

4.1 Configure System Accounting (auditd)

List of content

- 4.1.1 Configure Data Retention
 - 4.1.1.1 Ensure audit log storage size is configured (Not Scored)
 - 4.1.1.2 Ensure system is disabled when audit logs are full (Scored)
 - 4.1.1.3 Ensure audit logs are not automatically deleted (Scored)
- 4.1.2 Ensure auditd service is enabled (Scored)
- 4.1.3 Ensure auditing for processes that start prior to auditd is enabled (Scored)
- 4.1.4 Ensure events that modify date and time information are collected (Scored)
- 4.1.5 Ensure events that modify user/group information are collected (Scored)
- 4.1.6 Ensure events that modify the system's network environment are collected (Scored)
- 4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected (Scored)
- 4.1.8 Ensure login and logout events are collected (Scored)
- 4.1.9 Ensure session initiation information is collected (Scored)
- 4.1.10 Ensure discretionary access control permission modification events are collected (Scored)
- 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected (Scored)
- 4.1.12 Ensure use of privileged commands is collected (Scored)
- 4.1.13 Ensure successful file system mounts are collected (Scored)
- 4.1.14 Ensure file deletion events by users are collected (Scored)
- 4.1.15 Ensure changes to system administration scope (sudoers) is collected (Scored)
- 4.1.16 Ensure system administrator actions (sudolog) are collected (Scored)
- 4.1.17 Ensure kernel module loading and unloading is collected (Scored)
- 4.1.18 Ensure the audit configuration is immutable (Scored)

Description

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, `auditd` will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations.

Note: For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems. For 32 bit systems, only one rule is needed.

Note: Once all configuration changes have been made to `/etc/audit/audit.rules`, the `auditd` configuration must be reloaded:

```
# service auditd reload
```

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/centos7/4/1>

Last update: **2017/05/06 14:18**

