Autrace - Tool to check, count and monitor Linux processes

Many people still do not know what Autrace is? The information you need to know about Autrace will be shared by TipsMake in the article below.

Many people still do not know what Autrace is? The information you need to know about Autrace will be shared by ***TipsMake*** in the article below.

What is Autrace?

Autrace is a utility that allows running a process and saving the process's audit information in the file **/var/www/audit/audit.log** by adding audit rules.

To work, you first need to delete all existing audit rules.

Syntax for using autrace

```
# autrace -r program program-args
```

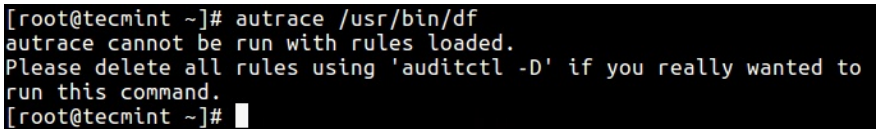
If you have any audit rules, autrace will show errors, for example:

On CentOS

```
# autrace /usr/bin/df
```

On Debian:

```
# autrace /bin/df
```



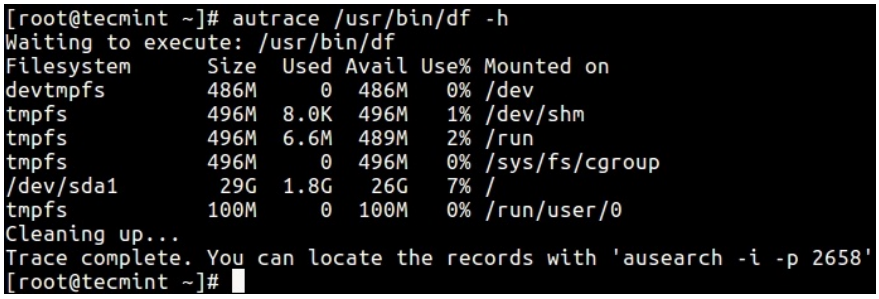
First you need to delete all audit rules using the following command:

```
# auditctl –D
```

The system will then run autrace with the program you want. In the example here, we are watching how the df command executes, showing the filesystem usage status.

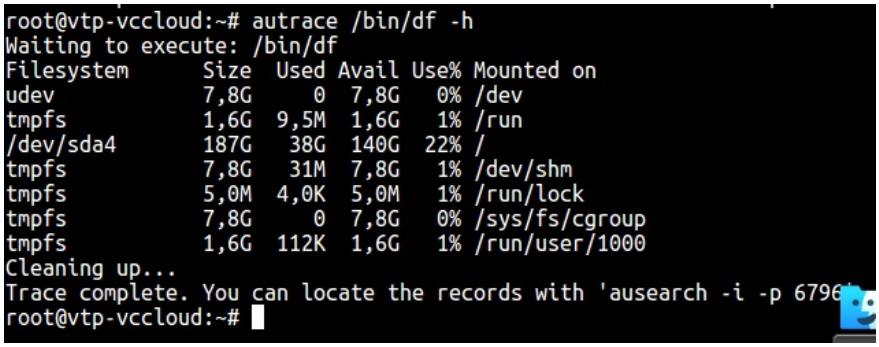
On CentOS :

```
# autrace /usr/bin/df -h
```



On Debian :

```
# autrace /bin/df -h
```



From the screenshot above, you can find all the log entries to play around with, explore from the log file using the ausearch function as follows.

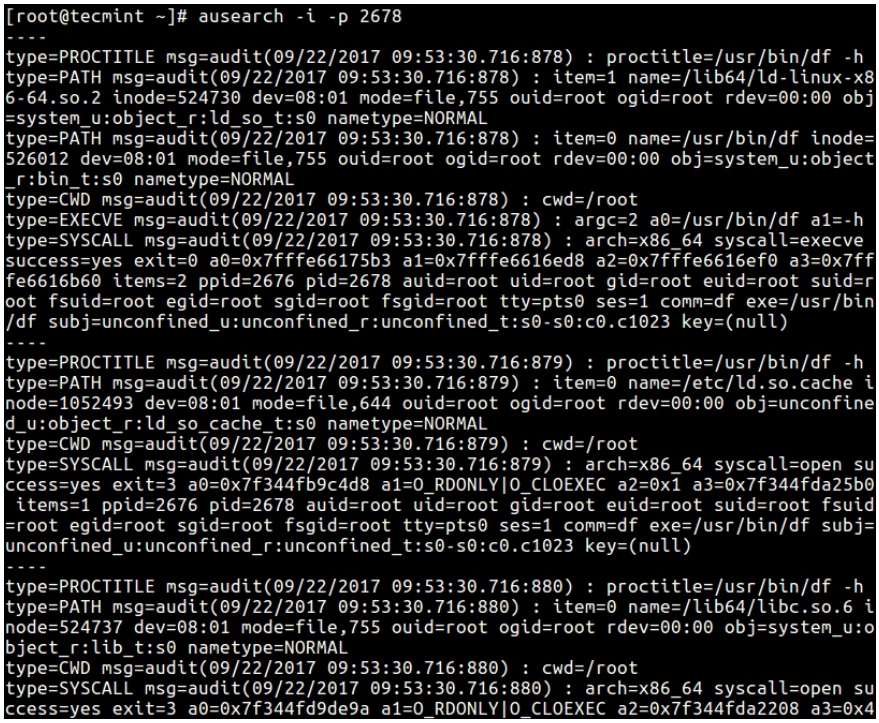
On Centos:

```
# ausearch -i -p 2658
```

In there:

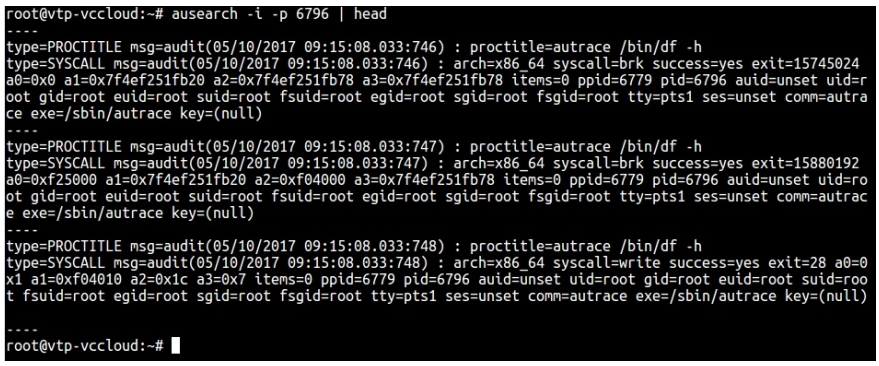
-i : Enables interpretation of numeric values ??into text

-p : Enter the process ID to search



On Debian:

```
# ausearch -i -p 6796
```



To output a detailed report, you can build a command that combines ausearch and aureport as follows

On Centos

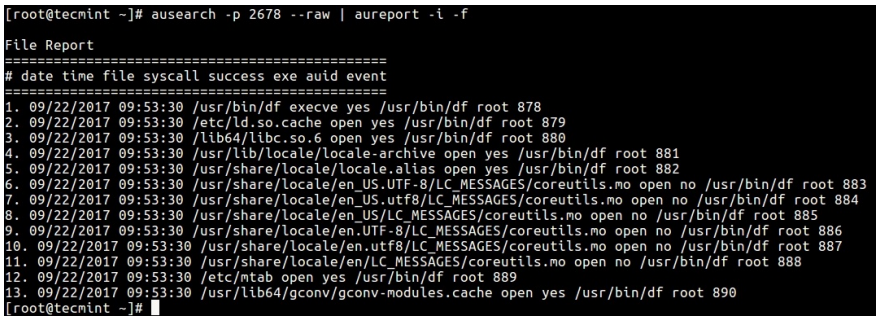
```
# ausearch -p 2678 --raw | aureport -i –f
```

In there:

--raw : Tell ausearch to send all raw input to aureport

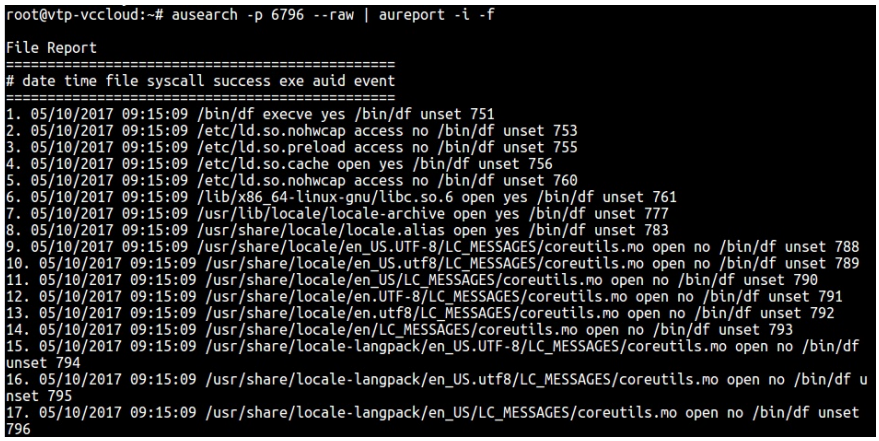
-f : Allows reporting on files as well as af_unix sockets

-i : Enables interpretation of numeric values ??into text



On Debian

```
# ausearch -p 6796 --raw | aureport -i –f
```



And you can also use the following command to limit the syscalls to be grouped together, which is necessary for analyzing the resource usage of the df process.

On Centos

```
# autrace -r /usr/bin/df -h
```

On Debian

```
# autrace -r /bin/df -h
```

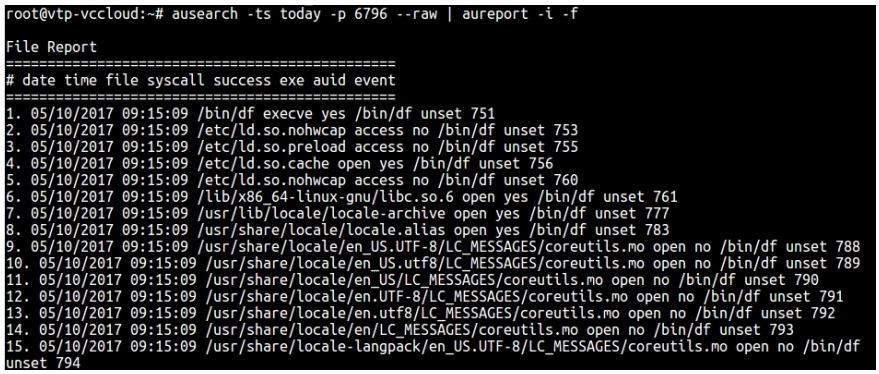
If you've ausearched a program in the past week, that means there's a lot of information going into the audit logs. To generate a report that only records events that happened today, you can use ausearch's -ts flag to specify the exact time to start searching for information:

On Centos

```
# ausearch -ts today -p 2768 --raw | aureport -i –f
```

On Debian

```
# ausearch -ts today -p 6796 --raw | aureport -i -f
```



That's all the basics you can use to control, monitor and track a Linux process using autrace. For more details, you can read the man pages.

According to TipsMake share

You finished reading the article "**Autrace - Tool to check, count and monitor Linux processes**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
