Migration of audit messages from snoopy to auditd

Author : admin

his article may be out of date and may be deleted in the future.

This article explains the migration from the previous service "Snoopy" to "Auditd". Only commands that are executed as a user with root rights should be recorded here.

Uninstall/disable snoopy

Configuration of auditd

Files needed
Auditd start/stop script

/etc/init.d/auditd

Rules for monitoring by auditd

/etc/audit/audit.rules

Auditd plugin for syslog service

/etc/audisp/plugins.d/syslog.conf

Edit the **/etc/audit/audit.rules** file
Auditd can be specifically configured to capture and exclude messages. The following list is helpful for excluding certain event entries ("**msgtype**"):

** 1000 - 1099 are for commanding the audit system*
** 1100 - 1199 user space trusted application messages*
** 1200 - 1299 messages internal to the audit daemon*
** 1300 - 1399 audit event messages*
** 1400 - 1499 kernel SE Linux use*
** 1500 - 1599 AppArmor events*
** 1600 - 1699 kernel crypto events*
** 1700 - 1799 kernel abnormal records*
** 1800 - 1999 future kernel use (maybe integrity labels and related events)*
** 2001 - 2099 unused (kernel)*
** 2100 - 2199 user space anomaly records*
** 2200 - 2299 user space actions taken in response to anomalies*

** 2300 - 2399 user space generated LSPP events*
** 2400 - 2499 user space crypto events*
** 2500 - 2999 future user space (maybe integrity labels and related events)*

Adding the rules

In order for auditd to record the desired events, rules must be defined.

List of rules set up

Below is a list and explanation of the rules set up:

-a exclude,always -F msgtype>=2400 -F msgtype