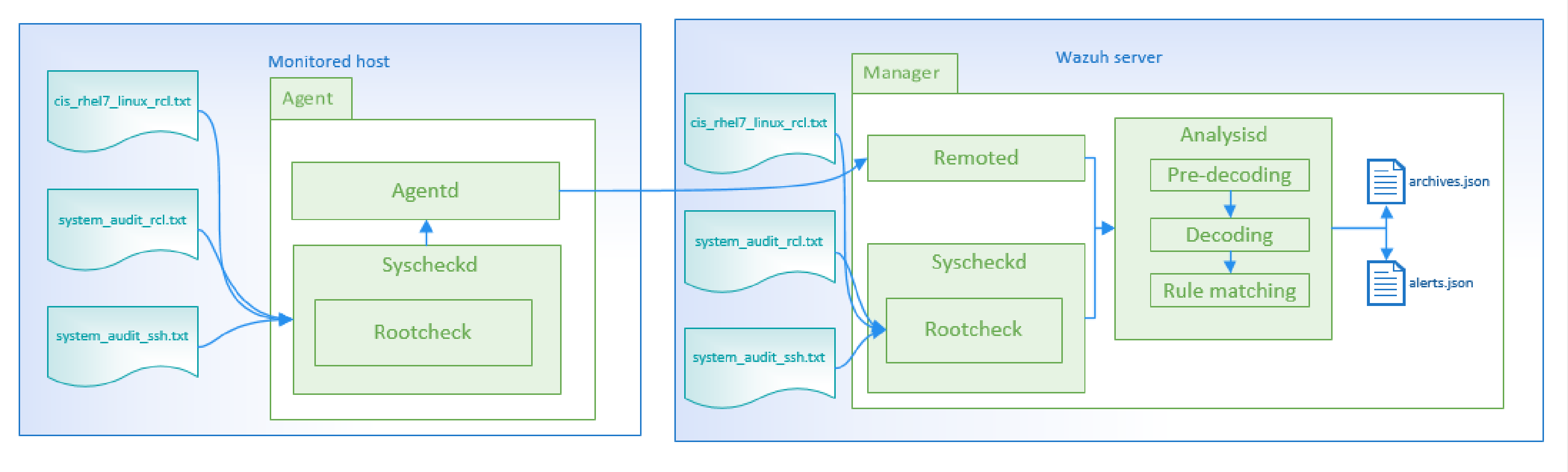
# How it works

*Rootcheck* allows to define policies in order to check if the agents meet the requirement specified.



The *rootcheck* engine can perform the following checks:

- check if a process is running
- check if a file is present
- check if the content of a file contains a pattern, or if a Windows registry key contains a string or is simply present.

Using these checks, the following policies have been developed:

| Policy | Description |
|---|---|
| cis_debian_linux_rcl.txt | Based on CIS Benchmark for Debian Linux v1.0 |
| cis_rhel5_linux_rcl.txt | Based on CIS Benchmark for Red Hat Enterprise Linux 5 v2.1.0 |
| cis_rhel6_linux_rcl.txt | Based on CIS Benchmark for Red Hat Enterprise Linux 6 v1.3.0 |
| cis_rhel7_linux_rcl.txt | Based on CIS Benchmark for Red Hat Enterprise Linux 7 v1.1.0 |
| cis_rhel_linux_rcl.txt | Based on CIS Benchmark for Red Hat Enterprise Linux v1.0.5 |
| cis_sles11_linux_rcl.txt | Based on CIS Benchmark for SUSE Linux Enterprise Server 11 v1.1.0 |
| cis_sles12_linux_rcl.txt | Based on CIS Benchmark for SUSE Linux Enterprise Server 12 v1.0.0 |
| system_audit_rcl.txt | Web vulnerabilities and exploits |
| win_audit_rcl.txt | Check registry values |
| system_audit_ssh.txt | SSH Hardening |
| win_applications_rcl.txt | Check if malicious applications are installed |

Alerts related to policy monitoring:

- 512: Windows Audit
- 514: Windows Application
- 516: Unix Audit

The policy and compliance monitoring databases are normally maintained on the manager, which distributes them to all the agents.

Example of an existing policy rule:

```
# PermitRootLogin not allowed
# PermitRootLogin indicates if the root user can log in via ssh.
$sshd_file=/etc/ssh/sshd_config;

[SSH Configuration - 1: Root can log in] [any] [1]
f:$sshd_file -> !r:^# && r:PermitRootLogin\.+yes;
f:$sshd_file -> r:^#\s*PermitRootLogin;
```

Alert example:

```
** Alert 1487185712.51190: - ossec,rootcheck,
2017 Feb 15 11:08:32 localhost->rootcheck
Rule: 516 (level 3) -> 'System Audit event.'
System Audit: CIS - RHEL7 - 6.2.9 - SSH Configuration - Empty passwords permitted {CIS: 6.2.9 RHEL7}
{PCI_DSS: 4.1}. File: /etc/ssh/sshd_config. Reference:
https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v1.1.0.pdf .
title: CIS - RHEL7 - 6.2.9 - SSH Configuration - Empty passwords permitted
file: /etc/ssh/sshd_config
```