FreeBSD Administration - Support #559

Install an OSSEC Server, Client, Web UI and Analogi Dashboard on FreeBSD

02/11/2015 03:33 PM - Daniel Curtis

Status:	Closed	**Start date:**	02/11/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Intrusion Detection/Prevention	**Estimated time:**	6.00 hours
Target version:	FreeBSD 9	**Spent time:**	11.50 hours

Description

OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. It also includes agentless monitoring for use with for example Cisco, HP or Juniper hardware.

This tutorial covers the installation of the OSSEC 2.8.0 server, the standard OSSEC Web UI and the Analogi dashboard on FreeBSD 9.2-RELEASE. It also covers OSSEC setup with MySQL support. Last but not least it shows you how to install the OSSEC agent on a *NIX system.

Pre-requisites

- Update the system and ports tree:

```
pkg update && pkg upgrade
portsnap fetch extract
```

- Install portmaster:

```
cd /usr/ports/ports-mgmt/portmaster
make install clean
pkg2ng
```

- Install py-htpasswd

```
portmaster security/py-htpasswd
```

Install OSSEC

- Install ossec-hids-server from ports:

```
portmaster security/ossec-hids-server
```

NOTE: Make sure to enable [X]MYSQL

Configure OSSEC

- Enable OSSEC service to start at boot:

```
echo 'ossechids_enable="YES"' >> /etc/rc.conf
```

- Edit the OSSEC config file:

```
vi /usr/local/ossec-hids/etc/ossec.conf
```

NOTE: The following settings are changed from the above file.

Configure mail settings

- Now let's configure the server the configuration. I modified the file to contain the following:

```
  <global>
    <email_notification>yes</email_notification>
    <email_to>admin@example.com</email_to>
    <smtp_server>smtp.example.com</smtp_server>
    <email_from>ossec@example.com</email_from>
  </global>
```

Configure syscheck

- Adjust the syscheck Interval - syscheck is OSSEC's integrity checking process and we can tell syscheck how often to scan and checksum the filesystem for evidence of unauthorized changes:

```
<syscheck>
    <!-- Frequency that syscheck is executed -- this is set to run every 12 hours -->
    <frequency>43200</frequency>
```

Specify Directories to Monitor

- Add/modify the directories to be monitored by OSSEC:

```
<!-- Directories to check  (perform all possible verifications) -->
    <directories report_changes="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories report_changes="yes" check_all="yes">/bin,/sbin</directories>
    <directories report_changes="yes" check_all="yes">/usr/local/etc,/usr/local/bin,/usr/local
/sbin</directories>
    <directories report_changes="yes" check_all="yes">/home/,/usr/local/home,/usr/local/www</d
irectories>
```

Specify Directories to Ignored

- Add/modify the directories to be ignored by OSSEC:

```
<!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/adjtime</ignore>
    <ignore>/etc/httpd/logs</ignore>
    <ignore>/etc/dumpdates</ignore>
    <ignore>/usr/local/ossec-hids/logs</ignore>
    <ignore>/usr/local/ossec-hids/queue</ignore>
    <ignore>/usr/local/ossec-hids/var</ignore>
    <ignore>/usr/local/ossec-hids/tmp</ignore>
    <ignore>/usr/local/ossec-hids/stats</ignore>
```

Configure Rootcheck

- The next stop in ossec.conf is the rootcheck section. Rootcheck is a component of OSSEC which scans the system for rootkits. Modify the section to match the following:

```
<rootcheck>
    <rootkit_files>/usr/local/ossec-hids/etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>/usr/local/ossec-hids/etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>
```

- Start OSSEC server:

```
service ossec-hids start
```

Specify Log Files to be Monitored

The files set in this example are:

1. /var/log/messages
2. /var/log/security
3. /var/log/auth.log
4. /var/log/maillog
5. /var/log/lpd-errs

- The code block below shows an example of what the modified lines should be. You will want to add log locations for the specific services you've installed and are running on the server; services like Nginx, Apache, etc.

```
<!-- Files to monitor (localfiles) -->

<localfile>

  <log_format>syslog</log_format>
    <location>/var/log/auth.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/security</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/messages</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/maillog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/lpd-errs</location>
  </localfile>
```

Adding Log File Entries with util.sh

Fixing the OSSEC util.sh script

- Open the util.sh file with vi:

```
vi /usr/local/ossec-hids/bin/util.sh
```

- Then replace ALL instances of **/var/ossec/etc/ossec.conf** with **/usr/local/ossec-hids/etc/ossec.conf**

- If you installed Nginx and its access and error log files are in the /var/log/nginx directory, you may add them to ossec.conf by using util.sh like so:

```
/usr/local/ossec-hids/bin/util.sh addfile /var/log/nginx/access.log
/usr/local/ossec-hids/bin/util.sh addfile /var/log/nginx/error.log
```

Alert on New Files

By default, OSSEC does not alert when new files are created in the system so we will change that behavior. There are two components to this change.

- Set syscheck - Scroll back up to the syscheck area os of ossec.conf and add an alertnewfiles line just under the frequency check interval:

```
<syscheck>
    <alert_new_files>yes</alert_new_files>
```

Modify the Rule's Classification Level

Although we've told syscheck to watch for newly created files, OSSEC won't actually notify us about them yet. For that we need to modify a default OSSEC rule.

- Open ossec_rules.xml:

```
vi /usr/local/ossec-hids/rules/ossec_rules.xml
```

  - The rule that fires when a file is added to a monitored directory is rule 554. Here's what it looks like:
    <rule id="554" level="0">
    <category>ossec</category>
    <decoded_as>syscheck_new_entry</decoded_as>
    <description>File added to the system.</description>
    <group>syscheck,</group>
    </rule>

- Open local_rules.xml This is where all user-modified OSSEC rules should go; you should **not** make changes to ossec_rules.xml

```
vi /usr/local/ossec-hids/rules/local_rules.xml
```

  - And add/modify the following change the notification level to 7 and tell OSSEC that this rule overwrites rule 554 from ossec_rules.xml. When done, the end of your local_rules.xml file should look like below. The first line is all that was changed from the original rule.

```
<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>

</group> <!-- SYSLOG,LOCAL -->

<!-- EOF -->
```

- Then restart OSSEC:

```
service ossec-hids restart
```

Install Nginx

- Install Nginx

```
portmaster www/nginx
```

- Start and enable nginx to start at boot:

```
echo 'nginx_enable="YES"' >> /etc/rc.conf
service nginx start
```

Install PHP

- Install PHP5 and other required packages:

```
portmaster lang/php5 databases/php5-mysql ftp/php5-curl graphics/php5-gd devel/pecl-intl devel
/pear graphics/pecl-imagick mail/php5-imap security/php5-mcrypt databases/pecl-memcached graph
ics/ming textproc/php5-pspell converters/php5-recode net-mgmt/php5-snmp databases/php5-sqlite3
 www/php5-tidy net/php5-xmlrpc textproc/php5-xsl
```

- Configure the default PHP settings

```
cp /usr/local/etc/php.ini-production /usr/local/etc/php.ini
```

Configure PHP-FPM

- Edit /usr/local/etc/php-fpm.conf:

```
vi /usr/local/etc/php-fpm.conf
```

  - Make the following changes:

```
events.mechanism = kqueue
listen = /var/run/php-fpm.sock
listen.owner = www
listen.group = www
listen.mode = 0666
```

- Enable PHP-FPM to start at boot:

```
echo 'php_fpm_enable="YES"' >> /etc/rc.conf
```

- Start PHP-FPM:

```
service php-fpm start
```

Configure Nginx to use PHP-FPM:

- Create a directory for a OSSEC Web UI:

```
mkdir /usr/local/www/ossec.example.com
```

- Edit /usr/local/etc/nginx/nginx.conf:

```
vi /usr/local/etc/nginx/nginx.conf
```

  - Add the following **ossec server block**:

```
server {
  listen       80;
  server_name  ossec.example.com;
  root         /usr/local/www/ossec-wui;
  access_log   /var/log/ossec.example.com-access.log;
  error_log    /var/log/ossec.example.com-error.log

  location / {
      index  index.php index.html index.htm;
  }

  # For all PHP requests, pass them on to PHP-FPM via FastCGI
  location ~ \.php$ {
     fastcgi_pass unix:/var/run/php-fpm.sock;
     fastcgi_param SCRIPT_FILENAME /usr/local/www/ossec-wui$fastcgi_script_name;
     fastcgi_param PATH_INFO $fastcgi_script_name;
     include fastcgi_params; # include extra FCGI params
  }
```

  - Add the following **analogi server block**:

```
server {
  listen       80;
  server_name  analogi.example.com;
  root         /usr/local/www/analogi;
  access_log   /var/log/analogi.example.com-access.log;
  error_log    /var/log/analogi.example.com-error.log

  location / {
      index  index.php index.html index.htm;
  }

  # For all PHP requests, pass them on to PHP-FPM via FastCGI
  location ~ \.php$ {
     fastcgi_pass unix:/var/run/php-fpm.sock;
     fastcgi_param SCRIPT_FILENAME /usr/local/www/analogi$fastcgi_script_name;
     fastcgi_param PATH_INFO $fastcgi_script_name;
     include fastcgi_params; # include extra FCGI params
  }
```

- Restart nginx:

```
service nginx restart
```

Install MariaDB

- Install MariaDB 5.5 server and client

```
portmaster databases/mariadb55-server databases/mariadb55-client
```

Configure MariaDB server

- Configure the MariaDB server

```
cp /usr/local/share/mysql/my-small.cnf /usr/local/etc/my.cnf
```

- Enable MariaDB to start at boot:

```
echo 'mysql_enable="YES"' >> /etc/rc.conf
```

- Start MariaDB

```
service mysql-server start
```

- Set password for mysql using the following command

```
mysql_secure_installation
```

- Restart mysql using the following commands:

```
service mysql-server restart
```

- Create a user and database for OSSEC. Open a MySQL shell:

```
mysql -u root -p
```

  - And run the following to create the **ossec** database with the **ossec_u** user

```
create database ossec;
grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.* to ossec_u;
set password for ossec_u = PASSWORD('SuperSecretPassword');
flush privileges;
quit;
```

Configure OSSEC database schema

The database also needs a schema. OSSEC provides the schema, it is located in the OSSEC github.

- Download latest OSSEC MySQL schema:

```
cd /usr/ports/security/ossec-hids-server/work/ossec-hids-2.8.1/src/os_dbd
```

- Import the schema into the ossec database:

```
mysql -u root -p ossec < mysql.schema
```

OSSEC MySQL configuration

- Add the database config to the ossec.conf file:

```
vi /usr/local/ossec-hids/etc/ossec.conf
```

  - And add the **database_output** block into the **ossec_config** block:

```
<ossec_config>
#...
    <database_output>
        <hostname>127.0.0.1</hostname>
        <username>ossec_u</username>
        <password>SuperSecretPassword</password>
        <database>ossec</database>
        <type>mysql</type>
    </database_output>
#...
</ossec_config>
```

- Enable the database in OSSEC:

```
/usr/local/ossec-hids/bin/ossec-control enable database
```

- And restart OSSEC:

```
service ossec-hids restart
```

Install OSSEC Web UI

- Download the web UI to /usr/local/www/ossec-wui:

```
cd /usr/local/www
git clone https://github.com/ossec/ossec-wui.git ossec-wui
mkdir -p /usr/local/www/ossec-wui/tmp/
chown -R www:www /usr/local/www/ossec-wui
chmod 666 /usr/local/www/ossec-wui/tmp/
```

- Make sure to add the **www** user to the ossec group, so nginx can access the ossec folder:

```
pw usermod www -G ossec
```

- Edit the ossec webui config:

```
vi /usr/local/www/ossec-wui/ossec_conf.php
```

  - And change the $ossec_dir path to the following:

```
/* Ossec directory */
$ossec_dir="/usr/local/ossec-hids";
```

- Change the ossec webui ownership to the nginx server:

```
chown -R www:www /usr/local/www/ossec-wui
```

- Run the setup script:

```
cd /usr/local/www/ossec-wui
./setup.sh
```

When correctly configured the OSSEC Web User Interface can be found at http://ossec.example.com/.

Install Analogi Web Dashboard

The Analogi dashboard is a nice and informative dashboard around OSSEC, which provides more visual information then the standard Web UI. The standard Web UI has better search functions, the Dashboard can be used for example on a Wall Mounted monitor and such.

WARNING: As of writing, 2/24/15, Analogi does not support OSSEC 2.8.

- Installation consists out of cloning the git repo and editing the settings file:

```
cd /usr/local/www/
git clone https://github.com/ECSC/analogi.git analogi
cp analogi/db_ossec.php.new analogi/db_ossec.php
vi analogi/db_ossec.php
```

- Edit the relevant settings for the MySQL database configuration:

```
define ('DB_USER_O', 'ossec_u');
define ('DB_PASSWORD_O', 'SuperSecretPassword');
define ('DB_HOST_O', '127.0.0.1');
define ('DB_NAME_O', 'ossec');
```

When correctly configured the Analogi web interface can be found at http://analogi.example.com/.

Client installation

Install the OSSEC client

Install OSSEC Client on FreeBSD

- Install OSSEC client on FreeBSD:

```
portmaster security/ossec-hids-client
```

- Start and enable ossec client:

```
echo 'ossechids_enable="YES"' >> /etc/rc.conf
```

```
service ossec-hids start
```

Install OSSEC Client on Debian

- Add the ossec alienvault repository key:

```
wget -O - http://ossec.alienvault.com/repos/apt/conf/ossec-key.gpg.key | apt-key add -
```

- Add OSSEC repository list:

```
echo “deb http://ossec.alienvault.com/repos/apt/debian wheezy main” >> /etc/apt/sources.list
```

- Install the OSSEC client:

```
apt-get update
apt-get install ossec-hids-agent
```

Generate a Client Key

Adding a client to OSSEC is quite simple. First you add the client to the server, which gives you a key. Then you add this key to the client, edit the config file on the client and that's it.

- First generate a key on the OSSEC server for this client. Do this by running:

```
/usr/local/ossec-hids/bin/manage_agents
```

  - Choose option **A**
  - Then entering the hostname: **client.example.com**
  - The IP: **10.0.0.4**
  - And **ID** (pressing enter will use the next available ID)

Retrieve the Client Key

- Next generate a key on the OSSEC server for this client. Do this by running:

```
/usr/local/ossec-hids/bin/manage_agents
```

  - Choose option **E**
  - Choose the ID number of the agent that the key will be generated for: **001**
  - Example output:

```
Agent key information for '001' is:
SD[...]AAUjd=
```

- Restart OSSEC for the new agents to take effect:

```
service ossec-hids restart
```

Install the Client Key

Install the Client Key on FreeBSD

- Switch to the OSSEC client and execute the manage_agents:

  ```
  /usr/local/ossec-hids/bin/manage_agents
  ```

  - Choose option **I**
  - Then paste the client key generated on the OSSEC server: **SD[...]AAUjd=**

- Edit the ossec config file:

  ```
  vi /usr/local/ossec-hids/etc/ossec.conf
  ```

  - And make sure the ossec server IP address is set:

    ```
    <client>
      <server-hostname>10.0.0.1</server-hostname>
    </client>
    ```

    Where 10.0.0.1 is your OSSEC server URL or IP.

- Now restart OSSEC on **both** the OSSEC server and the newly added client:

  ```
  service ossec-hids restart
  ```

Install the Client Key on Debian

- Switch to the OSSEC client and execute the manage_agents:

  ```
  /var/ossec/bin/manage_agents
  ```

  - Choose option **I**
  - Then paste the client key generated on the OSSEC server: **SD[...]AAUjd=**

- Edit the ossec config file:

  ```
  vi /var/ossec/etc/ossec.conf
  ```

  - And make sure the ossec server IP address is set:

    ```
    <client>
      <server-hostname>10.0.0.1</server-hostname>
    </client>
    ```

    Where 10.0.0.1 is your OSSEC server URL or IP.

- Now restart OSSEC on **both** the OSSEC server and the newly added client:

  ```
  service ossec restart
  ```

Repeat these steps for any client that needs to be added.

Bonus Tips

Here are a few bonus tips/config examples for OSSEC

Active Response

- If you've enabled Active Response you are protected from brute force attacks for ssh and some other pieces of software. Try it, login as a nonexistent user and check the web ui and logging:

```
tail -f /var/ossec/logs/active-responses.log
```

  - *Example output*:

```
Wed Jun 11 21:16:43 CEST 2014 /var/ossec/active-response/bin/host-deny.sh add - 198.211.118.121 1402514203.20760 5712
Wed Jun 11 21:16:43 CEST 2014 /var/ossec/active-response/bin/firewall-drop.sh add - 198.211.118.121 1402514203.20760 5712
```

Ignoring rules

- To very simply ignore rules based on rule id, add them to the XML file located in /usr/local/ossec-hids/rules/local_rules/xml, either on the ossec client for one machine or the ossec server to ignore on all machines:

```
<!-- Specify here a list of rules to ignore. -->
<!-- 3334 postfix start  -->
<!-- 3333 postfix stop -->
<rule id="100030" level="0">
    <if_sid>3333, 3334</if_sid>
    <description>List of rules to be ignored.</description>
</rule>
```

Monitoring additional log files

- The OSSEC agent by default only monitors a few log files. To add more, edit the /usr/local/ossec-hids/etc/ossec.conf file and add a line like this:

```
<localfile>
    <location>/var/log/*</location>
    <log_format>syslog</log_format>
</localfile>
```

This will add all files under /var/log. This might be a lot, you can also just add multiple <localfile> blocks with filenames.

Resources

- http://www.ossec.net/doc/
- https://raymii.org/s/tutorials/OSSEC_2.8.0_Server_Client_and_Analogi_Dashboard_on_Ubuntu.html
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-ossec-on-freebsd-10-1
- http://virtuallyhyper.com/2014/04/ossec-freebsd/* Add/modify the directories to be monitored by OSSEC:

History

#1 - 02/12/2015 08:03 PM - Daniel Curtis

- Description updated

#2 - 02/13/2015 01:09 PM - Daniel Curtis

- Subject changed from OSSEC Server, Client, Web UI and Analogi Dashboard on FreeBSD to Installing OSSEC Server, Client, Web UI and Analogi Dashboard on FreeBSD

- Description updated

- Status changed from New to In Progress

- % Done changed from 10 to 30

#3 - 02/13/2015 01:25 PM - Daniel Curtis

- Description updated

#4 - 02/14/2015 10:26 AM - Daniel Curtis

- Description updated

- % Done changed from 30 to 50

#5 - 02/14/2015 10:33 AM - Daniel Curtis

- Target version set to FreeBSD 9

#6 - 02/14/2015 12:10 PM - Daniel Curtis

- Category set to Intrusion Detection/Prevention

#7 - 02/14/2015 01:13 PM - Daniel Curtis

- Description updated

- % Done changed from 50 to 70

#8 - 02/14/2015 01:13 PM - Daniel Curtis

- Description updated

#9 - 02/14/2015 02:15 PM - Daniel Curtis

- Description updated

#10 - 02/17/2015 04:19 PM - Daniel Curtis

- Description updated

#11 - 02/17/2015 04:23 PM - Daniel Curtis

- Description updated

- % Done changed from 70 to 90

#12 - 02/17/2015 04:36 PM - Daniel Curtis

- Description updated

#13 - 02/17/2015 04:55 PM - Daniel Curtis

- Description updated

#14 - 02/17/2015 05:03 PM - Daniel Curtis

- Description updated

#15 - 02/17/2015 05:21 PM - Daniel Curtis

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

#16 - 02/17/2015 05:40 PM - Daniel Curtis

- Description updated

#17 - 02/18/2015 01:40 PM - Daniel Curtis

- Description updated

#18 - 02/22/2015 07:24 PM - Daniel Curtis

- Status changed from Resolved to Closed

#19 - 02/24/2015 07:32 PM - Daniel Curtis

- Description updated

#20 - 02/24/2015 08:32 PM - Daniel Curtis

- Description updated

#21 - 04/06/2015 08:43 PM - Daniel Curtis

- Subject changed from Installing OSSEC Server, Client, Web UI and Analogi Dashboard on FreeBSD to Install an OSSEC Server, Client, Web UI and Analogi Dashboard on FreeBSD

- Description updated

#22 - 04/06/2015 08:45 PM - Daniel Curtis

- Description updated

#23 - 04/11/2015 02:00 PM - Daniel Curtis

- Description updated