NAME

pam_ssh - authentication and session management with SSH private keys

SYNOPSIS

[*service-name*] *module-type control-flag pam_ssh* [*options*]

DESCRIPTION

The SSH authentication service module for PAM, **pam_ssh** provides functionality for two PAM categories: authentication and session management. In terms of the *module-type* parameter, they are the "auth" and "session" features.

SSH Authentication Module

The SSH authentication component provides a function to verify the identity of a user (**pam_sm_authenticate**()), by prompting the user for a passphrase and verifying that it can decrypt the target user's SSH key using that passphrase.

The following options may be passed to the authentication module:

use_first_pass If the authentication module is not the first in the stack, and a previous module obtained the user's password, that password is used to authenticate the user. If this fails, the authentication module returns failure without prompting the user for a password. This option has no effect if the authentication module is the first in the stack, or if no previous modules obtained the user's password.

try_first_pass This option is similar to the **use_first_pass** option, except that if the previously obtained password fails, the user is prompted for another password.

nullok Normally, keys with no passphrase are ignored for authentication purposes. If this option is set, keys with no passphrase will be taken into consideration, allowing the user to log in with a blank password.

SSH Session Management Module

The SSH session management component provides functions to initiate (**pam_sm_open_session**()) and terminate (**pam_sm_close_session**()) sessions. The **pam_sm_open_session**() function starts an SSH agent, passing it any private keys it decrypted during the authentication phase, and sets the environment variables the agent specifies. The **pam_sm_close_session**() function kills the previously started SSH agent by sending it a SIGTERM.

The following options may be passed to the session management module:

want_agent Start an agent even if no keys were decrypted during the authentication phase.

FILES

$HOME/.ssh/id_rsa	SSH2 RSA key
$HOME/.ssh/id_dsa	SSH2 DSA key
$HOME/.ssh/id_ecdsa	SSH2 ECDSA key
$HOME/.ssh/id_ed25519	SSH2 Ed25519 key

SEE ALSO

ssh-agent(1), pam.conf(5), pam(3)

AUTHORS

The **pam_ssh** module was originally written by Andrew J. Korty <*ajk@iu.edu*>. The current implementation was developed for the FreeBSD Project by ThinkSec AS and NAI Labs, the Security Research Division of Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program. This manual page was written by Mark R V Murray <*markm@FreeBSD.org*>.