Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'ausyscall.8'

$ man ausyscall.8

AUSYSCALL(8) System Administration Utilities AUSYSCALL(8)

NAME

ausyscall - a program that allows mapping syscall names and numbers

SYNOPSIS

ausyscall [arch] name | number | --dump | --exact

DESCRIPTION

ausyscall is a program that prints out the mapping from syscall name to number and reverse for the given arch. The arch can be anything re? turned by `uname -m`. If arch is not given, the program will take a guess based on the running image. Or for convenience, you can pass b32 or b64 to use the current arch but a specific ABI. You may give the syscall name or number and it will find the opposite. You can also dump the whole table with the --dump option. By default a syscall name lookup will be a substring match meaning that it will try to match all occurrences of the given name with syscalls. So giving a name of chown will match both fchown and chown as any other syscall with chown in its name. If this behavior is not desired, pass the --exact flag and it will do an exact string match.

This program can be used to verify syscall numbers on a biarch platform for rule optimization. For example, suppose you had an auditctl rule:

```
-a always, exit -S open -F exit=-EPERM -k fail-open
```

If you wanted to verify that both 32 and 64 bit programs would be au? dited, run "ausyscall i386 open" and then "ausyscall x86_64 open". (Or use the b32 and b64 option.) Look at the returned numbers. If they are different, you will have to write two auditctl rules to get complete coverage.

```
-a always,exit -F arch=b32 -S open -F exit=-EPERM -k fail-open
-a always,exit -F arch=b64 -S open -F exit=-EPERM -k fail-open
```

For more information about a specific syscall, use the man program and pass the number 2 as an argument to make sure that you get the syscall information rather than a shell script program or glibc function call of the same name. For example, if you wanted to learn about the open syscall, type: man 2 open.

OPTIONS

--dump Print all syscalls for the given arch

--exact

Instead of doing a partial word match, match the given syscall name exactly.

SEE ALSO

ausearch(8), auditctl(8).

AUTHOR

Steve Grubb

Red Hat Nov 2008 AUSYSCALL(8)