4.1.15 Ensure changes to system administration scope (sudoers) is collected (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers` will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier “scope.”

Rationale

Changes in the `/etc/sudoers` file can indicate that an unauthorized change has been made to scope of system administrator activity.

Audit

Run the following command and verify output matches:

```
# grep scope /etc/audit/audit.rules
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Remediation

Add the following line to the `/etc/audit/audit.rules` file:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/ubuntu1604/4/1/15

Last update: **2017/05/02 23:00**