

# OSSIM Install Guide for Debian GNU/Linux

Open Source Security Information Management (OSSIM)  
Document updated: Thu, 31 Mar 2005 10:28:07 GMT  
Authors: **David Gil** and **Sté phane Fournier**

## Index:

---

- 0. Before installing OSSIM
  - 1. ossim-mysql
  - 2. ossim-server
  - 3. ossim-agent
  - 4. ossim-framework
  - 5. ossim-utils
  - 6. ossim-contrib
  - 7. Post OSSIM installation
  - 8. TODO
  - A. Plugins

## 0. Before installing OSSIM

---

### 0.1 Installing Debian GNU/Linux

If you have **Debian** installed into your system, just go to the following section. If not, we recommend you to install it with the new **Debian Sarge Installer**.

### 0.2 Apt configuration

Edit the file `/etc/apt/sources.list` to set the repositories of **Debian Sarge** and **OSSIM**:

```
[ -- /etc/apt/sources.list -- ]
deb http://security.debian.org/ sarge/updates main
deb http://ftp.debian.org/debian/ sarge main
deb http://www.ossim.net/download/ debian/
```

Update your dpkg info with:

```
# apt-get update
```

Create a `/etc/apt/preferences` file like this:

```
[ -- /etc/apt/preferences -- ]
Package: *
Pin: release o=ossim
Pin-Priority: 995
```

This way apt will assign a higher priority to OSSIM packages and their dependencies. Please, see the `apt_preferences` manual page for more info.

### 0.3 Performance

Install a 2.6 Linux kernel. We notice a much better efficiency in terms of performances and in comparison with a 2.4 kernel (Debian default installation):

```
# apt-get update && apt-get install kernel-image-2.6-686
```

Install `hdparm` to also increase the performance of your hard drive, especially for the computer which will host the database:

```
# apt-get install hdparm
```

```
[ -- /etc/hdparm.conf -- ]
# Activate DMA + Safe Performance-enhancing Options
/dev/hda {
    dma = on
    lookahead = on
    mult_sect_io = 16
    interrupt_unmask = on
    read_ahead_sect = 64
}
```

### 0.4 Clean up your system

Install `deborphan` in order to remove orphaned libraries:

```
# apt-get install deborphan
# apt-get remove --purge `deborphan`
```

Configure your runlevel scripts. You may run on startup only the services you really want. Install a runlevel configuration tool like `rcconf` or `sysv-rc-conf`.

## 1. Install ossim-mysql

---

Install it:

```
# apt-get install ossim-mysql
```

Set a root password for your database:

```
# mysqladmin -u root password your_secret_password
```

Edit `/etc/mysql/my.cnf` and modify the `bind-address` entry if you want MySQL will listen on port TCP-3306 after restart.

Create the following databases:

```
# mysql -u root -p

mysql> create database ossim;
mysql> create database ossim_acl;
```

```
mysql> create database snort;
mysql> exit;
```

Then load the tables in the databases:

```
# zcat /usr/share/doc/ossim-mysql/contrib/create_mysql.sql.gz \
/usr/share/doc/ossim-mysql/contrib/ossim_config.sql.gz \
/usr/share/doc/ossim-mysql/contrib/ossim_data.sql.gz \
/usr/share/doc/ossim-mysql/contrib/realsecure.sql.gz | \
mysql -u root ossim -p

# zcat /usr/share/doc/ossim-mysql/contrib/create_snort_tbls_mysql.sql.gz \
/usr/share/doc/ossim-mysql/contrib/create_acid_tbls_mysql.sql.gz \
| mysql -u root snort -p
```

## 2. Install OSSIM Server

---

Install it with apt:

```
# apt-get install ossim-server
```

You will be prompt for your network properties and for your database connections. Use `dpkg-reconfigure ossim-server` if you want to update the server configuration (don't edit `/etc/ossim/server/config.xml` by hand)

## 3. Install OSSIM Agent

---

Install the plugins you want to use with OSSIM (see [appendix A](#))

Install ossim-agent:

```
# apt-get install ossim-agent
```

You will be prompt for your sensor configuration. Use `dpkg-reconfigure ossim-agent` if you want to update the agent configuration (don't edit `/etc/ossim/agent/config.xml` by hand)

## 4. Install OSSIM Framework

---

Install phpgacl package:

```
# apt-get install phpgacl
```

Install ossim-framework and all its dependencies:

```
# apt-get install ossim-framework
```

You will be prompt for your database configuration (ossim & ossim\_acl databases). Use `dpkg-reconfigure ossim-utils` and `dpkg-reconfigure ossim-framework` if you want to update the framework configuration (don't edit `/etc/ossim/framework/ossim.conf` by hand)

Access the framework [ <http://yourhost/ossim/> ] and go to configuration menu Configuration->Main (you should only change some passwords, if not, let us know as we'll try make a more fully automated installation).

## 5. Install OSSIM utils

---

The ossim-framework package depends on the ossim-utils one, so you need to have it installed. If you want to have it installed on another host:

```
# apt-get install ossim-utils
```

Maybe you'll have to reconfigure ossim-utils (dpkg-reconfigure ossim-utils) to configure the database access parameters of some scripts. We'll soon have a solution at this problem.

## 6. Install OSSIM contrib (optional)

---

The package ossim-contrib contains a set of patches, examples and configuration files used by the ossim distribution. This package is only useful for development purposes.

## 7. Post OSSIM installation

---

The package ossim is a meta-package which depends on the the other ones.

```
# apt-get install ossim
```

## 8. TODO

---

- Nessus integration
- OpenNMS integration

You can find more info on this [document](#) but be very careful with it since is quite deprecated.

## A. Install Plugins

---

### A.1 Snort

Install snort:

```
# apt-get install snort-mysql
```

Don't configure snort database via debconf, it's better that you edit the file /etc/snort/snort.conf by hand:

```
[ -- /etc/snort/snort.conf -- ]
..
var HOME_NET [192.168.0.0/16]
var EXTERNAL_NET !$HOME_NET
..
```

```
# splitted in two lines for readability
output database: alert, mysql, user=root password=yourdbpass dbname=snort
host=yourdbhost sensor_name=your_sensor_ip logfile=fast.log
..
# if you want spade support obtain a valid spade.conf file
# (for example from ossim source or from ossim-contrib package)
include spade.conf
..
```

Check out [Bleeding Edge of Snort web page](#) for up-to-date, bleeding edge snort rules. The false positive rate is extremely low for little tested signatures and they are being very useful to us:

```
# cd /etc/snort/rules/
# wget http://www.bleedingsnort.com/bleeding-all.rules
# echo "include \$RULE_PATH/bleeding-all.rules" >> /etc/snort/snort.conf
```

Update OSSIM database with the rules of your system:

```
# /usr/share/ossim/scripts/create_sidmap.pl /etc/snort/rules | \
mysql -u root ossim -p
```

## A.2 Ntop

Install Ntop:

```
# apt-get install librrd0 ntop
```

Define the password for the admin user:

```
# ntop -u ntop
>> Please enter the password for the admin user:
# ^C
# /etc/init.d/ntop start
```

Go to <http://yourhost:3000/> to see Ntop in action. Activate the rrdPlugin at Admin->plugins. Click on Host at Data Dump and specify your netmask at Hosts Filter.

In order to make RRD plugin of ntop working with ips instead of macs (needed by agent), edit `/etc/default/ntop` file and add `--no-mac` to `GETOPT=""`.

## A.3 Other plugins

As simple as:

```
# apt-get install p0f arpwatch pads tcptrack
```

Don't run arpwatch on boot, let ossim-agent do the job:

```
# update-rc.d -f arpwatch remove
```