NAME

faillock.conf − pam_faillock configuration file

DESCRIPTION

faillock.conf provides a way to configure the default settings for locking the user after multiple failed authentication attempts. This file is read by the *pam_faillock* module and is the preferred method over configuring *pam_faillock* directly.

The file has a very simple *name = value* format with possible comments starting with # character. The whitespace at the beginning of line, end of line, and around the = sign is ignored.

OPTIONS

dir=*/path/to/tally−directory*
The directory where the user files with the failure records are kept. The default is /var/run/faillock.

audit
Will log the user name into the system log if the user is not found.

silent
Don't print informative messages to the user. Please note that when this option is not used there will be difference in the authentication behavior for users which exist on the system and non−existing users.

no_log_info
Don't log informative messages via **syslog**(3).

local_users_only
Only track failed user authentications attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users. The **faillock**(8) command will also no longer track user failed authentication attempts. Enabling this option will prevent a double−lockout scenario where a user is locked out locally and in the centralized mechanism.

deny=*n*
Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds *n*. The default is 3.

fail_interval=*n*
The length of the interval during which the consecutive authentication failures must happen for the user account lock out is *n* seconds. The default is 900 (15 minutes).

unlock_time=*n*
The access will be re−enabled after *n* seconds after the lock out. The value 0 has the same meaning as value *never* − the access will not be re−enabled without resetting the faillock entries by the **faillock**(8) command. The default is 600 (10 minutes).

Note that the default directory that *pam_faillock* uses is usually cleared on system boot so the access will be also re−enabled after system reboot. If that is undesirable a different tally directory must be set with the **dir** option.

Also note that it is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.

even_deny_root
Root account can become locked as well as regular accounts.

root_unlock_time=*n*
This option implies **even_deny_root** option. Allow access after *n* seconds to root account after the account is locked. In case the option is not specified the value is the same as of the **unlock_time** option.

admin_group=*name*
If a group name is specified with this option, members of the group will be handled by this module the

same as the root account (the options **even_deny_root** and **root_unlock_time** will apply to them. By default the option is not set.

EXAMPLES

/etc/security/faillock.conf file example:

```
deny=4
unlock_time=1200
silent
```

FILES

/etc/security/faillock.conf
the config file for custom options

SEE ALSO

faillock(8), **pam_faillock**(8), **pam.conf**(5), **pam.d**(5), **pam**(8)

AUTHOR

pam_faillock was written by Tomas Mraz. The support for faillock.conf was written by Brian Ward.