Using SASL with the tcllib ldap client

The current SASL support for the ldap client has been tested with openLDAP 2.3 and CyrusSASL,

but is considered experimental.

The OpenLDAP slapd.conf file used for testing had the following entries to map the

SASL auth information, the actual SASL passwords were stored in the sasldb with the help

of saslpasswd2:

# SASL Mappings

#

sasl-host localhost

sasl-realm ldap

authz-regexp

uid=([^,]+),(cn=[^,]+,)?cn=digest-md5,cn=auth

ldap:///ou=SomeOU,dc=tcllib,dc=tcltk??one?(uid=$i)

authz-regexp

uid=([^,]+),(cn=[^,]+,)?cn=cram-md5,cn=auth

ldap:///ou=SomeOU,dc=tcllib,dc=tcltk??one?(uid=$i)

A rather typical user of that server would be for example:

cn=James Bond,ou=SomeOU,dc=tcllib,dc=tcltk

objectClass inetOrgPerson

cn James Bond

sn Bond

uid u007

Now you can SASL auth with the tcllib ldap client with the following:

package require ldap 1.6

set handle [ldap::connect localhost]

set auth [ldap::bindSASL u007 "mollypenny"]

if {$auth} {

puts "Succesfully bound with SASL"

} else {

puts "SASL bind failed"

}

To find out your real authzId, you can then use the ldap::whoami command.

puts "auhtzId: [ldap::whoami $handle]"