

4.1.1.1 Ensure audit log storage size is configured (Not Scored)

Profile Applicability

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

Description

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit

Run the following command and ensure output is in compliance with site policy:

```
# grep max_log_file /etc/audit/auditd.conf  
max_log_file = <MB>
```

Remediation

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

Notes

The `max_log_file` parameter is measured in megabytes.

From:

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

Permanent link:

<https://secscan.acron.pl/ubuntu1604/4/1/1/1>

Last update: **2017/05/02 13:33**

