Bugs & Wish list
LDAP authentication to AD broken | Tiki Wiki CMS Groupware :: Development

LDAP authentication to AD broken

Status
Closed

Subject
LDAP authentication to AD broken

Version
19.x

Category
- Error

Feature
External Authentication (LDAP, AD, PAM, CAS, etc)

Resolution status
Fixed or Solved

Submitted by
Wiebe

Volunteered to solve
rjsmel0

Keep informed
Marc Laporte

Lastmod by
Wiebe

Rating
(1)

Description
With the switch from Pear Net_LDAP2 to Zend\Ldap, the LDAP authentication to the AD is broken in Tiki 19.1.
With exactly the same configuration as with Tiki 18.3, I get this error message in the Action Log:

```
Error: 0x31 (Invalid credentials; 80090308: LdapErr: DSID-0C090400, comment: AcceptSecurityContext error, data 52e, v1db1):
sAMAccountName=wiebe.oudshoorn,cn=users,dc=moba-bv,dc=local at line 262 in D
```

I have done some research with WireShark to inspect the packages from and to the LDAP server, when someone logs in to the wiki:

Tiki 18.3:

Tiki 19.1:

It's very clear where this is going wrong. It's trying to do a bind request with only the username instead of username at domain.url (row 355 in 18.3 screenshot vs row 239 in 19.1 screenshot). Although LDAP bind type is set to 'AD', so according to lib\auth\ldap.php row 184 it should add the
correct information to the bind request instead of performing a 'plain' bind.

My LDAP settings:

Importance 8
Easy to solve? 5
Priority 40

Demonstrate Bug (Tiki 19+)
This bug has been demonstrated on show2.tiki.org

Demonstrate Bug (older Tiki versions)
This bug has been demonstrated on show.tikiwiki.org

Ticket ID 7050
Created Monday 25 March, 2019 15:20:30 GMT-0000 by Wiebe
LastModif Monday 19 August, 2019 11:32:11 GMT-0000

Comments

Marc Laporte 26 Mar 19 14:38 GMT-0000
Thanks for reporting and sorry about that. https://pear.php.net/package/Net_LDAP2/ was no longer maintained so we had to make a change.

We are looking into this. And thank you for your very detailed report.

Wiebe 26 Mar 19 15:52 GMT-0000
Thank you for looking into this issue! If there is anyway I can assist, please let me know.
Wiebe 25 Apr 19 08:37 GMT-0000

Hi Marc, any news on this bug?

rjsmelo 12 May 19 12:41 GMT-0000

Hi, can you test these versions:

trunk: https://sourceforge.net/p/tikiwiki/code/69985
19.x: https://sourceforge.net/p/tikiwiki/code/69986

It should be back using user@domain for binding, when selecting Active Directory binding type.

Wiebe 14 May 19 11:08 GMT-0000

Hi Ricardo,

Unfortunately I get this message:

___ Error
Email cannot be set because this email is already in use by another user___

And I'm not able to login.

rjsmelo 16 May 19 07:17 GMT-0000

Hi Wiebe,

Just to make sure I understand, you upgrade the instance (same DB) from 18.3 to 19.1 and now the same user/password cannot be used.

(The error above sounds like tiki is attempting to create a new user)

Wiebe>rjsmelo 20 May 19 21:15 GMT-0000

Replied to
Hi...

Hi Ricardo,
Sorry for my late reply, I didn't get a notification of your reply somehow?

I did indeed upgrade same DB from 18.3 to 19.1, same settings.
Trying to login a random AD user who already has logged in 18.3 by using his AD account.

Is it helpful to capture new traces with Wireshark?
Hi...

I was comparing 18.x and 19.x/20.x/trunk and indeed there is a difference in the case of the attributes (that can easily justify this behaviour).

Do you mind testing with one of the latest version?
trunk: https://sourceforge.net/p/tikiwiki/code/70177
20.x: https://sourceforge.net/p/tikiwiki/code/70176
19.x: https://sourceforge.net/p/tikiwiki/code/70178

Marc Laporte 19 Aug 19 11:30 GMT-0000

Should be fixed in latest 20.x (reported via email)

The original document is available at https://dev.tiki.org/item7050-LDAP-authentication-to-AD-broken