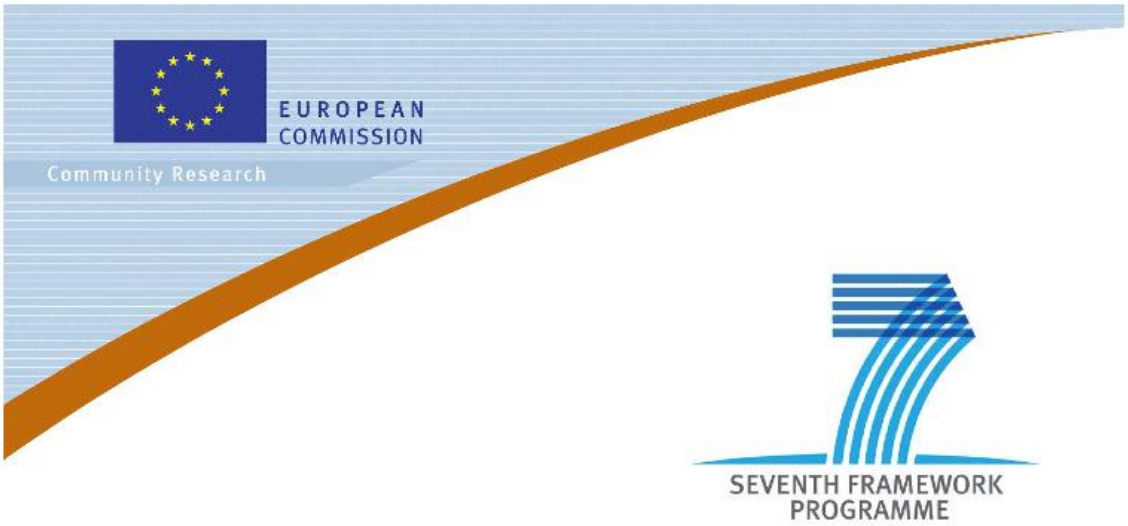


Private Public Partnership Project (PPP)
Large-scale Integrated Project (IP)

D.8.3.1b: FI-WARE Installation and Administration Guide

Project acronym: FI-WARE
Project full title: Future Internet Core Platform
Contract No.: 285248
Strategic Objective: FI.ICT-2011.1.7 Technology foundation: Future Internet Core Platform
Project Document Number: ICT-2011-FI-285248-WP8-D.8.3.1b
Project Document Date: 2012-11-12
Deliverable Type and Security: Public
Author: FI-WARE Consortium
Contributors: FI-WARE Consortium

1.1 Executive Summary

This document describes the installation and administration process of each Generic Enabler developed within in the "Security" chapter. The system requirements for the installation of a Generic Enabler are outlined with respect to necessary hardware, operating system and software. Each GE has a section dedicated to the software installation and configuration process as well as a section, which describes sanity check procedures for the system administrator to verify that the GE installation was successful.
This document consolidates new contents and also contents in previous issues of Release 1. The reason for re-delivering parts that were already issued is twofold:

- FI-WARE has made an effort to create a unified and improved format. The parts generated in the past are also provided in the new enhanced format for the sake of uniformity and readability.
- A single reference document per chapter is clearer and easier to handle that two incremental issues.

Reference to 1st private manual
The Identity Management One-IDM Generic Enabler GE will be offered as a service by the GE owner. Besides, the software release of the GE and the accompanying Installation and Administration guide are of PP dissemination level[1].
In accordance with the privacy restrictions requested by GE owner, both the software (binaries) and the Installation and Administration Guides were not reviewed by the FI-WARE coordinator or the Work Package leader and the responsibility for the quality and appropriateness of this part of the deliverables remain solely with the partner who is the GE owner.
The software (binaries) and the Installation and Administration Guides are accessible to the EC for reviewing purposes on a remote server located at 85.182.208.140 via ssh with user: EC and password to be disclaimed upon explicit request to the project coordinator. The partner who is the GE owner will govern this access.
Reference to 2nd private manual
The Identity Management GCP Generic Enabler GE will be offered as a service by the GE owner. Besides, the software release of the GE and the accompanying Installation and Administration guide are of PP dissemination level[1]
In accordance with the privacy restrictions requested by GE owner, both the software (binaries) and the Installation and Administration Guides were not reviewed by the FI-WARE coordinator or the Work Package leader and the responsibility for the quality and appropriateness of this part of the deliverables remain solely with the partner who is the GE owner.
The software (binaries) and the Installation and Administration Guides are accessible to the EC for reviewing purposes on a remote server hosted by DT and accessible via ssh with user: EC and password to be disclosed upon explicit request to the project coordinator. The partner who is the GE owner will ultimately provide this access.

1.2 About This Document

The "FI-WARE Installation and Administration Guide" comes along with the software implementation of components, each release of the document referring to the corresponding software release (as per D.x.2), to facilitate the users/adopters in the installation (if any) and administration of components (including configuration, if any).

1.3 Intended Audience

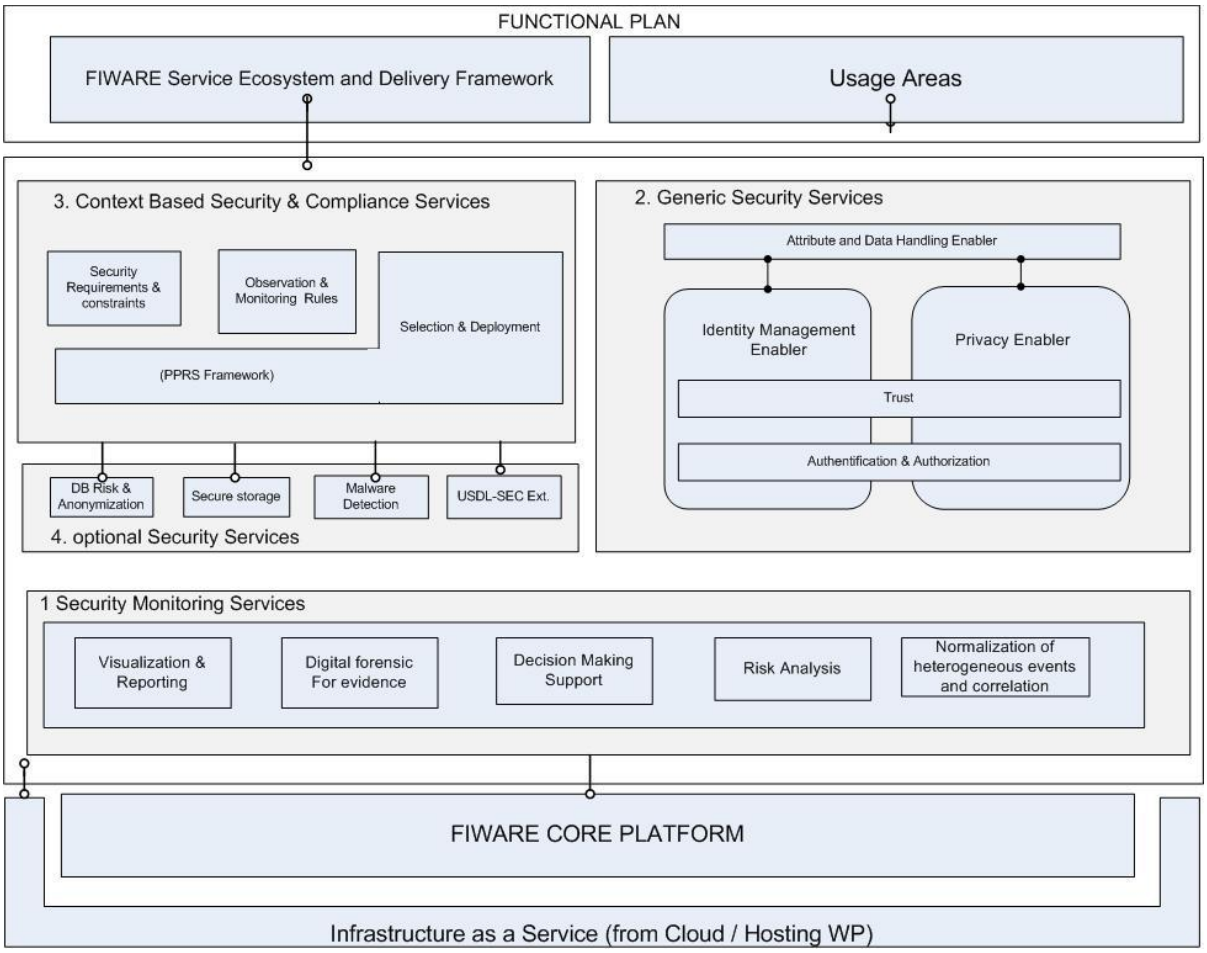
The document targets system administrators as well as system operation teams of FI-WARE Generic Enablers from the FI-WARE project.

1.4 Chapter Context

The overall ambition of the Security Architecture of FI-WARE is to demonstrate that the Vision of an Internet that is "secure by design" is becoming reality. Based on achievements to date and/or to come in the short-term (both from a technological but also a standardization perspective) we will show that "secure by design" is possible for the most important core (basic) and shared (generic) security functionalities as anticipated by the FI-WARE project and in accordance with the requirements of external stakeholders and users such as the FI PPP Use Case projects. The “secure by design” concept will, therefore, address both the security properties of the FI-WARE platform itself and the applications that will be built on top of it.
In this section the foreseen high-level functional architecture is described, introducing the main modules and their expected relationships, then depicting the most important modules in detail along with their main functionalities.
The high level architecture is formed by four main modules: Security monitoring mechanisms (M1), a set of General Core Security Mechanisms (e.g. Identity Management and Privacy solutions) (M2), Context-Based Security and Compliance (M3) where an enhanced version of USDL for security will support the matching of security goals with available security services while addressing compliance management, and a set of universally discoverable Optional Generic Security Services (M4) that will be instantiated at runtime and can be dynamically reconfigured (triggered by M3) based on the needs of specific scenarios.
The overall security plane of the FI-WARE architecture will interlink with practically all its functional modules. In order to simplify the description of these links subsequently the main components as well as their technical relationships with only the Application and Service Ecosystem and Delivery Framework and FI PPP Use Case projects are depicted:
The core general security mechanisms for the FI-WARE project will be provided by M2, including support for Identity Management, Authentication Authorization and Access, and Privacy. M3 will provide the required language and tools for describing services in the FI and their security needs. Where specific scenarios will require optional generic security services these can be consumed on a basis of what is provided by M4. A key architectural assumption is that security services may fail. Security monitoring mechanisms as provided by M1 may detect deviations with respect to the expected behaviour and signal this to M3 to take action (e.g. invoke alternative security services or trigger countermeasures if under attack).

FI-WARE GEs to be developed and/or integrated as part of the Security chapter will materialize the (Security) Reference Architecture sketched in Figure below. This Reference Architecture comprises:

- A component able to dynamically invoke and compose security services to answer related security needs while dealing with constraints which may apply (e.g. regulatory).
- A set of GEs for a number of shared security concerns (i.e. identity and access management as well as privacy and auditing) that are considered core and therefore present in any FI-WARE Instance.
- A set of optional Security GEs to address current and future requests from concrete Usage Areas.
- An advanced security monitoring system that covers the whole spectrum from acquisition of events up to display, going through analysis but also going beyond thanks to a digital forensic tool and assisted decision support in case of cyber attacks.



FI-WARE High Level Security Architecture

More information on the Security Chapter and FI-WARE in general can be found within the following pages:

http://wiki.fi-ware.eu
The Architecture of Security in FI-WARE
Materializing Security in FI-WARE

1.5 Structure of this Document

The document is generated out of a set of documents provided in the public FI-WARE wiki.
For the current version of the documents, please visit the public wiki at http://wiki.fi-ware.eu/
The following resources were used to generate this document:

D.8.3.1b FI-WARE Installation and Administration Guide front page
MulVal Attack Paths Engine - Installation and Administration Guide
Service Level SIEM - Installation and Administration Guide
Data Handling GE - Installation and Administration Guide
DB Anonymizer GE - Installation and Administration_Guide

1.6 Typographical Conventions

Starting with October 2012 the FI-WARE project improved the quality and streamlined the submission process for deliverables, generated out of the public and private FI-WARE wiki. The project is currently working on the migration of as many deliverables as possible towards the new system.
This document is rendered with semi-automatic scripts out of a MediaWiki system operated by the FI-WARE consortium.

1.6.1 Links within this document

The links within this document point towards the wiki where the content was rendered from. You can browse these links in order to find the "current" status of the particular content.
Due to technical reasons not all pages that are part of this document can be linked document-local within the final document. For example, if an open specification references and "links" an API specification within the page text, you will find this link firstly pointing to the wiki, although the same content is usually integrated within the same submission as well.

1.6.2 Figures

Figures are mainly inserted within the wiki as the following one:

```
[[Image:....|size|alignment|Caption]]
```

Only if the wiki-page uses this format, the related caption is applied on the printed document. As currently this format is not used consistently within the wiki, please understand that the rendered pages have different caption layouts and different caption formats in general. Due to technical reasons the caption can't be numbered automatically.

1.6.3 Sample software code

Sample API-calls may be inserted like the following one.

```
http://[SERVER_URL]?filter=name:Simth*&index=20&limit=10
```

1.7 Acknowledgements

The current document has been elaborated using a number of collaborative tools, with the participation of Working Package Leaders and Architects as well as those partners in their teams they have decided to involve.

1.8 Keyword list

FI-WARE, PPP, Architecture Board, Steering Board, Roadmap, Reference Architecture, Generic Enabler, Open Specifications, I2ND, Cloud, IoT, Data/Context Management, Applications/Services Ecosystem, Delivery Framework , Security, Developers Community and Tools , ICT, es.Internet, Latin American Platforms, Cloud Edge, Cloud Proxy.

1.9 Changes History

Release	Major changes description	Date	Editor
v1	First Version	2012-11-08	Thales
v2	Final Version	2012-11-12	Thales

1.10 Table of Contents

2 MulVal Attack Paths Engine - Installation and Administration Guide

You can find the content of this chapter as well in the wiki of fi-ware.

2.1 Introduction

Welcome the Installation and Administration Guide for the MulVAL-Attack-Paths Engine. The MulVAL-Attack-Paths Engine is part of the Security Monitoring Generic Enabler. The online documents are being continuously updated and improved, and will therefore be the most appropriate place to get the most up-to-date information on installation and administration.

2.2 System Installation

The Mulval Attack-Paths Engine is running on the CENTOS V5.
You can get the help from http://www.centos.org/docs/5/

The following steps need to be performed to get the Attack-Paths Engine up & running:
1. you need to install the XSB logic engine from http://xsb.sourceforge.net/.
2. You will also need to check whether GraphViz is already installed on your system by typing "dot".
3. If GraphViz is not installed, you need to install it at http://www.graphviz.org/
4. Make sure both the program "xsb" and "dot" reside in your PATH.
5. Basic Setup: The environmental variable MULVALROOT should point to this package's root folder Include $MULVALROOT/bin and $MULVALROOT/utils in PATH
6. You can run the MulVAL-Attack-Paths Engine directly, if you already have an input file: graph_gen.sh INPUT_FILE [OPTIONS]

2.3 System Administration

thank you to refer to the links http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/pdf/Virtual_Server_Administration/Red_Hat_Enterprise_Linux-5-Virtual_Server_Administration-en-US.pdf
This document provides information about installing, configuring, and managing Red Hat Virtual Linux Server (LVS) components.

2.4 Sanity Check Procedures

The Sanity Check Procedures are the steps that a System Administrator will take to verify that an installation is ready to be tested. This is therefore a preliminary set of tests to ensure that obvious or basic malfunctioning is fixed before proceeding to unit tests, integration tests and user validation.

2.4.1 End to End testing

You can run it to check whether the Attack Path Engine is working correctly with simple input file in testcases/nessus/nessus_report_apache_dos.nessus

./nessus_translate.sh ../testcases/nessus/nessus_report_fi-ware-1.nessus
./nessus_translate.sh ../testcases/nessus/nessus_report_apache_dos.nessus
./graph_gen.sh summ_oval.P -v -p

[root@wkslinux utils]# ./nessus_translate.sh
../testcases/nessus/nessus_report_apache_dos.nessus
NVD DB connection cannot be established
connection tested successfully
host name is: 172.17.5.51
CVE-2005-1794
port number is: 3389
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0519
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0520
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-2002-1117
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3192
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2003-1567
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2004-2320
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-0386
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3348
port number is: 80
protocol is: tcp[root@wkslinux utils]
./nessus_translate.sh ../testcases/nessus/nessus_report_apache_dos.nessus
NVD DB connection cannot be established
connection tested successfully
host name is: 172.17.5.51
CVE-2005-1794
port number is: 3389
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0519
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0520
port number is: 445
protocol is: tcp
host name is: 172.17.5.51
CVE-2002-1117
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3192
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2003-1567
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2004-2320
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-0386
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3348
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-0419
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3560
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3720
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-1623
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-1452
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-2068
port number is: 80 protocol is: tcp
host name is: 172.17.5.51 CVE-1999-0524

port number is: 0 protocol is: icmp

vulnerability(ies) detected
SQLException:Communications link failure

The last packet successfully received from the server was 1 337 070 930 429 milliseconds ago. The last packet sent successfully to the server was 0 milliseconds ago.
Output can be found in nessus.P.
Summarized vulnerability information can be found in summ_nessus.P and grps_nessus.P.
[root@wkslinux utils]#

host name is: 172.17.5.51
CVE-2011-0419
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3560
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3720
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-1623
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-1452
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-2068
port number is: 80[root@wkslinux utils]
./nessus_translate.sh ../testcases/nessus/nessus_report_apache_dos.nessus

NVD DB connection cannot be established
connection tested successfully
host name is: 172.17.5.51
CVE-2005-1794
port number is: 3389
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0519
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0520
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-2002-1117
port number is: 445
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3192
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2003-1567
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2004-2320
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-0386
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-3348
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2011-0419
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3560
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2009-3720
port number is: 80
protocol is: tcp

host name is: 172.17.5.51

CVE-2010-1623
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-1452
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-2010-2068
port number is: 80
protocol is: tcp

host name is: 172.17.5.51
CVE-1999-0524
port number is: 0
protocol is: icmp

vulnerability(ies) detected
SQLException:Communications link failure

The last packet successfully received from the server was 1 337 070 930 429 milliseconds ago. The last packet sent successfully to the server was 0 milliseconds ago.
Output can be found in nessus.P.
Summarized vulnerability information can be found in summ_nessus.P and grps_nessus.P.
[root@wkslinux utils]#

protocol is: tcp

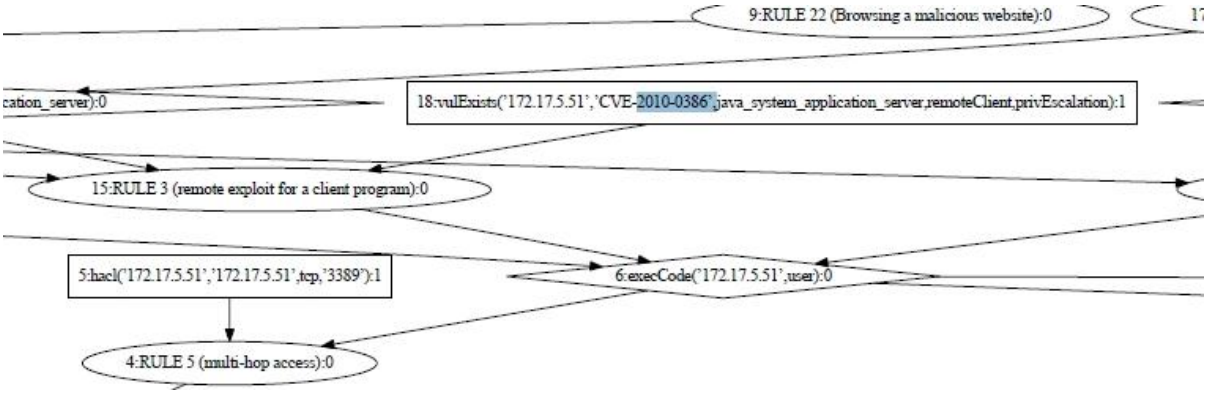
host name is: 172.17.5.51 CVE-1999-0524
port number is: 0
protocol is: icmp

vulnerability(ies) detected
SQLException:Communications link failure

The last packet successfully received from the server was 1 337 070 930 429 milliseconds ago.
The last packet sent successfully to the server was 0 milliseconds ago.
Output can be found in nessus.P.
Summarized vulnerability information can be found in summ_nessus.P and grps_nessus.P.
[root@wkslinux utils]#

A PDF file is generated after the computation of the attack paths .

Here's the screen capture.



2.4.2 List of Running Processes

- mysqld
- graph_gen.sh

2.4.3 Network interfaces Up & Open

```
[root@wkslinux utils]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:A2:00:07
          inet adr:172.17.5.46  Bcast:172.17.5.63  Masque:255.255.255.224
          adr inet6: fe80::250:56ff:fea2:7/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:726003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35796 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:62577070 (59.6 MiB)  TX bytes:5281653 (5.0 MiB)
          Interruption:59 Adresse de base:0x2024

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:HÃ´te
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:3731608 (3.5 MiB)  TX bytes:3731608 (3.5 MiB)
```

2.4.4 Databases

CVE database

2.5 Diagnosis Procedures

The Diagnosis Procedures are the first steps that a System Administrator will take to locate the source of an error in this part of the Security Monitoring GE. Once the nature of the error is identified with these tests, the system admin will very often have to resort to more concrete

and specific testing to pinpoint the exact point of error and a possible solution. Such specific testing is out of the scope of this section.

2.5.1 Resource availability

- RAM = 1 GB (minimum)
- HARD DISK = 20 GB (minimum)

2.5.2 Remote Service Access

- SSH

2.5.3 Resource consumption

- Memory consumption = 510 MB
- CPU Usage = 0,3%
- Thread runnning = N/A

2.5.4 I/O flows

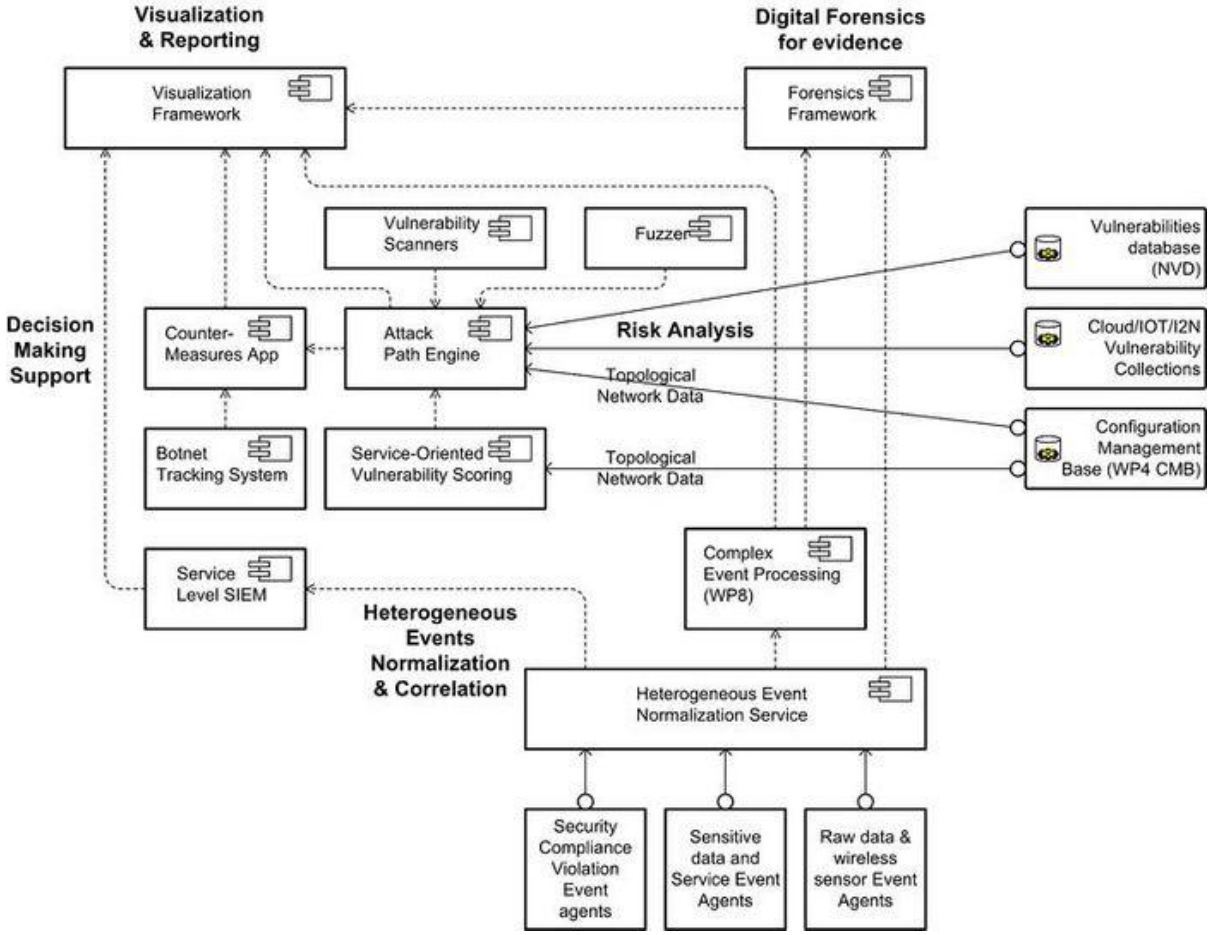
No I/O flows

3 Service Level SIEM - Installation and Administration Guide

You can find the content of this chapter as well in the wiki of fi-ware.

3.1 Service Level SIEM component introduction

The Service Level SIEM (SLS) provided for FI-WARE first release as service level SIEM component in the Security Monitoring GE is an Atos preconfigured version of the open source OSSIM SIEM.
This page describes the necessary steps to configure server & visualization framework OSSIM modules.
These OSSIM modules will be the core of the advanced Service Level SIEM (SLS) product (currently under development by Atos) for the Security Monitoring GE that is going to be delivered on future releases of FI-WARE.



Security Monitoring GE general architecture

Additional information about installation possibilities and OSSIM open source solution features can be found on official OSSIM - AlienVault Technical Documentation Web Page:
• http://communities.alienvault.com/community/documentation.html

3.2 Component Installation

OSSIM will be installed and configured in the FI-WARE Testbed VM accesible at IP: 130.206.81.165
However, the most important points from a clean installation are listed here:

3.2.1 Create a booteable DVD

OSSIM is distributed as a standalone Debian based Operative System.
You can download an burn the ISO from here: http://communities.alienvault.com/download-ossim

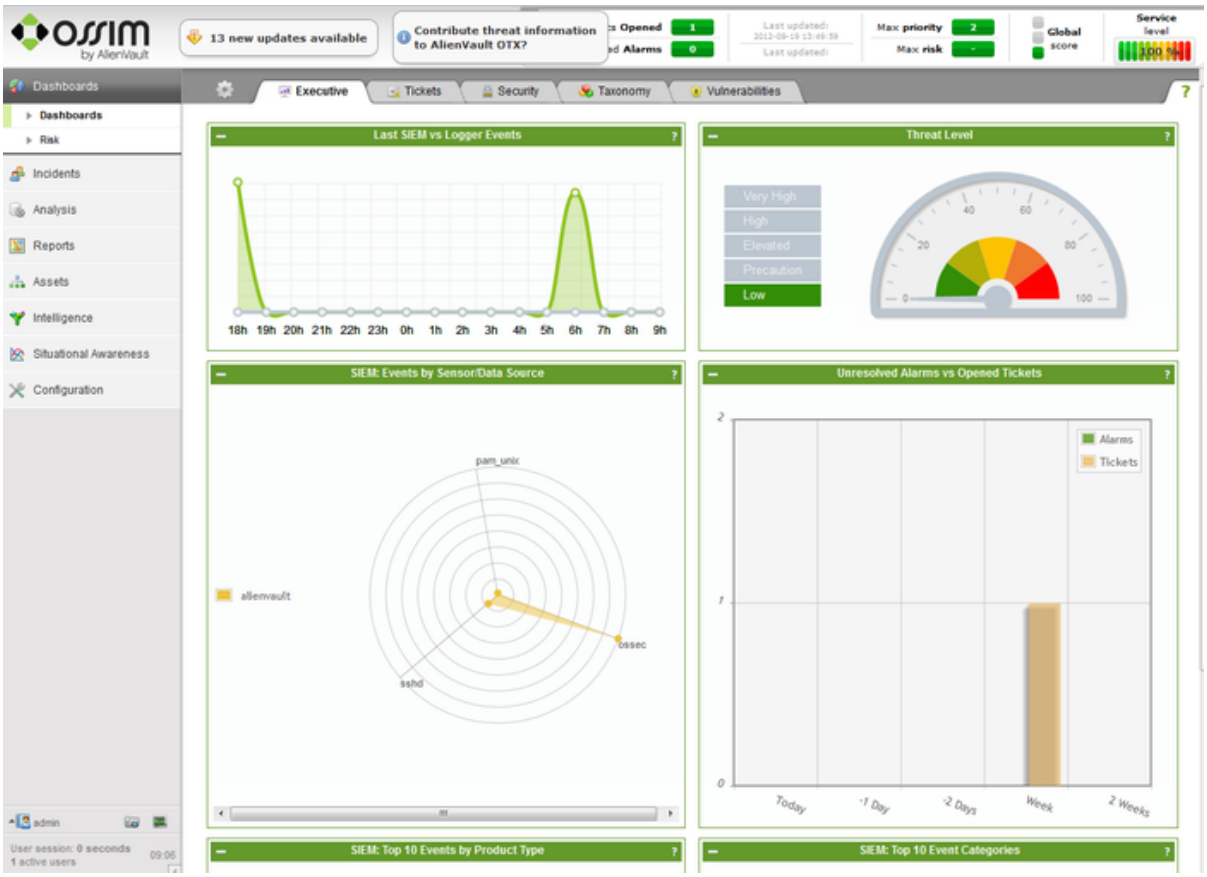
3.2.2 Install the OSSIM

Boot from the DVD to install the system. OSSIM requires a new partition in a physical or a virtual machine.
The wizard will require some parameters to configure the OSSIM (such as the IP, password, database, sensors available, etc).
These parameters can be changed at any time after the installation is completed, and also the wizard provides an automated installation that will configure the OSSIM with the default parameters with almost no user intervention.

The parameters are described in detail here: http://communities.alienvault.com/docs/Installation_Guide.pdf But an automated installation is enough for a beginner user, so you can safely go with this option.

3.2.3 OSSIM management interface

This is a web based interface accessible from the address https://ossimsiem.lab.fi-ware.eu/ossim/session/login.php Note that this interface is available only if the OSSIM was configured with the profile **Framework** in installation time (*the automated installation includes all the profiles by default*).



OSSIM management screeen

3.2.4 Fine tuning

The configuration parameters are stored in the file **/etc/ossim/ossim_setup.conf**, including the Database parameters/password.
If you want to change the server configuration, use the command:

```
# ossim-setup
```

This launches the Configuration Wizard

3.3 Component Installed

The demonstration version of the SIEM OSSIM based component that is part of the FI-WARE Monitoring GE is deployed under the following FI-WARE Testbed location:

- IP: *130.206.81.165*
- Port: *22*
- User: *root*
- Password: *<password>*

Users can update its keyboard and local layout (from default English – UK) by using the following OSSIM commands:

```
dpkg-reconfigure console-data
```

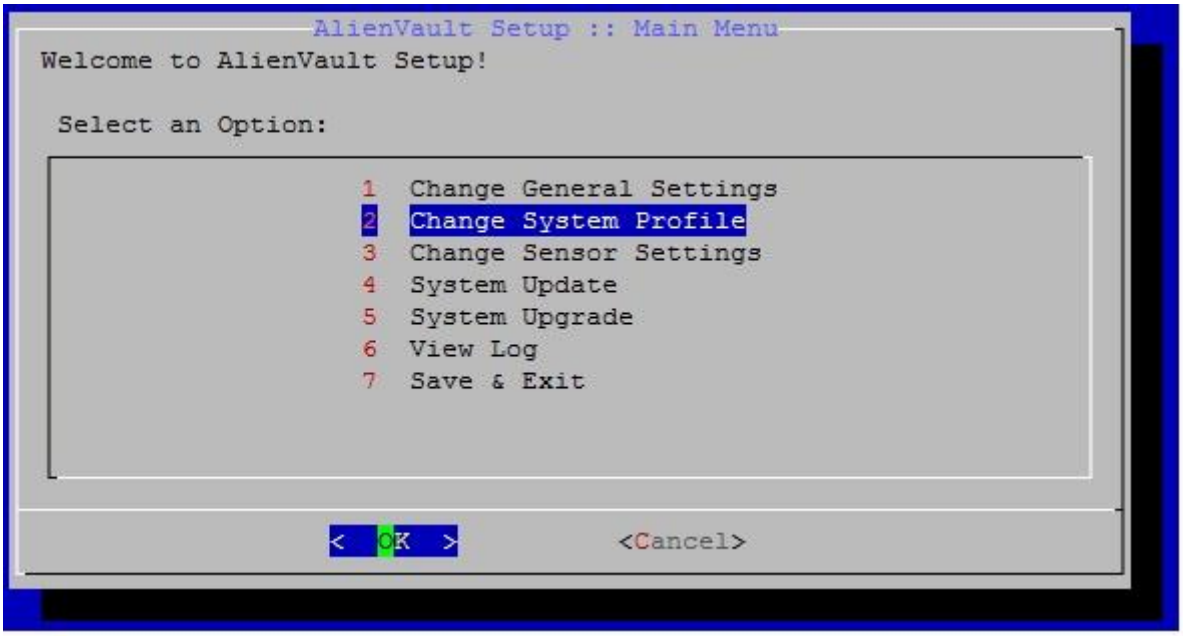
```
dpkg-reconfigure tzdata
```

3.3.1 Configuration

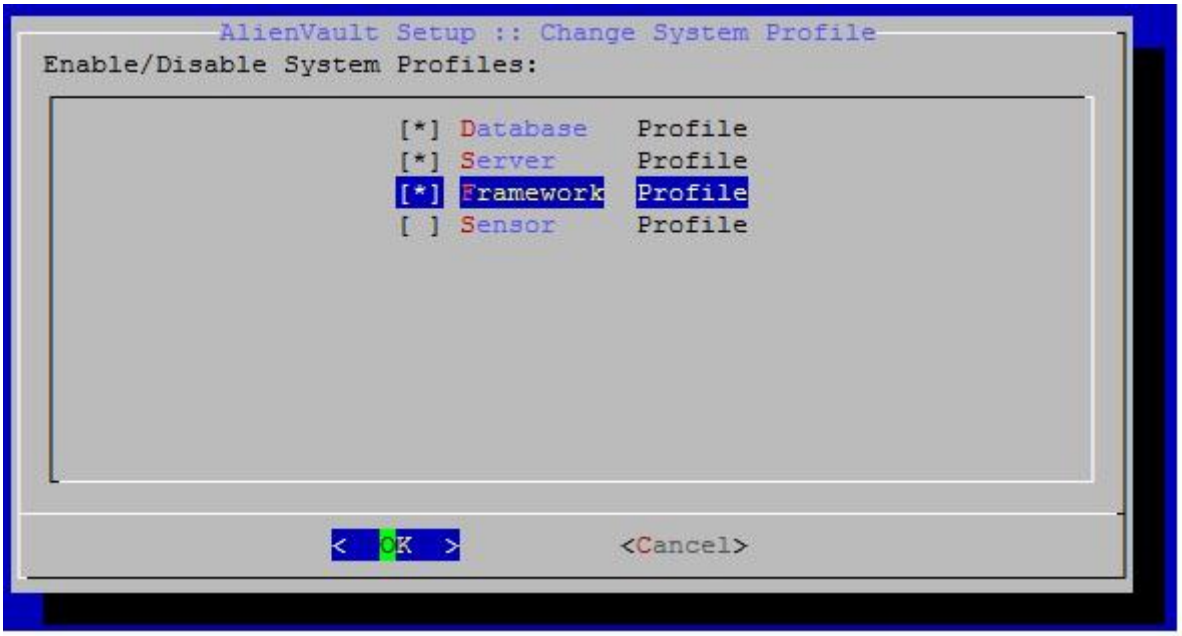
Both, server and visualization framework components and collector component can be configured by using the following OSSIM command:

```
# ossim-setup
```

- Under the Change System Profile settings option users are able to update server and local database configuration:

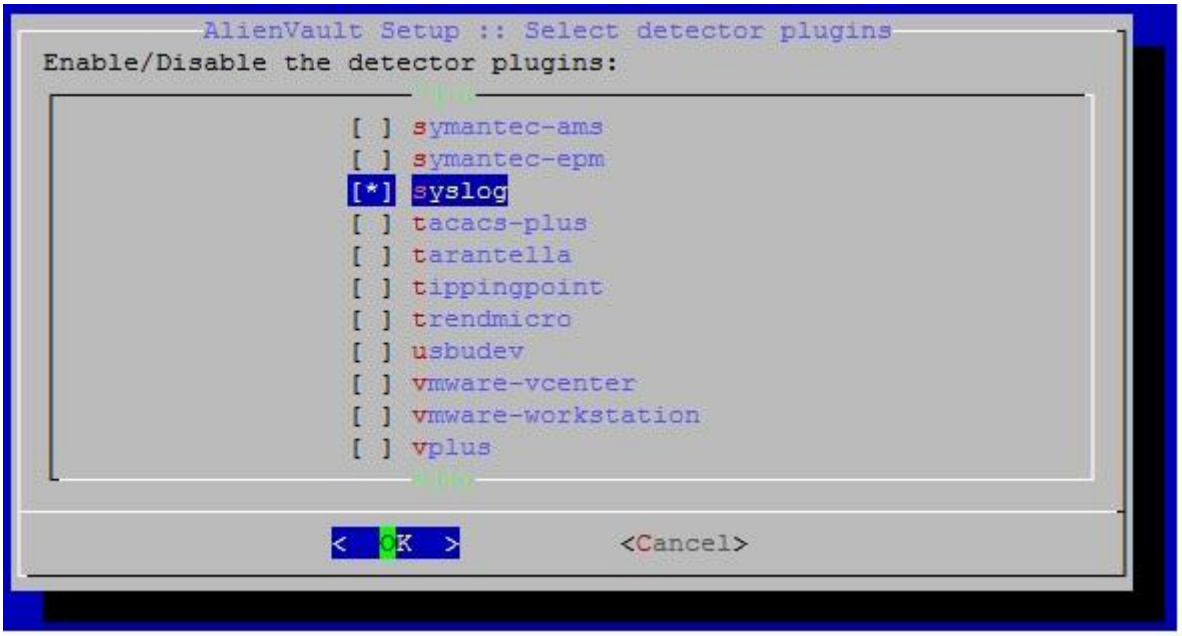


OSSIM Configuration screen



OSSIM Configuration screen

- By using Change Sensor Settings option users can enable or disable OSSIM detector & collector plug-ins. By default, only the OSSIM syslog & snare collector agent has been enabled in the component installed.



OSSIM Configuration screen

- Finally, the path where the log for OSSIM syslog & snare collector agent is being stored can be configured by editing the parameter location in the agent .cfg file under /etc/ossim/agent/plugins directory. If this is the case, the user should also restart the collector with the following command:

```
/etc/init.d/ossim-agent restart
```

3.3.1.1 *Configuration File*

The OSSIM configuration file (**/etc/ossim/ossim_setup.conf**) is separated in different sections, and each one is marked with a title in brackets, except for the first one, which has no title.
To mention the most relevant ones:

- **First section**:

Main configuration parameters, including the IP, hostname, mail server and profile of the OSSIM server.

- **[*database*]**

Database IP, port, db names, username, password.

- **[*framework*]**

Information regarding the framework IP/port.

- **[*sensor*]**

Active OSSIM sensors are listed here with the networks monitorized, network interfaces listening, etc.

- **[*server*]**

Active OSSIM plugins are listed here, which are in charge of translating detected events to OSSIM event format.

3.4 Sanity check procedures

The Sanity Check Procedures are the steps that a System Administrator will take to verify that an installation is ready to be tested. This is therefore a preliminary set of tests to ensure that obvious or basic malfunctioning is fixed before proceeding to unit tests, integration tests and user validation.
As the release 1.2 component version will be located at FI-WARE Testbed facilities, users only have to verify that the connection with Testbed V.M. is working properly.

- **Self diagnostic**

First, the user should check that the OSSIM server is functional and there are no potential problems, such as disk space depleted, CPU overload, or faulty internet connection.
Go to the Diagnostic Tool to check for these problems.

- **Position in the network**

Ideally, the OSSIM node should be placed in the gateway, firewall, or a place where it can sniff the packets that will go through the entire network or a subsection of the network. Otherwise it will only detect events from packets sent directly to it.

- **OSSIM in the same network**

Make sure that besides being connected, OSSIM has an IP address that belongs to the same network as the router/gateway/firewall.

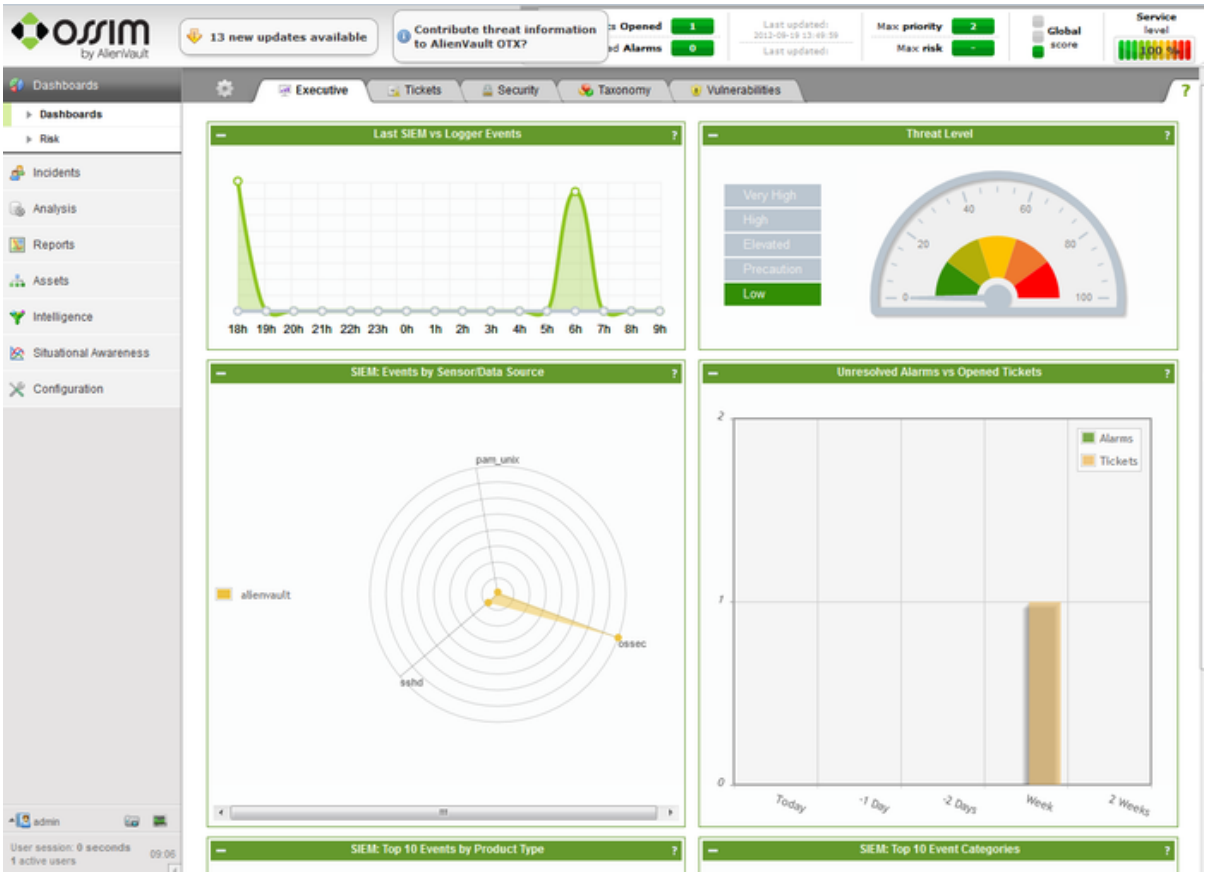
3.4.1 End to End testing

Users should validate the V.M. IP (130.206.81.165) is accessible for both SSH & HTTPS protocols:

- Under SSH protocol connection an standard Linux login screen is displayed
- Under HTTPS protocol connection the OSSIM Framework login page is displayed

OSSIM Framework login page

- Once login with the user and password provided for test (FI-test / siemtest) the main management OSSIM page will be displayed.



OSSIM management screen

In order to verify that basic installation has been performed without problems, go to the Diagnosis Procedures section.

3.4.2 List of Running Processes

There is a variety of required processes running in OSSIM.
Some of the most important ones are:

- OSSIM daemon **/usr/bin/ossim-server -d**
- MySQL Database **/usr/sbin/mysqld** (to store event data, alarms, tickets, etc)
- Python **/usr/bin/python -OOt /usr/bin/ossim-agent -d** (scripts for event translation/correlation)
- Apache **/usr/sbin/apache2 -k start** (for the administration interface)
- OpenVAS **/usr/sbin/openvasmd** (Vulnerability scanner)
- Pads **/usr/bin/pads_eth0** (Passive Asset Detection System: to detect other OSSIM nodes in the network)
- Arpwatch **/usr/sbin/arpwatch_eth0** (Ethernet/IP address pairing monitor)
- OSSEC (Host Intrusion Detection System)
    - **/var/ossec/bin/ossec-analysisd**
    - **/var/ossec/bin/ossec-logcollector**
    - **/var/ossec/bin/ossec-remoted**
    - **/var/ossec/bin/ossec-syscheckd**
    - **/var/ossec/bin/ossec-monitord**
- Osiris **/usr/sbin/osirisd /usr/sbin/osirismd** (Host integrity monitoring)
- Nagios **/usr/sbin/nagios3 -d /etc/nagios3/nagios.cfg** (Availability monitoring)

3.4.3 Network interfaces Up & Open

OSSIM listens the Ethernet card **eth0** for network event data.
The main administration interface is accessed from the standard SSL port **443** which can be accessed from here: *https://ossimsiem.lab.fi-ware.eu/ossim/index.php*

Additionally:

- OSSIM uses a MySQL database available in the port **3306**
- OSSIM can receive event data through the Syslog port **UDP/540**

Optionally, the **SSH** and **SFTP** are for comunication purposes, port **22**.

3.4.4 Databases

OSSIM uses a MySQL database which is created and configured from the ISO installation.
A password is created randomly at installation time and it is stored in the file:

```
/etc/ossim/ossim_setup.conf
```

Inside this file there is section for the DB configuration, including the IP, port, username and database names.

```
[database]
acl_db=ossim_acl
```

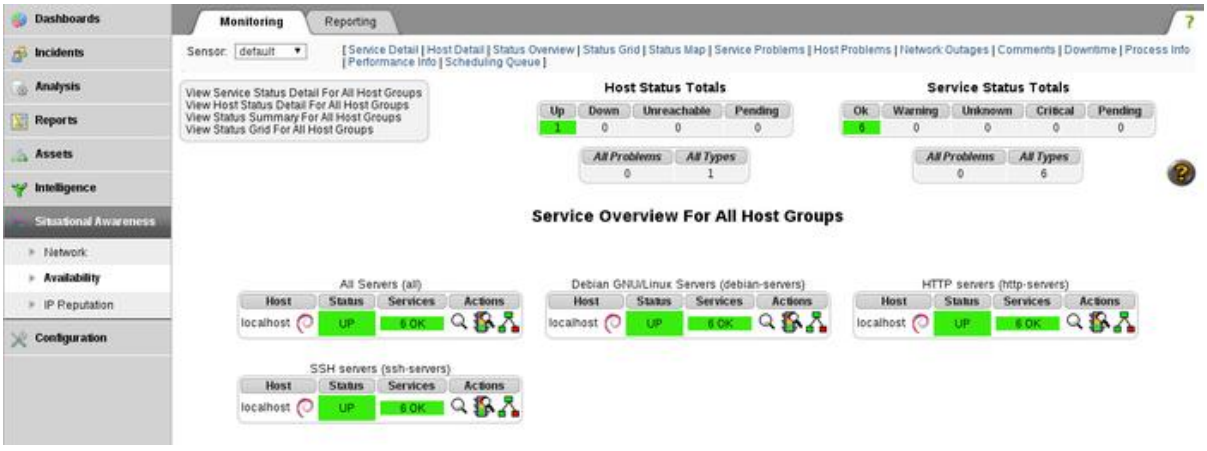
```
db_ip=127.0.0.1
db_port=3306
event_db=snort
ocs_db=ocsweb
ossim_db=ossim
osvdb_db=osvdb
pass=#PASSWORD#
rebuild_database=no
type=mysql
user=#USER#
```

3.5 Diagnosis Procedures

The Diagnosis Procedures are the first steps that a System Administrator will take to locate the source of an error in a GE. Once the nature of the error is identified with these tests, the system admin will very often have to resort to more concrete and specific testing to pinpoint the exact point of error and a possible solution. Such specific testing is out of the scope of this section.

The OSSIM main interface has a visual monitor with details about the *CPU load average*, *Disk space*, and *Network availability* of the different OSSIM instances in the network.
From here, the administrator can easily identify whether the cause of error comes from a network connection, or from the OSSIM machine itself.
The system also sends an email to the administrator account when the CPU load reaches a critical state, and when it lowers to the normal threshold again.
If the problem is just disk space, the OSSIM won't be able to store event data, but it will keep working. A suggested temporal solution would be to move the rotation syslog files, and the OSSIM database backup files to another storage disk.

To access this tool, go to the OSSIM main interface, and then to **Situational Awareness** -> **Availability** tab.



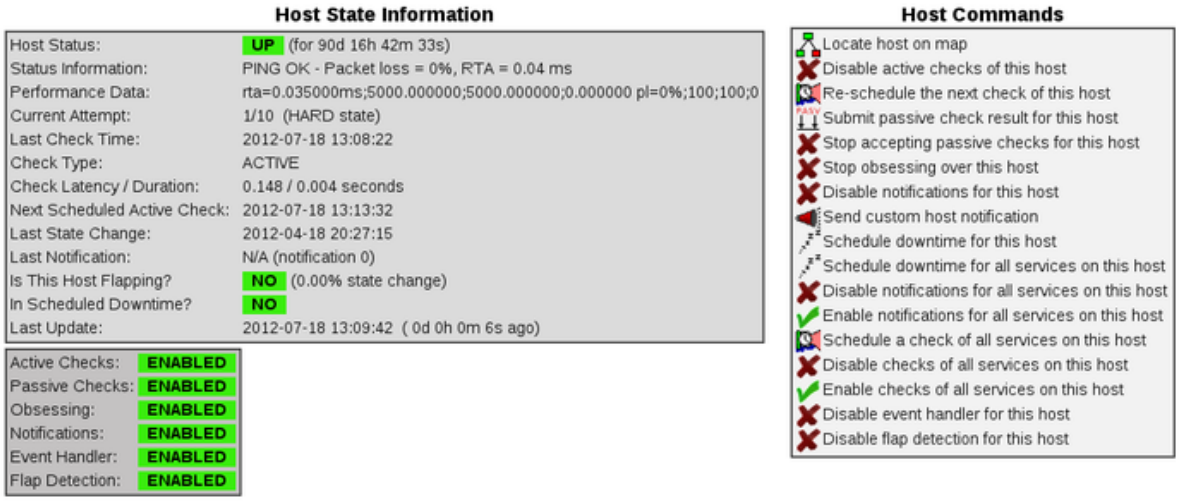
Diagnostics tool

Since the OSSIM architecture can be built as a tree of instances to secure different parts of the network (and send the collected event data to a main node), this interface is meant to centralize the monitoring of OSSIM machines in the network, and give the overview of the state of whole tree. (for this Use Case however, there is only one node which is called **localhost**).

For each OSSIM node in the network there are 3 diagnostics actions marked with 3 different icons:

- **Magnifying glass icon** (*Extended information of the node*)

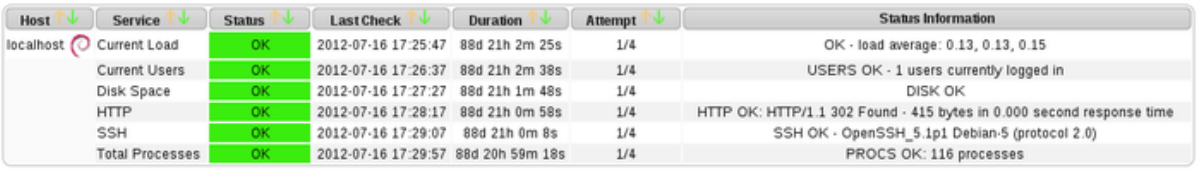
Here you can see information regarding the state, and tools to deactivate notification and checks for this node (e.g. for maintenance)



Extended info

- **Stoplight icon** (*Service details of the node*)

Here you can see the services state (up/down), network connection, CPU load, disk available, etc.



Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	2012-07-16 17:25:47	88d 21h 2m 25s	1/4	OK - load average: 0.13, 0.13, 0.15
	Current Users	OK	2012-07-16 17:26:37	88d 21h 2m 38s	1/4	USERS OK - 1 users currently logged in
	Disk Space	OK	2012-07-16 17:27:27	88d 21h 1m 48s	1/4	DISK OK
	HTTP	OK	2012-07-16 17:28:17	88d 21h 0m 58s	1/4	HTTP OK: HTTP/1.1 302 Found - 415 bytes in 0.000 second response time
	SSH	OK	2012-07-16 17:29:07	88d 21h 0m 8s	1/4	SSH OK - OpenSSH_5.1p1 Debian-5 (protocol 2.0)
	Total Processes	OK	2012-07-16 17:29:57	88d 20h 59m 18s	1/4	PROCS OK: 116 processes

Service details

- **Tree node icon** (*Locate host on map*)

This shows a map containing the relative position of the OSSIM nodes in the network to have an overview of the tree structure.

3.5.1 Resource availability

The availability is covered in the section Diagnosis Procedures

3.5.2 Remote Service Access

The system must be connected to the network in order to detect security events, and also take advantage of several features such as geo location based on IP.

There are several ways to remotely access the system and it's components:

- **Web based interface**
- **SSH login**
- **SFTP server**
- **MySQL event database**
- **Syslog server**

3.5.3 Resource consumption

The CPU consumption is rather complex to determinate, because it not only depends on the number of events sent to the OSSIM, but also on the complexity of the active correlation rules.
It is recommended to minimize the arithmetic operations applied in the correlation rules because these are the most resource consuming procedures and they are meant to be performed millions of times per second.

Also, if there is a point with too much network activity and it constantly overloads an OSSIM node, it is recommended to split the network and put an OSSIM instance on each subnetwork in order to balance the load.

3.5.4 I/O flows

Nothing but I/O flow on HTTPS & SSH standard ports.

4 Data Handling GE - Installation and Administration Guide

You can find the content of this chapter as well in the wiki of fi-ware.

4.1.1 System Requirements

First of all copy the installer zip file , extract the archive on your local folder that we will call $root. All the install files of these software are copied in $root\softwares

4.1.1.1 *Database*

We used the MySQL 5.1.43 database. In order to manage this database we used the EasyPHP 5.3.5 package that includes the Apache HTTP web server, PHP, MySQL and phpMyAdmin. The install including MySQL and PHP can be found here $root\softwares\EasyPHP-5.3.5.0-setup.exe

4.1.1.2 *Java VM*

The executable for the PPL engine requires Java version 1.6. In order to install it you can use the JDK file in $root\softwares\jdk-6u25-windows-i586.exe. 6. In order to configure correctly 16 your calsspath you can add a new variable PATH with the following value: \Program_Files\Java\ jdk1.6.0_21\bin

4.1.1.3 *Mozilla Firefox*

The demo is web-based and the user interface should be displayed in a browser. The user interface is a Firefox Plug-in that is compatible with the Firefox 4 Beta 3 version. For this reason this version of the browser must be installed and the setup file can be found in: $root\softwares\Firefox Setup 4.0 RC 1.exe

4.1.1.4 *PPL PolicyUI: Firefox Plug-in*

This plug-in is only available in the Install directory under the name PrimeLifePolicyUI.xpi. the file can be found in $root\partner_software\firefox_plugins\PrimeLifePolicyUI.xpi. In order to install the plug-in you just have to drag and drop this file into the Firefox browser. In order to configure it please set Set the PPL Engine URL to : http://localhost:9477/api/ and make sure that the suffix is empty. The default is .php

4.1.2 PPL Installation steps

The PPL engine is composed of three entities, a data subject, a data controller and a third party. Each entity uses its own database. They have to be created before resetting the database and launching the three entities. Here is the list of databases that need to be created:

- ppl
- ppl-dc

- ppl-dc-test
- ppl-ds-test

Once these databases are created you can either reset all databases with reset-productive.bat or for a specific entity with reset-productive-<entity>.bat.
After resetting the database each entity can be launched with its respective bat file: dc.bat and ds.bat.
How to manage an entity: Each entity runs its own webserver providing a web interface to manage it. Below is the url for each of them

- Data subject: http://localhost:9477/
- Data controller: http://localhost:8082/

4.1.3 Sanity Check Procedures

The Sanity Check Procedures are the steps that a System Administrator will take to verify that an installation is ready to be tested. This is therefore a preliminary set of tests to ensure that obvious or basic malfunctioning is fixed before proceeding to unit tests, integration tests and user validation.

4.1.3.1 *End to End testing*

To verify that the Data Handling GE service was correctly deployed on the application server:

- Data subject: http://localhost:9477/ an HTML frontend with the FIWARE logo is properly displayed
    - Another test can be to navigate with a web browser to URL: http://localhost:9477/api/pii

Execution log using cURL:

```
* About to connect() to <server> port 9477 (#0)
*   Trying <server>... connected
* Connected to <server> (<server> IP) port 9477 (#0)
> GET /api/pii HTTP/1.1
> User-Agent: curl/7.21.3 (i686-pc-linux-gnu) libcurl/7.21.3
OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.18
> Host: <server>:9477
> Accept: */*
>
< HTTP/1.1 200 OK
< Content-Type: text/xml; charset=utf-8
< Transfer-Encoding: chunked
< Server: Jetty(6.1.x)
<
* Connection #0 to host <server> left intact
* Closing connection #0
```

```
<piis>[a list of <pii> nodes, or nothing if no PIIs are
inserted]</piis>
```

- Data controller: http://localhost:8082 an HTML frontend with the FIWARE logo is properly displayed
    - Another test can be to navigate with a web browser to URL: http://localhost:9477/api/pii

Execution log using cURL:

```
* About to connect() to <server> port 8082 (#0)
*   Trying <server>... connected
* Connected to <server> (<server> IP) port 8082 (#0)
> GET /api/pii HTTP/1.1
> User-Agent: curl/7.21.3 (i686-pc-linux-gnu) libcurl/7.21.3
OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.18
> Host: <server>:8082
> Accept: */*
>
< HTTP/1.1 501 Not Implemented
< Content-Type: text/html; charset=utf-8
< Transfer-Encoding: chunked
< Server: Jetty(6.1.x)
<
* Connection #0 to <server> left intact
* Closing connection #0
["status":501]
```

This test actually ensures that the internal implementation correctly parses the incoming request, while at the same time producing a meaningful error message as result of the internal computation (the "["status":501]"). In case of deployment issues, a different error message is returned.

4.1.3.2 *List of Running Processes*

- cmd.exe
- java.exe
- mysqld.exe
- apache.exe
- easyphp.exe

4.1.3.3 *Network interfaces Up & Open*

N/A

4.1.3.4 *Databases*

Check whether MySQL instance is up and running, and reachable from the Application Server;
When using Easy PHP the Admin console is reachable at : http://127.0.0.1/home/mysql/
Check It the three DB are initiated as described in the previous section

4.1.4 Diagnosis Procedures

The Diagnosis Procedures are the first steps that a System Administrator will take to locate the source of an error in a GE. Once the nature of the error is identified with these tests, the system admin will very often have to resort to more concrete and specific testing to pinpoint the exact point of error and a possible solution. Such specific testing is out of the scope of this section.

4.1.4.1 *Resource availability*

It is important that the deployment (virtual/physical) machine has at least 2 CPUs, in order to manage effectively concurrent requests to different servers (Data Handling GE components + RDBMS backend). For optimal performances, a system should also have at least 4 GB RAM, and 5 GB storage to be dedicated to Data Handling + RDBMS needs.
Minimal requirements are 1 CPU, 500 MB RAM and 500 MB of application-dedicated storage.

4.1.4.2 *Remote Service Access*

N/A

4.1.4.3 *Resource consumption*

Resource consumption strongly depends on inputs. In our tests, a 8-core i5 CPU system with 16 GB RAM and 500 GB storage was able to deal with 4 concurrent requests

4.1.4.4 *I/O flows*

The only expected I/O flow is of type HTTPS (or HTTP), on standard ports, and inbound only. Requests interactivity should be low, even if a polling mechanism on an API method (getPolicyResult) could involve several requests to be executed from clients.

5 DB Anonymizer GE - Installation and Administration_Guide

You can find the content of this chapter as well in the wiki of fi-ware.

5.1.1 Introduction

DB Anonymizer is a Java Web Application, packaged in a WAR file. It uses a MySQL database in order to evaluate the adequateness of a specific anonymization policy, to be used to disclose a dataset. The dataset (in the form of a MySQL table SQL dump) will be passed to DB Anonymizer through its ReSTful API, together with an anonymization policy to analyse. At that point, DB Anonymizer will upload in its MySQL instance the received dataset, and perform the policy analysis.
As said, DB Anonymizer needs to receive a dump of a MySQL table, containing all data, together with a disclosure policy. Both inputs are mandatory to let the service's algorithm to be able to evaluate the effectiveness of the disclosure policy. Once the policy is evaluated, the table is dropped from the DB and the file dump is erased. The application server encapsulation model permits a complete isolation of each user's data, and any intermediate result created during algorithm's execution is deleted immediately at the end of the computation.
DB Anonimizer uses:

1. a MySQL instance
2. a Java Application Server (any should work, but only Apache Tomcat is supported)

In the remainder of this section, the configuration of these two elements is presented.

5.1.2 Installation

5.1.2.1 *Database*

DB Anonymizer has been tested using MySQL v5.5.X.

DB Configuration
DB Anonymizer expects to be able to access to a MySQL schema, **obligatorily called "census"**, using an account that has full grants on that specific schema. This is necessary to be able to create and drop tables, views, indexes and so on.
The DB schema should be empty, except for a table, that can be created using the following SQL statements:

```
DROP TABLE IF EXISTS `results`;
CREATE TABLE `results` (
  `idresults` int(11) NOT NULL AUTO_INCREMENT,
  `GID` bigint(20) NOT NULL,
  `result` text NOT NULL,
  `computed` tinyint(1) NOT NULL,
```

```
  PRIMARY KEY (`idresults`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

5.1.2.2 *Application Server*

While no specific Application Server functionalities are used, the application has been tested with Apache Tomcat 6.X and 7.X.

Application Server configuration

It is necessary to provide DB Anonymizer with a JDBC MySQL datasource, identified by a JNDI resource, that will be used in its computation processes.

To this extent, for Apache Tomcat, it is necessary to add a file named "context.xml" (or to edit it, if already existing) in its configuration directory (generally "conf").

It should contain the following information:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context>
    <!-- Specify a JDBC datasource -->

    <Resource name="jdbc/censusdb" auth="Container"
        type="javax.sql.DataSource" username="<username for MySQL>"
password="<password for MySQL>
        driverClassName="com.mysql.jdbc.Driver"
        url="jdbc:mysql://<address of MySQL DBMS >:3306/<database
schema name>?autoReconnect=true"
        maxActive="100" maxIdle="30" />

</Context>
```

Attributes *maxActive* and *maxIdle* are needed in order to enable the creation of a connection pooling to improve DB Anonymizer performances. These values should be fine tuned according to the characteristics of the deployment server. Please refer to this link for more information.

DB Anonymizer deployment

DB Anonymizer WAR package can be installed by copying it into "webapp" folder in Apache Tomcat. To install it on other Java Application Servers, please refer to their specific application server guidelines.

Remark: HTTPS/SSL

It is highly recommended to allow incoming connection to DB Anonymizer only through HTTPS. This can be achieved by using a front-end HTTPS server that will proxy all requests to DB Anonymizer, or by configuring the Application Server in order to accept only HTTPS/SSL connection. In the latter case, please refer to this link for more information.

5.1.3 Sanity Check Procedures

The Sanity Check Procedures are the steps that a System Administrator will take to verify that an installation is ready to be tested. This is therefore a preliminary set of tests to ensure that obvious or basic malfunctioning is fixed before proceeding to unit tests, integration tests and user validation.

5.1.3.1 *End to End testing*

To verify that the DB Anonymizer application was correctly deployed on the application server:

- check whether, at the URL http(s)://<server address>:<server port>/<any additional path that could have been set by application server administrator> an HTML frontend with the FIWARE logo is properly displayed;
- check if, at the URL http(s)://<server address>:<server port>/<any additional path that could have been set by application server administrator>/DBA?_wadl a WADL file describing the ReST API is available.

To verify that DB Anonymizer works correctly:

- verify that visiting with a web browser URL: <application path>/DBA/getPolicyResult?gid=<random number> would return the following message:

```
Error in retrieving the requested result
```

This would ensure that DB connection is properly set. Any other message could represent a possible deployment issue. Return codes are described in the API specification.

- launch the unit test suite as explained in DB Anonymizer Generic Enabler - Unit Testing Plan; again, if misbehaviours would happen, this could mean a deployment issue; return codes are described in the API specification. However, a redeployment is in general the best solution, as well as a re-creation of the DB schema.

5.1.3.2 *List of Running Processes*

- there should be a number of Java processes, depending on the Application Server configuration;
- mysql server process(es).

5.1.3.3 *Network interfaces Up & Open*

N/A

5.1.3.4 *Databases*

- check whether MySQL instance is up and running, and reachable from the Application Server;
- check whether the required MySQL database schema "census" is created, and the username supplied has granted all rights on it;
- check whether the required MySQL table is properly created into "census" with the query:

```
SELECT * FROM census.results;
```

It should return no results if the query is executed before the first DB Anonymizer execution.

5.1.4 Diagnosis Procedures

The Diagnosis Procedures are the first steps that a System Administrator will take to locate the source of an error in a GE. Once the nature of the error is identified with these tests, the system admin will very often have to resort to more concrete and specific testing to pinpoint the exact point of error and a possible solution. Such specific testing is out of the scope of this section.
The following sections have to be filled in with the information or an "N/A" ("Not Applicable") where needed. Do not delete section titles in any case.

5.1.4.1 *Resource availability*

Resource load of DB Anonymizer strongly depends on the size of incoming DB dump, and from the number of concurrent requests received. There are different aspects to consider, on the Application Server and on the MySQL DB.

- with respect to the Application Server:
  - DB Dumps can potentially contain significant amount of data. During the testing phase, dumps of GBs have been transferred and processed. Despite DB dumps are expected to be sent in zipped format, they are nevertheless uncompressed on the local Application Server storage, in order to be pre-parsed and then sent to the MySQL DB. Even if these dumps are deleted just after their analysis, it is recommended that several GBs of space are available, in order to sustain a significant number of concurrent requests.
- with respect to the MySQL DB:
  - the work load on the MySQL DB can be significant, therefore it is recommended to have a number of GBs of RAM and storage dedicated to MySQL, for the same reasons expressed for the Application Server. A number of CPU cores could be assigned to MySQL DBMS as well.

5.1.4.2 *Remote Service Access*

N/A

5.1.4.3 *Resource consumption*

Resource consumption strongly depends on inputs. In our tests, a 8-core i5 CPU system with 16 GB RAM and 500 GB storage was able to deal with 4 concurrent requests, with MySQL dumps of ~3 GB (uncompressed). These parameters did not affected dramatically server's performance, therefore they should considered safe values for a standard/heavy-load deployment.

5.1.4.4 *I/O flows*

The only expected I/O flow is of type HTTPS (or HTTP), on standard ports, and inbound only. Requests interactivity should be low, even if a polling mechanism on an API method (getPolicyResult) could involve several requests to be executed from clients.