pfSense - Feature #4923

Add LDAP support for RFC2307 style group membership

08/07/2015 12:24 PM - Jonathon Reinhart

Status:	Resolved	**Start date:**	08/07/2015
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	User Manager / Privileges	**Estimated time:**	0.00 hour
Target version:	2.3		

Description

Turnkey Linux OpenLDAP (which runs the phpLDAPadmin web UI) seems to define group membership differently than pfSense expects.

The groups are defined fined as one would expect: cn=admins,ou=Groups,dc=example,dc=com

But group membership is defined by a memberUid attribute on the **group object**.

Here's some example output from ldapvi --discover:

```
5 cn=jreinhart,ou=Users,dc=example,dc=com
givenName: Jonathon
sn: Reinhart
cn: jreinhart
uid: jreinhart
uidNumber: 1000
gidNumber: 500
homeDirectory: /home/users/jreinhart
loginShell: /bin/sh
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
mail: jreinhart@example.com

6 cn=admins,ou=Groups,dc=example,dc=com
cn: admins
gidNumber: 501
objectClass: posixGroup
objectClass: top
memberUid: jreinhart
```

I'm not sure if this is defined OpenLDAP or phpLDAPadmin, but it's the case on Turnkey Linux OpenLDAP (https://www.turnkeylinux.org/openldap)

From what I gather, pfSense is expecting group membership to be defined by an e.g. memberOf attribute on the **user object**.

Many users find themselves in a position like me, where we can successfully authenticate with LDAP, but group membership cannot be established:

- https://forum.pfsense.org/index.php?topic=67546.0
- https://forum.pfsense.org/index.php?topic=64180.0
- https://forum.pfsense.org/index.php?topic=48961.0

Can this incompatibility somehow be remedied?

Associated revisions

Revision f6f7f1c2 - 08/13/2015 01:57 PM - Jim Pingle

Add support for LDAP RFC2307 style group membership. Implements #4923

To activate, check the box for RFC2307 in the LDAP server settings and fill in the group object class (typically posixGroup).

Revision 149efbea - 09/14/2015 01:36 PM - Jim Pingle

Add support for LDAP RFC2307 style group membership. Resolves #4923

History

#1 - 08/10/2015 01:21 PM - Jonathon Reinhart

The sssd-ldap(5) man page (unrelated to this bug, just informational) gives a little more insight into this:

```
ldap_schema (string)
          Specifies the Schema Type in use on the target LDAP server. Depending on the selected schema, the d
efault attribute
          names retrieved from the servers may vary. The way that some attributes are handled may also differ
.

          Four schema types are currently supported:

          ·   rfc2307

          ·   rfc2307bis

          ·   IPA

          ·   AD

          The main difference between these schema types is how group memberships are recorded in the server.
 With rfc2307, group
          members are listed by name in the memberUid attribute. With rfc2307bis and IPA, group members are l
isted by DN and
          stored in the member attribute. The AD schema type sets the attributes to correspond with Active Di
rectory 2008r2
          values.

          Default: rfc2307
```

It appears that pfSense is expecting an Active Directory type schema, whereas The default OpenLDAP schema is following RFC2307, with a memberUid attribute.

So I guess this is a feature request to support RFC2307. When I get some time, I may look into hacking at this.

#2 - 08/11/2015 06:48 PM - Jim Pingle

- Subject changed from LDAP group membership incompatible with Turnkey Linux OpenLDAP / phpLDAPadmin to Add LDAP support for RFC2307 style group membership

- Category set to User Manager / Privileges

Changed the subject of the ticket to be a little more accurate. I was looking at this a few weeks ago myself but with a basic LDAP setup in OpenLDAP and not specifically with Turnkey Linux. There are some tutorials out there for changing OpenLDAP to use a rfc2307bis schema, but none of them were viable or had various other issues.

#3 - 08/12/2015 03:25 PM - Jim Pingle

- File ldap-rfc2307.diff added

- Assignee set to Jim Pingle

- Target version set to 2.3

- Affected Architecture All added

- Affected Architecture deleted ()

Attached patch is a bit of a hack but is just a proof of concept -- when applied it will find groups for the users in the way RFC2307 expects, though I had to hardcode the group objectClass as posixGroup.

Worst case, we may need a checkbox or drop-down to choose RFC2307 vs AD style group lookups (needs a better name) and another field to enter the group objectClass when selected. Patching into 2.2.x may not be too hard but 2.3 will have to wait until after the new GUI is merged.

To find the user entries in RFC2307 style you need a filter like this (find all groups containing the username as a Member):

- Base DN = the Base DN for the LDAP server, Filter = (&(objectClass=posixGroup)(memberUid=username)), memberUid attribute required in response

The response is an array of groups that need parsed in a style as shown in the attached patch.

To find the user entries in AD style, you need a filter like this (find all groups listed on the user record in memberOf):

- Base DN = the user's DN, Filter = (cn=$username), memberOf attribute required in response

The response is the user entry and the memberOf attribute contains an array of group names.

When adding the new option it should default to the current AD style

#4 - 08/13/2015 01:56 PM - Jim Pingle

Added a checkbox for RFC2307 and an input field for the group object class (defaults to posixGroup). To activate, check the box and fill in the group object class. Works fine here with a default OpenLDAP style setup. Box defaults to unchecked for the existing behavior which still works fine with AD.

#5 - 08/13/2015 01:56 PM - Jim Pingle

Leaving this open because the code will need to be brought into 2.3 after the bootstrap merge.

#6 - 08/13/2015 02:00 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset f6f7f1c244929016d2ab4664df6d969f664a54f0.

#7 - 08/13/2015 02:03 PM - Jim Pingle

- Status changed from Feedback to Assigned

#8 - 09/14/2015 01:40 PM - Jim Pingle

- Status changed from Assigned to Feedback

Applied in changeset 149efbeac4e6eaa9d8062f26bbc172c86020e231.

#9 - 11/10/2015 02:41 PM - Jim Pingle

- Status changed from Feedback to Resolved

This has been working for a while now.

#10 - 11/17/2015 02:11 AM - Felix Wolfsteller

It does not work for me as I expected, but I have to admit that I am a LDAP-noop.

My setup contains of

```
ou=Groups,dc=siebenlinden,dc=de
```

, under which we find
groupOfNames and

```
ou=People,dc=siebenlinden,dc=de
```

, where we find
posixAccount,organizationalPeople,person and **InetOrgPerson**.

As authentication containers, I give **ou=People,dc=siebenlinden,dc=de** .
User naming attribute is "uid", group naming attribe "cn" and group member attribute "member".

I ticked the RFC2307-Checkbox.
The respective group I test is also added as "pfsense-group". Authentication via Diagnostics->Authentication works, but the groups are not shown.

I also installed the memberOf overlay (server is slapd 2.4.31-1+nmu2ubuntu8.2, ubuntu 14.04), but as far as i understood (and what tools like ldapsearch seem to confirm) this does work for FILTERING objects, but does not really add the attribute. The tests to use this but without the RFC2307-Box ticked also failed.

Is there any way to debug this issue further for me?

pfsense is at 2.2.5-RELEASE (i386) .

#11 - 11/17/2015 02:29 AM - Felix Wolfsteller

Btw this is also featured in Feature #2869 iiuc.

#12 - 11/17/2015 03:17 AM - Felix Wolfsteller

I tried to find the code that does the ldap group lookup. If I am not mistaken, it is located at https://redmine.pfsense.org/projects/pfsense/repository/revisions/149efbeac4e6eaa9d8062f26bbc172c86020e231/entry/src/etc/inc/auth.inc#L1036 (root/src/etc/inc/auth.inc#1036).

I then fired up ldapsearch with the guessed parameters:

```
 ldapsearch -h MYHOST -W -b dc=siebenlinden,dc=de -D cn=ADMIN_CN -s sub '(&(objectClass=groupofnames)(member=F
IRSTNAME.LASTNAME))'
```

with CAPITALS filled correctly (FIRSTNAME.LASTNAME is the users uid).
To this query there were no results.

If I however correctly give the full DN as member-"variable", like

```
 ldapsearch -h MYHOST -W -b dc=siebenlinden,dc=de -D cn=ADMIN_CN -s sub '(&(objectClass=groupofnames)(member=D
N_OF_USER))'
```

the command resulted in the correct groups.

That makes sense to me. The code (and maybe RFC2307) assumes that the member attribute is filled with the username, whereas the typical setup and apparently the scheme wants to have a DN there. Probably there are different between posixGroup/memberUid and groupOfNames/member ...?

#13 - 11/17/2015 03:57 AM - Felix Wolfsteller

Felix Wolfsteller wrote:

> That makes sense to me. The code (and maybe RFC2307) assumes that the member attribute is filled with the username, whereas the typical setup and apparently the scheme wants to have a DN there. Probably there are different between posixGroup/memberUid and groupOfNames/member ...?

Man, I am sorry, that should not happen, the first answer to this feature request stated the differences between rfc2307 ("memberuid" with ...well uid) and rfc2307bis ("member" with dn).

Also, I could get the RFC2307-style (posixGroup with memberuid) working, by broadening the search scope to "entire subtree". Awesome. I understood some php code.

I opened a Feature Request for rfc2307bis support:
https://redmine.pfsense.org/issues/5461 .

#14 - 05/23/2017 07:10 AM - Jim Pingle

This is not a support system. For help, please post on the forum, mailing list, or use another support method.

#15 - 05/23/2017 08:37 AM - Anonymous

- File OpenLDAP.pcapng added

#16 - 05/23/2017 08:52 AM - Jim Pingle

This bug is old, and resolved. It works perfectly, and I use it every day. If you have an issue it is different than this. Discuss the issue first on the forum, mailing list, reddit, etc. Do not open a new issue until after it has been discussed and configuration issues have been ruled out definitively by others.

Files

ldap-rfc2307.diff	1.68 KB	08/12/2015	Jim Pingle
OpenLDAP.pcapng	1.98 KB	05/23/2017	Anonymous