

NAME

`pam_access` – PAM module for logdaemon style login access control

SYNOPSIS

`pam_access.so` [`debug`] [`nodefgroup`] [`noaudit`] [`accessfile=`*file*] [`fieldsep=`*sep*] [`listsep=`*sep*]

DESCRIPTION

The `pam_access` PAM module is mainly for access management. It provides logdaemon style login access control based on login names, host or domain names, internet addresses or network numbers, or on terminal line names, X `$DISPLAY` values, or PAM service names in case of non-networked logins.

By default rules for access management are taken from config file `/etc/security/access.conf` if you don't specify another file. Then individual `*.conf` files from the `/etc/security/access.d/` directory are read. The files are parsed one after another in the order of the system locale. The effect of the individual files is the same as if all the files were concatenated together in the order of parsing. This means that once a pattern is matched in some file no further files are parsed. If a config file is explicitly specified with the **`accessfile`** option the files in the above directory are not parsed.

If Linux PAM is compiled with audit support the module will report when it denies access based on origin (host, tty, etc.).

OPTIONS

`accessfile=`*/path/to/access.conf*

Indicate an alternative `access.conf` style configuration file to override the default. This can be useful when different services need different access lists.

`debug`

A lot of debug information is printed with **`syslog(3)`**.

`noaudit`

Do not report logins from disallowed hosts and ttys to the audit subsystem.

`fieldsep=`*separators*

This option modifies the field separator character that `pam_access` will recognize when parsing the access configuration file. For example: **`fieldsep=|`** will cause the default `:` character to be treated as part of a field value and `|` becomes the field separator. Doing this may be useful in conjunction with a system that wants to use `pam_access` with X based applications, since the **`PAM_TTY`** item is likely to be of the form `"hostname:0"` which includes a `:` character in its value. But you should not need this.

`listsep=`*separators*

This option modifies the list separator character that `pam_access` will recognize when parsing the access configuration file. For example: **`listsep=,`** will cause the default `' '` (space) and `'\t'` (tab) characters to be treated as part of a list element value and `,` becomes the only list element separator. Doing this may be useful on a system with group information obtained from a Windows domain, where the default built-in groups "Domain Users", "Domain Admins" contain a space.

`nodefgroup`

User tokens which are not enclosed in parentheses will not be matched against the group database. The backwards compatible default is to try the group database match even for tokens not enclosed in parentheses.

MODULE TYPES PROVIDED

All module types (**`auth`**, **`account`**, **`password`** and **`session`**) are provided.

RETURN VALUES

`PAM_SUCCESS`

Access was granted.

`PAM_PERM_DENIED`

Access was not granted.

`PAM_IGNORE`

`pam_setcred` was called which does nothing.

PAM_ABORT

Not all relevant data or options could be gotten.

PAM_USER_UNKNOWN

The user is not known to the system.

FILES

/etc/security/access.conf

Default configuration file

SEE ALSO

access.conf(5), **pam.d(5)**, **pam(7)**.

AUTHORS

The logdaemon style login access control scheme was designed and implemented by Wietse Venema. The pam_access PAM module was developed by Alexei Nogin <alexei@nagin.dnntm.ru>. The IPv6 support and the network(address) / netmask feature was developed and provided by Mike Becher <mike.becher@lrz-muenchen.de>.