

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
```

```
[root@tecmint ~]# autrace /usr/bin/df
autrace cannot be run with rules loaded.
Please delete all rules using 'auditctl -D' if you really wanted to
run this command.
[root@tecmint ~]#
```

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
```

```
[root@tecmint ~]# autrace /usr/bin/df -h
Waiting to execute: /usr/bin/df
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        486M  0    486M  0% /dev
tmpfs           496M  8.0K 496M  1% /dev/shm
tmpfs           496M  6.6M 489M  2% /run
tmpfs           496M  0    496M  0% /sys/fs/cgroup
/dev/sda1       29G   1.8G 26G   7% /
tmpfs           100M  0    100M  0% /run/user/0
Cleaning up...
Trace complete. You can locate the records with 'ausearch -i -p 2658'
[root@tecmint ~]#
```

On Debian :

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

```
root@vtp-vccloud:~# autrace /bin/df -h
Waiting to execute: /bin/df
Filesystem      Size  Used Avail Use% Mounted on
udev            7,8G  0    7,8G  0% /dev
tmpfs           1,6G  9,5M 1,6G  1% /run
/dev/sda4       187G  38G  140G 22% /
tmpfs           7,8G  31M  7,8G  1% /dev/shm
tmpfs           5,0M  4,0K 5,0M  1% /run/lock
tmpfs           7,8G  0    7,8G  0% /sys/fs/cgroup
tmpfs           1,6G  112K 1,6G  1% /run/user/1000
Cleaning up...
Trace complete. You can locate the records with 'ausearch -i -p 6796'
root@vtp-vccloud:~#
```

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

```
[root@tecmint ~]# ausearch -i -p 2678
----
type=PROCTITLE msg=audit(09/22/2017 09:53:30.716:878) : proctitle=/usr/bin/df -h
type=PATH msg=audit(09/22/2017 09:53:30.716:878) : item=1 name=/lib64/ld-linux-x86-64.so.2 inode=524730 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:ld_so_t:s0 nametype=NORMAL
type=PATH msg=audit(09/22/2017 09:53:30.716:878) : item=0 name=/usr/bin/df inode=526012 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:bin_t:s0 nametype=NORMAL
type=CWD msg=audit(09/22/2017 09:53:30.716:878) : cwd=/root
type=EXECVE msg=audit(09/22/2017 09:53:30.716:878) : argc=2 a0=/usr/bin/df a1=-h
type=SYSCALL msg=audit(09/22/2017 09:53:30.716:878) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x7ffffe66175b3 a1=0x7ffffe6616ed8 a2=0x7ffffe6616ef0 a3=0x7ffffe6616b60 items=2 ppid=2676 pid=2678 auid=root uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=df exe=/usr/bin/df subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
type=PROCTITLE msg=audit(09/22/2017 09:53:30.716:879) : proctitle=/usr/bin/df -h
type=PATH msg=audit(09/22/2017 09:53:30.716:879) : item=0 name=/etc/ld.so.cache inode=1052493 dev=08:01 mode=file,644 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:ld_so_cache_t:s0 nametype=NORMAL
type=CWD msg=audit(09/22/2017 09:53:30.716:879) : cwd=/root
type=SYSCALL msg=audit(09/22/2017 09:53:30.716:879) : arch=x86_64 syscall=open success=yes exit=3 a0=0x7f344fb9c4d8 a1=0_RDONLY|0_CLOEXEC a2=0x1 a3=0x7f344fda25b0 items=1 ppid=2676 pid=2678 auid=root uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=df exe=/usr/bin/df subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
----
type=PROCTITLE msg=audit(09/22/2017 09:53:30.716:880) : proctitle=/usr/bin/df -h
type=PATH msg=audit(09/22/2017 09:53:30.716:880) : item=0 name=/lib64/libc.so.6 inode=524737 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:lib_t:s0 nametype=NORMAL
type=CWD msg=audit(09/22/2017 09:53:30.716:880) : cwd=/root
type=SYSCALL msg=audit(09/22/2017 09:53:30.716:880) : arch=x86_64 syscall=open success=yes exit=3 a0=0x7f344fd9de9a a1=0_RDONLY|0_CLOEXEC a2=0x7f344fda2208 a3=0x4
```

On Debian:

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

```
root@vtp-vccloud:~# ausearch -i -p 6796 | head
----
type=PROCTITLE msg=audit(05/10/2017 09:15:08.033:746) : proctitle=atrace /bin/df -h
type=SYSCALL msg=audit(05/10/2017 09:15:08.033:746) : arch=x86_64 syscall=brk success=yes exit=15745024 a0=0x0 a1=0x7f4ef251fb20 a2=0x7f4ef251fb78 a3=0x7f4ef251fb78 items=0 ppid=6779 pid=6796 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts1 ses=unset comm=atrace exe=/sbin/atrace key=(null)
----
type=PROCTITLE msg=audit(05/10/2017 09:15:08.033:747) : proctitle=atrace /bin/df -h
type=SYSCALL msg=audit(05/10/2017 09:15:08.033:747) : arch=x86_64 syscall=brk success=yes exit=15880192 a0=0xf25000 a1=0x7f4ef251fb20 a2=0xf04000 a3=0x7f4ef251fb78 items=0 ppid=6779 pid=6796 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts1 ses=unset comm=atrace exe=/sbin/atrace key=(null)
----
type=PROCTITLE msg=audit(05/10/2017 09:15:08.033:748) : proctitle=atrace /bin/df -h
type=SYSCALL msg=audit(05/10/2017 09:15:08.033:748) : arch=x86_64 syscall=write success=yes exit=28 a0=0x1 a1=0xf04010 a2=0x1c a3=0x7 items=0 ppid=6779 pid=6796 auid=unset uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts1 ses=unset comm=atrace exe=/sbin/atrace key=(null)
----
root@vtp-vccloud:~# █
```

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

```
[root@tecmint ~]# ausearch -p 2678 --raw | aureport -i -f
File Report
=====
# date time file syscall success exe auid event
=====
1. 09/22/2017 09:53:30 /usr/bin/df execve yes /usr/bin/df root 878
2. 09/22/2017 09:53:30 /etc/ld.so.cache open yes /usr/bin/df root 879
3. 09/22/2017 09:53:30 /lib64/libc.so.6 open yes /usr/bin/df root 880
4. 09/22/2017 09:53:30 /usr/lib/locale/locale-archive open yes /usr/bin/df root 881
5. 09/22/2017 09:53:30 /usr/share/locale/locale.alias open yes /usr/bin/df root 882
6. 09/22/2017 09:53:30 /usr/share/locale/en_US.UTF-8/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 883
7. 09/22/2017 09:53:30 /usr/share/locale/en_US.utf8/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 884
8. 09/22/2017 09:53:30 /usr/share/locale/en_US/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 885
9. 09/22/2017 09:53:30 /usr/share/locale/en.UTF-8/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 886
10. 09/22/2017 09:53:30 /usr/share/locale/en.utf8/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 887
11. 09/22/2017 09:53:30 /usr/share/locale/en/LC_MESSAGES/coreutils.mo open no /usr/bin/df root 888
12. 09/22/2017 09:53:30 /etc/mtab open yes /usr/bin/df root 889
13. 09/22/2017 09:53:30 /usr/lib64/gconv/gconv-modules.cache open yes /usr/bin/df root 890
[root@tecmint ~]#
```

On Debian

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

```
root@vtp-vccloud:~# ausearch -p 6796 --raw | aureport -i -f
File Report
=====
# date time file syscall success exe auid event
=====
1. 05/10/2017 09:15:09 /bin/df execve yes /bin/df unset 751
2. 05/10/2017 09:15:09 /etc/ld.so.nohwcap access no /bin/df unset 753
3. 05/10/2017 09:15:09 /etc/ld.so.preload access no /bin/df unset 755
4. 05/10/2017 09:15:09 /etc/ld.so.cache open yes /bin/df unset 756
5. 05/10/2017 09:15:09 /etc/ld.so.nohwcap access no /bin/df unset 760
6. 05/10/2017 09:15:09 /lib/x86_64-linux-gnu/libc.so.6 open yes /bin/df unset 761
7. 05/10/2017 09:15:09 /usr/lib/locale/locale-archive open yes /bin/df unset 777
8. 05/10/2017 09:15:09 /usr/share/locale/locale.alias open yes /bin/df unset 783
9. 05/10/2017 09:15:09 /usr/share/locale/en_US.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df unset 788
10. 05/10/2017 09:15:09 /usr/share/locale/en_US.utf8/LC_MESSAGES/coreutils.mo open no /bin/df unset 789
11. 05/10/2017 09:15:09 /usr/share/locale/en_US/LC_MESSAGES/coreutils.mo open no /bin/df unset 790
12. 05/10/2017 09:15:09 /usr/share/locale/en.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df unset 791
13. 05/10/2017 09:15:09 /usr/share/locale/en.utf8/LC_MESSAGES/coreutils.mo open no /bin/df unset 792
14. 05/10/2017 09:15:09 /usr/share/locale/en/LC_MESSAGES/coreutils.mo open no /bin/df unset 793
15. 05/10/2017 09:15:09 /usr/share/locale-langpack/en_US.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df
unset 794
16. 05/10/2017 09:15:09 /usr/share/locale-langpack/en_US.utf8/LC_MESSAGES/coreutils.mo open no /bin/df u
nset 795
17. 05/10/2017 09:15:09 /usr/share/locale-langpack/en_US/LC_MESSAGES/coreutils.mo open no /bin/df unset
796
```

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

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

On Debian

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

If you've aused 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
```

```
root@vtp-vccloud:~# ausearch -ts today -p 6796 --raw | aureport -i -f
File Report
=====
# date time file syscall success exe audit event
=====
1. 05/10/2017 09:15:09 /bin/df execve yes /bin/df unset 751
2. 05/10/2017 09:15:09 /etc/ld.so.nohwcap access no /bin/df unset 753
3. 05/10/2017 09:15:09 /etc/ld.so.preload access no /bin/df unset 755
4. 05/10/2017 09:15:09 /etc/ld.so.cache open yes /bin/df unset 756
5. 05/10/2017 09:15:09 /etc/ld.so.nohwcap access no /bin/df unset 760
6. 05/10/2017 09:15:09 /lib/x86_64-linux-gnu/libc.so.6 open yes /bin/df unset 761
7. 05/10/2017 09:15:09 /usr/lib/locale/locale-archive open yes /bin/df unset 777
8. 05/10/2017 09:15:09 /usr/share/locale/locale.alias open yes /bin/df unset 783
9. 05/10/2017 09:15:09 /usr/share/locale/en_US.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df unset 788
10. 05/10/2017 09:15:09 /usr/share/locale/en_US.utf8/LC_MESSAGES/coreutils.mo open no /bin/df unset 789
11. 05/10/2017 09:15:09 /usr/share/locale/en_US/LC_MESSAGES/coreutils.mo open no /bin/df unset 790
12. 05/10/2017 09:15:09 /usr/share/locale/en.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df unset 791
13. 05/10/2017 09:15:09 /usr/share/locale/en.utf8/LC_MESSAGES/coreutils.mo open no /bin/df unset 792
14. 05/10/2017 09:15:09 /usr/share/locale/en/LC_MESSAGES/coreutils.mo open no /bin/df unset 793
15. 05/10/2017 09:15:09 /usr/share/locale-langpack/en_US.UTF-8/LC_MESSAGES/coreutils.mo open no /bin/df
unset 794
```

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

According to TipsMake share

You finished reading the article "**Atrace - 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.