STRACE COMMAND

Strace is one of the most powerful **process monitoring, diagnostic, instructional tool** of Linux. It also acts as a debugging tool that helps in troubleshooting issues

Following purposes:

- Debugging Programs
- Troubleshooting Programs
- Intercept System calls by a process
- Record system calls by a process
- Signals received by a process
- Trace running processes

To get the system call, argument, and the result of the call

```
[root@vivek ~]# strace ls
execve("/usr/bin/ls", ["ls"], 0x7fff15297a50 /* 26 vars */) = 0
brk(NULL)                               = 0x55e066b05000
arch_prctl(0x3001 /* ARCH_??? */, 0x7ffc831bee00) = -1 EINVAL (Invalid argument)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=67260, ...}) = 0
mmap(NULL, 67260, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f6f61433000
close(3)                                = 0
```

To count number of system calls

```
[root@vivek ~]# strace -c ls
anaconda-ks.cfg  initial-setup-ks.cfg
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 36.34    0.000157           4        32           mmap
 22.45    0.000097           2        36        13 openat
 10.65    0.000046           3        14           mprotect
  6.48    0.000028           1        25           close
  6.48    0.000028           1        24           fstat
  6.48    0.000028          28         1           futex
  4.63    0.000020           1        14           read
  2.08    0.000009           9         1           write
  1.85    0.000008           4         2           getdents64
  1.39    0.000006           3         2           ioctl
  0.93    0.000004           0         6           lseek
  0.23    0.000001           0         2         1 arch_prctl
  0.00    0.000000           0         1           munmap
  0.00    0.000000           0         3           brk
  0.00    0.000000           0         2           rt_sigaction
  0.00    0.000000           0         1           rt_sigprocmask
  0.00    0.000000           0         2         1 access
  0.00    0.000000           0         1           execve
  0.00    0.000000           0         2           statfs
  0.00    0.000000           0         1           set_tid_address
  0.00    0.000000           0         1           set_robust_list
  0.00    0.000000           0         1           prlimit64
------ ----------- ----------- --------- --------- ----------------
100.00    0.000432                   174        15 total
```

To trace particular or specific system calls.

```
[root@vivek ~]# strace -e trace=write ls
write(1, "anaconda-ks.cfg  initial-setup-k"..., 38anaconda-ks.cfg  initial-setup-ks.cfg
) = 38
+++ exited with 0 +++
```


CREATED BY:- VIVEK GANDHI

STRACE COMMAND

To trace network related system calls

```
[root@vivek ~]# strace -e trace=network nc -v -n 192.168.254.133
Ncat: Version 7.70 ( https://nmap.org/ncat )
socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(31337), sin_addr=inet_addr("192.168.254.133")}, 16) = -1 EINPROGRESS (Operation now in progress)
getsockopt(3, SOL_SOCKET, SO_ERROR, [111], [4]) = 0
Ncat: Connection refused.
+++ exited with 1 +++
```

To print timestamp of each call

```
[root@vivek ~]# strace -r ls
     0.000000 execve("/usr/bin/ls", ["ls"], 0x7ffd4608e308 /* 26 vars */) = 0
     0.000650 brk(NULL)                 = 0x560ceb9e1000
     0.000173 arch_prctl(0x3001 /* ARCH_??? */, 0x7fff3e03a990) = -1 EINVAL (Invalid argument)
     0.000207 access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
     0.000175 openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
     0.000186 fstat(3, {st_mode=S_IFREG|0644, st_size=67260, ...}) = 0
     0.000155 mmap(NULL, 67260, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7fa0ff77b000
     0.000167 close(3)                  = 0
```

To print time spent on system calls.

```
[root@vivek ~]# strace -T ls
execve("/usr/bin/ls", ["ls"], 0x7fff636843f8 /* 26 vars */) = 0 <0.000537>
brk(NULL)                               = 0x563e5b767000 <0.000103>
arch_prctl(0x3001 /* ARCH_??? */, 0x7ffd32bbd050) = -1 EINVAL (Invalid argument) <0.000090>
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory) <0.000093>
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3 <0.000081>
fstat(3, {st_mode=S_IFREG|0644, st_size=67260, ...}) = 0 <0.000076>
mmap(NULL, 67260, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f3953cbd000 <0.000077>
```

To print wall clock time of each system call.

```
[root@vivek ~]# strace -t ls
04:20:03 execve("/usr/bin/ls", ["ls"], 0x7ffc315b39c8 /* 26 vars */) = 0
04:20:03 brk(NULL)                      = 0x560b8f854000
04:20:03 arch_prctl(0x3001 /* ARCH_??? */, 0x7ffcf5fa4c90) = -1 EINVAL (Invalid argument)
04:20:03 access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
04:20:03 openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
04:20:03 fstat(3, {st_mode=S_IFREG|0644, st_size=67260, ...}) = 0
```

To print instruction pointer.

```
[root@vivek ~]# strace -i ls
[00007fb15257153b] execve("/usr/bin/ls", ["ls"], 0x7ffeea33a918 /* 26 vars */) = 0
[00007f515eba233b] brk(NULL)            = 0x55fe4d002000
[00007f515eba10c5] arch_prctl(0x3001 /* ARCH_??? */, 0x7fff0ef056a0) = -1 EINVAL (Invalid argument)
[00007f515eba300b] access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
[00007f515eba3131] openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
[00007f515eba2f57] fstat(3, {st_mode=S_IFREG|0644, st_size=67260, ...}) = 0
[00007f515eba3347] mmap(NULL, 67260, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f515ed9e000
```


CREATED BY:- VIVEK GANDHI