rootcheck

XML section name

```
<rootcheck>
</rootcheck>
```

Configuration options for policy monitoring and anomaly detection.

Options

- base_directory
- rootkit_files
- rootkit_trojans
- windows_audit
- system_audit
- windows_apps
- windows_malware
- scanall
- frequency
- disabled
- check_dev
- check_files
- check_if
- check_pids
- check_policy
- check_ports
- check_sys
- check_trojans
- check_unixaudit
- check_winapps
- check_winmalware
- skip_nfs

base_directory

The base directory that will be appended to the following options:

rootkit_files rootkit_trojans windows_malware windows_audit windows_apps systems_audit

Default value	/var/ossec
Allowed values	Path to a directory

rootkit_files

Change the location of the rootkit files database.

Default value	/var/ossec/etc/shared/rootkit_files.txt
Allowed values	A file with the rootkit files signatures

rootkit_trojans

Change the location of the rootkit trojans database.

Default value	/var/ossec/etc/shared/rootkit_trojans.txt
Allowed values	A file with the trojans signatures

windows_audit

Specifies the path to a Windows audit definition file.

Default value	n/a
Allowed values	Path to a Windows audit definition file

system_audit

Specifies the path to an audit definition file for Unix-like systems.

Default value	n/a
Allowed values	Audit definition file for Unix-like systems

windows_apps

Specifies the path to a Windows application definition file.

Default value	n/a
Allowed values	Path to a Windows application def. file

windows_malware

Specifies the path to a Windows malware definitions file.

Default value	n/a
Allowed values	Path to a Windows malware definitions file

scanall

Tells rootcheck to scan the entire system. This option may lead to some false positives.

Default value	no
Allowed values	yes, no

frequency

Frequency that the rootcheck is going to be executed (in seconds).

Default value	36000
Allowed values	A positive number (seconds)

disabled

Disables the execution of rootcheck.

Default value	no
Allowed values	yes, no

check_dev

Enable or disable the checking of /dev.

Default value	yes
Allowed values	yes, no

check_files

Enable or disable the checking of files.

Default value	yes
Allowed values	yes, no

check_if

Enable or disable the checking of network interfaces.

Default value	yes
Allowed values	yes, no

check_pids

Enable or disable the checking of process ID's.

Default value	yes
Allowed values	yes, no

check_policy

Enable or disable the checking of policy.

Default value	yes
Allowed values	yes, no

check_ports

Enable or disable the checking of network ports.

Default value	yes
Allowed values	yes, no

check_sys

Enable or disable checking for anomalous file system objects.

Default value	yes
Allowed values	yes, no

check_trojans

Enable or disable checking for trojans.

Default value	yes
Allowed values	yes, no

check_unixaudit

Enable or disable the checking of unixaudit.

Default value	yes
Allowed values	yes, no

check_winapps

Enable or disable the checking of winapps.

Default value	yes
Allowed values	yes, no

check_winaudit

Enable or disable the checking of winaudit.

Default value	1
Allowed values	0 , 1

check_winmalware

Enable or disable checking for Windows malware.

Default value	yes
Allowed values	yes, no

skip_nfs

Enable or disable the scanning of network mounted filesystems (Works on Linux and FreeBSD). Currently, skip_nfs will exclude checking files on CIFS or NFS mounts.

Default value	yes
Allowed values	yes, no

Default Unix configuration

```
<!-- Policy monitoring -->
  <rootcheck>
  <disabled>no</disabled>
  <check_unixaudit>yes</check_unixaudit>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>

  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>43200</frequency>

  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>

  <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
  <system_audit>/var/ossec/etc/shared/system_audit_ssh.txt</system_audit>
  <system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.txt</system_audit>

  <skip_nfs>yes</skip_nfs>
</rootcheck>
```