



SANTA-G TEST REPORT

SOFTWARE TEST AND VALIDATION REPORT

WP4 TASK4 - Verification and Quality Control

Document Filename: **CG-4.4-REP-v1.0-CYFRONET001-SANTA-G_TestReport.doc**

Work package: **WP4 TASK4 - Verification and Quality Control**

Partner(s): **CYFRONET**

Lead Partner: **LIP**

Config ID: **CG-4.4-REP-v1.0-CYFRONET001-SANTA-G_TestReport**

Document classification: **PUBLIC**

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 Lasoń on the behalf of the CrossGrid task 4.4 testbed verification and quality control.



Delivery Slip

	Name	Partner	Date	Signature
From				
Verified by				
Approved by				

Document Log

Version	Date	Summary of changes	Author
1-0-DRAFT-A	16/06/2004	Draft version	Patryk Lasoń
1-0-DRAFT-B	18/06/2004	Draft version	Patryk Lasoń
1-0-DRAFT-C	22/06/2004	Final version	Patryk Lasoń

CONTENTS

1. CONTEXT.....	4
1.1. TEST REQUEST	4
1.2. TEST TEAM.....	4
1.3. RESOURCES INVOLVED.....	4
2. TEST AND VALIDATION.....	5
2.1. SOFTWARE INSTALLATION.....	5
2.1.1. <i>MANUAL INSTALLATION</i>	5
2.1.2. <i>LCFG INSTALLATION</i>	5
2.2. SOFTWARE CONFIGURATION.....	6
2.3. ADDITIONAL TESTBED MODIFICATIONS	8
2.4. TEST DEVELOPMENTS	8
2.5. USABILITY.....	8
2.6. FUNCTIONALITY	8
2.6.1. <i>Unit tests</i>	8
2.6.2. <i>System tests</i>	10
2.6.3. <i>Stress tests</i>	10
2.7. COMPATIBILITY.....	10
2.8. SECURITY AND NETWORKING.....	10
2.9. PREVIOUSLY REPORTED ISSUES	10
3. ISSUES FOUND	13
3.1. ISSUES FOUND IN THE SOFTWARE	13
3.1.1. <i>Issue 001</i>	13
3.1.2. <i>Issue 002</i>	13
3.1.3. <i>Issue 003</i>	13
3.1.4. <i>Issue 004</i>	14
3.1.5. <i>Issue 005</i>	14
3.1.6. <i>Issue 006</i>	14
3.1.7. <i>Issue 007</i>	14
3.1.8. <i>Issue 008</i>	14
3.1.9. <i>Issue 009</i>	14
3.1.10. <i>Issue 010</i>	15
3.1.11. <i>Issue 011</i>	15
3.1.12. <i>Issue 012</i>	15
3.2. ISSUES FOUND IN THE DOCUMENTATION.....	15
3.2.1. <i>Issue 001</i>	15
4. RECOMMENDATION	16
5. EXEMPLARY INSTALLATION	17
5.1. R-GMA HOST.....	17
5.2. QUERYENGINE.....	18
5.3. SENSOR	20
5.4. VIEWER.....	21
6. REFERENCES	22
7. INTEGRATION/VALIDATION REQUEST	23

1. CONTEXT

Test and validation of the package SANTA-G v1.3.2 non-invasive network traffic monitoring tool 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:

“cg-wp3.3.2-santag-doc-1.3.2-1”.

Unit tests are provided in archive: “cg-wp3.3.2-santag-test-1.3.2.tar.gz”.

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 (zeus29.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 1.3.2. As required in the test request, the operating system used was RedHat 7.3. The EDG middleware was 2.0.0, but according to the SANTA-G test request a newer version of R-GMA was installed, namely 3.4.13 (version provided by EDG 2.0.0 is 3.2.22).

The tcpdump package was downloaded in RPM format from:

http://savannah.fzk.de/distribution/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 SANTA-G installation depends on the R-GMA installation (described in section 5), which was installed on the zeus24.cyf-kr.edu.pl node.

2.1.1. MANUAL INSTALLATION

First installation was manual. As described in SANTA-G Installation Guide in the “Example deployment” section, several packages were installed on the following nodes:

zeus25.cyf-kr.edu.pl (Storage Element) – SANTA-G QueryEngine

cg-wp3.3.2-santag-common-1.3.2-1

cg-wp3.3.2-santag-queryengine-1.3.2-1

zeus29.cyf-kr.edu.pl (Worker Node) – SANTA-G Sensor

cg-wp3.3.2-santag-common-1.3.2-1

cg-wp3.3.2-santag-sensor-1.3.2-1

snort-2.1.1-1

tcpdump-3.7.2-0

zeus30.cyf-kr.edu.pl (Worker Node) – SANTA-G Viewer

cg-wp3.3.2-santag-common-1.3.2-1

cg-wp3.3.2-santag-viewer-1.3.2-1

This type of installation is not suggested.

2.1.2. LCFG INSTALLATION

After manual installation the 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-1.3.2-1

cg-wp3.3.2-santag-queryengine-1.3.2-1

cg-wp3.3.2-santag-doc-1.3.2-1

cg-wp3.3.2-santag-examples-1.3.2-1

santag-client-rpm:

```
cg-wp3.3.2-santag-common-1.3.2-1
cg-wp3.3.2-santag-sensor-1.3.2-1
cg-wp3.3.2-santag-viewer-1.3.2-1
tcpdump-3.7.2-0
snort-2.1.1-1
```

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 CONFIGURATION

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]:
What is the maximum number of logfiles that should be rotated [5]:
Please enter the maximum size of each logfile (Mb) [5]:
```

Similar configuration was performed for the zeus29.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@zeus29 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]ueryEngine, [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
[/var/log/tcpdump]:
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]:

#####
# The configuration variables have been written to:
# /opt/cg/etc/santag/Sensor.conf
# The files can be edited by hand if required.
#####
```

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.

Issues related to the configuration and start of the daemons will be reported in section 3.

2.3. ADDITIONAL TESTBED MODIFICATIONS

A new version (v3.4.13) of the R-GMA was installed. The installation is described in the section 5.

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.

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, but it is necessary to change names of tracefiles. In the DYNAMIC mode tracefiles should be created with names supported by the Sensor after changing its mode to STATIC.

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 error detected in the QueryEngine daemon startup was related with absence of the “CanonicalProducer.props” file:

```
[root@zeus25 root]# /opt/cg/etc/init.d/cg-santag-queryengine start
Starting QueryEngine: [ OK ]
java.lang.NullPointerException
```

The file needed by the daemon was created with the following command:

```
echo "canonicalProducerServletLocation=http://zeus24.cyf-kr.edu.pl:8080/\
R-GMA/CanonicalProducerServlet" > /opt/edg/var/edg-rgma/CanonicalProducer.props
```

After this fix the QueryEngine daemon started successfully.

Sensor

The Sensor was started successfully in all modes.

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

There is one small difficulty. After capturing packets in DYNAMIC mode one must change the names of tracefiles to use them in STATIC mode. It will be more convenient if the DYNAMIC Sensor creates files with names which are automatically recognized by the STATIC Sensor.

Stopping the QueryEngine and the Sensors cause the script writes out [OK], but stopping not running daemon cause the same output which may be misleading. It should write [FAILED].

Unit tests provided by developers doesn't compile properly:

```
[root@zeus25 cg-wp3.3.2-santag-test] ant
PATH: /usr/share/java/xml-commons-apis.jar:/usr/share/java/jaxp_parser_impl.jar:/u
sr/share/java/ant-optional.jar:/usr/share/java/ant.jar:/usr/java/j2sdk1.4.1_01/lib
/tools.jar
Buildfile: build.xml

prepare:

compile:
[javac] Compiling 18 source files to /root/cg-wp3.3.2-santag-test/classes
[...]

BUILD FAILED
File:/root/cg-wp3.3.2-santag-test/build.xml:17: Compile failed; see the compiler
error output for details.
```

The solution is to set the path to the “junit.jar” file in the “/opt/edg/var/edg-rgma/rgma-defaults” file:

```
JUNIT JAR=/usr/share/java/junit.jar
```

After this fix 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:

TCPdump was downloaded from http://savannah.fzk.de/distribution/crossgrid/wp3/wp3_3-moninfr/ directory. No dependency errors occurred.

According to issue 002:

The configuration script still prompts probably non-appropriate place for log files i.e. /var/log/tcpdump as a place for tcpdump log files while in fact it should log output to somewhere under /opt/cg/ e.g. /opt/cg/var/log/santag-tcpdump or

/opt/cg/share/santag/exampleTrace as was recommended in the first version of T&V Report.

According to software issue 003 and 004:

Does not occur. Seems to be corrected.

According to issue 005:

Although the previous error does not occur this one is still applicable i.e. during the startup of the QueryEngine the error is returned but it writes out “[OK]”.

```
[root@zeus25 root]# /opt/cg/etc/init.d/cg-santag-queryengine start
Starting QueryEngine: [ OK ]
java.lang.NullPointerException
```

The second part of the issues related with the startup scripts was corrected by the developers:

```
[root@zeus25 root]# /opt/cg/etc/init.d/cg-santag-queryengine status
QueryEngine (29326) running..
```

```
[root@zeus29 santa-g]# /opt/cg/etc/init.d/cg-santag-sensor status
Owner: root Type: SNORT Time: Thu Jun 17 23:39:28 CEST 2004 PID: 27098
Sensor (27089) running..
```

According to software issue 006 and 007:

Does not occur.

According to software issue 008:

Does not occur.

Log files are created with file names which contain the fully qualified domain name of the host machine and a number which is increased with each new log file.

According to software issue 009:

Does not occur. File size is set by the “santag-config” script.

According to software issue 010:

Does not occur.

Packet types like ARP give an “Unsupported packet type” message but the viewer doesn’t hang.

According to software issue 011:

Does not occur.

The Viewer starts and gives error messages.

All documentation issues were corrected.

3. ISSUES FOUND

3.1. ISSUES FOUND IN THE SOFTWARE

3.1.1. Issue 001

(Severity: critical Priority: immediate)

The changes in the latest versions of R-GMA cause impossible to start the QueryEngine.

```
[root@zeus25 root]# /opt/cg/etc/init.d/cg-santag-queryengine start
Starting QueryEngine: [ OK ]
java.lang.NullPointerException
```

This issue was solved with the help of the test requester Stuart Kenny.

3.1.2. Issue 002

(Severity: critical Priority: immediate)

The QueryEngine daemon doesn't unmount NFS directories exported by the Sensors. These directories should also be removed on the QueryEngine side.

3.1.3. Issue 003

(Severity: critical Priority: immediate)

Compilation of the SANTA-G System and unit tests fails:

```
[root@zeus25 cg-wp3.3.2-santag-test] ant
PATH: /usr/share/java/xml-commons-apis.jar:/usr/share/java/jaxp_parser_impl.jar:/u
sr/share/java/ant-optional.jar:/usr/share/java/ant.jar:/usr/java/j2sdk1.4.1_01/lib
/tools.jar
Buildfile: build.xml

prepare:

compile:
[javac] Compiling 18 source files to /root/cg-wp3.3.2-santag-test/classes
[...]

BUILD FAILED
File:/root/cg-wp3.3.2-santag-test/build.xml:17: Compile failed; see the compiler
error output for details.
```

This issue was solved with the help of the test requester Stuart Kenny.

3.1.4. Issue 004

(Severity: high Priority: immediate)

The tracefiles should be created in directory in the /opt/cg/ tree i.e. /opt/cg/var/log/santag-tcpdump/.

This directory should also be a default location proposed by the “santag-config” script.

3.1.5. Issue 005

(Severity: high Priority: immediate)

The tracefiles should have the same names for DYNAMIC and STATIC modes.

In other case one must rename tracefiles created by the DYNAMIC Sensor to use them by the STATIC Sensor.

If it wasn't done the STATIC Sensor writes out the following message:

```
[root@zeus29 tcpdump]# /opt/cg/etc/init.d/cg-santag-sensor start
Starting Sensor: [ OK ]
Error starting sensor: Error starting Sensor:
Error, filename not correct format: name_count.ext
```

3.1.6. Issue 006

(Severity: critical Priority: immediate)

Direct file system access is needed to provide information from Sensors to the QueryEngine.

It might be a big security hole, if an intruder will find a bug in a Sensor and will be able to export a whole file system.

All data from tracefiles should be transferred through some kind of internal communication between Sensors and QueryEngine based possibly in Globus IO.

3.1.7. Issue 007

(Severity: critical Priority: immediate)

The user is not able to control the Sensor (starting, stopping, configuring) without logging – especially as root – on the requested machine.

The user should be able to do that through the Viewer after proper authentication and authorization.

3.1.8. Issue 008

(Severity: high Priority: immediate)

The cg-wp3.3.2-santag-sensor should be compiled with the dependency on the tcpdump 3.7 package.

3.1.9. Issue 009

(Severity: high Priority: immediate)

Stopping the daemon which is not running makes the script writes [OK]. It should write [FAILED].

3.1.10. Issue 010

(Severity: low Priority: low)

In the Viewer in the “Sensor Info” window should be one more column named i.e. “Sensor type” showing which types of the Sensors run.

3.1.11. Issue 011

(Severity: high Priority: high)

The Query Builder in the Viewer doesn’t allow to build a query containing the wildcard (*).

3.1.12. Issue 012

(Severity: low Priority: low)

The output of the daemon status should also contain the word “pid” before the number of the process i.e:

```
[root@zeus25 root]# /opt/cg/etc/init.d/cg-santag-queryengine status
QueryEngine (29326) running..
```

3.2. ISSUES FOUND IN THE DOCUMENTATION

3.2.1. Issue 001

(Severity: medium Priority: medium)

The third point from “Troubleshooting” section from the “SANTA-G User Guide” should be included in the “SANTA-G Installation Guide”.

4. RECOMMENDATION

According to already mentioned issues no recommendations are suggested.

5. EXEMPLARY INSTALLATION

This section provides exemplary installation of the SANTA-G.
RPM packages can be installed manually or using a LCFG server.
Unnecessary information was replaced by suspension points – [...].

5.1. R-GMA HOST

The Computing Element (zeus24.cyf-kr.edu.pl) node was chosen to be the R-GMA host.
We assume the tomcat4 is running.

Here are the steps needed to set up this installation:

1. Installing required RPM packages:

```
edg-rgma-common-3.4.13-1.noarch.rpm
edg-rgma-api-java-3.4.13-1.noarch.rpm
edg-rgma-servlets-3.4.13-1.noarch.rpm
MySQL-client-4.0.13-0.i386.rpm
MySQL-server-4.0.13-0.i386.rpm
```

2. Setting MySQL root password:

```
[root@zeus24 root]# /usr/bin/mysqladmin -u root password 'password'
[root@zeus24 root]# /usr/bin/mysqladmin -u root -h zeus24.cyf-kr.edu.pl password 'password'
```

3. Configuring the R-GMA:

```
[root@zeus24 root]# /opt/edg/sbin/edg-rgma-config
[...]
EDG Location directory? [/opt/edg]
[...]
Catalina (Tomcat V4) Home Directory? [/var/tomcat4]
Java Home Directory? [/usr/java/j2sdk1.4.1_01]
Do you want to use SSL connections? [n]
Which machine hosts the user servlets? [localhost] zeus24.cyf-kr.edu.pl
Which machine hosts the schema servlets? [localhost] zeus24.cyf-kr.edu.pl
Modify registry host or press "ENTER" to use current:? [zeus24.cyf-kr.edu.pl]
Enter additional Registry location or "ENTER" to finish:? []

PLEASE NOTE
=====
If you need to setup the database then run
    mysql -u root -p </opt/edg/var/edg-rgma/rgma-db-setup.sql
and enter the mysql root password when prompted

C
C
C
Configuration completed
```

4. Setting up the database:

```
mysql -u root -p </opt/edg/var/edg-rgma/rgma-db-setup.sql
```

5. Setting up the environment:

```
. /opt/edg/etc/profile.d/edg-rgma-env.sh
```

6. Checking the installation:

```
[root@zeus24 root]# /opt/edg/sbin/test/edg-rgma-check
```

This script had generated some errors, so some changes were made:

```
87,88c87,88
< icBox=`sed "s/^.*http:\\/\\/\\(.*)\\.*/\\1/" $RGMA_PROPS/Schema.props`
< monBox=`sed "s/^.*http:\\/\\/\\(.*)\\.*/\\1/" $RGMA_PROPS/StreamProducer.props`
---
> icBox=`sed "s/^.*http:\\/\\/\\(.*)\\.*/\\1/" $RGMA_PROPS/rgma.props`
> monBox=`sed "s/^.*http:\\/\\/\\(.*)\\.*/\\1/" $RGMA_PROPS/rgma.props`
105c105
< registry=`sed "s/^.*=\\(.*)\\/\\1/" $RGMA_PROPS/Registry.props`
---
> registry=`sed "s/^.*=\\(.*)\\/\\1/" $RGMA_PROPS/rgma.props`
124c124
< path=`sed "s/^.*=//" $RGMA_PROPS/$servlet.props`
---
> path=`grep $servlet $RGMA_PROPS/rgma.props | sed "s/^.*=//"`
```

These changes don't influence the R-GMA installation.

After the proper installation the R-GMA Browser is located here:

<http://zeus24.cyf-kr.edu.pl:8080/R-GMA/index.html>

5.2. QUERYENGINE

The QueryEngine was installed on the Storage Element (zeus25.cyf-kr.edu.pl) node.

Steps which were made:

1. Installing RPM packages:

```
edg-rgma-common-3.4.13-1.noarch.rpm
edg-rgma-api-java-3.4.13-1.noarch.rpm
edg-rgma-sqlutil-3.4.13-1.noarch.rpm
cg-wp3.3.2-santag-common-1.3.2-1.noarch.rpm
cg-wp3.3.2-santag-queryengine-1.3.2-1.noarch.rpm
```

2. Configuring the R-GMA:

```
[root@zeus25 root]# /opt/edg/sbin/edg-rgma-config
[...]
EDG Location directory? [/opt/edg]
[...]
Catalina (Tomcat V4) Home Directory? [/var/tomcat4]
Java Home Directory? [/usr/java/j2sdk1.4.1_01]
Do you want to use SSL connections? [n]
Which machine hosts the user servlets? [localhost] zeus24.cyf-kr.edu.pl
Which machine hosts the schema servlets? [localhost] zeus24.cyf-kr.edu.pl
Modify registry host or press "ENTER" to use current:? [zeus24.cyf-kr.edu.pl]
Enter additional Registry location or "ENTER" to finish:? []
[...]
Configuration completed
```

3. Configuring the QueryEngine:

```
[root@zeus25 root]# /opt/cg/sbin/santag-config
[...]
What are you configuring, [q]ueryEngine, [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]:
What is the maximum number of logfiles that should be rotated [5]:
Please enter the maximum size of each logfile (Mb) [5]:
[...]
```

4. Creating the "CanonicalProducer.props" file:

```
echo "canonicalProducerServletLocation=http://zeus24.cyf-kr.edu.pl:8080/R-GMA/CanonicalProducerServlet" > /opt/edg/var/edg-rgma/CanonicalProducer.props
```

5. Starting the QueryEngine:

```
/opt/cg/etc/init.d/cg-santag-queryengine start
Starting QueryEngine: [ OK ]
Schema path           =/opt/cg/etc/santag/Schema/db.schema
Reverse Schema path  =/opt/cg/etc/santag/Schema/db.rschema
```

5.3. SENSOR

The Sensor was installed on the Worker Node (zeus29.cyf-kr.edu.pl) node.

Steps which were made:

1. Installing required RPM packages:

```
cg-wp3.3.2-santag-common-1.3.2-1.noarch.rpm
cg-wp3.3.2-santag-sensor-1.3.2-1.noarch.rpm
tcpdump-3.7.2-0.i386.rpm
snort-2.1.1-1.i386.rpm
```

2. Configuring the Sensor:

```
[root@zeus29 root]# /opt/cg/sbin/santag-config
[...]
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]:
Enter the path to the directory which will store the TCPdump logfiles
[/var/log/tcpdump]:
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]:
[...]
```

3. Starting the Sensor:

```
/opt/cg/etc/init.d/cg-santag-sensor start
Starting Sensor: [ OK ]
tcpdump: listening on eth0

NetTracer Sensor running...
```

5.4. VIEWER

The Viewer was installed on the Worker Node (zeus30.cyf-kr.edu.pl) node.

Steps which were made:

1. Installing required RPM packages:

```
edg-rgma-common-3.4.13-1.noarch.rpm
edg-rgma-api-java-3.4.13-1.noarch.rpm
edg-rgma-sqlutil-3.4.13-1.noarch.rpm
cg-wp3.3.2-santag-viewer-1.3.2-1.noarch.rpm
```

2. Configuring the R-GMA:

```
[root@zeus30 root]# /opt/edg/sbin/edg-rgma-config
[...]
EDG Location directory? [/opt/edg]
[...]
Catalina (Tomcat V4) Home Directory? [/var/tomcat4]
Java Home Directory? [/usr/java/j2sdk1.4.1_01]
Do you want to use SSL connections? [n]
Which machine hosts the user servlets? [localhost] zeus24.cyf-kr.edu.pl
Which machine hosts the schema servlets? [localhost] zeus24.cyf-kr.edu.pl
Modify registry host or press "ENTER" to use current:? [zeus24.cyf-kr.edu.pl]
Enter additional Registry location or "ENTER" to finish:? []
[...]
Configuration completed
```

3. Starting the Viewer:

```
[root@zeus30 root]# /opt/cg/bin/startupViewer &
```

6. REFERENCES

- [1] <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/userdoc/installation.pdf>
- [2] <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/userdoc/user.pdf>
- [3] <http://savannah.fzk.de/websites/crossgrid/iteam/devguide/devguide-pdf/devguide-v2.1.1.pdf>

7. INTEGRATION/VALIDATION REQUEST

Request id: 108120865871.5592433539317

Component name: santag

Version (CVS tag): v1_3_2

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-gcc2.95.2/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.

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

Documentation:

Installation <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/userdoc/installation.pdf>

manual URL:

Users manual URL: <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/userdoc/user.pdf>

Development manual URL: <http://www.cs.tcd.ie/Stuart.Kenny/crossgrid/docs/santag/userdoc/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):

/tmp/santag-queryengine.out
/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:

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

(suggested)

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

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

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

(suggested)

Credentials (if any) used by the service:

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 request and a set of JUnit test cases.

Features to be tested:

All

Features not to be tested:

Test programs download URL: https://savannah.fzk.de/distribution/crossgrid/crossgrid/wp3/wp3_3-moninfr/cg-wp3.3.2-santag-test-1.3.2.tar.gz

Other considerations:

SANTA-G has previously been submitted for testing, version 1.1.2.

Contacts:

Test requester:

Name: Stuart Kenny

WP: 3 **Partner:** TCD

Task: 3.3.2 E-mail Stuart.Kenny@cs.tcd.ie

Developer/origin:

Name: Stuart Kenny

Project: crossgrid

WP: 3 **Partner:** TCD

Task: 3.3.2 E-mail: Stuart.Kenny@cs.tcd.ie