OpenLDAP Windows 版

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

ここでは、 openIdap-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/openIdap/0penIdap-2.2.29/openIdap-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SQL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。

🚰 Setup – OpenLDAP	
	Welcome to the OpenLDAP Setup Wizard
	This will install openIdap-2.2.29 on your computer.
	It is recommended that you close all other applications before continuing.
	Click Next to continue, or Cancel to exit Setup.
	[<u>Next></u>] Cancel

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。

🚰 Setup – OpenLDAP	
Select Components Which components should be installed?	R
Select the components you want to install; clear the components you install. Click Next when you are ready to continue.	u do not want to
Full installation	
 install OpenLDAP openIdap-2.2.29 ✓ install BDB-tools ✓ install OpenLDAP-slapd as NT service Install OpenLDAP-slurpd as NT service 	10.7 MB 0.3 MB
Current selection requires at least 11.4 MB of disk space.	
< <u>B</u> ack Ne	ext > Cancel

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(-d1はデバグオプションで、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て、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(<u>http://www.ldapbrowser.com/</u>)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 "dwonload" 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。

Server Connection Profile Wizard	i 🔟
	Please enter connection profile name
	Connection profile <u>n</u> ame: Localhost
	Click Next to continue.

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

Host Information		×
	Please ent	er server host information
	<u>H</u> ost:	localhost
	<u>P</u> ort:	389 Protocol version: 3
	Base <u>D</u> N:	dc=example,dc=com
		Eetch DNs (only LDAP v.3)
	<u>∏</u> <u>A</u> nonyr	nous bind
	Click Next	to continue.
〈 戻る(8) 〉 次へ(1)	0>	完了 キャンセル ヘルプ

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

Credentials	×
	Please enter user information
	User <u>D</u> N: cn=root,dc=example,dc=com
	Password: *****
	☐ Save password
	Click Next to continue.
く 戻る(<u>B</u>) 次へ	(N) > 完了 キャンセル 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 Settings		×
	Connection Options — <u>F</u> ilter: CobjectClas Timeout: 30	<u>E</u> ntry count limit: 1000
	Dereference Aliases —	connection (only LDAP v.3) © <u>S</u> earching © Al <u>w</u> ays
	☑ Enable <u>R</u> eferrals ☑ <u>C</u> onnect now	<u>A</u> dvanced
	♪〉 完了	キャンセル ヘルプ

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。

	cample,dc=com				<u>_ </u>
Eile Edit <u>V</u> iew <u>T</u> ools <u>H</u> elp					
← • → • 🗈 9, 9, % Pa 🕻	1 × 🖸 😭 🏪 🖬 • º 🛓 📜	IIII N?			
👔 🚰 📫 😿 (objectClass=*)	•				
Browser root ExampleProfile Localhost u=0, Localhost u=User u=Servers u=Servers u=Train u=Devel defined d	Name Colored Class Colored Cl	Value top person organizationalPerson inetOrgPerson 秋田 昌幸 m-akita@osrico.jp マネージャー テクニカルトレーニングセンター オープンソース総合研究所 inetOrgPerson e92a47ee-70f3-49a1-81bf-2ea4198f7de9 cn=root.dc=example.dc=com 200702220642332 200702220642332#000001#00#000000 cn=root.dc=example.dc=com 200702220642332 cn=Subschema	Type text attribute text attribute operational attribute operational attribute operational attribute operational attribute operational attribute operational attribute operational attribute operational attribute operational attribute	Size 3 6 20 13 6 6 6 18 18 18 45 36 13 36 25 15 32 25 15 12	
Successfully connected to localhost Schema cache does not exist or expired. LDAP Syntaxes: Total: 29 Invalid: 01 LDAPObjectClasses: Total: 48 Invalid: DuachingRules: Total: 33 Invalid: 00 DuAchingRules: Total: 27 Invalid: 01 MatchingRules: Total: 27 Invalid: 01 MatchingRules: Total: 27 Invalid: 01 Ressaces Ready. For Help, press F1	Fetching new one Duplicated: 0 Duplicated: 0 Uplicated: 0 0 Duplicated: 0 0 Duplicated: 0	FALSE	operational attribute	5 Schema loaded	

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。

🛓 Connect			×
Session List	Quick Connect		
	Session List: uofmichigan	New Edit Copy Delete Rename	
		Connect	Cancel

セッション名をつける。

🛃 New Session	×
Name Connection Options	
- Session	
Name: Localhost	
L	Save Cancel

次にコネクションタブを選択肢、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。

🕌 New Se	ssion				×
Name	Connection	Options			
- Host Info					
Host:	localhost			Port: 389	Version: 3 💌
Base DN:	dc=example,d	c=com			-
	Fetch DNs		SSL		Anonymous bind
- User Info					
User DN	: cn=root,dc=e	xample,dc=	com		append base DN
Password	:				
				Sav	/e Cancel

登録したセッションを選択し、接続(Connect)する。

🚣 Connect	×
Session List Quick Connect	
Session List: Localhost uofmichigan	New Edit Copy Delete Rename
	Connect Cancel

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。

LDAP Browser¥Editor v2.8.2 - [Idap://localhost/dc=example.dc=com]			
<u>File Edit View LDIF H</u> elp			
□ ●			
 dc=example,dc=com cn=root ou=User cn=Larry Anderson cn=Moe Anderson ou=Servers o=example o=example ou=Train cn=秋田 ou=Devel 	Attribute objectClass mail objectClass objectClass objectClass ou ou title givenName cn sn	Value V inetOrgPerson m-akita@osri.co.jp organizationalPerson person top オープンソース総合研究所 テクニカルトレーニングセンター マネージャー 昌幸 秋田 秋田	
Ready.			U

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

<u>Coral Directory & LDAP INFORMATION</u>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で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/

