```
bmsce@Ubuntu:~$ sudo apt-get install syslog-ng-core
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:

The following packages have unmet dependencies:
 syslog-ng-core : Depends: libjson-c4 (>= 0.13.1) but it is not installable
                  Depends: libssl1.1 (>= 1.1.1) but it is not installable
E: Unable to correct problems, you have held broken packages.
```

```
bmsce@Ubuntu:~$ sudo apt-get install syslog-ng-core
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libestr0 libfastjson4 linux-headers-6.2.0-34-generic
  linux-hwe-6.2-headers-6.2.0-34 linux-image-6.2.0-34-generic
  linux-modules-6.2.0-34-generic linux-modules-extra-6.2.0-34-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libivykis0
Suggested packages:
  syslog-ng-mod-sql syslog-ng-mod-mongodb syslog-ng-mod-smtp
  syslog-ng-mod-amqp syslog-ng-mod-geoip2 syslog-ng-mod-redis
  syslog-ng-mod-stomp syslog-ng-mod-riemann syslog-ng-mod-graphite
  syslog-ng-mod-python syslog-ng-mod-add-contextual-data syslog-ng-mod-getent
  syslog-ng-mod-stardate syslog-ng-mod-map-value-pairs syslog-ng-mod-snmp
  syslog-ng-mod-xml-parser syslog-ng-mod-http syslog-ng-mod-rdkafka
  syslog-ng-mod-extra syslog-ng-mod-examples syslog-ng-mod-slog
The following packages will be REMOVED:
```

```
bmsce@Ubuntu:~$ sudo systemctl start syslog-ng
bmsce@Ubuntu:~$ sudo systemctl enable syslog-ng
Synchronizing state of syslog-ng.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable syslog-ng
bmsce@Ubuntu:~$ sudo systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
     Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor pre>
     Active: active (running) since Wed 2023-12-06 22:59:43 PST; 2min 16s ago
       Docs: man:syslog-ng(8)
   Main PID: 37279 (syslog-ng)
      Tasks: 2 (limit: 13024)
     Memory: 89.2M
        CPU: 2.285s
     CGroup: /system.slice/syslog-ng.service
             └─37279 /usr/sbin/syslog-ng -F

Dec 06 22:59:43 Ubuntu systemd[1]: Starting System Logger Daemon...
Dec 06 22:59:43 Ubuntu syslog-ng[37279]: [2023-12-06T22:59:43.841694] WARNING: >
Dec 06 22:59:43 Ubuntu syslog-ng[37279]: [2023-12-06T22:59:43.864850] WARNING: >
Dec 06 22:59:43 Ubuntu systemd[1]: Started System Logger Daemon.
```

```
bmsce@Ubuntu:~$ sudo mv /etc/syslog-ng/syslog-ng.conf /etc/syslog-ng/syslog-ng.c
onf.BAK
bmsce@Ubuntu:~$ sudo gedit /etc/syslog-ng/syslog-ng.conf
```

```
bmsce@Ubuntu:~$ /etc/init.d/syslog-ng restart
Restarting syslog-ng (via systemctl): syslog-ng.service.
bmsce@Ubuntu:~$ sudo gedit syslog
```

```
bmsce@Ubuntu:~$ cd /var/log/
bmsce@Ubuntu:/var/log$ sudo gedit syslog
```

Part 2 : Audit trails using Linux audit parser

1) auditd or Linux Audit Daemon is a user-space component of the Linux Auditing System, responsible for collecting and writing audit log file records to the disk. Install it using below command

sudo apt-get install auditd audispd-plugins

```
bmsce@Ubuntu:/var/log$ cd ~
bmsce@Ubuntu:~$ sudo apt-get install auditd audispd-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libestr0 libfastjson4 linux-headers-6.2.0-34-generic
  linux-hwe-6.2-headers-6.2.0-34 linux-image-6.2.0-34-generic
  linux-modules-6.2.0-34-generic linux-modules-extra-6.2.0-34-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libauparse0
The following NEW packages will be installed:
  audispd-plugins auditd libauparse0
0 upgraded, 3 newly installed, 0 to remove and 5 not upgraded.
Need to get 309 kB of archives.
After this operation, 1,013 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
bmsce@Ubuntu:~$ service auditd start
bmsce@Ubuntu:~$ sudo gedit /etc/syslog-ng/syslog-ng.conf
```

```
 1 @version: 3.22
 2 @include "scl.conf"
 3 options {
ack one page (Alt+Left Arrow)
-click or pull down to show history
 6 keep-hostname(yes);
 7 };
 8 source s_local {
 9         system();
10         internal();
11 };
12 source s_network {
13 s       yslog(transport(tcp));
14 };
15 destination d_logs {
16         file(
17                 "/var/log/syslog-ng/logs.txt"
18                 owner("root")
19                 group("root")
20                 perm(0777)
21         );
22 };
23 log {
24         source(s_local); source(s_network); destination(d_logs);
25 };
```

```
bmsce@Ubuntu:~$ /etc/init.d/syslog-ng restart
Restarting syslog-ng (via systemctl): syslog-ng.service.
bmsce@Ubuntu:~$ sudo gedit /tmp/test.json
```

Open | test.json /tmp | Save

```
1 {"_auditd":
  {"ver":"3.0.7","uid":"0","type":"DAEMON_START","subj":"unconfined","ses":"4294967295","res":"succ
  generic","format":"enriched","auid":"4294967295","UID":"root"}}
2 {"_auditd":
  {"type":"CONFIG_CHANGE","subj":"unconfined","ses":"4294967295","res":"1\u001dAUID=\"unset\"","op"
3 {"_auditd":
  {"uid":"0","type":"SYSCALL","tty":"(none)","syscall":"44","suid":"0","success":"yes","subj":"unco
  \u001dARCH=x86_64","items":"0","gid":"0","fsuid":"0","fsgid":"0","exit":"60","exe":"/usr/sbin/
  auditctl","euid":"0","egid":"0","comm":"auditctl","auid":"4294967295","arch":"c000003e","a3":"0",
4 {"_auditd":{"type":"PROCTITLE","proctitle":"/sbin/auditctl\t-R\t/etc/audit/
  audit.rules","msg":"audit(1701933452.164:100):"}}
5 {"_auditd":
  {"type":"CONFIG_CHANGE","subj":"unconfined","ses":"4294967295","res":"1\u001dAUID=\"unset\"","op"
6 {"_auditd":
  {"uid":"0","type":"SYSCALL","tty":"(none)","syscall":"44","suid":"0","success":"yes","subj":"unco
  \u001dARCH=x86_64","items":"0","gid":"0","fsuid":"0","fsgid":"0","exit":"60","exe":"/usr/sbin/
  auditctl","euid":"0","egid":"0","comm":"auditctl","auid":"4294967295","arch":"c000003e","a3":"0",
7 {"_auditd":{"type":"PROCTITLE","proctitle":"/sbin/auditctl\t-R\t/etc/audit/
  audit.rules","msg":"audit(1701933452.164:101):"}}
8 {"_auditd":
  {"type":"CONFIG_CHANGE","subj":"unconfined","ses":"4294967295","res":"1\u001dAUID=\"unset\"","op"
9 {"_auditd":
  {"uid":"0","type":"SYSCALL","tty":"(none)","syscall":"44","suid":"0","success":"yes","subj":"unco
  \u001dARCH=x86_64","items":"0","gid":"0","fsuid":"0","fsgid":"0","exit":"60","exe":"/usr/sbin/
  auditctl","euid":"0","egid":"0","comm":"auditctl","auid":"4294967295","arch":"c000003e","a3":"0",
10 {"_auditd":{"type":"PROCTITLE","proctitle":"/sbin/auditctl\t-R\t/etc/audit/
  audit.rules","msg":"audit(1701933452.164:102):"}}
```

```
 1 Dec  5 02:16:15 Ubuntu systemd[1]: rsyslog.service: Sent signal SIGHUP to main process 663
   (rsyslogd) on client request.
 2 Dec  5 02:16:15 Ubuntu systemd[1]: Created slice User Slice of UID 128.
 3 Dec  5 02:16:15 Ubuntu snort[864]: Found pid path directive (/run/snort/)
 4 Dec  5 02:16:15 Ubuntu snort[864]: Running in IDS mode
 5 Dec  5 02:16:15 Ubuntu snort[864]:
 6 Dec  5 02:16:15 Ubuntu snort[864]:         --== Initializing Snort ==--
 7 Dec  5 02:16:15 Ubuntu snort[864]: Initializing Output Plugins!
 8 Dec  5 02:16:15 Ubuntu snort[864]: Initializing Preprocessors!
 9 Dec  5 02:16:15 Ubuntu snort[864]: Initializing Plug-ins!
10 Dec  5 02:16:15 Ubuntu snort[864]: Parsing Rules file "/etc/snort/snort.conf"
11 Dec  5 02:16:15 Ubuntu systemd[1]: Starting User Runtime Directory /run/user/128...
12 Dec  5 02:16:15 Ubuntu systemd[1]: Finished User Runtime Directory /run/user/128.
13 Dec  5 02:16:15 Ubuntu systemd[1]: Starting User Manager for UID 128...
14 Dec  5 02:16:15 Ubuntu systemd[1]: snort.service: Deactivated successfully.
15 Dec  5 02:16:16 Ubuntu systemd[1]: snort.service: Unit process 864 (snort) remains running
   after unit stopped.
16 Dec  5 02:16:16 Ubuntu systemd[1]: Stopped LSB: Lightweight network intrusion detection
   system.
17 Dec  5 02:16:16 Ubuntu systemd[1]: snort.service: Found left-over process 864 (snort) in
   control group while starting unit. Ignoring.
18 Dec  5 02:16:16 Ubuntu systemd[1]: This usually indicates unclean termination of a previous
   run, or service implementation deficiencies.
```