NAME

cap_rights_limit - limit capability rights

LIBRARY

Standard C Library (libc, -lc)

SYNOPSIS

#include <sys/capsicum.h>

int
cap_rights_limit(*int fd, const cap_rights_t *rights*);

DESCRIPTION

When a file descriptor is created by a function such as accept(2), accept4(2), fhopen(2), kqueue(2), mq_open(2), open(2), openat(2), pdfork(2), pipe(2), shm_open(2), socket(2) or socketpair(2), it is assigned all capability rights. Those rights can be reduced (but never expanded) by using the **cap_rights_limit**() system call. Once capability rights are reduced, operations on the file descriptor will be limited to those permitted by *rights*.

The *rights* argument should be prepared using cap_rights_init(3) family of functions.

Capability rights assigned to a file descriptor can be obtained with the cap_rights_get(3) function.

The complete list of the capability rights can be found in the rights(4) manual page.

RETURN VALUES

Upon successful completion, the value 0 is returned; otherwise the value -1 is returned and the global variable *errno* is set to indicate the error.

EXAMPLES

The following example demonstrates how to limit file descriptor capability rights to allow reading only.

```
cap_rights_t setrights;
char buf[1];
int fd;

fd = open("/tmp/foo", O_RDWR);
if (fd < 0)
        err(1, "open() failed");
```

```
if (cap_enter() < 0)
        err(1, "cap_enter() failed");

cap_rights_init(&setrights, CAP_READ);
if (cap_rights_limit(fd, &setrights) < 0)
        err(1, "cap_rights_limit() failed");

buf[0] = 'X';

if (write(fd, buf, sizeof(buf)) > 0)
        errx(1, "write() succeeded!");

if (read(fd, buf, sizeof(buf)) < 0)
        err(1, "read() failed");
```

ERRORS

cap_rights_limit() succeeds unless:

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

[EINVAL] An invalid right has been requested in *rights*.

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

[ENOTCAPABLE] The *rights* argument contains capability rights not present for the given file descriptor. Capability rights list can only be reduced, never expanded.

SEE ALSO

accept(2), accept4(2), cap_enter(2), fhopen(2), kqueue(2), mq_open(2), open(2), openat(2), pdfork(2), pipe(2), read(2), shm_open(2), socket(2), socketpair(2), write(2), cap_rights_get(3), cap_rights_init(3), err(3), capsicum(4), rights(4)

HISTORY

The **cap_rights_limit**() function 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.