

Re: pam_group question/proposal

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/stable/2007-03/msg00808.html>

- *From:* Craig Boston <craig@xxxxxxxxxxxxxxxx>
 - *Date:* Thu, 29 Mar 2007 21:49:37 -0500
-

On Fri, Mar 30, 2007 at 01:16:13AM +0400, Taras Savchuk wrote:

I tried to use pam_group to allow accessing imap(dovecot) only for users in certain group (users/groups stored in AD and checked out via LDAP/Kerberos), but pam_group is checking applicant's group membership. I'm sure, that in many cases is more useful to check group membership of target (authenticating) user, but not applicant. May be it's a good to add such functionality to pam_group (i.e. ability to chose target/applicant membership check) or create separate module?

I had a similar need a while back — for FreeBSD servers running winbind as members of an AD domain. I wanted to allow ssh access for AD users, but only those in a certain group. I was unable to find a PAM module that did exactly what I wanted, so I quickly wrote something to do what I needed. You can grab it here if you like:

http://www.gank.org/pam_admins-0.1.tar.gz

It's pretty rudimentary — it looks for a file with a hardcoded path of /etc/admins.conf containing a list of groups separated by newlines(1). If the target user is in any of the listed groups, the module returns success. If not, it returns failure.

There is also an optional minuid parameter that can be passed. If it is set, it takes a numeric UID. If the target user's UID is below minuid, the module returns PAM_IGNORE. The idea was that since I have winbind mapping AD users in the 10000–20000 range, I can specify minuid=10000 so that local users will still be able to log in. I have this line in my /etc/pam.d/sshd

```
account requisite pam_admins.so minuid=10000
```

It may not be exactly what you're looking for, but hopefully it can at least be of some help.

Craig

1. To be of any real use this should probably be changed to take the

Re: pam_group question/proposal

filename as a parameter. Otherwise only one set of required groups is possible per system.

freebsd-stable@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-stable>

To unsubscribe, send any mail to "freebsd-stable-unsubscribe@xxxxxxxxxxx"