Configuration

Basic usage

Syscheck is configured in ossec.conf. If you want more information about detailed configuration options, go to Syscheck. Usually you use the following sections: frequency, directories, ignore, alert_new_files

To configure syscheck, a list of files and directories must be provided. The `check_all` option checks md5, sha1, owner, and permissions of the file.

```
<syscheck>
    <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
    <directories check_all="yes">/root/users.txt,/bsd,/root/db.html</directories>
</syscheck>
```

Configuring scheduled scans

Syscheck has an option to configure the frequency to scan the system. This is the `frequency` option. In this example we configure syscheck to run every 10 hours.

```
<syscheck>
  <frequency>36000</frequency>
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin</directories>
</syscheck>
```

Configuring real-time monitoring

Real-time monitoring is configured with the `realtime` option. This option only works with directories, not for individual files. Real-time change detection is paused during periodic syscheck scans, and reactivates as soon as scans complete.

```
<syscheck>
        <directories check_all="yes" realtime="yes">c:/tmp</directories>
</syscheck>
```

Configure to report changes

Using `report_changes` option, we can see what specifically changed in text files. Be careful about which folders you set up to `report_changes`, because in order to report changes, Wazuh must copy every single file you want to monitor to a private location.

```
<syscheck>
        <directories check_all="yes" realtime="yes" report_changes="yes">/test</directories>
</syscheck>
```

Configure to ignore files

Files and directories can be omitted using the ignore option (or registry_ignore for Windows registry entries): In order to avoid false positives, syscheck can be configured to ignore certain files that we don't want to monitor with `ignore` tag (or registry_ignore for Windows registry entries).

```
<syscheck>
    <ignore>/etc/random-seed</ignore>
    <ignore>/root/dir</ignore>
    <ignore type="sregex">.log$|.tmp</ignore>
</syscheck>
```

Ignoring files via rules

It is possible to ignore files using rules:

```
<rule id="100345" level="0">
    <if_group>syscheck</if_group>
    <match>/var/www/htdocs</match>
    <description>Ignore changes to /var/www/htdocs</description>
</rule>
```

Changing severity

With a custom rule it is possible to alter the level of a syscheck alert when changes to a specific file or file pattern are detected:

```
<rule id="100345" level="12">
    <if_group>syscheck</if_group>
    <match>/var/www/htdocs</match>
    <description>Changes to /var/www/htdocs - Critical file!</description>
</rule>
```