Redmine - Defect #8068

LDAP Authentificaton doesn't verify certificate validity

2011-04-05 08:48 - Siegfried Vogel

Status:	Closed	**Start date:**	2011-04-05
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	LDAP	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	1.1.2

Description

Security-Bug:
LDAP Authentificaton doesn't verify certificate validity of the LDAP-server-certificate. Connection to the LDAP-Server with LDAPS is established, even if the server name in the certifitcate doesn't match or the certificate authority is not trustful.

Solution: If something is wrong with the certificate, or the certificate authority is not trustful, the connection to the LDAP-Server should be closed and any LDAP-Login should be disabled.

Related issues:

Related to Redmine - Defect #24970: Net::LDAP::LdapError is deprecated	**Closed**	
Related to Redmine - Patch #29606: Support self-signed LDAPS connections	**Closed**	
Has duplicate Redmine - Defect #8091: LDAP Authentificaton doesn't verify cer...	**Closed**	**2011-04-05**

History

#1 - 2011-04-05 09:49 - Etienne Massip

- Category set to LDAP

#2 - 2011-04-05 20:49 - Ruben Kruiswijk

A possible 'fix' should be made optional. Not every company uses certificates issued by official certificate authorities. Their are enough self-signed certificates that still have to work.

#3 - 2011-06-06 21:21 - Tony Edmonds

Whether the certificate is self-signed, signed by an in-house CA, or signed by an "official" CA, doesn't matter. Redmine should attempt to check the validity of the cert against information on the local machine. Nothing about a self-signed cert precludes this.

#4 - 2011-06-06 21:49 - Tony Edmonds

I can't work out how to fix this myself, but one possible workaround is to use socat to proxy the LDAP port (389) on localhost to the real LDAPS service, validating the certificate along the way.

socat TCP4-LISTEN:389,bind=localhost,reuseaddr,fork,su=nobody OPENSSL:ldapserver.example.com:636,cafile=/etc/ssl/certs/ldapcert.pem &

Then point Redmine to localhost for LDAP (non TLS).

#5 - 2017-08-03 16:17 - ciaran jessup

The 'fix' (which should really be on by default or you could be sending your passwords **anywhere** :) can be made by changing

source:trunk/app/models/auth_source_ldap.rb@16773#L147

to something along the lines of

```
                :encryption => {
                   method: :simple_tls,
                   tls_options: OpenSSL::SSL::SSLContext::DEFAULT_PARAMS
                 }
```

(note I've removed the optional check of self.tls, this is purely for reference purposes!!!)

If the change above is made then the certificate will be verified correctly, if the certificate is self signed or not available in the operating system's certificate stores for some other reason then the instructions here explain how to install the relevant certificate.

#6 - 2018-09-16 02:35 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

Resolved by r16773. The latest version of net-ldap verifies certificates by default.

#7 - 2018-09-16 02:36 - Go MAEDA

- Related to Defect #24970: Net::LDAP::LdapError is deprecated added

#8 - 2018-09-16 02:36 - Go MAEDA

- Related to Patch #29606: Support self-signed LDAPS connections added