Documentation › User manual › Reference › Local configuration › syscheck

syscheck

XML section name

```
<syscheck>
</syscheck>
```

Configuration options for file integrity monitoring.

Options

- directories
- ignore
- nodiff
- frequency
- scan_time
- scan_day
- auto_ignore
- alert_new_files
- scan_on_start
- windows_registry
- registry_ignore
- prefilter_cmd
- skip_nfs

directories

Use this option to add or remove directories to be monitored. The directories must be comma separated.

All files and subdirectories within the noted directories will also be monitored.

Drive letters without directories are not valid. At a minimum the '.' should be included (`D:\.`).

This is to be set on the system to be monitored (or in the `agent.conf`, if appropriate).

Default value	/etc,/usr/bin,/usr/sbin,/bin,/sbin
Allowed values	Any directory

Atributes:

realtime	This will enable real-time/continuous monitoring on Linux (using the inotify system calls) and Windows systems. Real time only works with directories, not individual files.	
	Allowed values	yes, no
report_changes	Report file changes. This is limited to text files at this time.	
	Allowed values	yes, no
check_all	All the following check_* options are used together.	
	Allowed values	yes, no

check_sum	Check the MD5 and SHA-1 hashes of the files. Same as using both `check_sha1sum="yes"` and `check_md5sum="yes"`.	
	Allowed values	yes, no
check_sha1sum	Check only the SHA-1 hash of the files.	
	Allowed values	yes, no
check_md5sum	Check only the MD5 hash of the files.	
	Allowed values	yes, no
check_size	Check the size of the files.	
	Allowed values	yes, no
check_owner	Check the owner of the files. On Windows, uid will always be 0.	
	Allowed values	yes, no
check_group	Check the group owner of the files/directories. Available for UNIX. On Windows, gid will always be 0 and the group name will be blank.	
	Allowed values	yes, no
check_perm	Check the UNIX permission of the files/directories. On Windows, this will only check the POSIX permissions.	
	Allowed values	yes, no
check_mtime	Check the modification time of a file. **New in version 2.0.**	
	Allowed values	yes, no
check_inode	Check the file inode. Available for UNIX. On Windows, inode will always be 0. **New in version 2.0.**	
	Allowed values	yes, no
restrict	Limit checks to files containing the entered string in the file name. Any directory or file name (but not a path) is allowed	
	Allowed value	string

ignore

List of files or directories to be ignored (one entry per line). Multiple lines may be entered to include multiple files or directories. These files and directories are still checked, but the results are ignored.

Default value	/etc/mtab
Allowed values	Any directory or file name

Attributes:

type	This is a simple regex pattern to filter out files so alerts are not generated

	Allowed values	sregex

nodiff

List of files to not compute the diff (one entry per line). It could be used for sensitive files like a private key, credentials stored in a file or database configuration, avoiding data leaking by sending the file content changes through alerts.

Default value	/etc/ssl/private.key
Allowed values	Any file name

Attributes:

type	This is a simple regex pattern to filter out files so alerts are not generated	
	Allowed values	sregex

frequency

Frequency that the syscheck will be run (in seconds).

Default value	21600
Allowed values	A positive number, time in seconds

scan_time

Time to run the scans. Times may be represented as 21pm or 8:30.

Default value	n/a
Allowed values	Time of day

Note

This may delay the initialization of real-time scans.

scan_day

Day of the week to run the scans(one entry per line). Multiple lines may be entered to include multiple registry entries.

Default value	n/a
Allowed values	Day of the week

auto_ignore

Specifies whether or not syscheck will ignore files that change too many times (after the third change).

Default value	yes
Allowed values	yes, no

Note

It is valid on: server and local.

alert_new_files

Specifies if syscheck should alert when new files are created.

Default value	no

Allowed values	yes, no

Note

It is valid on: server and local.

scan_on_start

Specifies if syscheck scans immediately when started.

Default value	yes
Allowed values	yes, no

windows_registry

Use this option to monitor specified Windows registry entries (one entry per line). Multiple lines may be entered to include multiple registry entries.

Default value	HKEY_LOCAL_MACHINE\Software
Allowed values	Any registry entry

Atributes:

arch	Select the Registry view depending on the architecture.	
	Default value	32bit
	Allowed values	32bit, 64bit, both

Note

New entries will not trigger alerts, only changes to existing entries.

registry_ignore

List of registry entries to be ignored. (one entry per line). Multiple lines may be entered to include multiple registry entries.

Default value	..CryptographyRNG
Allowed values	Any registry entry

prefilter_cmd

Run to prevent prelinking from creating false positives.

Default value	n/a
Allowed values	Command to prevent prelinking

Example:

```
<prefilter_cmd>/usr/sbin/prelink -y</prefilter_cmd>
```

Note

This option may negatively impact performance as the configured command will be run for each file checked.

skip_nfs

Specifies if syscheck should scan network mounted filesystems (Works on Linux and FreeBSD). Currently, skip_nfs will exclude checking files on CIFS or NFS mounts.

Default value	no
Allowed values	yes, no

Default Unix configuration

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

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

  <scan_on_start>yes</scan_on_start>

  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 3 times -->
  <auto_ignore>no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories check_all="yes">/bin,/sbin,/boot</directories>

  <!-- 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/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>

  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>

  <skip_nfs>yes</skip_nfs>
</syscheck>
```