Tips: LDAP と連携した WebCT 認証

概要

WebCT はグローバルデータベースと呼ばれる内部データベースを用いて WebCT ID 及びパスワードを認証しています。しかし既に外部に認証可能なシステムを構築している場合などは、パスワードをそのシステムに統合して管理したいとお考えになるのでは無いでしょうか。WebCT では現在、Kerberos 認証、LDAP 認証、カスタム認証という 3 つの外部認証方式をサポートしています。今回はその中から LDAP と連携した認証に関して説明します。LDAP サーバの中でもフリーの実装である OpenLDAP を RedHat Linux 7.3 に展開して、簡単なユーザ情報を持つディレクトリサービスを構築し、その中にパスワードを格納して WebCT の認証に利用してみることで WebCT の LDAP 認証がどのように行うことが出来るか見ていくことにします。

＊ LDAP と統合した認証を行う為には Institution ライセンスが必要となります＊

なお、今回は例示的にLDAPサーバの構築を行ないますが、LDAPの構築、運営自体に関するお問い合わせはサポートの対象外であることをご了承下さい。サーバの構築を行うといってもWebCTとの連携を示すだけの実験的なものです。十分に実験可能なシステム上で行うようにして下さい。可能であれば(VMWare: http://www.networld.co.jp/products/vmware/)のご使用をおすすめします(評価版もあります)。

この Tips は以下の内容を含んでいます

- OpenLDAP のインストール
- DIT の設計及びサーバの起動
- その他 LDAP Tips

OpenLDAP のインストール

今回は RedHat Linux 7.3 に限定した Tips になっているので、RPM パッケージを用いたインストールを行ないます。

まず、お使いのシステム内に既に OpenLDAP がインストールされているかどうかをチェックする必要があります。以下のコマンドを入力して下さい。

```
$ rpm -qa | grep openldap
```

単に**openldap-2.0.23-4**と表示される場合はmanとライブラリ等が入ったベースのパッケージのみがインストールされている状態になっています。OpenLDAPサーバを運営するためには、これ以外に以下のパッケージをインストールしなくてはいけません。(なお、以下のパッケージが表示された場合には、インストール作業は必要ありません。)

- openldap-clients
- openldap-servers
- (openldap-devel)

devel は開発用なので特に必要が無ければ入れる必要は無いでしょう。よって、ここでは、openldap-clients と openldap-servers のインストールを行います。

まずは openldap-clients のインストールから行ないます。openldap-licents は Red Hat Linux の disc2 にあるので、root になって Red Hat Linux の disc2 をマウントした後、rpm からインストールします。

以下、例を示します。

```
$ su
# mount /dev/cdrom /mnt
# cd /mnt/RedHat/RPMS
```

```
# rpm -ivh openldap-clients-2.0.23-4.i386.rpm
# cd
# umount /mnt
```

これで openldap-clients パッケージがインストールされました。

続いて openldap-servers をインストールします。

このパッケージは、make と libtool-libs に依存している関係上、これらのパッケージが入っていなければ先にインストールする必要があります。

(なお、make は disc1、libitool-libs は disc2 にあります)

上と同様の手順でマウント、及びインストールを行なって下さい。

DIT の設計及びサーバの起動

それでは、実際にディレクトリを作ってみます。

LDAP におけるディレクトリツリーのことを DIT(Directory Information Tree)と呼んでいます。今回は図 1 のような簡単な DIT を設計します。

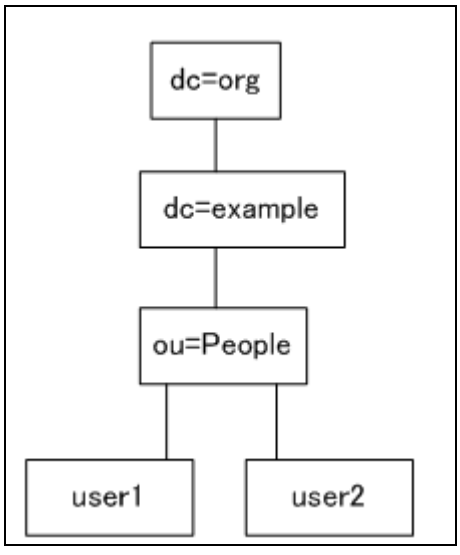


図 1 簡単な DIT

この DIT は dc=org, dc=example, ou=People 以下に user1 と user2 が属していることを意味しています。

例えば、user1 をさす場合、ディレクトリツリーを，(カンマ) で繋いで

```
cn=user1,ou=People,dc=example,dc=org
```

と表現します。

この例として、cn=user1, ou=People, dc=example, dc=orgを **DN** と言い、cn=user1 を **RDN** と言います。今回はこの図のようにou=People, dc=example, dc=org以下にWebCTのユーザ情報を作っていくことにします。

なお、この例では dc=example, dc=org という例示用ドメインでの定義をしていますが、実際にはお使いのドメインと合わせて運営することになるでしょう。

slapd.conf の修正

DIT の設計ができたらこれに基づいて openldap の設定ファイルを書き換える必要があります。設定ファイルは /etc/openldap/slapd.conf にあるのでこれを適当なエディタで編集します。

```
# vi /etc/openldap/slapd.conf
```

ファイルを開いたら以下のように記述された場所に移動します。概ね 60 行目辺りになります。

```
#######################################################
# ldbm database definitions
#######################################################

database        ldbm
suffix          "dc=my-domain,dc=com"
#suffix         "o=My Organization Name,c=US"
rootdn          "cn=Manager,dc=my-domain,dc=com"
#rootdn         "cn=Manager,o=My Organization Name,c=US"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw                secret
# rootpw                {crypt}ijFYNcSNctBYg
```

先頭に#が付くものはコメントとして無視されます。

suffix及びrootdnの項目を、先のDIT設計を踏まえて書き換えます。さらにrootpw　secretという部分のコメントを外し、ルートパスワードを**secret**にしてパスワードを設定します。(なお、パスワードの設定は、cryptなどを使ってハッシュ化することも可能です。これに関してはその他LDAP Tipsの項を参照して下さい)

以下書き換えた設定ファイルです。

```
database        ldbm
suffix          "dc=example,dc=org"
#suffix         "o=My Organization Name,c=US"
rootdn          "cn=Manager,dc=example,dc=org"
#rootdn         "cn=Manager,o=My Organization Name,c=US"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw                  secret
# rootpw                {crypt}ijFYNcSNctBYg
```

書き換えた部分は太字で示しています。

以上で OpenLDAP を利用するための最低限の設定が出来ました。root になって以下のコマンドを入力して OpenLDAP を起動させて下さい。

```
# /etc/init.d/ldap start
```

念のため ps コマンドや、root で netstat -tlp 等を起動して slapd というプロセスが ldap ポートを LISTEN しているか確認しておきます。slapd がデーモンの実体になります。

以下は netstat を使用した例です。

```
# netstat -tlp | grep ldap
tcp    0    0    *:ldap     *:*         LISTEN   3558/slapd
```

このように表示されていれば、slapd が ldap のポートを正常に Listen しています。

データの投入

データを投入する準備が整ったので、実際にデータを投入する作業を行います。openldapの場合、**slapadd**を用いたオフラインによるデータの投入方法と、**ldapadd**を用いたオンラインによるデータの投入方法がありますが、ここでは**ldapadd**によるオンラインのデータ投入を行なうことにします。

(slapaddで行う場合はアクセス権に気をつける必要があるので注意して下さい。詳細はその他LDAP Tipsを参照して下さい。)

データを投入するには以下のような**LDIF** と呼ばれるファイルを用意します。ここではroot.ldifというファイルを作成していますが、ファイル名はどのようなものでも構いません。

```
$ vi root.ldif
```

```
dn: dc=example,dc=org
objectClass: dcObject
dc: example

dn: ou=People,dc=example,dc=org
objectClass: organizationalUnit
ou: People
```

このファイルは dc=example,dc=org と ou=people,dc=example,dc=org のツリーを作ることを意味します。今回、WebCT ID を持つエントリは

cn=user1,ou=People,dc=example,dc=org

のように、ou=People,dc=example,dc=org の下に作成するのでした。しかし ldap をインストールしたばかりの状態では ou=People,dc=example,dc=org というエントリはまだ作成されていないので作る必要があります。この root.ldif は ou=People,dc=example,dc=org までを作成することを意味しています。

ファイルが作成できたら ldapadd コマンドでLDAP内に追加します。

```
$ ldapadd -x -D cn=Manager,dc=example,dc=org -W -f root.ldif
```

するとEnter LDAP Password: と表示されて、パスワードの入力が促されます。ここでOpenLDAPの設定の際にrootdnのパスワードとして指定した**secret**を入力すると、以下のようにエントリが作成されます。

```
adding new entry "dc=example,dc=org"

adding new entry "ou=People,dc=example,dc=org"
```

これで ou=People,dc=example,dc=org までが作成されました、ここからは People の下に WebCT ID の情報を持つエントリを作っていくことになります。

ユーザの追加

それでは、cn=user1 というユーザを作ってみましょう。この情報が WebCT ID の情報を持つエントリになります。

cn=user1 を定義したファイルを user1.ldif として編集したものが以下になります。

```
$ vi user1.ldif


dn: cn=user1, ou=People,dc=example,dc=org
 cn: user1
 objectClass: top
 objectClass: person
 userPassword: password # ここが WebCT Password になります
 sn: user1 # ここを WebCT ID とします
```

WebCT パスワードは userPassword に定義することになっていますが、WebCT ID に関してはどの属性を使っても構いません。ここでは sn としましたが、webctid などの属性を独自に定義してそこを見るようにしても良いです。これらは WebCT の設定で指定する事ができます。

これを先程と同じ手順で ldapadd することで user1 の情報が LDAP に入ります。

```
$ ldapadd -x -D cn=Manager,dc=example,dc=org -W -f user1.ldif
```

以降、ここ情報を基にして、WebCT での認証を行なえるように設定します。

WebCT での認証

LDAP を認証源として WebCT で認証を通すには以下の条件でサーバが設定されている必要があります。

- グローバルデータベースに LDAP と同じユーザのエントリがある
- 認証方法が LDAP に選択されている

あくまで、LDAP はパスワードの管理を委ねているだけであり、WebCT 内に実際のユーザ情報が存在しないとこれを利用することが出来ません。よって、まず管理インターフェースからユーザ情報を登録します。

管理インターフェースにアクセスして、**ユーザ管理** → **追加** を押し、ユーザの新規追加画面に移動します。すると以下のユーザの追加画面になります。

ここで WebCT ID に user1 を指定して下さい。パスワードは LDAP のパスワードが優先されるため、どのような値でもかまいません。今回は null と仮にしておきましょう。姓名に関しては特に記述する必要はありませんが、一応ユーザを認識するため名に LDAP、姓に USER と入力しておきます。

```
WebCT ID*: user1

パスワード*: null

名 : LDAP

姓 : USER
```

この情報を入力したのち、**追加** ボタンを押します。

これでユーザ情報が追加できました。次に LDAP を認証源とするよう WebCT の設定を行います。

管理インターフェースのトップに戻って **設定** ボタンを押

します。

サーバ設定 → ユーザ認証: で、**ユーザの認証方法**：のセレクトボックスを以下のように設定します。

```
内部 WebCT パスワードデータベース: 使用しない
 LDAP サーバ: 最初
MIT Kerberos V5 KDC または Windows 2000 ドメインコントローラ: 使用しない
認証方法をカスタマイズします: 使用しない
```

さらに LDAP の設定を以下のようにします。

```
LDAP 設定：
 LDAP サーバ名： localhost
 LDAP ポート：ldap
 Base DN: ou=People,dc=example,dc=org
 WebCT ID 属性： sn
 管理者 DN：cn=Manager,dc=example,dc=org
 管理者パスワード：secret
```

LDAP と WebCT が別にある場合は LDAP サーバ名に適切なサーバ名または IP アドレスを入力して下さい。またポートも LDAP のデフォルトの 389 以外に設定しているであれば適切なポート番号を入力する必要があります。

これでLDAPのパスワードが利用されるようになりました。つまりユーザ名にuser1、パスワードはWebCTのユーザ管理で設定したnullではなく、LDAPのuser1.ldifのuserPasswordで指定した **password**を入力することで、myWebCTにログイン出来るようになりました。試しにこれらの情報でmyWebCTにログインできるかどうかチェックして下さい。ログインできるようであればuser2.ldifなどでuser2 などのユーザをLDAPサーバとWebCTサーバにそれぞれ作成して、認証できるか試してみて下さい。

その他 LDAP Tips

以降 LDAP における小さな Tips を紹介していきます。

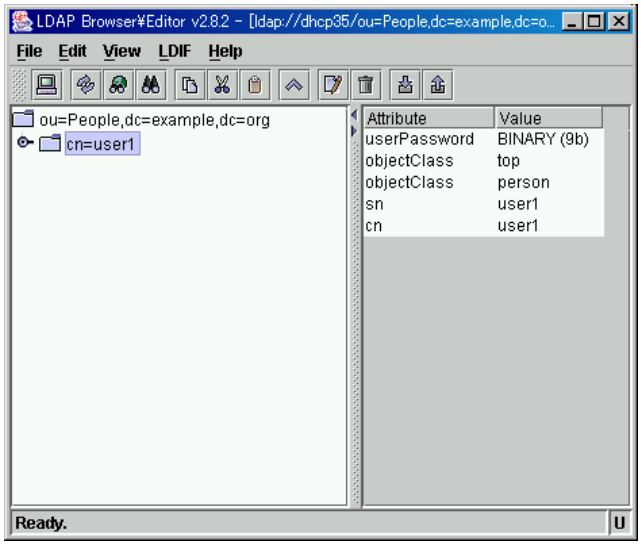
LDAP ディレクトリを GUI で操作したい

LDAP Browser/EditorというGUIでLDAPを表示または操作出来るJavaベースのソフトがあります。

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

Javaで書かれているので、javaランタイムが入っていなければhttp://java.sun.comより取得して下さい。

インストールはアーカイブをダウンロードし、展開後、windows なら lbe.bat を、linux なら lbe.sh を起動すればLDAP Browser/Editor が起動します。



コマンドラインが苦手でも GUI にてツリー表示してくれるので視覚的に操作できます。

管理パスワードをハッシュ化したい。

このガイドでは管理パスワードの設定時に rootpw secret とパスワードをそのまま記述しました。これは何らかの拍子で設定ファイルを覗かれるとパスワードがまる見えになってしまうため、セキュリティ上あまり好ましくありません。よって OpenLDAP は CRYPT, MD5, SMD5, SSHA さらには SHA といった形式を用いてパスワードをハッシュ化させることが可能になっています。これらは OpenLDAP に含まれる slappasswd というツールで簡単に生成できます。

例えば先の secret という文字列を SSHA でハッシュ化するには以下のようなコマンドになります。

```
$ /usr/sbin/slappasswd -h {SSHA} -s secret
```

すると以下のように標準出力に書かれるので、これをコピーして設定ファイルに書き込みます。

```
{SSHA}lvVB7rP6o2Ac91xQhNvyblilHpQOoN1v
```

エラーが出て ldapadd できない

本 Tips では特に解説していませんが、slapadd というツールでオフラインでデータが出来ます。これを行った後、ldap を起動して ldapadd から ldif ファイルを読もうとすると以下のエラーで停止することがあります。

```
ldap_add: Operations error


ldif_record() = 1
```

Red Hat Linux 7.3 の OpenLDAP パッケージでは、ldap というユーザを新規に作り、そのユーザ権限でデーモンが動いています。その関係上、LDAP のデータは ldap ユーザで書き込み可能になっている必要があるのですが、root で slapadd などの操作を行うと、データの所有者が root 変更され、デーモンがデータファイルを読みこめなくなってしまいます。

上記のエラーが出たときは、まず ldap のデータディレクトリを ls -l し、権限が正しく ldap になっているか確認して下さい。ldap のデータディレクトリは

```
/etc/openldap/slapd.conf
```

の directory の項目で設定します。(デフォルトでは /var/lib/ldap になっています)。権限が root などに変更されてしまった場合は chown で元の ldap に戻してやります。

LDAP をシステム起動時に自動起動する

Red Hat Linuxのデフォルトでは、パッケージをインストールしただけでは、スタートアップ時にデーモンが自動起動しません。Red Hat Linuxの場合ではrootから**setup**コマンドを使うと簡単に自動起動する設定に出来ます。

root になって setup と入力して Enter を押して下さい。するとセットアップユーティリティが起動するので、System services の ldap のチェックを付けて下さい。

参考 URL

OpenLDAP2.1 管理者ガイド

http://www.interq.or.jp/earth/inachi/openldap/admin/index-ja.html

LDAP Linux HOWTO

http://www.linux.or.jp/JF/JFdocs/LDAP-HOWTO.html

RedHat Linux 7.3 Official 第19章 LDAP

http://www.jp.redhat.com/manual/Doc73/RH-DOCS/rhl-rg-ja/ch-ldap.html

この Tips は以下の環境で確認しました。

- サーバ：WebCT3.8 日本語版 / RedhatLinux 7.3
- クライアント OS：Windows2000
- クライアントブラウザ：IE6.0SP1

(2003 年 12 月 17 日　福山 貴幸 作成)