3.

Create a file in your system. Whenever someone performs some action(read, write, execute) on that file, the event should be logged somewhere.

Answer:

We have different tools to watch a file. Some of them are;

- **iwatch**
- **auditd**

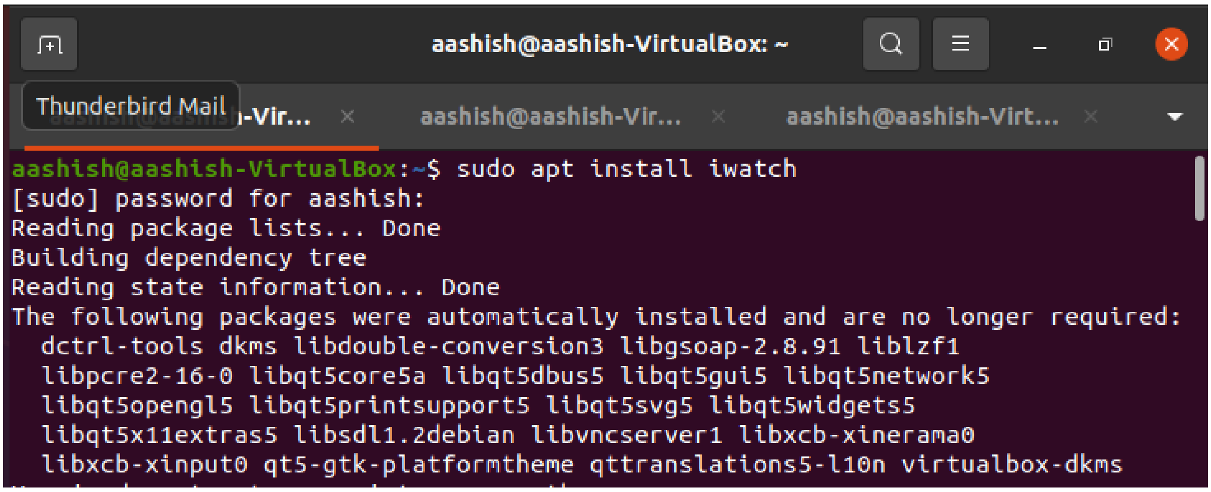
I have used the iwatch tool for this assignment.

Firstly, a file named testlog was created and another file named testlog.log was also created to store the log. And, read, write and execute permission was also granted using the following commands;

- **sudo touch testlog**
- **sudo chmod +777 testlog**
- **sudo touch testlog.log**
- **sudo chmod +777 teslog.log**

Then, we install iwatch using the following command;

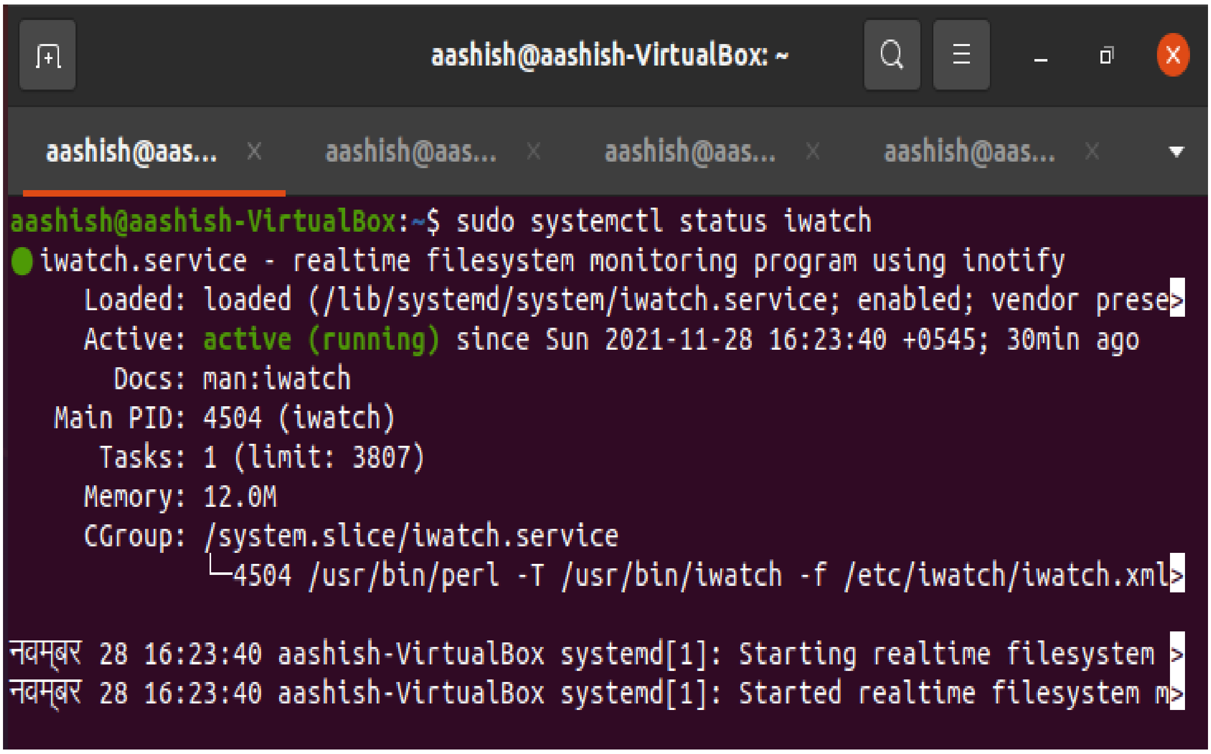
- **sudo apt install iwatch**



```
aashish@aashish-VirtualBox:~$ sudo apt install iwatch
[sudo] password for aashish:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dctrl-tools dkms libdouble-conversion3 libgsoap-2.8.91 liblzf1
  libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
  libqt5x11extras5 libsdl1.2debian libvncserver1 libxcb-xinerama0
  libxcb-xinput0 qt5-gtk-platformtheme qttranslations5-l10n virtualbox-dkms
```

To check the status of iwatch, we use;

- **sudo systemctl status iwatch**



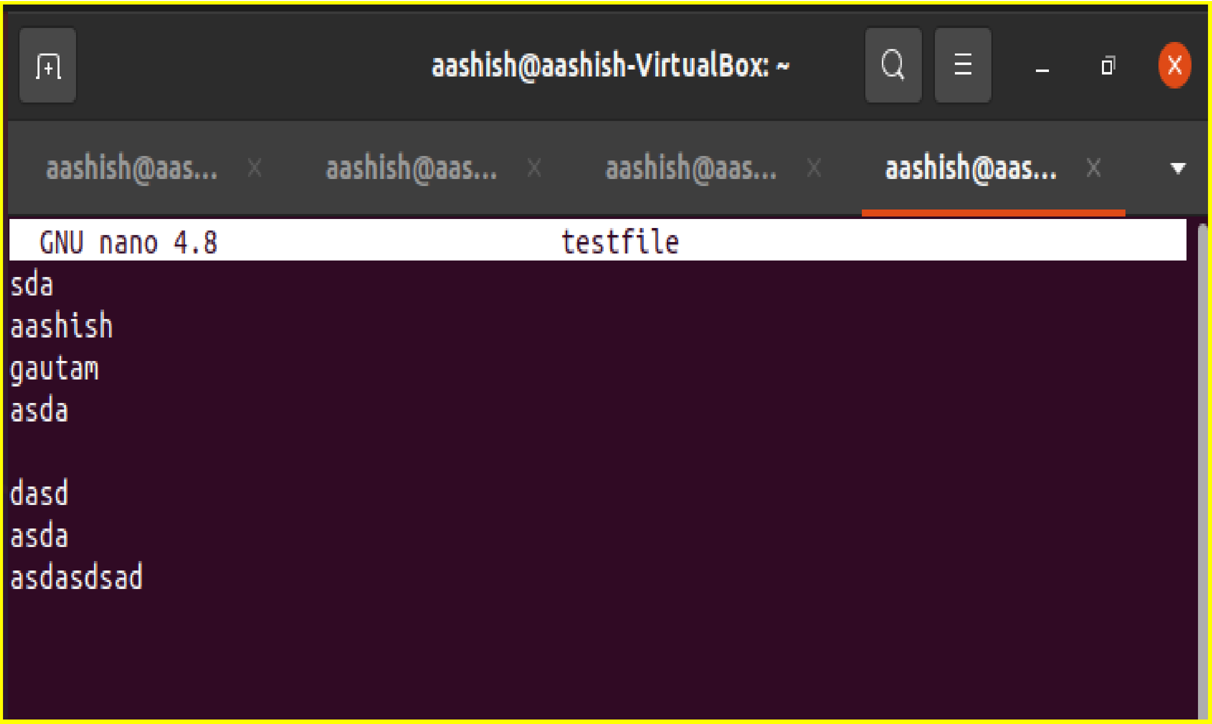
```
aashish@aashish-VirtualBox:~$ sudo systemctl status iwatch
● iwatch.service - realtime filesystem monitoring program using inotify
     Loaded: loaded (/lib/systemd/system/iwatch.service; enabled; vendor prese>
     Active: active (running) since Sun 2021-11-28 16:23:40 +0545; 30min ago
       Docs: man:iwatch
   Main PID: 4504 (iwatch)
      Tasks: 1 (limit: 3807)
     Memory: 12.0M
     CGroup: /system.slice/iwatch.service
             └─4504 /usr/bin/perl -T /usr/bin/iwatch -f /etc/iwatch/iwatch.xml>

नवम्बर 28 16:23:40 aashish-VirtualBox systemd[1]: Starting realtime filesystem >
नवम्बर 28 16:23:40 aashish-VirtualBox systemd[1]: Started realtime filesystem m>
```

Now, we append the testfile to testfile.log using the following command;

- **iwatch -e all_events testfile &> testfile.log**

Testfile was modified as follows;

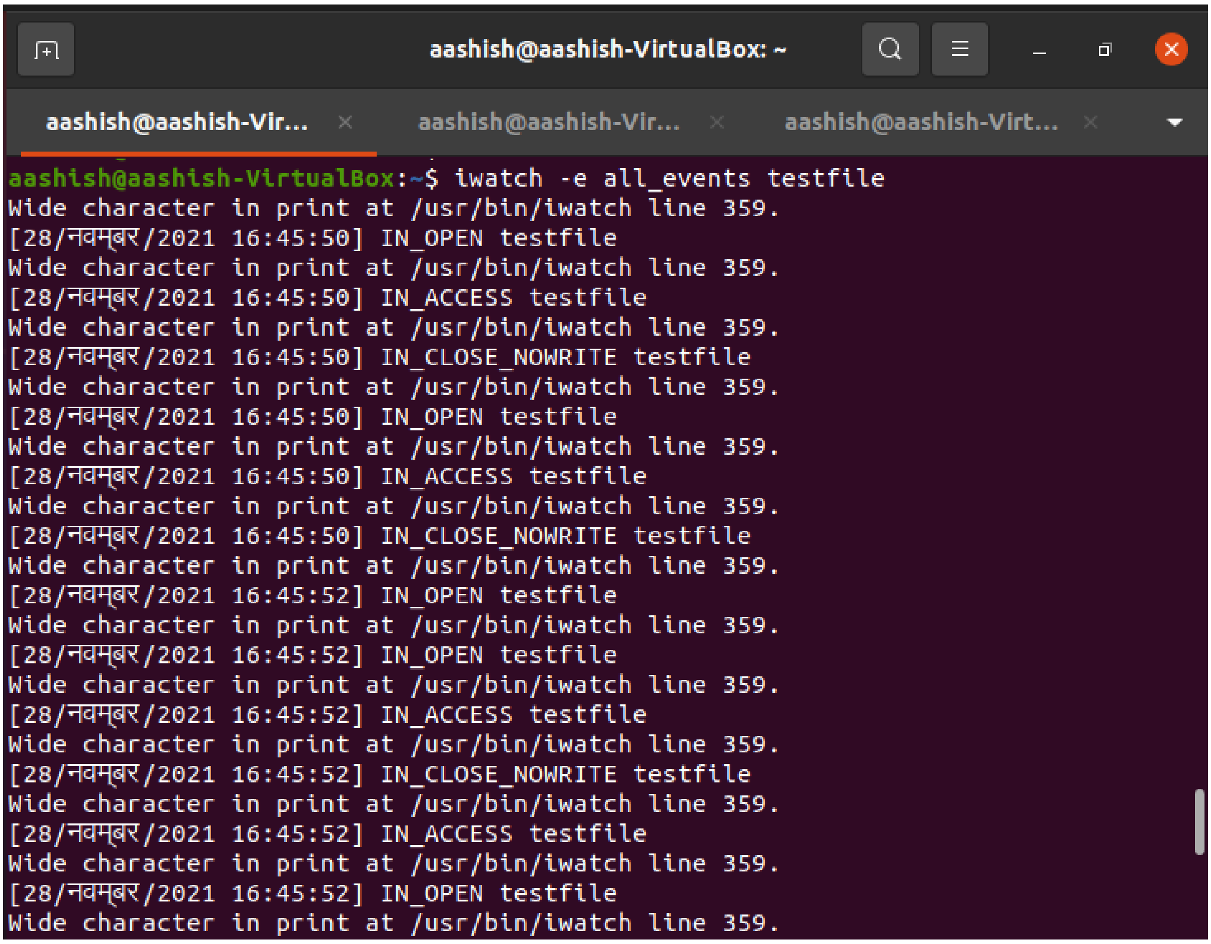


```
  GNU nano 4.8                    testfile
sda
aashish
gautam
asda

dasd
asda
asdasdsad
```

To watch the events, we use;

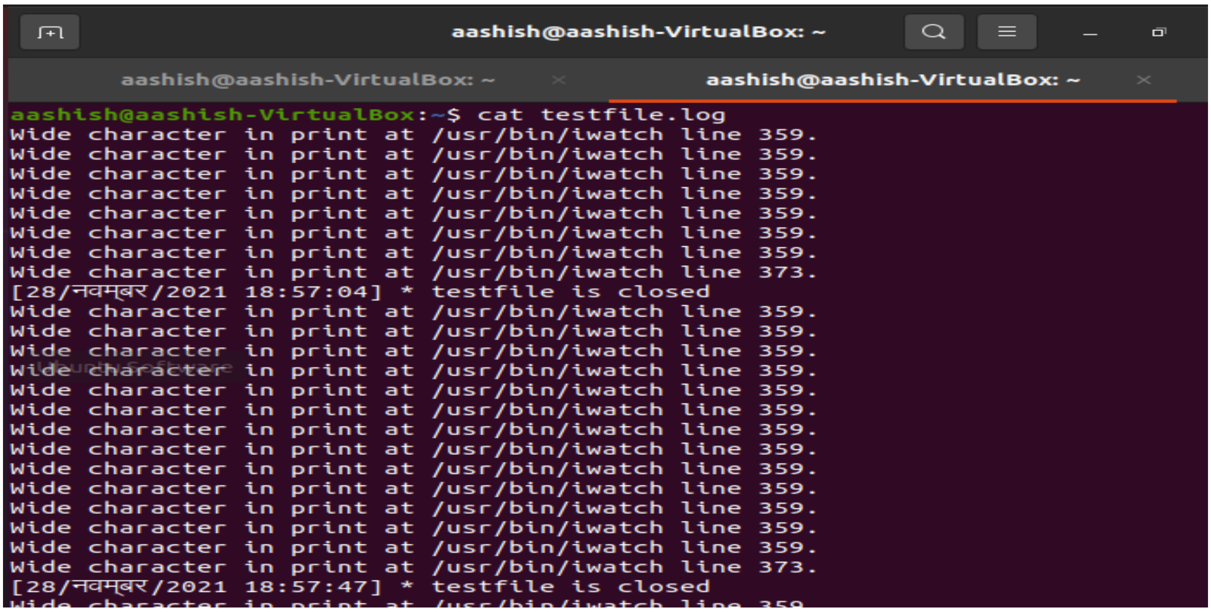
- **iwatch -e all_events testfile**



```
aashish@aashish-VirtualBox:~$ iwatch -e all_events testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_OPEN testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_ACCESS testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_CLOSE_NOWRITE testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_OPEN testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_ACCESS testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:50] IN_CLOSE_NOWRITE testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_OPEN testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_OPEN testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_ACCESS testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_CLOSE_NOWRITE testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_ACCESS testfile
Wide character in print at /usr/bin/iwatch line 359.
[28/नवम्बर/2021 16:45:52] IN_OPEN testfile
Wide character in print at /usr/bin/iwatch line 359.
```

To check the logs on testfile.log, we use;

- **cat test   file.log**


aashish@aashish-VirtualBox: ~
aashish@aashish-VirtualBox: ~
aashish@aashish-VirtualBox: ~
Ubuntu Software

```
aashish@aashish-VirtualBox:~$ cat testfile.log
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 373.
[28/नवम्बर/2021 18:57:04] * testfile is closed
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 359.
Wide character in print at /usr/bin/iwatch line 373.
[28/नवम्बर/2021 18:57:47] * testfile is closed
Wide character in print at /usr/bin/iwatch line 359
```