NAME

PAM, pam − Pluggable Authentication Modules for Linux

DESCRIPTION

This manual is intended to offer a quick introduction to **Linux−PAM**. For more information the reader is directed to the **Linux−PAM system administrators' guide**.

Linux−PAM is a system of libraries that handle the authentication tasks of applications (services) on the system. The library provides a stable general interface (Application Programming Interface − API) that privilege granting programs (such as **login**(1) and **su**(1)) defer to to perform standard authentication tasks.

The principal feature of the PAM approach is that the nature of the authentication is dynamically configurable. In other words, the system administrator is free to choose how individual service−providing applications will authenticate users. This dynamic configuration is set by the contents of the single **Linux−PAM** configuration file /etc/pam.conf. Alternatively, the configuration can be set by individual configuration files located in the /etc/pam.d/ directory. The presence of this directory will cause **Linux−PAM** to *ignore* /etc/pam.conf.

Vendor−supplied PAM configuration files might be installed in the system directory /usr/lib/pam.d/ or a configurable vendor specific directory instead of the machine configuration directory /etc/pam.d/. If no machine configuration file is found, the vendor−supplied file is used. All files in /etc/pam.d/ override files with the same name in other directories.

From the point of view of the system administrator, for whom this manual is provided, it is not of primary importance to understand the internal behavior of the **Linux−PAM** library. The important point to recognize is that the configuration file(s) *define* the connection between applications (**services**) and the pluggable authentication modules (**PAM**s) that perform the actual authentication tasks.

Linux−PAM separates the tasks of *authentication* into four independent management groups: **account** management; **auth**entication management; **password** management; and **session** management. (We highlight the abbreviations used for these groups in the configuration file.)

Simply put, these groups take care of different aspects of a typical user's request for a restricted service:

account − provide account verification types of service: has the user's password expired?; is this user permitted access to the requested service?

authentication − authenticate a user and set up user credentials. Typically this is via some challenge−response request that the user must satisfy: if you are who you claim to be please enter your password. Not all authentications are of this type, there exist hardware based authentication schemes (such as the use of smart−cards and biometric devices), with suitable modules, these may be substituted seamlessly for more standard approaches to authentication − such is the flexibility of **Linux−PAM**.

password − this group's responsibility is the task of updating authentication mechanisms. Typically, such services are strongly coupled to those of the **auth** group. Some authentication mechanisms lend themselves well to being updated with such a function. Standard UN*X password−based access is the obvious example: please enter a replacement password.

session − this group of tasks cover things that should be done prior to a service being given and after it is withdrawn. Such tasks include the maintenance of audit trails and the mounting of the user's home directory. The **session** management group is important as it provides both an opening and closing hook for modules to affect the services available to a user.

FILES

/etc/pam.conf
: the configuration file

/etc/pam.d
: the **Linux−PAM** configuration directory. Generally, if this directory is present, the /etc/pam.conf file is ignored.

/usr/lib/pam.d
: the **Linux−PAM** vendor configuration directory. Files in /etc/pam.d override files with the same name

in this directory.

<vendordir>/pam.d
the **Linux−PAM** vendor configuration directory. Files in /etc/pam.d and /usr/lib/pam.d override files with the same name in this directory. Only available if Linux−PAM was compiled with vendordir enabled.

ERRORS

Typically errors generated by the **Linux−PAM** system of libraries, will be written to **syslog**(3).

CONFORMING TO

DCE−RFC 86.0, October 1995. Contains additional features, but remains backwardly compatible with this RFC.

SEE ALSO

pam(3), **pam_authenticate**(3), **pam_sm_setcred**(3), **pam_strerror**(3), **PAM**(7)