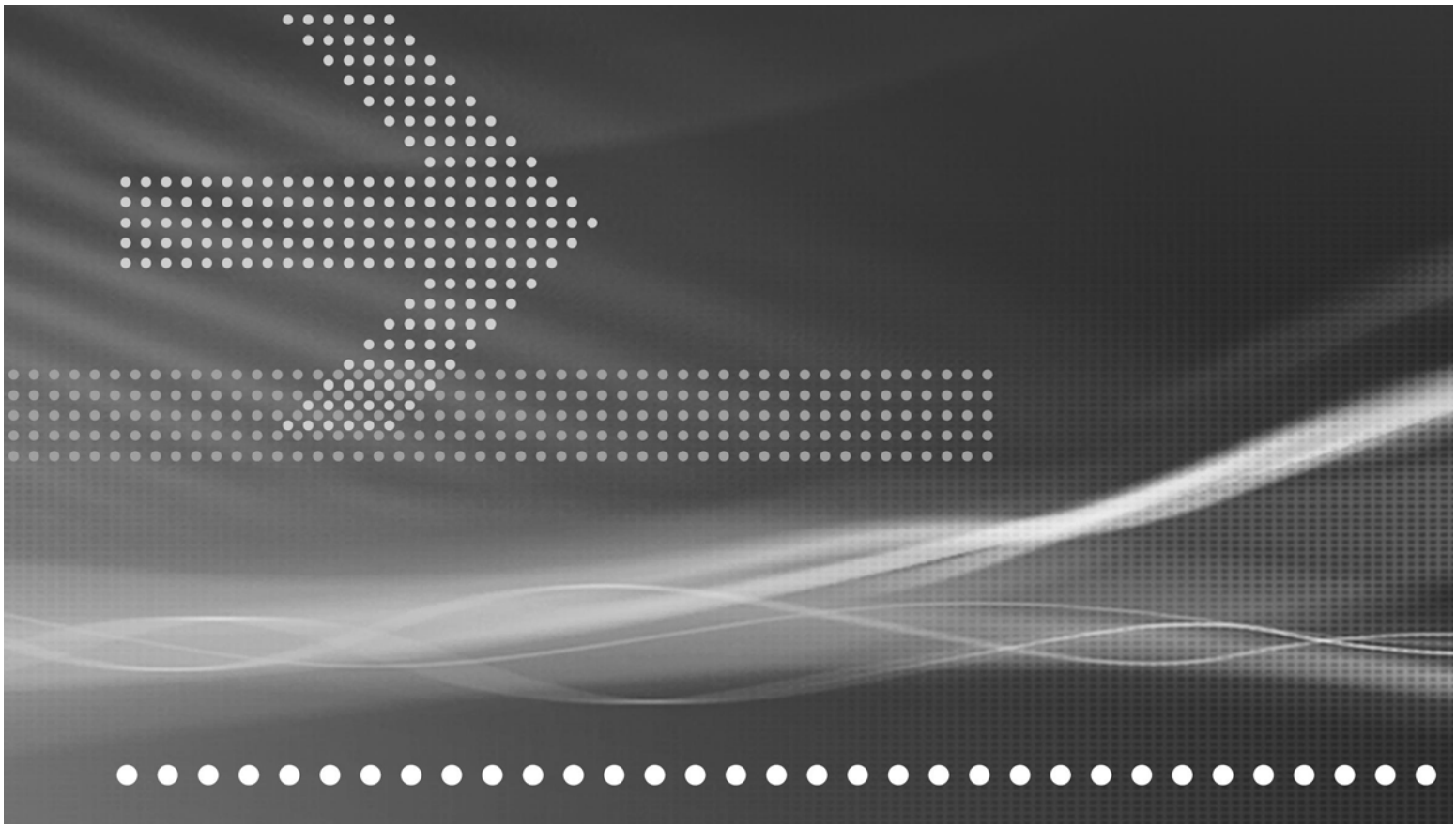

VitalQIP®

DNS/DHCP & IP MANAGEMENT SOFTWARE | LUCENT DNS RELEASE 4.1

BUILD 14 RELEASE NOTES

190-409-112R4.1
JANUARY 2010
ISSUE 10

Contents

List of tables

About this document

Purpose

This document provides important information about the contents of Lucent DNS 4.1 Build 14. It covers new features, system requirements, product installation and upgrades, as well as resolved problems and known issues.

Important! The content of this document is cumulative: it contains information already published to support previous builds. Resolved customer issues, for example, are organized by the build in which the fix occurred.

Reason for reissue

The Lucent DNS 4.1 Release Notes have been reissued to include a revision to CERT Advisory VU#418861, which addresses a potential cache poisoning vulnerability and to include CERT Advisory VU #360341 which addresses a vulnerability of the DNSSEC NSEC/NSEC3 validation code.

The following table shows the revision history of this document.

Issue number	Issue date	Version	Description of changes
10	January 2010	Build 14	An additional fix was included for CERT Advisory VU#418861 and a fix was made for CERT Advisory VU#360341. Refer to Table 4-1 on page 4-2, and Table 5-2 on page 5-3.
9	November 2009	Build 13	A fix was made for the CERT Advisory VU#418861 BIND 9 Cache Update from Additional Section. Refer to Table 4-1 on page 4-2, and Table 5-2 on page 5-3.
8	July 2009	Build 12	A fix was made for the CERT Advisory VU#725188 Remote Dynamic Update Message Denial of Service Vulnerability. Refer to Table 4-1 on page 4-2, and Table 5-2 on page 5-3.
7	January 2009	Build 11	Fixed document number and footer.

Issue number	Issue date	Version	Description of changes
6	December 2008	Build 11	• New supported platforms • Updated UNIX installation instructions • Updated for post installation requirements.
5	October 2008	Build 11	• New installation instructions section added • Resolution of issues: LDNS 945, 958, 960, 970, and 974 (Table 4-1).
4	July 2008	Build 6	A fix was made for the Advisory CERT VU#800113 DNS Cache Poisoning Issue (Table 5-2).
3	February 2008	Build 3	New features supported: • Persistent startup parameters on Windows • client-edns directive • Large file support • BIND 9 support • DNS statistics counters.

Conventions used

This document uses the following typographical conventions:

Appearance	Description
Italicized text	• File and directory names • Titles of publications • A value that the user supplies
Bold italicized text	• Emphasized information
graphical user interface text or key name	• Text that is displayed in a graphical user interface or in a hardware label • The name of a key on the keyboard
`input text`	Command names and text that the user types or selects as input to a system
`Italicized input text`	Input variable for which you must substitute another value. The angle brackets **<** and **>** also indicate the value is a variable.
`output text`	Text that a system displays or prints

Technical support

For assistance, contact your Welcome Center:

- For North America customers: **1-866-LUCENT8** (**582-3688**), Option 1, Option 2
- For Europe, Middle East, and Africa technical support: **00 800 00 LUCENT** or **+353 1692 4579**
- For Central and South America customers: **0800 89 19325** or **+55 11 3205 7626**

  Important! For other local CALA numbers consult the web site http://www.alcatel-lucent.com/support or contact your local sales rep.
- For Asia Pacific technical support:
  - **1800-458-236** (toll free from within Australia)
  - (IDD) **800-5823-6888** (toll free from Asia Pacific – China, Hong Kong, Indonesia, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, and Thailand)
  - **(613) 9614-8530** (toll call from any country)

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support web site (http://alcatel-lucent.com/support/) for contact information.

How to order

To order Alcatel-Lucent documents, contact your local sales representative or use the Online Customer Support Site (OLCS) web site (https://support.lucent.com).

How to comment

To comment on this document, go to the Online Comment Form (http://www.lucent-info.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Release components

Overview

Purpose

This chapter describes software and documentation deliverables included in this release.

Lucent DNS 4.1 Build 14 is based on ISC BIND 9.4.1-P1 with security fixes and enhancements from BIND 9.4.2-P2, 9.4.3-P3, 9.4.3-P4, and 9.4.3-P5 for BIND 9 CERT for VU#418861 and VU#360341. With the enhancements and fixes included in Lucent DNS 4.1 Build 14, Alcatel-Lucent recommends you replace earlier versions of Lucent DNS 4.1 with the current Lucent DNS 4.1 Build 14 or Lucent DNS 4.2 Build 14.

Important! For customers still using Lucent DNS 3.1 or BIND 8 servers, ISC's end of life announcement for BIND 8.x was effective on August 27, 2007. Since there are significant differences between BIND 8 and BIND 9, customers should familiarize themselves with the BIND 9 server in their labs prior to implementing in production. Contact Technical Support for assistance with upgrading servers from Lucent DNS 3.1 or BIND 8 to Lucent DNS 4.1.

Contents

This chapter covers these topics.

Software deliverables

The following table lists the software that comprises the Lucent DNS 4.1 Build 14 release.

Table 1-1 Software deliverables

Type	Platform	Directory	File
Lucent DNS Software	Linux	*/vitalqip/LDNS/DNS4.1/Linux/named941B14*	*ldns4.1.14-linux-gcc3.tar*
	Solaris	*/vitalqip/LDNS/DNS4.1/Solaris/named941B14*	*ldns4.1.14-solaris.2x.tar*
	Windows 2003/ Windows 2008	*/vitalqip/LDNS/DNS4.1/w2k/named941B14*	*ldns4.1.14-w2k.zip*

How to obtain software

VitalQIP Lucent DNS 4.1.B14 installation files are available for download via Alcatel-Lucent Electronic Delivery (ALED) services. ALED uses secure HTTP and FTP to download files and documentation. In order to use ALED, you must be registered with Alcatel-Lucent Global Support.

If you are not registered with Alcatel-Lucent Global Support, visit https://market.lucent.com/release/SPRegistrantTypeSvlt. If you need assistance in registering, contact the Alcatel-Lucent Customer Support Services:

- Inside the United States: 1 (866) 582-3688, prompt 7
- Outside the United States: 1 (630) 218-7688

You must have SSH installed and configured before downloading installation files. For more information about setting up secure FTP, visit https://download.support.lucent.com/cgi-bin/ssh_ftp.cgi. After you have set up secure FTP, you can connect via secure FTP and access the **Product|Version|Platform** directory to download the product's files. To download the product via secure HTTP, follow these steps:

1. If you have not registered, register at https://market.lucent.com/release/SPRegistrantTypeSvlt

2. Open a browser and go to https://support.lucent.com/portal/olcsHome.do.

3 Log in with your user name and password. The Customer Center is displayed.

4 Under Technical Support, click **Downloads**.

5 Click **U-Z**.

6 Under V, click on **VitalQIP®**.

7 Under Documentation and downloads, click **Downloads: Electronic Delivery**.

8 Select **LDNS** and click **Next**.

9 Select **4.1** and click **Next**.

10 Select the appropriate platform and click **Next**.

11 Select the file to download and click **Next**.

12 Specify the download directory on your local machine.

13 Click **Download** to use the legacy download agent, or **Download Plus** to use the GetPlus® download agent.

END OF STEPS

Document deliverables

Documentation available for this release

The following table lists the available documentation for the Lucent DNS 4.1 Build 14 release.

Table 1-2 Documentation list

Type	Directory	File
Release Notes	*/vitalqip/LDNS/DNS4.1/Linux/named941B14RN-Linux* */vitalqip/LDNS/DNS4.1/Solaris/named941B14RN-Solaris* */vitalqip/LDNS/DNS4.1/Windows/named941B14RN-Windows*	*LDNS41B14RN.pdf*

To obtain documentation

In addition to the ALED site, VitalQIP product documentation is available to customers through OnLine Customer Support (OLCS).

To navigate to OLCS, follow these steps:

1. Go to https://support.lucent.com/portal/productIndexByCat.do
2. Select the product category for which you require documentation. For example, for VitalQIP documentation, select **Network, Service Management and OSS**.
3. To obtain manuals, select **Manuals and Guides**. To obtain release notes, select **Release Information**.

2 New features

Overview

Purpose

The following sections identify the new features and/or capabilities contained in this release.

Contents

This chapter covers these topics.

Persistent startup parameters on Windows

Feature ID

Description

BIND 9 does not accept any parameters from the ImagePath registry entry, so any startup options must be manually entered at each start time. Since build 3, Lucent DNS 4.1 includes the ability to accept startup parameters from the ImagePath registry key: **HKEY_LOCAL_MACHINE**->**System**->**CurrentControlSet**->**Services**->**Lucent DNS Service**, for example:

```
C:\qip\named\bin\named.exe -n 2
```

client-edns directive

Feature ID

LDNS 00000887

Description

Qddns options must be placed in the named.conf file. This option can be used to prevent the DNS server from sending EDNS with outgoing queries. This directive was added in Lucent DNS 4.1, build 3.

The following can be added to the **qddns** block of the **options** block in *named.conf*:

```
client-edns no;
```

Valid values are yes and no. The default is yes. If the option is set to no, the DNS server will not add EDNS information to the additional section of outgoing DNS communication initiated by the DNS server. EDNS allows larger UDP packets than the standard 512 bytes, so this option should only be set to no when the environment is not conducive to routing the larger UDP packets.

Large file support (UNIX only)

Feature ID

LDNS00000912

Description

Some files can grow to a large size and cause the nameserver to exit. This feature has been added to allow access to files greater than 2GB in size (64-bit file sizes). Large file support was added in Lucent DNS 4.1, build 3 for Linux and Solaris.

BIND 9 support

Feature ID

R.DNS-00025 BIND Compatibility

Description

Lucent DNS 4.1 is based on ISC BIND 9.4, and now supports DNSSEC.

Important! BIND 9 support was added in Lucent DNS 4.0.

Additional information on BIND 9 can be found in the DNS & BIND Fifth Edition, by O'Reilly and Associates, and in the *BIND 9 Administrator's Reference Manual*, located at http://www.isc.org/sw/bind/arm94/Bv9ARM.pdf. See "Configuring Lucent DNS 4.1" on page 27 for information on configuring Lucent DNS.

DNS statistics counters

Feature ID

Description

Lucent DNS 4.1 returns the following counter statistics. Note that there is a difference between Lucent DNS 3.1, 4.0, and 4.1 counters. **`dupquery`** and **`droppedquery`** were added in Lucent DNS 4.1, build 3.

The counters, their definitions, and the supported releases are as follows:

Table 2-1 Lucent DNS 4.1 and BIND 9 counters (not available to SNMP)

Counter	Definition
dupquery	dupquery is incremented when a duplicate query, which is (not available to SNMP) already recursing, is received.
droppedquery	droppedquery is incremented when a duplicate of a query that is received, and the number of clients waiting for the same query is greater than the clients-per-query value (default of 10).

Table 2-2 Lucent DNS 4.x and BIND 9 counters (not available to SNMP)

Counter	Definition
success	Incremented when sending a response and the ANSWER section of the packet is populated.
referral	Incremented when sending a response and the AUTHORITY section of the packet contains the authoritative NS records.
nxrrset	Incremented when sending a response and the AUTHORITY section of the packet contains the authoritative SOA record.
nxdomain	Incremented when sending a response and the opcode is NXDOMAIN (3).
recursion	Incremented when a client request with opcode QUERY (0) begins the recursion process and the request passes recursion ACLs.
failure	Incremented when sending a response and the opcode is neither NOERROR (0) nor NXDOMAIN (3).

Table 2-3 Lucent DNS 4.x and 3.1 (available to SNMP)

Counter	Definition
RR	Incremented when a recursive response with opcode QUERY (0) or response to internal server query (SysQ) is successfully received.
RNXD	Incremented when a recursive response is successfully received with rcode NXDOMAIN (3).
RFwdR	Incremented when a recursive response is successfully received as a referral.
RDupR	Incremented when an RRset already exists in the response and is attempted to be added again.

Counter	Definition
RFail	Incremented when a recursive response is successfully received with rcode SERVFAIL (2).
RFErr	Incremented when a recursive response is successfully received with rcode FORMERR (1).
RErr	Incremented when a recursive response is successfully received with rcode not NOERROR (0), FORMERR (1), SERVFAIL (2), or NXDOMAIN (3).
RAXFR	Incremented when a client request for AXFR or IXFR is successfully received.
RLame	Incremented when a recursive response is successfully received which is determined to be lame (delegation to other than a subdomain and no answers in the ANSWER section of the packet).
ROpts	Incremented when a client request is received with options set (ie. for EDNS). This counter is not incremented if the query was an inverse query (IQuery).
SSysQ	Incremented when a request is created as part server operations, not on behalf of a client.
SAns	Incremented when sending a response and the ANSWER section of the packet is populated and the AA (authoritative) bit is on.
SFwdQ	Incremented each time a query is successfully restarted more than once.
SDupQ	Incremented each time a query is successfully restarted more than once.
SErr	Incremented when an attempt to send data over a socket encounters an error.
RQ	Incremented when a successful request is received. This counter is not incremented if the packet is malformed, requestor is blackholed, there is no matching view, or the request has a bad TSIG).
RIQ	Incremented when a client request is received with an opcode of IQuery (1).
RFwdQ	Incremented when a client request with opcode QUERY (0) begins the recursion process and the request passes recursion ACLs.
RDupQ	Incremented when a query response is received for which we are not awaiting a response.
RTCP	Incremented when a successful TCP request is received. This counter is not incremented if the packet is malformed, requestor is blackholed, there is no matching view, or the request has a bad TSIG).
SFwdR	Incremented when sending any response.

Counter	Definition
SFail	Incremented when the response to a client request has the rcode value of FORMERR (1).
SFErr	Incremented when the response to a client request has the rcode value of SERVFAIL (2).
SnaAns	Incremented when sending a response and the ANSWER section of the packet is populated and the AA (authoritative) bit is off.
SNXD	Incremented when sending a response and the opcode is NXDOMAIN (3).
RUQ	Incremented when a client request with opcode QUERY (0) is successfully received, but denied by the query ACL.
RURQ	Incremented when a client request with opcode QUERY (0) is denied recursion by recursion ACL or if there is not root hints for a root server referral.
RUXFR	Incremented when a client request for AXFR or IXFR is successfully received, but is denied by transfer ACL.
RUUpd	Incremented when a client request with opcode UPDATE (5) is successfully received, but denied by update ACL or policy.
DUAdded	Incremented when a client request with opcode UPDATE (5) is successfully received and a resource record is successfully added.
DUDeleted	Incremented when a client request with opcode UPDATE (5) is successfully received and a resource record is successfully deleted.

Sample statistics dump at shutdown:

```
20-Dec-2007 11:34:19.299 XSTATS 1198168459 1198168455 success=0
referral=0 nxrrset=0 nxdomain=0 recursion=0 failure=0 dupquery=0
droppedquery=0 RR=0 RNXD=0 RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0
RAXFR=0 RLame=0 ROpts=0 SSysQ=0 SAns=0 SFwdQ=0 SDupQ=0 SErr=0
RQ=0 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0 SFErr=0
SNaAns=0 SNXD=0 RUQ=0 RURQ=0 RUXFR=0 RUUpd=0 DUAdded=0
DUDeleted=0
```

3 Changes to interfaces, alarms, and messages

Overview

Purpose

This chapter describes changes to Lucent DNS for the 4.1 release.

Contents

This chapter covers these topics.

Default behavior change for allow-recursion

Description

In Lucent DNS 4.1 build 3, the default behavior of **`allow-recursion`** changed from Lucent DNS 4.0 to Lucent DNS 4.1.

The previous default behavior was to allow any IP, and the new default behavior is only to allow the localhost and localnets.

Default value change for minimal-responses

Feature ID

LDNS 00000904

Description

In Lucent DNS 4.1 build 3, the default for minimal-responses was changed from no to yes. This means that the DNS server will not include the name server and glue records in the authority and additional sections in answer responses.

Perform sanity checks on NS records within-zone names

Description

In Lucent DNS 4.1 build 3, the default is to check for address glue records for NS records with in-zone names. A warning will be logged if a check encounters a problem.

rndc freeze and thaw all zones

Description

In Lucent DNS 4.1 build 3, if there is no zone argument to rndc freeze or rndc thaw, all zones are frozen or thawed, respectively.

Limit recursive clients for a single query

Description

In Lucent DNS 4.1 build 3, a limit has been set for the number of recursive clients that can be waiting for a single query to resolve.

New BIND 9 options **`clients-per-query`** and **`max-clients-per-query`** are available to change the default values. The defaults, respectively, are 10 and 100.

New automatic empty zone creation

Description

In Lucent DNS 4.1 build 3, eleven new default zones are created at server startup.

This can be disabled per empty zone (**`disable-empty-zone "<zone>"`**), by policies, or for all empty zones (**`empty-zones-enable no;`**). The default setting is **`empty-zones-enable yes;`**

The default behavior is to create all 11 empty zones.

```
127.IN-ADDR.ARPA
254.169.IN-ADDR.ARPA
2.0.192.IN-ADDR.ARPA
255.255.255.255.IN-ADDR.ARPA
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
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
D.F.IP6.ARPA
8.E.F.IP6.ARPA
9.E.F.IP6.ARPA
A.E.F.IP6.ARPA
B.E.F.IP6.ARPA
```

DNSSEC is enabled by default

Description

In Lucent DNS 4.1 build 3, DNSSEC support is enabled by default. DNSSEC support can be disabled by setting the **`dnssec-enable no`** option.

New statistics

In Lucent DNS 4.1 build 3, new duplicate query statistics are available at exit and from rndc stats.

The new stats categories are **`dupquery`** and **`droppedquery`**. **`dupquery`** will be incremented when a duplicate query of a query that is already recursing is received. **`droppedquery`** will increment when a duplicate query of a query that is already recursing is received and the number of clients waiting for the same query is greater than the clients-per-query value (default of 10).

4 Resolved issues

Overview

Purpose

This chapter describes resolved issues in this release.

Contents

This chapter covers these topics.

Resolved issues

The following table identifies the customer reported issues that have been resolved in Lucent DNS 4.1.

Table 4-1 Customer-reported ARs resolved in Lucent DNS 4.1

Fault ID	AR number	Description of issue	Release fixed
LDNS00001130		A validating recursive nameserver may incorrectly cache records from the additional section of a query response. A BIND DNS Security CERT - CERT: VU#418861 has been amended, as described in Table 5-2 Known vendor issues on page 5-3. This build also includes a fix for VU#360341. DNSSEC NSEC/NSEC3 validation code could cause bogus NXDOMAIN responses.	Build 14
LDNS00001116		A validating recursive nameserver may incorrectly cache records from the additional section of a query response. If the nameserver is authoritative only, this will not occur. A BIND DNS Security CERT - CERT: VU#418861 has been issued, as described in Table 5-2 Known vendor issues on page 5-3.	Build 13
LDNS00001107	1-2376250	Badly formed DNS - incorrect AD bit set.	Build 13
LDNS00001100	1-2342105	BIND DNS Security CERT - CERT: VU#725188 for DNS 4.1. Remote Dynamic Update Message Denial of Service Vulnerability	Build 12
LDNS00000945		dig fails if no DNS server set in network IP protocol properties and no nameserver value in or invalid resolv.conf exists.	Build 11
LDNS00000974	1-1964446	Server does not respond to queries after error, “UDP client handler shutting down due to fatal receive error”.	Build 10
LDNS00000958	1-1916663 1-1925067 1-1925840 1-1926220	Bind-9.4.2-p1 security fix causes server crash.	Build 8

Fault ID	AR number	Description of issue	Release fixed
LDNS00000970	1-1948036	Getting error, “socket: too many open file descriptors”.	Build 7
LDNS00000960		Merge bind-9.4.2-p2 for udp source port performance improvement.	Build 7
LDNS00000956	1-1919820	Syntax error of option “empty-zones-enable” in LDNS 4.1 B3.	Build 6
LDNS00000944		**Merge bind-9.4.2-p1 for Bind 9 Security CERT VU#800113.**	Build 6
LDNS00000933	1-1792550	DNS 4.1 service exiting due to assertion failure.	Build 6
LDNS00000931	1-1770128	Cannot get the new bind 9 build (LDNS 4.1) installauto to work. Documentation change was made in DNS 4.1 Release Notes.	Build 3

LDNS00000920		*named-check.exe* fails to run with insist error.
		`INSIST(0)failed`
		`../named-checkzone.c:137:`
			Build 6

LDNS00000905		Incorporate l.root-servers update patch.	Build 3
LDNS00000904	1-1734954	LDNS 4.x should have “minimal-responses yes” by default.	Build 3
LDNS00000895	1-1336273 1-1381732	DNS Zone transfers fail with “quota reached” errors until DNS is stop/started.	Build 3
LDNS00000887	1-1669390	RFE/Defect for a Server policy that allows { edns no; }; to be set without having to specify a destination IP address.	Build 3
LDNS00000853	1-1555590	Malformed message errors in the event viewer - Lucent 4.x build 19.	Build 3
LDNS0000848	1-1553113	nslookup does not return results from dns servers configured with recursion no; **Working as designed:** The difference is that BIND9 nslookup does not print the referral NS records, but instead prints that the desired records were not found. This is not in error, but not as verbose as BIND8 nslookup.	Build 3
LDNS0000846	1-1535529	Server does not accept records longer than 255 characters for TXT record, with error “ran out of space”. **Working as designed:** TXT record type is limited to 255 characters of rdata per quoted string, not including the surrounding quotes.	Build 3
LDNS00000840		Message for slave zones “28-Sep-2006 14:09:21.139 general: error: zone domain.com/IN: zone serial has gone backwards”.	Build 3

Fault ID	AR number	Description of issue	Release fixed
LDNS00000832	1-1472724	Dynamic DNS Updates are lost when a DNS generation is pushed to a secondary server.	Build 3
LDNS00000810		named INSIST when reloading when ixfr-from-differences policy set.	Build 3
LDNS00000574	1-1064120	rndc qddns-push does not remove the ***.jnl** files - causes journal out of sync errors.	Build 3

5 Known issues

Overview

Purpose

This chapter describes known issues and workarounds if available for Lucent DNS 4.1 and other issues.

Contents

This chapter covers these topics.

Known issues and workarounds for Lucent DNS 4.1

The following table includes a list of known issues that were identified as customer impacting and/or outstanding customer problems that have not yet been resolved.

Table 5-1 Known issues and workarounds for Lucent DNS

Fault ID	AR number	Description of issue	Workaround
LDNS00000984	1-1979485	qddns-push error removing journal file in reload: permission denied causes subsequent journal write errors.	
LDNS00000880	1-1604261 1-1674155 1-1725790	The server is not answering DNS Queries in a timely manner.	For Windows, refer to "Persistent startup parameters on Windows", on page 2-2 for the workaround. For UNIX, add **–n 2** to the command line startup parameters.
LDNS00000889	1-1642141	Assertion failure: REQUIRE(rbtdb->furure_version == 0) failed.	
LDNS00000913	1-1730648	High memory usage when secure updates used.	

Known vendor issues

For a list of ISC BIND 9 issues that may also exist in Lucent DNS Server 4.x, see the CHANGES file in the latest distribution of ISC BIND 9, available from ftp://ftp.isc.org/isc/bind9/ under the corresponding BIND version folder.

The following table includes a list of known vendor issues that have been identified as customer impacting problems.

Table 5-2 Known vendor issues

Fault ID	Vendor	Description of issue	Workaround
LDNS00001130	ISC	Security CERT VU#418861 and VU#360341 Revised VU#418861: A nameserver with DNSSEC validation enabled may incorrectly add unauthenticated CNAME or DNAME records to its cache, either when processing client queries with checking disabled (CD) or when the nameserver internally triggers a query for missing records for recursive name resolution. CNAME or DNAME records added to cache in this way can be returned in response to a query with or without checking disabled (CD), and with or without requesting DNSSEC records (DO). VU#360341: DNSSEC NSEC/NSEC3 validation code could cause bogus NXDOMAIN responses. There was an error in the DNSSEC NSEC/NSEC3 validation code that could cause bogus NXDOMAIN responses (that is, NXDOMAIN responses for records proven by NSEC or NSEC3 to exist) to be cached as if they had validated correctly, so that future queries to the resolver would return the bogus NXDOMAIN with the AD flag set. This problem affects all DNSSEC-validating resolvers. It would be difficult to exploit due to other existing protections against cache poisoning (including transaction ID and source port randomization), but it could impair the ability of DNSSEC to protect against a denial-of-service attack on a secure zone. For further information, refer to https://www.isc.org.	Alcatel-Lucent recommends upgrading all DNS servers with DNSSEC validation enabled to DNS 4.1 Build 14.

Fault ID	Vendor	Description of issue	Workaround
LDNS00001116	ISC	Security CERT VU#418861 A nameserver with DNSSEC validation enabled may incorrectly add records to its cache from the additional section of responses received during resolution of a recursive client query. This behavior only occurs when processing client queries with checking disabled (CD) at the same time as requesting DNSSEC records (DO). **Note:** If the nameserver is authoritative only, this will not occur. For further information, refer to https://www.isc.org.	Alcatel-Lucent recommends upgrading all DNS servers with DNSSEC validation enabled to DNS 4.1 Build 13.
LDNS00001100	ISC	Security CERT VU#725188 Remote Dynamic Update Message Denial of Service Vulnerability. For further information, refer to https://www.isc.org or http://www.kb.cert.org/vuls/id/725188.	Alcatel-Lucent recommends upgrading all DNS servers to DNS 4.1 Build 12.
LDNS00000749	Red Hat	named cores on Linux with journal file greater than 2GB.	Delete *zonename.jnl* and restart the server. This is an OS limitation with files larger than 2GB; there are vendor patches available. Set the **`max-journal-size`** directive to less than 2GB (default is 4MB)
LDNS00000795 1-1333304 1-1343804 1-1374839 1-1420646	Intel	**Intel hyperthreading issue** Several customers have reported severe performance issues for Lucent DNS 4.x, Lucent DHCP, and other services when running with hyperthreading enabled. Intel hyperthreading is not supported. It is strongly recommended that Intel hyperthreading be turned off to avoid performance issues.	Set the number of CPUs with the command-line startup option “-n” to 1 or 2. Optionally, disable hyperthreading.
LDNS00000954	ISC	Crash when forwarding to IPv6 address and using query-source-v6 * port 5353.	

6 System requirements

Overview

Purpose

This chapter describes software and hardware requirements and compatibility restrictions.

Contents

This chapter covers these topics.

Supported platforms

Lucent DNS 4.1 is supported on the following platforms.

- Red Hat Enterprise Linux (AS,ES) 4, 5 - x86 and AMD64/Intel 64
- Solaris 9 UltraSPARC and 10 UltraSPARC (32 and 64 bit)
- Windows 2003 Enterprise or Standard Server (32 and 64 bit)
- Windows 2008 Standard and Enterprise Server (32 and 64 bit)

Important! Platform support is also dependent upon the VitalQIP Remote Server version. Reference the corresponding version of *VitalQIP Release Notes* for supported platforms. Lucent DNS 4.1 is supported on VitalQIP 6.2 Remote Servers running on operating systems that are also supported VitalQIP 7.x platforms.

Software requirements

The following table lists the minimum software requirements for VitalQIP and Lucent DNS.

Table 6-1 Software requirements for VitalQIP and Lucent DNS

Software	Version	Comments
VitalQIP	6.2	Lucent DNS 4.0, Build 15 is delivered with VitalQIP 6.2.
	7.0	Lucent DNS 4.0, Build 19 is delivered with VitalQIP 7.0, Build 460 (October 2006 Release). Lucent DNS 4.0, Build 21 is delivered with VitalQIP 7.0, Build 504.
	7.1	Lucent DNS 4.0, Build 22 is delivered with VitalQIP 7.1.
	7.2	Lucent DNS 4.1, Build 11 is delivered with VitalQIP 7.2.
	7.2 PR1	Lucent DNS 4.2, Build 12 is delivered with VitalQIP 7.2 PR1.

Hardware requirements

The following table lists the hardware requirements for VitalQIP remote servers to run Lucent DNS 4.1.

Table 6-2 Remote server hardware requirements

Platform	Requirements
Windows	500 MHz Pentium Processor, or higher 256 MB memory, minimum 300 MB of Disk Space
UNIX	300 MHz Processor 256 MB memory minimum per processor, more is strongly recommended 300 MB of Disk Space

7 Installation and upgrade notes

Overview

Purpose

This chapter contains notes on installation of Lucent DNS 4.1.

Contents

This chapter covers these topics.

Performing Lucent DNS 4.1 installation on Windows

When you are installing Lucent DNS 4.1 Build 14, ensure that you have met the system requirements described in the previous chapter and then refer to the documentation in Table 7-3 for further configuration information.

Important! Please refer to "Default behavior change for allow-recursion", on page 3-2 before you continue with the installation of Lucent DNS 4.1 Build 14.

The following table lists the files that are supplied with Lucent DNS 4.1 Build 14.

Table 7-1 Installation files on Windows

Filename	Description
named.exe	DNS server binary
rndc.exe	Remote name daemon control utility
dig.exe	DNS client utility
nsupdate.exe	DNS update utility
nslookup.exe	DNS client utility
named-checkconf.exe	Checks *named.conf* file syntax
named-checkzone.exe	Checks zone file syntax
rndc-confgen.exe	Generates rndc keys and configuration files
host.exe	DNS lookup utility
journalprint.exe	Utility to process binary BIND 9 journal files (<*db_file*>.*jnl*) and output the content as text
dnssec-keygen.exe	Not currently supported
dnssec-signzone.exe	Not currently supported

Pre-installation steps

Before you begin the upgrade, check the integrity of the installation file.

Perform the following steps:

1. Obtain the new Lucent DNS bundle and MD5.
2. If desired, verify the MD5 sum of the file with the supplied MD5 file.
3. Extract the Lucent DNS zip file to a *temp* directory.

END OF STEPS

Windows installation

To install Lucent DNS 4.1, follow these steps.

1. Stop Lucent DNS 4.1 (**named**) by selecting **Lucent DNS Service** and clicking **Stop** from the **VitalQIP Services Controller**.
2. Make a backup of the <*install_dir*>*bin* directory, if desired.
3. Create the desired install directory, such as *%QIPHOME%\named*, if it does not exist.
4. Create a *bin* and *etc* directory in the new install directory, if they do not exist. For example, *%QIPHOME%\named\bin* and *%QIPHOME%\named\etc*.
5. Copy the binaries into the <*install_dir*>*bin* directory.
6. From the <*install_dir*>*bin* directory, install the Lucent DNS 4.1 server by running one of the following command sequences:

If	Then
installing with manual startup	Run **named.exe -install <*install_dir*>** For example, **named.exe -install c:\qip\named** installs named so that the necessary files are found under *c:\qip\named*. The service will require a manual start after Windows starts.
installing with automatic startup	Run **named.exe – installauto <*install_dir*>** For example, **named.exe -installauto c:\qip\named** installs named so that the necessary files are found under *c:\qip\named* and the service will start automatically when Windows starts.

7 Add Lucent DNS Service to the Services Controller. Follow these steps:

a. Open the **Services Controller**.

b. Click **Configure**.

c. Click **Select Services**.

d. Click **Search**.

e. Highlight **Lucent DNS Service**.

f. Click **Add**.

g. Click **OK**.

h. Highlight **Lucent DNS Service** and check that the desired start type is selected (automatic or manual) and click **OK** again.

8 Start Lucent DNS 4.1 by selecting **Lucent DNS Service** and clicking **Start** from the **VitalQIP Services Controller**.

END OF STEPS

Post-installation requirement

rndc.exe should exist in the same location as specified in VitalQIP in **Server Profile->RNDC Path** and the *rndc.conf* should exist in the *<install_dir>/etc* directory and be configured appropriately in order to integrate with VitalQIP server update file generations.

Ensure the desired recursion access is set. To re-create the Lucent DNS 3.x or 4.0 recursion behavior, add the following lines to the corporate extensions section of the Server Profile:

```
option
     {
     allow-recursion { any; };
     allow-query-cache { any; };
      };
```

Without “allow-recursion” or “allow-query-cache” directives set, the default is to allow only localhost and localnets the ability to perform recursion and query the cache. The LDNS 3.1 and 4.0 default was to allow recursion and cache queries to “any”.

Performing Lucent DNS 4.1 installation on UNIX

When you are installing Lucent DNS 4.1 Build 14, ensure that you have met the system requirements described in the previous chapter and then refer to the documentation in Table 7-3 for further configuration information.

Important! Please refer to "Default behavior change for allow-recursion", on page 3-2 before you continue with the installation of Lucent DNS 4.1 Build 14.

The following table lists the files that are supplied with Lucent DNS 4.1 Build 14:

Table 7-2 Installation files on UNIX

Filename	Description
named	DNS server binary
rndc	Remote name daemon control utility
dig	DNS client utility
nsupdate	DNS update utility
nslookup	DNS client utility
named-checkconf	Checks named.conf file syntax
named-checkzone	Checks zone file syntax
rndc-confgen	Generates rndc keys and configuration files
host	DNS lookup utility
journalprint	Utility to process binary BIND 9 journal files (<*db_file*>.*jnl*) and output the content as text
dnssec-keygen	Not currently supported
dnssec-signzone	Not currently supported

Pre-installation steps

Before you begin the upgrade, check the integrity of the installation file.

Perform the following steps:

1. Obtain the new Lucent DNS bundle and MD5.
2. If desired, verify the MD5 sum of the bundle file with the supplied MD5 file.
3. Extract the Lucent DNS bundle to a *temp* directory. Execute:
   - For Linux: **`tar -xf ldns4.1.14-linux-gcc3.tar`**
   - For Solaris: **`tar -xf ldns4.1.14-solaris.2x.3.tar`**

END OF STEPS

UNIX installation

To install Lucent DNS 4.1, follow these steps.

1. Stop Lucent DNS 4.1 (*named*) by typing **`rndc stop`** or **`kill <named_pid>`** at a command line.
2. Make a backup of the named binaries. Prior to 7.2, named and utilities were located in */usr/sbin*. Starting with VitalQIP 7.2, **`named`** and utilities are located in *$QIPHOME/usr/bin*.
3. Copy the new binaries to *$QIPHOME/usr/bin* for 7.2 and */usr/sbin* for versions prior to 7.2.
4. Start Lucent DNS 4.1 by typing `<dns_path>/named` with command line options as desired or execute *$QIPHOME/etc/qip-rs-startup*.

END OF STEPS

Post-installation requirement

rndc should exist in the same location as specified in VitalQIP in **Server Profile->RNDC Path** and the *rndc.conf* should exist in the <*push_dir*> directory and be configured appropriately in order to integrate with VitalQIP server update file generations. Ensure that there is a link for */etc/named.conf* that points to <*push_dir*>*/named.conf*.

Uninstalling Lucent DNS 4.1 on Windows

To uninstall Lucent DNS 4.1 on Windows, follow these steps.

1. Stop Lucent DNS 4.1 (*named*) by selecting **Lucent DNS Service** and clicking **Stop** from the **VitalQIP Services Controller**.
2. Type the following command at a command line:
   `<install_dir>\bin\named -remove`
3. Remove the binaries specified in Table 7-1 from <*install_dir*>*\bin*.
4. Optionally, remove the data files and directory structure within <*install_dir*>.

5 Remove **Lucent DNS Service** from the **VitalQIP Service Controller** as follows**:**

a. In the **VitalQIP Service Controller**, click **Configure**.
b. Click **Select Services**.
c. In the **Managed Services** list, click **Lucent DNS Service**.
d. Click **Delete**.
e. Click **OK** to exit.

END OF STEPS

Uninstalling Lucent DNS 4.1 on UNIX

To uninstall Lucent DNS 4.1 on UNIX, follow these steps.

1 Stop Lucent DNS 4.1 by typing **`rndc stop`** or **`kill <named_pid>`** at a command line.

2 Remove the binaries specified in Table 7-2 from */usr/sbin*.

3 Optionally, remove the data files and directory structure within the *<named_QIP_push_directory>*.

END OF STEPS

Configuring Lucent DNS 4.1

Refer to the appropriate document in the following table for instructions on how to configure Lucent DNS 4.1.

Table 7-3 Configuration information

Document title	Part number	Chapter
VitalQIP 7.0, 7.1, and 7.2 User's Guide	190-409-068R7.0 190-409-068R7.1 190-409-068R7.2	Chapter 4, "Manage Servers", Lucent DNS 4.x Server Type

Document title	Part number	Chapter
VitalQIP 7.0 Administrator Reference Manual	190-409-042R7.0	Chapter 3, “Manage VitalQIP Services”: • Lucent DNS Service options • named - Lucent DNS service information Chapter 7, “Advanced DNS Configurations”: • Lucent DNS Directives • Secure Dynamic Update Support • External Objects and Resource Records Support
VitalQIP 7.1 and VitalQIP 7.2 Administrator Reference Manual	190-409-042R7.1 190-409-042R7.2	Chapter 2, “Manage VitalQIP Services”: • Configuring VitalQIP Service Controller • named - Lucent DNS service daemon Chapter 23, “Advanced DNS Configurations”: • Lucent DNS Directives • Secure dynamic updates support • External objects and resource records support • Improve DNS Push Functionality • Customize User Exit Scripts Chapter 24, "Troubleshoot DNS"
VitalQIP Services Manager 3.1 User’s Guide	190-409-037R7.1	Chapter 9, “DHCP and DNS Probes”: • DNS Probe Chapter 11, “Statistics on Services”: • Configure Statistics for the DHCP, DNS, and Message Services
VitalQIP SNMP Module 2.2 User’s Guide	190-409-038R7.1	Chapter 1, “SNMP Support for the Lucent DHCP and DNS Servers”: • Lucent DNS MIB variables

Glossary

A

ALED
Alcatel-Lucent Electronic Delivery

AR
Assistance Request

B

BIND
Berkeley Internet Name Domain

D

DNS
Domain Name System

F

FTP
File Transfer Protocol

G

GSS-TSIG
Generic Security Service Transaction Signature

H

HTTP
Hypertext Transfer Protocol

K

KDC
Key Distribution Center

S

SNMP
Simple Network Management Protocol

SP
Service Pack

W

WINS
Windows Internet Naming Service