# Alcatel-Lucent VitalQIP

## DNS/DHCP & IP MANAGEMENT SOFTWARE | Lucent DNS

**Release 5.1, Build 46**
**RELEASE NOTES**

190-409-112R5.1
March 2013
ISSUE 17

### Licenses

Refer to Appendix C, “Third party software license statements” in the *VitalQIP Release 7.3 Installation Guide* (190-409-043R7.3) for a complete description of all software licenses used to develop this product.

# Contents

## About this document

# About this document

## Purpose

This document provides important information about the contents of Lucent DNS 5.1 Build 46. 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

This document includes the following new features:

| Issue Number | Date of issue | Version | Description of changes |
|---|---|---|---|
| 17 | March 2013 | Build 46 | - LDNS0002371: Security fixes for CERT advisory CVE-2013-2266. Refer to Table , “Resolved issues in Lucent DNS 5.1, Build 46” (p. 4-2). |
| 17 | March 2013 | Build 46 | - LDNS0002308: Security fixes for CERT advisory CVE-2012-1033. Refer toTable , “Resolved issues in Lucent DNS 5.1, Build 46” (p. 4-2). |
| 16 | November 2012 | Build 44 | - Latest code from ISC BIND 9.7.7 is merged |
| 15 | October 2012 | Build 42 | - LDNS00002349: Security fixes for CERT advisory CVE-2012-5166. Refer to Table , “The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 42.” (p. 4-2). |

| Issue Number | Date of issue | Version | Description of changes |
|---|---|---|---|
| 14 | September 2012 | Build 41 | - LDNS00002344: Security fixes for CERT advisory CVE-2012-4244. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 41" (p. 4-2).<br>- LDNS00002339 is fixed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 41" (p. 4-2)<br>- LDNS00002291 is fixed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 41" (p. 4-2) |
| 14 | September 2012 | Build 41 | - Moved LDNS00001094 from Chapter 6, "Known issues" to Chapter 4, "Resolved issues". Refer to "Resolved issues in Lucent DNS 5.1, Build 41" (p. 4-2) |
| 13 | July 2012 | Build 40 | - LDNS00002311 is completed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 40" (p. 4-3). |
| 13 | July 2012 | Build 40 | - LDNS00001143 is fixed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 40" (p. 4-3).<br>- LDNS00002323: Security fixes for CERT advisory CVE-2012-3817. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 40" (p. 4-3). |
| 12 | June 2012 | Build 29 | - Security fixes are included for CERT advisory CVE-2012-1667.<br>- LDNS00002317 is fixed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 29" (p. 4-3) |
| 11 | June 2012 | Build 28 | - LDNS00002295, LDNS00002301, and LDNS00002307 are fixed. Refer to Table , "Resolved issues in Lucent DNS 5.1, Build 28" (p. 4-4). |

| Issue Number | Date of issue | Version | Description of changes |
|---|---|---|---|
| 10 | February 2012 | Build 16 | • LDNS00001446 is fixed. Refer to "Resolved issues in Lucent DNS 5.1, Build 16" (p. 4-4). |
| 9 | November 2011 | Build 15 | • Security fixes are included for CERT advisory CVE#2011-4313.<br>• LDNS00002297 is fixed. Refer to "Resolved issues in Lucent DNS 5.1, Build 15" (p. 4-5). |
| 8 | July 2011 | Build 12 | • Security fixes are included for CERT Advisories CVE#2011-2464 and CVE#2011-2465.<br>• LDNS00002292 is fixed. Refer to "Resolved issues in Lucent DNS 5.1, Build 12" (p. 4-5).<br>• Upgraded the BIND variable version to 9.7.3-P2 throughout the document.<br>• A note is added for named.pcy file. Refer to "Policies for SNMP Plugin" (p. 8-30). |
| 7 | June 2011 | Build 9 | • LDNS00001444 ia added to Table , "Known vendor issues" (p. 6-4).<br>• A note is added to "Supported platforms" (p. 7-2). |
| 7 | June 2011 | Build 9 | • Security fixes are included for CERT Advisories VU#795694.<br>• LDNS00002290 is fixed. Refer to "Resolved issues in Lucent DNS 5.1, Build 9" (p. 4-6).<br>• Upgraded the BIND variable version to 9.7.3-P1 throughout the document. |
| 6 | May 2011 | Build 8 | • LDNS00001725 is fixed. Refer to the last bullet point in step 5 of "UNIX installation" (p. 8-4). |
| 5 | March 2011 | Build 8 | • Upgraded the BIND variable version to 9.7.3 throughout the document. |
| 5 | March 2011 | Build 8 | • LDNS00001173 is fixed. Refer to "Configuring SNMP 3.0 on Solaris 10" (p. 8-13) |

| Issue Number | Date of issue | Version | Description of changes |
|---|---|---|---|
| 4 | January 2011 | Build 5 | • Configuring SNMP Traps is moved to common section. Refer to "Configuring SNMP Traps for all platforms" (p. 8-25) |
| 3 | December 2010 | Build 5 | • Added LDNS00001157 to resolved issues. Refer to "Resolved issues in Lucent DNS 5.1, Build 5" (p. 4-7).<br>• Updated configuring steps for SNMP 3.0. |
| 2 | December 2010 | Build 5 | • Updated the whole document for current build numbers, path and other changes. |
| 2 | December 2010 | Build 5 | • Security fixes are included for CERT Advisories VU#706148, VU#837744 and VU#510208. Refer to "Resolved issues in Lucent DNS 5.1, Build 5" (p. 4-7). |
| 1 | November 2010 | Build 4 | • Added 'recursion no' behavior to Known vendor Issues. Refer to "Known vendor issues" (p. 6-4) |
| 1 | November 2010 | Build 4 | • Added LDNS00001158 to Known issues. Refer to "Known issues and workarounds" (p. 6-2) |
| 1 | November 2010 | Build 4 | • IMR 908698 is fixed. Refer to "Shared libraries" (p. 8-3). |

## Conventions used

This document uses the following typographical conventions:

| Appearance | Description |
|---|---|
| *Italicized text* | • File and directory names<br>• Titles of publications<br>• A value that the user supplies |
| ***Bold italicized text*** | • Emphasized information |
| **graphic user interface text or key name** | • Text that is displayed in a graphical user interface or in a hardware label<br>• 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 |

| Appearance | Description |
|---|---|
| ***<input variable>*** | Input variable for which you must substitute another value. The angle brackets also indicate the value is a variable. |
| `output text` | Text that a system displays or prints |

## Related information

The following documents are referenced in these release notes:

- *VitalQIP Administrator Reference Manual* (part number: 190-409-042R7.3)

  This guide describes planning and configuring your network, information about the VitalQIP interface, advanced DNS and DHCP configurations, and troubleshooting.
- *VitalQIP Installation Guide* (part number: 190-409-043R7.3)

  This guide describes how to install the VitalQIP product.
- *VitalQIP Command Line Interface User's Guide* (part number: 190-409-044R7.3)

  This guide discusses and describes how to use the *VitalQIP Command Line Interface*.
- *VitalQIP Web Client User's Guide* (part number: 190-409-079R7.3)

  This guide describes how to use the web client interface.

## Technical support

If you need assistance with VitalQIP DNS, contact the Technical Assistance Center for your region. Contact information is provided in the following table..

| Phone | Email |
|---|---|
| 1. Go to http://alcatel-lucent.com/support/supportredirect.html.<br>2. Select your country. | support@alcatel-lucent.com |

## How to access

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

## 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 5.1 Build 46 is based on ISC BIND 9.7.7 and is compatible with VitalQIP 7.x and VitalQIP 8.x.

### Contents

This chapter covers these topics.

# Software deliverables

The following table lists the software that comprises the Lucent DNS 5.1 Build 46 release.

**Table 1-1 Software deliverables**

| Type | Platform | Directory | File |
|---|---|---|---|
| Lucent DNS Software | Linux | */vitalqip/LDNS/DNS5.1/Linux/DNS5.1B46-Linux* | *ldns5.1.46-linux-gcc3.tar* |
| | Solaris | */vitalqip/LDNS/DNS5.1/Solaris/DNS5.1B46-Solaris* | *ldns5.1.46-solaris.2x.tar* |
| | Solaris X86 | */vitalqip/LDNS/DNS5.1/Solaris-x86/DNS5.1B46-Solaris-x86* | *ldns5.1.46-solaris-x86.tar* |
| | Windows 2003/ Windows 2008 | */vitalqip/LDNS/DNS5.1/Windows/DNS5.1B46-Windows* | *ldns5.1.46-w2k.zip* |

**Note:** SNMP plugin (sub agent) is delivered along with DNS server software.

# How to obtain software

VitalQIP Lucent DNS 5.1 Build 46 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.alcatel-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.alcatel-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.alcatel-lucent.com/release/SPRegistrantTypeSvlt.

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

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

4 Click on **Customer Support** tab.

5 Click **Documentation and downloads**.

6 Click on **Product index.**

7 Click **V**.

8 Click on **VitalQIP®**.

**Note:** Although there is a **VitalQIP® DNS** link, it does not contain an electronic download entry. LDNS downloads are currently located under the **VitalQIP®** link.

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

10 Select **LDNS** and click **Next**.

11 Select **5.1** and click **Next**.

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

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

14 Specify the download directory on your local machine.

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

END OF STEPS

### Downloading Net-SNMP (Master agent)

**Table 1-2 Net-SNMP downloading locations**

| Type | Platform | Directory |
|---|---|---|
| Net-SNMP | Linux | http://net-snmp.sourceforge.net/download.html |
| | Solaris | http://sunfreeware.com |
| | Windows 2003/ Windows 2008 | http://www.net-snmp.org. |

**Note:** The above table gives the possible ways to get the SNMP master agent.

# Document deliverables

### Documentation available for this release

The following table lists the available documentation for the Lucent DNS 5.1 Build 46 release.

**Table 1-3 Documentation list**

| Document ID | Document title |
|---|---|
| 190-409-112R5.1 | VitalQIP DNS 5.1 Release Notes |

# To obtain documentation

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

To navigate OLCS, follow these steps:

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

# 2 New features

## Overview

### Purpose

The following sections identify the new features and/or capabilities contained in Lucent DNS 5.1.

### Contents

This chapter covers these topics.

# New feature

The following new feature is included in this release.

**Table 2-1 New features**

| Feature ID | Feature Name | Description |
|---|---|---|
| | Merge of ISC BIND 9.7.7 | The Lucent DNS server is based on BIND 9.7.7. |

# Lucent DNS directives

In common with previous versions, in Lucent DNS you can specify Lucent DNS-specific directives in a **qddns** block inside the **options** block in *named.conf*. Valid directives for the **qddns** block are as follows:

```
qddns {
    allow-secondary-update <boolean>;
    rrset-order <boolean>;
    unix-use-unbuffered-write-for-journal <boolean>;
    sync-journal-to-disk <boolean>;
    remove-cname-on-cname-and-other-data-error <boolean>;
    udp-socket-rcvbuf <integer>;
    retry-tcp-on-truncate <boolean>;
    client-edns <boolean>;
    snmp-stats <boolean>;
    edup {
       my-ip ( <ipv4_address> | <ipv6_address> );
       message-service-ip ( <ipv4_address> | <ipv6_address> );
       message-service-port <integer>;
       org-id <integer>;
       rr-types { <quoted_string>; ... };
       };
    gss-principal <quoted_string>
    max-rdataset-for-update <integer>;
    notify-after-load <boolean>;
    lock-isc-stats <boolean>;
    gss-max-contexts <integer>;
  };
```

The directives are described in the following table.

### Table 2-2 Lucent DNS directives

| Directive | Description |
|---|---|
| **`allow-secondary-update`** | The default value is **`yes`**. When the policy **`allow-secondary-update`** is set to **`yes`**, dynamic updates are allowed for slave zones. |
| **`rrset-order`** | The choices are:<br>• **`rrset-order "yes";`** (default)<br>• **`rrset-order "no";`**<br>When this directive is set to "no", no rrset-ordering is performed and the DNS server will return the set in the fixed order. If ISC's rrset-order is also specified, it will be ignored.<br>When this directive is set to "yes", the (BIND default) ordering is performed. However, if ISC's rrset-order is also specified, ISC's directive will have precedence.<br>**Note:** This directive can be set from the VitalQIP GUI with the **`RR Set Ordering`** Lucent DNS 4.x server parameter. Refer to "Lucent DNS 4.X server type", in Chapter 14 of the *VitalQIP Web Client User's Guide*. |
| **`unix-use-unbuffered-write-for-journal`** | ***Solaris only.*** The default value is **`no`**. On systems with a Solaris 2.8 C library only, **`named`** goes into an infinite loop while writing journal files. To work around this problem, set **`unix-use-unbuffered-write-for-journal`** to **`yes`**.<br>To make sure that the policy is in use, a debug level 10 message similar to the following is written to the log when a dynamic update is sent to **`named`**:<br>`Using write() instead of fwrite() as specified by policy`<br>**Important!** Only set this policy if the following conditions exist:<br>• **`named`** is running on Solaris 2.8<br>• **`named`** does not answer to any queries or zone transfers<br>• The CPU spikes to 100% for the **`named`** process<br>• After you have run **`pstack`** with the pid of **`named`** a few times, you consistently notice the following segment: |

```
ff18f638 _flsbuf (0, 482f38, 0, ff19a074, 0, 0) + 24

     ff193bf4 _fwrite_unlocked (ff1bfc28, 1, c, 482f38, ff0f14ad, 1) + 420
     ff19377c fwrite    (c, ff1c3a54, ff1bff48, 482f38, 1, ff0f14a8) + 88
     003433e4 isc_stdio_write (ff0f14a8, 1, c, 482f38, 0, 4b9bb34) + 44
     00102c38 journal_write (20a0460, ff0f14a8, c, 3759dc, 246, ff0f14b5) + 30
     0010473c dns_journal_begin_transaction (20a0460, 103b38, 1, 1, ff0f19ec, ff0f0124) + 184
     0010528c dns_journal_write_transaction (20a0460, ff0f1c14, 1, ff0f19ec, 4efd48, 40443c) + 44
     000b585c update_action (48f6d8, 24883d0, 48f6e0, 29720e8, 53a528, 0) + 2d64
     00325924 dispatch (489ee0, 0, 0, 0, 0, 0) + 614
     00325de4 run      (489ee0, ff1d5d38, 0, 5, 1, fe400000) + 14
     ff23b11c _thread_start (489ee0, 0, 0, 0, 0, 0) + 40
```

| Directive | Description |
|---|---|
| **sync-journal-to-disk** | The default value is **yes**. If **named** receives many dynamic updates in master zones or has many slave zones that are obtained via IXFR, **named** does not respond while syncing the journal files to disk. This is the default behavior of ISC code, which can be changed by setting **sync-journal-to-disk** to **no**. If the policy is set to **no**, **named** stops syncing the journal to disk with each write, and only flushes the buffer, which improves performance. |
| **remove-cname-on-cname-and-other-data-error** | The default value is **no**. When set to **yes**, if a CNAME and other data error is detected in a zone, the offending CNAME record is deleted and the zone loading continues. Additionally, an SNMP trap will be sent (if configured). |

| Directive | Description |
|---|---|
| **`udp-socket-rcvbuf`** | This policy can be used to increase the per-socket receive buffer size of UDP sockets bound to the interfaces. The default value of the UDP receive buffer size may be too small. If the system is fast and gets blasted with UDP queries, the buffer can get full and the queries will be lost.<br>Valid values are positive numeric integers. The default value is the system default. If the specified value is larger than the default, only then will an attempt be made to set it. If the specified value is too large, the value will be decremented until success. Since there is currently no suggested value, experiment with your system and set one. Remember that kernel sets memory aside for the buffer. This setting will apply to all query threads (default of one per CPU/core.)<br>If this policy is set to **`65535`**, information messages similar to the following will be written at startup:<br>`23-Jan-2009 14:18:39.706 Setting SO_RCVBUF of udp`<br>`socket 512 to 65535, Default is 32768`<br>`23-Jan-2009 14:18:39.706 +Successfully set SO_RCVBUF of`<br>`udp socket 512 to 65535`<br>`23-Jan-2009 14:18:39.706   Verifying... current value`<br>`of SO_RCVBUF is 65535`<br>`23-Jan-2009 14:18:39.710 listening on IPv4 interface`<br>`bge0, 10.100.30.50#53`<br>`23-Jan-2009 14:18:39.710 Setting SO_RCVBUF of udp`<br>`socket 513 to 65535, Default is 32768`<br>`23-Jan-2009 14:18:39.710 +Successfully set SO_RCVBUF of`<br>`udp socket 513 to 65535`<br>`23-Jan-2009 14:18:39.710   Verifying... current value`<br>`of SO_RCVBUF is 65535`<br>`23-Jan-2009 14:18:39.714 listening on IPv4 interface`<br>`bge1, 135.114.106.81#53`<br>`23-Jan-2009 14:18:39.714 Setting SO_RCVBUF of udp`<br>`socket 514 to 65535, Default is 32768`<br>`23-Jan-2009 14:18:39.714 +Successfully set SO_RCVBUF of`<br>`udp socket 514 to 65535`<br>`23-Jan-2009 14:18:39.714   Verifying... current value`<br>`of SO_RCVBUF is 65535` |

| Directive | Description |
|---|---|
| **`retry-tcp-on-truncate`** | The default value is **`yes`**. When the DNS server receives a query reply message and sees that the truncation bit is ON, according to DNS protocol, the DNS server retries the query by initiating a TCP connection with the same server. If TCP SYN is allowed to pass, but the ACK is blocked in the firewall, the TCP handshake cannot happen and many SYN_SENT half-open connections can be seen by running **`netstat`**. If too many requests arrive too fast, **`named`** runs out of file descriptors and cannot serve any requests.<br>If the policy **`retry-tcp-on-truncate`** is set to **`no`** in **`qddns`** block of the DNS server, query replies with the truncation bit set will not be retried using TCP. The DNS server accepts and continues with the partially received message. |
| **`client-edns`** | The default value is **`yes`**. This policy can be used to prevent the DNS server from sending EDNS with outgoing queries.<br>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. |
| **`snmp-stats`** | The default value is **`yes`**. If the policy **`snmp-stats`** is set to **`no`** in the **`qddns`** block, server statistics and zone maintenance statistics counters are not incremented for SNMP. It does not affect statistics counters obtained outside of SNMP. If queries are made via SNMP, all the **`dnsServCounters`** values will be zero. When this policy is on, the server and zone maintenance counter variables are incremented twice - once in ISC code(non-SNMP) and once in **`qddns`** code(for SNMP). |

| Directive | Description |
|---|---|
| **`edup`** | **`edup`** policies allow dynamic DNS updates to be sent back to VitalQIP. The following parameters can be specified:<br>• **`my-ip (`** ***`<IPv4 address>`*** **`)`** specifies the IPv4 address of the name server to use in the EDUP message.<br>• **`message-service-ip (`** ***`<IPv4 address>`*** **`)`** specifies the IPv4 address of the Message Service where the EDUP messages are sent.<br>• **`message-service-port`** ***`<integer>`*** specifies the Message Service port where the EDUP messages are sent.<br>• **`org-id`** ***`<integer>`*** specifies the Organization ID added to the EDUP message.<br>• **`rr-types {`** ***`<quoted string>; ...`*** **`};`** specifies the resource records for which it generate EDUP messages back to VitalQIP. These messages can only be generated from the dynamic updates of the types specified in this directive. Supported types are A, AAAA, CNAME, PTR, SRV, and TXT.<br>**Note:** The other rr-types are supported by server but they are not supported in the GUI. |

| Directive | Description |
|---|---|
| **`gss-principal`** | In versions of VitalQIP prior to VitalQIP 7.2 PR1, support for secure DNS updates required that this policy be used to specify the server principal name in **`'DNS@`*`<server name>.<domain>`*`'`** format.<br>In Lucent DNS 5.0, **`gss-principal`** is still available but, converted to **`tkey-gssapi-credential`** and *named* prints information messages similar to the following at startup:<br>`10-Apr-2009 13:18:46.901 converted gss-principal 'DNS@spirit.quadritek.lucent.com' to Kerberos 5 syntax 'DNS/spirit.quadritek.lucent.com'`<br>`...`<br>`10-Apr-2009 13:18:46.962 converting qddns gss-principal to ISC's tkey-gssapi-credential`<br>If *named.conf* has both **`gss-tsig`** and **`tkey-gssapi-credential`** defined, **`gss-principal`** takes precedence over **`tkey-gssapi-credential`**.<br>**Note:** In previous implementations of GSS-TSIG, setting the server principal name to **`yes`** caused the Lucent DNS server to determine its own principal name. In Lucent DNS 5.1, however, if **`gss-principal`** is set to **`yes`** or **`no`**, it is silently ignored. If **`gss-principal`** contains any other text string, it is used to make an attempt to acquire credentials. |
| **`max-rdataset-for-update`** | This policy can be used to prevent dynamic updates that will cause the server to consume large amounts of memory and potentially cause the server to be unusable. This can happen when a dynamic update with a different TTL is added to a large RRset.<br>Valid values are positive integers. The default is 500. A value of 0 is unlimited, which is ***not*** recommended. If the policy is enforced, warning type messages will be written to the log:<br>`Dynamic update refused, #RRs in RDATASET is 501, > 500 set by qddns policy max-rdataset-for-update` |

| Directive | Description |
|---|---|
| **`notify-after-load`** | The default value is **`no`**. The Lucent DNS server does not send notifies to slaves after startup. The ISC server's default behavior after startup, however, is to send notify messages to slave servers. Set this policy to **`yes`** if the ISC server's behavior is desired. |
| **`lock-isc-stats`** | The default value is **`no`**. ISC does not lock statistics counters in multi-core Solaris and Windows systems and as a result, the statistics counters on those systems may show slightly incorrect values and do not match Alcatel-Lucent SNMP counters. Set to **`yes`** for correct values in ISC's statistics counters. |
| **`gss-max-contexts`** | This policy can be used to specify a maximum number of GSS contexts with **`gss-max-contexts`** in the **`qddns`** block in the **`options`** section. When the maximum number of contexts are reached, all the old contexts will be freed and *named* will use the already freed memory. The default value of the max contexts is 5000.<br>The maximum allowable value for **`gss-max-contexts`** is a signed 32 bit integer (2147483647). Do not use a larger value or the context will become negative and dynamic updates will be rejected. |

# SNMP support

## Overview

### Purpose

The Lucent DNS 5.1 server supports the SNMP plugins that are compiled with Net-SNMP SDK v5.4.2.1. (http://www.net-snmp.org/)

## SNMP statistics counters support

In Lucent DNS 5.1, BIND 9.7 server and zone maintenance statistics are exposed via SNMP. All previously used counters have been replaced with those described in the following table.

**Note:** If you do not wish to expose the counters via SNMP, use the policy **`snmp-stats no`** in the **`qddns`** block. Setting **`snmp-stats`** to **`no`** does not disable SNMP, but shows the value of the counters as zero when queried via SNMP. Additionally, there is a slight performance improvement since the counter function is not called.

The following table describes the supported counters.

**Table 2-3 Statistics counters**

| MIB variable | OID | Description |
|---|---|---|
| dnsServCounterRequestv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.1.0 | IPv4 requests received. This also counts non query requests |
| dnsServCounterRequestv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.2.0 | IPv6 requests received. This also counts non query requests |
| dnsServCounterReqEdns0 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.3.0 | Requests with EDNS(0) received |
| dnsServCounterReqBadEDNSVer | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.4.0 | Requests with unsupported EDNS version received |
| dnsServCounterReqTSIG | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.5.0 | Requests with TSIG received |
| dnsServCounterReqSIG0 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.6.0 | Requests with SIG(0) received |
| dnsServCounterReqBadSIG | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.7.0 | Requests with invalid (TSIG or SIG(0)) signature received |

| MIB variable | OID | Description |
|---|---|---|
| dnsServCounterReqTCP | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.8.0 | TCP requests received |
| dnsServCounterAuthQryRej | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.9.0 | Authoritative (non recursive) queries rejected |
| dnsServCounterRecQryRej | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.10.0 | Recursive queries rejected |
| dnsServCounterXfrRej | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.11.0 | Zone transfer requests rejected |
| dnsServCounterUpdateRej | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.12.0 | Dynamic update requests rejected |
| dnsServCounterResponse | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.13.0 | Responses sent |
| dnsServCounterTruncatedResp | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.14.0 | Truncated responses sent |
| dnsServCounterRespEDNS0 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.15.0 | Responses with EDNS(0) sent |
| dnsServCounterRespTSIG | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.16.0 | Responses with TSIG sent |
| dnsServCounterRespSIG0 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.17.0 | Responses with SIG(0) sent |
| dnsServCounterQrySuccess | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.18.0 | Queries resulted in successful answer. This means the query which returns a NOERROR response with at least one answer RR |
| dnsServCounterQryAuthAns | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.19.0 | Queries resulted in authoritative answer |
| dnsServCounterQryNoauthAns | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.20.0 | Queries resulted in non authoritative answer |
| dnsServCounterQryReferral | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.21.0 | Queries resulted in referral answer |
| dnsServCounterQryNxrrset | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.22.0 | Queries resulted in in NOERROR responses with no data |
| dnsServCounterQrySERVFAIL | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.23.0 | Queries resulted in SERVFAIL |
| dnsServCounterQryFORMERR | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.24.0 | Queries resulted in FORMERR |

| MIB variable | OID | Description |
|---|---|---|
| dnsServCounterQryNXDOMAIN | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.25.0 | Queries resulted in NXDOMAIN |
| dnsServCounterQryRecursion | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.26.0 | Queries which caused the server to perform recursion in order to find the final answer |
| dnsServCounterQryDuplicate | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.27.0 | Queries which the server attempted to recurse but discovered an existing query with the same IP address, port, query ID, name, type and class already being processed |
| dnsServCounterQryDropped | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.28.0 | Queries for which the server discovered an excessive number of existing recursive queries for the same name, type and class and were subsequently dropped |
| dnsServCounterQryFailure | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.29.0 | Other query failures |
| dnsServCounterXfrReqDone | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.30.0 | Requested zone transfers completed |
| dnsServCounterUpdateReqFwd | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.31.0 | Dynamic update requests forwarded |
| dnsServCounterUpdateRespFwd | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.32.0 | Dynamic update responses forwarded |
| dnsServCounterUpdateFwdFail | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.33.0 | Dynamic update forward failed |
| dnsServCounterUpdateDone | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.34.0 | Dynamic updates completed |
| dnsServCounterUpdateFail | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.35.0 | Dynamic updates failed |
| dnsServCounterUpdateBadPrereq | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.36.0 | Dynamic updates rejected due to prerequisite failure |
| dnsServCounterZoneMaintNotifyOutv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.37.0 | IPv4 notifies sent |
| dnsServCounterZoneMaintNotifyOutv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.38.0 | IPv6 notifies sent |
| dnsServCounterZoneMaintNotifyInv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.39.0 | IPv4 notifies received |

| MIB variable | OID | Description |
|---|---|---|
| dnsServCounterZoneMaintNotifyInv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.40.0 | IPv6 notifies received |
| dnsServCounterZoneMaintNotifyRej | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.41.0 | Incoming notifies rejected |
| dnsServCounterZoneMaintSOAOutv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.42.0 | IPv4 SOA queries sent |
| dnsServCounterZoneMaintSOAOutv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.43.0 | IPv6 SOA queries sent |
| dnsServCounterZoneMaintAXFRReqv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.44.0 | IPv4 AXFR requested |
| dnsServCounterZoneMaintAXFRReqv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.45.0 | IPv6 AXFR requested |
| dnsServCounterZoneMaintIXFRReqv4 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.46.0 | IPv4 IXFR requested |
| dnsServCounterZoneMaintIXFRReqv6 | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.47.0 | IPv6 IXFR requested |
| dnsServCounterZoneMaintXfrSuccess | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.48.0 | Zone transfer requests succeeded |
| dnsServCounterZoneMaintXfrFail | 1.3.6.1.4.1.1751.1.48.1.2.2.1.2.49.0 | Zone transfer requests failed |

# Configuration policy values

The following table describes the new **qddns** policies that can be inspected via SNMP:

**Note:** In Lucent DNS 5.1, the configuration variables **dnsServConfigRecurs** and **dnsServConfigRoundRobin** are removed.

**Table 2-4 SNMP MIB variables for qddns policies**

| Policy | SNMP MIB variable | OID |
|---|---|---|
| snmp-stats | dnsServConfigQddnsSnmpStats | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.3.0 |
| retry-tcp-on-truncate | dnsServConfigQddnsRetryTcpOnTruncate | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.4.0 |
| client-edns | dnsServConfigQddnsClientEdns | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.5.0 |
| sync-journal-to-disk | dnsServConfigQddnsSyncJournalToDisk | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.6.0 |
| allow-secondary-update | dnsServConfigQddnsAllowSecondaryUpdate | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.7.0 |
| notify-after-load | dnsServConfigQddnsNotifyAfterLoad | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.8.0 |
| my-ip | dnsServConfigQddnsEdupMyIP | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.9.0 |
| message-service-ip | dnsServConfigQddnsEdupMessageServiceIP | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.10.0 |
| message-service-port | dnsServConfigQddnsEdupMessageServicePort | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.11.0 |

| Policy | SNMP MIB variable | OID |
|---|---|---|
| org-id | dnsServConfigQddnsEdupOrgId | 1.3.6.1.4.1.1751.1.48.1.2.2.1.4.12.0 |

# Query types

Lucent DNS 5.1 supports the following query types and hence are supported by the SNMP Module.

> **Note:** BIND 9 understands the RESERVED query types (31,32,34,100,101,102) but there is no code to support them and no way to send a query of those types using **`dig`** or any other BIND 9 tools.

**Table 2-5 Query types**

| Type Code | Name | Type Code | Name |
|---|---|---|---|
| 1 | A | 33 | SRV |
| 2 | NS | 34 | ATMA (RESERVED) |
| 3 | MD | 35 | NAPTR |
| 4 | MF | 36 | KX |
| 5 | CNAME | 37 | CERT |
| 6 | SOA | 38 | A6 |
| 7 | MB | 39 | DNAME |
| 8 | MG | 40 | NOT USED |
| 9 | MR | 41 | OPT |
| 10 | NULL | 42 | APL |
| 11 | WKS | 43 | DS |
| 12 | PTR | 44 | SSHFP |
| 13 | HINFO | 45 | IPSECKEY |
| 14 | MINFO | 46 | RRSIG |
| 15 | MX | 47 | NSEC |
| 16 | TXT | 48 | DNSKEY |
| 17 | RP | 49 | DHCID |
| 18 | AFSDB | 50-98 | NOT USED |

| Type Code | Name | Type Code | Name |
|---|---|---|---|
| 19 | X25 | 99 | SPF |
| 20 | ISDN | 100 | UINFO (RESERVED) |
| 21 | RT | 101 | UID (RESERVED) |
| 22 | NSAP | 102 | GID (RESERVED) |
| 23 | NSAP-PTR | 103 | UNSPEC |
| 24 | SIG | 104-248 | NOT USED |
| 25 | KEY | 249 | TKEY |
| 26 | PX | 250 | TSIG |
| 27 | GPOS | 251 | IXFR |
| 28 | AAAA | 252 | AXFR |
| 29 | LOC | 253 | MAILB |
| 30 | NXT | 254 | MAILA |
| 31 | EID (RESERVED) | 255 | ANY |
| 32 | NIMLOC (RESERVED) | 256* | DLV |

* 256 is the value of **`dnsServCounterQType`** index in the dnsServCounterTable MIB object. The query type used by BIND 9 is 32769, which means that if a DLV type query arrives, Lucent DNS maps 32769 to 256 for SNMP.

# Lucent DNS MIB variables

Alcatel-Lucent has modified the Lucent DNS server on all supported platforms to support SNMP. Some of the statistical information gathered by the DNS server through normal operations can be accessed through the Alcatel-Lucent MIB variables.

Alcatel-Lucent has implemented portions of the DNS MIB objects defined by RFC 1611 (DNS Server MIB Extensions) and many of the ISC BIND statistics counters. The DNS server MIB variables are categorically grouped in the following table. Refer to Table 2-6 for description of each MIB variable.

**Table 2-6 Summary of SNMP MIB variables for the Lucent DNS server**

| Function | MIB Variable(s) | Description |
|---|---|---|
| **System information:** | | |
| Server information | *dnsServSystemDescr* | Provides a textual description of the server. This value includes the full name and version identification of the server.<br>**Example:** *`QDDNS 5.1 build 46`* |
| Server Status | *dnsServSystemStatus* | The current status of the server:<br>• 1 – Some other state that is not listed in 2–4<br>• 2 – The service is being reset<br>• 3 – The service is initializing<br>• 4 – The service is running<br>**Note:** Once the server has been completely stopped, no status can be returned from this variable. |
| Number of seconds since service was started | *dnsServConfigUpTime* | If the server has a persistent state (for example, a process), this value will be the time elapsed (in seconds) since it started. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Number of seconds since service was last reset (config files were re-read) | *dnsServConfigResetTime* | This value is the time elapsed (in seconds) since the last time the name server was "reset".<br>**Note:** This counter can be re-setted using rndc commands **`reconfig, reload`** and **`qddns-push`**. However if a zone name is passed as an argument for **`reload`** and **`qddns-push`** commands, it will not get reset. |
| **Counter information by OP Code/class/resource record type:** | | |
| | *dnsServCounterEntry ::=*<br>*SEQUENCE {*<br>*dnsServCounterOpCode,*<br>*dnsServCounterQClass,*<br>*dnsServCounterQType,*<br>*dnsServCounterTransport,*<br>*dnsServCounterRequests,*<br>*dnsServCounterResponses*<br>*}* | Note that a table is provided that will allow request and response information counters to be accessed by OpCode, Class, Type, and Transport. |
| The DNS OP Code of this table entry | *dnsServCounterOpCode* | The DNS OP Code being counted in this row of the table:<br>• 0 – A standard query (QUERY)<br>• 4 - A notify (NOTIFY)<br>• 5 - A dynamic update (UPDATE)<br>Not common for direct access, but these values are defined and used in *dnsServCounterRequests* and *dnsServCounterResponses* requests. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| The DNS Class of this table entry | *dnsServCounterQClass* | The class of record being counted in this row of the table.<br>• 1 – 'IN' the Internet<br>• 3 – 'CH' the CHAOS class<br>Not common for direct access, but these values are defined and used in *dnsServCounterRequests* and *dnsServCounterResponses* requests. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| The DNS Record Type of this table entry | *dnsServCounterQType* | |

| Function | MIB Variable(s) | Description |
|---|---|---|
|  | 1 – Host address (A)<br>2 – Authoritative server (NS)<br>3 – Mail destination (MD)<br>4 – Mail forwarder (MF)<br>5 – Canonical name (CNAME)<br>6 – Start of authority zone (SOA)<br>7 – Mailbox domain name (MB)<br>8 – Mail group member (MG)<br>9 – Mail rename name (MR)<br>10 – Null resource record (NULL)<br>11 – Well known service (WKS)<br>12 – Domain name pointer (PTR)<br>13 – Host information (HINFO)<br>14 – Mailbox information (MWFO)<br>15 – Mail routing information (MX)<br>16 – Text strings (TXT)<br>17 – Responsible person (RP)<br>18 – AFS cell database (AFSDB)<br>19 – X_25 calling address (X25)<br>20 – ISDN calling address (ISDN)<br>21 – Router (RT)<br>22 – NSAP address (NSAP)<br>23 – Reverse NSAP lookup (deprecated) (NSAP-PTR)<br>24 – Security signature (SIG)<br>25 – Security key (KEY)<br>26 – X.400 mail mapping (PX))<br>27 – Geographical position (withdrawn) (GPOS) | 28 – Ip6 Address (AAAA)<br>29 – Location Information (LOC)<br>30 – Next domain (security) (NXT)<br>31 – Endpoint identifier (EID)<br>32 – Nimrod Locator (NIMLOC)<br>33 – Server Selection (SRV)<br>34 – ATM Address (ATMA)<br>35 – Naming Authority Pointer (NAPTR)<br>36 - Key Exchanger (KX)<br>37 - Certificate (CERT)<br>38 - IPv6 Host Address (A6)<br>39 - Name Redirection (DNAME)<br>40 - Kitchen Sink (SINK)<br>41 - EDNS0 Option (OPT)<br>42 - Lists of Address Prefixes (APL)<br>43- Delegation Signer (DS)<br>44 - SSH Key Fingerprint (SSHFP)<br>45 - IPSECKEY<br>46 - Resource Redord Signature (RRSIG)<br>47 - Next Secure (NSEC)<br>48 - DNS Public Key (DNSKEY)<br>49 - DHCP Identifier (DHCID)<br>99 - Sender Policy Framework (SPF)<br>100 - UINFO<br>101 - UID |

| Function | MIB Variable(s) | Description |
|---|---|---|
| | | 102 - GID<br>103 - UNSPEC<br>249 - Transaction Key(TKEY)<br>250 - Transition Signature - (TSIG)<br>251 - Incremental Transfer - (IXFR)<br>252 – A request for a transfer of an entire zone (AXFR)<br>253 – A request for mailbox-related records (MAILB, MB, MG, or MR)<br>254 – A request for mail agent RRs (MAILA (Obsolete—see MX)<br>255 – A request for any records (ANY)<br>256 - DNSSEC Look aside validation (DLV) |
| The transport layer used for the records of this table entry | *dnsServCounterTransport* | The transport that was used for these queries.<br>• 1 – The queries reported on this row were sent using UDP.<br>• 2 – The queries reported on this row were sent using TCP.<br>• 3 – The queries reported on this row were sent using a transport that was neither TCP nor UDP. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Number of queries that have been recorded in this table entry | *dnsServCounterRequests* | Number of requests that have been recorded in this row of the table. The counter information is accessed as follows: **dnsServCounter Requests.*<opcode>*. *<class>*.*<type>*. *<transport>***<br>The count of requested queries for IN A records over UDP by the server would be: **dnsServCounterRequest s.query.in.a.udp** or **dnsServCounter Requests.0.1.1.1**. See also "Counter information by OP Code/class/resource record type" (p. 2-17). * |
| Number of responses that have been recorded in this table entry | *dnsServCounterResponses* | Number of responses made by the server since initialization for the kind of response identified on this row of the table. The counter information is accessed as follows: **dnsServCounter Responses.*<opcode>*. *<class>*.*<type>*. *<transport>***<br>The count of query responses for IN A records over UDP by the server would be: **dnsServCounterRequest s.query.in.a.udp** or **dnsServCounter Responses.0.1.1.1**. See also "Counter information by OP Code/class/resource record type" (p. 2-17). * |
| IPv4 requests received | *dnsServCounterRequestv4* | IPv4 requests received. This also counts non-query requests. |
| IPv6 requests received | *dnsServCounterRequestv6* | IPv6 requests received. This also counts non-query requests. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Requests with EDNS(0) received | *dnsServCounterReqEdns0* | Requests with EDNS(0) received. |
| Requests with unsupported EDNS version received | *dnsServCounterReqBadEDNSVer* | Requests with unsupported EDNS version received. |
| Requests with TSIG received | *dnsServCounterReqTSIG* | Requests with TSIG received. |
| Requests with SIG(0) received | *dnsServCounterReqSIG0* | Requests with SIG(0) received. |
| Requests with invalid TSIG or SIG(0) signature received | *dnsServCounterReqBadSIG* | Requests with invalid TSIG or SIG(0) signature received. |
| TCP requests received | *dnsServCounterReqTCP* | TCP requests received. |
| Authoritative (non-recursive) queries rejected. | *dnsServCounterAuthQryRej* | Authoritative (non-recursive) queries rejected. |
| Recursive queries rejected | dnsServCounterRecQryRej | Recursive queries rejected. |
| Zone transfer requests rejected | *dnsServCounterXfrRej* | Zone transfer requests rejected. |
| Dynamic update requests rejected | *dnsServCounterUpdateRej* | Dynamic update requests rejected. |
| Responses sent | *dnsServCounterResponse* | Responses sent. |
| Truncated responses sent | *dnsServCounterTruncatedResp* | Truncated responses sent |
| Responses with EDNS(0) sent | *dnsServCounterRespEDNS0* | Responses with EDNS(0) sent. |
| Responses with TSIG sent | *dnsServCounterRespTSIG* | Responses with TSIG sent. |
| Responses with SIG(0) sent | *dnsServCounterRespSIG0* | Responses with SIG(0) sent. |
| Queries resulted in successful answer. | *dnsServCounterQrySuccess* | Queries resulted in successful answer. This means the query which returns a NOERROR response with at least one answer resource record. |
| Queries resulted in authoritative answer | *dnsServCounterQryAuthAns* | Queries resulted in authoritative answer. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Queries resulted in non-authoritative answer | *dnsServCounterQryNoauthAns* | Queries resulted in non-authoritative answer. |
| Queries resulted in referral answer | *dnsServCounterQryReferral* | Queries resulted in referral answer. |
| Queries resulted in in NOERROR responses | *nsServCounterQryNxrrset* | Queries resulted in in NOERROR responses with no data |
| Queries resulted in SERVFAIL | *dnsServCounterQrySERVFAIL* | Queries resulted in SERVFAIL. |
| Queries resulted in FORMERR | *dnsServCounterQryFORMERR* | Queries resulted in FORMERR. |
| Queries resulted in NXDOMAIN | *dnsServCounterQryNXDOMAIN* | Queries resulted in NXDOMAIN. |
| Queries which caused the server to perform recursion | *dnsServCounterQryRecursion* | Queries which caused the server to perform recursion in order to find the final answer. |
| Queries which the server attempted to recurse | *dnsServCounterQryDuplicate* | Queries which the server attempted to recurse but discovered an existing query with the same IP address, port, query ID, name, type and class already being processed. |
| Queries for which the server discovered an excessive number of existing recursive queries | *dnsServCounterQryDropped* | Queries for which the server discovered an excessive number of existing recursive queries for the same name, type and class and were subsequently dropped. |
| Other query failures | *dnsServCounterQryFailure* | Other query failures. |
| Requested zone transfers completed | *dnsServCounterXfrReqDone* | Requested zone transfers completed. |
| Dynamic update requests forwarded | *dnsServCounterUpdateReqFwd* | Dynamic update requests forwarded. |
| Dynamic update responses forwarded | *dnsServCounterUpdateRespFwd* | Dynamic update responses forwarded. |
| Dynamic update forward failed | *dnsServCounterUpdateFwdFail* | Dynamic update forward failed. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Dynamic updates completed | *dnsServCounterUpdateDone* | Dynamic updates completed. |
| Dynamic updates failed | *dnsServCounterUpdateFail* | Dynamic updates failed. |
| Dynamic updates prerequisite failed | *dnsServCounterUpdateBadPrereq* | Dynamic updates rejected due to prerequisite failure. |
| IPv4 notifies sent | *dnsServCounterZoneMaintNotifyOutv4* | IPv4 notifies sent. |
| IPv6 notifies sent | *dnsServCounterZoneMaintNotifyOutv6* | IPv6 notifies sent. |
| IPv4 notifies received | *dnsServCounterZoneMaintNotifyInv4* | IPv4 notifies received. |
| IPv6 notifies received | *dnsServCounterZoneMaintNotifyInv6* | IPv6 notifies received. |
| Incoming notifies rejected | *dnsServCounterZoneMaintNotifyRej* | Incoming notifies rejected. |
| IPv4 SOA queries sent | *dnsServCounterZoneMaintSOAOutv4* | IPv4 SOA queries sent. |
| IPv6 SOA queries sent | *dnsServCounterZoneMaintSOAOutv6* | IPv6 SOA queries sent. |
| IPv4 AXFR requested | *dnsServCounterZoneMaintAXFRReqv4* | IPv4 AXFR requested. |
| IPv6 AXFR requested | *dnsServCounterZoneMaintAXFRReqv6* | IPv6 AXFR requested. |
| IPv4 IXFR requested | *dnsServCounterZoneMaintIXFRReqv4* | IPv4 IXFR requested. |
| IPv6 IXFR requested | *dnsServCounterZoneMaintIXFRReqv6* | IPv6 IXFR requested. |
| Zone transfer requests succeeded | *dnsServCounterZoneMaintXfrSuccess* | Zone transfer requests succeeded. |
| Zone transfer requests failed | *dnsServCounterZoneMaintXfrFail* | Zone transfer requests failed. |
| **Performance/statistic counters by server:** | | |
| Minimum amount of time between receiving two DNS requests | *dnsServStatMinArrivalInterval* | The minimum amount of time between receiving two DNS request messages. A message is received at the server when the server is able to begin processing the message. This typically occurs immediately after the message is read into server memory. If no messages have been received or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Maximum amount of time between receiving two DNS requests | *dnsServStatMaxArrivalInterval* | The maximum amount of time between receiving two DNS request messages.  A message is received at the server when the server is able to begin processing the message.  This typically occurs immediately after the message is read into server memory.  If no messages have been received, this object contains a zero value.  The value is in milliseconds. |
| Number of seconds since the last DNS request was received | *dnsServStatLastArrivalTime* | The number of seconds since the last valid DNS request message was received by the server. Invalid messages do not cause this value to change.  If no valid messages have been received, this object contains a zero value. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Minimum response time to authoritative DNS requests | *dnsServStatAuthMinResponseTime* | The smallest time interval measured as the difference between the arrival of a DNS message at the server and the successful transmission of an authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Maximum response time to authoritative DNS requests | *dnsServStatAuthMaxResponseTime* | The largest time interval measured as the difference between the arrival of a DNS message at the server and the successful transmission of an authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Sum of the response times for authoritative DNS requests | *dnsServStatAuthSumResponseTime* | The sum of the response time intervals (in milliseconds), where a response time interval is measured as the difference between the arrival of a DNS message at the server and the successful transmission of an authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Minimum response time to non-authoritative DNS requests | *dnsServStatNonAuthMinResponseTime* | The smallest time interval measured as the difference between the arrival of a DNS message at the server and the successful transmission of a non-authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received or the interval is less than 1 ms, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Maximum response time to non-authoritative DNS requests | *dnsServStatNonAuthMaxResponseTime* | The largest time interval measured as the difference between the arrival of a DNS message at the server and the successful transmission of a non-authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Sum of the response times for non-authoritative DNS requests | *dnsServStatNonAuthSumResponseTime* | The sum of the response time intervals (in milliseconds), where a response time interval is measured as the difference between the arrival of a DNS message at the server and the successful transmission of an non-authoritative response to that message. A message is received at the server when the server is able to begin processing the message. A message is transmitted after the server has no further use for the message. Note that the operating system may still have the message queued internally. The operating system queue time is not to be considered as part of the response time. Invalid messages do not cause this value to change. If no valid messages have been received, this object contains a zero value. The value is in milliseconds. |
| **Configuration and settings:** | | |
| Seconds elapsed when the server is in a persistent state | *dnsServConfigUpTime* | If the server has a persistent state (for instance, a process), this value is the seconds elapsed since it started. For software without persistent state, this value is zero. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Seconds elapsed since the last time the name server was reset. | *dnsServConfigResetTime* | If the server has a persistent state (for instance, a process) and supports a reset operation (for instance, can be told to re-read configuration files), this value is the seconds elapsed since the last time the name server was reset. For software that does not have persistence state or does not support a reset operation, this value is zero.<br>**Note:** This counter can be re-set using rndc commands **`reconfig, reload`** and **`qddns-push`**. However if a zone name is passed as an argument for **`reload`** and **`qddns-push`** commands, it will not get reset. |
| Server statistics and zone maintenance statistics are not counted | *dnsServConfigQddnsSnmpStats* | If the policy **`snmp-stats`** is set to **`no`** in the **`qddns`** block, server statistics and zone maintenance statistics are not counted. All dnsServCounters values are set to zero. The default value for this policy is **`yes`**. When this policy is on, the server and zone maintenance counter variables are incremented twice - once for ISC statistics, and once fro SNMP statistics. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Finds the authoritative name server for that zone and sends a query in UDP | *dnsServConfigQddnsRetryTcpOnTruncate* | When a query is sent to a DNS server, it finds the authoritative name server for that zone and sends a query in UDP. If the reply from the recipient authoritative name server is more than 512 bytes, it sends a maximum of 512 bytes of data and also sets **`truncation bit`** in the message to the DNS server. When the DNS server receives the reply message from authoritative server, and the DNS server sees that the truncation bit is ON, according to DNS protocol, the DNS server initiates a TCP connection with the authoritative server to retry the query and obtain the full response data. If TCP is blocked in the firewall, TCP handshake cannot happen and many SYN_SENT half open connections can be seen by running **`netstat`**. If too many requests arrive too fast, **`named`** runs out of file descriptors and are not able to serve any requests. If the policy **`retry-tcp-on-truncate`** can be set to **`no`** in **`qddns`** block of the DNS server, the server will not attempt to connect to the authoritative server using TCP. The DNS server replies with the partial response data if any received. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| Turn off EDNS globally when the name server sends query to a remote name server as a client. | *dnsServConfigQddnsClientEdns* | A policy **`client-edns no`** can be specified in the **`qddn`**s block to turn off EDNS globally when the name server sends query to a remote name server as a client. If **`client-edns`** is set **`no`**, the per-server configuration with the server directive is ignored. The default value for **`client-edns`** is **`yes`**. The server acts like an ISC server. |
| Turn off syncing the journal files to disk. | *dnsServConfigQddnsSyncJournalToDisk* | If named receives many dynamic updates in master zones or has many slave zones which are obtained via IXFR, **`named`** does not respond while syncing the journal files to disk. This is the default behavior of ISC code. This default behavior can be changed with a new policy **`sync-journal-to-disk no;`** in the **`qddns`** block, which stops syncing the journal file to disk. Instead, just flushes the buffer. |
| Allow dynamic updates to slave zones | *dnsServConfigQddnsAllowSecondaryUpdate* | If the policy **`allow-secondary-update`** is set to **`yes`**, dynamic updates can be accepted in slave zones. The default value is **`yes`**. |
| Send notify messages to slaves zones | *dnsServConfigQddnsNotifyAfterLoad* | After start up, **`named`** sends notify messages to slaves zones. To avoid notify message overload, the default behavior is to not send notify messages at start up. The policy **`notify-after-load`** can be set to **`yes`** if the default behavior is not desired. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| IP address of the DNS server to use in EDUP messages | *dnsServConfigQddnsEdupMyIP* | IP address of the DNS server to use in EDUP messages. |
| IP address of Message Service where the EDUP messages are sent | *dnsServConfigQddnsEdupMessageServiceIP* | IP address of the Message Service where the EDUP messages are sent. |
| Message service port where the EDUP messages are sent. | *dnsServConfigQddnsEdupMessageServicePort* | Message service port where the EDUP messages are sent. |
| Organization ID used in the EDUP message | *dnsServConfigQddnsEdupOrgId* | Organization ID used in the EDUP message. |
| **DNS server SNMP traps:** | | |
| The DNS Server has started | *dnsServerStarted* | Sent by the DNS server when it started. |
| The DNS Server has stopped | *dnsServerStopped* | Sent by the DNS server during a normal, smooth, shutdown. |
| The DNS server has reloaded its configuration | *dnsServerReload* | Sent by the DNS server when it has been reloaded.<br>**Note:** This counter can be resetted using rndc commands **`reconfig, reload`** and **`qddns-push`**. However if a zone name is passed as an argument for **`reload`** and **`qddns-push`** commands, it will not get resetted. |

| Function | MIB Variable(s) | Description |
|---|---|---|
| The DNS server has detected an error in its configuration files | *dnsServerConfigError* | Sent by the DNS server when an error occurred while processing the DNS zone files.  This trap will be generated only if the following errors occur:<br>The server cannot find a file or directory that has been specified in the configuration.<br>The server has rejected a zone that it is trying to load, due to errors.<br>This trap is also sent if the qddns policy **remove-cname-on-cname-and-other-data-error** is set to **Yes**. In that case, the trap message will be CNAME and other data error, removing CNAME: (xyz). |
| The DNS has dumped its database to disk | *dnsServerDumped* | Sent by the DNS server when the DNS database files have been dumped to disk. |

# Trap object IDs (OIDs)

## Purpose

This section describes the components that comprise an SNMP trap. The Alcatel-Lucent enterprise-specific trap contents are defined by the following:

- DNS: **`VitalqipDnsTrapEntry`**

Similar trap variables are defined for DNS, as shown in the following table.

### Table 2-7 Trap variables

| vitalqipDnsTrapEntry in qddns.mib | Type | Description |
|---|---|---|
| vitalqipDnsTrIndex | Integer | Indicates which trap is received for *qddns.mib*:<br>1 = dnsServerStarted<br>2 = dnsServerStopped<br>3 = dnsServerReload<br>4 = dnsServerConfigError<br>5 = dnsServerDumped<br>For a description of the DNS traps, refer to the **DNS server SNMP traps** category at the end of Table 2-6. |
| vitalqipDnsTrSequence | Counter | Indicates how many times a specific trap is received. This number is a counter that will increment every time a specific trap is received. Such counters are only reset by DNS Starts or by a DNS Restart. |
| vitalqipDnsTrId | Integer | Indicates the application that generated the alarm. Currently, all traps are generated by the Monitor. The value is always 1. |
| vitalqipDnsTrText | 80-char string | An ASCII string describing the alarm condition/cause, for example:<br>`Lucent DNS stopped`<br>`Lucent DNS started` |

| vitalqipDnsTrapEntry in qddns.mib | Type | Description |
|---|---|---|
| vitalqipDnsTrPriority | Integer | Indicates the priority level as set on the agent for this class and type of trap. The DNS server send traps with the following priorities:<br>1 (inform) for start, stop, reload, failover returned control, subnet threshold descended, and ping response received.<br>2 (warning) a bad packet is received. Used when there are errors in the config file and when *qddns* finds CNAME and other data error in a zone or a file.<br>3 (minor) when a subnet threshold is exceeded.<br>4 (major) when a subnet is depleted.<br>5 (critical) when a failover is activated. |
| vitalqipDnsTrClass | Integer | This is not used and is set to the value of **vitalqipDnsTrIndex** (DNS). |
| vitalqipDnsTrType | Integer | This is not used and is set to the value of **vitalqipDnsTrIndex** (DNS). |
| vitalqipDnsTrTime | Counter | Indicates the time when the trap has occurred. It contains the number of seconds since UNIX epoch (midnight UTC of January 1, 1970). For example, the local time of the sub-agent host is:<br>1238788125 (which translates to Fri Apr 3 15:48:45 2009) |
| vitalqipDnsTrSuspect | 32-char string | The hostname where the sub-agent (*named*) is running. |
| vitalqipDnsTrDiagId | Integer | This is not used and is set to the value of **vitalqipDnsTrIndex** (DNS). |
| vitalqipDnsTrIteration | Integer | Indicates the total number of traps sent so far. |

### Sample DNS traps vitalqip

The following is the sample DNS trap received by a trap receiver. The definitions of the vitalqipDnsTr family of values are in the above table.

```
Received SNMPv2c Trap:
Community: public
From: 127.0.0.1
sysUpTime.0 = 00:10:09.16
```

```
snmpTrapOID.0 = dnsServerStarted
vitalqipDnsTrIndex = 1
vitalqipDnsTrSequence = 1
vitalqipDnsTrId = monitor(1)
vitalqipDnsTrText = Lucent DNS started
vitalqipDnsTrPriority = inform(1)
vitalqipDnsTrClass = 1
vitalqipDnsTrType = 1
vitalqipDnsTrTime = 1184960025
vitalqipDnsTrSuspect = spirit
vitalqipDnsTrDiagId = 1
vitalqipDnsTrIteration = 1


Received SNMPv2c Trap:
Community: public
From: 127.0.0.1
sysUpTime.0 = 00:10:09.61
snmpTrapOID.0 = dnsServerStopped
vitalqipDnsTrIndex = 2
vitalqipDnsTrSequence = 1
vitalqipDnsTrId = monitor(1)
vitalqipDnsTrText = Lucent DNS stopped
vitalqipDnsTrPriority = inform(1)
vitalqipDnsTrClass = 2
vitalqipDnsTrType = 2
vitalqipDnsTrTime = 1184960025
vitalqipDnsTrSuspect = spirit
vitalqipDnsTrDiagId = 2
vitalqipDnsTrIteration = 1
```

### Querying vitalqipDnsTrapEntry tables and variables

An administrator can query the DNS trap tables by using the **`gettable`** or other SNMP client utility. An administrator can also query a specific component of a thrown trap using **`snmpget`** or other SNMP client utility. For example,

**`vitalqipDnsTrTime.10`**

would return the time that the 10th trap in the vitalqipDnsTrapEntry table was thrown.

### Trap table rolling

The vitalqipDnsTrapTable can only hold up to 31 entries. When the 32nd DNS trap is thrown, the TrapTable overwrites the 1st trap with the 32nd trap. The 33rd trap will replace the 2nd trap and the table will continue in a FIFO manner, overwriting the oldest trap in the table with the newest trap.

# 3 Test results

## Overview

### Purpose

This chapter is not pertinent to the Lucent DNS 5.1 release.

# 4 Resolved issues

## Overview

### Purpose

This chapter describes resolved issues in this release.

### Contents

This chapter covers these topics.

# Resolved issues in Lucent DNS 5.1, Build 46

**The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 46.**

**Table 4-1 ARs resolved in Build 46 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS0002371 | | 1: Critical | A critical defect in BIND 9 allows an attacker to cause excessive memory consumption in named or other programs linked to libdns.<br>CVE-2013-2266<br>For more information refer to https://www.isc.org |
| LDNS00002308 | | 1: Critical | A critical defect in BIND 9 allows remote attackers to trigger continued resolvability of revoked domain names via a “ghost domain names“ attack.<br>CVE-2012-1033<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 42

**The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 42.**

**Table 4-2 ARs resolved in Build 42 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002349 | | 3: Medium | A specially crafted DNS data can cause a lockup in named.<br>CVE-2012-5166<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 41

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 41.

**Table 4-3 ARs resolved in Build 41 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002344 |  | 2: High | A specially crafted resource record could cause named to terminate.<br>CVE-2012-4244<br>For more information refer to https://www.isc.org |
| LDNS00002339 | 1-4039410 | 4: Low | DNS 5.1 Release Notes is missing information about the entry /var/agentx/master in the *snmpd.conf* file. |
| LDNS00002291 | 1-3333471 | 3: Medium | Documentation update for net snmp on LDNS release notes. |
| LDNS00001094 |  | 3: Medium | ***Windows only***. Journal write fail causes DDNS updates to fail. |

# Resolved issues in Lucent DNS 5.1, Build 40

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 40.

**Table 4-4 ARs resolved in Build 40 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00001143 | 1-2741399 | 3: Medium | Ability to send traps to multiple destinations. |
| LDNS00002311 |  | 3: Medium | Merge ISC BIND 9.7.6. |
| LDNS00002323 |  | 2: High | Heavy DNSSEC load assertion failure.<br>CVE-2012-3817<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 29

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 29.

**Table 4-5 ARs resolved in Build 29 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002317 |  | 2: High | Handling of zero length rdata can cause named to terminate unexpectedly.<br>Processing of DNS resource records where the rdata field is zero length may cause various issues for the servers handling them.<br>CVE: CVE-2012-1667<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 28

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 28.

**Table 4-6 ARs resolved in Build 28 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002295 | 1-3465111 | 3: Medium | Lucent DNS 5.1 crashes on Solaris, for non-quote terminated TXT record. |
| LDNS00002301 | 1-3645476 | 2: High | When compiled and tested on AMD hardware, Lucent DNS 5.1 has issues with Intel CPUs. |
| LDNS00002307 |  | 2: High | QDDNS 5.1 Build 15 crashes on Solaris platform (Solaris 10, V240). |

# Resolved issues in Lucent DNS 5.1, Build 16

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 16.

**Table 4-7 ARs resolved in Build 16 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00001446 | | 3: Medium | LDNS 5.1 /SNMP 3.0 is logging the following messages continually into snmpd log: truncating integer value > 32 bits in qddns snmp.log.<br>Whenever user restarts the daemons, the errors goes and comes back after sometime. |

## Resolved issues in Lucent DNS 5.1, Build 15

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 15.

**Table 4-8 ARs resolved in Build 15 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002297 | | 2: High | An unidentified network event causes BIND 9 resolvers to cache an invalid record; subsequent queries might crash the resolvers with an assertion failure.<br>CVE: CVE-2011-4313<br>For more information refer to https://www.isc.org |

## Resolved issues in Lucent DNS 5.1, Build 12

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 12.

**Table 4-9 ARs resolved in Build 12 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002292 | | 1: Critical | ISC BIND 9 Remote packet Denial of Service against Authoritative and Recursive Servers.<br>CVE: CVE-2011-2464 and CVE-2011-2465<br>For more information refer to https://www.isc.org |

**Table 4-10 ARs resolved in Build 12 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002292 |  | 1: Critical | ISC BIND 9 Remote packet Denial of Service against Authoritative and Recursive Servers.<br>CVE: CVE-2011-2464 and CVE-2011-2465<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 9

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 9.

**Table 4-11 ARs resolved in Build 9 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00002290 |  | 2: High | DNS systems use negative caching to improve DNS response time. This will keep a DNS resolver from repeatedly looking up domains that do not exist. Any NXDOMAIN or NODATA/NOERROR response will be put into the negative cache.<br>In this vulnerability, very large RRSIG RRsets included in a negative cache can trigger an assertion failure that will crash named (BIND 9 DNS) due to an off-by-one error in a buffer size check.<br>For more information refer to https://www.isc.org |

# Resolved issues in Lucent DNS 5.1, Build 8

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 8.

**Table 4-12 ARs resolved in Build 8 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00001169 | 1-3153690 | 3: Medium | When upgrading from Lucent DNS 4.0 to Lucent DNS 5.1, DNS does not respond to queries or save anything in the log files. It has to be manually stopped and restarted.<br>When an authoritative server processes a successful IXFR transfer or a dynamic update, there is a small time frame during which the IXFR/update coupled with a query may cause a deadlock. This deadlock causes the server to stop processing all requests. A high query rate and/or a high update rate increases the probability of this condition. CVE:CVE-2011-0414 / CERT:VU#559980 |

# Resolved issues in Lucent DNS 5.1, Build 5

The following table identifies issues that have been resolved in Lucent DNS 5.1, Build 5.

**Table 4-13 ARs resolved in Build 5 release**

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00000984 | 1-1979485 | 3: Medium | **`named`** failing to write journal file. The root cause is the failure to remove the old journal file or a new journal file was created prematurely. |
| LDNS00001157 |  | 3: Medium | • This is a document defect.<br>• The SNMP 3.0 configuration steps are incomplete. |

| Fault ID | AR number | Severity | Description of issue |
|---|---|---|---|
| LDNS00001159 |  | 2: High | • Failure to clear existing RRSIG records when a NO DATA is negatively cached could cause subsequent lookups to crash named. CVE: CVE-2010-3613 / CERT: VU#706148.<br>• Named (acting as DNSSEC validating resolver) could incorrectly mark zone data as insecure when the zone being queried is undergoing a key algorithm rollover. CVE: CVE-2010-3614 / CERT: VU#837744.<br>• Using "allow-query" in the "options" or "view" statements to restrict access to authoritative zones has no effect. CVE: CVE-2010-3615 / CERT: VU#510208. For more information refer to https://www.isc.org |

# 5 Changes to interfaces, alarms, and messages

## Overview

### Purpose

This chapter is not pertinent to the Lucent DNS 5.1 release.

# 6 Known issues

## Overview

### Purpose

This chapter describes known issues and workarounds if available for Lucent DNS 5.1.

### Contents

This chapter covers these topics.

# Known issues and workarounds

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 6-1 Known issues and workarounds**

| Fault ID | AR Number | Severity | Description of issue | Workaround |
|---|---|---|---|---|
| LDNS00001158 | | 3: Medium | DSA algorithm is not supported on Windows.<br>c:\qip\named\bin\dnssec-keygen.exe -q -r<br>../random.data -a DSA -b 768 -n zone example.<br>dnssec-keygen: fatal:failed to generate key example/DSA: algorithm is unsupported. | |
| LDNS00001010 | | 3: Medium | Changing controls statement from **`inet *`** to **`inet 127.0.0.1`** fails. | Use **`kill -HUP`** ***`<named_pid>`*** or **`restart named`**. |
| LDNS00001013 | | 3: Medium | Stopping **`named`** logs an exiting message but the process still exists. | |
| LDNS00001017 | | 3: Medium | False positive message logged for **`edns`** when initial query is truncated. | |

| Fault ID | AR Number | Severity | Description of issue | Workaround |
|---|---|---|---|---|
| LDNS00001022 | | 3: Medium | **`ip_conntrack`**: table full, dropping packet messages and server unreachable messages logged.<br>**Note:** This issue is fixed with HELIO00001112/ HELIO00006142 for the ALU appliance in qddns-5.1.12-2.x86_64.lpf or later. | To check the current max:<br>**`` `cat /proc/sys/net/ipv4/ip_conntrack_max` ``**<br>To check the current count:<br>**`` `cat /proc/sys/net/ipv4/netfilter/ip_conntrack_count` ``**<br>Set a new max for ipchains tracked connections:<br>**`` `echo "131072">/proc/sys/net/ipv4/ip_conntrack_max` ``** |
| LDNS00001033 | | 3: Medium | NOTIFY opcode counter from **`rndc qddns-stats`** does not increment. | Use the **`lock-isc-stats`** policy, described in Table 2-2, “Lucent DNS directives” (p. 2-3). Add the following:<br>**`{ lock-isc-stats yes; };`**<br>to the **`qddns`** options block in *named.conf*. |
| LDNS00001097 | | 2: High | *named* assertion exit during secure update stress test. | |
| LDNS00001120 | | 2: High | All zone transfers fail during and after stress test | The configured "transfers-out" value was "100" and changing this to 110 and running "rndc reconfig"  then allowed zone transfers to successfully complete. |

| Fault ID | AR Number | Severity | Description of issue | Workaround |
|---|---|---|---|---|
| LDNS00001124 | | 2: High | Server crashes on Windows 2008 when processing a TKEY from a native Windows client. Event Viewer shows faulting application named.exe. | Only affects Windows 2008: stop and restart the DNS service to recover or use Win2003 OS to avoid this problem. |

# Known vendor issues

For a list of ISC BIND 9 issues that may also exist in Lucent DNS 5.1, 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 6-2 Known vendor issues**

| Fault ID | Vendor | Description of issue | Workaround |
|---|---|---|---|
| LDNS00001207 | ISC | During stressed operations, the server may crash with a fault in the **libdns** module. This appears to be a race condition that happens sporadically on extremely busy servers during zone maintenance. This is most common on Windows, uncommon on Solaris Sparc, and not seen on Linux platforms. | Reduce the zone maintenance load on the server. |

| Fault ID | Vendor | Description of issue | Workaround |
|---|---|---|---|
| LDNS00001444 | Sun/Oracle Solaris | A defect of socket polling in certain versions of the Solaris kernel can cause Lucent DNS 5.1 (based on BIND 9.7) to go into a "sleeping" state under conditions of very large numbers of incoming queries.While in this state, DNS does not reply to queries or zone transfer requests and does not use CPU, and the only messages in the logs will be "client per query increased". But after a period of time -- perhaps a few minutes or perhaps up to an hour -- DNS will "wake up" by itself and return to normal. Also, DNS will "wake up" if a query or rndc command is done via the 127.0.0.1 loopback. | The Solaris defect is fixed in Solaris 10 Update 8 or higher, but since it is a kernel defect it is only fixed in the full Solaris update not in any patch bundle. A cron job to send queries or rndc commands via the 127.0.0.1 interface can also be work-around to keep "waking up" the DNS process. |
| LDNS00002310 | Microsoft | LDNS 5.1/Windows terminates when processing a TKEY query using RC4-HMAC or higher. | |

# 7 System requirements

## Overview

### Purpose

This chapter describes software and hardware requirements and compatibility restrictions.

### Contents

This chapter covers these topics.

# Supported platforms

Lucent DNS 5.1 is supported on the following platforms.

- VitalQIP Appliance and Red Hat Enterprise Linux (AS,ES) 5 (64 bit).
- Solaris 9 UltraSPARC,10 UltraSPARC (64 bit) and Solaris 10 X86 (64 bit).
- Windows 2003 Enterprise or Standard Server (32 and 64 bit), Service Pack 2.
- Windows 2008 Standard and Enterprise Server (32 and 64 bit), Service Pack 1 or above

**Note:** Lucent DNS 5.1 is 32-bit on Windows and 64-bit on all UNIX platforms. SNMP plug-ins are 64-bit on UNIX and 32-bit on Windows. The master agent (snmpd) can be 32-bit or 64-bit.

**Note:** Very busy DNS Servers (over 1000 queries per second) running on Solaris may encounter a known Solaris kernel defect: "*Bug 6724237: polling on /dev/poll can hang even though UDP data is available*", which can cause the problem identified in LDNS1444 (see Known Vendor Issues). This Solaris issue is fixed in Solaris 10 Update 8, though not in any patch. The Solaris update level can be determined by the command "**`cat /etc/release`**", and it should show output as:

```
Solaris 10 10/08 s10s_u6wos_07b SPARC
           Copyright 2008 Sun Microsystems, Inc.  All Rights
Reserved.
                        Use is subject to license terms.
                            Assembled 27 October 2008

               Solaris 10 10/09 (Update 8) Patch Bundle applied.
```

The "`s10s_u6`" in the first line shows that the original installation was Update 6, but the last line shows that Update 8 was applied and therefore the defect is fixed in this example. This is independent from the Solaris patch level as shown by "**`uname -a`**". If you experience this issue on Solaris 9, please contact Oracle/Sun for assistance and mention bug 6724237.

# Software requirements

Lucent DNS 5.1 is certified with the following VitalQIP releases:

- VitalQIP 7.2 PR3
- VitalQIP 7.3
- VitalQIP 8.0

**Important!** Platform support is also dependent on the VitalQIP remote server version.

Lucent DNS 5.1 is supported on VitalQIP 7.x and VitalQIP 8.x remote servers running 64-bit Unix versions of supported VitalQIP 7.x and VitalQIP 8.x platforms and 32-bit or 64-bit Windows versions of supported VitalQIP 7.x and VitalQIP 8.x platforms.

# Hardware requirements

The following table lists the hardware requirements for VitalQIP remote servers to run Lucent DNS 5.1.

**Table 7-1 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 |

# Compatibility restrictions

Lucent DNS 5.1 has the following compatibility restrictions.

**Table 7-2 Product compatibility**

| Product | Compatibility |
|---|---|
| VitalQIP | Lucent DNS 5.1 is supported with VitalQIP 7.x and VitalQIP 8.x running on only 64-bit Unix and 32 or 64-bit Windows platforms. |

| Product | Compatibility |
|---|---|
| SNMP Module | SNMP Module 3.0 is supported with VitalQIP 7.2 PR2 and above.<br>**Note:** The SNMP Module version must be SNMP 3.2 of the plug-in library.<br>Lucent DNS 5.1 supports the following SNMP plugins that are compatible with the Net-SNMP Master Agent:<br>Unix (64-bit) *libqddns_snmp.so*<br>Windows (32-bit) *qddns_snmp.dll* |
| VitalQIP AM appliance | AMS 1.5 and above. |
| Services Manager | Not currently supported. |

# 8 Installation and upgrade notes

## Overview

### Purpose

This chapter contains notes on installation of Lucent DNS 5.1.

### Contents

This chapter covers these topics.

# Performing Lucent DNS 5.1 installation on UNIX

When you are installing Lucent DNS 5.1, ensure that you have met the system requirements described in the previous chapter and then refer to the documentation in Table 8-3 for further configuration information.

The following table lists the files that are supplied with Lucent DNS 5.1. These files should be located in *$QIPHOME/usr/bin*.

**Table 8-1 Installation files on UNIX**

| Filename | Description |
|---|---|
| *dig* | DNS client utility |
| *dnssec-keygen* | DNSSEC key generation tool |
| *dnssec-signzone* | DNSSEC zone signing tool |
| *host* | DNS lookup utility |
| *journalprint* | Print zone journal in human-readable form |
| *named-checkconf* | Checks *named.conf* file syntax |
| *named-checkzone* | Checks zone file syntax |
| *named* | DNS server binary. For more information on **named** command line options, refer to "Command line interface" (p. 8-10) |
| *nslookup* | DNS client utility |
| *nsupdate* | DNS update utility |
| *rndc-confgen* | Generates **rndc** keys and configuration files |
| *rndc* | Remote name daemon control utility |
| *arpaname* | Translate IP addresses to the corresponding ARPA names |
| *ddns-confgen* | ddns key generation tool |
| *dnssec-dsfromkey* | DNSSEC DS RR generation tool |
| *dnssec-revoke* | Set the REVOKED bit on a DNSSEC key |
| *dnssec-keyfromlabel* | DNSSEC key generation tool |
| *dnssec-settime* | Set the key timing metadata for a DNSSEC key |
| *genrandom* | Generate a file containing random data |
| *isc-hmac-fixup* | Fixes HMAC keys generated by older versions of BIND |
| *nsec3hash* | Generate NSEC3 hash |

## Shared libraries

The following shared libraries are also installed with Lucent DNS 5.1. Lucent DNS 5.1 libraries should be located in *$QIPHOME/usr/lib64*.

- *libcom_err.so.3.0*
- *libgssapi_krb5.so.2.2*
- *libk5crypto.so.3.1*
- *libkrb5.so.3.3*
- *libkrb5support.so.0.1*
- *libqddns_snmp.so*

For Linux, the LD_LIBRARY_PATH must be set properly to make sure the delivered shared libraries are used. Add *$QIPHOME/usr/lib64* to this environment variable. For Solaris LD_LIBRARY_PATH_64 should be set properly to make sure the delivered shared libraries are used. Add *$QIPHOME/usr/lib64* to this environment variable. The LDNS 5.1 Build 12 library names are different from the previous build and require a symbolic link to the prior library name to properly load the shared libraries. Create the links as described below in the Unix Installation steps.

To verify 32-bit and 64-bit platforms on Solaris, enter the following:

```
isainfo -v
```

If the output is "`32-bit sparc applications`", it is a 32-bit machine. If the output is "`64-bit sparcv9 applications 32-bit sparc applications`", it is a 64-bit machine.

To verify 32-bit and 64-bit platforms on Linux, enter the following:

```
uname -m
```

If the output is x86_64, then it is a 64-bit kernel. If it is i386/i486/i586/i686, then it is a 32-bit kernel.

To verify that *named* is using the shared libraries, enter the following:

```
$ ldd $QIPHOME/usr/bin/named
```

## Before you begin

Before you begin the installation, 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 ldns5.1.46-linux-gcc3.tar`**
- For Solaris: **`tar -xf ldns5.1.46-solaris.2x.tar`**
- For Solaris X86: **`tar -xf ldns5.1.46-solaris-x86.tar`**

END OF STEPS

### UNIX installation

To install Lucent DNS 5.1, follow these steps.

1 Stop any previous versions of Lucent DNS (**`named`**) by typing **`rndc stop`** or **`kill`** ***`<named_pid>`*** at a command line.

2 Make a backup of the **`named`** binaries and then remove the original files. Prior to VitalQIP 7.2, **`named`** and utilities were located in */usr/sbin*. Starting with VitalQIP 7.2, **`named`** and utilities are located in *$QIPHOME/usr/bin*. No shared libraries were delivered prior to Lucent DNS 4.2.

3 Copy the new binaries, listed in Table 8-1, "Installation files on UNIX" (p. 8-2), to *$QIPHOME/usr/bin*.

4 Copy the shared library files, listed in "Shared libraries" (p. 8-3), to *$QIPHOME/usr/lib64*.

5 Change to the *$QIPHOME/usr/lib64* directory. Create symbolic links for the shared libraries as follows:

- **`ln -s libcom_err.so.3.0 libcom_err.so.3`**
- **`ln -s libgssapi_krb5.so.2.2 libgssapi_krb5.so.2`**
- **`ln -s libk5crypto.so.3.1 libk5crypto.so.3`**
- **`ln -s libkrb5.so.3.3 libkrb5.so.3`**

- **`ln -s libkrb5support.so.0.1 libkrb5support.so.0`**

**6** Ensure that you have sourced the *shrc* or *cshrc* file.

**7** Start Lucent DNS 5.1 by typing **`$QIPHOME/usr/bin/named`** with command line options as desired, or execute **`$QIPHOME/etc/qip-rs-startup`**.

END OF STEPS

### Post-installation requirement

**`rndc`** should exist in the same location as specified in VitalQIP in the **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 DNS server update file generations. Ensure that there is a link for */etc/named.conf* that points to <*push_dir*>*/named.conf*. The *named.pcy* file needs to be present in the */etc* folder. By default, Lucent DNS will check for the presence of *named.pcy* file in the */etc* folder.

## Performing Lucent DNS 5.1 installation on Windows

When you are installing Lucent DNS 5.1, ensure that you have met the system requirements described in the previous chapter and then refer to the documentation in Table 8-3 for further configuration information.

The following table lists the files that are supplied with Lucent DNS 5.1. *named* and utilities are located in *%QIPHOME%\named\bin*.

Table 8-2 Installation files on Windows

| Filename | Description |
|---|---|
| *dig.exe* | DNS client utility |
| *dnssec-keygen.exe* | DNSSEC key generation tool |
| *dnssec-signzone.exe* | DNSSEC zone signing tool |
| *host.exe* | DNS lookup utility |
| *journalprint.exe* | Print zone journal in human-readable form |
| *named-checkconf.exe* | Checks *named.conf* file syntax |
| *named-checkzone.exe* | Checks zone file syntax |
| *named.exe* | DNS server binary. For more information on **named** command line options, refer to "Command line interface" (p. 8-10) |
| *nslookup.exe* | DNS client utility |
| *nsupdate.exe* | DNS update utility |
| *rndc-confgen.exe* | Generates **rndc** keys and configuration files |
| *rndc.exe* | Remote name daemon control utility |
| *arpaname.exe* | Translate IP addresses to the corresponding ARPA names |
| *ddns-confgen.exe* | ddns key generation tool |
| *dnssec-dsfromkey.exe* | DNSSEC DS RR generation tool |
| *dnssec-revoke.exe* | Set the REVOKED bit on a DNSSEC key |
| *dnssec-keyfromlabel.exe* | DNSSEC key generation tool |
| *dnssec-settime.exe* | Set the key timing metadata for a DNSSEC key |
| *genrandom.exe* | Generate a file containing random data |
| *isc-hmac-fixup.exe* | Fixes HMAC keys generated by older versions of BIND |
| *nsec3hash.exe* | Generate NSEC3 hash |

## DLLs

The following DLLs are installed with Lucent DNS 5.1. Lucent DNS 5.1 DLLs are also located in *%QIPHOME%\named\bin*.

- *libbind9_qddns.dll*
- *libdns_qddns.dll*
- *libisc_qddns.dll*

- *libisccc_qddns.dll*
- *libisccfg_qddns.dll*
- *liblwres_qddns.dll*
- *libeay32.dll*
- *comerr32.dll* - part of Kerberos
- *gssapi32.dll* - part of Kerberos
- *msvcr71.dll* - part of Kerberos
- *k5sprt32.dll* - part of Kerberos
- *krb5_32.dll* - part of Kerberos
- *libxml2.dll* - part of *libxml2*
- *iconv.dll* - required by *libxml2*
- *zlib1.dll* - required by *libxml2*
- *qddns_snmp.dll* - snmp plugin

### Before you begin

Before you begin the installation, 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 5.1, follow these steps.

**1** Stop any existing Lucent DNS (*named*) by selecting **Lucent DNS Service** and clicking **Stop** from the **VitalQIP Services Controller**.

**2** Remove any previous version of Lucent DNS from the Windows registry by typing the following at a command line:

```
<install_dir>\bin\named –remove
```

**3** Make a backup of the *<install_dir>\bin* directory, if desired.

**4** Create the desired install directory*<install_dir>*, such as *%QIPHOME%\named*, if it does not exist.

**5** 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*.

**6** Copy the binaries and libraries into the *<install_dir>\bin* directory.

**7** From the *<install_dir>\bin* directory, install Lucent DNS 5.1 by running one of the following command sequences:

| If you wish to ... | Then ... |
|---|---|
| Install with manual startup | Run `named.exe –install <install_dir>`<br>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. |
| Install with automatic startup | Run `named.exe –installauto <install_dir>`<br>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. |

**8** 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.

i. Start Lucent DNS 5.1 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 DNS server update file generations.

Optionally configure the desired startup command line options for Lucent DNS 5.0 as shown in "Specifying named commands in Windows registry" (p. 8-12).

The *named.pcy* file needs to be present in the *<install_dir>/etc* folder. By default, Lucent DNS will check for the presence of *named.pcy* file in the *<install_dir>/etc* folder.

## Configuring Lucent DNS 5.1

Refer to the appropriate document in the following table for instructions on how to configure Lucent DNS 5.1.

**Table 8-3 Configuration information**

| Document title | Part number | Chapter |
|---|---|---|
| *VitalQIP 7.2 User's Guide* | 190-409-068R7.2PR2 | Chapter 4, "Manage Servers"<br>• Lucent DNS 4.x Server Type |

| Document title | Part number | Chapter |
|---|---|---|
| *VitalQIP 7.3 Administrator Reference Manual* | 190-409-042R7.3 | Chapter 2, “Manage VitalQIP services”<br>• Configure the VitalQIP Service Controller<br>• named - Lucent DNS Service daemon |
| | | Chapter 24, “Advanced DNS configurations”<br>• Lucent DNS directives<br>• Secure dynamic updates support<br>• External objects and resource records support<br>• Improve DNS push functionality<br>• Customize user exit scripts |
| | | Chapter 24, “Troubleshoot DNS” |
| *VitalQIP 8.0 Web Client User’s Guide* | 9YZ-04705-0001-TCZZA | Chapter 15 “DNS Server”, section “LUCENT DNS 3.X,LUCENT DNS 4.X, and LUCENT DNS 5.X server types” |
| *VitalQIP 8.0 Administrator Reference Manual* | 9YZ-04705-0001-RKZZA | Chapter 2, “Manage VitalQIP services”<br>• Configure the VitalQIP Service Controller<br>• named - Lucent DNS Service daemon |
| | | Chapter 24, “Advanced DNS configurations”<br>• Lucent DNS directives<br>• Secure dynamic updates<br>• External objects and resource records support<br>• Improve DNS push functionality<br>• Customize user exit scripts |

# Command line interface

## Command line options

The following command line options are available in Lucent DNS 5.1 for **`named`**.

### Usage

```
named [-4|-6] [-c conffile] [-y policyfile] [-d debuglevel] [-E
   engine-name] [-f|-g] [-n number_of_cpus] [-p port] [-s] [-t
   chrootdir] [-u username] [-m {usage|trace|record|size|mctx}] [-
   install] [-installauto] [-remove]
```

**Important!** When installed as a service on Windows, the path of **named** will be *<install_dir>\bin* and the *config* file must be located in the *<install_dir>\etc* directory. If no directory is specified with **-install** or **-installauto**, the default directory will be *<system- dir>\dns*.

Table 8-4 Command line parameters for named

| Option | Description |
|---|---|
| **-c *conffile*** | Starts **named** using the specified *conf* file |
| ***-y pcyfile*** | Starts **named** using the specified *policy* file |
| **-d *debuglevel*** | Starts **named** using the specified debug level |
| **-E *engine-name*** | Use a crypto hardware(Open SSL engine) for the crypto operations it supports. |
| **-f** | Runs **named** in the foreground |
| **-g** | Runs **named** in the foreground and sends all output to STDERR |
| **-n *number_of_cpus*** | Tells **named** how many processors exist on the system |
| **-p *port*** | Directs **named** to listen on the specified port |
| **-t *chrootdir*** | ***UNIX only***. Causes **named** to **chroot** to the specified directory |
| **-u *username*** | ***UNIX only***. Runs **named** as the specified user |
| **-v** | Prints **named** version information |
| **-s** | Prints memory statistics at exit (only available if running in foreground) |
| **-4** | Runs **named** over IPv4 transport only (IPv6 AAAA records are still resolved) |
| **-6** | Runs **named** over IPv6 transport only (IPv4 A records are still resolved) |
| **-install *<install_dir>*** | ***Windows only***. Installs the service in the registry using *<install_dir>* with manual startup |

| Option | Description |
|---|---|
| **`-installauto <install_dir>`** | ***Windows only***. Installs the service in the registry using <*install_dir*> with automatic startup |
| **`-remove`** | ***Windows only***. Removes the service from the registry |
| **`-m`** | Used for debugging, when run in foreground. |

# Specifying named commands in Windows registry

***Windows only***. Lucent DNS 5.1 allows you to specify **`named`** command line options, such as the number of worker threads (**`-n`**), in the registry (when **`named`** runs as a service). This is useful to allow automatic startup of named with the desired options. For example, limiting the number of worker threads with "**`-n 2`**" when the Lucent DNS Server detects more than the actual number of CPUs, or when the server CPU spikes to 90% or more after startup, or during cleaning intervals.

To specify the number of worker threads to use, for example, follow these steps.

1 Ensure that the Lucent DNS service is already installed.

2 Start **`regedit`** by selecting **Start->Run** and entering **`regedit`**.

3 Save a backup copy of the **`regedit`** file.

4 Go to **HKEY_LOCAL_MACHINE->SYSTEM->CurrentControlSet->Services->Lucent DNS Service**.

5 Double-click on **ImagePath** and add the arguments at the end of the text field. For example, to specify number of worker threads to 2, add **`-n 2`**:

```
g:\qip\named.exe -n 2
```

Some sample working ImagePath values are:

```
c:\qip\named dir\bin\named.exe -n 2
c:\qip\named dir\bin\named.exe -4 -n 2
c:\qip\named dir\bin\named.exe -4 -n 2
```

```
c:\qip\named dir\bin\named.exe -4 -n 2
c:\qip\named\bin\named.exe -4 -n 2
```

Some sample failure ImagePath values are:

```
c:\qip\named dir\bin\named.exe -4 -n 2
c:\qip\named dir\bin\named.exe -4 -n 2
```

**6** Press **OK**.

**7** Open the **Administrative Tools->Services** control and select the **Lucent DNS Service**. The argument `-n 2` should show up in the **Path to executable** field.

After starting the service, a message like: “`found x CPUs, using 2 worker threads`” will be in the EventLog for the above example.

END OF STEPS

# Configuring SNMP 3.0 on Solaris 10

Sun supplies Net-SNMP on Solaris 10.

To configure SNMP 3.0 with Sun-supplied Net-SNMP, follow these steps:

**1** Copy *qddns.mib* to the */etc/sma/snmp/mibs* directory.

**Note:** Remove the old *named.mib* from */etc/sma/snmp/mibs* if it exists from previous installations of the SNMP Module.

**2** Copy *libqddns_snmp.so* to the *$QIPHOME/usr/lib64* directory.

**3** Modify the */etc/sma/snmp/snmpd.conf* file to include the information from the supplied *sample_snmpd.conf* file.

```
##
# Minimal configuration file for Net-SNMP master agent snmpd.
# For more details on configuring the master agent and tools,
# plse refer to the Net-SNMP website (http://www.net-snmp.org).
rocommunity public
```

```
##
# Enable AgentX protocol.
# It is necessary for Alcatel-Lucent DNS server SNMP sub agents.
# For more details on configuring the master agent for AgentX
# support,
# please refer to the Net-SNMP website (http://www.net-snmp.org).
master agentx
agentxSocket /var/agentx/master
##
```

4 Create or modify */etc/sma/snmp/snmp.conf* by adding the following line to automatically load/translate the enterprise DNS MIB.

```
mibs +QDDNS-SERVER-MIB
```

5 Stop and start **snmpd** type typing:

```
# svcadm restart sma
or
# svcadm disable sma
# svcadm enable sma
```

6 Perform the following only if the above step fails or the installed snmp is not Sun's master agent.

```
# /etc/init.d/init.sma stop
# /etc/init.d/init.sma start
```

7 Optionally, add the snmp utilities directory to the path:

```
# export PATH=$PATH:/usr/sfw/bin
```

END OF STEPS

### Configuring Net-SNMP 5.4.2.1 on Solaris

If you encounter any issues with Sun-supplied Net-SNMP, do the following to install Net-SNMP 5.4.2.1:

1 Disable Sun’s SNMP.

To determine if Sun's SNMP is running, execute the following commands:

```
# ps -eaf|grep snmp
```

If you see the process **snmpd**, then Sun's SNMP daemons are running. To disable, execute the following commands:

```
# svcadm disable sma
```

Only use the following if the above fails or the installed snmp is not Sun's master agent:

```
# /etc/init.d/init.sma stop
```

2 Install and run Net-SNMP from http://www.sunfreeware.com.

END OF STEPS

### Install Net-SNMP

If you have a compiler, you can compile and install Net-SNMP yourself. But the easy option is to get the compiled package from http://www.sunfreeware.com/. Download netsnmp-5.4.2.1-sol10-sparc-local.gz and install it as follows:

```
# gunzip netsnmp-5.4.2.1-sol10-sparc-local.gz
# pkgadd -d netsnmp-5.4.2.1-sol10-sparc-local
```

If you see any dependency errors, then install the required packages as well. For example, the following may be required for the *netsnmp-5.4.2.1-sol10-sparc-local.gz* package:

- *libgcc-3.4.6-sol10-sparc-local.gz*
- *openssl-1.0.0.b-sol10-sparc-local.gz*
- *libiconv-1.2.5-sol10-sparc-local.gz*

### Creating snmpd.conf and testing

You can use the Alcatel-Lucent supplied *sample_snmpd.conf* (copy it as */usr/local/share/snmp/snmpd.conf*), use a minimal *snmpd.conf* file, or create one by running:

```
# snmpconf -g basic_setup
```

For more information about configuring SNMP traps, see "Configuring SNMP Traps for all platforms" (p. 8-25).

Answer the questions appropriately. Add the following at the end of the *snmpd.conf* file:

```
master agentx
agentxSocket /var/agentx/master
```

### Configuring Net-SNMP

To configure Net-SNMP, do the following:

1 Copy the file *qddns.mib* to */usr/local/share/snmp/mibs* directory.

2 Copy *libqddns_snmp.so* to the *$QIPHOME/usr/lib64* directory.

3 Create or modify the following to */usr/local/share/snmp/snmp.conf*:

```
mibs +QDDNS-SERVER-MIB
```

4 Copy the created *snmpd.conf* file to */usr/local/share/snmp/snmpd.conf.*

To run the master agent:

```
# /usr/local/sbin/snmpd
```

To run the master agent in foreground, type:

```
# /usr/local/sbin/snmpd -f -L -Dagentx
```

5 If required, create the startup script at */etc/rc3.d* directory to start the master agent at boot time.

END OF STEPS

# Configuring SNMP 3.0 on Solaris 10 X86

To configure SNMP 3.0 on Solaris 10 X86, follow these steps:

1 On Solaris 10 X86, if Sun's SNMP(**snmpdx**) is running, it must be stopped first.

2 Disable Sun's SNMP.

To determine if Sun's SNMP is running, execute the following commands:

```
# ps -eaf|grep snmp
```

If you see the process **snmpdx**, then Sun's SNMP daemons are running. To disable, execute the following commands:

```
# svcadm disable sma
```

Only use the following if the above fails or the installed snmp is not Sun's master agent:

```
# /etc/init.d/init.sma stop
```

3 Install and run Net-SNMP from http://www.sunfreeware.com.

END OF STEPS

### Install Net-SNMP

If you have a compiler, you can compile and install Net-SNMP yourself. But the easy option is to get the compiled package from http://www.sunfreeware.com/. Download netsnmp-5.4.2.1-sol10-X86-local.gz, then install it as follows:

```
# gunzip netsnmp-5.4.2.1-sol10-x86-local.gz
# pkgadd -d netsnmp-5.4.2.1-sol10-x86-local
```

If you see any dependency errors, then install the required packages as well. For example, the following may be required for the *netsnmp-5.4.2.1-sol10-x86-local.gz* package:

- *libgcc-3.4.6-sol10-x86-local.gz*
- *openssl-1.0.0.b-sol10-sparc-local.gz*
- *libiconv-1.2.5-sol10-x86-local.gz*

### Creating snmpd.conf and testing

You can use the Alcatel-Lucent supplied *sample_snmpd.conf* (copy it as */usr/local/share/snmp/snmpd.conf*), use a minimal snmpd.conf file, or create one by running:

```
# snmpconf -g basic_setup
```

For more information about configuring SNMP traps, see "Configuring SNMP Traps for all platforms" (p. 8-25).

Answer the questions appropriately.

1 Add the following at the end of the *snmpd.conf* file:

```
master agentx
agentxSocket /var/agentx/master
```

2 Copy the file *qddns.mib* to */usr/local/share/snmp/mibs* directory.

3 Copy *libqddns_snmp.so* to the *$QIPHOME/usr/lib64* directory.

4 Create or modify the following to */usr/local/share/snmp/snmp.conf*:

```
mibs +QDDNS-SERVER-MIB
```

5 Copy the created *snmpd.conf* file to */usr/local/share/snmp/snmpd.conf*

To run the master agent in foreground, type:

```
# snmpd -f -L -Dagentx
```

6 If required, create the startup script at */etc/rc3.d* directory to start the master agent at boot time.

END OF STEPS

# Configuring SNMP 3.0 on Solaris 9

To configure SNMP Module 3.0 on Solaris 9, follow these steps:

1 If Sun's SNMP (**snmpdx**) is running, it must be stopped first.

2 Disable Sun's SNMP.

To determine if Sun's SNMP is running, execute the following commands:

```
# ps -eaf|grep snmp
# ps -eaf|grep mibi
```

If you see the processes **snmpdx** and **mibiisa**, then Sun's SNMP daemons are running. To disable, execute the following commands:

```
# cd /etc/rc3.d
# ./S76snmpdx stop
# ./S77dmi stop
# mv S76snmpdx s76snmpdx
# mv S77dmi s77dmi
```

3 Install and run Net-SNMP from *http://www.sunfreeware.com/.*

END OF STEPS

### Install Net-SNMP

If you have a compiler, you can compile and install Net-SNMP yourself. But the easy option is to get the compiled package from http://www.sunfreeware.com/. Download netsnmp-5.4.2.1-sol9-sparc-local.gz, then install it as follows:

```
# gunzip netsnmp-5.4.2.1-sol9-sparc-local
# pkgadd -d netsnmp-5.4.2.1-sol9-sparc-local
```

If you see any dependency errors, then install the required packages as well. For example, the following may be required for the *netsnmp-5.4.2.1-sol9-sparc-local.gz* package:

- *libgcc-3.4.6-sol9-sparc-local.gz*
- *openssl-0.9.8l-sol9-sparc-local.gz*
- *libiconv-1.11-sol9-sparc-local.gz*

### Creating snmpd.conf and testing

You can use the Alcatel-Lucent supplied *sample_snmpd.conf* (copy it as */usr/local/share/snmp/snmpd.conf*), use a minimal snmpd.conf file, or create one by running:

```
# snmpconf -g basic_setup
```

For more information about configuring SNMP traps, see "Configuring SNMP Traps for all platforms" (p. 8-25).

Answer the questions appropriately.

1 Add the following at the end of the *snmpd.conf* file:

```
master agentx
agentxSocket /var/agentx/master
```

2 Copy the file *qddns.mib* to */usr/local/share/snmp/mibs* directory.

3 Copy *libqddns_snmp.so* to the *$QIPHOME/usr/lib64* directory.

4 Create or modify the following to */usr/local/share/snmp/snmp.conf:*

```
mibs +QDDNS-SERVER-MIB
```

5 Copy the created *snmpd.conf* file to */usr/local/share/snmp/snmpd.conf*

To run the master agent in the foreground, type:

```
# snmpd -f -L -Dagentx
```

6 Create the startup script in the */etc/rc3.d* directory to start the master agent at boot time.

END OF STEPS

## Configuring SNMP 3.0 on Linux

To configure SNMP Module 3.0 on Linux, follow these steps:

1 Ensure that there is no old snmp (snmpdm) running).

2 Install snmp package if not installed already.

3 Get packages for RH 86_x64 (net-snmp-5.3.1-24.el5.x86_64.rpm, net-snmp-utils-5.3.1-24.el5.x86_64.rpm, lm_sensors-2.10.0-3.1.x86_64.rpm).

> **Note:** In RH, yum should be used to install packages. yum can figure out dependencies. For master agent, the package net-snmp is needed and for the tools (snmpget, snmpwalk etc), the package net-snmp-utils is needed. Example on RH 5.3 system:

```
# yum search net-snmp
net-snmp.x86_64 : A collection of SNMP protocol tools and
   libraries.
net-snmp-devel.i386 : The development environment for the NET-SNMP
   project.
net-snmp-devel.x86_64 : The development environment for the NET-
   SNMP project.
net-snmp-libs.i386 : The NET-SNMP runtime libraries.
net-snmp-libs.x86_64 : The NET-SNMP runtime libraries.
net-snmp-perl.x86_64 : The perl NET-SNMP module and the mib2c
   tool.
```

```
net-snmp-utils.x86_64 : Network management utilities using SNMP,
   from the NET-
                      : SNMP project.

 # yum install net-snmp.x86_64
 # yum install net-snmp-utils.x86_64
```

**4** If you cannot use yum, then perform steps 5 through 7.

**5** Install libsensors (net-snmp dependency)

```
# rpm -iv /cdrom/Server/lm_sensors-2.10.0-3.1.x86_64.rpm
    Preparing packages for installation...
    lm_sensors-2.10.0-3.1
```

**6** Install snmp master agent (server)

```
# rpm -iv /cdrom/Server/net-snmp-5.3.1-24.el5.x86_64.rpm
    Preparing packages for installation...
    net-snmp-5.3.1-24.el5
```

**7** Install snmp utilities (clients).

```
# rpm -iv /cdrom/Server/net-snmp-utils-5.3.1-24.el5.x86_64.rpm
    Preparing packages for installation...
    net-snmp-utils-5.3.1-24.el5
```

**8** Copy the *qddns.mib* file to the */usr/share/snmp/mibs* directory.

**9** Remove the old *named.mib* from */usr/share/snmp/mibs* if it is there.

**10** Copy *libqddns_snmp.so* to the *$QIPHOME/usr/lib64* directory.

**11** Modify the /etc/snmp/snmpd.conf file to include the information from the supplied s*ample_snmpd.conf* file.

```
##
# Minimal configuration file for Net-SNMP master agent snmpd.
# For more details on configuring the master agent and tools,
# plse refer to the Net-SNMP website (http://www.net-snmp.org).
rocommunity public
# Enable AgentX protocol.
# It is necessary for Alcatel-Lucent DNS server SNMP sub agents.
# For more details on configuring the master agent for AgentX
# support,
# please refer to the Net-SNMP website (http://www.net-snmp.org).
master agentx
agentxSocket /var/agentx/master
##
# send trap to localhost
##
```

**12** Create or modify the */etc/snmp/snmp.conf* file by adding the following line to automatically load/translate the enterprise DNS mibs.

```
mibs +QDDNS-SERVER-MIB
```

**13** Stop and start snmpd type:

```
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
```

END OF STEPS

For more information about configuring SNMP traps, see "Configuring SNMP Traps for all platforms" (p. 8-25).

# Configuring SNMP 3.0(using Net-SNMP) on Windows

## OpenSSL installation

If choosing the ssl-enabled installation of Net-SNMP, download or build the openssl binaries.

**1** Download the latest 32-bit OpenSSL binary from http://www.slproweb.com/products/Win32OpenSSL.html (Win32 OpenSSL v0.9.8r Light).

**2** If running the installation displays a warning about runtime libraries, install the 32-bit runtime redistributables found at the same location (Visual C++ 2008 Redistributables).

**3** Install the package to c:\OpenSSL.

**4** Copy the binaries to the OpenSSL (/bin) directory rather than the default Windows directory, unless you are sure you know the impact.

**5** Set the PATH system environment variable to include “C:\Openssl\bin” if you chose the recommended copy location instead of the default (Windows) location.

END OF STEPS

### Net-SNMP installation

**1** Download and install SNMP from the Net-SNMP website.

**2** Use 32-bit version with or without ssl (tested with ssl).

**3** Use the default installation options (This is the tested configuration, although integration with Microsoft SNMP is optional).

**4** If you desire to run the master agent (*snmpd.exe*) or trap daemon (snmptrapd.exe) as services:

- **Run, Start Menu -> Programs -> Net-SNMP -> Service -> Register Agent Service** to “daemonize” the master agent
- **Run, Start Menu -> Programs -> Net-SNMP -> Service -> Register Trap Service** to “daemonize” the trap service
- You can remove the services by choosing the corresponding “**Unregister**” selection at the same start menu location.

END OF STEPS

### Configuration of SNMP Master Agent

**1** Copy the *sample_snmpd.conf* file to *<path_of_net-snmp>\etc\snmp\snmpd.conf* file.

**2** Ensure the following lines are in the *snmpd.conf* file:

```
master agentx
agentxSocket tcp:localhost:705
```

**3** Start the master agent.

END OF STEPS

For more information about configuring SNMP traps, see "Configuring SNMP Traps for all platforms" (p. 8-25).

### Configuration of SNMP plugins

By default, the Net-SNMP master agent talks the AgentX protocol through the Unix domain socket. However Windows does not have domain sockets. Therefore, the server plugins require a configuration file.

**1** *qddns_snmp_agent.conf* in <*path_of_net-snmp*>*\etc\snmp* directory with the text lines below:

```
##
#Talk to snmpd using TCP at port 705.
#snmpd has to be configued to listen to the same port
agentxSocket tcp:localhost:705
```

Ensure the plugin is in the *%QIPHOME%\lib* directory.

**2** Start the server.

END OF STEPS

### Configuration of SNMP Utilities

**1** Copy the *qddns.mib* file to the <path_of_net-snmp>\share\snmp\mibs directory.

**2** Copy *qddns_snmp.dll* to the *%QIPHOME%/lib* directory.

**3** If present, remove the old *named.mib*.

4 By default, Net-SNMP utilities do not load the enterprise DNS server mibs. Create or modify the general *snmp config* file (<path_of_net-snmp>\etc\snmp\snmp.conf) by adding the appropriate lines below:

```
mibs +QDDNS-SERVER-MIB
```

END OF STEPS

## Configuring SNMP Traps for all platforms

The Lucent DNS server uses AgentX protocol for sending traps. The following policies are used in *snmpd.conf* file for configuration of traps:

```
;
; For sending v2 traps to localhost
trap2sink 127.0.0.1 public
; For sending v2 traps to destination 10.10.4.2
trap2sink 10.10.4.2:162 public

; For sending v2 traps to destination 10.10.4.16
trap2sink 10.10.4.16:162 public

; For sending v1 traps to destination 10.10.4.1
trapsink 10.10.4.1:162 public

;You can send traps to multiple destinations. Add each destination
   seperately.
;trap2sink 10.10.4.2 public also can be used.Default port will be
   used.
```

### SNMP Trap Receiver

1 Create a *snmptrapd.conf* file in the *<path_of_net-snmp>\etc\snmp* directory and add the following lines:

```
disableAuthorization yes
authCommunity log public
```

2 Start the trap receiver.

END OF STEPS

**Note:** The Configuring SNMP Traps and SNMP Trap Receiver procedures are common for all operating systems.

## Verification

### Master Agent

Successful configuration will log something like the following in <path_of_net-snmp>\log\snmpd.log.

```
Turning on AgentX master support.
NET-SNMP version 5.4.2.1
```

If not, you may see the following in <path_of_net-snmp>\log\snmpd.log.

**Warning:** *No access control information is configured.*

It's unlikely this agent can serve any useful purpose in this state.

Run "**`snmpconf -g basic_setup`**" to help you configure the *snmpd.conf* file for this agent.

To test the functionality, send some snmp queries as follows:

```
$ snmpget -v1 -c public localhost sysUpTime.0
$ snmpget -v2c -c public -m ALL localhost sysUpTime.0
```

#### NET-SNMP version 5.4.2.1 Plugins

Successful DNS plugin connection to master agent will log something like the following in the <named_dir>\qddns_snmp.log.

```
2009-08-06 15:29:42 qddns_snmp_agent QDDNS SNMP module 3.0 Build 7
Starting
```

```
2009-08-06 15:29:42 qddns snmp agent Initializing agent

2009-08-06 15:29:42 qddns snmp agent Initializing snmp

2009-08-06 15:29:42 NET-SNMP version 5.4.2.1 AgentX subagent
connected

2009-08-06 15:29:42 qddns snmp agent Initializing dnsServSystem

2009-08-06 15:29:42 qddns snmp_agent Initialing trap data

2009-08-06 15:29:42 qddns snmp_agent Initializing
dnsServConfiguration

2009-08-06 15:29:42 qddns snmp agent Initializing
dnsServStatistics

2009-08-06 15:29:42 qddns snmp agent Initializing dnsServCounters

2009-08-06 15:29:42 qddns snmp_agent Initializing
dnsServCounterTable

2009-08-06 15:29:42 qddnss nmp agent Creating rows for counter
table

2009-08-06 15:29:43 qddns snmp agent Created 4392 rows

2009-08-06 15:29:43 qddns snmp agent going to processing loop
```

If not, you may see a line like the following, indicating an error in the configuration files:

```
2009-08-06 15:28:01 Warning: Failed to connect to the agentx
master agent ([NIL]):
```

### Trap Receiver

Successful configuration will log something similar to the following in <path_of_net-snmp\log\snmpd.log.

NET-SNMP version 5.4.2.1

If not, you may see the following in <path_of_net-snmp>\log\snmptrapd.log.

**Warning:** *no access control information configured.*

This receiver will not accept any incoming notifications.

NET-SNMP version 5.4.2.1.

### Utilities

Successful DNS mib loading and translation will look similar to the following, when running the snmptranslate -Tp -IR dnsServSystem command.

```
# snmptranslate  -Tp -IR dnsServSystem

+--dnsServSystem(1)
```

```
+-- -R-- String    dnsServSystemDescr(1)
|        Textual Convention: DisplayString
|        Size: 0..255
+-- -R-- EnumVal   dnsServSystemStatus(2)
```

Values: other(1), reset(2), initializing(3), running(4)

If not, you may see a line like the following, indicating an error.

```
Unknown object identifier: dnsServSystem
```

### ALU Appliance

There are 2 packages for the appliance. (the qddns server and the qddns-snmp plugin, with mib)

Remove the old proxy statements from the */etc/snmp/snmpd.conf* file.

Modify the */etc/snmp/snmpd.conf* file by adding the following line to enable AgentX master agent support.

> **Note:** The snmp package will have all the default setting, so there is no need to modify anything.

```
master agentx
agentXPerms 755 755 qip qip
```

stop and start snmpd

Running named

Ensure that the path of libqddns_snmp.so is in LD_LIBRARY_PATH environment variable start named:

Successful DNS plugin connection to master agent will log similar to the following in the *<named_dir>\qddns_snmp.log*.

```
2009-08-06 15:29:42 qddns_snmp_agent QDDNS SNMP module 3.2 Build
14 Starting

2009-08-06 15:29:42 qddns snmp agent Initializing agent

2009-08-06 15:29:42 qddns snmp agent Initializing snmp

2009-08-06 15:29:42 NET-SNMP version 5.7.1 AgentX subagent
connected

2009-08-06 15:29:42 qddns snmp agent Initializing dnsServSystem

2009-08-06 15:29:42 qddns snmp_agent Initialing trap data

2009-08-06 15:29:42 qddns snmp_agent Initializing
dnsServConfiguration

2009-08-06 15:29:42 qddns snmp agent Initializing
dnsServStatistics
```

```
2009-08-06 15:29:42 qddns snmp agent Initializing dnsServCounters
2009-08-06 15:29:42 qddns snmp_agent Initializing dnsServCounterTable
2009-08-06 15:29:42 qddnss nmp agent Creating rows for counter table
2009-08-06 15:29:43 qddns snmp agent Created 4392 rows
2009-08-06 15:29:43 qddns snmp agent going to processing loop
```

If not, you may see a line like the following, indicating an error in the configuration files.

```
2009-08-06 15:28:01 Warning: Failed to connect to the agentx master agent ([NIL]):
```

The subagent cannot connect to the master agent. Ensure that the master agent is running with proper agentx configuration.

### Testing SNMP queries

At this point, it is assumed that dns sub agents have successfully connected to master agent (snmpd). That means SNMP queries by dns OID should succeed. For example, to send query for dnsServSystem MIB variable:

```
bash-3.00# snmpwalk -v2c -c public 127.0.0.1 dnsServSystem
QDDNS-SERVER-MIB::dnsServSystemDescr.0 = STRING: "QDDNS 5.1 Build 16"
QDDNS-SERVER-MIB::dnsServSystemStatus.0 = INTEGER: running(4)
```

However, it is convenient to send queries by using MIB variables than OIDs. There are many ways to make MIB files available to Net-SNMP applications. For details, please look at the document TUT:Using and loading MIBS.

To verify that the MIB files are available to Net-SNMP clients, type the following:

```
$ snmptranslate  -Tp -IR dnsServSystem
```

You should see the following output:

```
+--dnsServSystem(1)
+-- -R-- String    dnsServSystemDescr(1)
|         Textual Convention: DisplayString
|         Size: 0..255
+-- -R-- EnumVal   dnsServSystemStatus(2)
```

Values: other(1), reset(2), initializing(3), running(4)

```
snmptranslate  -Tp -IR dnsServSystem
```

Now send some SNMP queries:

```
bash-3.00# snmpwalk -v2c -c public 127.0.0.1 vitalqipdnsTrapTable
QDDNS-SERVER-MIB::vitalqipDnsTrIndex.1 = INTEGER: 1
```

```
  QDDNS-SERVER-MIB::vitalqipDnsTrSequence.1 = Counter32: 1
  QDDNS-SERVER-MIB::vitalqipDnsTrId.1 = INTEGER: monitor(1)
  QDDNS-SERVER-MIB::vitalqipDnsTrText.1 = STRING: "Lucent DNS
  started"
  QDDNS-SERVER-MIB::vitalqipDnsTrPriority.1 = INTEGER: inform(1)
  QDDNS-SERVER-MIB::vitalqipDnsTrClass.1 = INTEGER: 1
  QDDNS-SERVER-MIB::vitalqipDnsTrType.1 = INTEGER: 1
  QDDNS-SERVER-MIB::vitalqipDnsTrTime.1 = Counter32: 1264765445
  QDDNS-SERVER-MIB::vitalqipDnsTrSuspect.1 = STRING: "qasn35"
```

Use snmp table to see the exact number of rows in the table.

```
# snmptable -v 2c -c public 127.0.0.1 vitalqipDnsTrapTable
SNMP table:
QDDNS-SERVER-MIB::vitalqipDnsTrapTable

vitalqipDnsTrIndex vitalqipDnsTrSequence vitalqipDnsTrId
   vitalqipDnsTrText vitalqipDnsTrPriority vitalqipDnsTrClass
   vitalqipDnsTrType vitalqipDnsTrTime vitalqipDnsTrSuspect
   vitalqipDnsTrDiagId vitalqipDnsTrIteration
monitor "Lucent DNS started" inform 1
1262788084             "qasn95" 1
```

### Policies for SNMP Plugin

The sample *named.pcy* file appears as shown below:

```
Alcatel-Lucent named Policy File
; Syntax of this file is key=value
; ; Any policies before the first section are considered global to
   all the
; sections. The same policy value in a section will override the
   one in the
; global section.
;
; A comment line starts with
; or # as first character
;-------------------------------------------------------------
;===========================================
; Global section
;===========================================
;====================================================
; The policy information of named follows
;====================================================
[Named]
;====================================================
; The policy information of snmp sub agent follows
;====================================================
   [SnmpSubAgent]
;;
```

```
; SnmpOn: Yes/No
; If yes, the snmp plugin will be loaded. Default is Yes.
   SnmpOn=Yes

;;
; LogFile: Filename/Path
; The path or name of the log file for snmp sub agent. Forward or
   back slash
; can be used for path in Windows.
; There are four special LogFile names: syslog, stdout, stderr
; If the name is syslog, stdout or stderr, the log messages will
   be written to
; Syslog, stdout and stderr respectively.If the policy is
   commented out,
; the plugin will try to write log to $QIPHOME/log/qdhcp_snmp.log,
; if the directory does not exists, it will try
; to write log to Syslog otherwise.
LogFile="h:/qddns_snmp.log"

;;
; TruncateLog: Yes/No
; If Yes, the log file for the sub agent will be truncated at
   startup time.
; Default is Yes.
TruncateLog=Yes
```

**Note:** On Solaris servers, the LogFile setting in */etc/named.pcy* must use the full path for the log file (for example LogFile=*/opt/qip/log/qddns_snmp.log*). If "$QIPHOME" is used in place of "*/opt/qip*" in the LogFile setting in */etc/named.pcy*, the qddns_snmp log file will never get created.

## Frequently Asked Questions

- **It does not work, what should I do?**

Look at qddns_snmp_agent.log file. Make sure the sub agent is connected to the master agent using AgentX protocol. Run the master agent in foreground to watch the log to stderr: snmpd -f -Dagetnx -L

**Sub agent is connected to master agent but none of the dns mib variables are returned, what should I do?**

The snmpd.conf file has some kind of access control set which is preventing the master agent to serve OIDs below certain configured OID. To verify that, replace the snmpd.conf file with the sample_snmpd.conf file or create a minimal conf file (read next question), restart snmpd and see if it works.

**Note:** On RH 5.x, the default /etc/snmp/snmpd.conf file restricts snmp queries to system + hrSystem. So, after dns sub agent is connected to master agent, if you query for any dns MIB variable you get a message saying No more variables left in this MIB View.

- **What does a minimal snmpd.conf file looks like?**

```
# The simplest snmpd.conf file without any sort of real access
  control
rocommunity public
master agentx
```

- **How do I know that I am using the latest MIB files?**

The MIB definitions are changed to QDDNS-SERVER-MIB for dns servers. So look at the output of the snmpget or snmpwalk and check the first word for the MIB definition.

- **How do the sub agents (named, dhcpd) communicate with the master agent (snmpd)?**

The SNMP sub-agent for DNS and DHCP servers uses AgentX protocol (RFC 2741) for communication with the master agent (snmpd). There are two sides to an AgentX connection and they need to agree about which socket address to use. If you are using a different socket, the master agent and sub-agent must be configured properly. Refer the snmp_config man page for directories where Net-SNMP looks for various configuration files. For the master agent, use AgentXSocket in the *snmpd.conf* file. For the DNS sub-agent, use AgentXSocket in the *qddns_snmp_agent.conf* file. For the DHCP sub-agent, use AgentXSocket in the *qdhcp_snmp_agent.conf* file. The default location of these files is *$HOME/.snmp*. However, use the *SNMPCONFPATH* environment variable to specify list colon separated directories.

**Note:** You do not need the files for sub-agents in UNIX as default values will work. They are required in Windows, as by default snmpd uses the UNIX domain socket that is not supported on Windows.

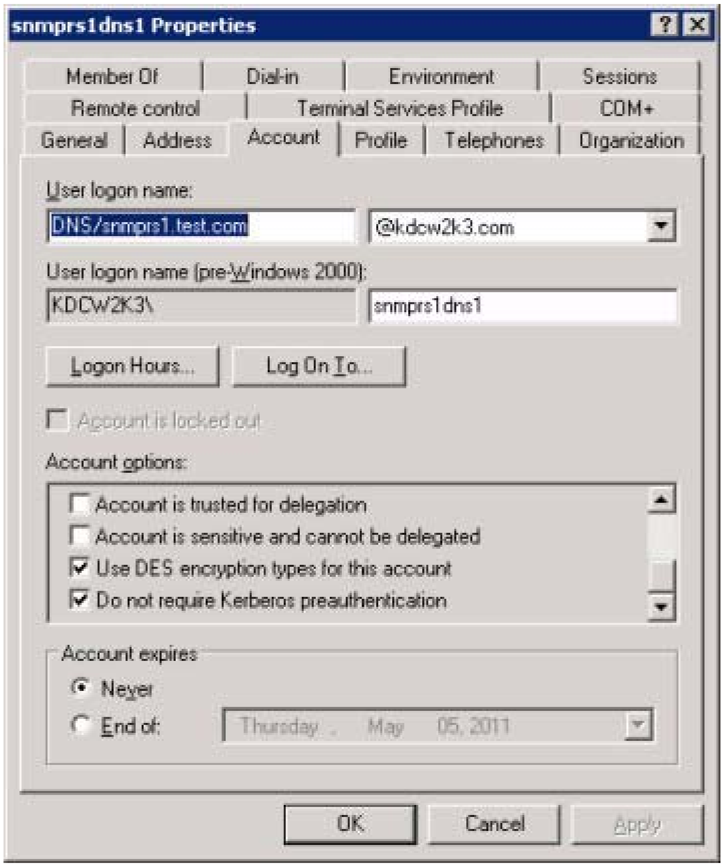
# Kerberos Notes for LDNS 5.1 Build 8 and later

Secure updates may fail, as LDNS 5.1 Build 8 and later has new Kerberos libraries on Unix platforms. If secure updates fail, perform the following steps.

1 Add the following to the DNS server's *krb5.conf* file.

```
[libdefaults]
allow_weak_crypto = true
```

**2** For the DNS Server's Windows account, click the **Account** tab and select the options **Use DES encryption types for this account** and **Do not require Kerberos preauthentication**.



User logon name: DNS/snmprs1.test.com @kdcw2k3.com

User logon name (pre-Windows 2000): KDCW2K3\ snmprs1dns1

□ Account is locked out

Account options:

□ Account is trusted for delegation
□ Account is sensitive and cannot be delegated
☑ Use DES encryption types for this account
☑ Do not require Kerberos preauthentication

Account expires

● Never
○ End of: Thursday , May 05, 2011

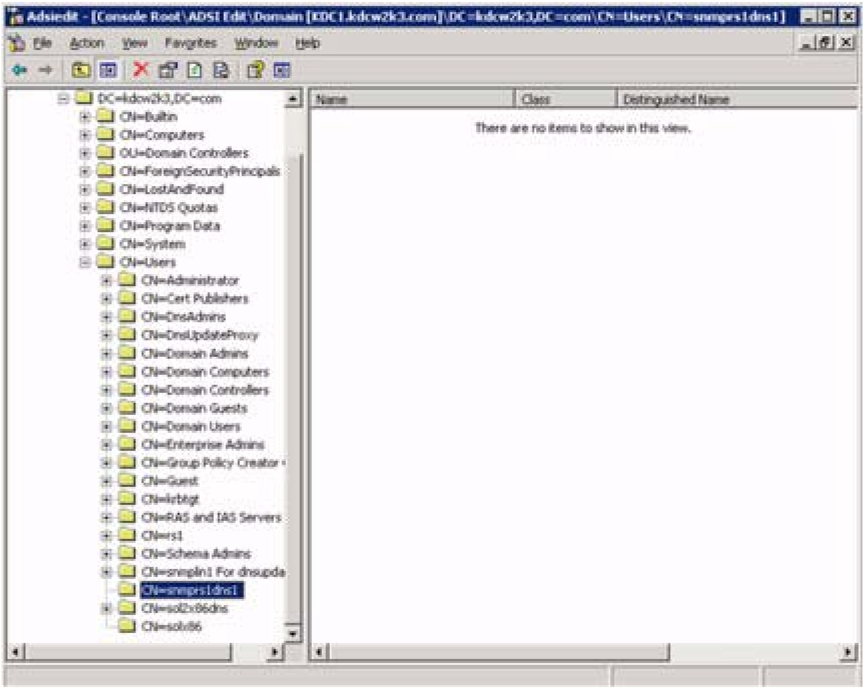
**3** You may see the following error in *named*.

```
"Message size is incompatible with encryption type"
```

To resolve this error, do the following on the Windows KDC machine.

1. Get ADSIEdit from Microsoft's website http://technet.microsoft.com/en-us/library/cc773354(WS.10).aspx.
2. Install ADSIEdit.
3. Run ADSIEdit.

4. Select **UserName** under **Domain->Users Path**, as shown below.

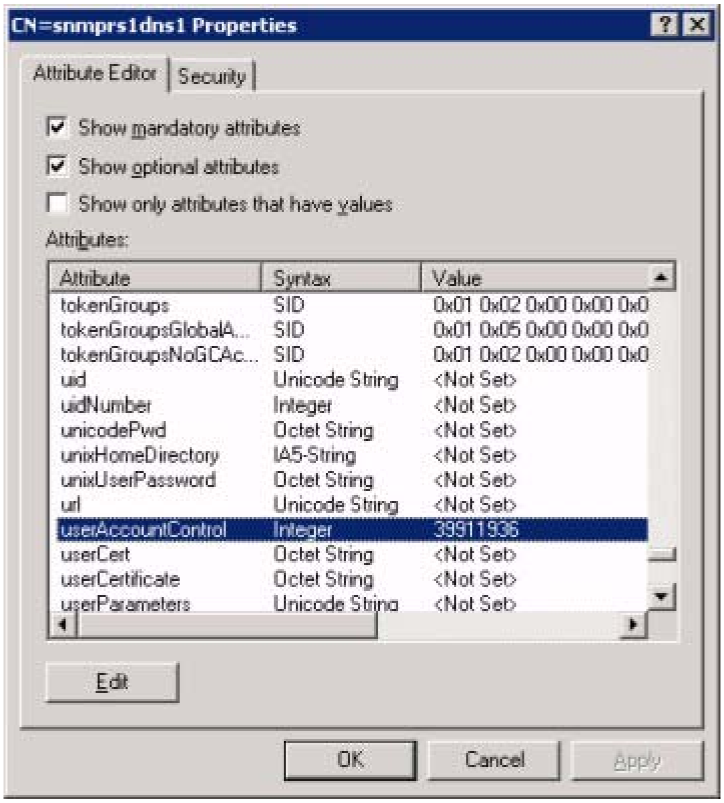


Adsiedit - [Console Root\ADSI Edit\Domain [KDC1.kdcw2k3.com]\DC=kdcw2k3,DC=com\CN=Users\CN=snmprs1dns1]

There are no items to show in this view.

5. Right-click **User** and select **Properties**.

6. Scroll down to the **Attribute Editor** tab and select the attribute **userAccountControl**, as shown below.



☑ Show mandatory attributes

☑ Show optional attributes

□ Show only attributes that have values

Attributes:

| Attribute | Syntax | Value |
|---|---|---|
| tokenGroups | SID | 0x01 0x02 0x00 0x00 0x0 |
| tokenGroupsGlobalA... | SID | 0x01 0x05 0x00 0x00 0x0 |
| tokenGroupsNoGCAc... | SID | 0x01 0x02 0x00 0x00 0x0 |
| uid | Unicode String | <Not Set> |
| uidNumber | Integer | <Not Set> |
| unicodePwd | Octet String | <Not Set> |
| unixHomeDirectory | IA5-String | <Not Set> |
| unixUserPassword | Octet String | <Not Set> |
| url | Unicode String | <Not Set> |
| userAccountControl | Integer | 39911936 |
| userCert | Octet String | <Not Set> |
| userCertificate | Octet String | <Not Set> |
| userParameters | Unicode String | <Not Set> |

7. Add **33554432** (hex 0x2000000) to the current value.
8. Click **OK**.
9. Restart (if required).

END OF STEPS