive servers. The SERVFAIL cache timeout is controlled by servfail-ttl, which defaults to 1 second and has an upper limit of 30.
- The `nxdomain-redirect` option specifies a DNS namespace to use for NXDOMAIN redirection. When a recursive lookup returns NXDOMAIN, a second lookup is initiated with the specified name appended to the query name. This allows NXDOMAIN redirection data to be supplied by multiple zones configured on the server, or by recursive queries to other servers. (The older method, using a single type redirect zone, has better average performance but is less flexible).
- A new `message-compression` option can be used to specify whether or not to use name compression when answering queries. Setting this to no results in larger responses, but reduces CPU consumption and may improve throughput. The default is yes.
- Added server-side support for pipelined TCP queries. Clients may continue sending queries via TCP while previous queries are processed in parallel. Responses are sent when they are ready, not necessarily in the order in which the queries were received. To revert to the former behavior for a particular client address or range of addresses, specify the address prefix in the "keep-response-order" option. To revert to the former behavior for all clients, use `keep-response-order { any; }`.
- `named` now preserves the capitalization of names when responding to queries: for instance, a query for "example.com" may be answered with "example.COM" if the name was configured that way in the zone file. Some clients have a bug causing them to depend on the older behavior, in which the case of the answer always matched the case of the query, rather than the case of the name configured in the DNS. Such clients can now be specified in the new no-case-compress ACL; this will restore the older behavior of `named` for those clients only.
- Fetch quotas are now compiled in by default:
  - These quotas limit the queries that are sent by recursive resolvers to authoritative servers experiencing denial-of-service attacks. They can both reduce the harm done to authoritative servers and also avoid the resource exhaustion that can be experienced by recursive servers when they are being used as a vehicle for such an attack.

- `fetches-per-server` limits the number of simultaneous queries that can be sent to any single authoritative server. The configured value is a starting point; it is automatically adjusted downward if the server is partially or completely non-responsive. The algorithm used to adjust the quota can be configured using the `fetch-quota-params` option.
- `fetches-per-zone` limits the number of simultaneous queries that can be sent for names within a single domain.

  NOTE:

  Unlike fetches-per-server, this value is not self-tuning.

- Specifying the keyword `auto` instead of a salt when using `rndc signing -nsec3param` will cause `named` to select a 64-bit salt at random.
- The following types have been implemented: CSYNC, NINFO, RKEY, SINK, TA, TALINK.
- The EDNS Client Subnet (ECS) option is now supported for authoritative servers; if a query contains an ECS option then ACLs containing ecs elements can match against the address encoded in the option. This can be used to select a view for a query, so that different answers can be provided depending on the client network.
- The `EDNS EXPIRE` option has been implemented on the client side, allowing a slave server to set the expiration timer correctly when transferring zone data from another slave server.

DNS Cookies

- Cookies are exchanged between client and server to provide IP address identity, helping to prevent attacks using forged IP addresses. Servers enforcing cookies are less susceptible to being used as an effective attack vector for DNS DDOS attacks.
- New commands include require-server-cookie and send-cookie (both default to ON in 9.11.0). Setting a cookie-secret will enable a cluster of BIND servers to share cookies. For more information, including the potential for DNS Cookies to expose EDNS compatibility problems, see **DNS Cookies in BIND 9** .

Catalog Zones

- A new method of provisioning secondary servers called **Catalog Zones** has been added. This method is an implementation of **draft-muks-dnsop-dns-catalog-zones/**.
- A catalog zone is a regular DNS zone which contains a list of member zones, along with the configuration options for each of those zones. When a server is configured to use a catalog zone, all the zones listed are added to the local server as slave zones. When the catalog zone is updated (for example, by adding or removing zones, or changing configuration options for existing zones) those changes will be put into effect. Since the catalog zone is itself a DNS zone, this means configuration changes can be propagated to slaves using the standard AXFR/IXFR update mechanism.
- This feature is considered experimental. It currently supports only basic features; more advanced features such as ACLs and TSIG keys are not yet supported. Sample catalog zone configurations can be found in the **Chapter 4** of the *BIND9 Administrator Reference Manual*.
- Support for master entries with TSIG keys has been added to catalog zones, as well as support for allow-query and allow-transfer.

For an overview of how to configure catalog zones, see **A Short Introduction to Catalog Zones**.

rndc (8)

- New features in provisioning
  - rndc delzone can now be applied to zones which were configured in named.conf; it is no longer restricted to zones which were added by `rndc addzone`.

NOTE:

This does not edit `named.conf`, the zone must be removed from the configuration or it will return when named is restarted or reloaded).

- `rndc modzone` can be used to reconfigure a zone, using similar syntax to `rndc addzone`.
- `rndc showzone` displays the current configuration for a specified zone.

- Other features
  - A read-only option is now available in the controls statement to grant non-destructive control channel access. In such cases, a restricted set of rndc commands are allowed, which can report information from named, but cannot reconfigure or stop the server. By default, the control channel access is not restricted to these read-only operations.
  - Added `rndc scan` to trigger an interface scan manually.
  - `rndc -q` causes `rndc` to suppress output other than error messages.
  - `rndc zonestatus` reports information about a specified zone.
  - A new `rndc delzone -clean` option removes zone files when a zone is deleted.
  - The serial number of a dynamically updatable zone can now be set using `rndc signing -serial number zonename`. This is particularly useful with inline-signing zones that have been reset. Setting the serial number to a value larger than that on the slaves will trigger an AXFR-style transfer.
  - To enable better monitoring and troubleshooting of RFC 5011 trust anchor management, the new rndc managed-keys can be used to check status of trust anchors or to force keys to be refreshed. Also, the managed-keys data file now has easier-to-read comments.
  - The `rndc` command now supports new key algorithms in addition to HMAC-MD5, including HMAC-SHA1, -SHA224, -SHA256, -SHA384, and -SHA512. The -A option to rndc-confgen can be used to select the algorithm for the generated key.
  - **Negative Trust Anchors**:

    The new rndc nta command can now be used to set a negative trust anchor (NTA), disabling DNSSEC validation for a specific domain; this can be used when responses from a domain are known to be failing validation due to administrative error rather than because of a spoofing attack. NTAs are strictly temporary; by default they expire after one hour, but can be configured to last up to one week. The default NTA lifetime can be changed by setting the nta-lifetime in named.conf. When added, NTAs are stored in a file (viewname.nta) in order to persist across restarts of the named server.

dig (1)

- When dig receives a truncated (TC=1) response or a BADCOOKIE response code from a server, it will automatically retry the query using the server COOKIE that was returned by the server in its initial response.
- The new mdig command is a version of dig that sends multiple pipelined queries and then waits for responses, instead of sending one query and waiting the response before sending the next.
- dig +ednsopt can now be used to set arbitrary EDNS options in DNS requests.
- dig +ednsflags can now be used to set yet-to-be-defined EDNS flags in DNS requests.
- dig +[no]ednsnegotiation can now be used enable / disable EDNS version negotiation.
- dig +header-only can now be used to send queries without a question section.
- dig +ttlunits causes dig to print TTL values with time-unit suffixes: w, d, h, m, s for weeks, days, hours, minutes, and seconds.
- dig +zflag can be used to set the last unassigned DNS header flag bit. This bit is normally zero.
- dig +dscp=value can now be used to set the DSCP code point in outgoing query packets.

- dig +mapped can now be used to determine if mapped IPv4 addresses can be used.
- dig +expire sends an EXPIRE option when querying. When this option is sent with an SOA query to a slave zone running on a server that supports the option, the response will report the time until the slave zone expires
- Added a new dig +subnet option to send an EDNS CLIENT-SUBNET option containing the specified address/prefix when querying.

dnssec-signzone(8)

- `dnssec-signzone -N` date also sets the serial number to YYYYMMDDNN.
- When re-signing a zone, the new `dnssec-signzone -Q` option drops signatures from keys that are still published but are no longer active.

named-checkconf(8)

`named-checkconf -px` will print the contents of configuration files with the shared secrets obscured, making it easier to share configuration (for example, when submitting a bug report) without revealing private information.

named-checkzone(8)

`named-checkzone` and `named-compilezone` can now read journal files, allowing them to process dynamic zones without the zones needing to be frozen first.

Feature changes

This version of BIND (HP-UX NameServer) for HP-UX 11i v3 operating systems includes the following changes in legacy features of various components.

named(8)

- The logging format used for querylog has been altered. It now includes an additional field indicating the address in memory of the client object processing the query.
- The default setting for the -U option (setting the number of UDP listeners per interface) has been adjusted to improve performance.
- Adaptive mutex locks are now used to improve performance under load.
- The timers returned by the statistics channel (indicating current time, server boot time, and most recent reconfiguration time) are now reported with millisecond accuracy.
- Updated the compiled-in addresses for H.ROOT-SERVERS.NET and L.ROOT-SERVERS.NET.
- NXDOMAIN responses to queries of type DS are now cached separately from those for other types. This helps when using grafted zones of type forward, for which the parent zone does not contain a delegation, such as local top-level domains. Previously a query of type DS for such a zone could cause the zone apex to be cached as NXDOMAIN, blocking all subsequent queries.

  NOTE:

  This change is only helpful when DNSSEC validation is not enabled. Grafted zones without a delegation in the parent are not a recommended configuration.

- Update forwarding performance has been improved by allowing a single TCP connection to be shared between multiple updates.
- Added support for OPENPGPKEY type.
- The names of the files used to store managed keys and added zones for each view are no longer based on the SHA256 hash of the view name, except when this is necessary because the view name contains characters that would be incompatible with use as a file name. For views whose names do

not contain forward slashes ('/'), backslashes ('\'), or capital letters - which could potentially cause namespace collision problems on case-insensitive filesystems - files will now be named after the view (for example, internal.mkeys or external.nzf). However, to ensure consistent behavior when upgrading, if a file using the old name format is found to exist, it will continue to be used.

- When encountering an authoritative name server whose name is an alias pointing to another name, the resolver treats this as an error and skips to the next server. Previously this happened silently; now the error will be logged to the newly-created **cname** log category.
- When using request-nsid, if the name server identifier received from the server contains printable characters, they will be logged in a human-readable string format in addition to hexadecimal.
- named will now log a warning when addresses of the wrong family are used in listen-on or listen-on-v6. Previously these were silently ignored.
- The timestamp included in RRSIG records can now be read as integers indicating the number of seconds since the UNIX epoch, in addition to being read as formatted dates in YYYYMMDDHHMMSS format.
- If named is not configured to validate answers, then allow fallback to plain DNS on timeout even when we know the server supports EDNS. This will allow the server to potentially resolve signed queries when TCP is being blocked.
- Large inline-signing changes should be less disruptive. Signature generation is now done incrementally; the number of signatures to be generated in each quantum is controlled by sig-signing-signatures number.
- Substantial improvements have been made in response-policy zone (RPZ) performance. Up to 32 response-policy zones can now be configured. Performance loss due to adding additional RPZs is minimal.
- A new nsip-wait-recurse directive has been added to RPZ, specifying whether to look up unknown name server IP addresses and wait for a response before applying RPZ-NSIP rules. The default is yes. If set to no, named will only apply RPZ-NSIP rules to servers whose addresses are already cached. The addresses will be looked up in the background so the rule can be applied on subsequent queries. This improves performance when the cache is cold, at the cost of temporary imprecision in applying policy directives.
- Within the response-policy option, it is now possible to configure RPZ rewrite logging on a per-zone basis using the log clause.
- The default preferred glue is now the address type of the transport the query was received over.
- On machines with 2 or more processors (CPU), the default value for the number of UDP listeners has been changed to the number of detected processors minus one.
- Zone transfers now use smaller message sizes to improve message compression. This results in reduced network usage.
- Added support for the AVC resource record type (Application Visibility and Control).
- minimal-responses now takes two new arguments: no-auth suppresses populating the authority section but not the additional section; no-auth-recursive does the same but only when answering recursive queries.
- At server startup time, the queues for processing notify and zone refresh queries are now processed in LIFO rather than FIFO order, to speed up loading of newly added zones.
- When answering queries of type MX or SRV, TLSA records for the target name are now included in the additional section to speed up DANE processing.
- named can now use the TCP Fast Open mechanism on the server side, if supported by the local operating system.

dig(1)

When dig receives a truncated (TC=1) response or a BADCOOKIE response code from a server, it will automatically retry the query using the server COOKIE that was returned by the server in its initial response.

rndc(8)

- rndc can now return text output of arbitrary size to the caller. (Prior to this, certain commands such as rndc tsig-list and rndc zonestatus could return truncated output.
- Changed rndc reconfig behavior so that newly added zones are loaded asynchronously and the loading does not block the server.
- Errors reported when running rndc addzone (for example, when a zone file cannot be loaded) have been clarified to make it easier to diagnose problems.
- rndc flushtree now flushes matching records from the address database and bad cache as well as the DNS cache.
- A comment is now included in .nzf files (which are used for adding new zones through rndc) to give the name of the associated view.

dnssec-keyfromlabel(8)

The -S and -i options to dnssec-keygen and dnssec-settime (to set up a successor key and set the prepublication interval) were inadvertently left out of dnssec-keyfromlabel". This has been corrected.

nsupdate(1)

By default, nsupdate will now check the correctness of hostnames when adding records of type A, AAAA, MX, SOA, NS, SRV or PTR. This behavior can be disabled with check-names no.

Installation of BIND (HP-UX NameServer)

Installing BIND (HP-UX NameServer) 9.11.1

Prerequisites

- OpenSSL A.01.00.02h or later
- Kerberos client

Installation instructions

To install BIND (HP-UX NameServer) 9.11.1, you need to complete the following steps:

Procedure

1. Review to ensure that your system meets BIND (HP-UX NameServer) 9.11.1 installation requirements.
2. Go to HPE Software Depot Home at: Software Depot Home.
3. Use **Search** button to browse for BIND (HP-UX NameServer). The product catalog page is displayed.
4. Select BIND (HP-UX NameServer) in the product catalog. BIND (HP-UX NameServer) page is displayed.
5. Read the **Overview** and **Installation** pages for BIND (HP-UX NameServer).
6. Click **Select** at the bottom right of any of these pages.
7. Select the appropriate release of HP-UX operating system.
8. Enter the registration information. Read and Accept the terms and conditions statements.
9. Click **Next>>**. The Electronic Delivery Receipt page is displayed.
10. Select BIND (HP-UX NameServer) 9.11.1 depot under Download Software.
11. Save BIND (HP-UX NameServer) 9.11.1 depot in a local directory, for example, /tmp.
12. To verify that BIND (HP-UX NameServer) 9.11.1 depot is downloaded properly in the local directory, enter the following HP-UX MD5 Secure Checksum command at the HP-UX prompt:

    ```
    # md5sum <depot_name>
    ```

    The result of this command must match the fingerprint provided in the Electronic Delivery Receipt. If the result does not match, download BIND (HP-UX NameServer) 9.11.1 depot again.

    NOTE:

    The HP-UX MD5 Secure Checksum software is not installed by default on the system. It is available at: Software Depot Home.

13. To install BIND (HP-UX NameServer) 9.11.1 depot, enter the following command at HP-UX prompt:

    ```
    # swinstall -s <fully_qualified_depot_source_path>
    ```

    The `swinstall` window is displayed.
14. Press the space bar to select the product that you wish to install.
15. Select **Install** in the **Action** menu. The Install Analysis window is displayed.
16. Select **OK** when the Status field displays a Ready message. The Install window is displayed. BIND (HP-UX NameServer) 9.11.1 software installation starts. The `swinstall` command loads BIND (HP-UX NameServer) 9.11.1 files on to the system in approximately five minutes.

17. Select **Done**, when the Status field displays a Completed message.
18. Select **File -> Exit** to exit from the `swinstall` window. The named daemon is pre-configured and starts after installation. The `swinstall` command installs BIND (HP-UX NameServer) in the `/opt` directory.

NOTE:

For more information on configuring and using BIND (HP-UX NameServer), see *BIND 9.11 Administrator Reference Manual* at BIND (HP-UX NameServer) Software Depot Pages and also available at **http://www.isc.org**.

Verifying BIND (HP-UX NameServer) 9.11.1 installation

To verify whether BIND (HP-UX NameServer) 9.11.1 depot is installed successfully on your system, enter the following command at the HP-UX prompt:

```
# swlist -l product <depot_name>
```

If BIND (HP-UX NameServer) 9.11.1 is installed properly, the following output is displayed on a HP-UX 11i v3 operating system.

```
# Initializing...
# Contacting target "hostname"...
#
# Target: hostname:/
HPUX-NameServer C.9.11.1.N HPUX Name Server
HPUX-NameServer.NameService C.9.11.1.N Berkeley Internet Name Domain Server
Protocol daemons and utilities.
```

Unsupported features

The following features supported in open source BIND, are not supported in HP-UX BIND(Name Server) 9.11.1.mm:

- Integrate contributed IDN code
- Integrate contributed DLZ code into named
- Allow dnstap packet logging
- GeoIP access control
- PKCS#11/Cryptoki support
- Native PKCS#11/Cryptoki support
- Use libseccomp system call filtering
- Very verbose query trace logging
- Use GNU libtool
- Python tools
- XML statistics
- JSON statistics
- HTTP zlib compression
- LMDB database to store configuration for addzone zones

Documentation for BIND 9.11.1

Manpages

Table 3: BIND (HP-UX NameServer) 9.11.1 Manpages

Manpage	Description
arpaname(1)	Utility to translate IP addresses (IPv4 and IPv6) to the corresponding IN- ADDR.ARPA or IP6.ARPA names.
delv(1)	DNS lookup and validation utility.
mdig(1)	DNS pipelined lookup utility.
named-rrchecker(1)	syntax checker for individual DNS resource records.
nsupdate(1)	Dynamic DNS update utility.
dig(1)	DNS lookup utility.
host(1)	Utility for DNS lookup.
dnssec-importkey(8)	Utility to import DNSKEY records from external systems so they can be managed.
dnssec-keyfromlabel(8)	DNSSEC key generation tool.
ddns-confgen(8)	Tool to generate a key for use by nsupdate and named.
dnssec-dsfromkey(8)	DNSSEC DS RR generation tool.
dnssec-settime(8)	Tool to set the key timing metadata for a DNSSEC key.
genrandom(8)	Tool to generate a file containing random data.
sc-hmac-fixup(8)	Fixes HMAC keys generated by older versions of BIND (HP-UX NameServer).
named-journalprint(8)	Utility to print zone journal in human-readable form.
named(8)	Daemon that reads BIND (HP-UX NameServer) configuration file, /etc/named.conf for initial data on resource records, and listens for queries. The named daemon is the Internet domain name server, and it requires super user privileges to execute.
nsec3hash(8)	Tool to generate an NSEC3 hash based on a set of NSEC3 parameters.
dnssec-revoke(8)	Tool to set the REVOKED bit on a DNSSEC key.

Table Continued

Manpage	Description
dnssec-signzone(8)	Tool to sign the DNSSEC zone.
dnssec-keygen(8)	Tool to generate keys for DNSSEC.
dnssec-verify(8)	Tool to verify DNSSEC zone.
named-checkconf(8)	Tool to check the syntax of the named configuration file.
rndc.conf(4)	rndc configuration file.
named.conf(4)	configuration file for named.
named-checkzone(8)	named-checkzone, named-compilezone - zone file validity checking or converting tool
named-compilezone(8)	named-checkzone, named-compilezone - zone file validity checking or converting tool.
tsig-keygen(8)	ddns key generation tool.
lwresd(8)	lightweight resolver daemon.
sig_named (1M)	send signals to the domain name server.
hosts_to_na(1M)	Program used to translate host table to name server file format.
rndc-confgen(8)	rndc key generation tool.
rndc (8)	name server control utility.

nslookup(1), dig(1), and host(1) can be used to troubleshoot BIND (HP-UX NameServer) 9.11.1.

Product documentation

For more information on configuring, administering, and using BIND (HP-UX NameServer), see *BIND 9 Administrator Reference Manual*, *HP-UX IP Address and Client Management Services Administrator Guide*, and Software Depot Pages for quick reference at:

- Hewlett Packard Enterprise Support Center (HPESC): **http://www.hpe.com/info/hpux-networking-docs**.
- Software Depot Pages of BIND (HP-UX NameServer): **BIND (HP-UX NameServer) Software Depot Page**.
- *BIND 9 Administrator Reference Manual* is available at **http://www.isc.org**.

Defect fixes across various releases of BIND (HP-UX NameServer)

Table 4: Defect fixed in BIND (HP-UX NameServer) 9.11.1 (C.9.11.1.2.0) release

Defect Identifier	Description
QXCR1001567752	**Title**: HP-UX: `named(8)` auto start on reboot. **Severity**: Medium. **Problem**: `named(8)` does not automatically start at reboot. **Details**: This CR implements fixes for the following defect: `named(8)` does not start automatically on a reboot even after changing value from **0 to 1** in `/etc/rc.config.d/namesvrs_dns`. **Resolution**: Links to the `named(8)` start and stop scripts are corrected to fix this defect.
QXCR1001561745	**Title**: HP-UX: `named(8)` and `lwresd(8)` are not working as expected. **Severity**: Serious. **Problem**: `named(8)` and `lwresd(8)` impacted by CVE-2017-3140, CVE-2017-3142, CVE-2017-3143. **Details**: This CR implements fixes for the following CVEs: 1. **CVE-2017-3140**: If `named(8)` is configured to use Response Policy Zones (RPZ) an error processing some rule types can lead to a condition where BIND will endlessly loop while handling a query. 2. **CVE-2017-3142**: An error in TSIG authentication can permit unauthorized zone transfers in `named(8)`. 3. **CVE-2017-3143**: An error in TSIG authentication can permit unauthorized dynamic updates in `named(8)`. **Resolution**: `named(8)` and `lwresd(8)` are modified to fix these CVEs.

Hewlett Packard Enterprise specific changes

Table 5: Hewlett Packard Enterprise specific changes in BIND (HP-UX NameServer) 9.11.1

Change identifier	Description
QXCR1000552734	Add an Option statement to disable the EDNS feature on BIND (HP-UX NameServer).
QXCR1000552677	DNS does not check for symbolic links.

Table Continued

Change identifier	Description
QXCR1000552678	DNS does not check if dynamic DNS log files are linked.
QXCR1000577501	rndc recursing - named.recursing output contains old data.
QXCR1000791343	Provide 64-bit binary for named for supporting larger cache size.

Known problems, issues, limitations, and workaround

There is no known problem or issue in BIND (HP-UX NameServer) 9.11.1.

Source code availability

The source code for HP-UX Name Server 9.11.1 can be downloaded from this **location**: (Open Source Software > Software Products > Operating Systems).

Related documentation

For more information about BIND (HP-UX NameServer), see the following documents at **http://www.hpe.com/info/hpux-networking-docs-11iv3**:

- BIND 9.11 Administrator Reference Manual
- HP-UX IP Address and Client Management Services Administrator Guide

Software and documentation availability in native languages

The product is supported only in English locale (LANG=C). Behavior of the product is unpredictable when LANG value is set to any other language code other than C. Documentation support for this product is also available only in English locale.

Reporting defects

You can report defects related to BIND (HP-UX NameServer) product.

Contact the local Hewlett Packard Enterprise representative to file a defect.

Support policies for HP-UX

For more information about support policy of HP-UX, see **HP-UX support policy**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.