VitalQIP® DNS/DHCP & IP Management Software

Appliance Management Software (AMS) | Release 1.6

Appliance Packages Configuration Guide

190-409-116R1.6
September 2010
Issue 2

Licenses

Refer to Appendix C, “Third party software license statements” in the *VitalQIP Release 7.2 Installation Guide* (190-409-043R7.2PR2) for a complete description of all software licenses used to develop this product.

Contents

About this document

Purpose

This Configuration Guide describes the package configurations for appliances maintained in the AMS GUI. Refer to this preface for the audience, organization, and typographical conventions used in the manual. The preface also describes the package contents, how to order additional manuals, and how to obtain technical support.

Reason for reissue

The following table lists the changes to the *Appliance Packages Configuration Guide*.

Issue	Feature name	Description	Feature impact
2		Added note after step 4.	"Modify snmpd.conf" (p. 1-55)
2	qdhcp-snmp package	Package information to activate the DHCP SNMP add-on module	"qdhcp-snmp" (p. 1-49)
2	qddns-snmp package	Package information to activate the DNS SNMP add-on module	"qddns-snmp" (p. 1-32)
1	qddns-ha	Upgrading DNS-HA from very old versions results in unpredictable behavior. Fixes HELIO00005892.	1-43
1	SelfReg	Added SelfReg configuration details	"SelfReg configuration" (p. 1-72)
1	ENUM 1.4	Added ENUM 1.4 configuration details	"enum-1.4" (p. 1-76)
1	LDRM Server	Added LDRM Server configuration details	"ldrm-server" (p. 1-77)
1	LDRM Remote	Added LDRM Remote configuration details	"ldrm-remote" (p. 1-79)

Issue	Feature name	Description	Feature impact
1	AMS GUI https instructions	Documented information about configuring ESM to use SSL for AMS server. Fixes HELIO00005885.	“Configure SSL between AMS and ESM/AMM” (p. 2-19)
1	Debug information	Documented the CLI commands used for debugging purposes.	“Debug information” (p. 2-22)

Intended audience

This manual is intended for Appliance Management Software users who plan to manage and administer an IP network address infrastructure. The reader is expected to understand basic networking concepts and have a working knowledge of the operating system that Appliance Management Software is running on. Two types of groups interact with Appliance Management Software:

- **Appliance Management Software administrators -** The Information Technology (IT) professionals who install, configure, and administer the Appliance Management Software product.
- **Appliance Management Software users -** The IT professionals who use Appliance Management Software as a service-level monitoring and capacity tool.

How to use this document

This manual is organized as follows:

Chapter 1, “Appliance packages”

This chapter describes the packages that are available to be deployed onto appliances using AMS. Generic configuration and debugging information is described.

Chapter 2, “ESM appliance package configuration”

This chapter describes how to customize ESM appliance configuration files, as well as how to deploy ESM Disaster Recovery and High Availability.

Appendix A, “VitalQIP policy files”

This appendix describes the policies that are in the condensed *qip.pcy* file that is included in the remote and enterprise server packages.

Appendix B, “Password encryption”

This appendix describes the **`qip-crypt`** CLI that is used to encrypt the **qipman** password.

Appendix C, "Appliance Install Manager"

This appendix describes the **aim** command, for use in troubleshooting packages installed on an appliance.

Conventions used

The following table lists the typographical conventions used throughout this manual.

Convention	Meaning	Example
Trebuchet bold	Names of items on screens.	Select the **Client** check box.
	Names of buttons you should click.	Click **OK**.
Courier	Output from commands, code listings, and log files	`# Name: Share shared-network _200_200_200_0`
Courier bold	Input that you should enter from your keyboard.	Run the following command: **c:\setup.exe**
	Names of commands and routines	The **qip_getapp1lst** routine returns the entire list of existing applications.
Courier bold italic	Input variable for which you must substitute another value. The angle brackets also indicate the value is a variable.	**isql -U sa -P *<sa_password>***
Times bold	Names of keys on the keyboard to be pressed.	Press **Enter** to continue.
	Uniform Resource Locators (URLs)	The VitalQIP product site can be found at http://www.alcatel-lucent.com/wps/portal/products/.
Times italics	Manual and book titles.	Refer to the *VitalQIP User's Guide*.
	Directories, paths, file names, and e-mail addresses.	A symbolic link must be created from */etc/ named.conf* that points to *named.conf*.
Times bold italic	Emphasis	***Read-only***. The name of the service element.

Related information

The following documents are referenced in this manual:

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

  This guide describes planning and configuring your network, information about the VitalQIP interface, advanced DNS and DHCP configurations, and troubleshooting.

- *VitalQIP User's Guide* (part number: 190-409-068)

  This guide describes how to set up and use the VitalQIP user interface on Windows and UNIX platforms.
- *VitalQIP AMM 1000 Quick Start Guide* (part number: 190-409-088)

  This quick start guide describes how to set up an AMM 1000 appliance and connect it to the network.
- *VitalQIP AMM 5000 Quick Start Guide* (part number: 190-409-117)

  This quick start guide describes how to set up an AMM 5000 appliance and connect it to the network.
- *VitalQIP ESM 1000 Quick Start Guide* (part number: 190-409-118)

  This quick start guide describes how to set up an ESM 1000 appliance and connect it to the network.
- *VitalQIP ESM 5000 Quick Start Guide* (part number: 190-409-119)

  This quick start guide describes how to set up an ESM 5000 appliance and connect it to the network.
- *VitalQIP AMS 1000 Quick Start Guide* (part number: 190-409-093)

  This quick start guide describes how to configure an AMS 1000 appliance on which the appliance vendor has preinstalled AMS.
- *VitalQIP Appliance Management Software User's Guide* (part number: 190-409-089)

  This guide describes how to set up appliances and administer them with AMS.
- *VitalQIP Appliance Manager Installation & Configuration Guide* (part number: 190-409-094)

  This guide describes how to install and configure the VitalQIP Appliance Management Software.

Product Training Support

Alcatel-Lucent University offers cost-effective educational programs that support the VitalQIP product. Our offerings also include courses on the underlying technology for the VitalQIP products (for example, DNS and DHCP). Our classes blend presentation, discussion, and hands-on exercises to reinforce learning. Students acquire in-depth knowledge and gain expertise by practicing with our products in a controlled, instructor-facilitated setting. If you have any questions, please contact us at 1 888 LUCENT8, option 2, option 2.

Technical support

If you need assistance with Appliance Management Software, you can contact the Welcome Center for your region. Contact information is provided in the following table.

Region	Address	Contact information
North America	Alcatel-Lucent 400 Lapp Road, Suite 101 East Whiteland, PA 19355 USA	Phone: 1-866-LUCENT8 (582-3688) Option 1, Option 2 Web: ***www.alcatel-lucent.com/support***
Europe, Middle East, and Africa	Alcatel-Lucent Voyager Place Shoppenhangers Road Maidenhead Berkshire SL6 2PJ UK	Phone: 00 800 00 LUCENT or +353 1 692 4579 E-mail: *emeacallcenter@alcatel-lucent.com* Web: ***www.alcatel-lucent.com/support***
Central and South America	Alcatel-Lucent Brasil S/A Avenida Marginal Direita Anchieta, 400 - Km 11,5 CEP: 04182-901 - Jardim Santa Cruz - Sao Paulo - SP Brazil	Phone: 0800 89 19325 or +55 11 3205 7626 For other local CALA numbers, consult the web site **http://www.alcatel-lucent.com/support** or contact your local sales representative.
Asia Pacific	Alcatel-Lucent Australia 280 Botany Road Alexandria NSW 2015 Australia	Phone: 1800-458-236 (toll free from within Australia) (IDD) 800-5823-6888 (toll free from Asia Pacific - China, Hong Kong, Indonesia, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, and Thailand) (613) 9614-8530 (toll call from any country) E-mail: *apactss@alcatel-lucent.com*

How to order

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

How to comment

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

1 Appliance packages

Overview

Purpose

This chapter describes the packages that are available to be deployed onto appliances using AMS. Generic configuration and debugging information is described.

Different versions of the packages are released as they become available. Information on specific package versions is included in the *AMS Release Notes*.

Contents

This chapter covers these topics.

Packages

Overview

Purpose

Appliance packages are delivered as *lpf* files. The appliances support several package operations including install, update (upgrade/downgrade), and remove.

Naming

A package filename includes the name, version, and architecture of the contents, for example, *qddns-4.1.11-2.i386.lpf*.

Versioning

The version string of a package is used to identify the release contained in a package.

For the given example, the entire version string is "4.1.11-2" with 4 being the major number, 1 the minor number, 11 the build number, and 2 the revision. The major, minor, and build number are determined by the upstream release of the application -- here *qddns*. The revision number represents a versioning of the package.

With each new upstream release or build, the application version number is changed.

The revision number is always initially 1. The revision number is incremented whenever a package is reissued. Changes to the application are not reflected in the revision number. When the application version is updated, the revision number is reset to 1.

Architecture

The package architecture describes the architecture of the binary executables contained in the package. In the previous example, the architecture was “i386”. Other valid architectures are “x86_64” and “noarch”. The “noarch” value identifies a package that does not contain binaries compiled for a specific platform. An example might be scripts or a data payload.

> **Note:** The architecture of the package is not necessarily the same as the architecture of a machine. For example, a 64-bit machine may be capable of executing 32-bit binaries

Firewall configuration

Customers with appliances that cross firewalls need to open relevant ports, based on individual package requirements. Information on individual services can be found in the documentation for those packages.

Current packages

The following table lists the types of packages that are available for AMS. The packages should be downloaded from the Alcatel-Lucent ALED website. Alcatel-Lucent releases updated versions of these package types as they become available.

Table 1-1 Appliance Manager packages

Package name	Description	Dependency
ad-remote	Contains the modules and configuration files that comprise the AutoDiscovery 2.3 Remote Agent Server.	jre-1.6.0-sun
ad-server	Contains the modules and configuration files that comprise the AutoDiscovery Server.	jre-1.6.0-sun vitalqip7.2-enterprise system-patch
bootstrap	Upgrades an AMM-1 based appliance to an AMM-2 based appliance.	AMM1 Image
jre-1.4.2-sun	Contains Sun's "java runtime" executable.	None
jre-1.5.0-sun	Contains Sun's "java runtime" executable.	None
jre-1.6.0-sun	Contains Sun's "java runtime" executable.	None
ntp-server	Contains the modules that comprise NTP Server.	None
probe-dhcp	Contains the DHCP probe executables and configuration files.	probe-server
probe-dns	Contains the DNS probe executables and configuration files.	probe-server
probe-server	Contains the probe-run and probe-results CLIs and the Probe service.	jre-1.6.0-sun
qddns	Contains the configuration files to run Lucent DNS 4.X on the appliance.	vitalqip-remote **Note:** Works with any vitalqip-remote package: 6.2, 7.0, 7.1 and 7.2.
qddns-anycast	Contains the configuration files that provide dynamic anycast support for an appliance cluster configuration, using an Interior Gateway Protocol (IGP) such as Open Shortest Path First (OSPF).	qddns
qddns-ha	Contains the configuration files to run DNS High Availability on appliance pairs.	qddns

Package name	Description	Dependency
qddns-userexits	Contains the configuration files to run DNS user exits on the appliance.	qddns
qdhcp	Contains the configuration files to run Lucent DHCP 5.X on the appliance.	vitalqip-remote **Note:** Works with any vitalqip-remote package: 6.2, 7.0,7.1 and 7.2.
qdhcp-manager	Contains the configuration files that are needed to activate the DHCP Configuration Manager on the appliances. **Note:** The dhcp-manager is a separately licensed package.	qdhcp system-patch(>20081105-0)
qdhcp-userexits	Contains the configuration files to run DHCP user exits on the appliance.	qdhcp
qip-snmp	Activates the VitalQIP SNMP add-on module for DHCP and DNS.	vitalqip-remote snmp-server **Note:** Works with any vitalqip-remote package: 6.2, 7.0, 7.1 and 7.2.
snmp-server	Installs the standard Redhat SNMP daemon from **net-snmp.org**.	None
sybase	Contains the Sybase database modules required to run the VitalQIP 6.2, 7.0, and 7.1 Enterprise Server.	None
sybase64	Contains the 64-bit Sybase database modules that are required to run the VitalQIP 7.2 Enterprise Server.	None
system-patch	Contains all “OS”-related patches for AMM1-based appliances.	AMM1-based appliance
system-patch2	Contains all “OS”-related patches for AMM2-based appliances.	AMM2-based appliance
tftp-server	Contains the modules that comprise TFTP Server.	None
vitalqip6.2-remote	Contains the modules and configuration files that comprise the VitalQIP 6.2 Remote Server.	jre-1.4.2-sun

Package name	Description	Dependency
vitalqip7.0-remote	Contains the modules and configuration files that comprise the VitalQIP 7.0 Remote Server.	jre-1.5.0-sun
vitalqip7.1-enterprise	Contains the modules and configuration files that comprise the VitalQIP 7.1 Enterprise Server.	jre-1.6.0-sun, sybase
vitalqip7.1-remote	Contains the modules and configuration files that comprise the VitalQIP 7.1 Remote Server.	jre-1.6.0-sun
vitalqip7.2-enterprise	Contains the modules and configuration files that comprise the VitalQIP 7.2 Enterprise Server.	jre-1.6.0-sun sybase64
vitalqip7.2-remote	Contains the modules and configuration files that comprise the VitalQIP 7.2 Remote Server.	jre-1.6.0-sun

ad-remote

Purpose

The **ad-remote** package contains the modules and configuration files that comprise the AutoDiscovery Remote Agent Server.

Before you begin

- To run the AutoDiscovery Remote CLIs, the AutoDiscovery environment needs to be sourced, as follows.

```
cd /opt/autodisc/etc
. ./adrc
```

- The **ad_client/canceljob** CLI only works for the Network Data Extractor (NDE).

Configuration

The following configuration files are supported by the **ad-remote** package.

- */opt/autodisc/config/AdAgentServer.properties*
- */opt/autodisc/config/AdAgentServerLog4j.properties*
- */opt/autodisc/config/AgentServerWrapper.conf*
- */opt/autodisc/config/AutoDiscoveryAgent.properties*
- */opt/autodisc/config/ReqHdlr_log4j.properties*
- */opt/autodisc/config/ad.cer*
- */opt/autodisc/config/keystore_ad*
- */opt/autodisc/config/truststore_ad*
- */opt/autodisc/lib/nde/nde.properties*

To configure the *AdAgentServer.properties* file, follow these steps.

1 Open the *AdAgentServer.properties* file in a text editor.

2 Locate the **DirectorHost** property and specify the IP address of the AutoDiscovery Server:

```
DirectorHost=<ip_address>
```

END OF STEPS

This is the minimal configuration required for AutoDiscovery Remote package. For further information on AutoDiscovery configuration files, refer to Chapter 7, “AutoDiscovery Properties Files” in the *AutoDiscovery User’s Guide* (190-409-065).

Important! Do not modify the default port settings in the configuration files since only the specific AutoDiscovery services ports are allowed by the appliance firewall rules.

Log files

The following AutoDiscovery services log files are located in the */opt/autodisc/log* directory:

- *ad_remote_agent.log*
- *reqhandler.log*

ad-server

Purpose

The **ad-server** package contains the modules and configuration files that comprise the AutoDiscovery Server.

Before you begin

To run the AutoDiscovery CLIs, both the VitalQIP environment and the AutoDiscovery environment need to be sourced, since the AutoDiscovery CLIs use some of the VitalQIP CLIs.

```
cd /opt/qip/etc
. ./qiprc
cd /opt/autodisc/etc
. ./adrc
```

AutoDiscovery Server activation

To support AutoDiscovery, ensure that the license key you obtain and deploy has AutoDiscovery enabled. For activation information, refer to "Activate license key on an ESM appliance" (p. 2-5).

Configuration

The following configuration files are supported by the **ad-server** package.

- */opt/autodisc/config/AutoDiscovery.properties*
- */opt/autodisc/config/DBupdate_log4j.properties*
- */opt/autodisc/config/Dbuwrapper.conf*
- */opt/autodisc/config/ObjectDeviceType.properties*
- */opt/autodisc/config/ReqHdlr_log4j.properties*
- */opt/autodisc/config/ad.cer*
- */opt/autodisc/config/keystore_ad*
- */opt/autodisc/config/truststore_ad*
- */opt/autodisc/defaultroot/conf/ADservlets.properties*
- */opt/autodisc/defaultroot/conf/ADservlets_log4j.properties*
- */opt/autodisc/lib/diff/config/DiffEngine.properties*
- */opt/autodisc/lib/diff/config/log4j.properties*
- */opt/autodisc/lib/nde/nde.properties*
- */opt/autodisc/tomcat/conf/server.xml*

Important! Do not modify the default port settings in the above configuration files since only the default AutoDiscovery services ports are allowed by the appliance firewall rules.

AutoDiscovery integration with VitalQIP web client

The AutoDiscovery Server web interface can be accessed from the VitalQIP web client interface by selecting **Add-Ons|AutoDiscovery**. To integrate the AutoDiscovery web interface with the VitalQIP web client interface, the */opt/qip/web/conf/qip.properties* configuration file needs to be modified and deployed to the ESM appliance. The *qip.properties* property file is shipped as part of the **`vitalqip7.2-enterprise`** package.

For further information on the *qip.properties* file, refer to Chapter 18 in the *VitalQIP Administrator Reference Manual*.

qip.properties configuration

To configure the *qip.properties* file so that the AutoDiscovery web interface is integrated with the VitalQIP web client, follow these steps.

1. In AMS, locate the appliance on which the **`vitalqip7.2-enterprise`** package is installed and expand the **Config Files** folder.

   Result: A list of Enterprise Server configuration files opens.

2. Select the **/opt/qip/web/conf/qip.properties** file.

   Result: The Config File Properties pane opens.

3. Click **Modify**.

   Result: The Config File Editor pane opens.

4. Enter the URL for the AutoDiscovery server, as well as the current version number.

   `auto_discovery.url = http://<ip address of autodiscovery server>:8082`

   `auto_discovery.version = 2.3`

5 If you wish to enter a comment, enter up to 255 alphanumeric characters in the **Comments** field.

6 Click **Deploy**.

Result: A dialog box opens with the message **Config File Deployed**.

7 Click **OK**.

Result: The updated *qip.properties* file is deployed to the appliance and all services are started.

8 Confirm that the revised *qip.properties* file was deployed successfully by bringing up the VitalQIP Web Client GUI on the ESM and selecting **Links|AutoDiscovery**.

END OF STEPS

Log files

The following AutoDiscovery services log files are located in the */opt/autodisc/log* directory:

- */opt/autodisc/log/ADDbupdate.log*
- */opt/autodisc/log/Dbuwrapper.log*

The AutoDiscovery web interface logs are located in */opt/autodisc/data/ADgui.log*.

The Tomcat server logs are located in */opt/autodisc/tomcat/logs/catalina.out*.

ad-server upgrades

If you wish to preserve older AutoDiscovery-related data (such as Profiles) during an AutoDiscovery Server package upgrade, do not delete the */opt/autodisc* folder from the appliance.

bootstrap

Purpose

The **bootstrap** package upgrades an AMM1-based appliance that runs on Red Hat Linux 4 (VitalQIP AM Release 1.4 and earlier) to an AMM2-based appliance that runs on Red Hat Linux 5 (VitalQIP AM Release 1.5 and above).

Before you begin

- The **bootstrap** package may only be assigned to an AMM1-based appliance that runs on Red Hat Linux 4.
- The **bootstrap** package should be deployed with a minimal set of packages, for example, just the **system-patch** package.
- The **bootstrap** package reinitializes the appliance. All existing packages and data on the machine are overwritten. Previously installed packages and customized configuration can be reinstalled from the AMS history once the upgrade is complete.
- The previous appliance configuration should be intact ***except*** for the user account password. This will need to be reset from AMS.

Configuration

To upgrade an AMM1-based appliance that runs on Red Hat Linux 4 to an AMM2-based appliance that runs on Red Hat Linux 5, follow these steps.

1. Download the **bootstrap** package and base image (*amm-base-20090715-1.tar.bz2*) from ALED.
2. Copy the base image to the *$AMSHOME/download* directory on the AMS machine.
3. Rename the file (or link it) to *amm-base.tar.bz2*.
4. Assign and deploy the **bootstrap** package on the appliance that is being upgraded.

   Result: The bootstrap environment is installed in */boot*.
5. Reboot the appliance and start the bootstrap environment.

   Result: The bootstrap process runs without user intervention, as follows.

a. All required configuration is validated.

b. The AMM2 software *amm-base.tar.bz2* is downloaded from the AMS. The appliance is rebooted back into the existing AMM1 environment.

Note: If any step fails, the upgrade halts. In cases of recoverable failure, for example, when the image cannot be downloaded from AMS, the appliance reboots back to the AMM1 environment.

c. The bootstrap environment proceeds by initializing new file systems.

d. Once the file systems are initialized, they are mounted and the AMM2 software is extracted. The new system is configured with the existing appliance configuration.

e. After configuration is complete, the appliance reboots and the AMM2 software is ready. The appliance version stored by the AMS has been updated.

Logging

If a syslog host is configured on the appliance, bootstrap logging is sent there. Otherwise, the console is the output destination. Also, in the event of a recoverable failure, a */boot/bootstrap.log* is placed in the original AMM1 installation.

jre-1.4.2.sun

Purpose

The **`jre`** package is Sun's Java runtime executable that is delivered independent of **`vitalqip`** packages. It is required to run VitalQIP Remote Services.

Configuration

None.

Log files

None.

jre-1.5.0.sun

Purpose

The **`jre`** package is Sun's Java runtime executable that is delivered independent of **`vitalqip`** packages. It is required to run VitalQIP Remote Services.

Configuration

None.

Log files

None.

jre-1.6.0.sun

Purpose

The **`jre`** package is Sun's Java runtime executable that is delivered independent of **`vitalqip`** packages. It is required to run VitalQIP Enterprise and Remote Services.

Configuration

None.

Log files

None.

ntp-server

Purpose

The **ntp-server** package contains the modules that comprise the Network Time Protocol (NTP) server. The Network Time Protocol provides time synchronization between computers over a network.

Configuration

The default configuration only has a local time source, which provides no time synchronization.

Time source: internal server or pool.ntp.org server

To enable synchronization, an appliance requires network access to an NTP server. You may use internal NTP servers available within your company, or publicly available ones provided by the **pool.ntp.org** project. To use **pool.ntp.org** servers, add the following lines to the *ntp.conf* file.

```
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org
```

By specifying multiple servers you provide additional redundancy.

Time source: AMS server

Alternatively, you can configure the NTP server to use the AMS server as a time source.

server *1.2.3.4*

Where ***1.2.3.4*** is replaced with the IP address of the AMS server.

By default, an appliance attempts to synchronize the local clock at boot with the configured AMS. Additionally, by using the AMS as the configured NTP server you ensure that all appliances remain synchronized after startup.

> **Note:** By default, the **ntpd** service is not running after AMS is installed. The **ntpd** service has to be started manually.

An appliance that is running NTP can also act as a time source for other machines. The default *ntp.conf* allows any host to sync with the appliance.

To prevent all machines from accessing the NTP server without explicit configuration, the default settings,

```
restrict default nomodify notrap noquery
restrict -6 default nomodify notrap noquery
```

should be changed to:

```
restrict default ignore
restrict -6 default ignore
```

To allow client machines on the 192.168.1.0/24 network to query and sync with the appliance, the following line should be in *ntp.conf*.

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

Log files

The NTP server logs to syslog. By default, a log message is placed in the system log file */var/log/messages*.

probe-dhcp

Purpose

The **probe-dhcp** package provides the configuration file that permits the following tests to be run:

- Grant Lease test (**grantlease**)
- Renew Lease test (**renewlease**)
- Verify Servers test(**verifyservers**)

Except for the Verify Servers test, all tests verify the health of the DHCP service on the local host. The DHCP Probe acts as a DHCP client simulator for all tests.

Ports

All messages from DHCP Probe to DHCP service are directed to DHCP server UDP port (67). Depending on the test, the probe receives responses on either DHCP server UDP port (67) or DHCP client UDP port (68).

Co-located DHCP client and DHCP service

When DHCP client and VitalQIP DHCP service are co-located on same server, the VitalQIP DHCP service requires the following conditions to be met for a lease to be granted to the client:

- The DHCP service is configured with **ListenOnLoopback** policy set to true and the **DHCPSocketAddr** policy is not defined.

- The DHCP service is configured to give out leases for the requests from subnet of IP address specified in **probeIpAddress** property.

  Note: Since the grant lease test and the renew lease test are run against the local DHCP service, the VitalQIP DHCP service must be configured as mentioned above for these tests to pass.

Package components

For the Grant Lease test and the Renew Lease test, the DHCP probe acts as a relay agent with giAddr set to the **probeIpAddress** property and unicasts requests to the local DHCP service on the loopback address (127.0.0.1).

Grant Lease test

Grant Lease test verifies that the local DHCP service is able to grant leases. The DHCP Probe acts as a DHCP client simulator and follows the DHCP DORA process to obtain a lease from the service running on the local host. Once the lease is obtained, the lease is released. If a lease cannot be obtained, the test fails.

Renew Lease test

Renew Lease test verifies that the local DHCP service is able to renew leases. The DHCP Probe acts as a DHCP client simulator. It runs the steps in the Grant Lease test to obtain the lease. Once the lease is obtained, the lease is renewed and then the lease is released. If a lease cannot be obtained or renewed, the test fails.

When the DHCP Probe is configured to run both Grant Lease and Renew Lease tests, the Grant Lease test is run first and the lease obtained is kept until the end of Renew Lease test.

Verify Servers test

The Verify Servers test verifies that the list of DHCP servers is up and responding to the lease requests. An administrator needs to specify the list of DHCP servers to verify in the **`verifyServers`** property. The local Lucent DHCP server can be specified using the loopback address `127.0.0.1`.

The DHCP probe unicasts a DISCOVER message and waits for responses. If all expected DHCP servers respond before the timeout, the test succeeds. If at least one DHCP server does not respond, the test fails.

Configuration

The DHCP Probe configuration is defined with properties set up in */opt/probe/conf/probe-dhcp.properties*, as described in the following table.

Table 1-2 DHCP Probe configuration properties

Property	Default	Description
`tests`	**`grantlease`**	Defines the list of DHCP tests to run. Allowed values are: **`grantlease`** – Grant Lease test **`renewlease`** – Renew Lease test **`verifyservers`** – Verify DHCP Servers test **Note:** For the **`grantlease`** test to pass, the DHCP server must be configured to give out the lease for the requests from subnet of **`probeIpAddress`**.

Property	Default	Description
verifyServers		Comma separated list of IP addresses of remote DHCP servers to verify. This property is required when tests is set to **verifyservers**.
probeInterval	15	Defines in minutes how often the probe gets run. If not defined, the default is 15 minutes. Minimum value is 1 and maximum value is 34560 (a week).
timeOut	1000	Time in milliseconds to wait before a test times out. The allowable range is from 10 to 2,000,000,000 (about 33 minutes). Each probe can have a different timeout value by setting this property with an appropriate value. If this property is not defined, the timeout is set to 500 milliseconds.
retryCount	0	Number of times to repeat the test before failing it. The allowable range is from 0 to 100. The default retry count of 0 means the test is failed if the first attempt fails, that is, there is no retry attempt.
retryInterval	2000	The amount of time in milliseconds to wait between the retry attempts. The allowable range is from 10 to 2,000,000,000 (about 33 minutes).
macAddress	00:00:00:00:00:0A	Specifies the MAC address to use in the 'chaddr' field of the messages for the lease grant and the renew lease requests. If the DHCP service is configured with MAC address pools, this property must be set to a valid MAC address from the pool. If not specified, a default private MAC address (00 00-00-00-00-00-0A) is used.
probeIpAddress	IP address of `eth0` interface	Specifies an IP address of one of the appliance interfaces that the DHCP probe should listen on and use as the IP address that the DHCP service should respond to ('giaddr' field in lease grant and lease renew messages, and 'ciaddr' field in the DHCPINFORM message). If not specified, this value defaults to the IP address of the `eth0` interface. This property is required when the local host has multiple interfaces and the DHCP service is not configured to give out the lease from subnet of `eth0` address or when the lease from subnet of `eth0` address is not desired.

Log files

Refer to "Log files" (p. 1-28).

probe-dns

Purpose

The **probe-dns** package provides the configuration file that enables the probe to act as a DNS client simulator. The DNS Probe tests the various DNS services by requesting known resolutions to ensure they are responding correctly. An AMS administrator needs to define the DNS server IP address, the query and its expected resolution, for each test that is to be run by the DNS Probe.

Query by name support

The DNS Probe supports querying of the following Resource Records by name:

A	DNAME	KX	NAPTR	RRSIG	TXT
A6	DNSKEY	LOC	NS	RT	WKS
AAAA	DS	MB	NSAP	SIG	X25
AFSDB	GPOS	MG	NSEC	SOA	
APL	HINFO	MINFO	PTR	SPF	
CERT	ISDN	MR	PX	SRV	
CNAME	KEY	MX	RP	SSHFP	

Port

All messages from the DNS Probe to the DNS service are directed to the DNS server UDP port (default 53).

Configuration

The DNS Probe configuration is defined with properties set up in */opt/probe/conf/probe-dns.properties*, as described in the following table. If at least one query times out, or is not resolved to its expected value, the test fails. As with the DHCP probe, the result of each test is maintained separately.

Table 1-3 DNS Probe configuration properties

Property	Description
tests	Defines the list of DNS tests to run. The default value is **defaultDnsTest**. Each test can have the following additional required and optional properties: ***<test_name>*_query*Required***. DNS query criteria. The format of the query requires the following arguments separated by semi-colons. Refer to Table 1-4 for more information on the query criteria. ***query_type;look_up_value;RCODE;list_of_expected_answers*** ***<test_name>*_query_*x***Specifies more than one query in a test where ***x*** is a sequential number starting with 1. ***<test_name>*_dns_ip*Optional***. Specifies the IP address of the DNS server. If not specified, the IP address of localhost is used. This property should be used when the local DNS server has more than one interface and a specific address needs to be used in the test, or when the query is for non-local DNS server.
probeInterval	Defines in minutes how often the probe is run. If not defined, the default is 15 minutes. Minimum value is 1 and maximum value is 34,560 (a week).
timeOut	Time in milliseconds to wait before a test times out. The allowable range is from 10 to 2,000,000,000 (about 33 minutes). Each probe can have a different timeout value by setting this property with an appropriate value. If this property is not defined, the default is 500 milliseconds.
retryCount	Number of times to repeat the test before failing it. The allowable range is from 0 to 100. The default retry count of 0 means the test is failed if the first attempt fails, that is, there is no retry attempt.
retryInterval	The amount of time in milliseconds to wait between the retry attempts. The allowable range is from 10 to 2,000,000,000 (about 33 minutes). The default value is 2000 milliseconds.

Table 1-4 Query criteria

Query type	Description
query_type	Type of query the DNS Probe performs. The query type can be specified by its name or a number. Any 16-bit integer can be used as query type but only supported names can be used as query type. Refer to "Query by name support" (p. 1-22).
look_up_value	The lookup host value.

Query type	Description
RCODE	The response code to expect in the response. The response code can be specified by its name or a number. Any 16-bit integer can be used as response code, but only the following names are supported names as response code: BADVERS, FORMERR, NOERROR, NOTAUTH, NOTIMP, NOTIMPL, NOTZONE, NXDOMAIN, NXRRSET, REFUSED, SERVFAIL, YXDOMAIN, YXRRSET. The response code is optional. If not provided, it defaults to NOERROR.
list_of_expected_answers	The resolve value for *look_up_value*. The following are supported as resolve values: • Wild card (*) Matches any value. The test only needs to be resolved to a value, but no specific answer is required. • Empty Non-resolvable query. No value is specified for queries that should not be resolved. • Any other string Complete RDATA string to match. Multiple RDATA strings can be specified using the comma as the delimiter. If multiple RDATA strings are specified, a match on any one RDATA string passes the test. **Note:** The format of the RDATA string for a resource record is a space separated list of fields that describes the resource. For example, the MX record's RDATA comprises two fields, "Preference" and "exchange". An example of its RDATA string is **10 mail2.mycompany.com.** where **10** is preference given to the RR and **mail2.mycompany.com.** is a domain name of the host acting as a mail exchange. The resolved value **10 mail2.mycompany.com.,20 mail3.mycompany.com.** can be used to indicate that an answer with RDATA equal to **10 mail2.mycompany.com.** or **20 mail3.mycompany.com.** passes the test.

Sample queries

- Query with RDATA string comparison (an answer that should match one of the RDATA strings in the *list_of_expected_answers* section):

```
dnstest1_query=A;www.example.com;NOERROR:135.245.1.1, 135.245.1.2
```

or

```
dnstest1_query=A;www.example.com;135.245.1.1,135.245.1.2
```

- Query with RCODE comparison (the response RCODE should be NXDOMAIN):

```
dnstest1_query=A;typo.example.com;NXDOMAIN;
```

- Query whose response should contain one or more answers but does not care what the answer is:

```
dnstest1_query=A;www.google.com;*
```

or

```
dnstest1_query= A;www.google.com;NOERROR;*
```

- Non-resolvable query (query whose response does not contain any answer):

```
dnstest1_query=A;nosuchdomain.example;
```

Log files

Refer to "Log files" (p. 1-28).

probe-server

Purpose

The **probe-server** package contains following components:

- Probe service
- Probe CLI
- Probe Results CLI

Probe service

The Probe service is a daemon process on the appliance that is managed from the Services page for the appliance in the AMS GUI. It has the following capabilities:

- Maintains list of deployed probes
- Schedules each deployed probe to run at its configured time interval
- Supports concurrent execution of various probes
- Maintains results of each probe as long as it persists in AMS
- Limits the amount of storage consumed for results
- Serves the Probe CLI and Probe Results CLI to process user requests.

At its start up or when the probe configuration changes, the Probe service refreshes the list of deployed probes and their configurations. The Probe service detects deployed probes by the presence of their modules and configuration files in appropriate directories. It also detects when a probe is deployed, undeployed or modified.

The Probe service ensures that all probes are configured correctly. If any probes are not configured properly or no tests are configured for a probe, the Probe service logs appropriate error messages and exits.

The Probe service limits the amount of disk space used for results by purging results older than a retention period that is configured with the **resultRetentionPeriod** property.

The Probe service listens on an administrative port configured with the **serverPort** property for commands from the CLIs. It supports the following commands:

Execute probe test	Executes the requested test and returns its result.
Get probe test result	Returns result of last execution of the requested probe test.
Get unsaved results	Returns all unsaved probe results of the requested probe.

Probe scheduling

When the service first starts or reloads, all tests are delayed by an amount of time configured with the **probeStartDelay** property**)**. The subsequent run of probe is scheduled based on its frequency.

Probe results

The following information is saved for each probe test:

- Probe name: DNS, DHCP
- Test name: (Probe specific)
- Scheduled: True or false
- Start time
- Stop time
- Status: (pass or fail)
- Additional information: For failed tests, the reason for failure is saved

Probe directory structure

The **`probe-server`** package is deployed under */opt/probe* with the following files.

/opt/probe/	Root directory of probe package.
/opt/probe/bin	Contains CLIs.
/opt/probe/conf	Conf directory for Probe service and each deployed probes. One property file with name *probe-$probeName.properties* exists for each deployed probe.
/opt/probe/data/	Base directory to store probe data.
/opt/probe/data/$probeName	Temporary storage of results data of probe *`$probeName`*. Contains one file for each instance of probe execution.
/opt/probe/etc	Contains probe source *rc* file (**`proberc`**) needed to set up shell environment for running CLI.
/opt/probe/log	Store logs.
/opt/probe/lib	Base directory containing libraries and modules for probe-server, CLI and contains one sub-directory for each deployed probe.
/opt/probe/lib/$probeName	Directory containing all modules/libraries need to run a probe *`$probeName`*

Probe service configuration

The Probe service's configuration is defined by *probe-server.properties* file, as described in the following table.

Table 1-5 Probe service properties

Property	Default	Description
`probeStartDelay`	60000 (1 minute)	Defines time (in milliseconds) to delay all tests by when the service first starts or reloads. Minimum value is 0.

Property	Default	Description
probePollInterval	10000 (10 seconds)	Defines (in milliseconds) how often the probe's configuration is checked to detect changes in probe deployment. Minimum value is 1000.
resultRetentionPeriod	72 (3 days)	Defines appliance retention period (in hours) for unsaved probe results (results not been polled by the AMS). Minimum value is 1.
resultPurgeFrequency	1	Defines (in hours) how often to clean old probe results file not collected by AMS. Minimum value is 1.
logFailedTestToSyslog	false	Controls sending of syslog messages on a probe test failure. If this property is enabled, all failed tests are logged in syslog.
serverPort	9000	Defines the TCP port that the Probe service listens on for CLI requests.

Log files

Logs of the Probe service and all probes are written to */opt/probe/log/probe-server.log*. **Log4j** is used for logging and */opt/probe/conf/log4j-probe.properties* is used to control log4j-based logging.

Probe CLI

The **probe-run** CLI executes the requested probe test and returns its results.

Synopsis

probe-run -p *<probeName>* -t *<testName>* [-l] [-h]

Description

Option	Long name	Required	Description
-p	**--probe**	Y	Probe Name (case insensitive). Valid values are: DNS or DHCP. Case insensitive.
-t	**--test**	Y	***Optional***. If not specified, all tests are run. Test Name (case insensitive). Name must match one of the tests defined for the selected probe.
-l	**--list**	N	Return a list of deployed probes or tests. If probe name is specified, then all tests supported by the probe is returned, else a list of deployed probes is returned.
-h	**--help**	N	Displays CLI usage.

Exit status

- Zero indicates success. The time-stamped result is printed to stdout.
- Non-zero indicates usage error or processing failure.

Return

Depending on the input options, either the time-stamped result of requested probe test, or a list of deployed probes/tests is returned.

Probe Results CLI

The **probe-results** CLI prints probe results. This CLI supports getting either the last probe result or all probe results that have not been persisted in AMS database. The results are printed to stdout by default. If the file option is specified, the results are saved in the specified file.

Synopsis

probe-results -p *<probeName>* [-l] [-f *<filename>*] [-c]

Description

Option	Long name	Required	Description
-p	**--probe**	Y	Name of the probe to get results for. Valid values are: DNS or DHCP. case insensitive.
-t	**--test**	Y	***Optional***. If not specified, results of all tests are returned. Name of the test to get the result for (case insensitive). Name must match one of the tests defined for the selected probe.
-l	**--last**	N	Get the result of last run. If this option is not specified, all uncleared results are returned.
-f	**--file**	N	Output probe results data to the specified file instead of stdout.
-c	**--clear**	N	Clear all reported results.
-h	**--help**	N	Display CLI usage.

Exit status

- Zero indicate success.
- Non-zero indicates usage error or processing failure.

Return

Probe results.

qddns

Purpose

The **qddns** package provides the configuration files that are required to activate VitalQIP DNS service on the appliance.

Configuration

Before you push DNS configuration files, ensure that you have a DNS 4.x server defined in the VitalQIP database.

To define a DNS server in VitalQIP, follow these steps.

1. Log into the VitalQIP database on the Enterprise Server.
2. Access the Server Profile (**Infrastructure -> Server -> Add New Server**), and define a DNS server as follows:
3. Select **Lucent DNS 4.x** as the **Server Type**.
4. Configure the **Default Directory** as **/opt/qip/named**.
5. Configure the **RNDC Path** as **/opt/qip/usr/bin**.
6. Set **Create "rndc.conf"** to True.
7. Add the following text to **Corporate Extension**:

```
options {
   pid-file "/opt/qip/named/named.pid";
};
```

8. Set other parameters as required. For further information, refer to the "Manage servers" chapter in the *VitalQIP User's Guide*.

END OF STEPS

Log files

The log file for the **qddns** package is */opt/qip/named/named.run*.

Upgrade

For information on upgrading **qddns** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

qddns-snmp

Purpose

The **qddns-snmp** package activates the DNS SNMP add-on module. It can be configured to send SNMP traps to any client.

Configuration

Create or modify */etc/snmp/snmp.conf* on the appliance, by adding the following line to automatically load and translate the enterprise DNS mib:

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

For more information about configuring **qddns-snmp**, refer to the *Lucent DNS Release notes.*

Log files

The DNS SNMP log file is located in */opt/qip/log/qddns_snmp.log*.

qddns-anycast

Purpose

The **qddns-anycast** package provides configuration files necessary to provide dynamic anycast support for an appliance cluster configuration, using an Interior Gateway Protocol (IGP) such as Open Shortest Path First (OSPF). The routing software for OSPF is provided by Quagga. For more information, refer to Quagga's web site http://www.quagga.net.

Note: Although a configuration file for the internal Border Gateway Protocol (iBGP) is included, it is not supported at this time.

WARNING

Creating an anycast configuration file requires detailed knowledge and expertise in network configuration . Alcatel-Lucent strongly recommends that a network expert with knowledge of the specific network be involved in this configuration. Thorough testing of the configuration must be performed before production deployment.

Although anycast cluster configuration was introduced in AM 1.4 and allowed customers to configure anycast on the appliance, administrators needed to configure their routers manually. With IGP support on the appliance, routers can be dynamically updated whenever the status of the VitalQIP DNS service (**qddns**) changes.

Note: **qddns-anycast** should be installed alongside **qddns** on an appliance that is configured as a member of an appliance cluster. The AMS GUI screen for querying the current Anycast status greys out appliances that are assigned to an appliance cluster, but do not have the **qddns-anycast** package installed.

IGP protocol

Routing protocols perceive multiple servers with the same anycast subnet as simply redundant paths to the same subnet. By using an IGP routing protocol, in this case OSPF, the "best" anycast instance is automatically determined by the routing protocol. Each OSPF instance regularly communicates with their immediate neighbors to exchange network topology information.

The **qddns-anycast** packages provides OSPF software, enabling an appliance to partake in this topology exchange, and a daemon that starts/stops the anycast interface based on the state of the **qip-named** service. When **qip-named** goes down, the anycast daemon stops the anycast interface (that is, `lo:1`). This topology change is detected by the OSPF daemon and relayed to its neighboring routers. (For this to happen, OSPF must be enabled on each appliance interface, including the anycast interface.) The router is

therefore kept up-to-date on the state of the appliance's anycast interface and propagated through your network. If a given appliance's anycast interface is down, the router will choose another appliance in the cluster, if available.

Configuration

A basic configuration typically includes the following steps.

1 Configure *anycast.conf* to use a routing daemon (by setting **`IGP_DAEMON= ospf`**). Refer to Table 1-6 below.

2 Configure the following parameters in *ospfd.conf*:

a. An optional **`password`** statement to enable telnet access to Quagga's built-in OA&M. For more information on setting up telnet access to Quagga tools, refer to "Establish a telnet session" (p. 1-36).

Note: These configuration steps do not breach security in the firewall. AMM security is enforced through a combination of firewall rules and restrictive listen addresses. By default, you need to run telnet on the same appliance serving Quagga's IGP daemon.

b. A **`router ospf`** statement, followed by OSPF parameter statements. Even a basic configuration needs a **`router-id`**, **`area`**, and **`network`**.

In this simple ospfd.conf example, the appliance's IP address is used for the router-id, the anycast subnet is 192.168.1.0/24, and the appliance's physical interface is connected to the 10.4.0.0/24 subnet.

```
router ospf
  router-id 192.168.1.2
  area 0.0.0.1 stub no-summary
  network 192.168.1.0/24 area 0.0.0.1
```

c. Remember that a separate network statement is necessary for each appliance interface you want to run the OSPF protocol, plus one more for the anycast subnet, for example,

```
# Be sure to include your anycast subnet:
  network 172.1.1.0/24 area 0.0.0.1
```

d. Optionally, enable other forms of debugging information via Quagga directives, for example,

```
debug ospf lsa          # Link state advertisements.
debug ospf nsm          # status, events, etc.
```

```
log file /var/log/quagga/ospfd.log
```

Refer to http://www.quagga.net for other debug options.

END OF STEPS

Table 1-6 anycast.conf parameters

Parameter	Default	Description
IGP_DAEMON	none	Selects the routing daemon to enable.Values can be one of **none**, **ospf**, (or **bgp)**.
POLL_TIME	60 seconds	Defines the frequency of checks to determine if the DNS process is running.
DELAY_ON_START_TIME	30 seconds	Time interval to wait before acting on a DNS restart. This interval verifies that the DNS process has time to initialize and remain stable, before activating the anycast IP interface. The time for OSPF to advertise that the anycast interface is activated varies from nearly instantaneous to several minutes.
USE_PROBE_TEST_NAME= <testName>	not set	If a probe test name is defined, the DNS test probe feature is activated. The test probe is invoked after the usual anycast checks indicate that DNS should be running.
SYSLOG	false	Used to report anycast interface changes.
SYSLOG_PRIORITY= <level>	WARNING	Indicates the syslog priority with which anycast interface changes are reported. <level> can have the values **EMERG**, **ALERT**, **CRIT**, **ERR**, **WARNING**, **NOTICE**, **INFO**, or **DEBUG**.
SYSLOG_FACILITY= <facility>	LOCAL0	Indicates the syslog level with which anycast interface changes are reported. <facility> can have the values **DAEMON**, **LOCAL0-7**, or **USER**.
LOG_FILE	*/opt/anycastd/log /anycastd.log*	
LOG_LEVEL	WARN	Values can be **ERROR**, **WARN** , **INFO**, or **DEBUG**. The level **WARN** generates the same messages as reported to SYSLOG.
OSPFD_TELNET_ADDRESS =127.0.0.1:2604		These properties configure Quagga's telnet listen address and port number. If omitted, the default port number is used. If specified, select a port larger than 1023.
BGPD_TELNET_ADDRESS =127.0.0.1:2605		

Establish a telnet session

As with all configuration files on AMM, Quagga's configuration files are maintained on AMS and pushed to AMM. However, authoring a Quagga IGP configuration using a text editor can be prone to errors. Instead, Alcatel-Lucent recommends using Quagga's native OAM as a scratch pad. When connected to Quagga's IGP via telnet, you can use its IOS-like command language for generating a configuration. Interactive prompts guide an administrator through these commands, which are immediately applied to the running configuration. Once a working configuration is achieved, a network administrator needs to make the running configuration persistent by copying and pasting the working commands from the telnet session back into the AMS GUI and deploying the IGP configuration file.

To establish a telnet connection to Quagga's IGP, perform the following steps.

1. Establish an "ssh" login to AMM.

2. Use **`telnet 127.0.0.1 <port>`** to connect to the IGP daemon. The default listen address and port number are configured by the **`<igp>_TELNET_ADDRESS`** parameter in the *anycast.conf* file.

END OF STEPS

Troubleshooting reasons the anycast interface may be down

Use this checklist to troubleshoot problems with anycast configuration.

Table 1-7 Troubleshooting anycast interface

Symptom	Solution
Does AMS report qddns is up?	If not, anycast is working properly since it shut down the anycast interface.
Do you have DNS probes configured?	If the DNS probe configured by **USE_PROBE_TEST_NAME** is failing, anycast is working properly, since it shut down the anycast interface.
Did the anycast service start?	If not, review the most recent configuration file changes to *anycast.conf*, *ospfd.conf,* or *bgpd.conf*. Check */opt/anycast/log/anycastd.log*.

Use these checklists to troubleshoot problems with anycast configuration on different routing protocols.

Table 1-8 Problems with routing protocols

Problem	Solution
Can you telnet into the routing daemon?	If not, either the daemon's configuration file does not have a password configured or *anycast.conf* has not been configured to start a routing daemon. In *anycast.conf*, refer to the **IGP_DAEMON** setting.

OSPF checklist

Use the following checklist to verify anycast configuration on the OSPF routing protocol.

1. Has the OSPF daemon been configured to use OSPF on the appliance interface(s)?
2. Using a telnet session into the ospf daemon, check the interfaces:

`show ip ospf interface`

3. Is OSPF enabled on the loopback interface "lo"? An example of normal output is given below:

```
lo is up
  Internet Address 192.168.111.222/32, Broadcast 192.168.111.222,
  Area 0.0.0.1
```

If not, the most likely reason is the anycast daemon has determined there is a problem with "named" and deliberately shutdown the anycast interface. (Review the anycast application checklist above.)

Otherwise, *ospfd.conf* is missing a network statement for your anycast subnet. For example,

```
router ospf
  network 192.168.111.0/24 area 0.0.0.1
```

4. Is OSPF enabled on at least one of the physical interfaces? Similar to the loopback interface, a physical interface must be up, and have OSPF enabled.
5. Check OSPF's routing entries:

   `show ip ospf route`

6. Check OSPF self-orig:

   `show ip ospf database self-orig`

7. Check if the OSPF "adjacency" has been created with the neighboring routers:

   `show ip ospf neighbor`

   Ensure that the state is Full for each of the adjacent routers. If not, the OSPF parameters may be incorrect. Your network administrator needs to compare the configuration of the appliance with the router. Perhaps the OSPF authentication, subnet mask, or any one of the OSPF parameters are incorrect. For detailed documentation of Quagga's OSPF parameters see http://www.quagga.net/docs.php.

qddns-ha

Purpose

The **`qddns-ha`** package allows the DNS High Availability Service to be configured on appliance pairs.

High Availability requirements

- Available only for DNS Service
- DNS High Availability is not available on the “ESM” appliances
- Both appliances must be defined as servers in VitalQIP
- Both appliances and the paired IP addresses must be on the same subnet

VitalQIP configuration

This topic describes some of the configuration steps that are required in VitalQIP so that high availability pairs of DNS servers can be set up. For setup of pairs in AMS, refer to the *AMS User’s Guide*.

To set up DNS servers in VitalQIP for High Availability, follow these steps.

1. Create DNS appliances in the AMS database with the desired non-shared IP addresses.
2. Create DNS servers in VitalQIP with the same non-shared IP addresses.
3. Create a DNS server in VitalQIP with the shared IP address.
4. Use the server with the shared IP address in your DHCP option templates.
5. Dynamic updates should be sent to both appliance IP addresses, not the paired IP.
6. Both servers have to be defined with the same options and with the same data in VitalQIP. The SOA override feature in VitalQIP may be used to ensure both appliances provide the same DNS server (MNAME) in the zone SOA. The NS records of the HA pair can be stealth to mask the individual appliances.

7 Slave servers to a paired IP may need to be configured with an allow-notify directive.

8 The paired appliances may need to be configured with a notify-source directive.

Note: The paired IP may be provided to DNS clients as their DNS server.

END OF STEPS

Configuration

To configure the DNS High Availability Service, follow these steps.

1 Connect a crossover cable between the appliance pairs using the Ethernet port.

2 Set up the Appliance Pair using the Appliances screen in the AMS GUI. Refer to Chapter 2 of the *Appliance Management Software User's Guide* for instructions.

3 Download the DNS High Availability **`qddns-ha`** package from the ALED website and load it into AMS. Refer to Chapter 4 of the *Appliance Management Software User's Guide* for instructions. The package contains the following configuration files:

- */etc/amm/conf.d/qddns-ha*
- */etc/ha.d/authkeys*
- */etc/ha.d/ha.cf*
- */var/lib/heartbeat/crm/cib.install.xml*

4 Associate the package with both appliances in the pair.

END OF STEPS

Troubleshooting High Availability

The following table contains questions and answers to questions that are frequently asked about High Availability.

Table 1-9 High availability FAQs

Question	Answer
What is the "health check" interval for the heartbeat?	The health check interval of the cluster IP address is 5 seconds.The heartbeat check is set up by the **`respawn root`** command in */etc/ha.d/ha.cf*: **`respawn root /usr/lib64/heartbeat/pingd -m 100 -d 5s`** This command is used to ping the gateway so that an appliance can determine network reachability. The **`-d`** parameter is a dampening period value of 5 seconds. The **`-m`** parameter is a multiplier used when computing scores. **Note:** An appliance should be able to ping its gateway within 5 seconds. The multiplier value should not be modified unless rules in *cib.xml* are changed.
What is the rule for "down *named*" ? For example, "no response to query in x seconds".	The **`rndc status`** command is executed every 15 seconds to check the status of *named*. If this status returns an error, a failover occurs.
If the heartbeat goes down, does it require a manual restart from AMS? If not, can it be configured?	If the heartbeat service goes down, it has to be restarted from AMS.
What other configuration points should I be aware of?	• Authentication keys can be configured in *authKeys*. It has been tested with **`sha`** and **`crc`** mechanism. • The time interval that named or cluster IP address is monitored is configurable via *cib.install.xml*. The default value is 15 seconds. Refer to "Sample cib.install.xml" (p. 40). **Note:** Exercise caution when lowering monitor intervals since too low a threshold could produce false reports of an outage. • Debug can be turned on or off in the *ha.cf* file. It is on by default.

Sample cib.install.xml

The following is an example of the *cib.install.xml* file.

```
<!--
  if this file is not modified it will be updated by the AMS
-->
 <cib admin_epoch="0" epoch="0" num_updates="0">
   <configuration>
     <crm_config>
       <cluster_property_set id="cib-bootstrap-options">
         <attributes>
```

```
        <nvpair id="cib-bootstrap-options-default-resource-stickiness"
name="default-resource-stickiness" value="300"/>
        <nvpair id="cib-bootstrap-options-default-resource-failure-
stickiness" name="default-resource-failure-stickiness" value="-100"/>
        <nvpair id="cib-bootstrap-options-symmetric-cluster"
name="symmetric-cluster" value="false"/>
      </attributes>
    </cluster_property_set>
  </crm_config>
  <nodes>
  </nodes>
  <resources>
    <group id="dns_pair_group">
      <primitive id="qip-named_ipaddress" class="ocf" type="IPaddr"
provider="heartbeat">
        <instance_attributes id="qip-named_ipaddress_attr">
          <attributes>
            <nvpair id="qip-named_ipaddress_ip" name="ip"
value="${appliancePair.ipAddress.address}"/>
             <nvpair id="qip-named_ipaddress_netmask" name="cidr_netmask"
value="${appliance.ipAddress.netmask}"/>
            <nvpair id="qip-named_ipaddress_nic" name="nic" value="eth0"/>
          </attributes>
        </instance_attributes>
        <operations>
          <op id="qip-named_ipaddress_monitor" name="monitor"
interval="15s" timeout="30s" start_delay="10s"/>
        </operations>
      </primitive>
      <primitive id="dns_pair" class="ocf" type="DNSpair"
provider="heartbeat">
        <operations>
          <op id="dns_pair_monitor" name="monitor" interval="15s"
timeout="30s" start_delay="10s"/>
        </operations>
      </primitive>
    </group>
    <primitive id="qip-named_node1" class="ocf" type="qip-named"
provider="heartbeat">
      <operations>
        <op id="qip-named_node1_monitor" name="monitor" interval="15s"
timeout="30s" start_delay="10s"/>
      </operations>
    </primitive>
    <primitive id="qip-named_node2" class="ocf" type="qip-named"
provider="heartbeat">
      <operations>
```

```
        <op id="qip-named_node2_monitor" name="monitor" interval="15s"
timeout="30s" start_delay="10s"/>
      </operations>
    </primitive>
  </resources>
  <constraints>
    <rsc_location id="run_dns_pair_group" rsc="dns_pair_group">
      <rule id="run_dns_pair_group_node1_rule" score="100">
        <expression id="run_dns_pair_group_node1_rule_expr"
attribute="#uname" operation="eq"
            value="${appliancePair.primaryAppliance.hostname}"/>
      </rule>
      <rule id="run_dns_pair_group_node2_rule" score="50">
        <expression id="run_dns_pair_group_node2_rule_expr"
attribute="#uname" operation="eq"
            value="${appliancePair.secondaryAppliance.hostname}"/>
      </rule>
    </rsc_location>
    <rsc_location id="run_qip-named_node1" rsc="qip-named_node1">
      <rule id="run_qip-named_node1_loc_rule" score="1000">
        <expression id="run_qip-named_node1_loc_rule_expr"
attribute="#uname" operation="eq"
            value="${appliancePair.primaryAppliance.hostname}"/>
      </rule>
    </rsc_location>
    <rsc_location id="run_qip-named_node2" rsc="qip-named_node2">
      <rule id="run_qip-named_node2_loc_rule" score="1000">
        <expression id="run_qip-named_node2_loc_rule_expr"
attribute="#uname" operation="eq"
            value="${appliancePair.secondaryAppliance.hostname}"/>
      </rule>
    </rsc_location>
    <rsc_colocation id="qip-named_not_same" from="qip-named_node1"
to="qip-named_node2" score="-INFINITY"/>
    <rsc_location id="qip-named_ipaddress_connected" rsc="dns_pair_group">
      <rule id="qip-named_ipaddress_connected_rule" score="-INFINITY"
boolean_op="or">
       <expression id="qip-named_ipaddress_connected_rule_expr_undefined"
attribute="pingd" operation="not_defined"/>
        <expression id="qip-named_ipaddress_connected_rule_expr_zero"
attribute="pingd" operation="lte" value="0"/>
      </rule>
    </rsc_location>
    <rsc_location id="qip-named_running" rsc="dns_pair_group">
      <rule id="qip-named_running_rule" score="-INFINITY" boolean_op="or">
        <expression id="qip-named_running_rule_expr_undefined"
attribute="qip-named-state" operation="not_defined"/>
```

```
          <expression id="qip-named_running_rule_expr_zero" attribute="qip-
  named-state" operation="lte" value="0"/>
        </rule>
      </rsc_location>
    </constraints>
   </configuration>
   <status>
   </status>
 </cib>
```

Log files

For AMM2 package:

- */opt/qddns-ha/log/force-ha-switchover.log*
- */opt/qddns-ha/log/updateCibXml.log*
- */var/log/ha-debug*
- */var/log/ha-log*

For AMM1 package:

- */opt/qddns-ha/log/updateCibXml.log*
- */var/log/ha-debug*
- */var/log/ha-log*

Upgrade

Management of the high availability crossover interface has been moved from the **qddns-ha** package to the AMS user interface. Appliances that are running **qddns-ha-1.0.1** need to be upgraded to the **qddns-ha-1.0.2** version or above.

Note: Some of the DNS-HA upgrades from very old versions(AMM1) to new/current version(AMM2) will not work properly. The older packages do not have "*system-required*" flag that prevents AMM1 packages to be deployed on AMM2 appliances. In such cases, uninstall the old package and install the new one.

To upgrade appliance pairs with the **qddns-ha-1.0.2** package, follow these steps.

1. In the **Appliances** tab, locate an appliance that is currently associated with the **qddns-ha-1.0.1** package.

2. In the Appliance Properties page, click the **Packages** tab.

   Result: The Packages page opens.

3 Click **Modify** and change the version associated with the **qddns-ha** package from the 1.0.1 version to 1.0.2 or above.

4 Click **Save**.

Result: The Modify Package Associations Confirmation dialog box opens.

5 Click **OK**.

Result: A confirmation dialog box opens with the message **Modified the appliance associations**.

6 Click **OK**.

Result: The Pending Deployments for Appliance page opens.

7 Click **Proceed** to continue with the deployment.

Result: Deployment begins and package status changes to indicate deployment is in progress.

8 When deployment is complete, a confirmation dialog box opens with the message **Package deployment on <appliance name> has finished**.

9 Click **OK**.

Result: The new package is associated with the appliance. Both packages are now listed in the appliance tree.

10 In the Package Properties page, click **Deploy**.

Result: The new package is deployed on the appliance and the old version is removed.

Important! This last step is mandatory for the **qddns-ha** package to be updated on the appliance. It must also be repeated for the other appliance in the pair.

END OF STEPS

qddns-userexits

Purpose

The **qddns-userexits** package provides the userexits files that allows the user to manipulate the DNS configuration file after the file has been created.

Configuration

The following configuration files for DNS user exits are located in */opt/qip/userexits*:

- *qipS2dnsuserexit*
- *qipS4dnsuserexit*
- *qipdnscnfuserexit*
- *qipprednscnfuserexit*
- *qipdnsuserexit*
- *qipprednsuserexit*

User exit setup

To set up a user exit, follow these steps:

1. Set the *FailOnFailedUserExit* parameter to **true** in the *qip.pcy* file. For information on this parameter, refer to "VitalQIP Remote Service policies" (p. A-14).

2. DNS file generation to the server should invoke the *userexit* file based on the config/update selection in the DNS generation screen. For further information, refer to the "Network services" chapter in the *VitalQIP User's Guide*.

END OF STEPS

Log files

None.

qdhcp

Purpose

The **qdhcp** package provides the configuration files that are required to activate the VitalQIP DHCP service on the appliance.

Configuration

Before you push DHCP configuration files from VitalQIP to the appliance, ensure that you have a DHCP 5.4 or 5.5 server defined in the VitalQIP database.

To define a DHCP server in VitalQIP, follow these steps:

1. Log into the VitalQIP database on the Enterprise Server.
2. Access the Server Profile (**Infrastructure -> Server -> Add New Server**), and define a DHCP server as follows:
3. Select **Lucent DHCP 5.4** or **Lucent DHCP 5.5** as the **Server Type**.
4. Configure the **Default Directory** as */opt/qip/dhcp*.
5. Set other parameters as required. For further information, refer to the "Manage servers" chapter in the *VitalQIP User's Guide*.

END OF STEPS

Log files

Log files for the **qdhcp** package are located in:

- */opt/qip/dhcp/dhcpd.stats*
- */opt/qip/log/dhcpd.log*

Upgrade

For information on upgrading **qdhcp** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Deploy packages for an appliance group

qdhcp-snmp

Purpose

The **qdhcp-snmp** package activates the DHCP SNMP add-on module. You can configure this package to send SNMP traps to any client.

Configuration

Create or modify */etc/snmp/snmp.conf* on the appliance, by adding the following line to automatically load and translate the enterprise DHCP mib:

```
mibs +QDHCP-SERVER-MIB
```

For more information about configuring **qdhcp-snmp**, refer to the *Lucent DHCP Release notes.*

Log files

The DHCP SNMP log file is located in */opt/qip/log/qdhcp_snmp.log*.

qdhcp-manager

Purpose

The **qdhcp-manager** package provides the configuration files that are required to activate the VitalQIP DHCP Configuration Manager on the appliance. The DHCP Configuration Manager is a web-based GUI that allows quick configuration of a Lucent DHCP server on the appliance. The web GUI is local to the DHCP server and only used to provision a single server. For more information on DHCP Configuration Manager, refer to the *DHCP Configuration Manager User's Guide* (190-409-122).

Note: The **qdhcp-manager** package is a separately licensed package and is not generally available for download from the ALED site.

Web server

Appliance Management Software uses a web server that runs as the **qdhcp-httpd** service. This service can be controlled from the AMS GUI.

To stop/start/kill/restart the service, you need to select the desired appliance in the AMS hierarchy, and select the **Services** tab when the Appliance Properties page is displayed.

Log files

Logs are located in the */opt/qdhcpmgr/log* directory. The following logs are maintained:

- *qdhcp_httpd.log* contains logs written by QDHCP Web Server. It logs html pages requested by the client.
- *qdhcp_manager.log* contains the DHCP Configuration Manager application log. The log level of this file is controlled via the **loglevel** property in the */opt/qdhcpmgr/conf/qdhcpmgr.properties* file. For more information on this property, refer to Appendix A in the *DHCP Configuration Manager User's Guide*.

qdhcp-userexits

Purpose

The **`qdhcp-userexits`** package provides the user exit files that allow the user to manipulate the DHCP configuration file after it has been created. The user exit is called after the *dhcpd.pcy* and *dhcpd.conf* files are created, but before the DHCP Service is notified to refresh the configuration files.

Configuration

The configuration file for DHCP user exits is */opt/qip/userexits/qipdhcpuserexit*.

User exit setup

To set up a user exit, follow these steps:

1. Set the `FailOnFailedUserExit` parameter to **`true`** in the *qip.pcy* file. For information on this parameter, refer to "VitalQIP Remote Service policies" (p. A-14).

2. DHCP file generation to the server should invoke the file *qipdhcpuserexit*. For further information, refer to the "Network services" chapter in the *VitalQIP User's Guide*.

END OF STEPS

Log files

None.

qip-snmp

Purpose

The **qip-snmp** package activates the VitalQIP SNMP add-on module. It can be configured to send SNMP traps to any client.

Configuration

The following **qip-snmp** configuration files are located in the */opt/qip/snmp/config* directory:

- *mgr.cnf*
- *snmpd.cnf*

Source environment

To run SNMP Research utilities such as **getone**, **getnext**, and so on, the SNMP environment needs to be sourced as follows:

```
. /opt/qip/snmp/etc/snmprc
```

Restart DNS and DHCP servers

To restart DNS and DHCP servers after the SNMP status has changed, follow these steps.

1. Locate the */etc/amm/conf.d/qip-snmp* config file in the Appliance (or Appliance Group hierarchy) and open the Config File Properties page.

2. Click **Modify**.

   Result: The Config File Editor opens.

3. Change the **RESTART_DEPENDENTS** entry to **yes**. Enter a comment if necessary.

4. Click **Save**.

   Result: A dialog box opens with the message **Config file changes saved**.

5 Click **OK**.

END OF STEPS

Log files

The SNMP add-on log file is located in */opt/qip/log/snmpd.log*.

Upgrade

For information on upgrading **`qip-snmp`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

snmp-server

Purpose

The **snmp-server** package installs the standard Redhat SNMP daemon from **net-snmp.org** on an appliance. It activates the default SNMP MIBs that monitor the health of the system, and can also act as an SNMP proxy for the VitalQIP Remote Service's SNMP agent, which permits both SNMP agents to be integrated on the same system. SNMP traps can also be set up in the configuration files to update external SNMP Managers, if required.

Configuration

The **snmp-server** configuration file is located in */etc/snmp/snmpd.cnf*.

Customers interested in changing the configuration should refer to the **net-snmp** documentation available at **http://www.net-snmp.org/docs**. The default configuration is designed to work as follows:

- SNMP protocols V1 and V2C are enabled (that is, authentication via a community string), using the traditional default value of **public**.
- Only read-only MIB access is enabled. Customers who want to change the variable ***sysContact*** should establish a different read-only value in the configuration file.
- MIB access is limited to a few select branches to prevent security vulnerability.

Table 1-10 MIBs available in default configuration

MIB::node	Reference	Description
SNMPv2 MIB::system (.1.3.6.1.2.1.1)	RFC 3418	Contains primarily static strings configured in *snmpd.conf*, such as **sysDescr**, **sysContact**, **sysName**, **sysLocation**, and so on. Example: **snmpget -c public -v 2c localhost ** **SNMPv2-MIB::sysName.0**
SNMPv2-MIB::snmp (.1.3.6.1.2.1.11)	RFC 3418	Contains metric regarding SNMP usage.
IF-MIB::interfaces (.1.3.6.1.2.1.2)	RFC 2863	Contains real-time network interface metrics such as operational status, byte counts, and so on. The following is a sample command to read and format the data in this portion of the MIB: **snmptable -c public -v2c localhost -Cl -Ci ** **-OX -Cb -Cw 64 IF-MIB::ifTable**

MIB::node	Reference	Description
IP-MIB::icmp (.1.3.6.1.2.1.5)	RFC 4293	Although most of the IP-MIB is blocked for security reasons, the ***icmp*** variables are essential for detecting and diagnosing networking faults. A sample query follows: **snmpwalk -c public -v 2c localhost icmp**
HOST RESOURCES-MIB::host (.1.3.6.1.2.1.25)	RFC 2790	Provides resource information covering disk, memory and CPU utilization, (excluding process parameters). Sample queries are as follows: • Disk Space (by filesystem; which includes swap): **snmpdf -c public -v2c localhost** • Running processes: **snmptable -c public -v2c localhost \ HOST-RESOURCES-MIB::hrSWRunTable**
UCD SNMP-MIB::ucdavis (.1.3.6.1.4.1.2021)	**www.net-snmp.org**	Provides additional system information; but restricted by the default configuration to only MIB nodes for memory, **systemStats**, and **laTable**. Sample queries are as follows: • CPU usage: **snmpget -c public -v 2c localhost \ UCD-SNMP-MIB::systemStats.ssCpuIdle.0** • Memory and swap space usage: **snmpwalk -c public -v 2c localhost \ UCD-SNMP-MIB::memory** • Load averages: **snmptable -c public -v2c localhost \ UCD-SNMP-MIB::laTable**
SNMPv2-SMI::enterprises.lucent (.1.3.6.1.4.1.1751)	VitalQIP	When VitalQIP Remote Services are installed, the **snmpd** daemon is configured to act as a proxy for these variables.

Modify snmpd.conf

The default configuration works “as-is”, but without the proxy for **qip-snmp** enabled. The most likely changes customers will make are as follows:

- Uncommenting the proxy statements in *snmpd.conf* if **qip-snmp** is installed.
- Enhancing security by changing the default “public” community string, which is controlled by the “com2sec” directive in **snmpd.conf**. The default is:

  com2sec notConfigUser default public

Note: There is no benefit in changing the "public" community password for the proxied **qip-snmp** server since its port (1161) is protected by a firewall. If it is changed, a corresponding change to the **qip-snmp** configuration is required.

- Changing the default values for **syslocation** and **syscontact**. The defaults are:

```
syslocation Unknown
syscontact  root <root@localhost>
```

To modify the *snmpd.conf* file, follow these steps.

1. Locate the */etc/snmp/snmp.conf* config file in the Appliance (or Appliance Group hierarchy) and open the Config File Properties page.

2. Click **Modify**.

   Result: The Config File Editor opens.

3. Make changes as needed and click **Save**.

   Result: A dialog box opens with the message **Config file changes saved**.

4. Click **OK**.

END OF STEPS

Note: Do not uncomment the proxy statements in *snmpd.conf* when using the snmp-server package with **qddns-snmp** and **qdhcp-snmp** packages. Uncomment these proxy statements only when using the snmp-server with the **qip-snmp** package.

Log files

The SNMP add-on log file is located in */var/log/snmpd.log*.

Upgrade

For information on upgrading **snmp-server** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

sybase

Purpose

The **sybase** package contains the 32-bit Sybase database modules that are required to run the VitalQIP 7.1 Enterprise Server.

The default Sybase server name is `QIPSYBASE`. The default **sa** password is `sy54dm1n`.

To log into **isql** as **sa**, use **ssh** to log into the appliance as **ammuser** and then issue the following commands:

```
$ . /opt/sybase/SYBASE.sh
$ isql -Usa -Psy54dm1n -SQIPSYBASE
```

Configuration

None.

Sybase services shutdown

Alcatel-Lucent recommends that all Sybase services be shut down before the hostname and/or the IP address of the ESM appliance is modified via the console menu or the USB thumb drive. Sybase services restart automatically after the ESM appliance is rebooted.

Sybase server upgrade

The **sybase** package must be uninstalled if you are upgrading Sybase from the 32-bit to the 64-bit version. Even after the **sybase** package has been uninstalled, a database instance is preserved in */opt/sybase/data*. Therefore, after uninstalling the **sybase** package, be sure to manually remove the */opt/sybase* directory. The **enterprise** and **sybase** packages can then be deployed again using AMS.

Log files

The log file for the data server is located in */opt/sybase/ASE-15_0/install/QIPSYBASE.log*.

The log file for the backup server is located in */opt/sybase/ASE-15_0/install/QIPSYBASE_BS.log*.

sybase64

Purpose

The **sybase64** package contains the 64-bit Sybase database modules that are required to run the VitalQIP 7.2 Enterprise Server.

The default Sybase server name is `QIPSYBASE`. The default **sa** password is `sy54dm1n`.

To log into **isql** as **sa**, use **ssh** to log into the appliance as **ammuser** and then issue the following commands:

```
$ . /opt/sybase/SYBASE.sh
$ isql -Usa -Psy54dm1n -SQIPSYBASE
```

Configuration

None.

Sybase services shutdown

Alcatel-Lucent recommends that all Sybase services be shut down before the hostname and/or the IP address of the ESM appliance is modified via the console menu or the USB thumb drive. Sybase services restart automatically after the ESM appliance is rebooted.

Sybase server downgrade

The **sybase64** package must be uninstalled if you are downgrading from the 64-bit Sybase package to the 32-bit version. Even after the **sybase64** package has been uninstalled, a database instance is preserved in */opt/sybase/data*. Therefore, after uninstalling the **sybase** package, be sure to manually remove the */opt/sybase* directory. The **enterprise** and **sybase** packages can then be deployed again using AMS.

Log files

The log file for the data server is located in */opt/sybase/ASE-15_0/install/ASE.log*.

The log file for the backup server is located in */opt/sybase/ASE-15_0/install/BS.log*.

system-patch

Purpose

The **system-patch** package contains all OS-related patches for AMM1-based appliances.

Configuration

None.

Log files

None.

Upgrade

System patches are cumulative. Therefore, you only need to install the latest patch.

To deploy a **system-patch** package, the appliance must be rebooted for the changes to be enabled.

For information on upgrading **system-patch** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Deploy packages for an appliance group

system-patch2

Purpose

The **system-patch2** package contains all OS-related patches for AMM2-based appliances.

Configuration

None.

Log files

None.

Upgrade

System patches are cumulative. Therefore, you only need to install the latest patch.

To deploy a **system-patch2** package, the appliance must be rebooted for the changes to be enabled.

For information on upgrading **system-patch2** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Deploy packages for an appliance group

tftp-server

Purpose

The **tftp-server** package provides TFTP (Trivial File Transfer Protocol) Server module files that are required to activate the TFTP Server service on the appliance. TFTP is a very simple file transfer protocol. It is typically used at boot time by devices with limited storage to retrieve configuration or firmware.

Configuration

Any served files must be placed on the appliance manually using **ssh** or using the File Management feature in the AMS GUI, as described in the *AMS User's Guide*. These files should be placed in the */opt/tftp/tftpboot* directory, should be owned by root and have permissions of 644. These files are not removed if the package is removed.

The TFTP server listens on port 69. The TFTP server allows access to any file in the *tftpboot* directory. New files are not accepted, but existing files may be overwritten if the file permission allows.

Log files

The TFTP server logs to syslog. By default, a log message is placed in the system log file */var/log/messages*.

vitalqip6.2-remote

Purpose

The **vitalqip6.2-remote** package contains the modules and configuration files that comprise the VitalQIP 6.2 Remote Server.

Configuration

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is delivered in the Remote Services package.

Configure the *qip.pcy* file as follows:

1. In the `[VitalQIP Remote Service]` section, define the address of the File Generation Server:

   FileGenerationServer=*<ip_address>*

2. If DHCP is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DHCP messages:

   MessageRoute=DHCP:A:0:QIP Update Service (DHCP):VitalQIP QIP Update Service:*<ip_address>*

3. If DNS with EDUP enabled is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DNS messages:

   MessageRoute=DNSUpdateRR:A:0:QIP Update Service (Update RR):VitalQIP QIP Update Service:*<ip_address>*

4. To enable the creation of log files, you can establish a default Debug setting in the Global section.

   For further information on the above VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

END OF STEPS

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-msgd.log*
- *qip-netd.log*

- *qip-rmtd.log*
- *qip-ssltd.log*

Upgrade

For information on upgrading **`vitalqip6.2-remote`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

vitalqip7.0-remote

Purpose

The **vitalqip7.0-remote** package contains the modules and configuration files that comprise the VitalQIP 7.0 Remote Server.

Configuration

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is delivered in the Remote Services package.

Configure the *qip.pcy* file as follows:

1 In the `[VitalQIP Remote Service]` section, define the address of the File Generation Server:

FileGenerationServer=*<ip_address>*

2 If DHCP is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DHCP messages:

MessageRoute=DHCP:A:0:QIP Update Service (DHCP):VitalQIP QIP Update Service:*<ip_address>*

3 If DNS with EDUP enabled is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DNS messages:

MessageRoute=DNSUpdateRR:A:0:QIP Update Service (Update RR):VitalQIP QIP Update Service:*<ip_address>*

4 To enable the creation of log files, you can establish a default Debug setting in the Global section.

For further information on the above VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

END OF STEPS

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-msgd.log*
- *qip-netd.log*

- *qip-rmtd.log*
- *qip-ssltd.log*

Upgrade

For information on upgrading **`vitalqip7.0-remote`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

vitalqip7.1-enterprise

Purpose

The **vitalqip7.1-enterprise** package contains the modules and configuration files related to the VitalQIP Enterprise Server.

Note: To start the VitalQIP Web Client on an ESM appliance, use port 8080 from any client:

http://*<appliance ip address>*:8080/qip

qip.pcy configuration file

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is available with the VitalQIP **enterprise** package. At a minimum, the policies in the following table need to be set. Refer to "Modify qip.pcy file policies on an ESM appliance" (p. 2-3) for information on how to modify *qip.pcy*. For further information on these VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

Table 1-11 Enterprise server appliance policies

Policy	qip.pcy section
Password (for **qipman**)	Global
Debug	Global
VitalQIP QIP Update Service MessageRoute=DNSUpdateRR	VitalQIP Message Service
VitalQIP QIP Update Service MessageRoute=DHCP	VitalQIP Message Service
VitalQIP DNS Update Service MessageRoute=DNSUpdateRR	VitalQIP Message Service
VitalQIP DNS Update Service MessageRoute=DNSUpdateObject	VitalQIP Message Service
FileGenerationServer	VitalQIP Remote Service

Note: If you configure the *qip.pcy* to use SSL, there can be only one key in qipkeystore. Use the **keytool** command to see the number of keys in qipkeystore. For example, **$/opt/jre-1.6.0-sun/bin/keytool -list -keystore /opt/qip/qipkeystore**.

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-dnsupdated.log*
- *qip-logind.log*
- *qip-msgd.log*

- *qip-netd.log*
- *qip-rmtd.log*
- *qip-qipupdated.log*
- *qip-rmisched.log*
- *qip-ssltd.log*
- *qipd.log*

The following installation log files are located in the */opt/qip/log* directory:

- *qip-install.log*
- *qip-result.log*

The Tomcat server log file is located in */opt/qip/tomcat/logs/catalina.out*.

Upgrade

For information on upgrading **`vitalqip7.1-enterprise`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

vitalqip7.1-remote

Purpose

The **vitalqip7.1-remote** package contains the modules and configuration files that comprise the VitalQIP 7.1 Remote Server.

Configuration

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is delivered in the Remote Services package.

Configure the *qip.pcy* file as follows:

1 In the `[VitalQIP Remote Service]` section, define the address of the File Generation Server:

FileGenerationServer=*<ip_address>*

2 If DHCP is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DHCP messages:

MessageRoute=DHCP:A:0:QIP Update Service (DHCP):VitalQIP QIP Update Service:*<ip_address>*

3 If DNS with EDUP enabled is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DNS messages:

MessageRoute=DNSUpdateRR:A:0:QIP Update Service (Update RR):VitalQIP QIP Update Service:*<ip_address>*

4 To enable the creation of log files, you can establish a default Debug setting in the Global section.

For further information on the above VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

END OF STEPS

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-msgd.log*
- *qip-netd.log*

- *qip-rmtd.log*
- *qip-ssltd.log*

Upgrade

For information on upgrading **`vitalqip7.1-remote`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

vitalqip7.2-enterprise

Purpose

The **vitalqip7.2-enterprise** package contains the modules and configuration files related to the VitalQIP Enterprise Server.

Note: To start the VitalQIP Web Client on an ESM appliance, use port 8080 from any client:

http://*<appliance ip address>*:8080/qip

qip.pcy configuration file

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is available with the VitalQIP **enterprise** package. At a minimum, the policies in the following table need to be set. Refer to "Modify qip.pcy file policies on an ESM appliance" (p. 2-3) for information on how to modify *qip.pcy*. For further information on these VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

Table 1-12 Enterprise server appliance policies

Policy	qip.pcy section
Password (for **qipman**)	Global
Debug	Global
VitalQIP QIP Update Service MessageRoute=DNSUpdateRR	VitalQIP Message Service
VitalQIP QIP Update Service MessageRoute=DHCP	VitalQIP Message Service
VitalQIP DNS Update Service MessageRoute=DNSUpdateRR	VitalQIP Message Service
VitalQIP DNS Update Service MessageRoute=DNSUpdateObject	VitalQIP Message Service
FileGenerationServer	VitalQIP Remote Service

Note: If you configure the *qip.pcy* to use SSL, there can be only one key in qipkeystore. Use the **keytool** command to see the number of keys in qipkeystore. For example, **$/opt/jre-1.6.0-sun/bin/keytool -list -keystore /opt/qip/qipkeystore**.

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-cached.log*
- *qip-dnsupdated.log*
- *qip-logind.log*

- *qip-msgd.log*
- *qip-netd.log*
- *qip-rmtd.log*
- *qip-qipupdated.log*
- *qip-rmisched.log*
- *qip-ssltd.log*
- *qipd.log*

The following installation log files are located in the */opt/qip/log* directory:

- *qip-install.log*
- *qip-install-result.log*

The Tomcat server log file is located in */opt/qip/tomcat/logs/catalina.out*.

Upgrade

For information on upgrading **`vitalqip7.2-enterprise`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

SelfReg configuration

Configure SelfReg as follows:

1 Configure the */opt/qip/web/WEB-INF/web.xml* file and uncomment the SelfReg servelet section.

END OF STEPS

vitalqip7.2-remote

Purpose

The **vitalqip7.2-remote** package contains the modules and configuration files that comprise the VitalQIP 7.2 Remote Server.

Configuration

An abbreviated version of the VitalQIP policies file, *qip.pcy*, is delivered in the Remote Services package.

Configure the *qip.pcy* file as follows:

1. In the `[VitalQIP Remote Service]` section, define the address of the File Generation Server:

   FileGenerationServer=*<ip_address>*

2. If DHCP is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DHCP messages:

   MessageRoute=DHCP:A:0:QIP Update Service (DHCP):VitalQIP QIP Update Service:*<ip_address>*

3. If DNS with EDUP enabled is running, in the `[VitalQIP Message Service]` section, define the IP address of the VitalQIP QIP Update Service that handles DNS messages:

   MessageRoute=DNSUpdateRR:A:0:QIP Update Service (Update RR):VitalQIP QIP Update Service:*<ip_address>*

4. To enable the creation of log files, you can establish a default Debug setting in the Global section.

   For further information on the above VitalQIP policies, refer to "VitalQIP policy files" (p. A-1).

END OF STEPS

Log files

The following VitalQIP services log files are located in the */opt/qip/log* directory:

- *qip-cached.log*
- *qip-msgd.log*

- *qip-netd.log*
- *qip-rmtd.log*
- *qip-ssltd.log*

Upgrade

For information on upgrading **`vitalqip7.2-remote`** packages, refer to the following topics in the *AMS User's Guide*:

Packages

- Import a package

Appliance

- Associate packages with an appliance
- Configure packages for an appliance
- Review pending deployments and deploy packages

Appliance groups

- Associate packages with an appliance group
- Configure packages for an appliance group
- Deploy packages for an appliance group

END OF STEPS

enum-1.4

Purpose

The **`enum-1.4`** package activates the VitalQIP ENUM add-on module.

Configuration

Configure the *`enum.properties`* and *`enumgui.properties`* files as follows:

1 Replace the <*REPLACE_HOSTIP_HERE*> with the actual IP address of the appliance.

END OF STEPS

Login to enum

To start the ENUM Web Client on an ESM appliance, use port 8083 from any client:

`http://<appliance ip address>:8083`

Log files

The ENUM add-on log files are located in:

/opt/enum/log/enum.log

/opt/enum/log/NB_Server.log

The Tomcat server log file is located in */opt/enum/tomcat/logs/catalina.out*.

ldrm-server

Purpose

The **ldrm-server** package writes and tests rules and compiles these rules into the *rules.jar* file.

Before you begin

Ensure the following:

- Jython and JDK should be installed.
- Working knowledge of Jython is required for creating rules.
- DHCP server should be enabled with LDRM callout. Additional Policies section in DHCP server should be set as below:

```
APICalloutLibraryName1=libldrm_api
```

- Ensure that the following callouts are enabled in the additional policy section of the DHCP server:

```
APIPacketReceiptCallout1=1
APIDiscoverCallout1=1
APIRequestCallout1=1
APIAckCallout1=1
APIBootpCallout1=1
```

Configuration

Do the following:

1. Configure *ldrmcompiler.properties* and specify the JDK and Jython home directory, if it is not set to the default value specified in the configuration file.
2. Configure *rules.py* file and add the rules for LDRM to process.
3. Click the package commands icon on the LDRM server package.
4. **Run** compile-rules.

Verify that *rules.jar* has been created successfully and copied to the stage directory.

END OF STEPS

Troubleshooting

If *rules.jar* creation is not successful:

- In */opt/qip/ldrm/conf/ldrmcompiler.properties*, check if the JDK and Jython path are specified properly. If not, provide proper paths and run compile-rules.
- If paths are proper, check */opt/qip/ldrm/conf/rules.py* for proper rules.

ldrm-remote

Purpose

The **ldrm-remote** package modifies fields and options of both incoming and outgoing DHCP packets based on the rules set by the **ldrm-server** package.

Before you begin

The DHCP server should be enabled with the LDRM callout. The “Additional Policies” section in the DHCP server should be set as below:

APICalloutLibraryName1=libldrm_api

Ensure that the following callouts are enabled in the additional policy section of the DHCP server:

APIPacketReceiptCallout1=1

APIDiscoverCallout1=1

APIRequestCallout1=1

APIAckCallout1=1

APIBootpCallout1=1

Configuration

None

Log files

The log files are available in the following location:

/opt/qip/log/LDRMCallout.log

/opt/qip/log/ldrm.log

2 ESM appliance package configuration

Overview

Purpose

This chapter contains information on customizing ESM appliance configuration files, as well as procedural steps for deploying ESM Disaster Recovery.

Contents

This chapter covers these topics.

Configuration file handling

Overview

Purpose

This section contains the following information:

- Customizing *qip.pcy* on an ESM appliance
- Activating the ESM appliance license key
- Downgrading **`enterprise`** and **`sybase`** packages
- Reusing previously customized configuration files

  During package upgrades, it is important that configuration files that were customized for the previous installation of the package be preserved for reuse after the latest version of a package has been installed. This is particularly important for the ESM appliance license key file (*.Lic*).
- Deploying ESM Disaster Recovery

Modify qip.pcy file policies on an ESM appliance

Purpose

To configure the *qip.pcy* file on an ESM appliance.

Procedure

To modify policies on an enterprise server appliance, follow these steps.

1. In AMS, locate the appliance on which the **`vitalqip7.2-enterprise`** package is installed, and expand the **Config Files** folder.

   Result: A list of Enterprise Server configuration files opens.

2. Select the **/opt/qip/qip.pcy** file.

   Result: The Config File Properties pane opens.

3. Click **Modify**.

   Result: The Config File Editor pane opens.

4. Use the **Find** option if necessary to locate the policies in Table 1-11.

5. In the `[Global]` section, specify an encrypted password for the **qipman** user. The password can be encrypted using the **`qip-crypt`** utility shipped with the Enterprise Server.

   The default encrypted password for the **qipman** user is already provided in the default *qip.pcy* file. Alcatel-Lucent recommends that the default password be changed for security reasons.

   ```
   User=qipman
   Password=029b66069308af88eb4ab9068efb41a44b82
   ```

   For information on **`qip-crypt`**, refer to "qip-crypt" (p. B-2).

6. In the [`VitalQIP Message Service`] section, define the message routes for DNS and DHCP messages.

MessageRoute=DNSUpdateRR:A:0:QIP Update Service (Update RR):VitalQIP QIP Update Service:*<ip_address_of_qip_update_service>*

MessageRoute=DHCP:A:0:VitalQIP QIP Update Service - DHCP:VitalQIP QIP Update Service:*<ip_address_of_qip_update_service>*

MessageRoute=DNSUpdateRR:A:0:DNS Update Service (Update RR):VitalQIP DNS Update Service:*<ip_address_of_dns_update_service>*

MessageRoute=DNSUpdateObject:A:0:VitalQIP DNS Update Service - DNSUpdateObject:VitalQIP DNS Update Service:*<ip_address_of_dns_update_service>*

7 In the `[VitalQIP Remote Service]` section, specify the address of the File Generation Server:

FileGenerationServer=*<ES IP address>*

8 Additionally, you can establish a default Debug setting in the `[Global]` section of *qip.pcy* to enable the creation of log files. It is set to **None** by default.

Important! Do not modify the default port settings in the *qip.pcy* file. Only these specific ports for the default ES services are allowed by the appliance firewall rules.

9 If you wish to enter a comment, enter up to 255 alphanumeric characters in the **Comments** field.

10 Click **Push**.

Result: A dialog box opens with the message **Config File pushed(deployed) to the appliance**.

11 Click **OK**.

Result: The *qip.pcy* file is pushed to the appliance and all services are started.

END OF STEPS

Activate license key on an ESM appliance

Purpose

To activate the license key on an ESM appliance (since ESM appliances are shipped with no license key for VitalQIP).

Before you begin

Before activating an ESM appliance in AMS, perform a query to pull in the embedded package status of the ESM appliance into the AMS database. For instructions on how to perform a query, refer to "Manage configuration history", in Chapter 2 of the *Appliance Management Software User's Guide*.

Procedure

To activate a license key, follow these steps.

1. Procure a VitalQIP license key from Alcatel-Lucent and save it as a text file on your local machine.

2. In AMS, locate the appliance on which the **`vitalqip7.1-enterprise`** or **`vitalqip7.2-enterprise`** package is installed and expand the **Config Files** folder.

   Result: A list of Enterprise Server configuration files opens.

3. Select the **/opt/qip/.Lic** file.

   Result: The Config File Properties page opens.

4. Click **Modify**.

   Result: The Config File Editor page opens.

5. Select the **Upload** option and click **Browse**.

   Result: A File Upload dialog box opens in your browser.

6. Locate the *.Lic* file that you saved on your local machine and select it.

Result: The license key is imported into the Config File Editor window.

7 If you wish to enter a comment, enter up to 255 alphanumeric characters in the **Comments** field.

8 Click **Push**.

Result: A dialog box opens with the message **Config File pushed(deployed) to the appliance**.

9 Click **OK**.

Result: The license key file is pushed to the appliance and all services are started.

10 Confirm that the license key was deployed successfully by bringing up the VitalQIP Web Client GUI on the enterprise server.

END OF STEPS

Downgrade Enterprise/Sybase package

Purpose

To downgrade an ESM appliance to a previous version of the **`vitalqip-enterprise`** package.

Before you begin

- You need to uninstall and reinstall Sybase ***only*** if the downgraded Enterprise package version requires an older version of Sybase or a different architecture (32-bit/64-bit) version of Sybase.
- Use the **ammuser** account and a remote login tool, such as **`putty`**, to perform maintenance work on an ESM appliance. For information on setting up **ammuser**, refer to "Enable a user account login", in the *Appliance Management System User's Guide*.

Procedure

To revert to a previous version of the Enterprise and Sybase packages, follow these steps.

Method 1

1 Back up your data using VitalQIP export utility, as follows.

a. In AMS, shut down all VitalQIP services.

b. Log into the appliance as **ammuser**.

c. Run the export script:

`/opt/qip/usr/bin/exportdb.sh`

The database is exported to the `/opt/qip/export/<current_time>` directory. Any errors are logged in */opt/qip/log/qip-export.ammuser.log*. The results of the export are logged in */opt/qip/qip-result.ammuser.log*.

2 Unassociate the Enterprise (current latest version) and Sybase packages, and then perform a Deploy from AMS.

3 On the ESM, remove all files/directories under */opt/qip* ***except*** for */opt/qip/export* (and children) directory (removing the */opt/qip/export/** directory would remove the backed up data from step 1c above).

4 In AMS, locate the appliance in the Appliances hierarchy, click the **Configuration History** tab, and roll back to an earlier version of the Enterprise and Sybase package configuration.

5 Restore data using the VitalQIP import utility, as follows.

a. In AMS, shut down all VitalQIP services.

b. Log into the appliance as **ammuser**.

c. Run the import script `/opt/qip/usr/bin/importdb.sh <path_to_import_dir>`, for example:

`/opt/qip/usr/bin/importdb.sh /opt/qip/export/<exported_dir_name>`

Any errors are logged in */opt/qip/log/qip-import.ammuser.log*. The results of the import are logged in */opt/qip/qip-result.ammuser.log*.

END OF STEPS

Method 2

1 Back up your data using the VitalQIP export utility, as follows.

a. In AMS,shut down all VitalQIP services.

b. Log into the appliance as **ammuser**.

c. Run the export script:

`/opt/qip/usr/bin/exportdb.sh`

The database is exported to the `/opt/qip/export/<current_time>` directory. Any errors are logged in */opt/qip/log/qip-export.ammuser.log*. The results of the export are logged in */opt/qip/qip-result.ammuser.log*.

2 Unassociate the Enterprise (current latest version) and Sybase packages, and then perform a Deploy from AMS.

3 On the ESM, remove all files/directories under */opt/qip* ***except*** for */opt/qip/export* (and children) directory (removing the */opt/qip/export/** directory would remove the backed up data from step 1c above).

4 Associate the Sybase package and the previous version of the Enterprise package. Then deploy via AMS.

Note: AMS does not allow the selection of an older version of an Enterprise package in the Associate packages screen when a more recent version is available in the AMS database. First, disassociate the package from all appliances and then delete the more recent version from the **Packages** menu.

5 Restore data using the VitalQIP import utility, as follows.

a. In AMS, ensure that all VitalQIP services are shut down.

b. Log onto the appliance as **ammuser**.

c. Run the import command `/opt/qip/usr/bin/importdb.sh <path_to_import_dir>`, for example:

`/opt/qip/usr/bin/importdb.sh /opt/qip/export/<exported_dir_name>`

Any errors are logged in */opt/qip/log/qip-import.ammuser.log*. The results of the import are logged in */opt/qip/qip-result.ammuser.log*.

END OF STEPS

Upgrade ESM appliance from VitalQIP 7.1 to VitalQIP 7.2

Purpose

To upgrade an ESM appliance that uses the **`vitalqip71-enterprise`** and 32-bit **`sybase`** packages to an enterprise package that uses a 64-bit version of Sybase (**`sybase64`**).

Before you begin

Use the **ammuser** account and a remote login tool, such as **`putty`**, to perform maintenance work on an ESM appliance. For information on setting up **ammuser**, refer to "Enable a user account login", in the *Appliance Management System User's Guide*.

Procedure

To upgrade an ESM appliance from 32-bit Sybase to 64-bit Sybase, follow these steps.

1 Back up your data using the VitalQIP export utility, as follows.

a. In AMS,shut down all VitalQIP services.

b. Log into the appliance as **ammuser**.

c. Run the export script:

`/opt/qip/usr/bin/exportdb.sh`

The database is exported to the `/opt/qip/export/<current_time>` directory. Any errors are logged in */opt/qip/log/qip-export.ammuser.log*. The results of the export are logged in */opt/qip/qip-result.ammuser.log*.

2 In AMS, unassociate the older vitalqip-enterprise and **`sybase`** packages, and then deploy.

3 On the ESM appliance, remove all files/directories under */opt/qip* ***except*** for */opt/qip/export* (and children) directory (removing the */opt/qip/export/** directory would remove the backed up data from step 1c above).

4 Manually remove the */opt/sybase* directory.

5 In AMS, associate the **`sybase64`** package and the newer version of the Enterprise package that requires it (for example **`vitalqip7.2-enterprise`**), and then deploy.

6 Restore data using the VitalQIP import utility, as follows.

a. In AMS, ensure that all VitalQIP services are shut down.

b. Log onto the appliance as **ammuser**.

c. Run the import command `/opt/qip/usr/bin/importdb.sh <path_to_import_dir>`, for example:

`/opt/qip/usr/bin/importdb.sh /opt/qip/export/<exported_dir_name>`

Any errors are logged in */opt/qip/log/qip-import.ammuser.log*. The results of the import are logged in */opt/qip/qip-result.ammuser.log*.

END OF STEPS

Configure ESM to use SSL for GUI and remote servers

Purpose

To configure an appliance to use SSL communication for GUI and remote servers.

Procedure

To configure an ESM appliance to use SSL communication, follow these steps.

1. Log in as **root** and SSH to the ESM Appliance.

2. Create a set of keys for VitalQIP running on the ESM Appliance. You are prompted to create a keystore password. The certificate is valid for ten years. Execute the following.

```
/opt/jre-1.6.0-sun/bin/keytool -genkey -keyalg RSA -alias vitalqip -validity
   3652 -keystore /opt/qip/qipkeystore
```

Result: After running this command, you are prompted for a series of questions.

```
Enter keystore password:
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Enter key password for vitalqip
(RETURN if same as keystore password):
```

3. Please remember the password, because you need to enter it later in the password value and also at step 6) when you encrypt the password for entry at later steps in the *qip.pcy* file of each machine. The rest of the questions are informational. When you are prompted at the end for a key password, hit return, as you want to keep the key password and keystore password the same.

4. Create a self-signed certificate file for VitalQIP. You are prompted for the keystore password you created in step 2 above. Execute the following.

```
/opt/jre-1.6.0-sun/bin/keytool -export -alias vitalqip -keystore
   /opt/qip/qipkeystore -file /opt/qip/vitalqip.cer
```

5 Change the **cacerts** password to match the password you chose above for the qipkeystore. Execute the following.

```
/opt/jre-1.6.0-sun/bin/keytool -storepasswd -new <password> -keystore
   /opt/jre-1.6.0-sun/lib/security/cacerts -storepass changeit
```

6 Import the self signed certificate into the ESM Appliance **cacerts** keystore. Execute the following.

```
/opt/jre-1.6.0-sun/bin/keytool -import -alias vitalqip -keystore /opt/jre-
   1.6.0-sun/lib/security/cacerts -file /opt/qip/vitalqip.cer -storepass
   <password>
```

7 Securely transfer the certificate file (*vitalqip.cer*) and the keystore (*qipkeystore*) to $QIPHOME on the machine running the GUI client or remote server. Also, transfer the files to the machine where you are running the AMS Web GUI (any machine with a Web browser).

8 Run **qip-crpyt *<your_storepass_password>***. You will need the encrypted string produced in some of the steps below.

9 Log in to the GUI Client or Remote Server machine and run Steps 7 to 8 as root/administrator:

10 Change the **cacerts** password on the GUI client or Remote Server to the password you chose above.

ALU Appliance

```
/opt/jre-1.6.0-sun/bin/keytool -storepasswd -new <password> -keystore
   /opt/jre-1.6.0-sun/lib/security/cacerts -storepass changeit
```

Non Appliance

```
$QIPHOME/jre/bin/keytool -storepasswd -new <password> -keystore
   $QIPHOME/jre/lib/security/cacerts -storepass changeit
```

11 Import the self signed certificate into the GUI client or Remote Server cacerts keystore.

ALU Appliance

```
/opt/jre-1.6.0-sun/bin/keytool -import -alias vitalqip -keystore /opt/jre-
   1.6.0-sun/lib/security/cacerts -file /opt/qip/vitalqip.cer -storepass
   <password>
```

Non Appliance

```
$QIPHOME/jre/bin/keytool -import -alias vitalqip -keystore
   $QIPHOME/jre/lib/security/cacerts -file $QIPHOME/vitalqip.cer -storepass
   <password>
```

12 Log into the AMS GUI and perform the following steps for ESM and AMM.

13 From Appliance -> Packages (or Appliance Groups -> Packages), click **Configure** next to the VitalQIP Enterprise or VitalQIP Remote package.

Result: A new Configure Package browser window opens.

14 Click on the Config File */opt/qip/qipkeystore*.

15 Select the **Upload** option and browse to the file on your machine from where you launched the AMS GUI.

16 Select the *qipkeystore* file you transferred from the ESM (Step 7 above).

17 Click on the Config File */opt/qip/vitalqip.cer*.

18 Select **Upload** option and browse to the file on your machine from where you launched the AMS GUI.

19 Select the *vitalqip.cer* file you transferred from the ESM (Step 7 above).

20 Click on the Config File */opt/qip/qip.pcy*.

21 Select the **Edit this config file** option and make the following changes.

- Replace the MessageRoute in *qip.pcy* with SecureMessageRoute so that it appears as:

```
SecureMessageRoute =
   <id>:<flags>:<ACK_timeout>:<desc>:<port>:<Server_IP>:?<*#>
```

- In the Global section, change:

  `;SecureIncomingMessageServiceConnections = false` to
  `SecureIncomingMessageServiceConnections = true`

- In the VitalQIP SSL Tunnel Service section, uncomment and edit these two lines:

```
PassPhrase = <encrypted_password_from_qip-crypt_output>
KeysFile = qipkeystore
```

22 ***On ESM appliance only***.

- In the `[VitalQIP RMI QAPI Service]` section, add/update the following:

```
QAPISSL_Scheduler.Secure = true
QAPISSL_Scheduler.PassPhrase = <encrypted_password_from_qip-crypt_output>
QAPISSL_Scheduler.KeysFile = qipkeystore
```

- In the `[VitalQIP RMI Scheduler Service]` section, add/update the following:

```
SchedulerNames = QAPISSL_Scheduler
QAPISSL_Scheduler.ExecutorName = QAPI
QAPISSL_Scheduler.Secure = true
QAPISSL_Scheduler.PassPhrase = <encrypted_password_from_qip-crypt_output>
QAPISSL_Scheduler.KeysFile = qipkeystore
QAPISSL_Scheduler.BasePort = 62469
QAPISSL_Scheduler.Port = 62468 UserJVMOpt = -
   Djava.security.policy==/opt/qip/rmisched-security.policy
QAPISSL_Scheduler.VirtualMachineParams = -
   Djava.security.policy==/opt/qip/rmisched-security.policy
```

23 ***On AMM appliance*** (and ESM if the ESM is being used as a remote server as well).

- In the `[VitalQIP Remote Service]` section, add/update the following:

```
SchedulerName = QAPISSL_Scheduler
RequireSSLConnection=true
```

24 Deploy the changes to the respective appliances.

25 Log into the non-appliance GUI client and remote servers and perform these steps:

26 Edit the *$QIPHOME\qip.pcy* and make the following changes

- Replace the MessageRoute in *qip.pcy* with SecureMessageRoute so that it appears:

```
SecureMessageRoute =
   <id>:<flags>:<ACK_timeout>:<desc>:<port>:<Server_IP>:?<*#>
```

- In the Global section, change:

```
;SecureIncomingMessageServiceConnections = false
```

to

```
SecureIncomingMessageServiceConnections = true
```

- In the VitalQIP SSL Tunnel Service Section, uncomment and edit these two lines:

```
PassPhrase = <encrypted_password_from_qip-crypt_output>
KeysFile = qipkeystore
```

- In the `[VitalQIP Remote Service]` section, add/update the following:

```
SchedulerName = QAPISSL_Scheduler
RequireSSLConnection=true
```

27 Restart the VitalQIP Message Service and VitalQIP SSL Tunnel Service on all configured systems, as well as the VitalQIP RMI Scheduler Service on the ESM appliance, and the VitalQIP Remote Service on the remote servers.

END OF STEPS

Configure ESM to use SSL for VitalQIP Web Client

Purpose

To configure an ESM appliance for SSL access to the VitalQIP Web Client.

Procedure

To configure an ESM appliance for SSL access to the VitalQIP Web Client, follow these steps.

1 Log in as **`root`** and SSH to the ESM Appliance.

2 Create a set of keys for VitalQIP running on the ESM Appliance. You are prompted to create a keystore password. The certificate is valid for ten years. Execute the following.

```
/opt/jre-1.6.0-sun/bin/keytool -genkey -keyalg RSA -alias vitalqip
-validity 3652 -keystore /opt/qip/tomcat/conf/tomcatkeystore
```

Result: After running this command, you are prompted for a series of questions.

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=<>, OU=<>, O=<>, L=<>, ST=<>, C=<> correct?
[no]: yes

Enter key password for <vitalqip>
(RETURN if same as keystore password):
Re-enter new password:
```

3 In AMS, click the **Services** tab in the Properties page for the ESM appliance, select the **`qip-tomcat`** service and click **Stop**.

4 Click the **Packages** tab, locate the VitalQIP Enterprise package in the *Direct Packages* list and click **Configure**.

Result: A Configure Package browser window opens.

5 From Appliance -> Packages (or Appliance Groups -> Packages), click **Configure** next to the VitalQIP Enterprise package.

Result: A new Configure Package browser window opens.

6 Click on the Config File */opt/qip/tomcat/conf/server.xml*.

7 Select the **Edit this config file** option and make the following changes:

a. Comment the `Non-SSL Connector` section.

b. Uncomment the `SSL Connector` section.

8 Click the **Services** tab again in the Properties page for the ESM appliance, select the **qip-tomcat** service and click **Start**.

9 Log into the ESM using this address: **https://<*ESM_IP_address*>:8443/qip**

END OF STEPS

Configure SSL between AMS and ESM/AMM

Purpose

To configure an ESM appliance for SSL access to the AMS server.

Procedure

To configure an ESM appliance for SSL access to the AMS server, follow these steps.

1 SSH log in to AMS server as **root**.

2 Create a set of keys for AMS server. You are prompted to create a keystore password. The certificate is valid for ten years. Execute the following.

```
/opt/ams/jre/bin/keytool -genkey -keyalg RSA -alias vitalqip
-validity 3652 -keystore /opt/ams/tomcat/conf/amskeystore
```

Result: After running this command, you are prompted for a series of questions.

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=<>, OU=<>, O=<>, L=<>, ST=<>, C=<> correct?
[no]: yes
Enter key password for <vitalqip>
(RETURN if same as keystore password):
Re-enter new password:
```

3 Stop the AMS Tomcat server.

```
cd $AMSHOME/etc
./ams-stop-server
```

4 Edit the */opt/ams/tomcat/conf/server.xml* file. Comment out the Non-SSL connector and add the SSL connector as follows:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080
<Connector port="8080" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true" />
-->
<!-- SSL Connector - Start -->
<Connector port="8443"
maxHttpHeaderSize="8192"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
scheme="https"
secure="true"
clientAuth="false"
sslProtocol="TLS"
keystoreType="JKS"
keystoreFile="/opt/ams/tomcat/conf/amskeystore"
keystorePass="password_from_step1"/>
<!-- SSL Connector - End -->
```

5 Start the Tomcat server.

```
cd $AMSHOME/etc
./ams-start-server
```

6 Execute the following command:

```
/sbin/iptables -L -nv
```

Ensure the presence of a firewall rule to allow port 8443 traffic.

7 If there is no rule for port 8443, edit the */etc/sysconfig/iptables* file, by logging in as **root**.

8 Add the following entry for port 8443.

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport
   8443 -j ACCEPT
```

9 Restart iptables by executing the following command:

```
/sbin/service iptables restart
```

10 Display the rule for port 8443 by executing the following command:

```
/sbin/iptables -L -nv
```

END OF STEPS

Configure AMS URI on ESM/AMM Appliance from console/serial access.

enable>config>ams

https://<AMS_IP_Address:8443/ams/amsrpc

save, verify and authenticate Appliance to communicate with AMS Server on SSL.

Debug information

Purpose

For debugging purposes, check the status of the node directly on the box by using the following commands.

CLI commands

Logon to a node as super user and run the following commands:

- To check the active node and service state

```
/usr/sbin/crm_mon -V -1
```

- To see the service fail count

```
/usr/sbin/crm_failcount -G -r <service name>
```

- To reset the service fail count to zero

```
/usr/sbin/crm_failcount -v 0 -r <service name>
```

A VitalQIP policy files

Overview

Purpose

This appendix describes the policies that are in the condensed *qip.pcy* file included in the remote and enterprise server packages.

Contents

This appendix covers these topics.

Global section

The global section of the policy file is where you set up policies that affect the entire *qip.pcy* file. For example, debug polices established in this section are treated as global and are passed to every service. Do not modify the Global Section header because the installation program uses it to insert specific values, such as the server name, user name and encrypted password.

Debug

Value	Default: None Allowed: See below.
Description	This policy sets the global debug level and is passed to every service.

The debug policy

Each VitalQIP service (with the exception of RMI QAPI, which uses Java debug policies only) has a **debug** policy that can be specified in either the Global section or in a specific policy section of *qip.pcy*. Most clients and CLIs read the policy file in the same way that services do, and adhere to the value specified for the debug policy.

Important! When you wish to diagnose a potential problem, first access the Event Viewer in Windows or *syslog* in UNIX to determine the problem.

The following table shows the values for the debug policy that can compose a string.

Table A-1 Debug policy values

Function	Values
Debug level	The following values can be used for the debug level: **All** - The maximum level of debugging; all levels. **LevelCritical** - A critical error is one that shuts down the program. Only critical messages are logged. **LevelError** - An error has occurred, but the program should continue. Critical messages are included. **LevelWarning** - The program has encountered an unexpected issue but continues. Errors and critical messages are included with these warnings. **LevelInfo** - These are informational messages about the program events and flow. These messages include critical messages, errors, and warnings. **LevelDebug** - Indicates that all levels should be logged. **None** - No debugging. This is the default.
List of application/library layers from which to display debug messages	The following values are the application/library layers: **Application** - The program itself (service, client, CLI). **QSICommon** - The low level common library. **QSINet** - The network related library. **QIPDB** - The core VitalQIP database routine library. **QAPI** - The VitalQIP business layer API.

Function	Values
Additional debug features	The following values are additional debug features: **FeatureTimestamp** - Each message in the log is prefixed with a date/time stamp in DDD, MMM dd hh:mm:ss.ms format, for example, Tue, May 31 13:10:30.456. **FeatureDeltaTime** - Time is displayed as the difference from the previous message. **FeatureRelativeTime** - Time is displayed as the difference from the first message. **FeatureISO8601** - Each line is prefixed with date and time in a format that conforms to ISO 8601. The date/time stamp format is YYYY-MM-DDThh:mm:ss.ms, where the capital letter T is used to separate the date and time components, for example, 2005-05-31T13:10:30.456 **FeatureSeverityStamp** - Each line is prefixed with its severity. **FeatureBackup** - This creates a copy of a previous debug file to *<debugfile>.bak_1.log* before logging to the current debug file (*.log* is kept to maintain application association). To specify the number of backup debug files you wish to maintain, set the **DebugRotateMaxDepth** policy to a value greater than 1. **FeatureModule** - This displays the library/location of the original message. **FeatureThreadStamp** - Each line is prefixed with its thread ID. **FeatureStackTrace** - This displays function entrance and must be enabled when you submit bugs on VitalQIP. **FeatureFullStackTrace** - Displays function exit as well as entrance. **FeatureProfile** - Function execution times are displayed (also enables FeatureStackTrace). **FeatureValues** - Values read from or written to the VitalQIP database are printed to the debug log file. **FeatureRotateLogs** - Enables log file rotation (starts new log file).

For example, to enable debugging for the application and QSICommon, for warning messages and above with a timestamp, specify:

```
debug = LevelWarning Application QSICommon FeatureTimestamp
```

To enable maximum debugging, specify:

```
debug = All
```

By default, debug files are located in *$QIPHOME/log*.

Log file rotation

If you enable **FeatureRotateLogs**, you can ensure that log files rotate automatically using two additional debug policies: **DebugRotateFileSize** and **DebugRotateInterval**. Both policies have default values of zero, meaning that no rotation occurs based on size or time. These policies can be used together.

- Use **DebugRotateFileSize** to specify the maximum debug file size. For example:

  `DebugRotateFileSize=500K` - New debug file starts at 500K

  `DebugRotateFileSize=50M` - New debug file starts at 50 MB

- Use **DebugRotateInterval** to specify how often to rotate the debug file. For example:

  `DebugRotateInterval=90m` - New debug file starts every 90 minutes

  `DebugRotateInterval=12h` - New debug file starts every 12 hours

  `DebugRotateInterval=2d` - New debug file starts every 2 days

Debug filenames

Debug filenames may contain format characters that expand to date strings. For example, **`DebugFile=qip-msgd.%A.%B.%d.log`** would translate into a filename such as:

```
$QIPHOME/log/qip-msgd.Wednesday.April.2.log
```

Your platform may support many additional format strings. Use an Internet search engine to search for **`strftime Linux`**.

> **Note:** You can prefix a filename with the '|' character to send debug to a filter program (for example, **`DebugFile="|my_debug_filter"`**). Filter programs are restarted if they crash, although some debug output may be lost.

Sample debug filename format characters are described in the following table.

Table A-2 Debug filename format characters

Character	Description
%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%d	Day of month as decimal number (01 - 31)
%H	Hour in 24-hour format (00 - 23)
%j	Day of year as decimal number (001 - 366)
%m	Month as decimal number (01 - 12)

Character	Description
%M	Minute as decimal number (00 - 59)
%S	Second as decimal number (00 - 61)
%w	Weekday as decimal number (0 - 6; Sunday is 0)
%W	Week of year as decimal number, with Monday as first day of week (00 - 53)
%y	Year without century, as decimal number (00 - 99)
%Y	Year with century, as decimal number
%Z	Time-zone name or abbreviation; no characters if time zone is unknown
%%	Percent sign

Message Service behavior

The VitalQIP Message Service performs the following functions:

- Queues messages until they can be processed by another service
- Forwards SSL-enabled or cleartext messages to multiple destinations
- Provides message queue length restrictions
- Provides disk-based storage for messages
- Accepts messages from more than one source
- Provides reliable transport for remote sources
- Maintains compatibility with previous version of the Message Service

The VitalQIP Message Service queues messages from the DHCP server, DNS server, DHCP monitor services, the VitalQIP GUI, and the VitalQIP QIP Update Service and forwards the messages to other services. The final destination of messages sent to the VitalQIP Message Service depends entirely upon the message type. For example, the DHCP server sends messages of type 1 that are typically sent to the VitalQIP QIP Update Service.

VitalQIP Message Service policy

MessageRoute

Value	Default: See Table A-3 for definitions of the values Allowed: <id>, <flags>, <ACK timeout>, <desc>, <port/servicename>, <Server IP>, <backup>
Description	The Message Service is generic. It forwards and routes multiple message types to any number of destinations controlled by this policy. The **MessageQueue** policy is controlled by the **MessageRoute** policy. This policy defines a destination for message of type <*id*>. The <*id*> must be the same as the <*id*> in the **MessageQueue** policy.

The MessageRoute policy is specified as:

```
MessageRoute =
   <id>:<flags>:<ACK_timeout>:<desc>:<service_name>:<Server_IP>:…<*#>
```

Note: You can use either commas (,) or colons (:) to separate the values.

This policy defines where messages are sent/routed. There can be any number of MessageRoutes for a given message type. The following table describes the MessageRoute values.

Table A-3 MessageRoute values

MessageRoute value	Description
Message ID <*id*>	Numeric. The Message ID uniquely identifies the type of messages received by the Message Service. It must agree with the <*id*> of the MessageRoute policy. Currently, the following message types are handled: **1 or DHCP** - Messages which come from a DHCP server. **3 or Audit** - Audit messages which are sent from the VitalQIP client and QIP Update Service. **9 or DNSUpdateObject** - Messages that describe an object to be updated in DNS. Such messages are sent from the VitalQIP client and from QIP Update Service to the DNS Update Service. VitalQIP clients only send these messages if the **Use DNS Update Service** policy is set to True. **10 or DNSUpdateRR** - Messages that describe a resource record added to or removed from a DNS server. Such messages are sent from DNS servers and from VitalQIP clients to the DNS Update Service. VitalQIP clients only send these messages if the **Use DNS Update Service** policy is set to True.

MessageRoute value	Description
Flags <*flags*>	The Flags field specifies a list of values for message processing. Each space in the flags field corresponds to one configuration value. Currently, three flag field spaces are defined. Valid values for field 1 are: **A** - **Asynchronous**. Messages are sent asynchronously with respect to other routes. See "Asynchronous example" (p. A-11). Valid values for field 2 are: **L** - Lockstep. Used in combination with the first field as follows: **.** - Indicates that the route uses the default behavior for a flag. It is used as a placeholder since the flags are position dependent. It does not need to be specified. Valid values for field 3 are: **B** - **Load Balance**. Balance message delivery between each destination. A MessageRoute "load balances" when it has a message to send and it has not received an ACK for a message that it has sent previously. See "Load Balance example" (p. A-12). **R** - **Primary Reconnect**. Treats the first destination as primary and attempts to reconnect. It is independent of the preceding two flags (for example ALR, SLR, A.R, S.R). See "Primary Reconnect example" (p. A-12).
ACK Timeout <*ack timeout*>	The number of seconds to wait for an ACK from the server (default is 0, no timeout). Use of this value is not recommended since another message is sent to the service immediately upon timeout. If multiple messages are sent due to multiple timeouts, the TCP queue to the service may fill up.
Destination Description <*desc*>	The description of the message route (for example, you could use the description "QIP Update Service" for messages destined for **`qip-qdhcpd`**).

MessageRoute value	Description
Destination Port Name <*port/servicename*>	The port or service name of where the message is being sent. Port names must be defined in the appropriate services file. The port and service names are as follows: **qip-dns**- VitalQIP DNS Update Service **qip-qdhcp**- VitalQIP QIP Update Service **qip-msgd** - VitalQIP Message Service Use the port name if the target service is listening on its well-known port. Use the service name if the service is listening on an ephemeral port tunneled through the Message Service. The Message Service uses the MessageServicePort value to contact the IP address specified in the IP Address of the Primary Server <*server_ip*> and requests a conduit connection to the service specified in the port name of the message route.
IP Address of the Primary Server <*server_ip*>	The IP address of the enterprise server running on the specified port in the Destination Port Name <*port/servicename*>.
Backup Servers <…>	A list of alternate servers where there is a service running on the specified port specified in the Destination Port Name <*port*>.
<*#>	Destination multiplier. Allows you to specify the number of connections you wish to open for load balancing on the backup servers, rather than listing duplicate destinations multiple times.

The following are MessageRoute examples:

Asynchronous example

```
MessageRoute = 1:A:0:QIPUpdateService: VitalQIP QIP Update
   Service:192.0.2.22:192.0.2.25
MessageRoute = 1:A:0:DNSUpdateService: VitalQIP DNS Update
   Service:127.0.0.1:192.0.2.1:192.0.2.3
```

These message routes have the following characteristics:

- They define two routes for messages of type 1 (QIP Update messages).
- Due to the ‘A’ flag, messages are sent to both destinations as fast as possible. In other words, the Message Service does not wait for messages to be sent to the QIP Update Service before sending messages to the DNS Update Service.
- The first route is to the port defined by VitalQIP QIP Update Service, and messages are sent to 192.0.2.22 unless it is down, in which case messages are sent to 192.0.2.25.
- The second route tries to update the DNS Update Service on the local machine, but if that service is not up, it attempts to update the Lucent DNS Service on 192.0.2.1. If that service is down, it sends messages to 192.0.2.3.

Primary Reconnect example

You can configure the Message Service to reconnect to a primary destination for a given route by specifying "R" in the third space of the Flags field. Previously, if multiple destinations were configured for a route, each destination was treated equally: the Message Service would not attempt to "reconnect" to the first destination (primary).

```
MessageRoute = 1:A.R:0:QIPUpdateService:qip-qdhcp:127.0.0.1:3119:127.0.0.1
```

This message route has the following characteristics:

- Each type 1 message attempts to connect to **`qip-qdhcp`** on the local host.
- If it is down, it sends messages to the DNS Update Service on port 3119.
- The Message Service actively attempts to restore a connection to **`qip-qdhcp`** indefinitely.

Load Balance example

```
MessageRoute 1:A.B:0:QIPUpdateService:VitalQIP QIP Update
   Service:192.0.2.7*3
```

The on-demand load balancing example above has the following characteristics:

Each type 1 message is sent to the QIP Update Service:

- Upon startup, the Message Service will make three connections to 192.0.2.7.
- If the Message Service receives message *n*, it will send it to 192.0.2.7 and wait for an ACK (ACK1).
- If ACK1 is received from 192.0.2.7 before the next message (*n+1*) is received, message *n+1* will be sent to 192.0.2.7 on the first connection since that connection is free to process another message.
- If message *n+1* is received before ACK1, message *n+1* will be sent to 192.0.2.7 using a different connection.
- Similarly, if message *n+2* is received before ACK1 and ACK2, message *n+2* will be sent to 192.0.2.7 using the third connection.
- Suppose all destinations are processing a message and the Message Service is waiting for an ACK from each. If message *n+3* is received, it will be queued and the Message Service will wait for the ACKs. Whichever process/thread on 192.0.2.7 is the first to respond with an ACK will get message *n+3*.
- In all cases, the next message in the queue is sent to the first destination to respond with an ACK. If the first destination always responds with an ACK before the next message is queued, that destination will process all the messages and there is no reason to bother the other destinations.

Note: In the above example, where three different processes are running on the same host address, throughput is increased because each process can perform the necessary

CPU processing while the others are blocked, waiting for disk access to update the database. For database operations where it may be beneficial to have the database server running on the same machine as the QIP Update Service and the Audit Update Service, this would provide nearly equivalent, and sometimes greater throughput than specifying different addresses.

VitalQIP Remote Service policies

FileGenerationServer

Value	Default: None Allowable value: RMI Scheduler Service's IP address
Description	This policy specifies where this Remote Service has its files generated.

FailOnFailedUserExit

Value	Default: False Allowed: True | False
Description	This policy determines if a network generation fails when a user exit returns a non-zero value. The following values can be specified: **True** - a network generation fails by having the user exit return a non-zero value. **False** - the Remote Service continues network generation even if the user exit fails.

B Password encryption

Overview

Purpose

This appendix describes the **`qip-crypt`** CLI that is used to encrypt the **qipman** password.

Contents

This appendix covers these topics.

qip-crypt

qip-crypt allows you to encrypt a password. **qip-crypt** takes the password as the first argument and sends a hexadecimal-string encrypted password to *STDOUT*. The **qip-crypt** CLI command must be run again and the new password placed in the *qip.pcy* file if the **qipman** password, the **qipadmin** password, the Schedule Password, or the Update Password is changed.

Important! **qip-crypt** is only intended for use with a password in the *qip.pcy* file. It should not be used to encrypt the database login. Database logins can be encrypted using third-party tools.

Synopsis

qip-crypt [***password***]

Parameters

qip-crypt recognizes the following parameters:

password	Specifies your current password. The **qipadmin** password must be alphanumeric with no special characters. Although **qip-crypt** accepts special characters, Sybase's sp_password will not.

C Appliance Install Manager

Overview

Purpose

This appendix describes the **aim** command, for use in troubleshooting packages installed on an appliance.

Contents

This appendix covers these topics.

aim command

Overview

The **aim** (Appliance Install Manager) command manages the **lpf** packages on an appliance. It is invoked by AMS, but may be useful during troubleshooting.

Usage

aim *<options>*

Options

Available options are:

--version	Prints version.
--info	Prints installation information.
--list	Lists installed packages.
--list-files *<package-name>*	Lists the contents of an installed package.
--install *<package-file>*	Installs a package.
--update *<package-file>*	Updates an installed package.
--verify *<package-name>*	Verifies an installed package.
--remove *<package-name>*	Removes an installed package.

Examples

The **list** option displays the installed packages, for example:

```
$ aim --list
jre-1.6.0-sun-1.6.0.04-1
vitalqip7.1-remote-7.1.155-3
qddns-4.1.3-2
```

The **list-files** option requires a package name and displays the files installed by a package, for example:

```
$ aim --list-files qddns
/etc/
/etc/amm/
/etc/amm/conf.d/
/etc/amm/conf.d/qip-named
/etc/amm/iptables.d/
/etc/amm/iptables.d/qip-named
/etc/init.d/
/etc/init.d/qip-named
/opt/
/opt/qip/
/opt/qip/named/
```

```
/opt/qip/named/.keep
/opt/qip/named/named.conf.default
/opt/qip/named/rndc.conf.default
/opt/qip/usr/
/opt/qip/usr/bin/
/opt/qip/usr/bin/dig
/opt/qip/usr/bin/dnssec-keygen
/opt/qip/usr/bin/dnssec-signzone
/opt/qip/usr/bin/host
/opt/qip/usr/bin/journalprint
/opt/qip/usr/bin/named
/opt/qip/usr/bin/named-checkconf
/opt/qip/usr/bin/named-checkzone
/opt/qip/usr/bin/nslookup
/opt/qip/usr/bin/nsupdate
/opt/qip/usr/bin/rndc
/opt/qip/usr/bin/rndc-confgen
```

Glossary

A

A
Address

A6
IPv6 address

AAAA
IPv6 address

AFSDB
AFS (Andrew File System) Data Base location

ALED
Alcatel-Lucent Electronic Delivery

AM
Appliance Manager

AMM
Appliance Management Module

AMS
Appliance Management Software ,

APL
Address Prefix List

C

CERT
Certificate

CLI
Command Line Interface

CNAME
Canonical name for a DNS alias

D

DHCP
Dynamic Host Configuration Protocol

DNAME
DNAME record providing aliases for a whole domain

DNS
Domain Name System

DNSKEY
Stores public key used in the DNSSEC authentication process

DORA
Discover Offer Request Acknowledge

DS
Delegation Signer

E

EDUP
External Dynamic Update Propagation

ESM
Enterprise Server Module

G

GPOS
Geographical position

H

HA
High Availability

HINFO
Host Information

I

iBGP
internal Border Gateway Protocol

IGP
Interior Gateway Protocol

ISDN
Integrated Services Digital Network

J

JRE
Java runtime executable

K

KEY
Public key, as used in DNSSEC

KX
Key Exchanger

L

LOC
Location information

M

MAC
Media Access Control

MB
Mail Box

MG
Mail Group member

MIBs
Management Information Bases

MINFO
Mailbox or mailing list information

MNAME
Defines the domain name of the name server that was the original or primary source of data for this zone

MR
Mail Rename domain name

MX
Mail Exchanger

N

NAPTR
Naming authority pointer

NDE
Network Data Extractor

NS
Authoritative Name Server

NSAP
Network Service Access Point address

NSEC
NextSECure resource record

NTP
Network Time Protocol

O

OSPF
Open Shortest Path First

P

PTR
domain name Pointer

PX
Pointer to X.400/RFC822 mail mapping information

R

RCODE
Response Code

RDATA
Resource record data

RP
Responsible Person

RRSIG
Resource Record SIGnature, part of the DNSSEC standard

RT
Route Through

S

SIG
Signature (Cryptographic public key signature)

SNMP
Simple Network Management Protocol

SOA
Start Of Authority

SPF
Sender Policy Framework

SRV
Server selection

SSHFP
SSH Key Fingerprint

SSL
Secure Socket Layer

T

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TXT
Text string

U

UDP
User Datagram Protocol

URL
Uniform Resource Locator

W

WKS
Well-Known Service

X

X25
X25 PSDN (Public Switched Data Network) address

Index