NAME

pwquality.conf − configuration for the libpwquality library

SYNOPSIS

/etc/security/pwquality.conf

/etc/security/pwquality.conf.d/.conf*

DESCRIPTION

pwquality.conf provides a way to configure the default password quality requirements for the system passwords. This file is read by the libpwquality library and utilities that use this library for checking and generating passwords.

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.

The libpwquality library also first reads all **.conf* files from the */etc/security/pwquality.conf.d* directory in ASCII sorted order. The values of the same settings are overridden in the order the files are parsed.

OPTIONS

The possible options in the file are:

difok
: Number of characters in the new password that must not be present in the old password. (default 1)

  The special value of 0 disables all checks of similarity of the new password with the old password except the new password being exactly the same as the old one.

minlen
: Minimum acceptable size for the new password (plus one if credits are not disabled which is the default). (See **pam_pwquality**(8).) Cannot be set to lower value than 6. (default 8)

dcredit
: The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password. (default 0)

ucredit
: The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. (default 0)

lcredit
: The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. (default 0)

ocredit
: The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. (default 0)

minclass
: The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others). (default 0)

maxrepeat
: The maximum number of allowed same consecutive characters in the new password. The check is disabled if the value is 0. (default 0)

maxsequence
: The maximum length of monotonic character sequences in the new password. Examples of such sequence are ’12345’ or ’fedcb’. Note that most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password. The check is disabled if the value is 0. (default 0)

maxclassrepeat
: The maximum number of allowed consecutive characters of the same class in the new password. The check is disabled if the value is 0. (default 0)

gecoscheck
If nonzero, check whether the words longer than 3 characters from the *GECOS* field of the user's **passwd** (5) entry are contained in the new password. The check is disabled if the value is 0. (default 0)

dictcheck
If nonzero, check whether the password (with possible modifications) matches a word in a dictionary. Currently the dictionary check is performed using the cracklib library. (default 1)

usercheck=*N*
If nonzero, check whether the password (with possible modifications) contains the user name in some form. It is not performed for user names shorter than 3 characters. (default 1)

usersubstr=*N*
If greater than 3 (due to the minimum length in usercheck), check whether the password contains a substring of at least *N* length in some form. (default 0)

enforcing=*N*
If nonzero, reject the password if it fails the checks, otherwise only print the warning. This setting applies only to the pam_pwquality module and possibly other applications that explicitly change their behavior based on it. It does not affect **pwmake** (1) and **pwscore** (1). (default 1)

badwords
Space separated list of words that must not be contained in the password. These are additional words to the cracklib dictionary check. This setting can be also used by applications to emulate the gecos check for user accounts that are not created yet.

dictpath
Path to the cracklib dictionaries. Default is to use the cracklib default.

retry=*N*
Prompt user at most *N* times before returning with error. The default is *1*.

enforce_for_root
The module will return error on failed check even if the user changing the password is root. This option is off by default which means that just the message about the failed check is printed but root can change the password anyway. Note that root is not asked for an old password so the checks that compare the old and new password are not performed.

local_users_only
The module will not test the password quality for users that are not present in the */etc/passwd* file. The module still asks for the password so the following modules in the stack can use the **use_authtok** option. This option is off by default.

SEE ALSO

pwscore (1), **pwmake** (1), **pam_pwquality** (8)

AUTHORS

Tomas Mraz <tmraz@redhat.com>