

perfSONAR MDM 3.2 Administrator's Guide

Last updated: 19-08-2009

Manual version 1.0

Activity: SA2

Dissemination level: PU

Document code: GN3-09-098

Authors: Antoine Delvaux (DANTE), Gina Kramer (DANTE), Piotr Pikusa (PSNC), Mario Reale (GARR), Szymon Trocha (PSNC), Domenico Vicinanza (DANTE)

Table of Contents

1	Introduction	1
2	Getting Started	3
2.1	Deciding which Services to Install	3
2.2	Supported Platforms	4
2.3	Supported Browsers	4
2.4	Prerequisite Software	4
2.4.1	Installing Prerequisite Software Using Packages	5
2.4.2	Starting and Stopping Tomcat	7
3	Lookup Service	8
3.1	System Architecture	8
3.2	Installing	10
3.2.1	Prerequisite Software	10
3.2.2	Installing on Linux	10
3.2.3	Testing the Installation	12
3.3	Configuring the LS	13
3.3.1	Mandatory Basic Configuration	13
3.3.2	Optional Advanced Configuration	16
3.4	Testing Your Deployment	17
4	Authentication Service	19
4.1	System Architecture	19
4.2	Installing	20
4.2.1	Prerequisite Software	20
4.2.2	Installing on Linux	21
4.2.3	Testing the Installation	22
4.3	Configuring the AS	22
4.3.1	Mandatory Basic Configuration	23
4.3.2	Optional Advanced Configuration	25
4.4	Testing Your Deployment	26
5	RRD MA	29
5.1	System Architecture	30
5.2	Installing	30

5.2.1	Prerequisite Software	31
5.2.2	Installing on Linux	31
5.2.3	Testing the Installation	33
5.3	Configuring the RRD MA	34
5.3.1	Creating a Metadata Configuration File	34
5.3.2	Configuring Basic Settings	35
5.4	Testing Your Deployment	41
5.5	Installation and Configuration: Best Practice	43
6	SQL MA	45
6.1	System Architecture	46
6.2	Installing	46
6.2.1	Prerequisite Software	47
6.2.2	Installing on Linux	47
6.2.3	Testing the Installation	49
6.3	Configuring the SQL MA	50
6.3.1	Mandatory Basic Configuration	50
6.3.2	Optional Advanced Configuration	53
6.3.3	Configuring the SQL MA to Store Data	54
6.4	Testing Your Deployment	55
6.5	SQL MA Stitching	57
6.5.1	Exposing Your MySQL or PostgreSQL Database to the SQL MA	58
6.5.2	Creating the Metadata Configuration File	59
6.5.3	Applying Your Metadata Configuration	60
7	BWCTL MP	62
7.1	System Architecture	62
7.2	Installing	63
7.2.1	Prerequisite Software	63
7.2.2	Testing the BWCTL	64
7.2.3	Setting the TCP Window Size	65
7.2.4	Installing on Linux	65
7.2.5	Setting up the Web Admin Interface	66
7.2.6	Testing the Installation	67
7.3	Configuring the BWCTL MP	68
7.3.1	Mandatory Basic Configuration	68
7.3.2	Optional Advanced Configuration	70
7.4	Integrating the BWCTL MP with Your System	71
7.5	Testing Your Deployment	71

8	Telnet/SSH MP	73
8.1	System Architecture	74
8.2	Installing	74
8.2.1	Prerequisite Software	75
8.2.2	Installing on Linux	75
8.2.3	Testing the Installation	77
8.3	Configuring the SSH/Telnet MP	77
8.3.1	Creating a Metadata Configuration File	77
8.3.2	Configuring Basic Settings	79
8.4	Testing Your Deployment	84
8.5	Securing the Telnet/SSH MP with a Reverse Proxy	85
8.5.1	Enabling Reverse Proxy in Apache	86
9	Using Authentication	88
9.1	Restricting Access to Resources	88
9.2	Accessing Protected Resources	89
9.2.1	Getting a GIdP account	89
10	Upgrading from a Previous Release	90
10.1	Upgrading on RedHat	90
10.1.1	Prerequisites	90
10.1.2	Full upgrade	90
10.1.3	Upgrading selected packages	90
10.1.4	Troubleshooting the upgrade	91
10.2	Upgrading on Debian	91
10.2.1	Prerequisites	91
10.2.2	Full upgrade	91
10.2.3	Upgrading selected packages	91
10.2.4	Troubleshooting the upgrade	92
	Glossary	93
	Index	94

Table of Figures

Figure 3.1: LS system architecture.	8
Figure 3.2: Global LS.	9
Figure 4.1: AS system architecture.	19
Figure 5.1: RRD MA system architecture.	30
Figure 6.1: SQL MA system architecture.	46
Figure 7.1: BWCTL MP system architecture.	62
Figure 8.1: Telnet/SSH MP system architecture.	74

1 Introduction

The perfSONAR MDM 3.2 release for LHCOPN provides a set of services that are designed to support perfSONAR's rollout in the Large Hadron Collider Optical Private Network (LHCOPN). perfSONAR web services allow you to access network performance metrics from your own domain or from any other European REN network. You can also perform network monitoring actions in the different network domains.

Using out-of-the-box or customised web-interfaces you can track and eliminate network problems and performance bottlenecks quickly, and identify and prevent potential performance issues before service disruption occurs.

The perfSONAR MDM 3.2 release comprises the following perfSONAR web services:

Lookup Service (LS)

The LS keeps track of which perfSONAR web services are available. The web services can register with the LS in regular intervals to signal that they are running, so that other clients (usually visualisation tools) can then request this information from the LS to find out which services are available.

Authentication Service (AS)

The AS provides authentication to protect perfSONAR web services from unrestricted access. By specifying request types that require authentication before they are executed by the web service, access can be restricted to users who have a GÉANT identity provider account (GIdP account), so that only they can send messages of the specified types.

RRD MA

The RRD MA retrieves IP interface information: link utilisation, link capacity, input errors and output drops.

SQL MA

The SQL MA retrieves circuit/lightpath status and IP interface information: link utilisation, link capacity, input errors and output drops.

BWCTL MP

The BWCTL MP measures achievable throughput (TCP) and UDP throughput between two BWCTL clients.

SSH/Telnet MP

The SSH/Telnet MP executes requests for RTT, SHOW command and traceroute information.

2 Getting Started

Important points before you start:

- It is recommended that you install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you require the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second, before you install any of the other services.

2.1 Deciding which Services to Install

The following table provides an overview of which functionality the different perfSONAR web services provide.

	LS	AS	RRD MA	SQL MA	BWCTL MP	SSH/ Telnet MP
View E2E Circuit Monitoring information				✓		
Detect congestion			✓	✓		
Detect path changes			(✓)	(✓)		✓
Detect abnormal link behaviour/ performance degradation			✓	✓	✓	
Test / verify TCP transfer					✓	
Detect small packet loss					✓	
Assess impact of network configuration changes					✓	
Assess incident impact					✓	
Assess user experience					✓	
Access show commands (Looking						✓
Discover other network monitoring functionalities.	✓					
Authenticate tool users		✓+	✓*	✓*	✓	✓*

(?) indirect observation

* optional functionality

+ mandatory to access authenticated perfSONAR web services

2.2 Supported Platforms

The following platforms are supported:

- Red Hat Enterprise Linux 4.x or 5.x
- Debian 4.0

Note: The perfSONAR services can also be installed on the following platforms. However, as these platforms are untested and not explicitly supported, no specific installation instructions are provided for them in this guide (unofficial installation hints may be available on the GÉANT Multi-Domain Services Knowledgebase which can be accessed at <http://kb.perfsonar.eu>):

- Fedora 8
- CentOS 5.1
- Ubuntu 7.10 / 8.04 LTS

2.3 Supported Browsers

The following browsers are supported:

- Mozilla Firefox

2.4 Prerequisite Software

The perfSONAR services require some software to be present on their host machine, before they can be installed:

	LS 1.4	AS 1.2	RRD MA 3.2	SQL MA 2.2	SSH/ Telnet MP 1.3.4.2	BWCTL MP 0.51
Java JDK 1.5 or higher	x	x	x	x	x	
Tomcat 5.5 or higher	x	x	x	x	x	
eXist 1.2.3	x		x	x	x	
RRDtool 1.2.x			x			
rrdtool 1.1-1			x			
MySQL 5.x				x		
iPerf 2.0.2 or higher						x
BWCTL 1.2a						x
Perl 5.8.8 or higher						x
ntp						x
Apache HTTP Server						x
OWAMP						

* optional

2.4.1 Installing Prerequisite Software Using Packages

Except for the Java JDK 1.5, you do not need to install the required dependencies manually (unless explicitly stated in the appropriate service installation section). Adding perfSONAR repositories to the system configuration ensures that when you are installing a particular service, all required prerequisite software is downloaded and installed at the same time.

On Red Hat

To install the 3.1 release

1. Use the RPM repository in which security updates and bug fixes are enabled. As root, execute the following command:

```
cd /etc/yum.repos.d
```

2. For 32 bit machines (i386), use:

```
wget http://downloads.perfsonar.eu/repositories/rpm/perfsonar-stable.repo
```

For 64 bit machines (86_64), use:

```
wget http://downloads.perfsonar.eu/repositories/rpm/perfsonar-stable-x86\_64.repo
```

If you are not using Red Hat, you need to search and enable repositories that contain the pre-requisites. For example, for Scientific Linux 5:

[http://linuxsoft.cern.ch/dag/redhat/el4/en/\\$basearch/dag/](http://linuxsoft.cern.ch/dag/redhat/el4/en/$basearch/dag/)

3. Install the pre-requisite Java. Enable the RedHat 5 Supplemental Repository on Red Hat as follows:
 - a. Go to <https://rhn.redhat.com/>
 - b. Log in to the Red Hat support network providing your Red Hat login and password.
 - c. Click the **Systems** tab.
 - d. Click the name of the system for which you want to enable the repository.
 - e. Click **Alter Channel Subscriptions**.
 - f. Check the box next to **RHEL Supplementary from the Release Channels** for Red Hat Enterprise Linux 5.
 - g. Click the **Change Subscriptions** button.
4. As root, execute the following command to install the JDK:

```
yum install java-1.5.0-sun tomcat5
```

Alternatively, you can download JAVA from <http://developers.sun.com/downloads>, install the JDK and set the **JRE_HOME** and **JAVA_HOME** variables. For example for JDK v 1.5.0, update 14:

```
export JRE_HOME=/usr/java/jdk1.5.0_14/jre
export JAVA_HOME=/usr/java/jdk1.5.0_14
```

On Debian

To install the 3.1 release

Note: if you want to install RRD MA or SQL MA, ignore this section and go straight to the relevant manual section (for RRD MA, see *Installing* on page 30 and for SQL MA, see *Installing* on page 46).

1. Make apt aware of the new software repositories by issuing the following command as root:

```
cd /etc/apt/sources.list.d
wget http://downloads.perfsonar.eu/repositories/deb/perfsonar-stable.list
```

2. Download the package key:

```
wget http://downloads.perfsonar.eu/repositories/perfsonar.asc
```

3. Import the key:

```
apt-key add perfsonar.asc
```

4. Check the import:

```
apt-key list
```

5. Clear & update the repo (this is optional):

```
apt-get clean
apt-get update
```

6. In a text editor, open the **/etc/apt/sources.list** file, and find the line:

```
deb http://<host> etch main contrib
```

For example:

```
deb http://ftp.debian.org etch main contrib
```

7. Add “non-free” to the end of the line, so it looks as follows (note that the host may vary):

```
deb http://ftp.debian.org etch main contrib non-free
```

8. As root, execute the following commands to install the JDK:

```
apt-get update
apt-get install sun-java5-jdk
```

9. You can now switch between different JDK's using the alternatives command:

```
update-alternatives --config java
update-alternatives --config javac
```

Note:

- For .deb-based distributions, Tomcat is configured to use the Tomcat security manager. This manager restricts I/O of Java code to a list of defined file operations. If some web services are not working, this may be due to read/write permission errors in the log files. In this case you should turn off the security manager in **/etc/default/tomcat5.5** by setting **TOMCAT5_SECURITY** to **no**.

- The perfSONAR services installation includes the SOAPMonitorService which by default runs on port 5001. If this conflicts with any other applications in your system, you can change this port in the **WEB-INF/web.xml** file in your perfSONAR service installation directory, using the following parameters:

```
<param-name>SOAPMonitorPort</param-name>  
<param-value>5001</param-value>
```

2.4.2 Starting and Stopping Tomcat

You can start and stop any of the perfSONAR web services by starting and stopping Tomcat. If you make configuration changes to a perfSONAR service, you need to start/restart Tomcat to apply these changes.

To start Tomcat use the command:

```
/etc/init.d/tomcat5.5 start      - Debian  
/etc/init.d/tomcat5 start      - Red Hat
```

To stop Tomcat use the command:

```
/etc/init.d/tomcat5.5 stop     - Debian  
/etc/init.d/tomcat5 stop      - Red Hat
```

To restart Tomcat use the command:

```
/etc/init.d/tomcat5.5 restart  - Debian  
/etc/init.d/tomcat5 restart    - Red Hat
```

You can also use the Tomcat Manager Web interface to start and stop individual services.

3 Lookup Service

The Lookup Service (LS) allows you to check which web services are available on the network.

Every time a service starts running, it can register with the LS to signal its availability and provide a description of its capabilities. Other clients (usually visualisation tools) can then request this information to find out which services are available. Keep Alives are used to keep the status of registered services up-to-date.

3.1 System Architecture

Local

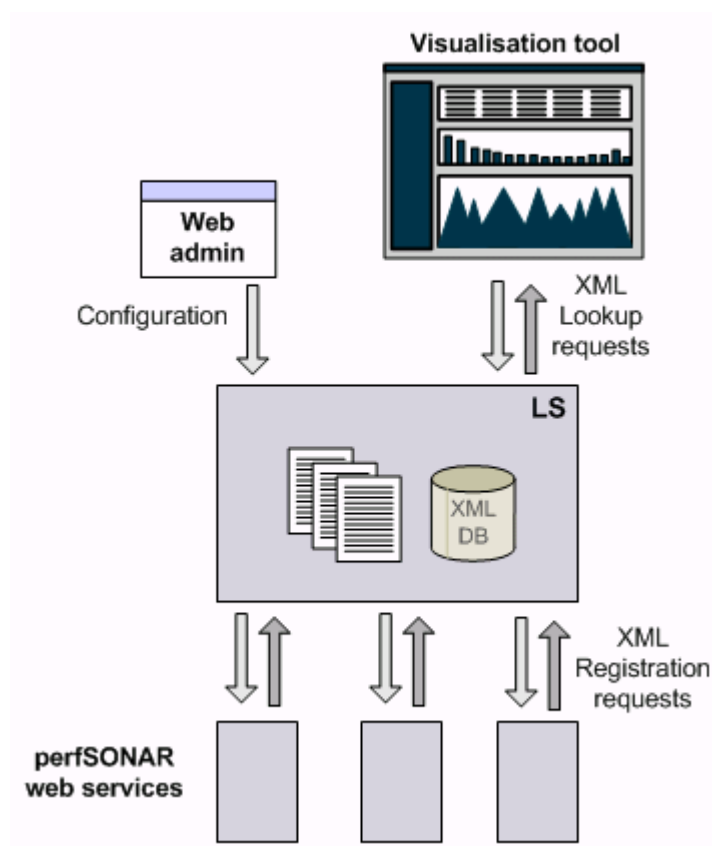


Figure 3.1: LS system architecture.

The perfSONAR web services in your domain register with one or more Lookup Services in your domain by sending an XML request (registering with multiple LS provides failover). The Lookup Services stores the status of the services in its XML database and confirms that services have successfully registered by returning an XML response.

Clients (usually visualisation tools) send XML queries to the Lookup Service to find out which web services they can access. In response, the Lookup Service returns a list of the currently available services.

The LS is configured via a Web Admin interface which is included in the LS installation. The Web Admin interface initialises the XML database storage for meta configuration and also writes all settings to files (non-meta configuration information) from where they are applied to the LS.

Global

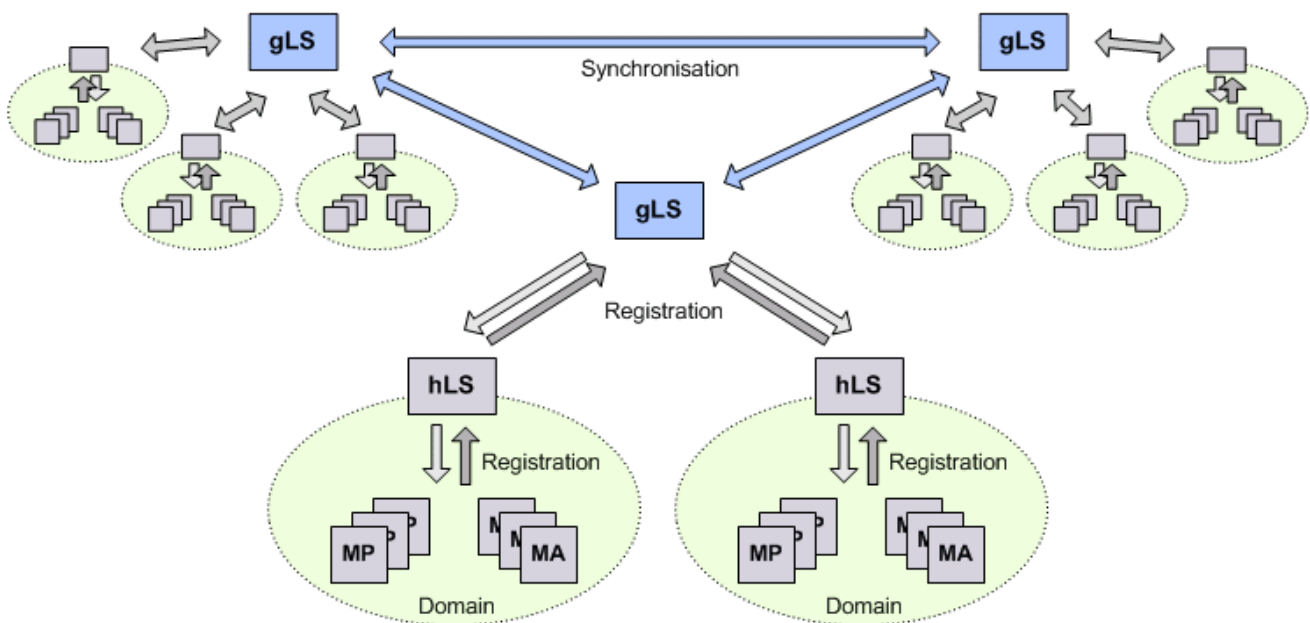


Figure 3.2: Global LS.

The home Lookup Services (hLS) in each domain registers with a global Lookup Service (gLS) which is maintained by a perfSONAR partner organisation (for example, GÉANT). Each gLS is regularly synchronised with all other gLS instances to ensure they have an up-to-date global view of which web services are available. This information is passed on to the local hLS instances, who in turn pass it on in reply to Lookup requests issued by clients (usually visualisation tools), providing full visibility of services that are available outside the local domain.

3.2 Installing

Note:

- It is recommended that you install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you require the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.

3.2.1 Prerequisite Software

The LS requires the following software to be present on its host machine. This software is installed automatically, when you run yum or apt-get to install the web service. Alternatively, you can install the prerequisite software manually

- Java JRE 5
- Tomcat 5.x
- eXist 1.2.x

See *Prerequisite Software* on page 4 for details.

3.2.2 Installing on Linux

If you are running a Linux operating system, you can install the LS using RPM distributions or in a non-RPM distribution. If you are using Debian, you need to install the LS using Debian packages.

To install using RPM distributions:

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the LS are also installed.

```
yum search jdk          (if you have used a repository to install JDK)
```

```
yum search tomcat5
```

```
yum search exist
```

2. Install the RPM package:

```
sudo yum install perfsonar-java-xml-ls.noarch
```

Prerequisite software is included in the package and automatically installed.

3. Copy the following files:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/var/lib/tomcat5/common/endorsed

cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/var/lib/tomcat5/common/endorsed

cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/var/lib/tomcat5/common/endorsed

cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/var/lib/tomcat5/common/endorsed

cp /var/lib/tomcat5/webapps/geant2-java-xml-ls/WEB-INF/lib/xercesImpl-
2.8.0.jar /var/lib/tomcat5/common/endorsed
```

Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy.sh>

4. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

To install using Debian packages:

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the LS are also installed.

```
apt-cache search jdk          (if you have used a repository to install JDK)
apt-cache search tomcat5
apt-cache search exist
```

2. To install the LS web service and dependencies (if required) use the following command (for all architectures):

```
sudo apt-get install perfsonar-java-xml-ls
```

3. Copy the following files:

```
cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/usr/share/tomcat5.5/common/endorsed

cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/usr/share/tomcat5.5/common/endorsed

cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/xml-apis.jar
/usr/share/tomcat5.5/common/endorsed

cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed

cp -v /var/lib/tomcat5.5/webapps/geant2-java-xml-ls/WEB-
INF/lib/xercesImpl-2.8.0.jar /usr/share/tomcat5.5/common/endorsed
```

Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy-DEB.sh>

4. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

3.2.3 Testing the Installation

You can test if you have installed the LS correctly by checking if the Web Admin pages can be displayed. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

To test the installation:

Open a Mozilla browser and enter the following URL:

`http://<host>:<port>/geant2-java-xml-ls`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-xml-ls>

If you have installed the LS correctly, the Web Admin pages are displayed. If you cannot access the Web Admin page (your browser displays "Failed to connect"), ensure that you do not have firewalls which prevent access to the page (hardware or s/w like iptables).

Once you have successfully tested your installation, you need to configure the service (see *Configuring the LS* on page 13).

3.3 Configuring the LS

Before you can use the LS, you need to configure it. For this you can use the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

3.3.1 Mandatory Basic Configuration

To configure the settings that the LS requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

http://<host>:<port>/geant2-java-xml-ls

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-xml-ls>

2. Under the **Basic Configuration** heading in the navigation panel, click **Service**.
A login prompt is displayed.
3. Enter your login details (the default login is `perfsonaruser` and `perfsonarpass`), and click **OK**.
The basic service configuration settings page is displayed. This page lists the settings that the LS requires to be configured to be able to run:

eXist Configuration

This section allows you to set the login details for the Web Admin pages.

Would you like to use eXist DB XML

Select **on** to register the LS with the eXist database (this is required).

Enter the location of the eXist database

Enter the URL to the location where your eXist database is installed.

Specify the service username for the eXist user

Enter the service username for the LS user of the eXist database. It is recommended that you use the default value.

Specify the user password for eXist

Specify the password that LS users have to enter to log in to the eXist database.

Specify the administration password for eXist

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Would you like to initialise the database structure?

Select **yes** to initialise the eXist database. Initialising the database adds the user access details you have configured to the database. If you already have a database containing data and don't want to remove it, you should not initialise your database structure, as this will remove all your LS data.

LS Configuration

This section allows you to register your home Lookup Service with a global Lookup Service.

Do you wish to register with an LS

Select **yes** to register your hLS with a gLS. This means that your hLS keeps the gLS informed which services are available in its local home domain. The gLS passes this information on to Lookup Services in other domains, so that the availability of services can be seen globally.

Enter the service name

Enter a name for your hLS service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Enter a description for the service

Enter a description for the hLS service. The gLS displays this to clients as part of the hLS' capability details.

Enter the service administrator's email address

Enter the email address of the hLS administrator. The gLS displays this to clients as part of the hLS' capability details.

Enter the name of the organization running this service

Enter the email address of the organisation who is hosting the hLS. The gLS displays this to clients as part of the hLS' capability details.

Enter the explicit gLS URL

Enter the URL of one or more gLS that you want to register your hLS with (if you want to register with multiple gLS, you must separate the individual URLs with commas).

Note: if you are using the **root.hints** file, filling in this field is not mandatory because the file automatically provides a list of available gLS services.

Example: <http://remotehost:8180/geant2-java-xml-ls/services/LookupService>

Enter the URL of root.hints

Enter the URL of one or more **root.hints** lists of global LS instances. Your hLS will randomly chose a gLS to register with from this list (if you want to use multiple **root.hints** lists, you must separate the individual URLs with commas).

Example: <http://www.perfsonar.net/gls.root.hints>

Set the registration interval (seconds)

Enter the amount of time (in seconds) to elapse between registration requests to the gLS. By default this is 43200 seconds (12 hours).

Enter the service access point of the hLS

Enter the URL to the location where your hLS is installed.

Example: <http://myhost:8180/geant2-java-xml-ls/services/LookupService>

Authentication Configuration

If you have installed an Authentication Service or are permitted to use a third party AS, this section allows you to enable authentication for your hLS by registering it with this AS. This means that you can restrict specific request types to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

Do you wish to enable authentication

Select **on** if you want to restrict access to your hLS. This means that only users who have a GIdP account can send messages of the types specified in the **Enter the message types which should be authenticated** field to your hLS.

Enter the URL address of the Authentication Service

Enter the URL of the AS that you are using to authenticate users. This can be an AS you have installed yourself or a third party AS that you are permitted to use.

Enter the message types which should be authenticated

Enter a CSV of the types of message for which you require authentication. You can restrict the following message types:

- **LSRegisterRequest**

Request that web services send to an LS to register with it or to update their Lookup information (general metadata including, for example, the service's name, type and URL).

- **LSDeregisterRequest**
Request that web services send to an LS to unregister from it. This removes the services Lookup information from the LS.
- **LSQueryRequest**
Request that clients (usually visualisation tools) send to an LS to query which services are available.
- **LSControlRequest**
Internal control requests (not currently used).
- **LSKeepaliveRequest**
Request that web services which are already registered with an LS send to it in order to notify it that they are still running (if a registered service does not send **LSKeepaliveRequest** within specific intervals after first registering, the LS assumes that it is no longer available) .

4. Click **apply**.

5. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 17).

3.3.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

1. Log on to the Web Admin pages.
2. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the LS according to your requirements.
3. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
4. Click **apply** to apply your modifications.
5. Under the **Advanced Configuration** heading in the navigation panel, click **Logging**.
The advanced service configuration settings page is displayed. This page lists the logging settings that you can configure to customise the LS according to your requirements.
6. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.

Note that if you want to send all logging data to a syslog server, you need to enable syslog message logging by pointing the **service.log.log4j.config** setting to the **log4j.syslog.properties** configuration file rather than the **log4j.properties** configuration file (the **service.log.log4j.config** setting is located on the **Advanced Configuration Service** page in the **Internals** group).

7. Click **apply** to apply your modifications.
8. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
9. Enter your login details (the default username is admin and an empty password field, unless you have set an administration password) and click **OK**.

The **eXist Database Administration** page is displayed. This page comprises the following tabs:

Manage Collections

This tab lists the eXist resources and their details (owners, groups, permissions and creation dates). You can select a resource and click **Edit Resource** to change its details or **Delete Resource** to delete it. You can also create a new resource by clicking **Create Resource**, specifying the required details and clicking **Create**.

Manage Users

This tab lists the eXist users and their details (groups and homes). You can select a user and click **Edit** to change their details or **Delete** to delete them. You can also create a new user by clicking **Create**, specifying the required details and clicking **Create**.

10. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).
If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 17).

3.4 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the LS correctly:

1. Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**.
The **Deployment test** page is displayed.
2. Click the **start test** button to check if you have deployed the LS correctly.

If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the LS correctly by using the perfsonarUI client to send an EchoRequest to it.

To send an EchoRequest:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the LS:
http://<host>:<port>/geant2-java-xml-ls/services/LookupService
<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-xml-ls/services/LookupService>

3. In the **Execute query** section, click **Query** to send an EchoRequest to the LS. If you have installed the service correctly an EchoResponse is returned. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"
  messageIdRef="message1208947296" type="EchoResponse"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
    metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
      the echo response from the service.</nmwgr:datum>
    </nmwg:data>
  </nmwg:message>
```

4 Authentication Service

The Authentication Service (AS) provides authentication to protect perfSONAR web services from unrestricted access. If you configure your web services to register with the AS, you can specify the request types that require authentication before they are executed. This means that only users who have a GÉANT identity provider account (GIdP account) can send messages of the specified types to your web services, while unauthorised users cannot access them.

The AS accepts all identities that are issued by any eduGAIN-connected identity provider without any further checks. Any user can install an identity provider (using the IdP software) and get valid identities which are accepted by all AS deployments.

4.1 System Architecture

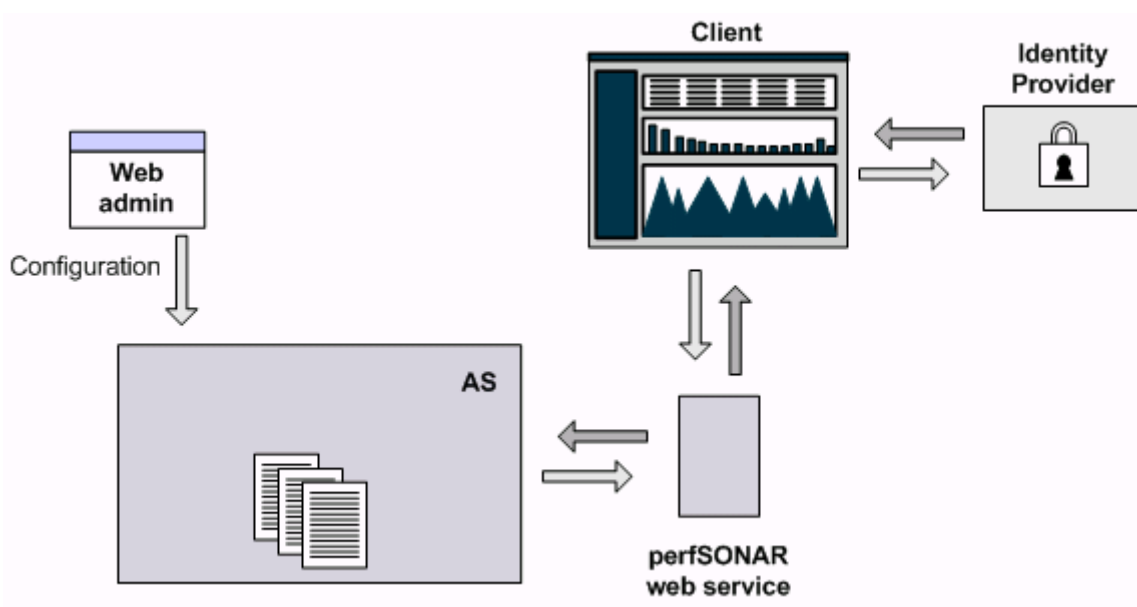


Figure 4.1: AS system architecture.

If a perfSONAR web service is integrated with the AS, any request that a client sends to this web service includes authentication information which identifies the user of the client (if a web client is used) or the location of the client (if an automated client is used). This authentication information is provided by the GIdP.

The perfSONAR web service then sends an XML request to the Authentication Service to check if the received authentication information is valid. The Authentication Service checks the authentication information and returns an XML reply that indicates if the authentication was successful.

The AS is configured via a Web Admin interface which is included in the AS installation. The Web Admin interface stores the configuration settings in files (non-meta configuration information) from where they are applied to the AS.

4.2 Installing

Note:

- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- It is recommended that you also install the Lookup Service, so you are able to check which services you can access across the network.
- If you require the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.
- It is recommended that you do not install AS on the same machine as any service that requires eXist (for example, LS, RRD MA, SQL MA or Telnet/SSH MP).
- Before you start installing the AS, it is recommended that you check the system time of your server as some authentication information requires to be checked against it. You can synchronise your server's system time using the Network Time Protocol (NTP).

4.2.1 Prerequisite Software

The AS requires the following software to be present on its host machine. This software is installed automatically, when you run yum or apt-get to install the web service. Alternatively, you can install the prerequisite software manually

- Java JDK 1.5
- Tomcat 5.5

See *Prerequisite Software* on page 4 for details.

4.2.2 Installing on Linux

If you are running a Linux operating system, you can install the AS using RPM distributions or in a non-RPM distribution. If you are using Debian, you need to install the AS using Debian packages.

Note: it is recommended that you do not install AS on the same machine as any service that requires eXist (for example, LS, RRD MA, SQL MA or Telnet/SSH MP).

To install using RPM distributions:

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the AS are also installed.

```
yum search jdk          (if you have used a repository to install JDK)
yum search tomcat5
```

2. Install the RPM package:

```
sudo yum install perfsonar-java-as.noarch
```

Prerequisite software is included in the package and automatically installed.

3. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

To install using Debian packages:

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the AS are also installed.

```
apt-cache search jdk          (if you have used a repository to install JDK)
apt-cache search tomcat5
```

2. Install the AS and dependencies (if required):

```
sudo apt-get install perfsonar-java-as.deb
```

3. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

4.2.3 Testing the Installation

You can test if you have installed the AS correctly by checking if the Web Admin pages can be displayed. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

To test the installation:

Open a Mozilla browser and enter the following URL:

`http://<host>:<port>/geant2-java-as`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/geant2-java-as>

If you have installed the AS correctly, the Web Admin pages are displayed. If you cannot access the Web Admin page (your browser displays "Failed to connect"), ensure that you do not have firewalls which prevent access to the page (hardware or s/w like iptables).

Once you have successfully tested your installation, you need to configure the service (see *Configuring the AS* on page 22).

4.3 Configuring the AS

Before you can use the AS, you need to configure it. For this you can use the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

4.3.1 Mandatory Basic Configuration

To configure the settings that the AS requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

http://<host>:<port>/geant2-java-as

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/geant2-java-as>

2. Under the **Basic Configuration** heading in the navigation panel, click **Service**.
A login prompt is displayed.
3. Enter your login details (the default login is `perfsonaruser` and `perfsonarpass`) and click **OK**.

The basic service configuration settings page is displayed. This page lists the settings that the AS requires to be configured in order to be able to run:

LS Configuration

This section allows you to register your AS with the Lookup Service.

Do you wish to register with an LS

Select **yes** to register the AS with the Lookup Service. This means that every time the AS starts running, it signals its availability to the LS. From there other clients (usually visualisation tools) can see that the AS is available and check its capabilities.

Enter the service name

Enter a name for the AS service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Enter a description for the service

Enter a description for the AS service. The LS displays this to clients as part of the AS' capability details.

Enter the service administrator's email address

Enter the email address of the AS administrator. The LS displays this to clients as part of the AS' capability details.

Enter the name of the organization running this service

Enter the email address of the organisation who is hosting the AS. The LS displays this to clients as part of the AS' capability details.

Enter the LS URL

Enter the URL of the LS that you want to register the AS with.

Example: <http://localhost:8080/xml-Is/services/LookupService>

Set the registration interval (milliseconds)

Enter the amount of time (in milliseconds) to elapse between registration requests to the Lookup Service. By default this is 43200000 milliseconds (12 hours).

Enter the service access point

Enter the URL to the location where your AS is installed.

Example: <http://myhost:8080/geant2-java-as/services/AuthService>

Administration Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the username for logging in to the admin pages

Specify the username that users have to enter to log in to the Web Admin pages.

Enter the **password** for logging in to the admin pages

Specify the password that users have to enter to log in to the Web Admin pages (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Authentication Configuration:

This section allows you to set up secure authentication.

Enter the full path to the TrustStore file containing the CA certs

This configuration entry has a default value that points to eduGAIN/perfSONAR trust store. It is recommended that you do not change the default as it disables the AS from accepting eduGAIN/perfSONAR certified user identities.

Enter the password for the TrustStore file

The password that protects the specified TrustStore file. You must not change this, unless the TrustStore or its password has been manually changed.

Enter the full path to a file containing valid Component IDs in eduGAIN

The full path to the file which contains a list of acceptable Identifiers. You must not change this as these identifiers specify eduGAIN identity providers that are supported by the AS. Currently, all identity providers including SASL CA are accepted.

Enter the maximum lifetime (milliseconds) token allowed in the service

Identity verification requests that are sent to the AS contain identities or tokens that include a timestamp which indicates their issue date and time. The age of the token is calculated and if it is less than the value specified in this field, the identity considered valid.

It is recommended that you do not change the default value.

4. Click **apply**.
5. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 26).

4.3.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

1. Log on to the Web Admin pages.
2. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the AS according to your requirements.
3. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
4. Click **apply** to apply your modifications.
5. Under the **Advanced Configuration** heading in the navigation panel, click **Logging**.
The advanced service configuration settings page is displayed. This page lists the logging settings that you can configure to customise the AS according to your requirements.

Note that if you want to send all logging data to a syslog server, you need to enable syslog message logging by pointing the **service.log.log4j.config** setting to the **log4j.syslog.properties** configuration file rather than the **log4j.properties** configuration file (the **service.log.log4j.config** setting is located on the **Advanced Configuration Service** page in the **Internals** group).
6. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
7. Click **apply**.
8. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 26).

4.4 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the AS correctly:

1. Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**. The **Deployment test** page is displayed.
2. Click the **start test** button to check if you have deployed the AS correctly. If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the AS correctly by using the perfonarUI client to send an EchoRequest or a LookupInfoRequest to it.

To send an EchoRequest:

1. Start PerfonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the AS:
http://<host>:<port>/geant2-java-as/services/AuthService

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/geant2-java-as/services/AuthService>

3. In the **Execute query** section, click **Query** to send an EchoRequest to the AS. If you have installed the service correctly an EchoResponse is returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"
  messageIdRef="message1208947296" type="EchoResponse"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
    metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
    the echo response from the service.</nmwgr:datum>
```

```
</nmwg:data>
</nmwg:message>
```

To send a LookupInfoRequest:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the AS:

http://<host>:<port>/<service>/services/AuthService

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/geant2-java-as/services/AuthService>

3. In the **Query** field, enter the following LookupInfoRequest:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl" type="LookupInfoRequest"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="meta">
    <nmwg:eventType>http://schemas.perfsonar.net/tools/admin/lookup
info/2.0</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="data" metadataIdRef="meta"/>
</nmwg:message>
```

4. In the **Execute query** section, click **Query** to send the LookupInfoRequest to the AS. If you have installed the service correctly a LookupInfoResponse is returned. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl_resp" messageIdRef="idl" type="LookupInfoResponse"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="localhost.localdomain.841f726:11957c178d1:-7f30"/>
  <nmwg:data id="localhost.localdomain.841f726:11957c178d1:-7f2f"
metadataIdRef="localhost.localdomain.841f726:11957c178d1:-7f30">
    <psservice:datum
xmlns:psservice="http://ggf.org/ns/nmwg/tools/org/perfsonar/service/1.
0/">
      <psservice:service>
        <psservice:serviceName>perfSONAR AS</psservice:serviceName>
```

```
<psservice:accessPoint>http://localhost:8080/perfSONAR-
AS/services/AuthService</psservice:accessPoint>
<psservice:serviceType>as</psservice:serviceType>
<psservice:serviceDescription>perfSONAR
AS</psservice:serviceDescription>
<psservice:serviceVersion>1.0</psservice:serviceVersion>
<psservice:organization>my organisation</psservice:organization>
<psservice:contactEmail>user@domain</psservice:contactEmail>
</psservice:service>
</psservice:datum>
</nmwg:data>
</nmwg:message>
```

5 RRD MA

The Round Robin Database Measurement Archive (RRD MA) stores time-series data that is usually collected by SNMP-based measurement tools. It provides the following measurements: RRD MA

- IP interface link utilisation
- IP interface link capacity
- IP interface input errors
- IP interface output drops

You can access the data using the perfsonarUI web client or the DFN CNM.

Note: Setting up the RRD MA consists of two mandatory phases:

- Installation (see *Installing* on page 30)
You need to install the service on a server in your domain.
- Configuration (see *Configuring the RRD MA* on page 34)
You need to create a metadata configuration file that defines how the RRD MA should deal with measurement data, and configure basic settings that determine the location of components that the RRD MA interacts with, set access credentials etc. The service is then started up or restarted to apply the configuration.

5.1 System Architecture

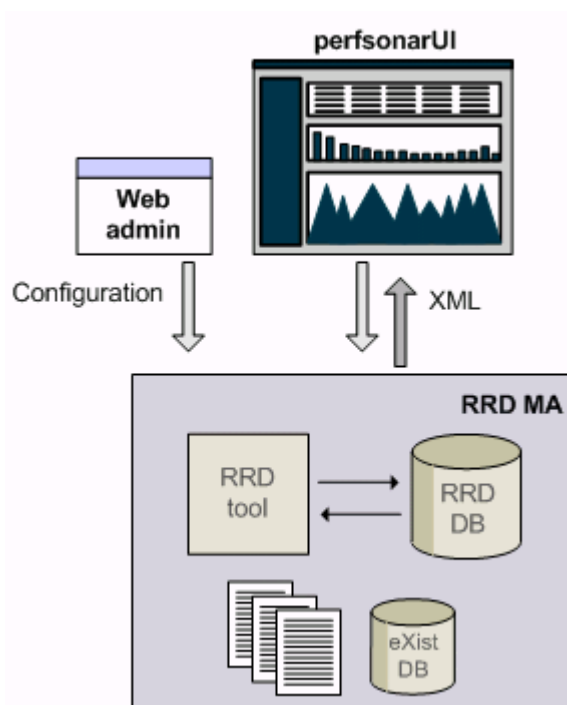


Figure 5.1: RRD MA system architecture.

When users access archived data from the RRD MA from the perfsonarUI web client, perfsonarUI sends an XML request to the RRD MA. The RRD MA then retrieves the data from the RRD DB via the RRD tool and returns an XML reply to the client.

The RRD MA is configured via a Web Admin interface which is included in the RRD MA installation. The Web Admin interface stores the configuration settings in an eXist database (meta configuration information) and files (non-meta configuration information) from where they are applied to the RRD MA.

5.2 Installing

Note:

- It is recommended that you also install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you are also installing the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.

5.2.1 Prerequisite Software

The RRD MA requires the following software to be present on its host machine. This software is installed automatically, when you run `yum` or `apt-get` to install the web service. Alternatively, you can install the prerequisite software manually

- Java JDK 1.5
- Tomcat 5.5
- eXist 1.1.x or 1.2.x
- RRDtool 1.2.x

See *Prerequisite Software* on page 4 for details.

5.2.2 Installing on Linux

If you are running a Linux operating system, you can install the RRD MA using RPM distributions or in a non-RPM distribution. If you are using Debian, you need to install the RRD MA using Debian packages.

To install using RPM distributions:

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the RRD MA are also installed.

```
yum search rrdjtool
yum search jdk          (if you have used a repository to install JDK)
yum search rrdtool
yum search rrdtool-devel
yum search tomcat5
yum search exist
```

2. Install the RRD MA web service and dependencies (if required):

```
sudo yum install perfsonar-java-rrd-ma
```

Prerequisite software is included in the package and automatically installed.

3. Copy the following files:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/var/lib/tomcat5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/var/lib/tomcat5/common/endorsed
```

```
cp /var/lib/tomcat5/webapps/geant2-java-rrd-ma/WEB-INF/lib/xercesImpl-2.8.0.jar /var/lib/tomcat5/common/endorsed
```

Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy.sh>

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

To install using Debian packages:

- In a text editor, open the `/etc/apt/sources.list` file, and find the line:

```
deb http://<host> etch main contrib
```

For example:

```
deb http://ftp.debian.org etch main contrib
```

- Add “non-free” to the end of the line, so it looks as follows (note that the host may vary):

```
deb http://ftp.debian.org etch main contrib non-free
```

- As root, execute the following commands to install the JDK:

```
apt-get update
apt-get install sun-java5-jdk
```

- You can now switch between different JDK's using the alternatives command:

```
update-alternatives --config java
update-alternatives --config javac
```

- Execute the following command to install rrdtool:

```
apt-get install rrdtool
```

(This installs version 1.2.15.)

- Execute the following commands to add the perfSONAR-mdm-3.1 repository, if you have not already done this (see *Installing Prerequisite Software Using Packages* on page 5):

```
cd /etc/apt/sources.list.d
wget http://downloads.perfsonar.eu/repositories/deb/perfsonar-mdm-3.1.list
wget http://downloads.perfsonar.eu/repositories/perfsonar.asc
apt-key add perfsonar.asc
apt-get clean
apt-get update
```

- Execute the following command to install the RDD MA web service:

```
apt-get install perfsonar-java-rrd-ma
```

8. In the `/etc/default/tomcat5.5` Tomcat configuration file, uncomment and set the **TOMCAT5_SECURITY** and **CATALINA_OPTS** parameters as follows:

```
TOMCAT5_SECURITY=no
CATALINA_OPTS="-Djava.awt.headless=true -Xmx128M -server -
Djava.library.path=/usr/lib"
```

9. Copy the eXist xml library files into the Tomcat-endorsed library directory:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xercesImpl-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/usr/share/tomcat5.5/common/endorsed/
```

10. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

5.2.3 Testing the Installation

You can test if you have installed the RRD MA correctly by checking if the Web Admin pages can be displayed. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

To test the installation:

Open a Mozilla browser and enter the following URL:

`http://<host>:<port>/geant2-java-rrd-ma`

`<host>`

The IP address or name of the machine that hosts the web service.

`<port>`

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-rrd-ma>

If you have installed the RRD MA correctly, the Web Admin pages are displayed. If you cannot access the Web Admin page (your browser displays "Failed to connect"), ensure that you do not have firewalls which prevent access to the page (hardware or s/w like iptables).

Once you have successfully tested your installation, you need to configure the RRD MA (see *Configuring the RRD MA* on page 34).

5.3 Configuring the RRD MA

Before you can use the RRD MA, you need to:

1. Create a metadata configuration file that defines how the RRD MA should deal with measurement data.
2. Configure basic settings that determine the location of components that the service interacts with, set access credentials etc.

5.3.1 Creating a Metadata Configuration File

To be able to understand the measurement data that the RRD MA provides access to, it needs meta information that puts the data into context. For example, metadata that defines:

- the IP interface address for which measurement data is collected
- the DNS name of the network element in which the IP interface is hosted
- the IP interface 's capacity

The meta information is stored in an XML metadata configuration file which you need to create for your network. The RRD MA provides an example XML metadata configuration file which contains some test data that you can use as a template for creating your own file, in the following location:

```
/usr/lib/perfsonar/services/geant2-java-rrd-ma/rrd-database_TEST.xml
```

You can also use the following documents which provide a sample metadata configuration file and explain the required format:

```
/usr/lib/perfsonar/services/geant2-java-rrd-ma/WEB-INF/classes/perfsonar/conf/rrd-database_TEST.xml
```

```
/usr/share/doc/geant2-java-rrd-ma/Metadata_Configuration_Specification.doc
```

Once you have created your XML metadata configuration file, you are ready to configure basic settings for the RRD MA (see *Configuring Basic Settings* on page 35).

Note: To save time (especially for large networks) and avoid errors, it is recommended that you use automated scripts and tools to generate your metadata configuration.

5.3.1.1 Changing the Metadata Configuration File

If at any point you want to change which metadata configuration file the RRD MA is using (for example, because you have amended your XML file or created a new one), you need to instruct the RRD MA to use your new file as follows:

1. Log on to the Web Admin pages (see *Mandatory Basic Configuration* on page 36).
2. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
3. Log on using the service credentials you provided when you configured the service for the first time (by default the rrdmaservice username and a password chosen by you), and click **OK**.
The **eXist Database Administration** page is displayed.
Note: you must not log in as admin user to upload/change metadata config files.
4. Display the **Manage Collections** tab.
5. Click the name of the previously created RRD MA collection (listed in the Resource column). By default this is **rrdmaconfig**.
6. A list of XML files or resources that are stored in this collection is displayed. This list is either empty or may contain the default RRD MA config file (**rrd-database_TEST.xml**).
7. Click the **Create Resource** button.
8. Browse to the metadata configuration file that you have created for your RRD MA, and click the **Create** button to upload it.
9. Click **Refresh** to update the file list.
10. Select the default/dummy metadata configuration file and click the **Delete Resource** button to delete it.
11. Click the **log out** button to log out.

You can now test your new configuration using perfsonar UI. You should be able to see all the interfaces that you have configured. If you have any problems check the format of the file, follow all the steps above and try again.

5.3.2 Configuring Basic Settings

You can configure basic setting using the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

5.3.2.1 Mandatory Basic Configuration

To configure the settings that the RRD MA requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

http://<host>:<port>/geant2-java-rrd-ma

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-rrd-ma>

2. Under the **Basic Configuration** heading in the navigation panel, click **Service**.
A login prompt is displayed.
3. Enter your login details (the default login is `perfsonaruser` and `perfsonarpass`) and click **OK**.
The basic service configuration settings page is displayed. This page lists the settings that the RRD MA requires to be configured in order to be able to run:

eXist Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the URI location of the eXist database

Enter the URI to the location where your eXist database is installed (use port 8080 for RPM and port 8180 for DEB).

Example: `xmldb:exist://localhost:8080/exist/xmlrpc`

Enter the service username for the eXist user

Enter the service username for the RRD MA user of the eXist database. It is recommended that you use the default value.

Example: `rrdmaservice`

Enter the password for the eXist user

Specify the password that RRD MA users have to enter to log in to the eXist database (this is a string of your choice unless you are integrating with a pre-existing eXist database, in which case you may choose to specify the password of an existing user account).

Example: `rrdmaconfig`

Do you wish to create a user with this name

Select **yes** if you want to create a new user account for the RRD MA user in eXist (if you are integrating with a pre-existing eXist database and want to use an existing eXist user account, select **no**).

Select **no** if you are re-configuring the RRD MA (if you have previously configured the RRD MA, an account already exists).

Enter the eXist administration password

This field is displayed if you selected to create a new eXist user account. Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Example: `exist`

Enter the full path of the metadata configuration file

Enter the full path to the XML metadata configuration file you previously created (see *Creating a Metadata Configuration File* on page 34). By default the path to an example metadata configuration file is specified, which comes with the service. This file contains some test data that you can use as a template for creating your own file.

Normally you should create your own XML metadata configuration file before you start configuring the RRD MA. However, if you have not done this, you can keep the default path to the example file, and create your own XML file at a later stage (see *Changing the Metadata Configuration File* on page 35).

After the basic configuration, the XML file you point to is copied from the specified location to the eXist database. The file should still be kept and its path should not be changed after the configuration because it might be used by the service in special circumstances.

Example: `/tmp/rrd-my-config.xml`

Do you wish to change the eXist admin password

Select **yes** or **no** to indicate if you want to change the eXist administrator password.

Enter the eXist administration password

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Confirm the new eXist administration password

Re-enter the password for the eXist administrator.

Enter the old eXist administration password

If you install the RRD MA and already have an existing eXist installation, the Web Admin pages cannot access the admin password of the existing eXist database. Enter the existing eXist admin password in this field, so the RRD MA can access it. If you want to keep the existing password, you also need to enter it in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** field. If you want to change it, enter the password that you want to replace it with in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** field.

LS Configuration

This section allows you to register your RRD MA with the Lookup Service.

Do you wish to register with an LS

Select **yes** to register the RRD MA with the Lookup Service. This means that every time the RRD MA starts running, it signals its availability to the LS. From there other clients (usually visualisation tools) can see that the RRD MA is available and check its capabilities.

Enter the service name

Enter a name for the RRD MA service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Enter a description for the service

Enter a description for the RRD MA service. The LS displays this to clients as part of the RRD MA's capability details.

Enter the service administrator's email address

Enter the email address of the RRD MA administrator. The LS displays this to clients as part of the RRD MA's capability details.

Enter the name of the organization running this service

Enter the email address of the organisation who is hosting the RRD MA. The LS displays this to clients as part of the RRD MA's capability details.

Enter the LS URL

Enter the URL of the LS that you want to register the RRD MA with (use port 8080 for RPM and port 8180 for DEB).

Example: <http://localhost:8180/xml-ls/services/LookupService>

Set the registration interval (milliseconds)

Enter the amount of time (in milliseconds) to elapse between registration requests to the Lookup Service. By default this is 43200000 milliseconds (12 hours).

Enter the service access point

Enter the URL to the location where your RRD MA is installed.

Example: <http://myhost:8180/geant2-java-rrd-ma/services/MeasurementArchiveService>

Administration Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the username for logging in to the admin pages

Specify the username that users have to enter to log in to the Web Admin pages.

Enter the password for logging in to the admin pages

Specify the password that users have to enter to log in to the Web Admin pages (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Authentication Configuration

If you have installed an Authentication Service or are permitted to use a third party AS, this section allows you to enable authentication for your RRD MA by registering it with this AS. This means that you can restrict specific request types to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

Do you wish to enable authentication

Select **yes** if you want to restrict access to the RRD MA. This means that only users who have a GIdP account can send messages of types specified in the **Enter the message types which should be authenticated** field to the RRD MA.

Enter the URL address of the Authentication Service

Enter the URL of the AS that you are using to authenticate users. This can be an AS you have installed yourself or a third party AS that you are permitted to use.

Enter the message types which should be authenticated

Enter a CSV of the types of message for which you require authentication. You can restrict the following message types:

- **MetadataKeyRequest**
Requests a list of all supported devices and the commands they support.
- **SetupDataRequest**
Executes commands on the devices the RRD MA is connected to.
- **MeasurementArchiveStoreRequest**
Stores measurement data in the RRD MA.

4. Click **apply** to apply your modifications.
5. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the RRD MA according to your requirements.
6. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
7. Click **apply**.

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7) to apply your configuration changes (if you used deb to install the RRD MA, use `/etc/init.d/geant2-tomcat5.5 restart` to restart Tomcat).

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 41).

5.3.2.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

- Log on to the Web Admin pages.
- Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the RRD MA according to your requirements.
- Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
- Click **apply** to apply your modifications.
- Under the **Advanced Configuration** heading in the navigation panel, click **Logging**.
The advanced service configuration settings page is displayed. This page lists the logging settings that you can configure to customise the RRD MA according to your requirements.

Note that if you want to send all logging data to a syslog server, you need to enable syslog message logging by pointing the `service.log.log4j.config` setting to the `log4j.syslog.properties` configuration file rather than the `log4j.properties` configuration file (the `service.log.log4j.config` setting is located on the **Advanced Configuration Service** page in the **Internals** group).
- Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
- Click **apply** to apply your modifications.
- Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
- Enter your login details (the default username is admin and an empty password field, unless you have set an administration password) and click **login**.

The **eXist Database Administration** page is displayed. This page comprises the following tabs:

Manage Collections

This tab lists the eXist resources and their details (owners, groups, permissions and creation dates). You can select a resource and click **Edit Resource** to change its details or **Delete Resource** to delete it. You can also create a new resource by clicking **Create Resource**, specifying the required details and clicking **Create**.

Manage Users

This tab lists the eXist users and their details (groups and homes). You can select a user and click **Edit** to change their details or **Delete** to delete them. You can also create a new user by clicking **Create**, specifying the required details and clicking **Create**.

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7) to apply your configuration changes (if you used deb to install the RRD MA, use `/etc/init.d/geant2-tomcat5.5 restart` to restart Tomcat).

If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 41).

5.4 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the RRD MA correctly:

- Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**. The **Deployment test** page is displayed.
- Click the **start test** button to check if you have deployed the RRD MA correctly. If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the RRD MA correctly by using the perfonarUI client to send an EchoRequest or a LookupInfoRequest to it (you can also find additional example requests in `$PATH_TO_YOUR_SERVICE/WEB-INF/samples/requests`).

To send an EchoRequest:

- Start PerfonarUI and display the **Playground** page.
- In the **Service address** field, enter the URL to the RRD MA service:

`http://<host>:<port>/geant2-java-rrd-ma/services/MeasurementArchiveService`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-rrd-ma/services/MeasurementArchiveService>

- In the **Execute query** section, click **Query** to send an EchoRequest to the RRD MA. If you have installed the service correctly an EchoResponse is returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"
  messageIdRef="message1208947296" type="EchoResponse"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
    metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
      the echo response from the service.</nmwgr:datum>
    </nmwg:data>
  </nmwg:message>
```

To send a LookupInfoRequest:

- Start PerfsonarUI and display the **Playground** page.
- In the **Service address** field, enter the URL to the RRD MA service:

http://<host>:<port>/geant2-java-rrd-ma/services/MeasurementArchiveService

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-rrd-ma/services/MeasurementArchiveService>

- In the **Query** field, enter the following LookupInfoRequest:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl" type="LookupInfoRequest"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="meta">
    <nmwg:eventType>http://schemas.perfsonar.net/tools/admin/lookup
      info/2.0</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="data" metadataIdRef="meta" />
</nmwg:message>
```

4. In the **Execute query** section, click **Query** to send the LookupInfoRequest to the RRD MA. If you have installed the service correctly a LookupInfoResponse is returned. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl_resp" messageIdRef="idl1" type="LookupInfoResponse"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="localhost.-3056f7be:11977e9a1c8:-7a42"/>
  <nmwg:data id="localhost.-3056f7be:11977e9a1c8:-7a41"
metadataIdRef="localhost.-3056f7be:11977e9a1c8:-7a42">
    <psservice:datum
xmlns:psservice="http://ggf.org/ns/nmwg/tools/org/perfsonar/service/1.
0/">
      <psservice:service>
        <psservice:serviceName>perfSONAR RRD MA</psservice:serviceName>
        <psservice:accessPoint>http:// localhost:8180/geant2-java-rrd-
ma/services/MeasurementArchiveService</psservice:accessPoint>
        <psservice:serviceType>ma</psservice:serviceType>
        <psservice:serviceDescription>perfSONAR RRD
MA</psservice:serviceDescription>
        <psservice:serviceVersion>3.1</psservice:serviceVersion>
        <psservice:organization>PSNC</psservice:organization>
        <psservice:contactEmail>user@my_domain</psservice:contactEmail>
      </psservice:service>
    </psservice:datum>
  </nmwg:data>
</nmwg:message>
```

5.5 Installation and Configuration: Best Practice

To ensure that the RRD MA works properly, you need to make sure you install and configure it correctly. The following best practices will help you to avoid potential problems with the RRD MA or its data display in the perfsonarUI interface.

- Avoid using eXist directly through the eXist web interface (<http://localhost:<port>/geant2-java-rrd-ma/exist>, where **<port>** is 8080 or 8180) to manage collections. Instead, use the tools that the Web Admin pages provide. If you cannot avoid using the eXist administration interface, remember that the collections must be owned by the **rrdmaservice** user, so you should log in as **rrdmaservice** user and not as **admin**.

- By default, after the installation eXist already has the administrative user (user: `admin`, password: not set) configured (this does not apply if you are integrating with a pre-existing eXist database).
- Make sure that the RRD data you are publishing (pointed to by the XML configuration file) are hosted in a directory to which the user running Tomcat has Read access.
- Ensure your machine has the correct time settings (the clock must show the correct time and date), otherwise you may experience data display problems.
- Ensure that your XML configuration file and its host directory are readable by the Tomcat user.
- Make sure that the schema versions for NM-WS namespaces data reported in the initial section of the XML configuration are the recommended ones. These values must be set as follows (see *Creating a Metadata Configuration File* on page 34):

```
<nmwg:store xmlns:nmwgt="http://ggf.org/ns/nmwg/topology/2.0/"
xmlns:nmtm="http://ggf.org/ns/nmwg/time/2.0/"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/"
xmlns:perfsonar="http://ggf.org/ns/nmwg/tools/org/perfsonar/1.0/"
xmlns:netutil="http://ggf.org/ns/nmwg/characteristic/utilization/2.0/"
xmlns:errors="http://ggf.org/ns/nmwg/characteristic/errors/2.0/"
xmlns:discards="http://ggf.org/ns/nmwg/characteristic/discards/2.0/"
xmlns="http://ggf.org/ns/nmwg/base/2.0/">
```

You must also ensure that all required data and meta data formats are correct in the various entries of the file (see *Creating a Metadata Configuration File* on page 34).

6 SQL MA

The SQL Measurement Archive (SQL MA) stores link data that is collected by measurement tools. It provides the following measurements:

- IP interface link utilisation
- IP interface link capacity
- IP interface input errors
- IP interface output drops
- Circuit / lightpath status
- Achievable throughput (TCP)
- UDP throughput

You can access the data using the personarUI web client (for IP link utilisation) or E2EMon (for circuit/lightpath status).

6.1 System Architecture

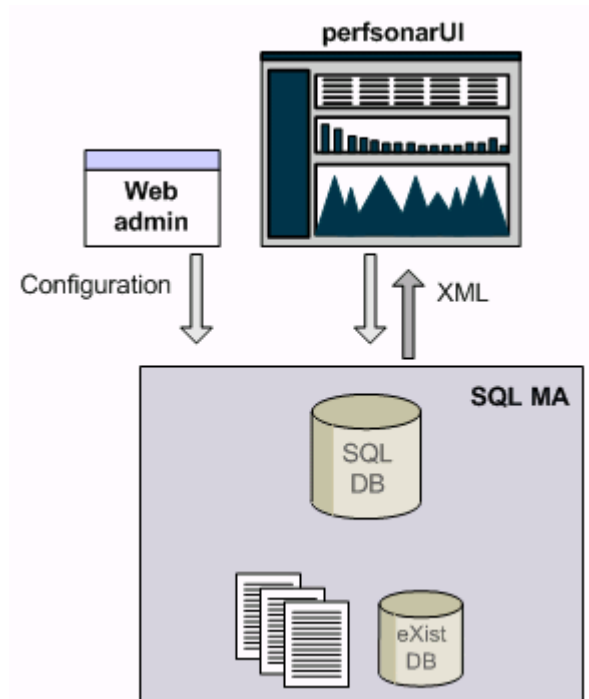


Figure 6.1: SQL MA system architecture.

When users access archived data from the SQL MA from the perfsonarUI web client, perfsonarUI sends an XML request to the SQL MA. The SQL MA then retrieves the data from the SQL DB and returns an XML reply to the client.

The SQL MA is configured via a Web Admin interface which is included in the SQL MA installation. The Web Admin interface stores the configuration settings in an eXist database (meta configuration information) and files (non-meta configuration information) from where they are applied to the SQL MA.

6.2 Installing

Note:

- It is recommended that you also install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you are also installing the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.

6.2.1 Prerequisite Software

The SQL MA requires the following software to be present on its host machine, before it can be installed:

- Java JDK 1.5
- Tomcat 5.5
- eXist 1.1.x or 1.2.x
- MySQL 5.x

See *Prerequisite Software* on page 4 for details.

6.2.2 Installing on Linux

If you are running a Linux operating system, you can install the SQL MA using RPM distributions or in a non-RPM distribution. If you are using Debian, you need to install the SQL MA using Debian packages.

To install using RPM distributions:

1. If you don't have relational database installed, execute the following command to install MySQL:

```
yum install mysql mysql-server
```

Make sure your database is configured and running (for more details, see the MySQL manual at <http://dev.mysql.com/doc/refman/5.0/en/index.html>).

2. Make sure that you configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the SQL MA are also installed.

```
yum search jdk          (if you have used a repository to install JDK)
```

```
yum search tomcat5
```

```
yum search exist
```

```
yum search mysql
```

3. Install the RPM package:

```
sudo yum install perfsonar-java-sql-ma.noarch
```

Prerequisite software is included in the package and automatically installed.

4. Execute the following command to create the database schema:

```
mysql -u root -p <
```

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql
```

5. Copy the following files:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/var/lib/tomcat5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/geant2-java-sql-ma/WEB-INF/lib/xercesImpl-
2.8.0.jar /var/lib/tomcat5/common/endorsed
```

Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy.sh>

6. Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

To install using Debian packages:

1. If you don't have relational database installed, execute the following command to install MySQL:

```
apt-get install mysql-server
```

Make sure your database is configured and running (for more details, see the MySQL manual at <http://dev.mysql.com/doc/refman/5.0/en/index.html>).

2. Execute the following command to install Java SQL MA service:

```
apt-get install perfsonar-java-sql-ma
```

3. Execute the following command to create the database schema:

```
mysql -u root -p <
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-
INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql
```

4. In the `/etc/default/tomcat5.5` Tomcat configuration file, uncomment and switch off **TOMCAT5_SECURITY** as follows:

```
TOMCAT5_SECURITY=no
```

5. Copy the eXist XML library files into the Tomcat-endorsed library directory:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/usr/share/tomcat5.5/common/endorsed/
```

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xercesImpl-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/usr/share/tomcat5.5/common/endorsed/
```

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

6.2.3 Testing the Installation

You can test if you have installed the SQL MA correctly by checking if the Web Admin pages can be displayed. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

To test the installation:

Open a Mozilla browser and enter the following URL:

`http://<host>:<port>/geant2-java-sql-ma`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-sql-ma>

If you have installed the SQL MA correctly, the Web Admin pages are displayed. If you cannot access the Web Admin page (your browser displays "Failed to connect"), ensure that you do not have firewalls which prevent access to the page (hardware or s/w like iptables).

Once you have successfully tested your installation, you need to configure the SQL MA (see *Configuring the SQL MA* on page 50).

6.3 Configuring the SQL MA

Before you can use the SQL MA, you need to configure it. For this you can use the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

6.3.1 Mandatory Basic Configuration

To configure the settings that the SQL MA requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

http://<host>:<port>/geant2-java-sql-ma

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-sql-ma>

2. Under the **Basic Configuration** heading in the navigation panel, click **Service**.

A login prompt is displayed.

3. Enter your login details (the default login is `perfsonaruser` and `perfsonarpass`) and click **OK**.

The basic service configuration settings page is displayed. This page lists the settings that the SQL MA requires to be configured in order to be able to run:

Administration Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the username for logging in to the admin pages

Specify the username that users have to enter to log in to the Web Admin pages.

Enter the password for logging in to the admin pages

Specify the password that users have to enter to log in to the Web Admin pages (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Authentication Configuration

If you have installed an Authentication Service or are permitted to use a third party AS, this section allows you to enable authentication for your SQL MA by registering it with this AS. This means that you can restrict specific request types to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

Do you wish to enable authentication

Select **yes** if you want to restrict access to the SQL MA. This means that only users who have a GIdP account can send messages of types specified in the **Enter the message types which should be authenticated** field to the SQL MA.

Enter the URL address of the Authentication Service

Enter the URL of the AS that you are using to authenticate users. This can be an AS you have installed yourself or a third party AS that you are permitted to use.

Enter the message types which should be authenticated

Enter a CSV of the types of message for which you require authentication. You can restrict the following message types:

- **MetadataKeyRequest**
Requests a list of all supported devices and the commands they support.
- **SetupDataRequest**
Executes commands on the devices the RRD MA is connected to.
- **MeasurementArchiveStoreRequest**
Stores measurement data in the RRD MA.

LS Configuration

This section allows you to register your SQL MA with the Lookup Service.

Do you wish to register with an LS

Select **yes** to register the SQL MA with the Lookup Service. This means that every time the SQL MA starts running, it signals its availability to the LS. From there other clients (usually visualisation tools) can see that the SQL MA is available and check its capabilities.

Enter the service name

Enter a name for the SQL MA service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Enter a description for the service

Enter a description for the SQL MA service. The LS displays this to clients as part of the SQL MA's capability details.

Enter the service administrator's email address

Enter the email address of the SQL MA administrator. The LS displays this to clients as part of the SQL MA's capability details.

Enter the name of the organisation running this service

Enter the email address of the organisation who is hosting the SQL MA. The LS displays this to clients as part of the SQL MA's capability details.

Enter the LS URL

Enter the URL of the LS that you want to register the SQL MA with.

Example: <http://localhost:8180/geant2-java-xml-ls/services/LookupService>

Set the registration interval (milliseconds)

Enter the amount of time (in milliseconds) to elapse between registration requests to the Lookup Service. By default this is 43200000 milliseconds (12 hours).

Enter the service access point

Enter the URL to the location where your SQL MA is installed.

Example: <http://myhost:8180/geant2-java-sql-ma/services/MeasurementArchiveService>

eXist Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the URI location of the eXist database

Enter the URI to the location where your eXist database is installed.

Enter the service username for the eXist user

Enter the service username for the SQL MA user of the eXist database. It is recommended that you use the default value.

Enter the password for the eXist user

Specify the password that SQL MA users have to enter to log in to the eXist database.

Do you wish to create a user with this name

Select **yes** or **no** to indicate if you want to create this user in eXist.

Enter the eXist administration password

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Enter the full path of the metadata configuration file

Enter the full path to the XML metadata configuration file required for stitching (see *SQL MA Stitching* on page 57). By default the path to an example metadata configuration file is specified, which comes with the service. This file contains some test data that you can use as a template for creating your own file.

While initialising SQL MA this XML file will be copied from this location to the eXist database, so that the SQL MA can start to use it.

Do you wish to change the eXist admin password

Select **yes** or **no** to indicate if you want to change the eXist administrator password.

Enter the eXist administration password

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Confirm the new eXist administration password

Re-enter the password for the eXist administrator.

Enter the old eXist administration password

If you install the SQL MA and already have an existing eXist installation, the Web Admin pages cannot access the admin password of the existing eXist database. Enter the existing eXist admin password in this field, so the SQL MA can access it. If you want to keep the existing password, you also need to enter it in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** fields. If you want to change it, enter the password that you want to replace it with in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** fields.

4. Click **apply**.
5. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 55).

6.3.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

1. Log on to the Web Admin pages.
2. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the SQL MA according to your requirements.
3. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
4. Click **apply** to apply your modifications.

5. Under the **Advanced Configuration** heading in the navigation panel, click **Logging**.
The advanced service configuration settings page is displayed. This page lists the logging settings that you can configure to customise the SQL MA according to your requirements.

Note that if you want to send all logging data to a syslog server, you need to enable syslog message logging by pointing the **service.log.log4j.config** setting to the **log4j.syslog.properties** configuration file rather than the **log4j.properties** configuration file (the **service.log.log4j.config** setting is located on the **Advanced Configuration Service** page in the **Internals** group).
6. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
7. Click **apply** to apply your modifications.
8. Under the **Advanced Configuration** heading in the navigation panel, click **SQL MA Admin**.
9. The SQL MA administration page is displayed. This page lists the iBATIS files used by the SQL MA and their details (metric type, database URL, database name, user name and table name). You can select an iBATIS file and click **Edit File** to change its details or **Delete File** to delete it. You can also create a new iBATIS file by clicking **Create File**, specifying the required details and clicking **Create**.
10. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
11. Enter your login details (the default username is admin and an empty password field, unless you have set an administration password) and click **OK**.
12. The **eXist Database Administration** page is displayed. This page comprises the following tabs:
 - Manage Collections**

This tab lists the eXist resources and their details (owners, groups, permissions and creation dates). You can select a resource and click **Edit Resource** to change its details or **Delete Resource** to delete it. You can also create a new resource by clicking **Create Resource**, specifying the required details and clicking **Create**.
 - Manage Users**

This tab lists the eXist users and their details (groups and homes). You can select a user and click **Edit** to change their details or **Delete** to delete them. You can also create a new user by clicking **Create**, specifying the required details and clicking **Create**.
13. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 55).

6.3.3 Configuring the SQL MA to Store Data

By default the SQL MA does not store new data that is sent to it. To store new data that it receives from other perfSONAR web services:

1. Open the **/etc/geant2-java-sql-ma/service.properties** file in a text editor.

2. Find the **service.ma.message_types** variable and enter a comma-separated list of the message types connected to the data that you want the service to store (default values are sufficient).

For example:

```
service.ma.message_types=MetadataKeyRequest,SetupDataRequest,EchoRequest
```

You can find further details about message types in the **/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/doc** directory in the following files:

Installation_Actions_Specification.doc

Functional specification.doc

3. Find the **service.ma.xmldb.db_store** variable and set it to **on**.
4. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

6.4 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the SQL MA correctly:

1. Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**. The **Deployment test** page is displayed.
2. Click the **start test** button to check if you have deployed the SQL MA correctly. If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the SQL MA correctly by using the perfsonarUI client to send an EchoRequest or a LookupInfoRequest to it.

To send an EchoRequest:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the SQL MA service:

```
http://<host>:<port>/geant2-java-sql-ma/services/MeasurementArchiveService
```

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-sql-ma/services/MeasurementArchiveService>

3. In the **Execute query** section, click **Query** to send an EchoRequest to the SQL MA. If you have installed the service correctly an EchoResponse is returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"messageIdRef="message1208947296"
type="EchoResponse" xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
the echo response from the service.</nmwgr:datum>
  </nmwg:data>
</nmwg:message>
```

To send a LookupInfoRequest:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the SQL MA service:

http://<host>:<port>/geant2-java-sql-ma/services/MeasurementArchiveService

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8180/geant2-java-sql-ma/services/MeasurementArchiveService>

3. In the **Query** field, enter the following LookupInfoRequest:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl" type="LookupInfoRequest"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="meta">
    <nmwg:eventType>http://schemas.perfsonar.net/tools/admin/lookup
info/2.0</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="data" metadataIdRef="meta"/>
</nmwg:message>
```

4. In the **Execute query** section, click **Query** to send the LookupInfoRequest to the SQL MA. If you have installed the service correctly a LookupInfoResponse is returned. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="idl_resp" messageIdRef="idl" type="LookupInfoResponse"
xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="localhost.-3056f7be:11977e9a1c8:-7a3e"/>
  <nmwg:data id="localhost.-3056f7be:11977e9a1c8:-7a3d"
metadataIdRef="localhost.-3056f7be:11977e9a1c8:-7a3e">
    <psservice:datum
xmlns:psservice="http://ggf.org/ns/nmwg/tools/org/perfsonar/service/1.
0/">
      <psservice:service>
        <psservice:serviceName>perfSONAR SQL MA</psservice:serviceName>
        <psservice:accessPoint>http://localhost:8180/geant2-java-sql-
ma/services/MeasurementArchiveService</psservice:accessPoint>
        <psservice:serviceType>ma</psservice:serviceType>
        <psservice:serviceDescription>perfSONAR SQL
MA</psservice:serviceDescription>
        <psservice:serviceVersion>2.0</psservice:serviceVersion>
        <psservice:organization>PSNC</psservice:organization>
        <psservice:contactEmail>user@domain</psservice:contactEmail>
      </psservice:service>
    </psservice:datum>
  </nmwg:data>
</nmwg:message>
```

Once you have successfully tested your deployment, you need to perform SQL MA stitching (see *SQL MA Stitching* on page 57).

6.5 SQL MA Stitching

To be able to understand the measurement data that the SQL MA provides access to, it needs meta information that puts the data into context. For example, metadata that defines:

- the IP interface address for which measurement data is collected
- the DNS name of the network element in which the IP interface is hosted
- the IP interface 's capacity

The meta information is stored in an XML metadata configuration file which you need to create for your network and then apply to your SQL MA. This process is referred to as “stitching”. Before you can perform this you need to expose your MySQL or PostgreSQL database to the SQL MA.

6.5.1 Exposing Your MySQL or PostgreSQL Database to the SQL MA

Before you can carry out the stitching process, you need to be familiar with the structure of the SQL database/tables in which your measurements are stored. If you don't yet have a structure, it is recommended that you use the default structure described here:

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql
```

(MySQL database structure)

If you are planning to use the recommended table structures, note down the names of the SQL tables that you intend to use. The SQL MA uses iBATIS configuration files to keep track of tables and table data access. Each SQL table is represented by at least one iBATIS file. The information contained in each file is mostly about table name, database location, username, password, etc.

The following table lists the default database tables and the associated iBATIS filenames. These iBATIS files are created and made available by default. You only need to change their values.

Metric Family	Metric	SQL Table Name	iBATIS File Name	Database Particulars (URL, username, password)
Packet	Utilisation	perfsonar-utilisation	ibatis-SqlMapConfig-utilization.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
	Errors	perfsonar-utilisation	ibatis-SqlMapConfig-errors.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
	Discards	perfsonar-discards	ibatis-SqlMapConfig-discards.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
Circuit/ lightpath status	Domain link	domain_link	ibatis-SqlMapConfig-L2-status-domain.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
	Interdomain link	interdomain_link	ibatis-SqlMapConfig-L2-status-interdomain.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma

Metric Family	Metric	SQL Table Name	iBatis File Name	Database Particulars (URL, username, password)
BWCTL tests	lperf	perfsonar_lperf	ibatis-SqlMapConfig-lperf.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
	OWAMP	clmp_owamp	ibatis-SqlMapConfig-clmp-owamp.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma
	BWCTL	clmp_bwctl	ibatis-SqlMapConfig-clmp-bwctl.xml	jdbc:mysql://127.0.0.1 , perfsonar_ma , perfsonar_ma

Note: To help you compile the information, you may want to create a similar table to list your own database tables, the associated iBatis files and database access particulars.

To change iBatis file values on the system:

1. Check that you have created all necessary SQL tables, usernames and passwords in your SQL database.
2. Log on to the Web Admin pages (see *Mandatory Basic Configuration* on page 50).
3. Under the **Advanced Configuration** heading in the navigation panel, click **SQL MA Admin**.

The SQL MA administration page is displayed. This page lists the iBatis files used by the SQL MA and their details (metric type, database URL, database name, user name and table name). You can select an iBatis file and click **Edit File** to change its details or **Delete File** to delete it. You can also create a new iBatis file by clicking **Create File**, specifying the required details and clicking **Create**.

6.5.2 Creating the Metadata Configuration File

The following documents provide sample metadata configuration files and explain the required format:

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/sql-database-L2status_TEST.xml (lightpath status)
```

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/sql-database_discards_TEST.xml (discards)
```

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/conf/sql-database_errors_TEST.xml (errors)
```

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/sql-database_utilization_TEST.xml
```

(utilisation)

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/sql-database_iperf_TEST.xml
```

(iperf)

```
/usr/lib/perfsonar/services/geant2-java-sql-ma/WEB-INF/classes/perfsonar/conf/mysql-sqlma-dbsetup.sql/sql-database_clmp-owamp.xml
```

(owamp)

Note: To save time (especially for large networks) and avoid errors, it is recommended that you use automated scripts and tools to generate your metadata configuration.

6.5.3 Applying Your Metadata Configuration

Once you have created your metadata configuration file and checked that it has the required format, you need to configure your SQL MA to use your metadata configuration file instead of the default test/dummy file:

1. Log on to the Web Admin pages (see *Mandatory Basic Configuration* on page 50).
2. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
3. Log on using the service credentials you provided when you configured the service for the first time (by default the sqlmaservice username and a password chosen by you), and click **OK**.
4. The **eXist Database Administration** page is displayed.
Note: you must not log in as admin user to upload/change metadata config files.
5. Display the **Manage Collections** tab.
6. Click the name of the previously created SQL MA collection (listed in the Resource column). By default this is **sqlmaconfig**.
A list of XML files or resources that are stored in this collection is displayed. This list is either empty or may contain the default SQL MA config file (**sql-database_TEST.xml**).
7. Click the **Create Resource** button.
8. Browse to the metadata configuration file that you have created for your SQL MA, and click the **Create** button to upload it.
9. Click **Refresh** to update the file list.

10. Select the default/dummy metadata configuration file and click the **Delete Resource** button to delete it.
11. Click the **log out** button to log out.

You can now test your new configuration using perfsonar UI. You should be able to see all the interfaces that you have configured. If you have any problems check the format of the file, follow all the steps above and try again.

7 BWCTL MP

The Bandwidth Controller Measurement Point (BWCTL MP) executes on-demand bandwidth tests between two BWCTL tools (a BWCTL tool is a wrapper around the iperf bandwidth test tool). It provides the following measurements:

- Achievable throughput (TCP)
- UDP throughput

You can access the data using the perfsonarUI web client or the command line client.

7.1 System Architecture

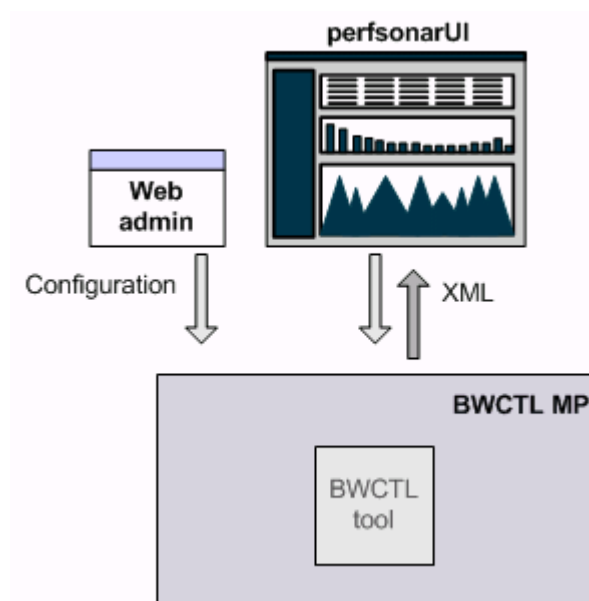


Figure 7.1: BWCTL MP system architecture.

When users request throughput measurements between 2 hosts running the BWCTL tool from perfsonarUI, the client sends an XML request to the BWCTL MP (this normally resides on one side of the tested path). The BWCTL MP then executes the measurement using the BWCTL tool (a wrapper around the Iperf bandwidth test tool) and returns the requested data to the client in an XML response.

The BWCTL MP can be configured via a Web Admin interface which is provided with an external package. The Web Admin interface stores the configuration settings in the **perfSONAR.conf** file which is part of the perfSONAR base installation.

7.2 Installing

Note:

- It is recommended that you also install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you are also installing the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.

7.2.1 Prerequisite Software

For the BWCTL to be able to work properly, you need to provide the following software:

- **iperf**
The BWCTL MP requires iperf version 2.0.2, as version 2.0.4 has an interval statistics bug (http://sourceforge.net/tracker/?func=detail&aid=1934426&group_id=128336&atid=711371). You can find iperf 2.0.2 RPMs for RedHat Enterprise Linux at <http://dag.wieers.com/rpm/packages/iperf/>. RPM packages are also available on RPMforge: <https://rpmrepo.org/RPMforge>. DEBs are available at <http://ftp.debian.org/debian/pool/main/i/iperf/>.
- **BWCTL**
You can find the BWCTL software at <http://e2epi.internet2.edu/bwctl/> (includes an installation and user manual). You need to install bwctl, bwctl-aespasswd, and bwctl-server, which contains the bwctl daemon. At the moment, it is not recommended to use bwctl 1.3 as this may have backwards compatibility problems. Use version 1.2a instead.
- **Perl**
Version 5.8.8 or later requires the Perl interpreter. Most Linux distributions provide a Perl interpreter and Perl packages. Any needed Perl modules not provided can be found on RPMforge.

- ntp
As BWCTL tests rely on accurate time synchronisation, it is recommended that you install an ntpd. Most Linux distributions provide ntpd packages.
- Apache
To use the web front-end to configure the BWCTL MP, you need to install Apache. This is provided by most Linux distributions as an httpd package.

Before you install the BWCTL MP, it is recommended that you manually test your BWCTL installation to ensure that BWCTL itself is running properly. You should also check that the TCP window size is set correctly to ensure that it won't limit the box throughput.

7.2.2 Testing the BWCTL

Start the BWCTL daemon and run a test from your host to another host that also has BWCTL installed and the daemon running. If everything works fine, your perfSONAR daemon should have no problems executing tests using this BWCTL installation.

If you should encounter any problems, do the following:

- If you have firewalls running, make sure that the BWCTL control port (4823) for TCP, and ports above 5000 (iperf) for UDP/TCP are open between the test boxes.
Example iptables rule for the BWCTL control port:

```
-A INPUT -p tcp --dport 4823 -j ACCEPT
```
- Make sure that the **bwctld.limits** file allows for measurements between the two boxes. See the BWCTL documentation for further information.
- Make sure that ntp is set up and running properly. The BWCTL tool will not report any results if the time synchronisation is not set up correctly. See the BWCTL documentation for further information.
- Make sure that the network connection between the two boxes is working properly. Check the control cables and network cards, and use standard tools like ping to test if you can get a connection.
- Make sure that you are using compatible BWCTL tool versions. Version 1.3 is currently not working with older versions. It is recommended that you use version 1.2a instead.

7.2.3 Setting the TCP Window Size

After you have installed BWCTL on your hosts, you need to check that the TCP window size is properly configured on each of the hosts to ensure that it doesn't limit the throughput of the box. Due to TCP's flow control mechanism and network delay on the testing path, TCP window size can limit the maximum theoretical throughput regardless of the bandwidth of the network path. For further information, see:

<http://kb.pert.geant2.net/PERTKB/WindowBasedTransmission>

<http://kb.pert.geant2.net/PERTKB/WindowScalingOption>

To set the TCP window size:

1. On each of your BWCTL host machines, set up policies to allow tests to be run between the machines.
2. Measure the Round Trip Time (RTT) delay between the hosts.
3. Set the TCP window size on each host according to the Bandwidth-Delay Product (BDP). For further information, see:

<http://kb.pert.geant2.net/PERTKB/EndSystemTuning>

<http://kb.pert.geant2.net/PERTKB/BandwidthDelayProduct>

4. Configure your BWCTL installations to use the TCP window size you have set using the throughput test argument **-w** (mandatory) or **-W** (advisory). See <http://e2epi.internet2.edu/bwctl/bwctl.man.html> for further information.

7.2.4 Installing on Linux

If you are running a Linux operating system, you can install the BWCTL MP using RPM distributions. If you are using Debian, you need to install the BWCTL MP using Debian packages.

To install using RPM distributions

1. Log on as root to the machine on which you want to host the BWCTL MP.
2. Check that you have installed all prerequisite software (see *Installing Prerequisite Software Using Packages* on page 5).

Note: The RPMs have dependencies for Perl modules which might not be part of your distribution. RPM informs you about missing dependencies, so you can complete your Perl environment properly.

On Red Hat Enterprise Linux, the Perl modules may not be known to your standard yum repository. These packages can be found on RPMforge. See <https://rpmrepo.org/RPMforge/Using> for information how to set up your system properly for using RPMforge packages.

As RPMforge has an old version of perl-XML-LibXML, you need to get this package from another source. Use RPM Search to find an appropriate package.

3. If you are using a Red Hat distribution you can install the packages using:

```
yum install perfsonar-oppd-mp-bwctl.noarch
```

4. Install the web admin user interface:

```
yum install perfsonar-oppd-WebAdmin
```

Once you have finished installing, you need to set up the Web Admin interface (see *Setting up the Web Admin Interface* on page 66).

To install using Debian packages

1. Log on as root to the machine on which you want to host the BWCTL MP.
2. To install the BWCTL MP web service and dependencies (if required) use the following command (for all architectures):

```
sudo apt-get install perfsonar-oppd-mp-bwctl
```

3. Install the web admin user interface:

```
sudo apt-get install perfsonar-oppd-WebAdmin
```

Once you have finished installing, you need to set up the Web Admin interface (see *Setting up the Web Admin Interface* on page 66).

7.2.5 Setting up the Web Admin Interface

Once you have installed the Web Admin package, a new **WebAdmin** directory is created in **/usr/lib/perfsonar/services/oppd/geant2-perl-bwctl-mp/**. This directory is linked to your Apache environment in **/var/www/html/** and contains the Web Admin interface files. Before you can use the interface, you need to set up your Apache to use the Web Admin interface by ensuring that your Apache is able to execute cgi-scripts.

On Red Hat based systems

1. If you are running SELinux, execute the following commands to set the required execution permissions (if you are running another UNIX flavour, skip to step 2):

```
chcon -t httpd_sys_content_t
/usr/lib/perfsonar/services/oppd/geant2-perl-bwctl-mp/cgi-bin/test.pl
chcon -t httpd_sys_content_t
/usr/lib/perfsonar/services/oppd/geant2-perl-bwctl-mp/cgi-bin/finish.pl
chcon -t httpd_sys_content_t
/usr/lib/perfsonar/services/oppd/geant2-perl-bwctl-mp/cgi-bin/wizard.pl
chcon -t httpd_sys_content_t
/usr/lib/perfsonar/services/oppd/etc/oppd.conf
```

2. Open your **/etc/httpd/conf/httpd.conf** file in a text editor, and check that it contains the following line:

```
AddHandler cgi-script .cgi .pl
```

3. You may only have to remove a # character in front of the line to make it work.

4. In the file **/etc/httpd/conf/htusers**, create a key for a user called “bwctl” (the Apache configuration for the WebAdmin expects a user called “bwctl” to authenticate):

```
htpasswd -c /etc/httpd/conf/htusers bwctl
[type password]
```

If you are not familiar with this procedure, it is recommended that you read the Apache tutorials about `cgi` and `authorisation`, which explain all necessary steps in more detail (<http://httpd.apache.org/docs/2.0/howto/cgi.html> and <http://httpd.apache.org/docs/2.0/howto/auth.html>).

5. After configuring Apache, reload the `httpd` daemon to read in the new configuration.

Once you have finished installing and setting up the Web Admin interface, it is recommended that you test your installation (see *Testing the Installation* on page 67).

On Debian based systems

1. Open your **/etc/apache2/apache2.conf** file in a text editor, and check that it contains the following line:

```
AddHandler cgi-script .cgi .pl
```

You may only have to remove a `#` character in front of the line to make it work.

2. In the file **/etc/apache2/htusers**, create a key for a user called “bwctl” (the Apache configuration for the WebAdmin expects a user called “bwctl” to authenticate):

```
htpasswd -c /etc/httpd/conf/htusers bwctl
[type password]
```

3. If you are not familiar with this procedure, it is recommended that you read the Apache tutorials about `cgi` and `authorisation`, which explain all necessary steps in more detail (<http://httpd.apache.org/docs/2.0/howto/cgi.html> and <http://httpd.apache.org/docs/2.0/howto/auth.html>).

4. After configuring Apache, reload the `httpd` daemon to read in the new configuration.

Once you have finished installing and setting up the Web Admin interface, it is recommended that you test your installation (see *Testing the Installation* on page 67).

7.2.6 Testing the Installation

To test if you have correctly installed the BWCTL MP:

1. Change to the path **/usr/lib/perfsonar/services/oppd/bin**.
2. Type `./oppd.pl -nologfile -nopidfile`. If you have installed the BWCTL MP correctly, the `perfSONAR` daemon for BWCTL MP starts with the notification **notice: oppd service started**. You can stop the daemon with **ctrl-c**.

To test your Web Admin installation, check if you can display the Web Admin pages. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

Open a Mozilla browser and enter the following URL:

`http://<host>/geant2-perl-bwctl-mp/index.html`

`<host>`

The IP address or name of the machine that hosts the web service.

For example:

<http://localhost/geant2-perl-bwctl-mp/index.html>

If you have installed the Web Admin correctly and followed the steps for setting up Apache, the Web Admin pages are displayed. Note you will be asked a username and password first.

Once you have successfully tested your installation, you need to configure the service (see *Configuring the BWCTL MP* on page 68).

7.3 Configuring the BWCTL MP

Before you can use the BWCTL MP, you need to configure it. For this you can use the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

7.3.1 Mandatory Basic Configuration

To configure the settings that the BWCTL MP requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

`http://<host>/geant2-perl-bwctl-mp/index.html`

`<host>`

The IP address or name of the machine that hosts the web service.

For example:

<http://localhost/geant2-perl-bwctl-mp/index.html>

If you have set up authentication, a login prompt is displayed.

2. Enter your login details, and click **OK**.
3. Under the **Basic Configuration** heading in the navigation panel, click **Service**.

The basic service configuration settings page is displayed. This page lists the settings that the BWCTL MP requires to be configured in order to be able to run:

BWCTL Configuration

This section allows you to configure BWCTL-specific settings.

Enter the path to the BWCTL binary

Enter the path to the directory in which the BWCTL binary file is stored.

LS Configuration

This section allows you to register your BWCTL MP with the Lookup Service.

Do you wish to register with an LS

Select **yes** to register the BWCTL MP with the Lookup Service. This means that every time the BWCTL MP starts running, it signals its availability to the LS. From there other clients (usually visualisation tools) can see that the BWCTL MP is available and check its capabilities.

Enter the service name

Enter a name for the BWCTL MP service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Give a description of the service

Enter a description for the BWCTL MP service. The LS displays this to clients as part of the BWCTL MP's capability details.

Enter the contact email address

Enter the email address of the BWCTL MP administrator. The LS displays this to clients as part of the BWCTL MP's capability details.

Enter the name of the organization running this service

Enter the email address of the organisation who is hosting the BWCTL MP. The LS displays this to clients as part of the BWCTL MP's capability details.

Give the LS url

Enter the URL of the LS that you want to register the BWCTL MP with.

Example: <http://localhost:8080/xml-ls/services/LookupService>

Give the registration interval in seconds

Enter the amount of time (in seconds) to elapse between registration requests to the Lookup Service. By default this is 3600 seconds (1 hour).

Give the service hostname

Enter the URL to the location where your BWCTL MP is installed.

Example: <http://localhost>

Give the service port

Enter the port on which the BWCTL MP listens for requests.

Example: 8090

AS Configuration

If you have installed an Authentication Service or are permitted to use a third party AS, this section allows you to enable authentication for your BWCTL MP by registering it with this AS. This means that you can restrict requests to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

Do you wish to enable authentication

Select **yes** if you want to restrict access to the BWCTL MP. This means that only users who have a GIdP account can send messages to the BWCTL MP.

Enter the URL address of the Authentication Service

Enter the URL of the AS that you are using to authenticate users. This can be an AS you have installed yourself or a third party AS that you are permitted to use.

4. Click **apply**.

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 71).

7.3.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

1. Log on to the Web Admin pages.
2. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
The advanced service configuration settings page is displayed. This page lists the settings that you can configure to customise the BWCTL MP according to your requirements.
3. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
4. Click **apply**.

If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 71).

7.4 Integrating the BWCTL MP with Your System

If you are installing the BWCTL MP on a Linux system, you can use the start/stop script provided by the perfSONAR base package. It is located in `/etc/init.d/oppd` and enables you to conveniently start/stop the perfsonar daemon, or to automatically start/stop the daemon during startup/shutdown of your system by linking the script to different runlevels.

To ensure a smooth BWCTL test environment, it is recommended that you set up permissions in your `/etc/bwctld/bwctld.limits` file. Note that firewalls can also prevent BWCTL tests, so you need to set up appropriate rules. If your NTP daemon is not properly set up to use accurate time sources, your BWCTL tests will also be inaccurate or fail altogether.

7.5 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the BWCTL MP correctly:

1. Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**. The **Deployment test** page is displayed.
2. Click the **start test** button to check if you have deployed the BWCTL MP correctly. If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the BWCTL MP MP correctly by using the perfsonarUI client:

1. Start the PerfSONAR daemon:

```
/usr/lib/perfsonar/services/bin/perfsonar.pl -nologfile -nopicfile
```

If you are running on Fedora/Red Hat, log in as root and start the daemon using:

```
service perfsonar start
```

2. Start PerfsonarUI and display the **Playground** page.
3. In the **Service address** field, enter the URL to the BWCTL MP service:

`http://<host>:<port>/services/MP/BWCTL`

`<host>`

The IP address or name of the machine that hosts the web service.

`<port>`

The port on which the web service listens for commands. By default this is 8090.

For example:

<http://localhost:8090/services/MP/BWCTL>

4. In the **Execute query** section, click **Query** to send an EchoRequest to the BWCTL MP. If you have installed the service correctly an EchoResponse is returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"
  messageIdRef="message1208947296" type="EchoResponse"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
    metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
      the echo response from the service.</nmwgr:datum>
    </nmwg:data>
  </nmwg:message>
```

8 Telnet/SSH MP

The Telnet/SSH Measurement Point (MP) retrieves configuration and running information from network hardware and encapsulate this information in SOAP messages. Clients can request this information from the MP to retrieve the following measurements from otherwise unreachable devices:

- RTT
- Show Command
- Traceroute

You can access the data using the Looking Glass web client.

Note: Setting up the Telnet/SSH MP consists of two mandatory phases:

- Installation (see *Installing* on page 74)
You need to install the service on a server in your domain.
- Configuration (see *Configuring the SSH/Telnet MP* on page 77)
You need to create a metadata configuration file that defines how the Telnet/SSH MP should deal with commands, and configure basic settings that determine the location of components that the Telnet/SSH MP interacts with, set access credentials etc. The service is then started up or restarted to apply the configuration.

8.1 System Architecture

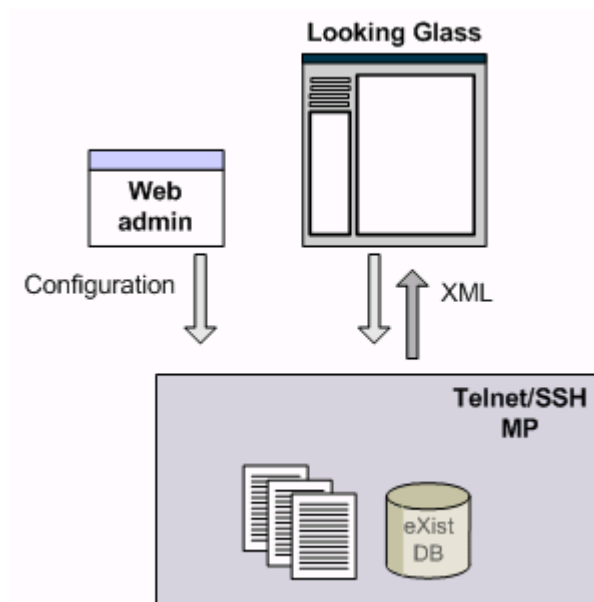


Figure 8.1: Telnet/SSH MP system architecture.

When users request RTT, Show Command or Traceroute information from the Looking Glass, the client sends an XML request to the Telnet/SSH MP. The Telnet/SSH MP then retrieves the requested information from the routers it connects to and returns the requested data to the client in an XML response.

The Telnet/SSH MP is configured via a Web Admin interface which is included in the Telnet/SSH MP installation. The Web Admin interface stores the configuration settings in an eXist database (meta configuration information) and files (non-meta configuration information) from where they are applied to the Telnet/SSH MP.

8.2 Installing

Note:

- It is recommended that you also install the Lookup Service, so you are able to check which services you can access across the network.
- It is recommended that you install the Authentication Service, so you can enable authentication for your web services.
- If you are also installing the Lookup Service and the Authentication Service, you should install the Lookup Service first and the Authentication Service second before you install any of the other services.

8.2.1 Prerequisite Software

The Telnet/SSH MP requires the following software to be present on its host machine, before it can be installed:

- Java JDK 1.5
- Tomcat 5.5
- eXist 1.1.x or 1.2.x

See *Prerequisite Software* on page 4 for details.

8.2.2 Installing on Linux

If you are running a Linux operating system, you can install the Telnet/SSH MP using RPM distributions or in a non-RPM distribution. If you are using Debian, you need to install the Telnet/SSH MP using Debian packages.

To install using RPM distributions

1. Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the Telnet/SSH MP are also installed.

```
yum search jdk          (if you have used a repository to install JDK)
yum search tomcat5
yum search exist
```

2. Install the RPM package:

```
sudo yum install perfsonar-java-sshtelnet-mp.noarch
```

Prerequisite software is included in the package and automatically installed.

3. Copy the following files:

```
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/var/lib/tomcat5/common/endorsed/
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/xml-apis.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/var/lib/tomcat5/common/endorsed
cp /var/lib/tomcat5/webapps/ps-mdm-sshtelnet-mp/WEB-INF/lib/xercesImpl-
2.8.0.jar /var/lib/tomcat5/common/endorsed
```

- Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy.sh>

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

To install using Debian packages

- Make sure you have configured the system repositories properly, so that the perfSONAR repository is enabled (see *Installing Prerequisite Software Using Packages* on page 5). This ensures that all dependencies required by the Telnet/SSH MP are also installed.

```
apt-cache search jdk          (if you have used a repository to install JDK)
```

```
apt-cache search tomcat5
```

```
apt-cache search exist
```

- To install the Telnet/SSH MP web service and dependencies (if required) use the following command (for all architectures) :

```
sudo apt-get install perfsonar-java-sshtelnet-mp
```

- Copy the following files:

```
cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/resolver-1.2.jar
/usr/share/tomcat5.5/common/endorsed
```

```
cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/xalan-2.7.1.jar
/usr/share/tomcat5.5/common/endorsed
```

```
cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/xml-apis.jar
/usr/share/tomcat5.5/common/endorsed
```

```
cp -v /var/lib/tomcat5.5/webapps/exist/WEB-INF/lib/serializer-2.9.1.jar
/usr/share/tomcat5.5/common/endorsed
```

```
cp -v /var/lib/tomcat5.5/webapps/ps-mdm-sshtelnet-mp/WEB-
INF/lib/xercesImpl-2.8.0.jar /usr/share/tomcat5.5/common/endorsed
```

- Alternatively, you can use the following script:

<http://downloads.perfsonar.eu/repositories/scripts/exist-jars-endorsed-copy-DEB.sh>

- Restart Tomcat (see *Starting and Stopping Tomcat* on page 7).

Once you have finished installing, it is recommended that you test your installation.

8.2.3 Testing the Installation

You can test if you have installed the Telnet/SSH MP correctly by checking if the Web Admin pages can be displayed. The Web Admin pages are a web interface that you need to configure the service, once you have successfully tested its installation.

To test the installation:

Open a Mozilla browser and enter the following URL:

`http://<host>:<port>/ps-mdm-sshtelnet-mp`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/ps-mdm-sshtelnet-mp>

If you have installed the Telnet/SSH MP correctly, the Web Admin pages are displayed. If you cannot access the Web Admin page (your browser displays "Failed to connect"), ensure that you do not have firewalls which prevent access to the page (hardware or s/w like iptables).

Once you have successfully tested your installation, you need to configure the service (see *Configuring the SSH/Telnet MP* on page 77).

8.3 Configuring the SSH/Telnet MP

Before you can use the Telnet/SSH MP, you need to:

1. Create a metadata configuration file that defines how the Telnet/SSH MP should deal with SHOW commands.
2. Configure basic settings that determine the location of components that the service interacts with, set access credentials etc.

8.3.1 Creating a Metadata Configuration File

To be able to execute SHOW commands on routers, the Telnet/SSH MP needs these commands to be defined for each router. This definition is made in an XML metadata configuration file which you need to create for your network.

You need to configure a set of SHOW commands that the Telnet/SSH MP can execute and a list of routers that these commands can be executed on. You can find information about the available commands here:

```
/usr/lib/perfsonar/services/ps-mdm-sshtelnet-mp/WEB-INF/doc/commands/
```

- `commands-complete-list.xls`
A complete set of commands that the MP supports.
- `commands_minimum_set.xls`
Strongly recommended set of commands to be configured.

To create an XML metadata configuration file for your network, you can use the following scripts:

- **CSV Generator script**
Used to generate a CSV file of routers and commands that you may wish to enable. This is useful for large networks and if you want to configure a large number of routers.
- **Configuration Tool**
Used to generate the metadata configuration file. To generate this file, you need to provide a list of commands and routers. For this you can use one of the following:
 - The CSV file generated by the CSV Generator script.
 - A previously generated metadata configuration file which you edit using the tool.
 - The tool's command line feature to provide the list of routers and commands. This is suitable if you have a small number of routers (up to 5).

These scripts and a readme file that contains additional explanations are stored in the following location:

```
/usr/lib/perfsonar/services/ps-mdm-sshtelnet-mp/WEB-INF/classes/perfsonar/contrib/metadata_configuration_tools/
```

The following document provides a sample metadata configuration file and explains the required format. If you don't want to use the scripts provided to generate a metadata config file, it is recommended that you use the sample metadata config file in this document as a template.

```
/usr/lib/perfsonar/services/ps-mdm-sshtelnet-mp/WEB-INF/doc/Metadata  
Configuration file for SSHTelnet 1.3.doc
```

Note: The sample file is Cisco-specific and needs to be adapted for alternative equipment. Passwords must be BASE64 encoded.

Once you have created your XML metadata configuration file, you are ready to configure basic settings for the Telnet/SSH MP (see *Configuring Basic Settings* on page 79).

8.3.1.1 Changing the Metadata Configuration File

If at any point you want to change which metadata configuration file the Telnet/SSH MP is using (for example, because you have amended your XML file or created a new one), you need to instruct the Telnet/SSH MP to use your new file as follows:

Note: Make sure your new metadata configuration file is named as **sshtelnetmetadata.xml**. This will reduce the number of configuration steps.

1. Log on to the Web Admin pages (see *Mandatory Basic Configuration* on page 80).
2. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
A login prompt is displayed.
3. Log on using the service credentials you provided when you configured the service for the first time (by default the **sshtelnet** username and a password chosen by you), and click **OK**.
The **eXist Database Administration** page is displayed.
Note: you must not log in as admin user to upload/change metadata config files.
4. Display the **Manage Collections** tab. Here, you can find the dummy/test metadata configuration file **sshtelnetmetadata.xml**.
5. Select the default/dummy metadata configuration file and click the **Delete Resource** button to delete it.
6. Click the **Create Resource** button.
7. Browse to the metadata configuration file that you have created for your Telnet/SSH MP, and click the **Create** button to upload it.
8. Click **Refresh** to update the file list. Confirm that your new file is present on the system.
9. Click the **log out** button to log out.

You can now test your new configuration using the Looking Glass UI. You should be able to see all the commands that you have configured. If you have any problems check the format of the file, follow all the steps above and try again.

8.3.2 Configuring Basic Settings

You can configure basic setting using the perfSONAR Web Administration pages, a web interface that provides a central point from which you can configure all the service's settings.

The Web Admin pages are split into basic and advanced configuration. Only the basic configuration is mandatory, the advanced configuration is optional and not normally needed.

Note: The purpose of the Web Admin pages is to aid you in the initial configuration that the service requires after its installation. It does not store the modifications you make to the service's configuration and displays the original default values if you open it again. That means that if you want to use the Web Admin pages to reconfigure the service at any point, you must again specify values for all settings, if you don't want to overwrite their configuration with the original default settings.

8.3.2.1 Mandatory Basic Configuration

To configure the settings that the Telnet/SSH MP requires:

1. Open a Mozilla browser and enter the following URL to display the Web Admin pages:

`http://<host>:<port>/ps-mdm-sshtelnet-mp`

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/ps-mdm-sshtelnet-mp>

2. Under the **Basic Configuration** heading in the navigation panel, click **Service**.
A login prompt is displayed.
3. Enter your login details (the default login is `perfsonaruser` and `perfsonarpass`) and click **OK**.
The basic service configuration settings page is displayed. This page lists the settings that the Telnet/SSH MP requires to be configured in order to be able to run:

LS Configuration

This section allows you to register your Telnet/SSH MP with the Lookup Service.

Do you wish to register with an LS

Select **yes** to register the Telnet/SSH MP with the Lookup Service. This means that every time the Telnet/SSH MP starts running, it signals its availability to the LS. From there other clients (usually visualisation tools) can see that the Telnet/SSH MP is available and check its capabilities.

Enter the service name

Enter a name for the Telnet/SSH MP service. It is recommended that you include an identifier of the domain that the service belongs to in the service's name.

Enter a description for the service

Enter a description for the Telnet/SSH MP service. The LS displays this to clients as part of the Telnet/SSH MP' capability details.

Enter the service administrator's email address

Enter the email address of the Telnet/SSH MP administrator. The LS displays this to clients as part of the Telnet/SSH MP' capability details.

Enter the name of the organisation running this service

Enter the email address of the organisation who is hosting the Telnet/SSH MP. The LS displays this to clients as part of the Telnet/SSH MP's capability details.

Enter the LS URL

Enter the URL of the LS that you want to register the Telnet/SSH MP with.

Example: <http://localhost:8080/xml-ls/services/LookupService>

Set the registration interval (milliseconds)

Enter the amount of time (in milliseconds) to elapse between registration requests to the Lookup Service. By default this is 900000 milliseconds (15 minutes).

Enter the service access point

Enter the URL to the location where your Telnet/SSH MP is installed.

Example: <http://myhost:8080/ps-mdm-sshtelnet-mp/services/TelnetSSH>

eXist Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the URI location of the eXist database

Enter the URI to the eXist database.

Enter the service username for the eXist user

Enter the service username for the Telnet/SSH MP user of the eXist database. It is recommended that you use the default value.

Enter the password for the eXist user

Specify the password that Telnet/SSH MP users have to enter to log in to the eXist database.

Do you wish to create a user with this name

Select **yes** or **no** to indicate if you want to create this user in eXist.

Enter the eXist administration password

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Enter the name of the metadata configuration file

Enter the name of the XML metadata configuration file you previously created (see *Creating a Metadata Configuration File* on page 77). By default the name of an example metadata configuration file is specified, which comes with the service.

Enter the full path to the metadata configuration file

Enter the full path to the XML metadata configuration file you previously created (see *Creating a Metadata Configuration File* on page 77). By default the path to an example metadata configuration file is specified, which comes with the service. This file contains some test data that you can use as a template for creating your own file.

Normally you should create your own XML metadata configuration file before you start configuring the Telnet/SSH MP. However, if you have not done this, you can keep the default path to the example file, and create your own XML file at a later stage (see *Changing the Metadata Configuration File* on page 79).

When you restart Tomcat at the end of the configuration, the XML file you point to is copied from the specified location to the eXist database and to the location of the example config file (`/etc/ps-mdm-sshtelnet-mp/sshtelnetmetadata.xml`), so that the Telnet/SSH MP can start to use it.

Example: `/tmp/telnetssh-my-config.xml`

Do you wish to change the eXist admin password

Select **yes** or **no** to indicate if you want to change the eXist administrator password.

Enter the eXist administration password

Enter the password for the eXist administrator (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Confirm the new eXist administration password

Re-enter the password for the eXist administrator.

Enter the old eXist administration password

If you install the Telnet/SSH MP and already have an existing eXist installation, the Web Admin pages cannot access the admin password of the existing eXist database. Enter the existing eXist admin password in this field, so the Telnet/SSH MP can access it. If you want to keep the existing password, you also need to enter it in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** fields. If you want to change it, enter the password that you want to replace it with in the **Enter the eXist administration password** and the **Confirm the new eXist administration password** fields.

Administration Configuration

This section allows you to set the login details for the Web Admin pages.

Enter the username for logging in to the admin pages

Specify the username that users have to enter to log in to the Web Admin pages.

Enter the password for logging in to the admin pages

Specify the password that users have to enter to log in to the Web Admin pages (if this field displays an asterisk, you must enter the correct password anyway because the value in this field always overwrites the current configuration).

Authentication Configuration

If you have installed an Authentication Service or are permitted to use a third party AS, this section allows you to enable authentication for your Telnet/SSH MP by registering it with this AS. This means that you can restrict specific request types to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

Do you wish to enable authentication

Select **yes** if you want to restrict access to the Telnet/SSH MP. This means that only users who have a GIdP account can send restricted messages to the Telnet/SSH MP.

Enter the URL address of the Authentication Service

Enter the URL of the AS that you are using to authenticate users. This can be an AS you have installed yourself or a third party AS that you are permitted to use.

Enter the message types which should be authenticated

Enter a CSV of the types of message for which you require authentication. You can restrict the following message types:

- **MetadataKeyRequest**
Requests a list of all supported devices and the commands they support.
- **SetupDataRequest**
Executes commands on the devices the Telnet/SSH MP is connected to.

4. Click **apply**.
5. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

Once you have completed the basic configuration, you should test your deployment (see *Testing Your Deployment* on page 84).

8.3.2.2 Optional Advanced Configuration

The advanced configuration is optional and not normally needed.

To configure advanced settings:

1. Log on to the Web Admin pages.
2. Under the **Advanced Configuration** heading in the navigation panel, click **Service**.
3. The advanced service configuration settings page is displayed. This page lists the service settings that you can configure to customise the Telnet/SSH MP according to your requirements.
4. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
5. Click **apply** to apply your modifications.
6. Under the **Advanced Configuration** heading in the navigation panel, click **Logging**.

7. The advanced service configuration settings page is displayed. This page lists the logging settings that you can configure to customise the Telnet/SSH MP according to your requirements.
8. Note that if you want to send all logging data to a syslog server, you need to enable syslog message logging by pointing the **service.log.log4j.config** setting to the **log4j.syslog.properties** configuration file rather than the **log4j.properties** configuration file (the **service.log.log4j.config** setting is located on the **Advanced Configuration Service** page in the **Internal** group).
9. Drag your mouse cursor over each of the listed settings to display a brief description of them. Check if the default values suit your environment and modify them if you need to.
10. Click **apply** to apply your modifications.
11. Under the **Advanced Configuration** heading in the navigation panel, click **eXist Database**.
12. A login prompt is displayed.
13. Enter your login details (the default username is admin and an empty password field, unless you have set an administration password) and click **OK**.
14. The **eXist Database Administration** page is displayed. This page comprises the following tabs:
 - Manage Collections**

This tab lists the eXist resources and their details (owners, groups, permissions and creation dates). You can select a resource and click **Edit Resource** to change its details or **Delete Resource** to delete it. You can also create a new resource by clicking **Create Resource**, specifying the required details and clicking **Create**.
 - Manage Users**

This tab lists the eXist users and their details (groups and homes). You can select a user and click **Edit** to change their details or **Delete** to delete them. You can also create a new user by clicking **Create**, specifying the required details and clicking **Create**.
15. Restart Tomcat to apply your configuration changes (see *Starting and Stopping Tomcat* on page 7).

If you have made any changes to advanced configuration, you should test your deployment (see *Testing Your Deployment* on page 84).

8.4 Testing Your Deployment

You can use the Web Admin pages to check if you have deployed the Telnet/SSH MP correctly:

1. Under the Web Admin pages' **Basic Configuration** heading in the navigation panel, click **Test**. The **Deployment test** page is displayed.
2. Click the **start test** button to check if you have deployed the Telnet/SSH MP correctly.

If your deployment is correct a Success message is displayed. If a message notifies you that the deployment test failed, you should reinstall Tomcat and your web service. Contact support if the problem persists.

Alternatively, you can check if you have deployed the Telnet/SSH MP correctly by using the perfsonarUI client to send an EchoRequest to it. To send an EchoRequest:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Service address** field, enter the URL to the Telnet/SSH MP:
http://<host>:<port>/ps-mdm-sshtelnet-mp/services/TelnetSSH

<host>

The IP address or name of the machine that hosts the web service.

<port>

The port on which the web service listens for commands. By default this is 8080 if you used RPM to install and 8180 if you used DEB to install.

For example:

<http://localhost:8080/ps-mdm-sshtelnet-mp/services/TelnetSSH>

3. In the **Execute query** section, click **Query** to send an EchoRequest to the Telnet/SSH MP. If you have installed the service correctly an EchoResponse is returned. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<nmwg:message id="message1208947296_resp"
  messageIdRef="message1208947296" type="EchoResponse"
  xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
  <nmwg:metadata id="resultCodeMetadata">
    <nmwg:eventType>success.echo</nmwg:eventType>
  </nmwg:metadata>
  <nmwg:data id="resultDescriptionData_for_resultCodeMetadata"
    metadataIdRef="resultCodeMetadata">
    <nmwgr:datum xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/">This is
      the echo response from the service.</nmwgr:datum>
    </nmwg:data>
  </nmwg:message>
```

Once you have successfully tested your deployment, you need to perform Telnet/SSH MP stitching.

8.5 Securing the Telnet/SSH MP with a Reverse Proxy

Because the MP is at the same directly connected to protected network equipment and accessible over the Internet, extra precaution must be taken to ensure its integrity and protect it against malicious attacks. A reverse proxy server can be set up to provide the required security.

A reverse proxy is a server with a generic interface which is typically used between one or more web servers and the Internet. All incoming requests are routed through the proxy server, which either deals with the request itself or passes some or all of it on to the web server. By providing a virtual layer that separates the MP's Internet interface from its network interface, the proxy server secures the Telnet/SSH MP.

8.5.1 Enabling Reverse Proxy in Apache

To enable reverse proxy functionality in Apache, you need to load and configure the following modules:

- **mod_proxy**
The core module deals with proxy infrastructure and configuration and managing a proxy request.
- **mod_proxy_http**
This handles fetching documents with HTTP and HTTPS.
- **mod_proxy_html**
This rewrites HTML links into a proxy's address space.
- **mod_headers**
This modifies HTTP request and response headers.

All these modules are all included in the core Apache distribution (except **mod_proxy_html**) and you can enable them easily in the Apache build process. For example:

```
$ ./configure --enable-so --enable-mods-shared="proxy proxy_http proxy_ftp
proxy_connect headers"
$ make
# make install
```

If you are adding proxying to an existing installation, you should use `apxs` instead:

```
# apxs -c -i [module-name].c
noting that mod_proxy itself is in two source files
(mod_proxy.c and proxy_util.c).
```

This leaves **mod_proxy_html**, which is not included in the core distribution. **mod_proxy_html** is a third-party module, and requires the third-party library **libxml2**. Do the following:

1. Check **libxml2** is installed. If you have a version older than 2.5.10, you should upgrade (a bug in earlier versions can, in some cases, severely affect performance).
2. From <http://apache.webthing.com/> download **mod_proxy_html.c**.
3. Build **mod_proxy_html** with `apxs`:

```
# apxs -c -I/usr/include/libxml2 -i mod_proxy_html.c
```

4. To configure the reverse proxy, add the following statements in the **httpd.conf** file enable the modules:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule headers_module modules/mod_headers.so
LoadModule deflate_module modules/mod_deflate.so
LoadFile /usr/lib/libxml2.so
LoadModule proxy_html_module modules/mod_proxy_html.so
```

5. Make sure that **ProxyRequests** is set to **Off** (if you fail to do this, your server turns into an open proxy which can be exploited by bots scanning the web for open proxies).
6. Use **ProxyPass** to set up proxy rules for the Telnet/SSH MP:

```
ProxyPass /TelnetSSH/ http://mdm-1.par.fr.geant2.net:8090/ps-mdm-sshtelnet-mp/services/TelnetSSH
```

7. Restart Apache to execute your configuration changes (it is recommended you use the "apachectl graceful" argument to do this).

As proxy requests are supported, <http://www.proxy.com/TelnetSSH/> maps to <http://mdm-1.par.fr.geant2.net:8090/ps-mdm-sshtelnet-mp/services/TelnetSSH>. However, **ProxyPass** just sends traffic straight through. For example, if the client misspelled the destination service URL, the response for <http://www.proxy.com/TelnetSSH> proxies to <http://mdm-1.par.fr.geant2.net:8090/ps-mdm-sshtelnet-mp/services/TelnetSSH> which generates the response:

```
HTTP/1.1 302 Found
Location: http://mdm-1.par.fr.geant2.net:8090/ps-mdm-sshtelnet-mp/services/TelnetSSH
(etc)
```

However, from the outside world this is seen as a "No such host" error.

8. Use the **ProxyPassReverse** command to enable the proxy to re-map the **Location** header to its own address space and return a valid URL:

```
ProxyPassReverse /TelnetSSH/ http://mdm-1.par.fr.geant2.net:8090/ps-mdm-sshtelnet-mp/services/TelnetSSH
```

The proxy re-maps the **Location** header to its own address space and can now return a valid URL:

```
HTTP/1.1 302 Found
Location: http://www.proxy.com/TelnetSSH/
```

9 Using Authentication

If you have installed an Authentication Service or are permitted to use a third party AS, you can enable authentication for your web services by registering them with this AS (see your web services' *Mandatory Basic Configuration* section). This means that you can restrict specific request types to only be executable by users with a GIdP account, while the requests of unauthorised users are ignored.

9.1 Restricting Access to Resources

If you have installed the Authentication Service, you can enable or disable authentication for your web services using your web services' Web Admin pages (see your web services' *Mandatory Basic Configuration* section).

You can test that you have successfully enabled authentication for a web service as follows:

1. Start PerfsonarUI and display the **Playground** page.
2. In the **Query Options** section, click **Options** to display the **Options** dialog.
3. Check the **Enable authentication and authorization** box, and click **OK**.
4. In the **Service address** field, enter the URL to the web service for which you have enabled authentication.
5. In the **Query** section, paste a query message. Note that this must be a message type that you have specified as requiring authentication (when you enabled authentication for the web service).
6. In the **Execute Query** section, click **Query** to send your query.

If you have enabled authentication successfully, you are prompted for your GIdP login details before the service returns a response. If you are not prompted to log in, you have either not enabled authentication or not enabled authentication for the type of message you have sent.

9.2 Accessing Protected Resources

To be able to access protected resources, you need authentication credentials. These are given to you if you get a GIdP (GÉANT Identity Provider) account. GIdP is a temporary IdP setup for early adopters of GÉANT services, which already exploits the eduGAIN framework and implementation. This is a temporary measure until IdPs in NRENs and end institutions are fully adapted to make use of the eduGAIN framework. Participants will then be able to use their local IdP accounts.

9.2.1 Getting a GIdP account

Most European NREN have a GIdP User Administrator from whom NREN members can request GIdP accounts. To find out who your GIdP UA is go to <http://gidp.geant2.net> and click the **NREN Contact Information** link. If you don't have a GIdP representative, please contact `gidp-service-admin` at `dante.org.uk`.

To get registered, you need to provide the following details:

- Name(s)
- Work address
- Phone & Fax
- Email address(es)
- Organisation
- Position within the organisation

You may also be asked to provide information about specific project memberships and your role within these projects.

10 Upgrading from a Previous Release

This section tells you how to upgrade a previously installed perfSONAR services version (using the repositories as described in *Getting Started* on page 3) using the standard tools from your distribution.

10.1 Upgrading on RedHat

10.1.1 Prerequisites

You must be using our stable repository for this upgrade to work smoothly. See *Installing Prerequisite Software Using Packages* on page 5 for information on how to configure yum to use the stable repository.

10.1.2 Full upgrade

If your distribution is up to date, the easiest way to upgrade your perfSONAR installation is to issue the following command:

```
yum upgrade
```

10.1.3 Upgrading selected packages

If you wish to upgrade only a selected set of packages (perhaps only the perfSONAR packages), you must use the following command:

```
yum upgrade <list of packages to upgrade>
```

Or more specifically for upgrading only the perfSONAR packages:

```
yum upgrade geant2-java-as  
yum upgrade geant2-java-rrd-ma  
yum upgrade geant2-java-sql-ma  
yum upgrade ps-mdm-java-sstelnets-mp  
yum upgrade geant2-java-xml-ls  
yum upgrade oppd  
yum upgrade oppd-mp-bwctl  
yum upgrade perl-NMWG
```

10.1.4 Troubleshooting the upgrade

If anything doesn't work as expected during the execution of the upgrade, remove the upgrade using `yum remove <list of packages to remove>` and then reinstall it.

10.2 Upgrading on Debian

10.2.1 Prerequisites

You must be using our stable repository for this upgrade to work smoothly. See *Installing Prerequisite Software Using Packages* on page 5 for information on how to configure yum to use the stable repository.

10.2.2 Full upgrade

If your distribution is up to date, the easiest way to upgrade your perfSONAR installation is to issue the following commands:

```
apt-get update
apt-get dist-upgrade
```

10.2.3 Upgrading selected packages

If you wish to upgrade only a selected set of packages (perhaps only the perfSONAR packages), you must use the following commands:

```
apt-get update
apt-get install <list of packages you want to upgrade>
```

Or more specifically for upgrading only the perfSONAR packages:

```
apt-get install perfsonar-java-as
apt-get install perfsonar-java-rrd-ma
apt-get install perfsonar-java-sql-ma
apt-get install perfsonar-java-ssh-telnet-mp
apt-get install perfsonar-java-xml-ls
apt-get install perfsonar-oppd
apt-get install perfsonar-oppd-mp-bwctl
apt-get install perl-NMVG
```

10.2.4 Troubleshooting the upgrade

If anything doesn't work as expected during the execution of the upgrade, remove the upgrade using `apt-get remove <list of packages to remove>` and then reinstall it.

Glossary

AS	Authentication Service
BWCTL	Bandwidth Test Controller, a tool for establishing bandwidth; currently a wrapper around Iperf.
CL	Command Line
GIdP	GÉANT Identity Provider
gLS	global Lookup Service
hLS	home Lookup Service
IdP	Identity Provider
LHCOPN	Large Hadron Collider Optical Private Network
LS	Lookup Service
MA	Measurement Archive
MP	Measurement Point
NREN	National Research and Education Network
OS	Operating System
OWAMP	One-Way Active Monitoring Protocol
perfSONAR	Performance focused Service Oriented Network monitoring Architecture
REN	Research Exchange Network
UA	User Administrator

Index

A

- Authentication
 - GIdP, 19, 88
- Authentication Service, 1, 19
 - Configuration, 22
 - Installing, 20
 - Testing Deployment, 26
 - Testing the Installation, 22

B

- BWCTL MP, 1, 62
 - Configuration, 68
 - Installing, 63
 - Integrating with your system, 71
 - Testing Deployment, 71
 - Testing the Installation, 67

C

- Configuration
 - Authentication Service, 22
 - BWCTL MP, 68
 - Looukup Service, 13
 - RRD MA, 34
 - SQL MA, 50
 - SSH/Telnet MP, 77

G

- GIdP, 19, 88
 - Getting a GIdP account, 89
- gLS, 9

H

- hLS, 9

I

- iBATIS files, 58
- Installing
 - Authentication Service, 20
 - BWCTL MP, 63
 - Lookup Service, 10
 - Prerequisite software, 4
 - RRD MA, 30
 - SQL MA, 46
 - Telnet/SSH MP, 74

L

- Lookup Service, 1, 8
 - gLS, 9
 - hLS, 9
 - Installing, 10
- Looukup Service
 - Configuration, 13
 - Testing Deployment, 17
 - Testing the Installation, 12

P

- perfSONAR, 1
 - Functionality, 3
 - Prerequisite software, 4
- Prerequisite software, 4

R

- RRD MA, 1, 29
 - Best Practice, 43
 - Configuration, 34
 - Installing, 30
 - Testing Deployment, 41

Testing the Installation, 33

S

SQL MA, 1, 45

Configuration, 50

iBATIS files, 58

Installing, 46

Metadata, 57

Stitching, 57

Testing Deployment, 55

Testing the Installation, 49

SSH/Telnet Mp

Configuration, 77

SSH/Telnet MP, 2

Supported

Browsers, 4

Platforms, 4

T

Telnet/SSH MP, 73

Installing, 74

Reverse Proxy Security, 85

Testing Deployment, 84

Testing the Installation, 77

Testing

Authentication Service Deployment, 26

Authentication Service Installation, 22

BWCTL MP Deployment, 71

BWCTL MP Installation, 67

Lookup Service Installation, 12

Lookup Service Deployment, 17

RRD MA Deployment, 41

RRD MA Installation, 33

SQL MA Deployment, 55

SQL MA Installation, 49

Telnet/SSH MP Deployment, 84

Telnet/SSH MP Installation, 77

Tomcat

Starting and Stopping, 7

U

Upgrade

Debian, 91

RedHat, 90