4.1.1 Configure Data Retention

List of content

Description

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

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

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

Last update: **2017/05/06 14:39**