



# SANTA-G TEST REPORT

## SOFTWARE TEST AND VALIDATION REPORT

### WP4 TASK4 - Verification and Quality Control

---

Document Filename:	<b>CG-4.4-REP-v1.0-CYFRONET002-SANTA-G_TestReport.doc</b>
Work package:	<b>WP4 TASK4 - Verification and Quality Control</b>
Partner(s):	<b>CYFRONET</b>
Lead Partner:	<b>LIP</b>
Config ID:	<b>CG-4.4-REP-v1.0-CYFRONET002-SANTA-G</b>
Document classification:	<b>PUBLIC</b>

---

**Abstract:** This report describes the validation performed on the package SANTA-G developed by CrossGrid WP 3 task 3.3.2. The tests were performed by Patryk Lason on the behalf of the CrossGrid task 4.4 testbed verification and quality control.



### Delivery Slip

	Name	Partner	Date	Signature
<b>From</b>				
<b>Verified by</b>				
<b>Approved by</b>				

### Document Log

Version	Date	Summary of changes	Author
1-0-DRAFT-A	13/08/2004	Draft version	Patryk Lason
1-0-DRAFT-B	16/08/2004	Final version	Patryk Lason

---

## CONTENTS

<b>1.CONTEXT.....</b>	<b>4</b>
1.1.TEST REQUEST .....	4
1.2.TEST TEAM.....	4
1.3.RESOURCE INVOLVED.....	4
<b>2.TEST AND VALIDATION .....</b>	<b>5</b>
2.1.SOFTWARE INSTALLATION.....	5
2.1.1.LCFG INSTALLATION .....	5
2.2.SOFTWARE INSTALLATION.....	6
2.3.ADDITIONAL TESTBED MODIFICATIONS .....	7
2.4.TEST DEVELOPMENTS .....	7
2.5.USABILITY .....	7
2.6.FUNCTIONALITY .....	7
2.6.1.Unit tests .....	8
2.6.2.System tests.....	8
2.6.3.Stress tests.....	8
2.7.COMPATIBILITY.....	8
2.8.SECURITY AND NETWORKING.....	8
2.9.PREVIOUSLY REPORTED ISSUES .....	9
<b>3.ISSUES FOUND .....</b>	<b>10</b>
3.1.ISSUES FOUND IN THE SOFTWARE .....	10
3.1.1.Issue 001, bugtracker #522 .....	10
3.1.2.Issue 002, bugtracker #523 .....	10
3.1.3.Issue 003, bugtracker #524 .....	10
3.1.4.Issue 004, bugtracker #525 .....	10
3.1.5.Issue 005, bugtracker #526 .....	10
3.1.6.Issue 006, bugtracker #527 .....	10
3.2.ISSUES FOUND IN THE DOCUMENTATION.....	10
3.2.1.Issue 001, bugtracker #528.....	10
<b>4.RECOMMENDATION .....</b>	<b>11</b>
<b>5.REFERENCES .....</b>	<b>12</b>
<b>6.INTEGRATION/VALIDATION REQUEST .....</b>	<b>13</b>

## 1. CONTEXT

Test and validation of the package SANTA-G developed by CrossGrid WP 3 task 3.3.2.

### 1.1. TEST REQUEST

A properly formatted request test form was placed on the web site. Test request was sent by Jorge Gomes. All required manuals are provided in a RPM package. Unit tests are provided in an archive.

The test requester was Stuart Kenny (stuart.kenny@cs.tcd.ie) from TCD and CrossGrid WP3 task 3.3.2. The test was authorized by Jorge Gomes (jorge@lip.pt) from the WP4 integration team.

### 1.2. TEST TEAM

The tests were performed by task 4.4 member from CYFRONET

- Patryk Lason (p.lason@cyf-kr.edu.pl)

### 1.3. RESOURCES INVOLVED

The tests involved an **R-GMA server** system installed on a Computing Element (zeus24.cyf-kr.edu.pl), a Storage Element (zeus25.cyf-kr.edu.pl) hosting a **SANTA-G QueryEngine**, and two Worker Nodes (zeus05.cyf-kr.edu.pl – hosting a **SANTA-G Sensor**; zeus30.cyf-kr.edu.pl – hosting a **SANTA-G Viewer**).

## 2. TEST AND VALIDATION

### 2.1. SOFTWARE INSTALLATION

The SANTA-G packages were provided in RPM format, the version was 1.3.4. As required in the test request, the operating system used was RedHat 7.3. The EDG middleware was 2.0.0. According to the SANTA-G test request an R-GMA software was installed, namely 3.4.31 (the R-GMA software was not included in current release and not installed on the testbed).

The tcpdump package was downloaded in RPM format from:

[http://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3\\_3-moninfr/](http://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3_3-moninfr/)

The snort package was downloaded in RPM format from:

<http://www.snort.org/dl/binaries/linux/old/snort-2.1.1-1.i386.rpm>

This is the last version, which depends on the GLIBC v2.2.

The ant package was downloaded in RPM format from:

<http://datagrid.in2p3.fr/distribution/external/RPMS/ant-1.5-5jpp.noarch.rpm>

The SANTA-G installation depends on the R-GMA installation, which was installed on the zeus24.cyf-kr.edu.pl node.

#### 2.1.1. LCFG INSTALLATION

An LCFGng server was used for the installation of the RPM's. The following RPM lists were created:

**santag-server-rpm:**

- cg-wp3.3.2-santag-common-1.3.4-1
- cg-wp3.3.2-santag-queryengine-1.3.4-1
- cg-wp3.3.2-santag-doc-1.3.4-1
- cg-wp3.3.2-santag-examples-1.3.4-1

**santag-client-rpm:**

- cg-wp3.3.2-santag-common-1.3.4-1
- cg-wp3.3.2-santag-sensor-1.3.4-1
- cg-wp3.3.2-santag-viewer-1.3.4-1
- cg-wp3.3.2-santag-examples-1.3.4-1
- tcpdump-3.7.2-0
- snort-\*-\*

The “santag-server-rpm” file was included in the zeus25.cyf.kr.edu.pl list and the “santag-client-rpm” file was included in worker nodes lists.

The software was properly installed and no dependency problems were detected.

Unit tests were installed on the zeus25.cyf-kr.edu.pl.

The software installs under /opt/cg as required by the Crossgrid guidelines. Other installation procedures seem to be compliant with these guidelines.

## 2.2. SOFTWARE INSTALLATION

The configuration has to be done manually after the installation. The node zeus24cyf-kr.edu.pl had R-GMA already configured and running. MySQL and tomcat4 were also running. That node was chosen to be R-GMA server. The SANTA-G components are configured by “santag-config” script.

### QueryEngine

Here is a configuration of the QueryEngine:

```
[root@zeus25 root]# /opt/cg/sbin/santag-config

----- SANTA-G Setup Script -----

Please report any problems to Stuart Kenny at stuart.kenny@cs.tcd.ie

What are you configuring, [q]queryEngine, [s]ensor, [v]iewer or [a]ll [a]: q
SANTA-G Location [/opt/cg]:
R-GMA props file location [/opt/edg/var/edg-rgma]:
Please enter the ID of the site on which the QueryEngine is being run [csTCDie]:
Cyfronet
Please enter the port number on which the QueryEngine should listen [8998]:
Please enter the mount point on which the QueryEngine should mount remote Sensor
directories [/mnt/santag]:
Turn on QueryEngine logging (y/n) [y]:
Where should the logfiles be stored [/opt/cg/var/log/santag]:
```

Similar configuration was performed for the zeus05.cyf-kr.edu.pl node, which was chosen to host a SANTA-G Sensor and for the zeus30.cyf-kr.edu.pl, where a SANTA-G Viewer runs.

### Sensor

Here is a configuration of the Sensor:

```
[root@zeus05 root]# /opt/cg/sbin/santag-config

----- SANTA-G Setup Script -----

Please report any problems to Stuart Kenny at stuart.kenny@cs.tcd.ie

What are you configuring, [q]queryEngine, [s]ensor, [v]iewer or [a]ll [a]: s
SANTA-G Location [/opt/cg]:
Please enter the fully qualified domain name of the QueryEngine host [localhost]:
zeus25.cyf-kr.edu.pl
Please enter the port number on which the QueryEngine is listening [8998]:
Enter type of sensor to start (s)tatic, (d)ynamic, (sn)ort [d]: d
Enter the path to the directory which will store the TCPdump logfiles
[/opt/cg/var/log/santag-tcpdump]:
*** WARNING /opt/cg/var/log/santag-tcpdump is not a directory ***
Would you like to create it now (y/n) [y]:
How many log files should the Sensor store in a queue [5]:
When the max queue size is reached should the Sensor delete the oldest file (y/n
) [y]:
Enter the maximum size for files in the queue (Mb) [3]:
Please enter the TCPdump args you would like to use [-a tcp or udp or icmp]:
```

## Snort

The snort can be run in two modes supported by the SANTA-G: FAST and FULL. FAST writes alerts to the default "alert" file in a single-line, syslog style alert message. FULL writes the alert to the "alert" file with the full decoded header.

These modes are set in the `/etc/sysconfig/snort` file.

## STARTUP FILES

The distribution provides scripts to start the Query Engine, the Sensor and the Viewer on the chosen nodes:

```
/opt/cg/etc/init.d/cg-santag-queryengine  
/opt/cg/etc/init.d/cg-santag-sensor  
/opt/cg/bin/startupViewer
```

No configuration was needed to prepare unit tests. All steps needed to run tests were clearly described in the "README" file included in the tests archive.

## 2.3. ADDITIONAL TESTBED MODIFICATIONS

An R-GMA software was installed (v3.4.31).

## 2.4. TEST DEVELOPMENTS

No software was developed by the test team to test and validate the software.

## 2.5. USABILITY

The SANTA-G software deployment depends critically on the correct deployment and configuration of the R-GMA software distributed by EDG.

The SANTA-G is easy to deploy but not easy to understand and use. The user interface produces correct output and the interactive response time is acceptable.

The SANTA-G depends also on the NFS software.

## 2.6. FUNCTIONALITY

There are three modes in which the Sensor can be configured: DYNAMIC, STATIC and SNORT.

In the DYNAMIC mode Sensor captures live network packets using TCPdump and writes them to a tracefile. Number of tracefiles and their size are configured with the "santag-config" script.

In the STATIC mode the Sensor provides information from existing tracefiles. After capturing network packets with the DYNAMIC Sensor one can analyze them with the STATIC Sensor.

One small difficulty are the filenames. They contain a timestamp and file number, and it's hard to give a proper basename during the configuration.

The SNORT mode makes possible for a user to analyze alerts file available from the snort process.

Unfortunately one need to log on the machine as root to change the Sensor type. It's impossible to do that using the Viewer.

### 2.6.1. Unit tests

The tests performed consisted of the following:

- Correct startup of the QueryEngine daemon
- Correct startup of the Sensor in all modes
- Correct pass of the tests delivered by the SANTA-G developers

#### QueryEngine

The QueryEngine daemon was started successfully.

#### Sensor

The Sensor was started successfully in all modes.

The NFS daemon must be running on each node hosting the Sensor.

#### Tests provided by developer

All tests were run correctly.

### 2.6.2. System tests

The “system tests” consisted in executing the Viewer, opening and inspecting/querying the tracefiles through the Query Engine using Sensors running on the one or more nodes.

No errors occurred.

### 2.6.3. Stress tests

No “stress tests” were performed.

## 2.7. COMPATIBILITY

The software is compliant with the other components of the distribution.

The software is compatible with EDG 2.0 middleware.

## 2.8. SECURITY AND NETWORKING

The execution of the Sensors requires root access to the systems where the sensors are to be executed. The TCP port used for communication between the Query Engine and the Sensor and Viewer has a default value of 8998. However, the port number can be set to any other value by the SANTA-G configuration script.

The tracefiles are available from the QueryEngine through NFS, so on the each node hosting the Sensor a NFS daemon must be running.

There are no authentication/authorization methods provided to prevent an intruder from accessing the information from Sensors.

## 2.9. PREVIOUSLY REPORTED ISSUES

**According to software issue 001:**

Does not occur.

**According to software issue 002:**

Does not occur.

**According to software issue 003:**

Does not occur.

**According to software issue 004:**

Does not occur.

**According to software issue 005:**

Does not occur.

**According to software issues 006 and 007:**

Not tested.

**According to software issue 008:**

Does not occur.

**According to software issue 009:**

Does not occur.

**According to software issue 010:**

Not solved (severity and priority: low).

**According to software issue 011:**

Does not occur.

**According to software issue 012:**

Does not occur.

**According to documentation issue 001:**

Does not occur.

### 3. ISSUES FOUND

#### 3.1. ISSUES FOUND IN THE SOFTWARE

##### 3.1.1. Issue 001, bugtracker #522

(Severity: high, priority: high)

QueryEngine doesn't unmount logs from sensors after shutting down the QueryEngine.

##### 3.1.2. Issue 002, bugtracker #523

(Severity: high, priority: high)

After restarting the QueryEngine one has to restart all Sensors. There ought to be kind of internal communication between Sensors and QueryEngine, to avoid that situation.

##### 3.1.3. Issue 003, bugtracker #524

(Severity: medium, priority: medium)

The Sensor's package should depend on the nfs-utils package.

Startup script should also check if the NFS daemon runs, and write appropriate message.

##### 3.1.4. Issue 004, bugtracker #525

(Severity: medium, priority: medium)

LCFG configuration objects not provided. Mentioned in documentation, but not provided.

##### 3.1.5. Issue 005, bugtracker #526

(Severity: medium, priority: medium)

The STATIC Sensor configuration is misleading - providing a proper filename results appearing warning.

##### 3.1.6. Issue 006, bugtracker #527

(Severity: medium, priority: medium)

Filenames' timestamps are hard to recognize. There should be separation marks.

#### 3.2. ISSUES FOUND IN THE DOCUMENTATION

##### 3.2.1. Issue 001, bugtracker #528

(Severity: medium Priority: medium)

Documentation should be improved:

- Package dependencies
- R-GMA installation and configuration manuals should be provided
- Web links to packages should be provided (i.e. to the ant package)

#### 4. RECOMMENDATION

I suggest setting the 'MINOR ISSUES' flag to this version of the SANTA-G.

**I would recommend the deployment after closing major bugs, but all bugs should be closed.**

## 5. REFERENCES

- [1] [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/installation/installation.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/installation/installation.pdf)
- [2] [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/user/user.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/user/user.pdf)
- [3] [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/developer/developer.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/developer/developer.pdf)

---

## 6. INTEGRATION/VALIDATION REQUEST

**REQUEST ID: 108989255526.6454872516082**

**Component name:** SANTA-G

**Version (CVS tag):** v1\_3\_4                      **Request priority:** 2

**Package brief description:**

SANTA-G NetTracer that allows a user to analyse the ethernet network traffic on a site

**Code:**

**Source code in X# CVS ? (Y/N):** Y

**Autobuild generates RPMs ? (Y/N):** Y

**Software download URL:** <https://savannah.fzk.de/distribution/crossgrid/autobuilt/i386-rh7.3-gcc3.2.2/wp3/RPMS/>

**List of RPMs produced:**

cg-wp3.3.2-santag-common  
cg-wp3.3.2-santag-queryengine  
cg-wp3.3.2-santag-sensor  
cg-wp3.3.2-santag-viewer  
cg-wp3.3.2-santag-doc  
cg-wp3.2.2-santag-examples

**Changes:**

**List of all bugs fixed by this release:**

All documentation and software issues found in previous test request report, except for issues 006 and 007

**List of backwards compatibility issues (installation, configuration or run-time):**

None

**Documentation:**

**Installation manual URL:** [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/installation/installation.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/installation/installation.pdf)

**Users manual URL:** [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/user/user.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/user/user.pdf)

**Development manual URL:** [https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3\\_3\\_2-santag/userdoc/developer/developer.pdf](https://savannah.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/wp3_3_2-santag/userdoc/developer/developer.pdf)

**Software requirements URL:** <http://www.eu-crossgrid.org/Deliverables/M3pdf/Task3.3-SRS.pdf>

**Software design URL:** <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/deliverables/CG3.3.2-D3.2-v1.2-TCD020-SantaGDesign.pdf>

## Files:

### List of all configuration files (with full path):

/opt/cg/sbin/santag-config  
/opt/cg/etc/santag/QueryEngine.conf  
/opt/cg/etc/santag/Sensor.conf  
/opt/cg/etc/cg-santag.conf (config file for init.d scripts)

### List of all log files (with full path):

\$CG\_TMP/santag-queryengine.out  
\$CG\_TMP/santag-sensor.out  
/opt/cg/var/santag-sensors.info

### List of LCFG configuration objects (and versions):

/etc/obj/santag (v1.1)  
/usr/lib/lcfg/conf/santag/template  
/usr/lib/lcfg/defaults/server/santag-1.def

### List of daemons provided:

/opt/cg/etc/cg-santag-queryengine  
/opt/cg/etc/cg-santag-sensor

### List of init.d scripts and supported directives (start, stop, restart, etc.):

/opt/cg/etc/cg-santag-queryengine start, stop, restart, status  
/opt/cg/etc/cg-santag-sensor start, stop, status, restart, status

## Deployment:

### Affected machine types (UI, WN, CE, SE, etc) and packages to be deployed on each:

WN:  
cg-wp3.3.2-santag-common  
cg-wp3.3.2-santag-sensor

SE (suggested):

cg-wp3.3.2-santag-common  
cg-wp3.3.2-santag-queryengine

**Component dependencies (required libraries, packages, etc.):**

QueryEngine:  
edg-rgma-common  
edg-rgma-sqlutil  
edg-rgma-api-java  
Java

Sensor:  
Java  
Tcpdump >= 3.7.2

Viewer:  
edg-rgma-common  
edg-rgma-sqlutil  
edg-rgma-api-java  
Java

**Credentials (if any) used by the service:**

None

**List of service ports (inbound,outbound):**

Configurable

**Who communicates with the service and from where:**

The R-GMA server from the R-GMA host machine

**Range of temporary ports used by the service (inbound,outbound):**

QueryEngine outbound port 8080 to R-GMA Server, inbound from R-GMA server and sensors is configurable

**Testing and Validation:****Unit tests that have been performed on the package:**

Previous test requests and a set of JUnit test cases

**Features to be tested:**

Tests to see if previously reported issues have been solved.

**Features not to be tested:**

Functionality related to reported issues 006 and 007

**Test programs download** [https://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3\\_3-monifrcg-wp3.3.2-santag-test-1.3.4.tar.gz](https://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3_3-monifrcg-wp3.3.2-santag-test-1.3.4.tar.gz)

URL:

**Other considerations:**

It may not be possible to deploy in the whole testbed as the R-GMA dependencies are still missing from the LCG2 release

**Contacts:**

**Test requester:**

**Name:** Stuart Kenny

**WP:** 3 **Partner:** TCD

**Task:** 3.3 E-mail [Stuart.Kenny@cs.tcd.ie](mailto:Stuart.Kenny@cs.tcd.ie)

**Developer/origin:**

**Name:** Stuart Kenny

**Project:** crossgrid

**WP:** 3 **Partner:** TCD

**Task:** 3.3 E-mail: [Stuart.Kenny@cs.tcd.ie](mailto:Stuart.Kenny@cs.tcd.ie)

**6.1. DELETE THIS REQUEST:**

**Password:**

Delete

**6.1.1. Click the BACK browser button to return.**

**Credentials (if any) used by the service:**

None

**List of service ports (inbound,outbound):**

Configurable

**Who communicates with the service and from where:**

The R-GMA server from the R-GMA host machine

**Range of temporary ports used by the service (inbound,outbound):**

QueryEngine outbound port 8080 to R-GMA Server, inbound from R-GMA server and sensors is configurable

**Testing and Validation:**

**Unit tests that have been performed on the package:**

Previous test requests and a set of JUnit test cases

**Features to be tested:**

Tests to see if previously reported issues have been solved.

**Features not to be tested:**

Functionality related to reported issues 006 and 007

**Test programs  
download  
URL:**

[https://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3\\_3-monifr/cg-wp3.3.2-santag-test-1.3.4.tar.gz](https://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3_3-monifr/cg-wp3.3.2-santag-test-1.3.4.tar.gz)

**Other considerations:**

It may not be possible to deploy in the whole testbed as the R-GMA dependencies are still missing from the LCG2 release

**Contacts:**

**Test requester:**

**Name:** Stuart Kenny

**WP:** 3 **Partner:** TCD

**Task:** 3.3 **E-mail:** [Stuart.Kenny@cs.tcd.ie](mailto:Stuart.Kenny@cs.tcd.ie)

**Developer/origin:**

**Name:** Stuart Kenny

**Project:** crossgrid

**WP:** 3 **Partner:** TCD

**Task:** 3.3 **E-mail:** [Stuart.Kenny@cs.tcd.ie](mailto:Stuart.Kenny@cs.tcd.ie)