Redmine - Defect #20699

ldap error - not permitted to logon at this workstation

2015-09-08 18:22 - Alexander Ryabinovskiy

Status:	New		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:	LDAP		**Estimated time:**	0.00 hour
Target version:				
Resolution:			**Affected version:**	3.1.0

Description

I configured "LDAP authentication" for our Active Directory.
On Windows 2003 server x68 and Windows 2012 server x64 login attempts ends with the error (logged using WireShark):

```
LDAPMessage bindResponse(1) invalidCredentials (80090308: LdapErr: DSID-0C090334, comment: AcceptS
ecurityContext error, data 531, vece)
```

which means "not permitted to logon at this workstation". The solution is to add AD server to "userWorkstations" list of each domain user, and it works. But it is a bad solution and our administrators does not accept this.
This behavior was commented a year ago:
#1913#note-29

History

#1 - 2015-10-08 08:48 - Toshi MARUYAMA

- Description updated

#2 - 2017-09-21 04:40 - xuezhi li

I had the same problem with you. Have you solved this problem without adding AD server to "userWorkstations" list of each domain user?

#3 - 2017-11-22 15:38 - Alexander Ryabinovskiy

xuezhi li wrote:

> I had the same problem with you. Have you solved this problem without adding AD server to "userWorkstations" list of each domain user?

No, currently I`m using solution with Apache + sspi mod :(
http://www.redmine.org/boards/2/topics/127?page=2

#4 - 2017-12-13 12:15 - Alexander Ryabinovskiy

- File redmine_auth_source_ldap_531fix.diff added

I used this patch for auth_source_ldap to enable ldap authentification in my situation.
The idea is based on this description of "error 531" and confirmed with my tests:

```
80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893
HEX: 0x531 - not permitted to logon from this workstation
DEC: 1329 - ERROR_INVALID_WORKSTATION (Logon failure: user not allowed to log on to this computer.)
LDAP[userWorkstations: <multivalued list of workstation names>]
NOTE: Returns only when presented with valid username and password/credential.
```

So, if this error was returned - username / password are ok, and I return "true" as a authenticate_dn result.
I understand that searching in error text is not very good solution, but I don`t have any other, and it works.

Files

redmine_auth_source_ldap_531fix.diff	1.12 KB	2017-12-13	Alexander Ryabinovskiy