auth_ldap module for saslauthd

Saslauthd can use an LDAP directory for authentication/authorization.

Sections:

1. BUILD SASLAUTHD WITH LDAP SUPPORT

Ensure that you have the OpenLDAP (http://www.openldap.org) libraries 2.1 or higher. Fetch the latest cyrus-sasl package, 2.1.17 or higher, ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/.

Unpack cyrus-sasl:
gzip -dc cyrus-sasl-2.1.17.tar.gz | tar xf -
or
tar zxf cyrus-sasl-2.1.17.tar.gz (if your tar supportz gzip)

cd cyrus-sasl-2.1.17
./configure --with-ldap (you may need to add other options, check doc/index.html for more)
make
make install

2. START SASLAUTHD WITH LDAP

Create /usr/local/etc/saslauthd.conf and add the following (modify to fit your environment):
ldap_servers: ldap://10.1.1.15/ ldap://10.1.1.25/
ldap_bind_dn: cn=operator,ou=Profile,o=foo.com
ldap_password: secret

Do not specify ldap_bind_*/ldap_password if you want to bind anonymously to your ldap server(s).

Run saslauthd:
saslauthd -a ldap

If you want to specify a different configuration file, you can do something like:
saslauthd -a ldap -O /etc/saslauthd.conf

For more command line options, check 'man saslauthd'

3. TESTING

First build testsaslauthd:
cd $sasl_src/saslauthd
make testsaslauthd

Run test utility:
./testsaslauthd -u igor -p secret
0: OK "Success."

If you get output other then Success, turn debug level for the auth syslog facility and check the syslog file. Hopefully this will give you enough information to make adjustements in the startup and/or configuration files.

4. PARAMETERS

The following are available ldap parameters. There are quite a few of those, but only ldap_servers may need to be specified. The defaults for all other parameters are adequate for most installations.

Do not use quotes (\"\') in the parameter values. The defaults are specified within the first set of <>. There may be a second set of <> which provide available values.

ldap_auth_method: <bind|fastbind> <bind|custom|fastbind>
Specify an authentication method.

The bind method uses the LDAP bind facility to verify the password. The bind method is not available when ldap_use_sasl is turned on. In that case saslauthd will use fastbind.

'bind' is the default auth method. When ldap_use_sasl is enabled, 'fastbind' is the default.

The custom method uses userPassword attribute to verify the password. Suppored hashes: crypt, md5, smd5, sha and ssha. Cleartext is supported as well.

The fastbind method (when 'ldap_use_sasl: no') does away with the search and an extra anonymous bind in auth_bind, but makes two assumptions:
1. Expanding the ldap_filter expression gives the user's fully-qualified DN
2. There is no cost to staying bound as a named user

ldap_bind_dn: <none>
Specify DN (distinguished name) to bind to the LDAP directory. Do not specify this parameter for the anonymous bind.

ldap_bind_pw: <none>
Alias for ldap_password.

ldap_default_domain: <none>
Alias for ldap_default_realm.

ldap_default_realm: <none>
The default realm is assigned to the %r token when realm is not available. See ldap_filter for more.

ldap_deref: <none> <search|find|always|never>
Specify how aliases dereferencing is handled during search.

ldap_filter: <uid=%u>
Specify a filter. The following tokens can be used in the filter string:

%% = %
%u = user
%U = user portion of %u (%U = test when %u = test@domain.tld)

```
      %d   = domain portion of %u if available (%d = domain.tld when %u =
             %test@domain.tld), otherwise same as %r
      %1-9 = domain tokens (%1 = tld, %2 = domain when %d = domain.tld)
      %s   = service
      %r   = realm
      %D   = user DN (available for group checks)

      The %u token has to be used at minimum for the filter to be useful.  If
      ldap_auth_method is 'bind', the filter will search for the DN
      (distinguished name) attribute.  Otherwise, the search will look for
      the 'ldap_password_attr' (see below) attribute.

ldap_group_attr: <uniqueMember>
    Specify what attribute to compare the user DN against in the group. If
    ldap_group_dn is not specified, this parameter is ignored.  If
    ldap_group_match_method is not attr, this parameter is ignored.

ldap_group_dn: <none>
    If specified, the user has to be part of the group in order to authenticate
    successfully.  Tokens described in 'ldap_filter' (see above) can be used
    for substitution.

ldap_group_filter: <none>
    Specify a filter. If a filter match is found then the user is in the group.
    Tokens described in 'ldap_filter' (see above) can be used for for
    substitution. If ldap_group_dn is not specified, this parameter is ignored.
    If ldap_group_match_method is not filter, this parameter is ignored.

ldap_group_match_method: <attr> <attr|filter>
    Specify whether the group match method uses ldap_group_attr or
    ldap_group_search.  If ldap_group_dn is not specified, this parameter is
    ignored.

ldap_group_search_base: <if not specified, it defaults to ldap_search_base>
    Specify a starting point for the group search: e.g. dc=foo,dc=com.  Tokens
    described in 'ldap_filter' (see below) can be used for substitution.

ldap_group_scope: <sub> <sub|one|base>
      Group search scope.

ldap_password: <none>
      Specify the password for ldap_bind_dn or ldap_id if
      ldap_use_sasl is turned on.  Do not specify this parameter for the
      anonymous bind.

ldap_password_attr: <userPassword>
        Specify what password attribute to use for password verification.

ldap_referrals: <no>
      Specify whether or not the client should follow referrals.

ldap_restart: <yes>
      Specify whether or not LDAP I/O operations are automatically restarted
      if they abort prematurely.

ldap_id: <none>
      Specify the authentication ID for SASL bind.

ldap_authz_id: <none>
      Specify the proxy authorization ID for SASL bind.

ldap_mech: <none>
      Specify the authentication mechanism for SASL bind.
```

ldap_realm: <none>
      Specify the realm of authentication ID for SASL bind.

ldap_scope: <sub> <sub|one|base>
      Search scope.

ldap_search_base: <none>
      Specify a starting point for the search: e.g. dc=foo,dc=com. Tokens
      described in 'ldap_filter' (see below) can be used for substitution.

ldap_servers: <ldap://localhost/>
      Specify URI(s) refering to LDAP server(s), e.g. ldaps://10.1.1.2:999/.
      You can specify multiple servers separated by a space.

ldap_start_tls: <no>
      Use StartTLS extended operation. Do not use ldaps: ldap_servers when
      this option is turned on.

ldap_time_limit: <5>
      Specify a number of seconds for a search request to complete.

ldap_timeout: <5>
      Specify a number of seconds a search can take before timing out.

ldap_tls_check_peer: <no> <yes|no>
      Require and verify server certificate. If this option is yes,
      you must specify ldap_tls_cacert_file or ldap_tls_cacert_dir.

ldap_tls_cacert_file: <none>
      File containing CA (Certificate Authority) certificate(s).

ldap_tls_cacert_dir: <none>
      Path to directory with CA (Certificate Authority) certificates.

ldap_tls_ciphers: <DEFAULT>
      List of SSL/TLS ciphers to allow. The format of the string is
      described in ciphers(1).

ldap_tls_cert: <none>
      File containing the client certificate.

ldap_tls_key: <none>
      File containing the private client key.

ldap_use_sasl: <no>
      Use SASL bind rather than simple bind when connecting to the ldap
      server.

ldap_version: <3> <2|3>
      Specify the LDAP protocol version. If ldap_start_tls and/or
      ldap_use_sasl are enabled, ldap_version will be automatiacally set to
      3.

5. NOTES

For better performance ensure that the attributes specified in ldap_filter are
indexed.

My testing shows that 'custom' is 2-3 times faster than 'bind'
ldap_auth_method. The 'fastbind' auth_method is just as fast or faster. The
slower performace of the 'bind' auth_method is caused by two extra calls to
ldap_bind() per each authentication.

SASL bind should be used with the 'fastbind' auth_method:

```
ldap_servers: ldaps://10.1.1.2/
ldap_use_sasl: yes
ldap_mech: DIGEST_MD5
ldap_auth_method: fastbind
```

At this time this is not the best performing solution because openldap (2.1.x) cannot reuse existing connection for multiple ldap_sasl_bind()s. This will hopefully change when openldap 2.2 comes out.

6. TODO

- Port to other ldap libraries
- There may be bind problems when following referrals. Normally this is not an issue.
- Allow to specify an attribute other than userPassword for use in the custom authentication method. (Done)
- Add more password hashes such as md5, sha etc (Done)
- Make a suggestion (possibly another authentication method?) (added fastbind) thanks to Simon Brady <simon.brady@otago.ac.nz>

7. FEEDBACK

Feedback is much appreciated! Please drop me a note if you are successfully using ldap-enabled saslauthd. Any code improvements and/or suggestion are welcome.

If you have questions, send email to cyrus-sasl@lists.andrew.cmu.edu. Please include relevant information about your saslauthd setup: at minimum provide your saslauth.conf, output from syslog and which directory server you're using.

8. AUTHOR

Igor Brezac <igor@ipass.net>.