

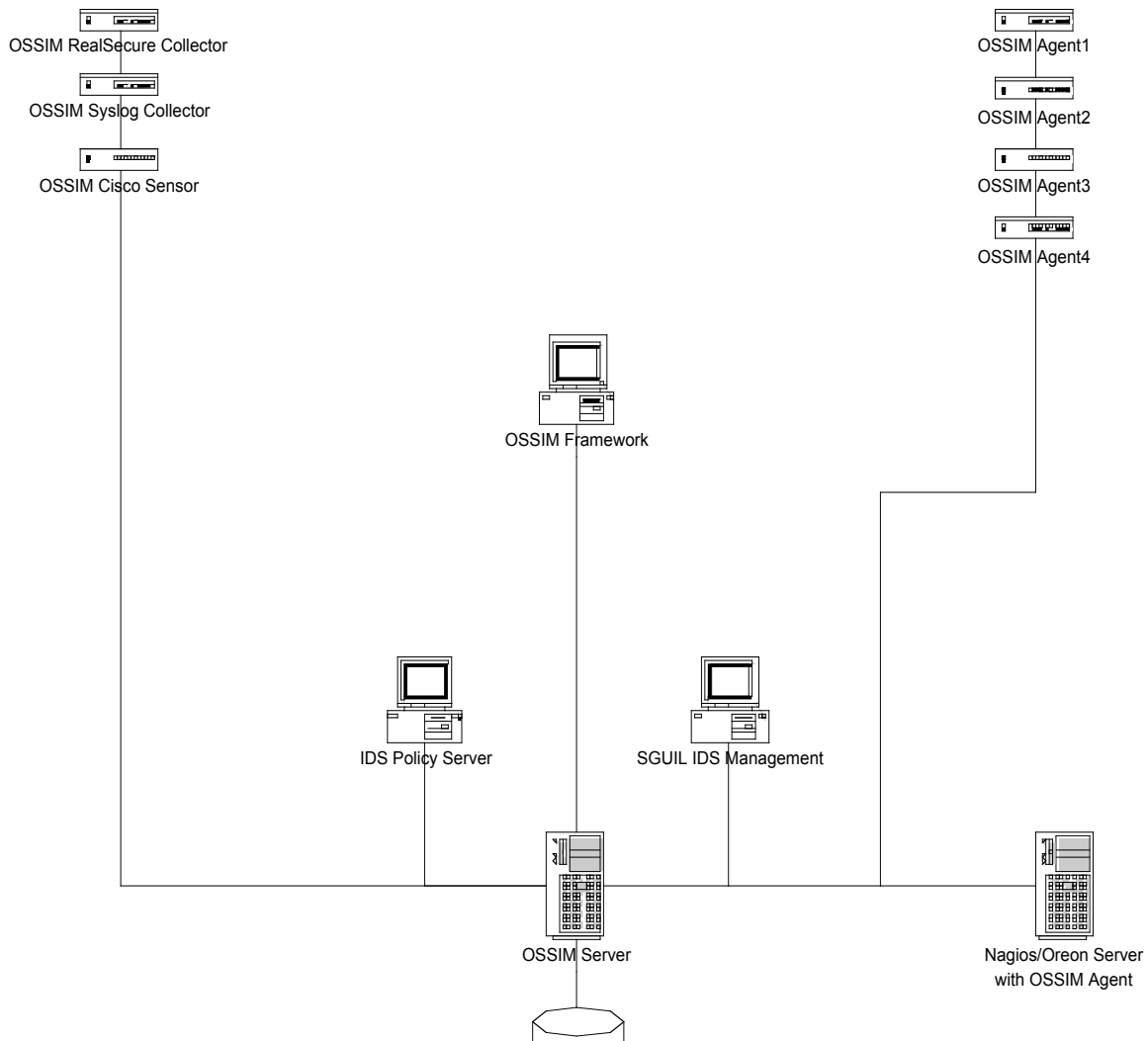
# **OSSIM-Agents Inside a Distributed Enterprise**

J Hybinette, CISM, CISSP, CEH, ISSAP, ISSMP, IAM, IEM

## **System**

When OSSIM is in a distributed enterprise it is necessary to place the OSSIM-agents “sensors” in various locations throughout the enterprise. Many of these sensors have to be installed onto hosts that already run some type of monitoring/sensor software such as Nagios, where others can be generically installed on dedicated sensor machines.

## OSSIM Infrastructure



The OSSIM-agents are divided into two groups:

### **Specialty Agent**

This is an ossim-agent that is installed only to serve one purpose to collect data from. The Specialty agents are as following:

- Realsecure Collector
- Syslog Collector (server)
- Cisco Collector
- Nagios Collector
- Ntsyslog Collector
- IIS Collector

- Apache Collector

Others could be considered specialty agents as well depending on the enterprise.

### **Generic Agent**

The generic agent is a type of agent that can easily be installed on its own server and distributed throughout the enterprise. This agent includes the following:

- Snort
- TcpTrack
- P0f
- Pads
- RRD
- Ntop
- Arpwatch
- Nessus
- Nmap
- Syslog (local)

This again may be a little different depending on how the enterprise looks.

## **Generic OSSIM-Agent (Debian)**

A generic agent can easily be installed on its own host machine below are the complete instructions on how to construct such a machine from scratch. Because of some of the software used on this machine such as the Nessus and Ntop a decent amount of memory is required to be installed on the host machine. Absolute minimum would be 1 GB of RAM, but to get some decent performance 2 GB or better is recommended. It is also recommended to use two separate Ethernet interfaces for security reasons and flexibility. The procedure below will install the system onto a machine with dual NICs.

Download the latest Debian ISO from [www.debian.org](http://www.debian.org). Insert the cd into the agent and reboot.

Select the proper locale and networking settings.

Manually edit the partition table:

Make 2 partitions swap and filesystem. The swap should be 2 times the amount of RAM on the agent and the rest can be dedicated to the filesystem. Specify the filesystem to use reiserfs, yes to formatting it and / as mount point. The second partition should be assigned swap. Then save and continue.

Answer yes to install the GRUB boot loader

The agent will now eject the CD and reboot itself. Select time zone, users and password.

Archive access method for apt:  
Select http and proper mirrors

The agent will now start to download required software.

Do not check any type when asked for software to install. The system is being manually configured.

Configure exim for local delivery only when asked

Reboot system and log in. Then the sources.list has to be updated so OSSIM and programs can be installed properly.

Edit the `/etc/apt/sources.list` and add:

```
deb http://ftp.us.debian.org/debian stable main
deb-src http://ftp.us.debian.org/debian stable main

deb http://ftp.us.debian.org/debian testing main
deb-src http://ftp.us.debian.org/main testing main

deb http://ftp.us.debian.org/debian/ unstable main
# deb-src http://ftp.us.debian.org/debian/ unstable main

deb http://security.debian.org/ stable/updates main

## OSIM Sources

deb http://ftp.debian.org/debian testing main
deb http://secure-testing.debian.net/debian-secure-testing testing/security-
updates main
deb http://www.ossim.net/download/ Debian/
```

Note, the sources list may look different in some cases. This is only an example. Update apt resources:

```
# apt-get update
```

No errors should show when doing this. Next step is to install an updated kernel image onto the agent:

```
# apt-get install linux-image-2.6.15-1-686
```

This could be any other suitable (newer) image as well. Install links as a text based web browser. Framebuffers may be enabled when desired. To do this edit the `/boot/grub/menu.lst` and add `vga=791` or other preferred setting to the kernel statement. Reboot the agent with the new kernel.

Upgrade your system

```
# apt-get upgrade
```

Install a text based web browser:

```
# apt-get install links
```

Get the public key so that Debian secure testing applications can be downloaded

# links <http://secure-testing.debian.net>

From there download the archive signing key. To install the key:

```
# apt-key add ziyi-2005-7.asc
```

key name may be named differently in some cases.

## Networking

The Debian installer gives a chance to configure a single network interface, but multiple ethernet interfaces may have to be configured.

The primary network configuration file is `/etc/network/interfaces`. The following example shows a configuration that brings up network interfaces on two different NICs: one with a static IP address, and a one that gets its configuration via DHCP.

```
/etc/network/interfaces
auto lo eth0 eth1
iface lo inet loopback
iface eth0 inet static
    address 192.0.34.72
    netmask 255.255.255.0
    gateway 192.0.34.1
iface eth1 inet dhcp
```

Note that interfaces with static IPs require `address`, `netmask`, and `gateway` directives. By using multiple `address` directives, multiple IP addresses on a single NIC may be claimed.

I don't know of any way to predict which NIC will be assigned to which interface, if you have multiple NICs. However, the mapping is preserved across reboots, so once you figure it out, you don't have to worry about it changing on you.

DNS lookup is configured in the file `/etc/resolv.conf`. The most common directives used are `search`, which specifies which domain names to try when a FQDN is not specified, and `nameserver`, which specifies the IP address of a domain name server

```
/etc/resolv.conf
search example.com
nameserver 192.0.34.2
nameserver 192.0.34.3
```

Multiple instances can be used of both the search and nameserver directives to specify multiple search domains and name server, which will be tried in the order specified. For more information on these and other directives, man resolv.conf.

When done making changes to the network configuration, then activate the changes by entering

```
# /etc/init.d/networking restart
```

and check up on the status of the configured interfaces with

```
$ /sbin/ifconfig
```

```
eth1    Link encap:Ethernet  HWaddr 00:04:76:CF:FC:F2
        inet addr:192.0.34.72  Bcast:255.255.255.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:347855 errors:0 dropped:0 overruns:0 frame:0
        TX packets:98030 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:119402525 (113.8 MiB)  TX bytes:17369382 (16.5 MiB)
        Interrupt:9 Base address:0x8000
```

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:6261 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6261 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1922477 (1.8 MiB)  TX bytes:1922477 (1.8 MiB)
```

## Snort

### Configuration on the OSSIM Server Box

Next step will be to have snort to log in to the snort database on the OSSIM server. First edit the /etc/mysql/my.cnf file and make sure the bind address is set to the external ip on the server. To test from the agent try:

```
# telnet serveripaddress 3306
```

to see if the external mysql port is open and functioning.

Next user rights have to be established to snort database on the OSSIM server so that remote agents can log in to the database.

```
# mysql -u root snort -p
# Enter password: *****
mysql> grant create,insert,select,update,delete on snort.* to snort"%";
mysql> set password for snort@"%" = password ( 'passwordhere' );
mysql> flush privileges;
mysql> quit
```

This is assuming that the user is “snort” on the remote agents. This can also be easily managed with mysql-admin if it is installed.

### Configuring OSSIM agent box

Install snort:

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

Delete the db-pending-config from snort

```
# rm /etc/snort/db-pending-config
```

Configure snort to send data to the OSSIM server. To do this edit the /etc/snort/snort.conf file and add:

```
output database: alert, mysql, user=snort password=yourdbpass dbname=snort
host=yourdbhost sensor_name=your_sensor_ip
```

```
output alert_fast: alert
```

edit /etc/snort/snort.debian.conf and verify it listens to eth1 and the proper networks.

Make sure the snort installation works:

```
# /etc/init.d/snort start
```

Check and see if started successfully by checking the Syslog messages. If not starting and error messages are generated. First stop snort like:

```
# /etc/init.d/snort stop
```

Correct the errors and restart. Usually errors are generated because of missing rule sets. To fix this go to [www.snort.org](http://www.snort.org) and register. Then download the new rules into snort.

It is recommended to centrally manage the snort rule sets where distributed agents are used. One program is policy manager which can be obtained from

<http://www.activeworx.org>

Policy manager is a windows based program. If no policy manager is used it may be a good idea to install oinkmaster instead to automatically update the signatures for snort. Furthermore the bleedingsnort rule set may be handy.

<http://www.bleedingsnort.com>

check to see if snort is running

```
# ps ax |grep snort
```

and

```
# lsof -n -i |grep snort
```

You should see snort connecting to the remote OSSIM server

## **OSSIM-Agent**

Install the ossim-agent

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

Now edit the /etc/ossim/agent/config.xml file. In this file you can:

- Change address where the server is listening.
- Activate/deactivate watchdog
- Activate/deactivate plugins
- Configure plugins.
- Etc

Change the following:

sensor IP to your IP on eth0

Interface should be set to eth1

Serverip should be set to the ossim-server ip address

Ossim\_db should be changed to:

```
“mysql:OSSIM_Server_Ip:ossim:ossim:putyourossimpasswordhere”
```

Under plugins add

```
&tcptrack;
```

Next user rights have to be established to the ossim database on the OSSIM server so that remote agents can log in to the database.

```
# mysql -u root snort -p
# Enter password: *****
mysql> grant create,insert,select,update,delete on ossim.* to ossim@"%";
mysql> set password for ossim@"%" = password ( 'passwordhere' );
mysql> flush privileges;
mysql> quit
```

This is assuming that the user is ossim on the remote agents.

After this, mysqldb needs to be installed for the client to work properly

```
# apt-get install python2.3-mysqldb
```

ossim-agent also calls for the rrd\_plugin.pl script. To obtain this"

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

Then change the /etc/ossim/framework/ossim.conf like:

```
#####
# OSSIM db configuration
#####
ossim_type=mysql
ossim_base=ossim
ossim_user=ossim
ossim_pass=EnterYour PasswordHere
ossim_host=EnterYourOssimServerHostHere
ossim_port=3306
```

Install applications for ossim-agent

```
# apt-get install tcptrack
# apt-get install arpwatch
# apt-get install pads
# apt-get install p0f
# apt-get install rrdtool
# apt-get install nessus (not required)
# apt-get install nessusd
# apt-get install nmap
```

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

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

## ntop

Install ntop

```
# wget http://internap.dl.sourceforge.net/sourceforge/ntop/ntop-3.1.tgz
# tar -xzvf ntop-3.1.tgz
```

We need to get the ossim ntop patches for ntop to work. For that we need to download ossim.

```
# wget http://internap.dl.sourceforge.net/sourceforge/os-sim/os-sim-0.9.8.tar.gz
# tar -xzvf os-sim-0.9.8.tar.gz
```

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

Define the password for the admin user

```
# ntop -u ntop
>> Please enter the password for the admin user:
# ^C
```

In order to make RRD plugin in ntop to work with ips which is needed by the OSSIM agent, edit the `/etc/default/ntop` and add `-no-mac` to the `GETOPT="` variable. Be sure to remove the `#` in front of the `GETOPT`.

We want ntop to listen to eth1 in lieu of eth0. To do this edit `/var/lib/ntop/init.cfg`. Then edit:

```
INTERFACES="eth1"
```

Then start ntop

```
# /etc/init.d/ntop start
```

To test ntop, use a web browser to log in to the agent server like

<http://ip-on-agent-server:3000/>

ntop should now appear in the browser. Be sure rrdtool works by seeing graphs in the Global Traffic Statistics window. Now configure ntop to listen on eth1 by selecting admin -> configure->startup options. Then select eth1 as the capture interface. Then save the changes.

To protect the ntop pages by assigning access rights. Do this by selecting admin -> configure -> Protect URLs. Then select Add URL. Leave the URL box empty and be sure the authorized user is admin, then add the URL. Next time when logging in to ntop, you should be asked for username and password.

## Nessus

The nessusd needs to be configured before it can be used. First assign a user and password:

```
# nessus-adduser  
Login: ossim  
Autentication (pass/cert) [pass] : <hit return>  
Login Password: YourPasswordHere  
Login Password (again): YourPasswordHere
```

```
Yada yada yada.....  
Ctrl-D
```

```
Is that ok ? [y]  
User added
```

Update plugins:

```
# nessus-fetch -plugins  
# nessus-update-plugins
```

## **Policy Manager Installation and Configuration**

Policy Manager from Activeworx is a windows based utility that allows to easily manage snort rules sets in a distributed enterprise.

Download Policy manager from <http://www.activeworks.org> and install it with default options.

It may be a good idea to back up the snort.conf file on the snort host before using Policy Manager.

Also on the snort host create a policy user for Policy Manager to use

```
# adduser policy
```