

Defining allowed/denied TLS Version for LDAPS in a configuration file

2022/05/09 19:06 - Admin Redmine

ステータス:	New	開始日:	2022/05/09
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:	LDAP_28	予定工数:	0.00時間
対象バージョン:		作業時間:	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/33662	status_id:	1
category_id:	28	tracker_id:	2
version_id:	0	plus1:	0
issue_org_id:	33662	affected_version:	
author_id:	463207	closed_on:	
assigned_to_id:	0	affected_version_id:	
comments:	0		

説明

Our LDAP-Server only provides TLS version 1.0 and 1.1. The newer versions 1.2 and 1.3 are currently not possible because of other connected systems. So enabling LDAPS (without certificate verification because of a self signed certificate - ticket #29606) fails in my network.

I am working on redmine version 4.1.1. For a quick workaround I have modified the file auth_source_ldap.rb to disallow version 1.2 and 1.3 by adding the appropriate options. A configurable list of allowed / denied TLS-versions (or min/max version?) in a configuration file would avoid future redmine-version-upgrade-problems (which would overwrite my manual fix).

Here is my dirty debug workaround:

```
def initialize_ldap_con(ldap_user, ldap_password)
  options = { :host => self.host,
              :port => self.port
            }
  if tls
    options[:encryption] = {
      :method => :simple_tls,
      # Always provide non-empty tls_options, to make sure, that all
      # OpenSSL::SSL::SSLContext::DEFAULT_PARAMS as well as the default cert
      # store are used.
      :tls_options => { :verify_mode => verify_peer? ? OpenSSL::SSL::VERIFY_PEER : OpenSSL::SSL::VERIFY_NONE,
                        :options => OpenSSL::SSL::OP_NO_TLSv1_3 + OpenSSL::SSL::OP_NO_TLSv1_2
                      }
    }
  end
end
```

履歴

#1 - 2022/05/10 17:00 - Admin Redmine

- カテゴリをLDAP_28 にセット