Rocky Enterprise Linux 9.2 Manual Pages on command 'capability.conf.5'

C:\>man capability.conf.5

CAPABILITY.CONF(5) Linux-PAM Manual CAPABILITY.CONF(5)

NAME

capablity.conf - configuration file for the pam_cap module

DESCRIPTION

Each line of the file consists of two fields; the fields define:

<capability-list>

One or more comma-separated capabilities, specified as either the textual capability name, or numeric capability value. Text name(s) and numeric value(s) may be intermixed.

The special capability name all may be used to enable all capabilities known to the local system.

The special capability name none may be used to disable all current inheritable capabilities.

NOTE: No whitespace is pemitted between the values. The names all and none may not be combined with any other capabilities.

<username>

One or more whitespace-separated usernames, or the wildcard *.

NOTE: The first matching entry is used. Thus, only a single matching username entry, and/or a single wildcard entry, may be used. A matching username entry must precede the wildcard entry in order to be effective.

IMPORTANT: <capability-list> replaces the current process' inherited capabilities; i.e. there is no provision for adding/subtracting from the current set. In most

environments, the inheritable set of the process performing user authentication is 0 (empty).

If any capability name or numeric value is invalid/unknown to the local system, the capabilities will be rejected, and the inheritable set will not be modified.

EXAMPLES

These are some example lines which might be specified in /etc/security/capability.conf.

```
# Simple
cap_sys_ptrace              developer
cap_net_raw                 user1
# Multiple capablities
cap_net_admin,cap_net_raw    jrnetadmin
# Identical, but with numeric values
12,13                       jrnetadmin
# Combining names and numerics
cap_sys_admin,22,25         jrsysadmin
# Next line has no effect; user1 already matched above
5,12,13                     user1
# Insure any potential capailities from calling process are dropped
none                        luser1 luser2
# Allow anyone to manipulate capabilities
# Will NOT apply to users matched above !
cap_setpcap                 *
```

SEE ALSO

pam_cap(8), pam.d(5), pam(7), capabilities(7)

AUTHOR

pam_cap was initially written by Andrew G. Morgan <morgan@kernel.org>