Redmine - Defect #4283

LDAP attributes should be read as user

2009-11-24 23:06 - Felix Schäfer

Status:	New	**Start date:**	2009-11-24
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	LDAP	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

Currently, the LDAP Auth source connects as the "redmine" user to look for the DN associated to a username, and gathers all the necessary info needed to create a user in redmine in the same process, and only then authenticates the user against LDAP. The problem here is that the "redmune" user in LDAP needs some access to all the needed attributes for all users in the LDAP.

To avoid this, it is good practice in the LDAP world to use the "application" LDAP user to look up the DN corresponding to a username, and then look up additional attributes when connected as the user itself, not as the "application" user.

I think I could provide a patch if needed.

History

#1 - 2009-11-30 23:01 - Felix Schäfer

- File lookup_LDAP_attributes_as_user.patch added

I had a quick shot at this one and came up with the attached patch against current git (8b8c24e61f37cee0904ad8d44184da58a2f8ca43). I couldn't do extensive testing, because my dev redmine doesn't have access to an LDAP server, but the attribute-fetching query gave the expected results in irb, so that should work.

#2 - 2009-12-28 18:53 - Joe Heck

I tried the patch against 0.87 released code - I'm afraid the patch didn't apply cleanly.

I also read through the patch though, and it still requires you to authenticate/bind with a userid/password from the configuration prior to attempting to authenticate/bind with the user's provided account and credentials. I tried a variation on the theme, but found I needed to prefix the domain to the login to authenticate/bind to AD over LDAPS.

#3 - 2010-01-04 10:18 - Felix Schäfer

Hello Joe,

I whipped up the patch on trunk, so I'm not too surprised it didn't work on stable. Regarding usernames with AD: yeah, AD is a little picky, but you'ld have to prefix the login with the domain either way, even with the stock LDAP implementation, but I think it's mentioned in the guide (I've never worked with AD though, so that's all hear-say more than evidence).

Regarding the need to connect to the LDAP server with the "global" credentials upfront:

> To avoid this, it is good practice in the LDAP world to use the "application" LDAP user to look up the DN corresponding to a username, and then look up additional attributes when connected as the user itself, not as the "application" user.

Basically, most LDAP servers will only let you connect using a DN, you can't just use the "login" redmine uses, so the authentication scheme first must find the DN corresponding to the login name using the "redmine" DN, and can then connect to the LDAP server with the user DN. Currently, all operation are done through the redmine DN, which forces you to have a user in LDAP that has read rights on the names and mail addresses of everyone, with the approach of first looking up the DN corresponding to the login, you only need the redmine user to have search rights on the login attribute in LDAP.

I'm sorry if that's not very clear, but english is "only" the third language I learned. Tell me if there still is any understanding problems so I can try to be clearer.

#4 - 2013-01-14 11:19 - Daniel Felix

Any news on this suggestion? I'm sure the patch won't work with the current trunk. But the basic idea behind it sounds good.

Files