root@ubuntuWebServer:~# sudo auditctl -a exit,always -F path=/etc/passwd -F perm=rwa

root@ubuntuWebServer:~# ausearch -f /etc/passwd

----

time->Fri Apr 27 17:25:14 2018

type=PROCTITLE msg=audit(1524875114.559:104): proctitle=7375646F00617564697463746C002D6100657869742C616C77617973002D4600706174683D2F6574632F706173737764002D46007065726D3D727761

type=PATH msg=audit(1524875114.559:104): item=0 name="/etc/passwd" inode=787237 dev=fc:01 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL

type=CWD msg=audit(1524875114.559:104): cwd="/root"

type=SYSCALL msg=audit(1524875114.559:104): arch=c000003e syscall=2 success=yes exit=4 a0=7f3c361c0c50 a1=80000 a2=1b6 a3=80000 items=1 ppid=22033 pid=22047 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=9 comm="sudo" exe="/usr/bin/sudo" key=(null)

root@ubuntuWebServer:~# auditctl -R /etc/audit/audit.rules

No rules

enabled 1

failure 1

pid 21794

rate\_limit 0

backlog\_limit 320

lost 10

backlog 1

backlog\_wait\_time 15000

root@ubuntuWebServer:~# autrace /bin/ls /tmp

Waiting to execute: /bin/ls

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-dovecot.service-UZRAvR

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-systemd-timesyncd.service-iM2ATP

vmware-root

Cleaning up...

Trace complete. You can locate the records with 'ausearch -i -p 22066'

root@ubuntuWebServer:~# auditctl -D

No rules

root@ubuntuWebServer:~# autrace /bin/ls /tmp

Waiting to execute: /bin/ls

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-dovecot.service-UZRAvR

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-systemd-timesyncd.service-iM2ATP

vmware-root

Cleaning up...

Trace complete. You can locate the records with 'ausearch -i -p 22073'

Waiting to execute: /bin/ls

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-dovecot.service-UZRAvR vmware-root

systemd-private-b9d6901dd6fd4e1393f1a62773a5402b-systemd-timesyncd.service-iM2ATP

Cleaning up...

Trace complete. You can locate the records with 'ausearch -i -p 22178'

root@ubuntuWebServer:~# ausearch --start recent -p 22178 --raw | aureport --file --summary

File Summary Report

===========================

total file

===========================

6 /etc/ld.so.nohwcap

2 /tmp

1 /bin/ls

1 /lib64/ld-linux-x86-64.so.2

1 /etc/ld.so.preload

1 /etc/ld.so.cache

1 /lib/x86\_64-linux-gnu/libselinux.so.1

1 /lib/x86\_64-linux-gnu/libc.so.6

1 /lib/x86\_64-linux-gnu/libpcre.so.3

1 /lib/x86\_64-linux-gnu/libdl.so.2

1 /lib/x86\_64-linux-gnu/libpthread.so.0

1 /sys/fs/selinux

1 /selinux

1 /proc/filesystems

1 /usr/lib/locale/locale-archive