NAME

pam_unix - UNIX PAM module

SYNOPSIS

[*service-name*] *module-type control-flag pam_unix* [*options*]

DESCRIPTION

The UNIX authentication service module for PAM, **pam_unix** provides functionality for three PAM categories: authentication, account management, and password management. In terms of the *module-type* parameter, they are the "auth", "account", and "password" features. It also provides a null function for session management.

UNIX Ss Authentication Module

The UNIX authentication component provides functions to verify the identity of a user (**pam_sm_authenticate**()), which obtains the relevant passwd(5) entry. It prompts the user for a password and verifies that this is correct with crypt(3).

The following options may be passed to the authentication module:

debug syslog(3) debugging information at LOG_DEBUG level.

use_first_pass If the authentication module is not the first in the stack, and a previous module obtained the user's password, that password is used to authenticate the user. If this fails, the authentication module returns failure without prompting the user for a password. This option has no effect if the authentication module is the first in the stack, or if no previous modules obtained the user's password.

try_first_pass This option is similar to the **use_first_pass** option, except that if the previously obtained password fails, the user is prompted for another password.

auth_as_self This option will require the user to authenticate themselves as themselves, not as the account they are attempting to access. This is primarily for services like su(1), where the user's ability to retype their own password might be deemed sufficient.

nullok If the password database has no password for the entity being authenticated, then this option will forgo password prompting, and silently allow authentication to succeed.

NOTE: If **pam_unix** is invoked by a process that does not have the privileges required to access the password database (in most cases, this means root privileges), the **nullok** option may cause **pam_unix** to allow any user to log in with any password.

emptyok If the password database contains the password for the entity being authenticated, but the password matches an empty string, then this option will forgo password prompting, and silently allow authentication to succeed.

The difference between this and **nullok** is that it avoids prompting for password when the password is set to an empty string, as opposed to not being set.

local_pass Use only the local password database, even if NIS is in use. This will cause an authentication failure if the system is configured to only use NIS.

nis_pass Use only the NIS password database. This will cause an authentication failure if the system is not configured to use NIS.

UNIX Ss Account Management Module

The UNIX account management component provides a function to perform account management, **pam_sm_acct_mgmt**(). The function verifies that the authenticated user is allowed to log into the local user account by checking the following criteria:

- locked status of the account compatible with pw(8) **lock**;
- the password expiry date from passwd(5);
- login.conf(5) restrictions on the remote host, login time, and tty.

The following options may be passed to the management module:

debug syslog(3) debugging information at LOG_DEBUG level.

UNIX Ss Password Management Module

The UNIX password management component provides a function to perform password management, **pam_sm_chauthtok**(). The function changes the user's password.

The following options may be passed to the password module:

debug syslog(3) debugging information at LOG_DEBUG level.

no_warn suppress warning messages to the user. These messages include reasons why the user's authentication attempt was declined.

local_pass forces the password module to change a local password in favour of a NIS one.

nis_pass forces the password module to change a NIS password in favour of a local one.

FILES

/etc/master.passwd default UNIX password database.

SEE ALSO

passwd(1), getlogin(2), crypt(3), getpwent(3), syslog(3), nsswitch.conf(5), passwd(5), pam(3), pw(8), yp(8)

BUGS

The **pam_unix** module ignores the PAM_CHANGE_EXPIRED_AUTHTOK flag.