NAME

pam_winbind - PAM module for Winbind

DESCRIPTION

This tool is part of the **samba**(7) suite.

pam_winbind is a PAM module that can authenticate users against the local domain by talking to the Winbind daemon.

SYNOPSIS

Edit the PAM system config /etc/pam.d/service and modify it as the following example shows:

```
   ...
   auth      required       pam_env.so
   auth      sufficient     pam_unix2.so
+++ auth      required       pam_winbind.so  use_first_pass
   account   requisite      pam_unix2.so
+++ account   required       pam_winbind.so  use_first_pass
+++ password  sufficient     pam_winbind.so
   password  requisite      pam_pwcheck.so  cracklib
   password  required       pam_unix2.so    use_authtok
   session   required       pam_unix2.so
+++ session   required       pam_winbind.so
   ...
```

Make sure that pam_winbind is one of the first modules in the session part. It may retrieve kerberos tickets which are needed by other modules.

OPTIONS

pam_winbind supports several options which can either be set in the PAM configuration files or in the pam_winbind configuration file situated at /etc/security/pam_winbind.conf. Options from the PAM configuration file take precedence to those from the configuration file. See **pam_winbind.conf**(5) for further details.

debug
: Gives debugging output to syslog.

debug_state
: Gives detailed PAM state debugging output to syslog.

require_membership_of=[SID or NAME]

If this option is set, pam_winbind will only succeed if the user is a member of the given SID or NAME. A SID can be either a group-SID, an alias-SID or even an user-SID. It is also possible to give a NAME instead of the SID. That name must have the form: *MYDOMAIN\mygroup* or *MYDOMAIN\myuser* (where '\' character corresponds to the value of *winbind separator* parameter). It is also possible to use a UPN in the form *user@REALM* or *group@REALM*. pam_winbind will, in that case, lookup the SID internally. Note that NAME may not contain any spaces. It is thus recommended to only use SIDs. You can verify the list of SIDs a user is a member of with wbinfo --user-sids=SID.

This option must only be specified on a auth module declaration, as it only operates in conjunction with password authentication.

use_first_pass

By default, pam_winbind tries to get the authentication token from a previous module. If no token is available it asks the user for the old password. With this option, pam_winbind aborts with an error if no authentication token from a previous module is available.

try_first_pass

Same as the use_first_pass option (previous item), except that if the primary password is not valid, PAM will prompt for a password.

use_authtok

Set the new password to the one provided by the previously stacked password module. If this option is not set pam_winbind will ask the user for the new password.

try_authtok

Same as the use_authtok option (previous item), except that if the new password is not valid, PAM will prompt for a password.

krb5_auth

pam_winbind can authenticate using Kerberos when winbindd is talking to an Active Directory domain controller. Kerberos authentication must be enabled with this parameter. When Kerberos authentication can not succeed (e.g. due to clock skew), winbindd will fallback to samlogon authentication over MSRPC. When this parameter is used in conjunction with *winbind refresh tickets*, winbind will keep your Ticket Granting Ticket (TGT) up-to-date by refreshing it whenever necessary.

krb5_ccache_type=[type]

When pam_winbind is configured to try kerberos authentication by enabling the *krb5_auth* option,

it can store the retrieved Ticket Granting Ticket (TGT) in a credential cache. The type of credential cache can be controlled with this option. The supported values are: *KCM* or *KEYRING* (when supported by the system's Kerberos library and operating system), *FILE* and *DIR* (when the DIR type is supported by the system's Kerberos library). In case of FILE a credential cache in the form of /tmp/krb5cc_UID will be created - in case of DIR you NEED to specify a directory. UID is replaced with the numeric user id. The UID directory is being created. The path up to the directory should already exist. Check the details of the Kerberos implmentation.

When using the KEYRING type, the supported mechanism is "KEYRING:persistent:UID", which uses the Linux kernel keyring to store credentials on a per-UID basis. The KEYRING has its limitations. As it is secure kernel memory, for example bulk sorage of credentils is for not possible.

When using th KCM type, the supported mechanism is "KCM:UID", which uses a Kerberos credential manaager to store credentials on a per-UID basis similar to KEYRING. This is the recommended choice on latest Linux distributions, offering a Kerberos Credential Manager. If not we suggest to use KEYRING as those are the most secure and predictable method.

It is also possible to define custom filepaths and use the "%u" pattern in order to substitute the numeric user id. Examples:

krb5_ccache_type = DIR:/run/user/%u/krb5cc
: This will create a credential cache file in the specified directory.

krb5_ccache_type = FILE:/tmp/krb5cc_%u
: This will create a credential cache file.

Leave empty to just do kerberos authentication without having a ticket cache after the logon has succeeded. This setting is empty by default.

cached_login
: Winbind allows one to logon using cached credentials when *winbind offline logon* is enabled. To use this feature from the PAM module this option must be set.

silent
: Do not emit any messages.

mkhomedir
: Create homedirectory for a user on-the-fly, option is valid in PAM session block.

warn_pwd_expire
: Defines number of days before pam_winbind starts to warn about passwords that are going to expire. Defaults to 14 days.

PAM DATA EXPORTS

This section describes the data exported in the PAM stack which could be used in other PAM modules.

PAM_WINBIND_HOMEDIR
: This is the Windows Home Directory set in the profile tab in the user settings on the Active Directory Server. This could be a local path or a directory on a share mapped to a drive.

PAM_WINBIND_LOGONSCRIPT
: The path to the logon script which should be executed if a user logs in. This is normally a relative path to the script stored on the server.

PAM_WINBIND_LOGONSERVER
: This exports the Active Directory server we are authenticating against. This can be used as a variable later.

PAM_WINBIND_PROFILEPATH
: This is the profile path set in the profile tab in the user settings. Normally the home directory is synced with this directory on a share.

SEE ALSO

pam_winbind.conf(5), **wbinfo**(1), **winbindd**(8), **smb.conf**(5)

VERSION

This man page is part of version 4.13.17 of Samba.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.

This manpage was written by Jelmer Vernooij and Guenther Deschner.