

OpenLDAP Windows 版

OpenLDAP の Windows 版の情報が、<http://lucas.bergmans.us/hacks/openldap/>にある。バイナリパッケージが用意されていて、<http://download.bergmans.us/openldap/>アーカイブの実体が存在する。

ここでは、[openldap-2.2.29](#) が最新のものとして存在する。この文書を執筆時点での最新は **OpenLDAP 2.3.37** となっているため、やや古いのであるが、テストに用いるには問題ないだろう。ここでは、Windows 版バイナリの OpenLDAP をインストールして、BDB(BerkeleyDB)を使ったシンプルな LDAP の設定例を紹介する。また、Windows で利用可能なフリーの LDAP クライアントとエディタも紹介しておく。

OpenLDAP Windows 版のインストール

まず、OpenLDAP Windows 版のバイナリパッケージをダウンロードする。

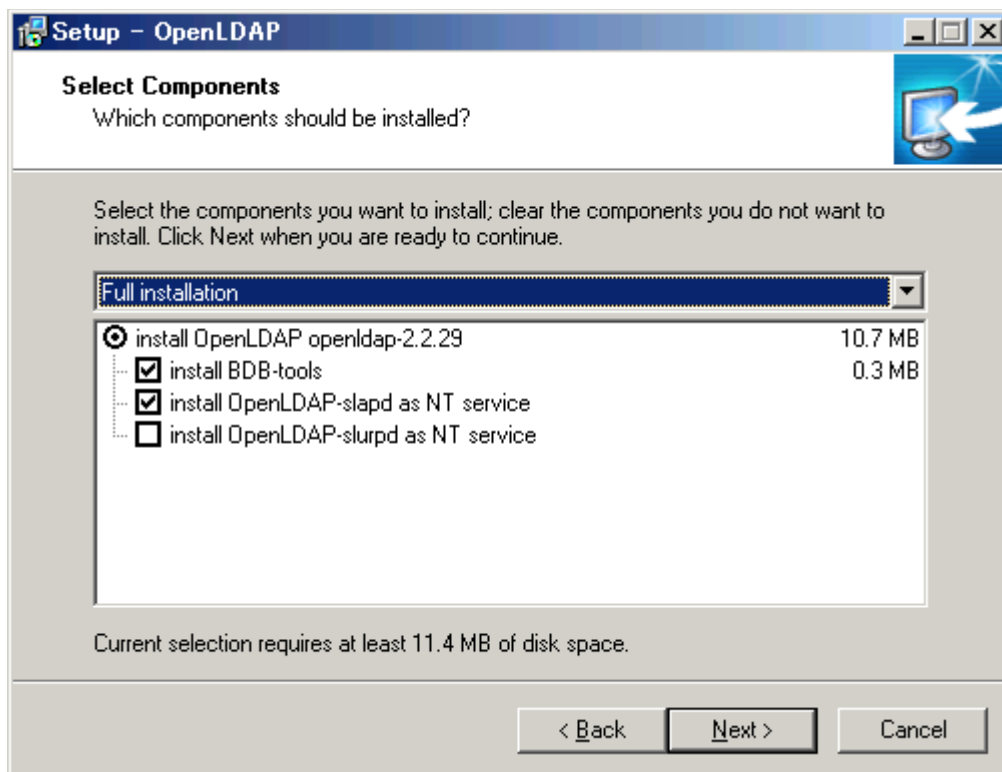
http://download.bergmans.us/openldap/openldap-2.2.29/openldap-2.2.29-db-4.3.29-openssl-0.9.8a-win32_Setup.exe

(実際には2つあり、BDB 対応のみと、BDB と S Q L に対応したパッケージが用意されている。ここでは、SQL にも対応したパッケージで説明する。)

上記 URL でインストールしたパッケージは .exe 形式で、実行するとインストーラが起動するので、ダイアログにしたがってインストールをする。



インストールの過程で、Windows サービスとしてインストールすることも選択可能である。Windows サービスへの登録は、インストール後にコマンド行でも可能である。



インストールが終わると、OpenLDAP フォルダ（デフォルトでは、“c:\Program Files\OpenLDAP\”）に実行ファイルと設定ファイルがインストールされる。

OpenLDAP BDB の設定

ここでは、ドメインを “example.com”、管理用コモン名を “root” として設定を行うことにする。LDAP サーバは slapd という名前のプログラムで、その設定は slapd.conf ファイルに行う。インストールした Windows 版 OpenLDAP には、この slapd.conf ファイルの雛形が用意されている。このファイルを編集し、BDB のデータベースの定義を次のように記述する。

```
database          bdb
suffix            "dc=example,dc=com"
rootdn            "cn=root,dc=example,dc=com"
rootpw            secret
directory         ./data
```

OpenLDAP のサーバ起動

設定が終わったら、slapd.exe を実行し、LDAP サーバを起動する（-d 1 はデバッグオプションで、レベル 1 を指定、サーバの動作状況が出力がされる）。

```
C:\Program Files\OpenLDAP> .\slapd -d 1
```

LDIF ファイルから root ノードの初期化

root ノードの情報を LDIF フォーマットでファイルに作成し、ldapadd コマンドでその内容を LDAP サーバに登録する。

ここでは、rootnode.ldif というファイル名で次の内容の LDIF ファイルを作成する。

```
dn: dc=example,dc=com
objectclass: top
objectclass: dcObject
objectclass: organization
o: Example
dc: example

dn: cn=root,dc=example,dc=com
objectclass: organizationalRole
cn: Root
```

このファイルの内容を、次のようなコマンドラインで LDAP サーバに登録する。

```
C:\Program Files\OpenLDAP> .\ldapadd.exe
-D "cn=root,dc=example,dc=com"
-w secret -v -f rootnode.ldif
(実際は 1 行)
```

登録が済んだら、ldapsearch コマンドで実際に LDAP サーバに問い合わせ、内容を確認する。

```
C:\Program Files\OpenLDAP>.\ldapsearch -x -s base (objectclass=*)
```

Windows 版 LDAP クライアント

Softerra 社(<http://www.ldapbrowser.com/>)は、LDAP.v2 と LDAP.v3 のプロトコルに対応した LDAP 管理ツール製品を開発していて、Softerra LDAP Browser は無料で使える LDAP クライアントである(Softerra LDAP Administrator は有料)。Web サイトの “download” ページから ldapbrowser26.msi というインストーラがダウンロードできるので、これを実行し、インストールを行う。

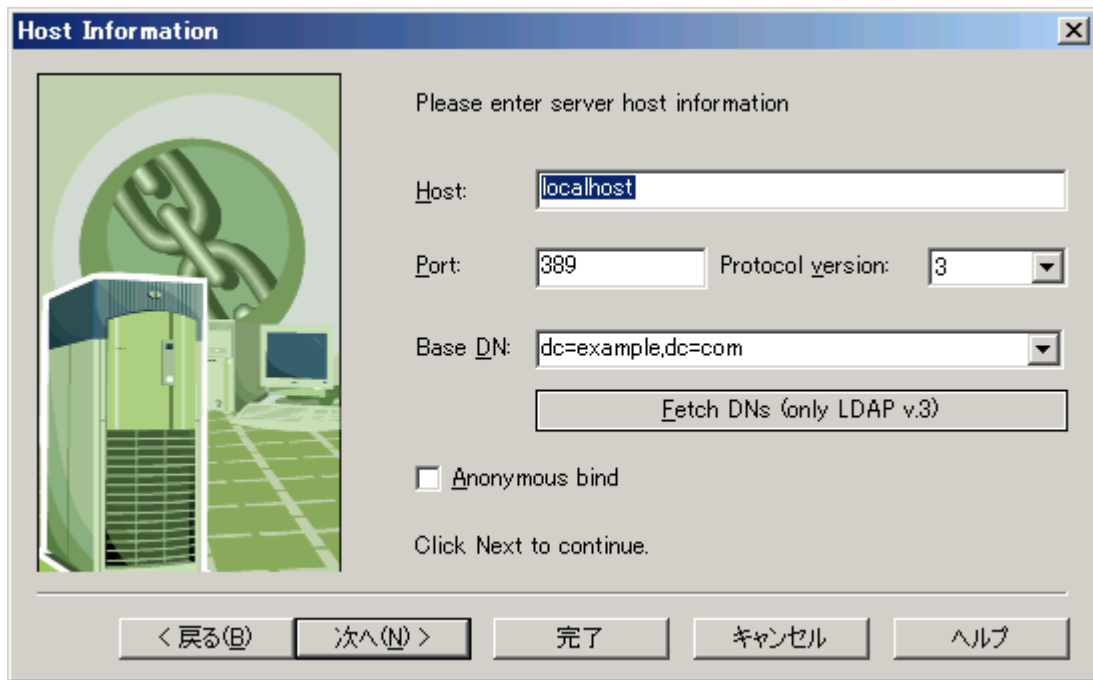


インストール後、LDAP Browser 2.6 を起動し、サーバや識別名、管理アカウントなどを設定して、LDAP サーバにアクセスできる。

まず、[File] -> [New Profile] でダイアログを開き、プロファイル名を指定する。



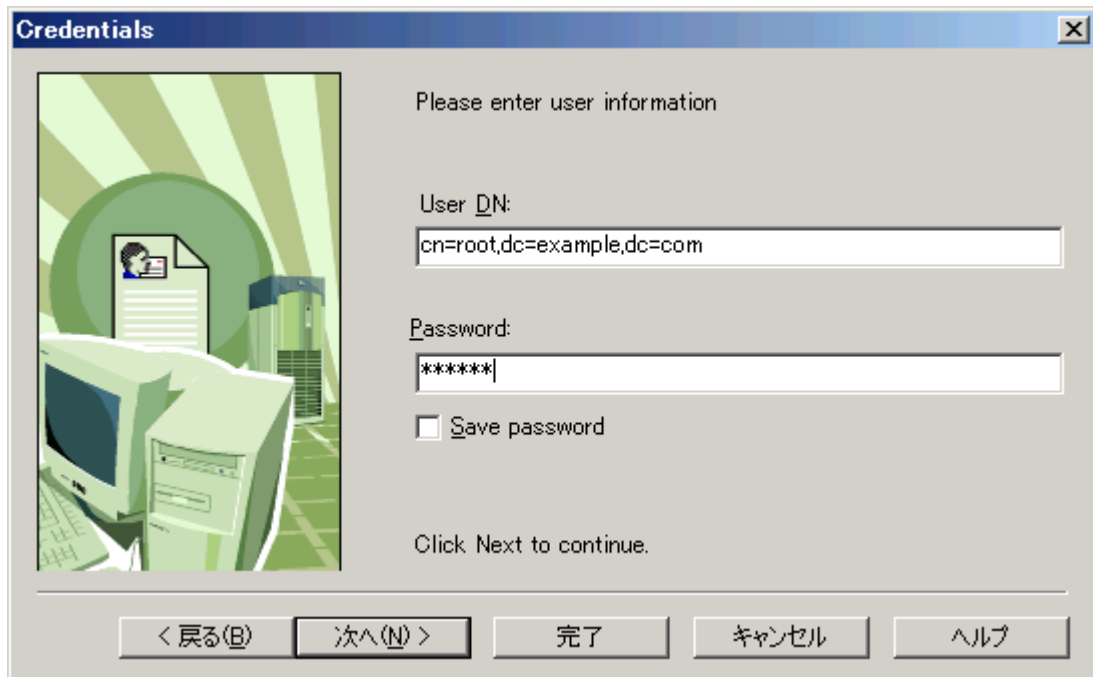
次に、サーバの情報(Host, Port)とベース・ディストリングウィッシュネーム(Base DN)を指定する。



The 'Host Information' dialog box is titled 'Host Information' and contains the following elements:

- A decorative image on the left showing server racks and a network diagram.
- The text 'Please enter server host information'.
- Input fields for 'Host' (containing 'localhost'), 'Port' (containing '389'), and 'Protocol version' (a dropdown menu set to '3').
- A dropdown menu for 'Base DN' containing 'dc=example,dc=com'.
- A button labeled 'Fetch DN's (only LDAP v.3)'.
- An unchecked checkbox labeled 'Anonymous bind'.
- The instruction 'Click Next to continue.'
- Navigation buttons at the bottom: '< 戻る(B)', '次へ(N) >', '完了', 'キャンセル', and 'ヘルプ'.

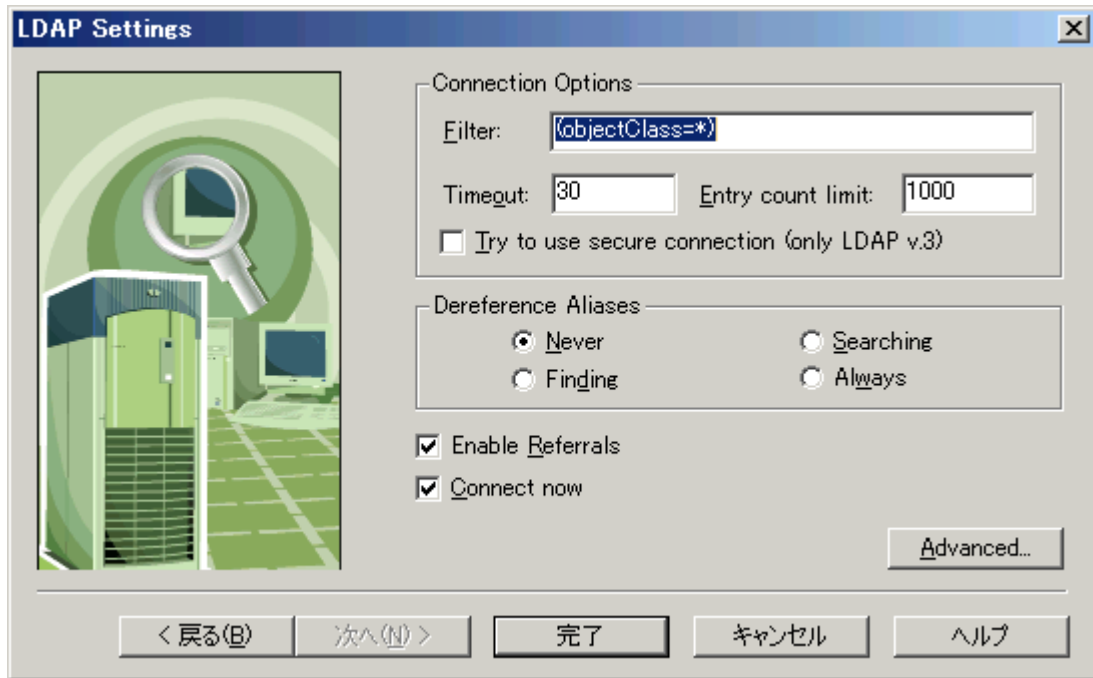
そして、ユーザのディストリングウィッシュネーム(User DN)とパスワード(Password)を指定する。



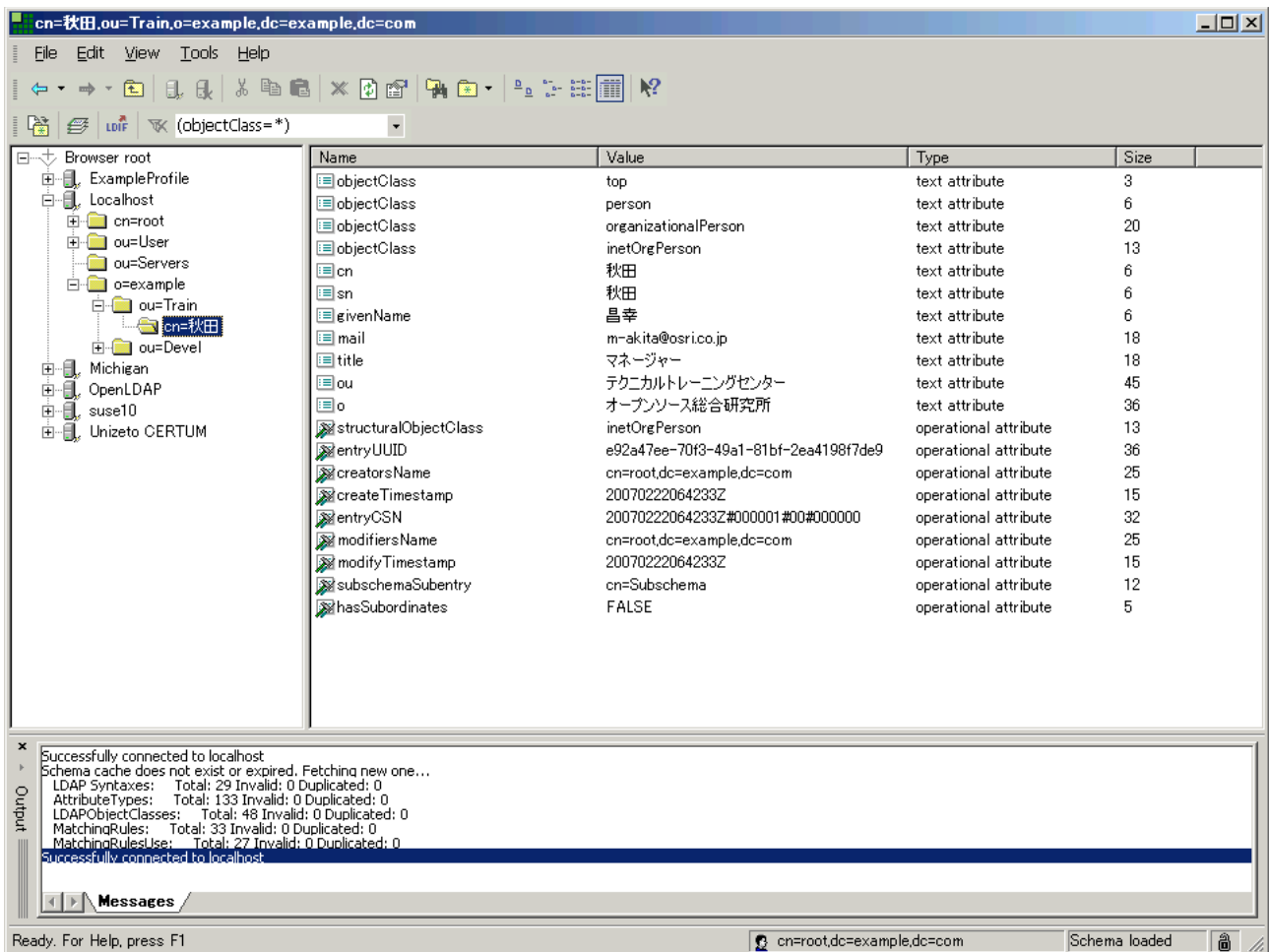
The 'Credentials' dialog box is titled 'Credentials' and contains the following elements:

- A decorative image on the left showing a computer monitor, keyboard, and server rack.
- The text 'Please enter user information'.
- An input field for 'User DN' containing 'cn=root,dc=example,dc=com'.
- An input field for 'Password' containing '*****'.
- An unchecked checkbox labeled 'Save password'.
- The instruction 'Click Next to continue.'
- Navigation buttons at the bottom: '< 戻る(B)', '次へ(N) >', '完了', 'キャンセル', and 'ヘルプ'.

最後に、検索の条件（フィルタ）を指定して完了する。



LDAP ブラウザに情報が表示される。見たい属性をクリックすることで内容を確認することができる。



LDAP Browser/Editor

LDAP Browser/Editor は Java で書かれた LDAP のブラウザ兼エディタで、

<http://www-unix.mcs.anl.gov/~gawor/ldap/>

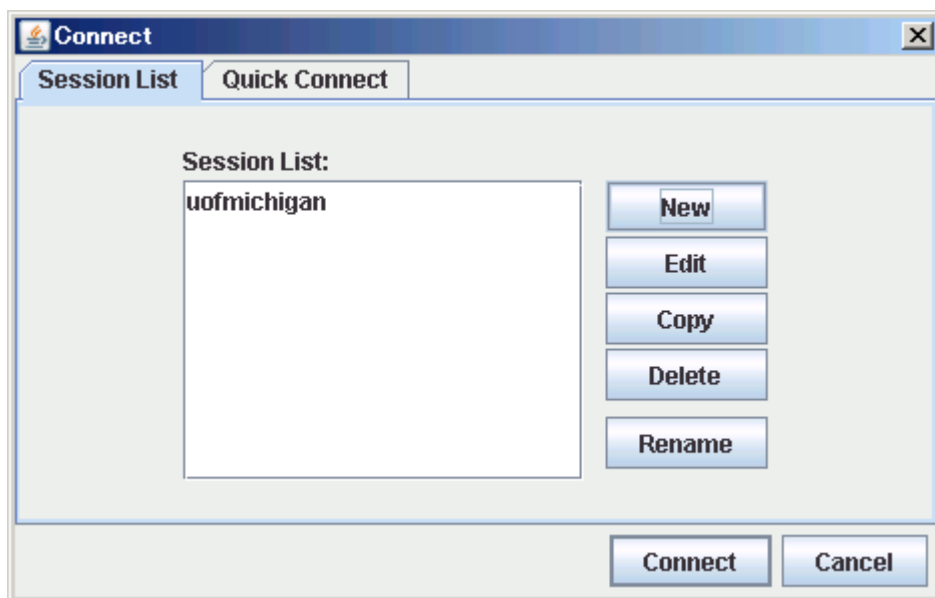
に情報がある。

ダウンロードページから、

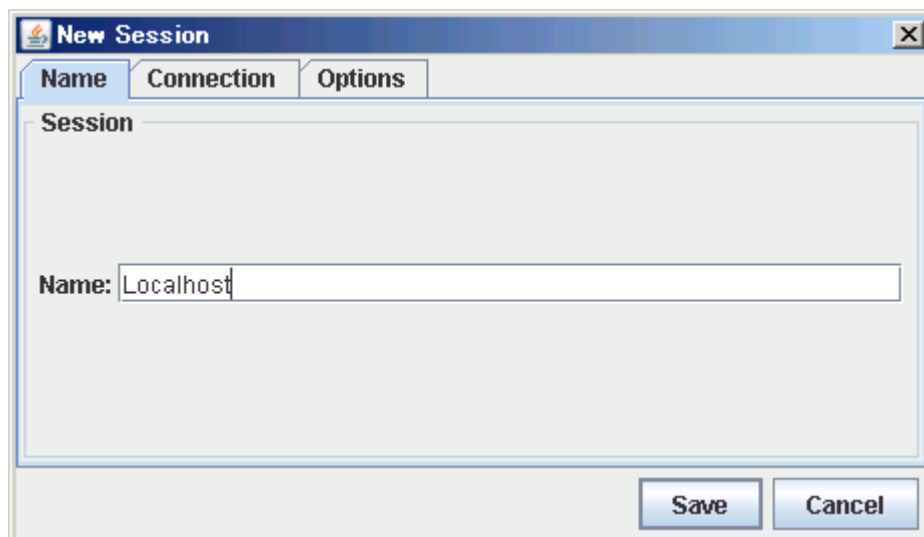
<http://www-unix.mcs.anl.gov/~gawor/ldap/dwld/bin-dwld.cgi?fileid=282b2zip>

をダウンロードして展開し、lbe.bat を実行することで起動できる。ただし、Java の実行環境が必要。

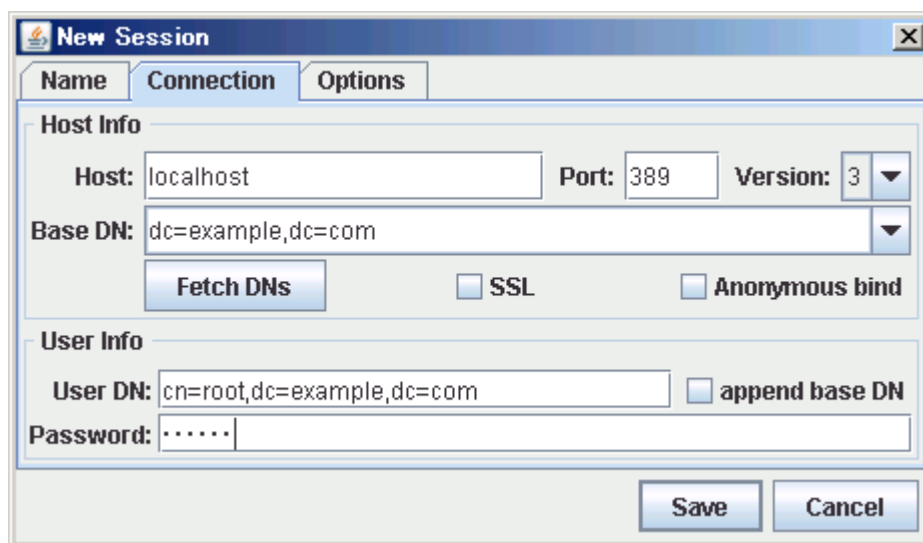
実行後、まず最初にセッションリストにはデフォルトのミシガン大学しかないので[New]を選択する。



セッション名をつける。

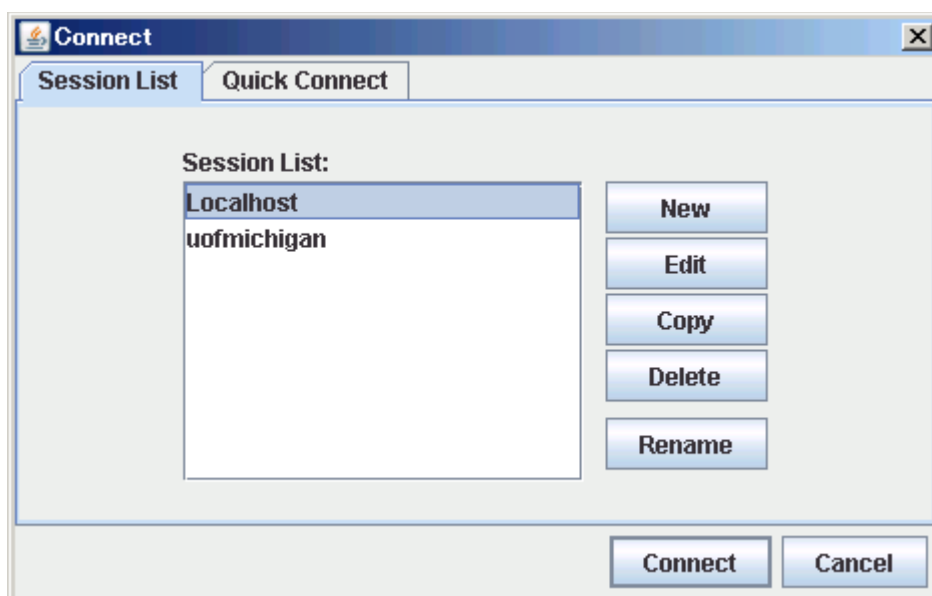


次に接続タブを選択肢、ベースDNを入力する。そして、“Anonymous bind”のチェックをはずし、User DN と Password を入力し保存(Save)する。



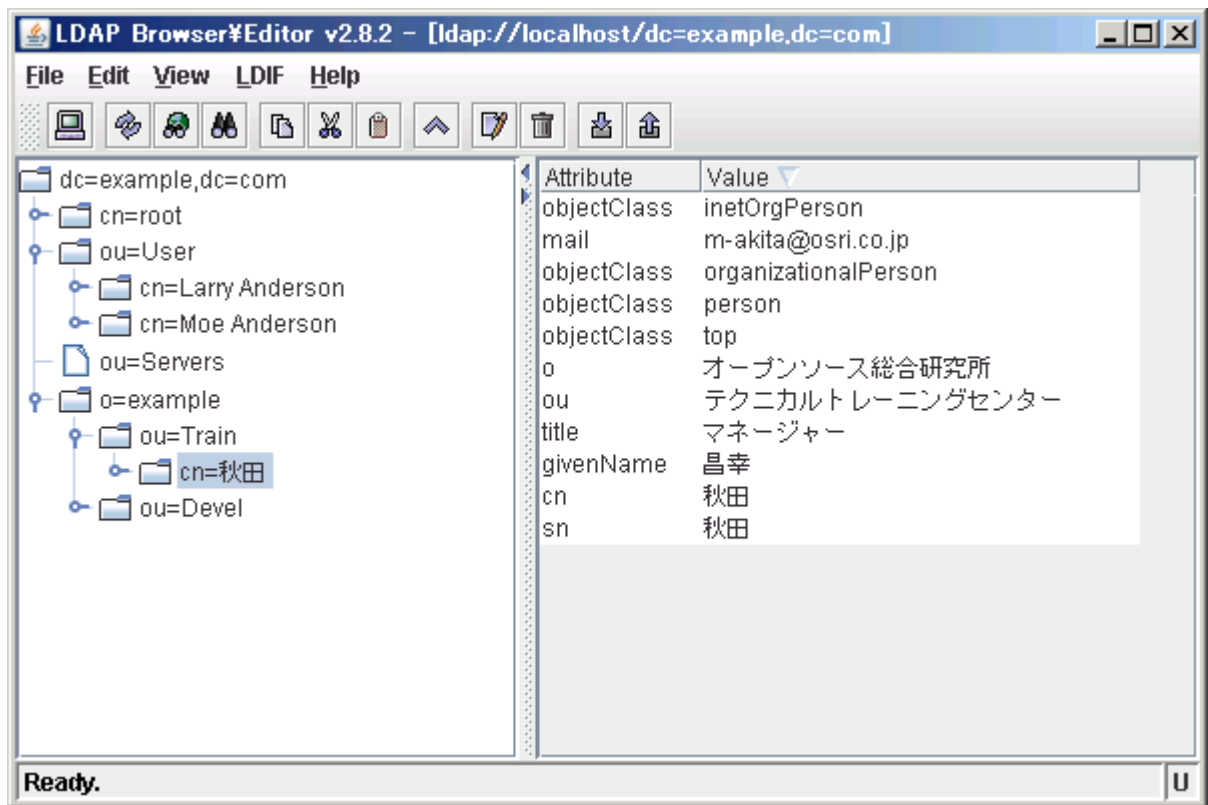
The screenshot shows the 'New Session' dialog box with the 'Options' tab selected. The 'Host Info' section contains the following fields: Host (localhost), Port (389), Version (3), and Base DN (dc=example,dc=com). There are checkboxes for 'Fetch DNs', 'SSL', and 'Anonymous bind'. The 'User Info' section contains the User DN (cn=root,dc=example,dc=com) and a checkbox for 'append base DN'. The Password field is masked with dots. 'Save' and 'Cancel' buttons are at the bottom right.

登録したセッションを選択し、接続(Connect)する。



The screenshot shows the 'Connect' dialog box with the 'Session List' tab selected. The 'Session List' contains two entries: 'Localhost' and 'uofmichigan'. To the right of the list are buttons for 'New', 'Edit', 'Copy', 'Delete', and 'Rename'. At the bottom right are 'Connect' and 'Cancel' buttons.

LDAP サーバの情報が表示されるので、左側ペインで見たい項目をダブルクリックすると右側ペインにその内容が表示される。



右側ペインでは編集したい項目をダブルクリックすると編集用のダイアログボックスがポップアップする。ただし、日本語の対応は不十分であり、変更ができないことがある。

その他の LDAP 管理ツール

参考までに、LDAP サービスの設定情報として有用な Coral Directory と PHPLDAPAdmin について少し触れておく。

Coral Directory

[Coral Directory & LDAP INFORMATION](#) では、CoralDirectory という製品を通して LDAP にさまざまな認証を統合する方法を紹介している。ここで管理しようとするデータには以下のものがある。

- Apache Basic 認証
- DHCP の IP アドレス
- E メールアドレス帳
- 電子証明書(公開鍵)
- Web サイトブックマーク

※注意) Coral Directory はシェアウェアのため、サポートやバージョンアップのためには料金が発生する。

CoralDirectory は現在、日本のみでシェアウェア配布されております(日本以外はフリーウェア)。しかし実質日本でも機能制限なしで配布しているのがフリーウェアとして扱われます。もし使用される対価(Vector の場合 2,205 円を支払ってもらえれば、主なアップデート情報をメール配信します。
(<http://bhd.staba.jp/ldap/CoralLS.htm> より)

phpLDAPAdmin

phpLDAPAdmin は PHP で書かれた LDAP 管理ツールで、LDAP 対応の PHP を実行できる Web サーバ上で実行可能である。phpLDAPAdmin を利用することにより、LDAP 情報のリモート管理を Web ブラウザから行うことが可能になる。ただし、ネットワーク経由でアクセスをする場合は、SSL/TLS の安全なセッションを経由することをお勧めする。

<http://phpldapadmin.sourceforge.net/>

