Configuration

1. Basic usage
2. Configure periodic scans
3. Root access to SSH

Basic usage

To configure the options for rootcheck, go to the Rootcheck section in ossec.conf. The most common configuration options are: frequency and system-audit

Basic example to configure audit polices:

```
<rootcheck>
  <system_audit>./db/system_audit_rcl.txt</system_audit>
  <system_audit>./db/cis_debian_linux_rcl.txt</system_audit>
  <system_audit>./db/cis_rhel_linux_rcl.txt</system_audit>
</rootcheck>
```

Configure periodic scans

This is a basic configuration to run a scan every 10 hours.

```
<rootcheck>
   <frequency>36000</frequency>
   <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_debian_linux_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_rhel_linux_rcl.txt</system_audit>
   <system_audit>/var/ossec/etc/shared/cis_rhel5_linux_rcl.txt</system_audit>
 </rootcheck>
```

Root access to SSH

1. First you need to create your custom audit file (audit_test.txt):

```
# PermitRootLogin not allowed
# PermitRootLogin indicates if the root user can log in by 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;
```

2. Reference our new file in the rootcheck options:

```
<rootcheck>
   <system_audit>/var/ossec/etc/shared/audit_test.txt</system_audit>
</rootcheck>
```