# 20.2.2 Практическое задание

1. Составьте конфиг *auditd* такой, чтобы:
   * + логировать **изменение** файлов в */etc, /home, /root, /var/spool/cron, /var/spool/at, /boot*;
     + логировать все *syscall execve, execveat*, кроме */lib/systemd/systemd-logind*.
   1. Проверить конфиг, выполнив изменение каких-либо файлов в */etc* (поправить какой-либо конфиг, например).
   2. Найти события, связанные с изменением конфига с помощью любой из утилит.

Ответ предоставить в виде отчёта по пунктам, конфиг и найденные логи приложить отдельными текстовыми файлами с названиями (расширение можно любое) — auidtd.config (в этот файл необходимо приложить конфиг), event\_log (в этот файл приложить отфильтрованные события, которые относятся к изменению каких-либо конфигов). В отчёте необходимо прописать команды, с помощью которых вы производили поиск, и логику (что искали) и что нашли.

Например:

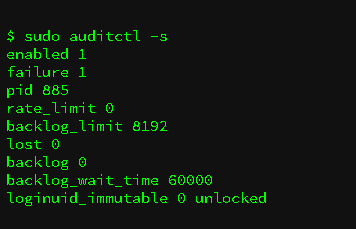
*Использовал cat /var/log/audit | grep “execve” — искал все вызовы syscall execve, с целью дальнейшей их фильтрации по имени исполняемого файла. Поиск с помощью grep мне не подошёл — неудобно смотреть события, поэтому решил воспользоваться утилитой aureport с ключами...*

1. Уста­новим и нас­тро­им все под­систе­мы ауди­та.

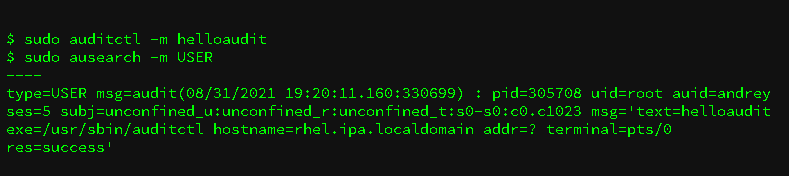
sudo dnf install audit

sudo systemctl enable --now auditd

Ста­тус работы под­систе­мы ауди­та:



Для тес­та есть воз­можность отпра­вить тек­сто­вое сооб­щение в под­систе­му ауди­та и убе­дить­ся, что соот­ветс­тву­ющее событие попало в жур­нал ауди­та.



Отслеживать доступ к файлам и попытки их изменения:

auditctl -w /etc/ -p wa

auditctl -w /home/ -p wa

auditctl -w /root/ -p wa

auditctl -w /var/spool/cron -p wa

auditctl -w /var/spool/at -p wa

auditctl -w /boo -p wa

Изменения конфигурации вступят в силу после перезапуска демона auditd:

sudo service auditd restart

Для удобства парсинга воспользуемся утилитой aureport.

sudo aureport -s execve