https://blog.rapid7.com/2017/06/30/how-to-install-and-configure-ossec-on-ubuntu-linux/

System Requirements

* Newly deployed Ubuntu 16.04 server.
* A static IP address 192.168.15.189 is configured on your server.
* Hostname localhost is setup on your server

Install Required Dependencies

First, you will need to update your system with the latest stable version. You can do this with the following command:

apt-**get** update -y

apt-**get** upgrade -y

OSSEC requires gcc, libc, apache and PHP. You can install all these packages with the following command:

apt-**get** install build-essential gcc make apache2 libapache2-mod-php7.0 php7.0 php7.0-cli php7.0-common apache2-utils unzip wget sendmail inotify-tools -y

Install OSSEC

First, download the latest version of the OSSEC from GitHub repository with the following command:

wget https://github.com/ossec/ossec-hids/archive/2.9.0.tar.gz

Once the download is completed, extract the downloaded file with the following command:

tar -xvzf 2.9.0.tar.gz

Next, change the directory to the extracted directory, then run install.sh to install OSSEC:

cd ossec-hids-2.9.0

sh install.sh

You will be prompted to answer some questions:

Select your language, if your language is English then type en and press Enter:

(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:en

You should see the following output:

OSSEC HIDS v2.9.0 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.

You must have a C compiler pre-installed **in** your system.

- System: Linux Node1 4.4.0-45-**generic**

- User: root

- Host: localhost

 -- Press ENTER to **continue** **or** Ctrl-C to abort. --

Press Enter, you should see the following output:

1- What kind of installation **do** you want (server, agent, **local**, hybrid **or** help)? **local**

Choose local to monitor the server it has been installed on then press Enter:

- Server installation chosen.

2- Setting up the installation environment.

- Choose **where** to install the OSSEC HIDS [/var/ossec]:

Choose OSSEC install location and press Enter:

- Installation will be made at /**var**/ossec .

3- Configuring the OSSEC HIDS.

3.1- Do you want e-mail notification? (y/n) [y]: y

Type y and press Enter if you want to get e-mail notification:

- What's your e-mail address? root@localhost

- We found your SMTP server as: 127.0.0.1

- Do you want to use it? (y/n) [y]: y

Type your local e-mail address and press Enter:

3.2- Do you want to run the integrity check daemon? (y/n) [y]:

 - Running syscheck (integrity check daemon).

Press Enter for integrity check daemon:

3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

 - Running rootcheck (rootkit detection).

Press Enter for rootkit detection engine:

- Do you want to enable active response? (y/n) [y]:

 - Active response enabled.

Press Enter to enable active response:

- Do you want to enable the firewall-drop response? (y/n) [y]:

 - firewall-drop enabled (**local**) **for** levels >= 6

Press Enter to enable the firewall-drop response:

- Default white list **for** the active response:

 - 192.168.15.1

- Do you want to **add** more IPs to the white list? (y/n)? [n]: n

Type n and press Enter if you don’t want to add white list:

3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]:

 - Remote syslog enabled.

Press Enter to enable remote Syslog:

- If you want to monitor any other file, just change the

ossec.conf **and** **add** a **new** localfile entry.

Any questions about the configuration can be answered

**by** visiting us online at http://www.ossec.net .

--- Press ENTER to **continue** ---

Finally, Press Enter to start installation. Once the installation succeeds, you should see the following output:

- System **is** Debian (Ubuntu **or** derivative).

- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:

 /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:

 /var/ossec/bin/ossec-control stop

- The configuration can be viewed **or** modified at /**var**/ossec/etc/ossec.conf

Thanks **for** **using** the OSSEC HIDS.

If you have any question, suggestion **or** **if** you find any bug,

contact us at contact@ossec.net **or** **using** **our** **public** maillist at

ossec-list@ossec.net

( http://www.ossec.net/main/support/ ).

More information can be found at http://www.ossec.net

--- Press ENTER to finish (maybe more information below). ---

- In order to connect agent **and** server, you need to **add** each agent to the server.

Run the 'manage\_agents' to **add** **or** **remove** them:

/var/ossec/bin/manage\_agents

Once the installation is completed, start OSSEC with the following command:

/var/ossec/bin/ossec-control start

You should see the following output:

Starting OSSEC HIDS v2.9 (**by** Trend Micro Inc.)...

Started ossec-maild...

Started ossec-execd...

Started ossec-analysisd...

Started ossec-logcollector...

Started ossec-syscheckd...

Started ossec-monitord...

Completed.

After starting OSSEC, you should also get an e-mail alert. You can check this with the following command:

mail

You should see the e-mail looks like the following:

[-- Message 3 -- 27 lines, 663 bytes --]:

From ossecm@localhost Sat Jun 17 21:25:11 2017

Message-Id: <201706171555.v5HFtBJu004798@localhost>

To: <root@localhost>

From: OSSEC HIDS <ossecm@localhost>

Date: Sat, 17 Jun 2017 21:25:11 +0530

Subject: OSSEC Notification - localhost - Alert level 3

OSSEC HIDS Notification.

2017 Jun 17 21:24:57

Received From: localhost->ossec-monitord

Rule: 502 fired (level 3) -> "Ossec server started."

Portion of the log(s):

ossec: Ossec started.

Now, OSSEC is working fine and will also send an e-mail alert.

Configure OSSEC

The default configuration of OSSEC works fine. The OSSEC mail configuration file is located inside /var/ossec/etc/ directory.
Now, open the OSSEC main configuration file ossec.conf using the following command:

nano /**var**/ossec/etc/ossec.conf

The first configuration options is the E-mail configurations which you specified during installation. You can change this setting at any time:

**<global>**

 **<email\_notification>**yes**</email\_notification>**

 **<email\_to>**root@localhost**</email\_to>**

 **<smtp\_server>**127.0.0.1**</smtp\_server>**

 **<email\_from>**ossecm@localhost**</email\_from>**

**</global>**

By default, OSSEC does not alert when a new file is added to the server. You can change that by adding a new line just under the section as shown below:

**<syscheck>**

 <!-- Frequency that syscheck is executed - default to every 22 hours -->

 **<frequency>**79200**</frequency>**

 **<alert\_new\_files>**yes**</alert\_new\_files>**

OSSEC does not send real-time alerts by default. You will also need to change is in the list to directories that OSSEC should check. By default, the directories are shown below:

<!-- Directories to check (perform all possible verifications) -->

**<directories** **check\_all**="yes"**>**/etc,/usr/bin,/usr/sbin**</directories>**

**<directories** **check\_all**="yes"**>**/bin,/sbin**</directories>**

You will need to modify the above two lines to make OSSEC report changes in real-time. Replace the both lines with the following:

**<directories** **report\_changes**="yes" **realtime**="yes" **check\_all**="yes"**>**/etc,/usr/bin,/usr/sbin**</directories>**

**<directories** **report\_changes**="yes" **realtime**="yes" **check\_all**="yes"**>**/var/www,/bin,/sbin**</directories>**

Save and close the file when you are finished.

Next, you will need to modify the rules file local\_rules.xml located inside /var/ossec/rules directory. This file contains rules for new file added to the system.

nano /**var**/ossec/rules/local\_rules.xml

Add the following lines between ... sections:

**<rule** **id**="554" **level**="7" **overwrite**="yes"**>**

 **<category>**ossec**</category>**

 **<decoded\_as>**syscheck\_new\_entry**</decoded\_as>**

 **<description>**File added to the system.**</description>**

 **<group>**syscheck,**</group>**

**</rule>**

Save and close the file when you are finished. Then restart OSSEC with the following command:

/var/ossec/bin/ossec-control restart

If all is well OSSEC restarts with no errors.

Install OSSEC Web UI

First, download the latest version of the OSSEC Web UI source from GitHub repository:

wget https://github.com/ossec/ossec-wui/archive/master.zip

After downloading, extract the downloaded file with the following command:

unzip master.zip

Next, move the extracted directory to the apache web root directory:

mv ossec-wui-master /**var**/www/html/ossec

Next, install OSSEC Web UI with the following command:

cd /**var**/www/html/ossec

./setup.sh

Answer all the questions as shown below:

trap: SIGHUP: bad trap

Setting up ossec ui...

Username: admin

New password:

Re-type **new** password:

Adding password **for** user admin

Enter your web server user name (e.g. apache, www, nobody, www-data, ...)

www-data

You must restart your web server after **this** setup **is** **done**.

Setup completed successfully.

Finally, restart apache with the following command:

systemctl restart apache2

Test OSSEC

Now OSSEC is up and running. It’s time to check OSSEC whether it is working or not.

Try to make some changes in /etc/network/interfaces, /etc/rc.local, /etc/fstab and /etc/aliases file.

After making changes, you should receive an e-mail alert saying that something changed to your system. You can check an e-mail with the following command:

mail

Check all the mails with Alert level 7, you should see the following alerts:

Integrity checksum changed **for**: '/etc/aliases'

Integrity checksum changed **for**: '/etc/fstab'

Integrity checksum changed **for**: '/etc/rc.local'

Integrity checksum changed **for**: '/etc/mail/aliases'

Integrity checksum changed **for**: '/etc/mail/aliases.db'

Integrity checksum changed **for**: '/etc/network/interfaces'

You can also check the OSSEC alert by accessing OSSEC Web UI.