

Integrating Snort-2.9.5.x with the AlienVault OSSIM 4.1 SIEM on Linux based systems.

Last Revised on July 31, 2013.

The document below uses the following color codes for items/steps the user should be aware of during the configuration AlienVault OSSIM 4.1 SIEM and Snort-2.9.5.x:

Note: The information below also applies to those users running Snort 2.9.4.x.

Blue - informational messages and comments

Orange – These are commands that the user types at the shell prompt

Red – **Read carefully before proceeding.**

Tested successfully on the following operating systems:

CentOS 6.x (64-bit)

OpenSUSE 12.x (64-bit)

Before proceeding, I **strongly recommend backing up rsyslog.conf and snort.conf.**

Here are the bare minimum requirements to get Snort 2.9.5.x to send alerts to the AlienVault OSSIM 4.1 SIEM via **rsyslog** and modifying **snort.conf** to direct the alert(s) to **rsyslog**.

On systems that are running snort sensor(s) you wish to monitor with OSSIM 4.1 SIEM, do the following:

Locate the **rsyslog.conf** file, this is usually found in **/etc**, **make a backup of it**, and add the information below to it (after the last **ModLoad** directive found towards the top of the file):

```
# Added for OSSIM integration with snort
$SystemLogRateLimitInterval 10
$SystemLogRateLimitBurst 500
#$SystemLogSocketFlowControl on
#$AddUnixListenSocket /var/snort/dev/log
local1.info @@192.168.1.180:514
```

The '**local1.info**' line means that any TCP/UDP message that '**rsyslog**' processes for the '**local1**' logging facility is to be sent to IP address 192.168.1.180 port 514 (in this case, that IP address is the OSSIM 4.1 SIEM).

After modifying this file, stop and start **rsyslog** on your system.

Next, set up the OSSIM 4.1 SIEM to handle remote logging from your snort sensors, to do this, log into the OSSIM 4.1 box as 'root' via [ssh](#), and add/modify the following files below:

Create '[remote-snort-sensors.conf](#)' in [/etc/rsyslog.d](#) using your favorite editor, and add the lines below to the file:

```
# Remote Snort sensor logging
$ModLoad imtcp
$InputTCPServerRun 514
# do this in FRONT of the local/regular rules
if $fromhost-ip == '192.168.1.95' then /var/log/snort/alert
& ~
if $fromhost-ip == '192.168.1.40' then /var/log/snort/alert
& ~
#if $fromhost-ip == '10.0.10.2' then /var/log/snort/alert
#& ~
#if $fromhost-ip == '10.0.10.2' then /var/log/snort/alert
#& ~
```

Now, in the above file, the '[imtcp](#)' is the [rsyslog](#) input module for receiving TCP connections and the '[InputTCPServerRun 514](#)' tells [rsyslog](#) to listen on [port 514](#) for incoming traffic.

The [\\$fromhost-ip](#) lines should be set up for each snort sensor that you want OSSIM 4.1 to log alerts for, in my case, I have two IP addresses since I'm using two snort sensors. If the IP address matches, it will send the information to [/var/log/snort/alert](#).

Edit the file '[/etc/rsyslog.conf](#)' on the OSSIM 4.1 box and add the following lines to it (make sure you **make a copy of this file** before proceeding):

```
$SystemLogRateLimitInterval 10
$SystemLogRateLimitBurst 500
```

This will increase the rate at which [rsyslog](#) will accept messages before it drops them due to rate-limiting.

After doing this, stop and start [rsyslog](#) in [/etc/init.d](#) to have it re-read the '[remote-snort-sensors.conf](#)' and '[rsyslog.conf](#)' files.

Next, go back to your snort sensor box and try this test to see if logging messages are sent to the OSSIM box (which will show up on the OSSIM box in [/var/log/snort/alert](#)):

```
logger -p local1.info "Test from OpenSUSE 12.3" <enter>
```

If this succeeds, you will see the following in `/var/log/snort/alert` on the OSSIM box:

Mar 28 08:04:08 xyzzzy bill: Test from OpenSUSE 12.3

The above message means that the system that snort is running on can send messages to the OSSIM 4.1 box via `rsyslog`.

In the OSSIM 4.1 system itself, use `'alienvault-setup'` as `root` and do the following:

scroll down to option 3 - Change Sensor Settings and hit `<enter>`

scroll down to option 3 - Enable/Disable detector plugins `<enter>`

scroll down to the `snort_syslog plugin`, and if there is no asterisk `'*'` next to it, hit the space bar to make an asterisk `'*'` appear.

After this, select `'OK'` and then option 7 - save and exit `<enter>`, which will cause OSSIM 4.1 to update the detection plug-ins.

Note - The enabling of the `snort_syslog plugin` can also be done as part of the OSSIM 4.1 installation process, you will be asked this if you select `'custom install'` when OSSIM 4.1 prompts you.

On the snort sensor box, you will need to modify `'snort.conf'`, but make a **backup copy of this file before proceeding (just in case)**.

In the `snort.conf` file, go down to the section marked `'Step #6'` and add the following lines so that it looks like the information below:

```
# syslog
output alert_fast: snort.fast
output alert_syslog: LOG_LOCAL1 LOG_INFO
```

This tells snort to write its local alerts to `'snort.fast'` in `/var/log/snort`, and that it will send any informational logs to the `LOG_LOCAL1` facility, which `rsyslog` will send to the OSSIM 4.1 sensor (if the logger test above succeeded).

Save and exit the `snort.conf` file.

Next, go to `/etc/sysconfig` and examine the `'snort'` file (this is a configuration file for snort on most linux based systems), and if the line `ALERTMODE=fast` appears, comment it out by using a `'#'` (hash) symbol at the front of the line. If you do NOT have this file, check the init script for snort to make sure that the `-A option` for snort startup is **NOT enabled** as this would cause snort to log events to `'alert'` in `/var/log/snort` rather than send them to the snort sensor.

Save and exit any files, and then [stop/start snort](#) to have it reprocess '[snort.conf](#)'. At this point, if all is working well, you should be able to send some test traffic to the snort sensor and the [alerts should show up in the OSSIM 4.1 web interface under the Dashboard](#), and they should appear in [/var/log/snort/alert](#) on the OSSIM 4.1 system, as shown below:

```
Mar 28 08:06:47 xyzyy snort[26801]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:42 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:43 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:44 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:45 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:46 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:47 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:48 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:49 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:50 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
Mar 28 08:06:51 foobar snort[2455]: [1:1000001:1] ICMP Ping Traffic Seen
[Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168.1.10 ->
192.168.1.40
```

As you can see, the IP address of the OSSIM 4.1 system (192.168.1.180) does not appear in the above traffic, but rather the source IP address of the machine I sent the ping test from (192.168.1.10) and the destination address of the snort sensor (192.168.1.40) is displayed.

If you go to the [Web Interface in OSSIM 4.1](#), under [Dashboards | Last SIEM vs Logger Events](#) (click on [Security Events](#)), you should see messages that have the following information displayed:

Signature	Date GMT-7:00	Sensor	Source	Destination
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:31	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:30	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:29	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:28	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:27	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:26	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:25	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:24	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:23	alienvault	Host-0800498c721c	
snort: Generic event Host-0800d484b21c	2013-04-11 08:54:22	alienvault	Host-0800498c721c	

If you move your mouse over the first Host entry, it will display the Source IP address, and if you move the mouse over the second Host entry, it will display the Destination IP address.

This document is a work-in-progress, and as more operating systems are tested with OSSIM 4.1, they will be added to this document.

Andrew Lemin provided a great deal of assistance in helping me to get alerts from snort to show up in OSSIM 4.1, and he is working on a more comprehensive document for Snort-2.9.5.x/OSSIM/OSSEC integration under BSD (Unix) based operating systems.

If you have any questions, comments, or suggestions, please email me at:

wp02855@gmail.com (wp02855 at gmail dot com)

Bill Parker