

NAME

cr_canseejailproc - determine if subjects may see entities in sub-jails

SYNOPSIS

int

cr_canseejailproc(*struct ucred *u1, struct ucred *u2*);

DESCRIPTION

This function is internal. Its functionality is integrated into the function `cr_bsd_visible(9)`, which should be called instead.

This function checks if a subject associated to credentials *u1* is denied seeing a subject or object associated to credentials *u2* by a policy that requires both credentials to be associated to the same jail. This is a restriction to the baseline jail policy that a subject can see subjects or objects in its own jail or any sub-jail of it.

This policy is active if and only if the `sysctl(8)` variable `security.bsd.see_jail_proc` is set to zero.

As usual, the superuser (effective user ID 0) is exempt from this policy provided that the `sysctl(8)` variable `security.bsd.suser_enabled` is non-zero and no active MAC policy explicitly denies the exemption (see `priv_check_cred(9)`).

RETURN VALUES

The `cr_canseejailproc()` function returns 0 if the policy is disabled, both credentials are associated to the same jail, or if *u1* has privilege exempting it from the policy. Otherwise, it returns ESRCH.

SEE ALSO

`cr_bsd_visible(9)`, `priv_check_cred(9)`

AUTHORS

This manual page was written by Olivier Certner <olce.freebsd@certner.fr>.