NAME

cap_ioctls_limit, **cap_ioctls_get** **-** manage allowed ioctl commands

LIBRARY

Standard C Library (libc, -lc)

SYNOPSIS

#include <sys/capsicum.h>

int
cap_ioctls_limit(*int fd*, *const unsigned long *cmds*, *size_t ncmds*);

ssize_t
cap_ioctls_get(*int fd*, *unsigned long *cmds*, *size_t maxcmds*);

DESCRIPTION

If a file descriptor is granted the CAP_IOCTL capability right, the list of allowed ioctl(2) commands can be selectively reduced (but never expanded) with the **cap_ioctls_limit**() system call. The *cmds* argument is an array of ioctl(2) commands and the *ncmds* argument specifies the number of elements in the array. There can be up to *256* elements in the array. Including an element that has been previously revoked will generate an error. After a successful call only those listed in the array may be used.

The list of allowed ioctl commands for a given file descriptor can be obtained with the **cap_ioctls_get**() system call. The *cmds* argument points at memory that can hold up to *maxcmds* values. The function populates the provided buffer with up to *maxcmds* elements, but always returns the total number of ioctl commands allowed for the given file descriptor. The total number of ioctls commands for the given file descriptor can be obtained by passing NULL as the *cmds* argument and *0* as the *maxcmds* argument. If all ioctl commands are allowed (CAP_IOCTL capability right is assigned to the file descriptor and the **cap_ioctls_limit**() system call was never called for this file descriptor), the **cap_ioctls_get**() system call will return CAP_IOCTLS_ALL and will not modify the buffer pointed to by the *cmds* argument.

RETURN VALUES

The **cap_ioctls_limit**() function returns the value 0 if successful; otherwise the value -1 is returned and the global variable *errno* is set to indicate the error.

The **cap_ioctls_get**() function, if successful, returns the total number of allowed ioctl commands or the value CAP_IOCTLS_ALL if all ioctls commands are allowed. On failure the value -*1* is returned and the global variable errno is set to indicate the error.

ERRORS

The **cap_ioctls_limit**() and **cap_ioctls_get**() system calls will fail if:

[EBADF] The *fd* argument is not a valid descriptor.

[EFAULT] The *cmds* argument points at an invalid address.

[ENOSYS] The running kernel was compiled without **options CAPABILITY_MODE**.

The **cap_ioctls_limit**() system call may also return the following errors:

[EINVAL] The *ncmds* argument is greater than *256*.

[ENOTCAPABLE] *cmds* would expand the list of allowed ioctl(2) commands.

SEE ALSO

cap_fcntls_limit(2), cap_rights_limit(2), ioctl(2)

HISTORY

The **cap_ioctls_get**() and **cap_ioctls_limit**() system calls first appeared in FreeBSD 8.3. Support for capabilities and capabilities mode was developed as part of the TrustedBSD Project.

AUTHORS

This function was created by Pawel Jakub Dawidek <*pawel@dawidek.net*> under sponsorship of the FreeBSD Foundation.