File integrity monitoring

File integrity monitoring is the capability that allows us to know if any file has changed. The component responsible for this task is called **syscheck**. This component compares the cryptographic checksum and other attributes of a known good file or Windows registry key against the checksum and attributes of the same after it has been modified.

Contents

- How it works
- Configuration
  - Basic usage
  - Configuring scheduled scans
  - Configuring real-time monitoring
  - Configure to report changes
  - Configure to ignore files
  - Ignoring files via rules
  - Changing severity
- FAQ
  - How often does syscheck run?
  - What is the CPU usage like on the agents?
  - Where are all the checksums stored?
  - Can I ignore files in a directory?
  - Can Wazuh report changes in the content of a text file?
  - How does Wazuh verify the integrity of files?
  - Does Wazuh monitor any directories by default?
  - Can I force an immediate syscheck scan?
  - Does Syscheck start when Wazuh start?
  - Does Wazuh alert when a new file is created?