Chapter 3

OSSEC HIDS Configuration

Solutions in this chapter:

- **Understanding the OSSEC HIDS Configuration File**
- **Configuring Logging/Alerting Options**
- **Declaring Rule Files**
- **Reading Log Files**
- **Configuring Integrity Checking**
- **Configuring an Agent**
- **Configuring Advanced Options**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

After a long and restful weekend, Marty rushed into work to check on the newly deployed OSSEC HIDS agents and servers. To his pleasant surprise, all the test servers were still running and there were no indications of any errors. Looking at the logs collected by the OSSEC HIDS servers, Marty also noted that his scripted attacks were detected by the OSSEC HIDS agents and reported to the OSSEC HIDS server. His scripted modifications to critical system files and brute force authentication attacks were also reported. "I can't wait to tell Simran!" Marty thought. Marty scheduled a meeting to talk to Simran about the results of his testing, and she suggested involving the heads of some of the other departments, namely David Schuster and Antoine Joseph. David Schuster, the department head of operations, was responsible for the installation and maintenance of all servers, desktops, and networking equipment within the organization. Antoine Joseph, the department head for incident handling and response, was responsible for the monitoring of all systems within the organization and the teams deployed to "fight fires" in the event of an incident.

With Simran, Antoine, and David in the room, Marty began his presentation by familiarizing everyone with the current challenges and introducing the OSSEC HIDS as a solution. He explained how easy it is to deploy the OSSEC HIDS on multiple servers with different operating systems, how all events can be centralized to a single server, how additional servers can be added as the event load increased, and how alerts can be generated from the received events. "I've heard of applications like this in the past," said Antoine. "What benefit does my team get from this product besides something else to support? I need something that's going to alert me to potential incidents and not force me to sit someone in front of a dashboard 24/7." Marty smiled, as he knew Antoine was going to raise this question early in the meeting. "Actually Antoine, the OSSEC HIDS allows you to configure alerts to be sent to individual email addresses, email groups, and even SMS-enabled devices like a cell phone or pager." Marty paused to take a sip of water. "You can also configure the OSSEC HIDS to generate emails based on the severity of the alerts, the alert groupings, the subnet, or the agent. You can even limit the number of emails sent per hour so your analyst isn't inundated with emails about the same issue." Antoine nodded a couple of times to let everything sink in.

"OK," said David, "how does this OSSEC HIDS thing communicate between the agents and the server? I don't want to have to open up all kinds of special ports just so these things can communicate." Marty did his best not to roll his eyes, sigh, or react negatively in any way. In dealing with David before, Marty knew that David's primary concern was always opening new ports between network segments to allow communication between client and server application deployments. Marty understood that it was David's job to have such concerns, but that sometimes got in Marty's way when deploying new technologies around the network. "Well, I have good news for you, David!" exclaimed Marty with a smile. "This time, we can change the communication port on the agent and the server to whatever you need so we don't need to open any additional firewall rules if we don't want to." David smiled and

started to formulate his next question. "And if we pick a port that the firewall or NIDS tries to inspect" Marty jumped in to cut David's next question off before he asked it, "We can just create exclusion rules for those agents and the server." David let his smile slip away and tried to ask his final question, but Marty jumped in again. "And to answer your last question, David, the communication channels are encrypted so you don't have to worry about someone seeing the generated alerts from, say, the Web servers out on the DMZ." Simran looked at David and noticed he wasn't smiling, but, at the same time, wasn't upset. "Sounds good, Marty," said David. "It's also good to see you did your homework this time. An outsider might think that we may have had conversations like this before."

"What's the next step, Marty?" asked Simran. "Well, I think we should expand our test bed and get Antoine's team involved in some of the rule writing," responded Marty. "David, can you work with Marty on expanding this test environment?" Simran said, looking at David, "Involve whomever you need on your team to get this rolling." " Antoine," Simran shifted her focus, "once David and Marty have the agents and servers installed, can you bring your team together for a session so Marty can show them how to write the rules for alert generation?" Both David and Antoine looked at each other, nodded, and exclaimed "Can do, boss."

As with any intrusion detection system, or security software for that matter, there are important post-installation configurations you must perform. After you install the OSSEC HIDS, you might need to tweak and tune it according to your needs. The OSSEC HIDS has multiple configuration options that are covered this chapter. Additional configuration steps relating to specific parts of the OSSEC HIDS are covered in later chapters in this book.

Tools & Traps…

OSSEC HIDS File Locations

On a Unix, Linux, or BSD installation of the OSSEC HIDS, your default installation path is /var/ossec. Whichever directory was specified during installation, the OSSEC HIDS will chroot to that directory during startup and read the configuration files and rules from it.

Here is a list of all the OSSEC HIDS directories and files on a typical Unix, Linux, or BSD installation:

- */var/ossec/bin*—Directory containing all binaries used by the OSSEC HIDS.
- */var/ossec/etc*—Directory containing all configuration files needed by the OSSEC HIDS.

Continued

- *ossec.conf*—The main OSSEC HIDS configuration file.
- *internal_options.conf*—A file with additional configuration options.
- *decoders.xml*—A file containing decoders used to normalized the logs.
- *client.keys*—A file containing authentication keys used in agent/server communication.

- */var/ossec/logs*—Directory containing all OSSEC HIDS related log files.
  - *ossec.log*—OSSEC HIDS main logs (error, warn, info, and so on).
  - *alerts/alerts.log*—OSSEC HIDS alert log.
  - *active-responses.log*—OSSEC HIDS active response logs.
- */var/ossec/queue*—Directory containing OSSEC HIDS queue files.
  - *agent-info*—Directory containing agent specific information (operating system, OSSEC HIDS version, and so on).
  - *syscheck*—Directory containing integrity checking data with a separate log file for each agent.
  - *rootcheck*—Directory containing rootkit information and policy monitoring data for each agent.
  - *rids*—Directory containing agent message IDs.
  - *fts*—File containing first time seen (FTS) entries. For more information on FTS, see Chapter 4.
- */var/ossec/rules*—Directory containing all OSSEC HIDS rules.
- */var/ossec/stats*—Directory containing OSSEC HIDS statistical information such as number of logs per second, and so on.

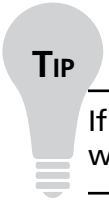
On the Windows installation, everything is located under *C:\Program Files\ossec-agent*, unless a different path is specified during installation:

- *C:\Program Files\ossec-agent\ossec.conf*—Main OSSEC HIDS configuration file.
- *C:\Program Files\ossec-agent\internal_options.conf*—Additional configuration options.
- *C:\Program Files\ossec-agent\ossec.log*—OSSEC HIDS main logs (*error*, *warn*, *info*, and so on).

Understanding the OSSEC HIDS Configuration File

To fully understand the OSSEC HIDS configuration file, we will start with the configuration options for the local/server installations on Unix, Linux, and BSD. After we thoroughly understand how local/server configurations are performed, we will discuss OSSEC HIDS agent configuration on Unix and Windows.

The main OSSEC HIDS configuration file, named *ossec.conf*, is an Extensible Markup Language (XML) based file. XML was chosen instead of a flat text configuration file for a couple of reasons. The primary reason is that XML files are easy to read and those with a working knowledge of the OSSEC HIDS should be able to find the section they're looking for. Another reason is that the XML format allows for easy-to-follow hierarchical nesting of tags, which makes it easier to figure out where the configuration starts, where it ends, and what section it's associated with. In addition, XML files are designed to be written programmatically and are able to be edited in anything from a text editor to an XML editing application.



TIP

If you are not familiar with XML, try some of the resources available at xml.org: www.xml.org/xml/resources_focus_beginnerguide.shtml.

The OSSEC HIDS configuration options are located in the *<ossec_config></ossec_config>* root tag. The configuration options are further divided into a series of subelements. Table 3.1 shows the subelement tags and what is contained in each section.

Table 3.1 ossec.conf Subelements

Subelement	Description
<global>	Global (general) configuration options used in server/ local installations
<alerts>	Email and log alerting options
<email_alerts>	Granular email alerting options
<remote>	Configuration options related to remote connections and agents (server only)
<database_output>	Database output options
<rules>	List of included rules

Continued

Table 3.1 Continued. ossec.conf Subelements

Subelement	Description
<client>	Agent related configuration options
<localfile>	Configuration options for monitored log files
<syscheck>	Configuration options for integrity checking
<rootcheck>	Configuration options for rootkit detection and policy monitoring
<command>	Configuration options for active-response
<active-response>	Additional configuration options for active-response

Configuring Logging/Alerting Options

The first step in configuring your OSSEC HIDS deployment is tuning the alert and log capabilities of the system. The OSSEC HIDS provides powerful email alerting capabilities with very granular control of the alert types generated.

Also included with the OSSEC HIDS is the ability to centralize events and logs from deployed OSSEC HIDS agents. Each agent can be configured to send events to an OSSEC HIDS server for further analysis and alert generation. If your deployment becomes quite large, or the events require long-term storage, the OSSEC HIDS can be configured to log to a database. Storing this information becomes important for your incident handling team to analyze large amounts of data. In addition, if your organization must achieve certain regulatory compliance goals, this long-term event storage becomes a requirement.

Alerting with Email

Every alert has a severity level from 0 to 15, with 15 being the highest and 0 the lowest. By default, the OSSEC HIDS logs every alert with a severity level of 1 to 15. In addition, the OSSEC HIDS generates email messages for every alert above a 7 severity level.

If you want to change how severity levels are handled, you must change the *<log_alert_level></log_alert_level>* and *<email_alert_level></email_alert_level>* tags in the *<alerts></alerts>* section. In the following example, we have switched the configuration to only log for severities above 2 and only send emails for severities above 8.

```
<ossec_config>
  <alerts>
    <log_alert_level>2</log_alert_level>
    <email_alert_level>8</email_alert_level>
  </alerts>
</ossec_config>
```

In addition to logging for every alert, or logging for every event that matches specific rules, you can configure the OSSEC HIDS to log everything received. Certain compliance regulations and industry standards, such as the Payment Card Industry (PCI) data security standard, Sarbanes-Oxley Act (SOX), and Health Insurance Portability and Accountability Act (HIPAA), among others, have specific requirements surrounding log collection and retention. Each regulation and act has detailed requirements, but if you decide to log everything, you can specify *yes* between the *<logall></logall>* tag in the *<global></global>* section.

```
<ossec_config>
  <global>
    <logall>yes</logall>
  </global>
</ossec_config>
```

WARNING

Just because you can log everything, does not mean you should. Storing information uses disk space, and the more information you log, the more space your saved logs use.

Configuring Email

Email alerts are an integral part of the OSSEC HIDS because email allows for rapid response in the event of an incident. Why would you want to wait until your administrator discovers an error, when you can send him an email immediately letting him know what happened?

Basic Email Configuration

In the *<global></global>* configuration section, you can specify which email addresses receive the generated email alerts.

NOTE

Whenever an alert has a severity higher than the *<log_alert_level>* option, an email is sent.

In the following example, we will configure the OSSEC HIDS to send emails to John and Mike, who are the security administrators of our fake company *fakeinc.com*. First, we must enable email notification using the *<email_notification></email_notification>* tag. Changing

the tag from *no* to *yes* enables the email notification functionality. After the tag is set to yes, we must then indicate the email addresses to receive our email alerts. We use the *<email_to></email_to>* tag to specify each alert recipient email address. The Simple Mail Transfer Protocol (SMTP) server must also be specified. Using the *<smtp_server></smtp_server>* tag, you can indicate which outbound SMTP server to use. The SMTP server can be specified using a fully qualified hostname or valid IPv4 IP address. Specify who is sending the email alert by using the *<email_from></email_from>* tag. Within the tag, specify an email address to associate with generated email alerts. This email address is the *From:* or *Sender:* address, depending on your email client, in the received email alert.

Finally, to safeguard our email server and avoid a flood of emails, we have configured a maximum threshold of 20 emails per hour using the *<email_maxperhour></email_maxperhour>* tag. If, within an hour, more than 20 emails are generated, the emails are grouped and sent together at the end of the hour.

```
<ossec_config>
  <global>
    <email_notification>yes</email_notification>
    <email_to>john@fakeinc.com</email_to>
    <email_to>mike@fakeinc.com</email_to>
    <smtp_server>smtpserver.fakeinc.com.</smtp_server>
    <email_from>ossecm@fakeinc.com</email_from>
    <email_maxperhour>20</email_maxperhour>
  </global>
</ossec_config>
```

To disable email notifications, simply change the *<email_notification></email_notification>* tag to *no*:

```
<ossec_config>
  <global>
    <email_notification>no</email_notification>
  </global>
</ossec_config>
```

Granular Email Configuration

If the basic email options are not enough, other options provide more granular email alerting capabilities. If you need your alert emails in a format suitable for Short Message Service (SMS), or text messaging for a cell phone or pager, or if you must alert only one administrator, there are granular email options to suit your needs.

In our company, *fakeinc.com*, we have an administrator, Peter, whose only responsibility is the security of Web servers on a network segment. Because his only responsibility is for those servers, we only want to alert him of Apache HTTP server alerts. The following granular

email configuration allows us to only send Peter email alerts for alerts that fall into the *apache* group of rules. Using the *<group></group>* tag, we can easily indicate what grouping of alerts should be sent to the specified email address:

```
<ossec_config>
  <email_alerts>
    <email_to>peter@fakeinc.com</email_to>
    <group>apache</group>
  </email_alerts>
</ossec_config>
```

We might also want to send an SMS for the on-call administrator, if the alert severity is above *10*. Using the *<level></level>* tag, we can indicate which severity level of email alerts should be emailed to the on-call administrator. The *sms* value, specified within the *<format></format>* tag, ensures that the sent emails are formatted for an SMS-capable device.

```
<ossec_config>
  <email_alerts>
    <email_to>oncall@fakeinc.com</email_to>
    <level>10</level>
    <format>sms</format>
  </email_alerts>
</ossec_config>
```

Finally, we have a Windows administrator who is responsible for the entire 10.1.1.0/24 network. His primary concern, however, is two critical Windows servers. The Windows servers, configured within the OSSEC HIDS as *win2k1* and *winxpAD*, both have OSSEC HIDS agents installed, as does every other server in the 10.1.1.0/24 subnet. Using the *<event_location></event_location>* tag ensures that an email alert is generated for any alert that occurs on the 10.1.1.0/24 subnet, the *win2k1* server, or the *winxpAD* server:

```
<ossec_config>
  <email_alerts>
    <email_to>cc@fakeinc.com</email_to>
    <event_location>win2k1|winxpAD|10.1.1</event_location>
  </email_alerts>
</ossec_config>
```

NOTE

Use the pipe "|" character to separate multiple event locations.

Receiving Remote Events with Syslog

An OSSEC HIDS server type installation allows for the collection of events from remote agents, as explained in Chapter 2, and from any system using syslog (TCP and UDP). To receive events from additional remote agents, you must add a new *<remote></remote>* section with *secure* defined within the *<connection></connection>* tag. This tag should already exist if you selected the server type installation.

```
<ossec_config>
  <remote>
    <connection>secure</connection>
  </remote>
</ossec_config>
```

We can also use the *<allowed-ips></allowed-ips>* tag to explicitly state which IP address we allow connections from. In the following example, we used the *<allowed-ips></allowed-ips>* tag in conjunction with the *<connection></connection>* tag to indicate that we expect OSSEC HIDS agent connections from the 192.168.10.0/24 network:

```
<ossec_config>
  <remote>
    <connection>secure</connection>
    <allowed-ips>192.168.10.0/24</allowed-ips>
  </remote>
</ossec_config>
```

For remote syslog, instead of specifying *secure* within the *<connection></connection>* tag, you must change it to *syslog*. Additionally, you must specify which IP addresses (or networks) are allowed to send syslog data to your OSSEC HIDS server. In the following example, we used the *<connection>syslog</connection>* tag to indicate that we allow syslog messages, and the *<allowed-ips></allowed-ips>* tag to define networks 192.168.2.0/24 and 192.168.1.0/24.

```
<ossec_config>
  <remote>
    <connection>syslog</connection>
    <allowed-ips>192.168.2.0/24</allowed-ips>
    <allowed-ips>192.168.1.0/24</allowed-ips>
  </remote>
</ossec_config>
```

Configuring Database Output

The OSSEC HIDS does not require a database to function, but you could find it useful to have all your alerts in a database. If you have multiple servers, it is beneficial to centralize all

your collected alert information. Table 3.2 shows the available options for configuring your OSSEC HIDS server to log to a database.

Table 3.2 Database Logging Configuration Options

Variable	Value	Description
<hostname>	Any valid IP address	IP address of the database server
<username>	Any valid username	Username to access the database
<password>	Any password	Password to access the database
<database>	Database name	Database name to store the alerts
<type>	Database type, options are *mysql* or *postgresql*	Type of database to use

Before you configure the database output, you must make sure the OSSEC HIDS is compiled to support database logging. To see how your OSSEC HIDS install was configured, run *ossec-dbd* with the *-V* flag. This indicates which database your currently installed OSSEC HIDS server will support.

```
# /var/ossec/bin/ossec-dbd -V

  OSSEC HIDS v1.4 - Daniel B. Cid
  Compiled with MySQL support.
  Compiled with PostgreSQL support.
```

If, for any reason, it says **Compiled without any Database support.**, you must reinstall the OSSEC HIDS with database support.

NOTE

Before you reinstall, make sure you have the necessary database libraries. See Chapter 1 for more information.

To enable database support during installation, you must run the following commands before the *install.sh* script:

```
$ cd ossec-hids-1.4
$ cd src; make setdb; cd ..
$ ./install.sh
```

To enable the database after the installation is complete, run the following command:

```
# /var/ossec/bin/ossec-control enable database
```

To configure the database support within the OSSEC HIDS, we must define the database settings using the *<database_output></database_output>* tag. In our example, we are using the server 192.168.2.32 as indicated by the *<hostname></hostname>* tag. We have also indicated that we are logging in to a MySQL server, as the *db_test* user, with password *db_pass1*, as noted within the *<type></type>*, *<username></username>*, and *<password></password>* tags. We also specify the database we want to connect to, *ossecdb*, within the *<database></database>* tag.

```
<ossec_config>
  <database_output>
    <hostname>192.168.2.32</hostname>
    <username>db_test</username>
    <password>db_pass1</password>
    <database>ossecdb</database>
    <type>mysql</type>
  </database_output>
</ossec_config>
```

NOTE

At the time of this writing, only the MySQL and PostgreSQL database are supported as valid database *<type>* variables.

After you have configured and restarted the OSSEC HIDS, you should see the following message in the /var/ossec/logs/ossec.log file, indicating that the OSSEC HIDS was successful in connecting to your specified database:

```
# /var/ossec/bin/ossec-control restart
# grep ossec-dbd /var/ossec/logs/ossec.log
2007/11/26 11:31:22 ossec-dbd: Connected to database 'ossecdb' at '192.168.2.32'.
2007/11/26 11:31:38 ossec-dbd: Started (pid: 8242).
```

Declaring Rule Files

The rules section, defined by the *<rules></rules>* tag, is used to declare which rule files are loaded when the OSSEC HIDS starts. Typically, these declarations will not need to be changed. There is only one valid tag, *<include></include>*, which allows you to specify which rule

file to load. Please note that every rule file must be located within the rules directory at /var/ossec/ rules/.

An example, from our default configuration, shows how these rule declaration statements are used.

```
<ossec_config> <!- rules global entry ->
  <rules>
    <include>rules_config.xml</include>
    <include>pam_rules.xml</include>
    <include>sshd_rules.xml</include>
  </rules>
<ossec_config>
```

To add more rules, you must add new *<include></include>* tag and specify the rule filename and extension. For example, the OSSEC HIDS policy rules ship disabled by default. To enable these rules, you must add a new *<include></include>* tag and specify the *policy_rules.xml* policy rules file.

```
<ossec_config> <!- rules global entry ->
  <rules>
    <include>policy_rules.xml</include>
  </rules>
<ossec_config>
```

If you want to know which rules are loaded when the OSSEC HIDS starts, you can investigate the *ossec.conf* file or look at your *ossec.log* file. When the OSSEC HIDS starts, a log entry is generated as each rule file is successfully loaded:

```
# grep "Reading rules file" /var/ossec/logs/ossec.log
…
2007/10/30 00:10:24 ossec-analysisd: Reading rules file: 'pix_rules.xml'
2007/10/30 00:10:24 ossec-analysisd: Reading rules file: 'named_rules.xml'
2007/10/30 00:10:24 ossec-analysisd: Reading rules file: 'smbd_rules.xml'
2007/10/30 00:10:24 ossec-analysisd: Reading rules file: 'vsftpd_rules.xml'
2007/10/30 00:10:24 ossec-analysisd: Reading rules file: 'pure-ftpd_rules.xml'
..
```

NOTE

The OSSEC HIDS rules are explained in more detail in Chapter 4.

Reading Log Files

When you install the OSSEC HIDS, a number of files, typically existing on the specified operating system, are automatically monitored. In some circumstances, depending on your operating system and file system structure, some files might not be automatically monitored. You do, however, have the ability to specify additional files for monitoring by the OSSEC HIDS.

NOTE

The ability to specify additional files is true of all OSSEC HIDS installation types.

To configure the OSSEC HIDS to monitor additional files, you must first use the *<localfile></localfile>* tag. After you have indicated that you want to monitor a new system file, you must specify the log format and file location. To specify the log format, you must use the *<log_format></log_format>* tag. Table 3.3 indicates the possible values for the *<localfile></localfile>* section, and Table 3.4 indicates the possible values for the *<log_format></log_format>* tag. The *<location></location>* tag allows you to indicate the location of the new file for monitoring. The following example shows how you would configure the OSSEC HIDS to monitor the /var/log/messages file:

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

The following example shows how you can configure the OSSEC HIDS to monitor a custom Apache log file; in this case, the /var/www/logs/server1/error_log file. Because this is an Apache log file, we can specify the corresponding value, *apache*, within the *<log_format></log_format>* tag:

```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/www/logs/server1/error_log</location>
  </localfile>
</ossec_config
```

NOTE

If you have an application that logs one log entry per line to a file, you can use the *syslog* log format within the *<log_format></log_format>* tag. This ensures that the file is properly handled by the OSSEC HIDS.

Another powerful feature of the OSSEC HIDS is the ability to specify *strftime* variables within the *<location></location>* tag. If you have a log file with a date as part of the filenaming scheme, and the file follows the format /var/log/custom-*YYYY-Mmm-DD*.log (for example, /var/log/custom-2007-Nov-06.log), you can easily monitor the file using:

```
<ossec_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/custom-%Y-%b-%d.log</location>
  </localfile>
</ossec_config
```

Tools & Traps…

Using *strftime* Expressions

The *strftime()* function within the C/C++ programming language allows you to return a string from your input data and format it according to the conversion specifiers you use. The conversion specifiers are typically seen as a percent sign, %, followed by a single uppercase or lowercase character. The OSSEC HIDS *<location></location>* tag allows you use these conversion specifiers to match on filenames. The supported conversion specifiers are:

%*a*—Abbreviated weekday name (e.g., **Thu**)
%*A*—Full weekday name (e.g., **Thursday**)
%*b*—Abbreviated month name (e.g., **Aug**)
%*B*—Full month name (e.g., **August**)
%*c*—Date and time representation (e.g., **Thu Sep 22 12:23:45 2007**)
%*d*—Day of the month (01–31) (e.g., **20**)
%*H*—Hour in 24 h format (00–23) (e.g., **13**)
%*I*—Hour in 12 h format (01–12) (e.g., **02**)
%*j*—Day of the year (001–366) (e.g., **235**)

Continued

%*m*—Month as a decimal number (01–12) (e.g., **02**)
%*M*—Minute (00–59) (e.g., **12**)
%*p*—AM or PM designation (e.g., **AM**)
%*S*—Second (00–61) (e.g., **55**)
%*U*—Week number with the first Sunday as the first day of week one (00–53) (e.g., **52**)
%*w*—Weekday as a decimal number with Sunday as 0 (0–6) (e.g., **2**)
%*W*—Week number with the first Monday as the first day of week one (00–53) (e.g., **21**)
%*x*—Date representation (e.g., **02/24/79**)
%*X*—Time representation (e.g., **04:12:51**)
%*y*—Year, last two digits (00–99) (e.g., **76**)
%*Y*—Year (e.g., **2008**)
%*Z*—Timezone name or abbreviation (e.g., **EST**)
%%—A % sign (e.g., **%**)

More information can be found at the following Web sites:

- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vclib/html/_crt_strftime.2c_.wcsftime.asp
- www.php.net/strftime
- www.cplusplus.com/reference/clibrary/ctime/strftime.html

Table 3.3 <localfile> Options

Options	Values	Description
<location>	Any log file (e.g., */var/log/messages*)	The full path and filename of file to be monitored by the OSSEC HIDS.
<log_format>	*syslog* *snort-full* *snort-fast* *squid* *iis* *eventlog* *nmapg* *mysql_log* *postgresql_log* *apache*	The format of the log file being read. If the log has one entry per line, the syslog type is recommended. Table 3.4 provides more details on each log format type.

Table 3.4 <log_format> Types

<log_format> Type	Description
syslog	Used to read generic syslog messages and any one-line-per-message log file (includes IIS, squid, apache, snort-fast, etc).
snort-full	Used to read Snort formatted logs that use the FULL output format.
snort-fast	Used to read Snort formatted logs that use the FAST output format.
squid	Used to read squid proxy server formatted logs.
iis	Used to read IIS formatted logs.
eventlog	Used to read Windows Event logs.
nmapg	Used to read nmap "greppable" formatted logs.
mysql_log	Used to read MySQL server formatted logs.
postgresql_log	Used to read PostgreSQL server formatted logs.
apache	Used to read Apache HTTP server formatted logs.

Configuring Integrity Checking

Integrity checking can be enabled on all OSSEC HIDS installation types (server, local, and agent). Integrity checking comes with a feature-rich default configuration that monitors all configuration files and binaries on Unix, Linux, and BSD operating systems (/etc, /bin, and so on), and monitors the system directory on Windows (C:\Windows\System32). The default configuration also monitors some key Windows registry entries for changes.

The integrity checking configuration is separated into three main tags. The *<frequency></frequency>* tag indicates how often syscheck should scan the system, in seconds, looking for changes.

The *<directories></directories>* tag lists the directories to monitor. Additional *checks* can be specified to only check file size changes, group ownership changes, etc. Table 3.5 explains all possible variable options for the <directories></directories> tag.

The *<ignore></ignore>* tag allows to you exclude files or directories from file integrity checks. The *<ignore></ignore>* tag has an additional simple regular expression variable called *sregex*. Table 3.6 explains the possible *sregex* options.

Table 3.5 *<directories></directories>* Options

Option	Description
check_all	Perform all available integrity checks
check_sum	Use MD5/SHA1 to check the integrity of files
check_size	Check files for size changes
check_owner	Check files for ownership changes
check_group	Check files for group ownership changes
check_perm	Check files for permission changes

Table 3.6 sregex Options

Option	Description
^	Specify the beginning of the text; e.g., <ignore type="sregex">^apache</ignore>
$	Specify the end of the text; e.g., <ignore type="sregex">.log$</ignore>
|	Specify an *OR* between multiple patterns; e.g., <ignore type="sregex">.log$\|.htm$</ignore>

The default configuration to monitor a Unix, Linux, or BSD operating system is:

```
<ossec_config>
  <syscheck>
    <frequency>86400</frequency>
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/bin,/sbin</directories>
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/mnttab</ignore>
  </syscheck>
</ossec_config>
```

NOTE

Multiple directories can be specified using a comma-separated list.

For example, if you wanted to monitor your Apache HTTP Web server files in the /var/www/htdocs/ directory, you would configure the *<syscheck></syscheck>* section and *<directories></directories>* tag as follows:

```
<ossec_config>
  <syscheck>
    <directories check_all="yes">/var/www/htdocs</directories>
  </syscheck>
</ossec_config>
```

On Windows, there are some more options available to monitor the Windows registry. The *<windows_registry></windows_registry>* tag allows you to specify a list of registry keys to monitor.

The *<registry_ignore></registry_ignore>* tag allows you to specify registry keys to exclude from integrity checking.

A sample configuration to monitor the *HKEY_LOCAL_MACHINE\Security* Registry key is:

```
<ossec_config>
  <syscheck>
    <windows_registry>HKEY_LOCAL_MACHINE\Security</windows_registry>
  </syscheck>
</ossec_config>
```

NOTE

The HKEY_LOCAL_MACHINE subtree contains information about the local computer system, including hardware and operating system data, such as bus type, system memory, device drivers, and startup control parameters. The Security key contains security information used by the system and network.

Tools & Traps…

Files Monitored in Windows by Default

The OSSEC HIDS monitors several key directories, files, and registry keys by default. The first declaration is that anything in the *system32* directory should be monitored.

Continued

The default Windows directory is called by using the %WINDIR% system variable.

```
<!-- Default files to be monitored - system32 only. -->
  <directories check_all="yes">%WINDIR%/system32</directories>
```

Several files within the system32 directory are excluded as they are constantly changing. If these directories were monitored, they might generate an excessive amount of events. Depending on your environment, you may choose to remove some of these exclusions so the files changes are reported to your OSSEC HIDS server.

```
<!-- Default files to be ignored. -->
  <ignore>%WINDIR%/System32/LogFiles</ignore>
  <ignore>%WINDIR%/system32/wbem/Logs</ignore>
  <ignore>%WINDIR%/system32/config</ignore>
  <ignore>%WINDIR%/system32/CatRoot</ignore>
  <ignore>%WINDIR%/system32/wbem/Repository</ignore>
  <ignore>%WINDIR%/system32/dllcache</ignore>
  <ignore>%WINDIR%/system32/inetsrv/History</ignore>
  <ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$</ignore>
```

Several important Windows registry keys are monitored for changes. These registry keys are related to policy, version, services, control, and security information. The Internet Explorer Registry information is also monitored.

```
<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Policies</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
CurrentVersion</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Security</windows_registry>
```

Quite a few registry keys are excluded, as they frequently change through regular use of a Windows operating system. Depending on your environment, you may choose to remove some of these exclusions so the registry key changes are reported to your OSSEC HIDS server.

```
<!-- Windows registry entries to ignore. -->
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Installer\UserData</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Group Policy\State</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\WindowsUpdate</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\Cache</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
CurrentVersion\ProfileList</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
CurrentVersion\Prefetcher</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Classes\Interface
</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Classes\TypeLib
</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Classes\MIME</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Classes\Software
</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Software\Classes\CLSID</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Security\Policy\Secrets</registry_
ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users
</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
DeviceClasses</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
Watchdog</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
MediaCategories</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
Windows</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
hivelist</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
ServiceCurrent</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print
</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager</registry_ignore>
```

Continued

```
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
Eventlog</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
RemoteAccess\Performance</registry_ignore>
<registry_ignore>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
W32Time\TimeProviders\NtpClient</registry_ignore>
<registry_ignore type="sregex">\Enum$</registry_ignore>
```

Configuring an Agent

The OSSEC HIDS agent does not perform any analysis or processing of alerts. All collected information is forwarded to the server for further processing and alert generation. The *<client></client>* configuration section allows you to specify your OSSEC HIDS server IP or hostname and the port used to send events.

The *<server-ip></server-ip>* tag allows you to specify the IP address of your OSSEC HIDS server using any valid IPv4 address. The *<server-hostname></server-hostname>* tag allows you to use a fully qualified hostname instead of an IP address. The *<port></port>* tag allows you to specify any port number, from 1 to 65535, to send events to your OSSEC HIDS server. This port number, that has a default value of 1514 if not explicitly defined, has to be the same port that is configured on your OSSEC HIDS server.

For example, to tell your agent that the OSSEC HIDS server is located at 192.168.1.1, and is configured to receive events on port 1519 instead of the default 1514 port, you can use the configuration as follows:

```
<client>
  <server-ip>192.168.1.1</server-ip>
  <port>1519</port>
</client>
```

If you know the fully qualified hostname, in this case *os1.fakeinc.com*, of your OSSEC HIDS server, you can use the configuration as follows:

```
<client>
  <server-hostname>os1.fakeinc.com</server-hostname>
  <port>1519</port>
</client>
```

Configuring Advanced Options

The main configuration of the OSSEC HIDS is located within the *ossec.conf* file. However, some advanced configuration features are located within the *internal_options.conf* file. These options, as stated within the configuration file, should be handled with care, as they are

responsible for runtime configurations. Any errors within this file may cause your OSSEC HIDS agent or server to not start if not properly configured.

Typically, this file is only used to enable advanced debugging of OSSEC HIDS issues. Table 3.7 describes the options and provides the default values in case you need to revert your changes.

Table 3.7 *internal_options.conf* Options

Option	Default Value	Description
analysisd.default_timeframe=	360	Default frequency used by rules that have "frequency" enabled. Default 360, Min 60, Max 3600.
analysisd.stats_maxdiff=	25000	Maximum difference on the number of alerts per hour in the stats alerting. Default 25000, Min 10, Max 99999.
analysisd.stats_mindiff=	250	Minimum difference on the number of alerts per hour in the stats alerting. Default 250, Min 10, Max 99999.
analysisd.stats_percent_diff=	30	How much to differ from the average number of alerts before alerting. Default 30, Min 5, Max 999.
analysisd.fts_list_size=	32	Size of the FTS list in memory. It is recommended that you do not change this value.
analysisd.fts_min_size_for_str=	14	FTS minimum string size. It is recommended that you do not change this value.
logcollector.loop_timeout=	2	How often *logcollector* checks for new entries in the logs. Default 2, Min 1, Max 999.
logcollector.open_attempts=	8	Number of attempts to open a file. Default 8, Min 0, Max 999.
remoted.recv_counter_flush=	128	How often *remoted* flushes agent message id counter entries to disk. It is recommended that you do not change this value.

Continued

Table 3.7 Continued. *internal_options.conf* Options

Option	Default Value	Description
remoted.comp_average_ printout=	19999	How often *remoted* should print the agent message id counter. It is recommended that you do not change this value.
maild.strict_checking=	1	Specifies if the internal OSSEC HIDS mail server should perform strict checking of the SMTP connection. This is enabled by default.
maild.groupping=	1	Specifies if the internal OSSEC HIDS mail server should group and send multiple alerts into one email message. This is enabled by default.
maild.full_subject=	0	Specifies if the internal OSSEC HIDS mail server should send the alert email with a verbose subject. This is disabled by default.
monitord.day_wait=	10	Amount of seconds to wait before compressing and signing the files. Default 10 seconds, Min 1, Max 999.
monitord.compress=	1	If the OSSEC HIDS should compress the logs after each day. This is enabled by default.
monitord.sign=	1	If the OSSEC HIDS should sign the logs at the end of each day. This is enabled by default.
monitord.monitor_agents=	1	If the OSSEC HIDS should monitor the agents and alert if any go offline. This is enabled by default.
syscheck.sleep=	2	Syscheck checking/usage speed. To avoid large CPU/memory usage, you can specify how long to sleep after generating the checksum of the specified number of files. The default sleep time is 2 seconds.

Continued

Table 3.7 Continued. *internal_options.conf* Options

Option	Default Value	Description
syscheck.sleep_after=	15	The number of files to generate checksums for before sleeping. The default number of files is 15.
dbd.reconnect_attempts=	10	Maximum number of reconnect attempts to the database. Default 10, Min 0, Max 999.
windows.debug=	0	Used to enable the debugging of Windows agents. This is disabled by default.
syscheck.debug=	0	Used to enable the debugging of the *syscheck* daemon. This is disabled by default.
remoted.debug=	0	Used to enable the debugging of the *remoted* daemon. This is disabled by default.
analysisd.debug=	0	Used to enable the debugging of the *analysisd* daemon. This is disabled by default.
logcollector.debug=	0	Used to enable the debugging of the *logcollector* daemon. This is disabled by default.
agent.debug=	0	Used to enable the debugging of the *agent* daemon. This is disabled by default.

NOTE

It is always good practice to back up your configuration file prior to making changes to it.

Summary

The OSSEC HIDS main configuration file, named *ossec.conf*, is an XML-based file that contains several sections and tags for configuring logging and alerting options, rule and log files, integrity checking and agents. To be able to fully use the OSSEC HIDS, you must have a thorough understanding of how the *ossec.conf* file is used.

With the *ossec.conf* file, you can set specific alerts to email specific people and log the alerts to a database for further analysis. For best support and response, the *ossec.conf* file can be set up for email notifications to a cell phone or pager using SMS.

The *<include>* tag within the *<rules>* section allows you to specify which rule files to load when the OSSEC HIDS starts. By declaring each file in the rule section, and placing each file in the */var/ossec/rules* directory, you ensure that alerts will be generated as defined by the selected rules.

The OSSEC HIDS can also be configured to read other, typically operating system specific, local log files. You simply specify the log format and file location in the *<localfile>* tag of the *ossec.conf* file to include a file for monitoring.

Integrity checking for all operating systems is handled by the *<syscheck>* section of the *ossec.conf* file. There are three main tags: *<frequency>*, *<directories>*, and *<ignore>* for all operating systems. On a Windows system, there are two additional tags, *<windows_registry>* and *<registry_ignore>*, which can be used to include or exclude specific registry keys for monitoring.

Because the OSSEC HIDS agent does not perform any analysis or processing of alerts, you must use the *<server-ip>* or *<server-hostname>* and *<port>* tags to indicate where the agent events are sent. These values represent the IP address and port of your OSSEC HIDS server.

Solutions Fast Track

Understanding the OSSEC HIDS Configuration File

- ☑ The main OSSEC HIDS configuration file is called *ossec.conf* and is typically located in the *etc/* directory where your OSSEC HIDS software is installed.
- ☑ The configuration file is an Extensible Markup Language (XML) based file to make it easy for users to tailor their OSSEC HIDS deployment for their environment.
- ☑ The OSSEC HIDS configuration options are located within the *<ossec_config>* tag. Additional configuration tags are divided into subelements within this root tag.

Configuring Logging/Alerting Options

- ☑ The OSSEC HIDS provides powerful email alerting capabilities with very granular control of the alert types generated.
- ☑ Events are sent to an OSSEC HIDS server, and alerts can be sent to recipients via email or SMS notifications. These alerts can also be written to a database.
- ☑ Remote events from deployed OSSEC HIDS agents or syslog events from third-party devices can be received by your OSSEC HIDS server.

Declaring Rule Files

- ☑ The rules section, defined by the *<rules></rules>* tag, is used to declare which rule files are loaded when the OSSEC HIDS starts.
- ☑ To add more rules, you must add a new *<include></include>* tag and specify the rule file name and extension.
- ☑ If you want to know which rules are loaded when the OSSEC HIDS starts, you can investigate the *ossec.conf* file or look at your *ossec.log* file.

Reading Log Files

- ☑ When you install the OSSEC HIDS, a number of files, typically existing on the specified operating system, are automatically monitored.
- ☑ To configure the OSSEC HIDS to monitor additional files, you must first use the *<localfile></localfile>* tag.
- ☑ If you have an application that logs one log entry per line to a file, you can use the syslog log format within the *<log_format></log_format>* tag. This ensures that the file is properly handled by the OSSEC HIDS.

Configuring Integrity Checking

- ☑ Integrity checking can be enabled on all OSSEC HIDS installation types (server, local, and agent).
- ☑ The integrity checking configuration is separated into three main tags: *<frequency>*, *<directories>*, and *<ignore>* for all operating systems.
- ☑ The *<windows_registry></windows_registry>* tag allows you to specify a list of registry keys to monitor, while the *<registry_ignore></registry_ignore>* tag allows you to specify a list of keys to ignore.

Configuring an Agent

- ☑ The OSSEC HIDS agent does not perform any analysis or processing of alerts.
- ☑ The <*server-ip*></*server-ip*> tag allows you to specify the IP address of your OSSEC HIDS server using any valid IPv4 address, while the <*server-hostname*> </*server-hostname*> tag allows you to use a fully qualified hostname instead of an IP address.
- ☑ The <*port*></*port*> tag allows you to specify any port number, from 1 to 65535, to send events to your OSSEC HIDS server.

Configuring Advanced Options

- ☑ Some advanced configuration features are located within the *internal_options.conf* file.
- ☑ Any errors within this file may cause your OSSEC HIDS agent or server to not start if not properly configured.
- ☑ It is always good practice to back up your configuration file prior to making changes to it.

Frequently Asked Questions

Q: Will I ever have to modify the *internal_options.conf* file?

A: It is very rare that you will ever have to modify the *internal_options.conf* file. It is recommended that you don't modify the file, as it contains internal options that, if edited incorrectly, might cause your OSSEC HIDS to not function properly. Generally, the *internal_options.conf* file is reserved for troubleshooting and debugging issues you might be having.

Q: Could the *ossec.conf* file ever get corrupted?

A: Like any text file, the *ossec.conf* could become corrupt if improperly modified. It is generally a good idea to back up your configurations to avoid any long-term downtime resulting from a corrupted configuration file.

Q: What will happen if the *ossec.conf* file is corrupted?

A: If your *ossec.conf* file becomes corrupted, the OSSEC HIDS will fail to start. The configuration file is needed for the OSSEC HIDS to function properly.

Q: If I have a remote agent, what information do I place within the <*remote*> tags? Is it an IP address?

A: The <*remote*> tag is used to declare what type of events the OSSEC HIDS server is receiving from that particular source. Using the <*connection*> tag, you can specify if the events are coming from an OSSEC HIDS agent using the **secure** option. To indicate that the source of the events is a syslog-based device, you must use the **syslog** option. To identify the source of the events, you must use the <*allowed-ips*> tag. This tag allows you to specify the IP address or network range, using CIDR notation, the events will be coming from.

Q: What type of information is emailed to a person when an alert is triggered?

A: The agent location, filename, description, rule level, rule description, rule id, event time, and the log (or message) that caused the alert.

Q: Can I customize the information that is emailed?

A: At the time of this writing, the OSSEC HIDS does not provide a mechanism to change the information that is sent in the alert email. This is, however, on the roadmap for a future release.

Q: If I decide to log all information to a database, is the information encrypted?

A: The information logged by the OSSEC HIDS is not encrypted in the database. This is being investigated further as a future possibility.

Q: When declaring rules files, what specific file types are supported?

A: The OSSEC HIDS rules files can have any file extension provided they are written using the OSSEC HIDS XML syntax.

Q: Is there a limit to the number of rules files I can include?

A: The OSSEC HIDS does not limit the number of rules you can use.

Q: How will I know if a rules file does not load successfully?

A: If a rules file fails to load, a corresponding message will be seen in the *ossec.log*.

Q: Can I monitor any type of local file?

A: Any type of local file can be monitored by the OSSEC HIDS.

Q: On a Windows system, do I have to give a specific location of the local file for monitoring?

A: When defining a local file for monitoring, you must ensure that you use the full path and filename.

Q: Can I monitor specific local files?

A: Yes, you can configure the OSSEC HIDS to monitor any file on the local file system where the agent is installed.

Q: Are spaces, periods, or any special characters acceptable when defining your directories in the integrity checking section?

A: When defining your *<directories></directories>* entries, you must ensure that you define valid directories. You can, however, use PATH variables (e.g., SYSTEM_ROOT) on Windows systems to specify directory locations.

Q: How will I know if I have incorrectly typed a registry key for integrity checking?

A: A corresponding log will be shown in the *ossec.log* indicating that the OSSEC HIDS was unable to read the registry key in question.

Q: When specifying information in the syscheck section, are the variables case sensitive?

A: If you are configuring your syscheck section for a Linux system, the variables are case sensitive. On Windows, they are not.

Q: Can I configure an agent for alert processing?

A: Only the OSSEC HIDS server can be configured for alert processing.

Q: If I have a remote agent, is there any special configuration I must perform other than specifying the server IP and port?

A: Only the OSSEC HIDS server IP address and port need be defined. You must, however, ensure that the authentication keys are properly created for the agent on the OSSEC HIDS server.

Q: For a remote agent, can I use the fully qualified hostname of the OSSEC HIDS server?

A: Yes, you can use the *<server-hostname></server-hostname>* tag in place of the *<server-ip></server-ip>* tag.