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

$ man pam_console.8

pam_console(8) System Administrator's Manual pam_console(8)

NAME

pam_console - determine user owning the system console

SYNOPSIS

session optional pam_console.so

auth required pam_console.so

DESCRIPTION

pam_console.so is designed to give users at the physical console (vir? tual terminals and local xdm-managed X sessions by default, but that is configurable) capabilities that they would not otherwise have, and to take those capabilities away when the are no longer logged in at the console. It provides two main kinds of capabilities: file permissions and authentication.

When a user logs in at the console and no other user is currently logged in at the console, pam_console.so will run handler programs specified in the file /etc/security/console.handlers such as pam_con? sole_apply which changes permissions and ownership of files as de? scribed in the file /etc/security/console.perms. That user may then

log in on other terminals that are considered part of the console, and as long as the user is still logged in at any one of those terminals, that user will own those devices. When the user logs out of the last terminal, the console may be taken by the next user to log in. Other users who have logged in at the console during the time that the first user was logged in will not be given ownership of the devices unless they log in on one of the terminals; having done so on any one termi? nal, the next user will own those devices until he or she has logged out of every terminal that is part of the physical console. Then the race can start for the next user. In practice, this is not a problem; the physical console is not generally in use by many people at the same time, and pam_console.so just tries to do the right thing in weird cases.

When an application attempts to authenticate the user and this user is already logged in at the console, pam_console.so checks whether there is a file in /etc/security/console.apps/ directory with the same name as the application servicename, and if such a file exists, authentica? tion succeeds. This way pam_console may be utilized to run some system applications (reboots, config tools) without root password, or to enter user password on the first system login only.

ARGUMENTS

debug turns on debugging

allow_nonroot_tty

gain console locks and change permissions even if the TTY's owner is not root.

handlersfile=filename

tells pam_console.so to get the list of the handlers from a dif? ferent file than /etc/security/console.handlers

EXAMPLE

/etc/pam.d/some-system-tool:

auth sufficient pam_rootok.so

auth required pam_console.so

/etc/pam.d/some-login-service:

auth sufficient pam_console.so

auth required pam_unix.so

session required pam_unix.so

session optional pam_console.so

FILES

/var/run/console/

/var/run/console/console.lock

/etc/security/console.apps

/etc/security/console.handlers

SECURITY NOTES

When pam_console "auth" is used for login services which provide possi?

bility of remote login, it is necessary to make sure the application

correctly sets PAM_RHOST variable, or to deny remote logins completely.

Currently, /bin/login (invoked from telnetd) and gdm is OK, others may

be not.

SEE ALSO

console.perms(5)

console.apps(5)

console.handlers(5)

pam_console_apply(8)

/usr/share/doc/pam*/html/index.html

BUGS

Let's hope not, but if you find any, please report them via the "Bug

Track" link at http://bugzilla.redhat.com/bugzilla/

AUTHORS

Michael K. Johnson <johnsonm@redhat.com>

Support of console.handlers and other improvements by Tomas Mraz <tm?

raz@redhat.com>

Red Hat 2005/10/4 pam_console(8)