LDAP Account Manager 利用者ガイド

オープンソース・ソリューション・テクノロジ株式会社

2007 年 4 月 3 日 初版

目次

1.概要

LDAP Account Manager(以降 LAM)は、LDAP に登録されたアカウント情報を Web インターフェース上で管理するためのツールです。

本ドキュメントは RedHat Enterprise Linux4(x86 版)、および CentOS4(x86 版)で OSS テクノロジ提供の LAM を利用する方法を説明します。

2.LAM のインストール

LAM を利用するために必要な RPM パッケージとして、OSS テクノロジより以下のパッケージを提供します。(バージョン番号等はパッケージのアップデートに伴い変更されることがあります。)

- ldap-account-manager-1.3.0-1.1_OSSTECH.noarch.rpm
- mhash-0.9.2-3.i386.rpm
- mhash-devel-0.9.2-3.i386.rpm
- perl-Archive-Tar-1.26-1.1_OSSTECH.noarch.rpm
- perl-Class-ErrorHandler-0.01-1.1_OSSTECH.noarch.rpm
- perl-Class-Loader-2.03-1.2.1_OSSTECH.noarch.rpm
- perl-Compress-Zlib-1.41-1.1_OSSTECH.i386.rpm
- perl-Convert-ASCII-Armour-1.4-1.2.1_OSSTECH.noarch.rpm
- perl-Convert-PEM-0.07-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-CBC-2.17-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DES-2.05-3.1_OSSTECH.i386.rpm
- perl-Crypt-DES_EDE3-0.01-1.2.1_OSSTECH.noarch.rpm
- perl-Crypt-DH-0.06-1.1_OSSTECH.noarch.rpm
- perl-Crypt-DSA-0.13-1.1_OSSTECH.noarch.rpm
- perl-Crypt-IDEA-1.08-1.1_OSSTECH.i386.rpm
- perl-Crypt-Primes-0.50-1.1_OSSTECH.i386.rpm
- perl-Crypt-RSA-1.57-1.1_OSSTECH.noarch.rpm
- perl-Crypt-Random-1.25-1.2.1_OSSTECH.noarch.rpm
- perl-Data-Buffer-0.04-1.2.1_OSSTECH.noarch.rpm
- perl-Digest-MD2-2.03-1.2.1_OSSTECH.i386.rpm
- perl-IO-Socket-SSL-0.999-1.1_OSSTECH.noarch.rpm
- perl-Jcode-2.03-1.1_OSSTECH.i386.rpm
- perl-Math-GMP-2.04-1.1_OSSTECH.i386.rpm
- perl-Math-Pari-2.010706-1.1_OSSTECH.i386.rpm
- perl-Module-Build-0.2611-1.2.1_OSSTECH.noarch.rpm
- perl-Net-SSH-Perl-1.30-2.1_OSSTECH.noarch.rpm
- perl-Net-SSLeay-1.25-3.1_OSSTECH.i386.rpm
- perl-Quota-1.5.1-1.2.1_OSSTECH.i386.rpm
- perl-Sort-Versions-1.5-1.2.1_OSSTECH.noarch.rpm
- perl-String-CRC32-1.4-1.1_OSSTECH.i386.rpm
- perl-Tie-EncryptedHash-1.21-1.2.1_OSSTECH.noarch.rpm
- perl-Unicode-Map-0.112-0.2.1_OSSTECH.i386.rpm
- perl-Unicode-Map8-0.12-0.2.1_OSSTECH.i386.rpm

- perl-Unicode-MapUTF8-1.11-1.1_OSSTECH.noarch.rpm
- perl-Unicode-String-2.09-1.1_OSSTECH.i386.rpm
- php-4.3.9-3.22.3.i386.rpm
- php-devel-4.3.9-3.22.3.i386.rpm
- php-domxml-4.3.9-3.22.3.i386.rpm
- php-gd-4.3.9-3.22.3.i386.rpm
- php-imap-4.3.9-3.22.3.i386.rpm
- php-ldap-4.3.9-3.22.3.i386.rpm
- php-mbstring-4.3.9-3.22.3.i386.rpm
- php-mhash-4.3.9-3.22.3.i386.rpm
- php-mysql-4.3.9-3.22.3.i386.rpm
- php-ncurses-4.3.9-3.22.3.i386.rpm
- php-odbc-4.3.9-3.22.3.i386.rpm
- php-pear-4.3.9-3.22.3.i386.rpm
- php-pgsql-4.3.9-3.22.3.i386.rpm
- php-snmp-4.3.9-3.22.3.i386.rpm
- php-xmlrpc-4.3.9-3.22.3.i386.rpm

パッケージのインストールは rpm コマンドで行います。上記パッケージが/tmp/lam ディレクトリに用意されている場合、root 権限にて、次のコマンドでパッケージをインストールします。

```
# cd  /tmp/lam
# rpm -ihv *.rpm
```

なお、ファイル名が php-xxx のパッケージのうち、php-mhash パッケージ以外は、OS 標準で提供されていますので、既にこれらの php-xxx パッケージがシステムにインストールされている場合は php-mhash パッケージ以外のインストールは不要です。

3.LAM の初期設定

3.1.PHP の設定

LAM を利用する前に、/etc/php.ini の memory_limit の値を 32M に設定します。

```
memory_limit = 32M
```

3.2.LAM の設定ファイルの準備

続いて LAM の初期設定ファイルを作成します。/var/www/html/lam/config に設定ファイルのサンプルとして、config.cfg_sample がありますので、このファイルを config.cfg としてコピーし、パスワードとプロファイル名を設定します。

```
# cd /var/www/html/lam/config
# cp config.cfg_sample config.cfg
# vi config.cfg

# password to add/delete/rename configuration  profiles
password: secret

# default profile, without ".conf"
default: lam
```

上記設定では、パスワードを"secret"、デフォルトプロファイルの設定ファイルを lam.conf として設定しています。

次に lam.conf の初期設定ファイルを作成します。config.cfg ファイルと同じディレクトリ(/var/www/html/lam/config)に、サンプルとして lam.conf_sample ファイルがありますので、このファイルをコピーして lam.conf を作成します。

```
# cd /var/www/html/lam/config
# cp lam.conf_sample lam.conf
```

最後に、config.cfg と lam.conf のパーミッションを apache ユーザに変更します。

```
# chown  apache:apache config.cfg
# chown apache:apache lam.conf
```

3.3.Web サーバの起動

LAM の初期設定が完了したら、Web サーバを起動します。

```
# /sbin/service httpd start
```

既に Web サーバが起動している場合は、start の代わりに restart を指定して再起動します。

```
# /sbin/service httpd restart
```

4.LAM の LDAP 基本設定

ここまでの初期設定が完了したら、以降は Web ブラウザから LAM を利用することができます。

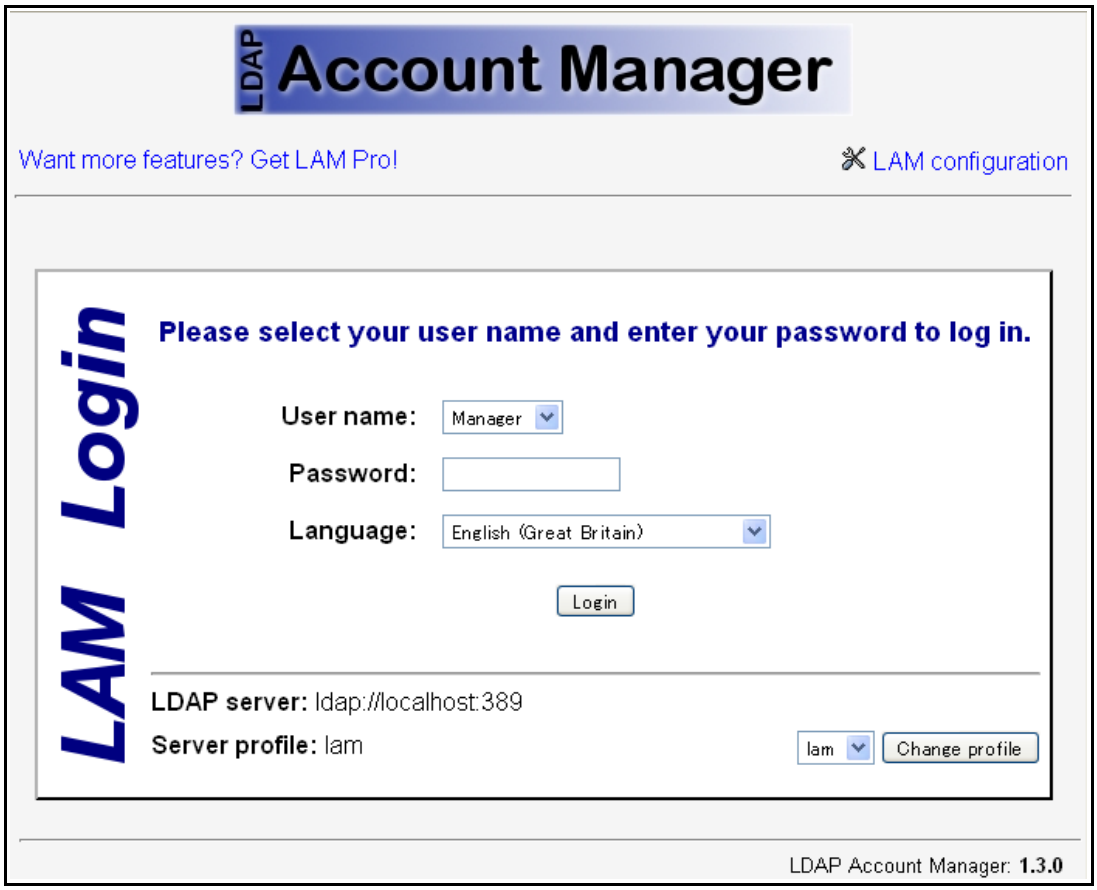
4.1.LAM のログイン画面

Web ブラウザから、LAM にログインするため、下記の URL にアクセスを行います。

http://localhost/lam/index.html

[注意] リモートからアクセスする際には、ファイアーウォールなどによるアクセス拒否の設定が行われている場合がありますので、HTTP 経由のアクセスが可能になるようにネットワークの設定を変更してください。

正常に設定が完了していれば、ログイン画面（画面 1)が Web ブラウザに表示されます。

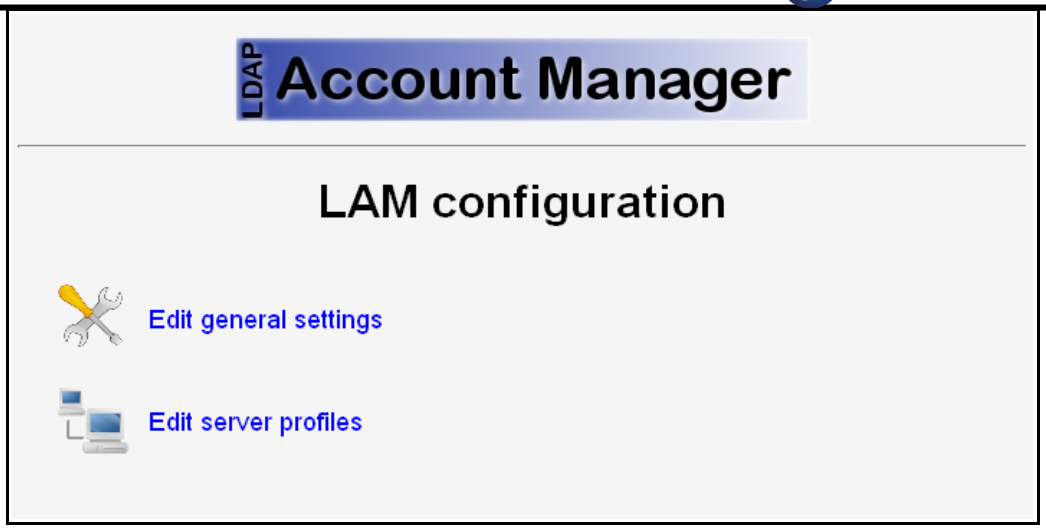


画面 1: LAM のログイン画面

通常はこのログイン画面から、LDAP を管理するためにログインを行います。

4.2.LDAP 関連の基本設定

LAM の初期設定ファイル(lam.conf)では、各パラメータにサンプルの値が指定されていますので、実際の運用環境に適した値に、設定を変更する必要があります。そのために、LAM のログイン画面の右上にある「LAM Configuration」をクリックし、画面 2 に移ります。

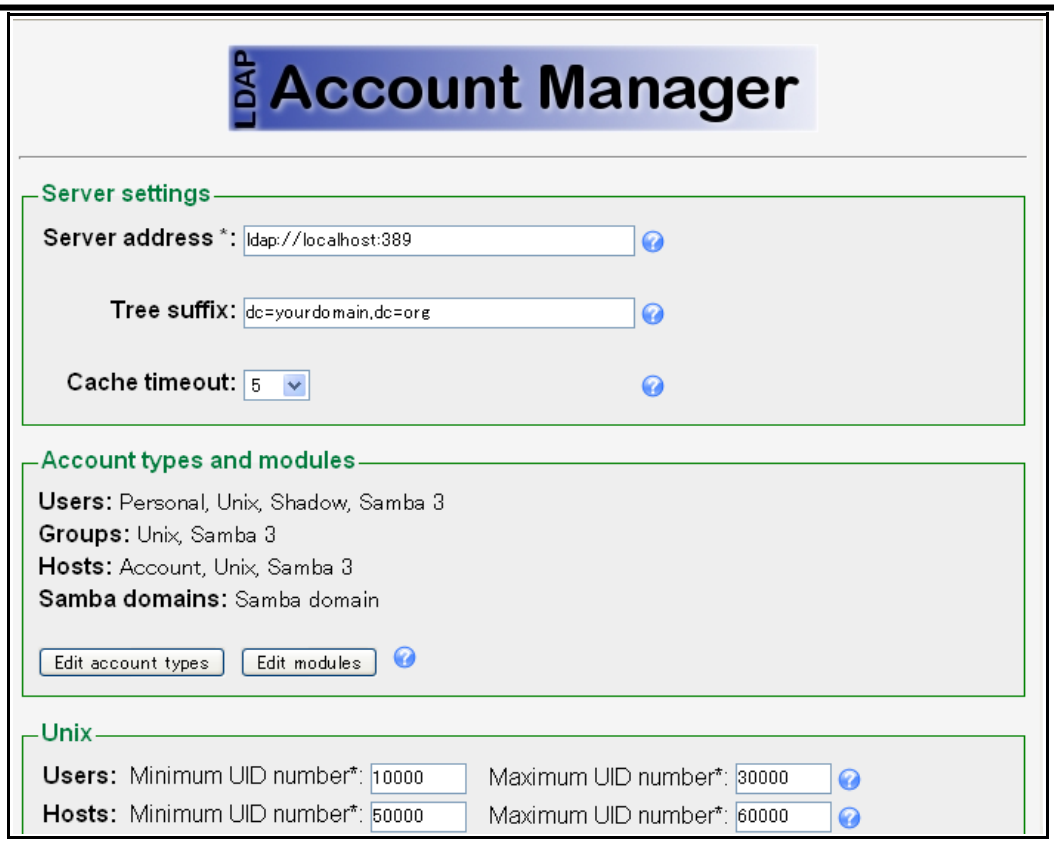


画面 2: LAM configuration の選択画面

画面 2(LAM configuration)では、「Edit server profiles」を選択します。続けて、パスワードの入力画面(画面 3)が表示されます。ここで入力するパスワードは、lam.conf の passwd の項目に設定されているパスワードを入力します。サンプルファイルの lam.conf_sample ではパスワードとして”lam”が設定されていますので、このサンプルファイルを利用して lam.conf を作成した場合は、パスワードの入力欄に”lam”を入力し、「OK」をクリックします。

画面 3: パスワード入力画面

パスワードの認証が正常に行われると、管理する LDAP 関連の項目を設定する画面(画面 4)が表示されます。



画面 4: LDAP 関連の基本設定

本ドキュメントでは、LAM がインストールされているサーバーと同じマシンに、OpenLDAP による LDAP サーバが構築されているものとして、説明を行います。本ドキュメントの設定例として、/etc/openldap/slapd.conf には、次の値が設定されているものとします。

- suffix “dc=example,dc=jp”
- rootdn “cn=Manager,dc=example,dc=jp”
- rootpw secret

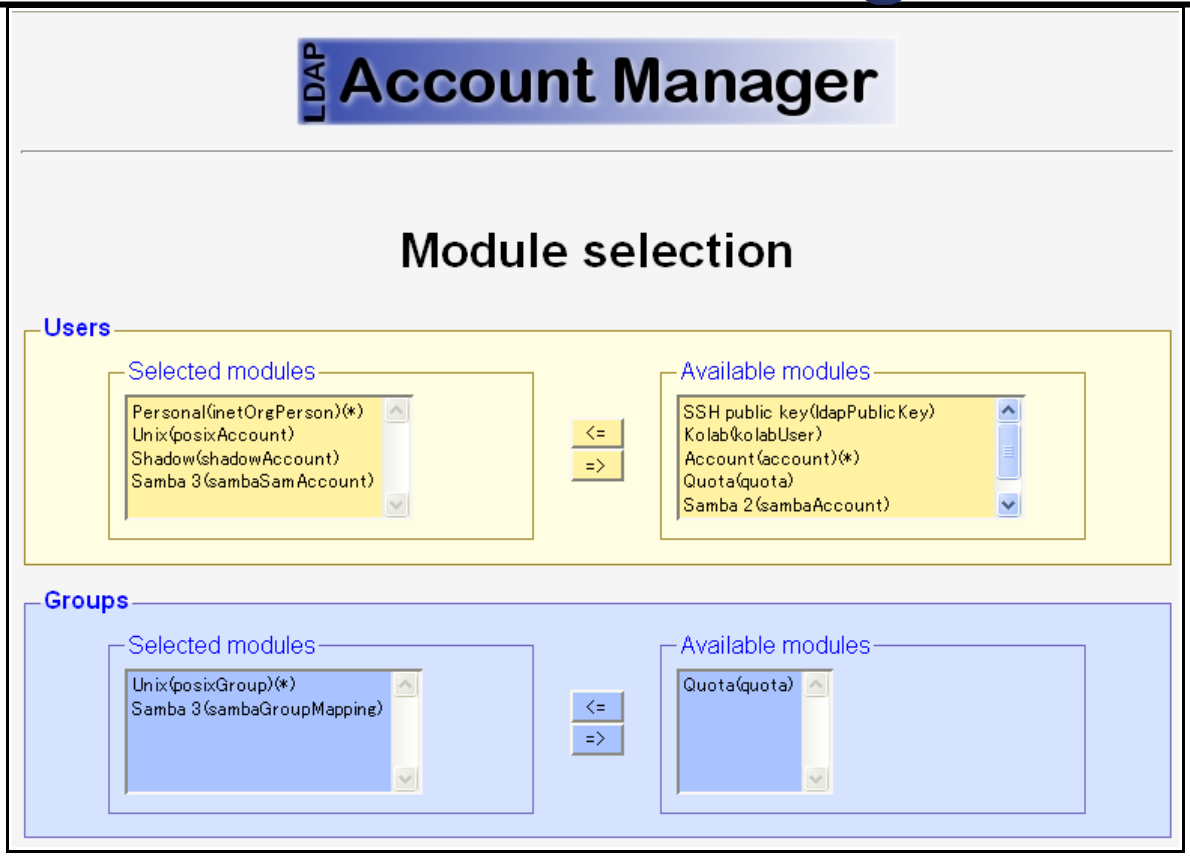
これらの設定値は、運用環境に合わせて、読み替えてください。

なお、これらの値が設定された slapd が下記コマンドで起動されているものとします。

```
# /sbin/service ldap start
```

画面 4 で表示されている LDAP 関連の基本設定を、運用環境に合わせて設定を行います。

まず最初に「Account types and modules」の「Edit modules」をクリックし、画面 5 を表示させます。



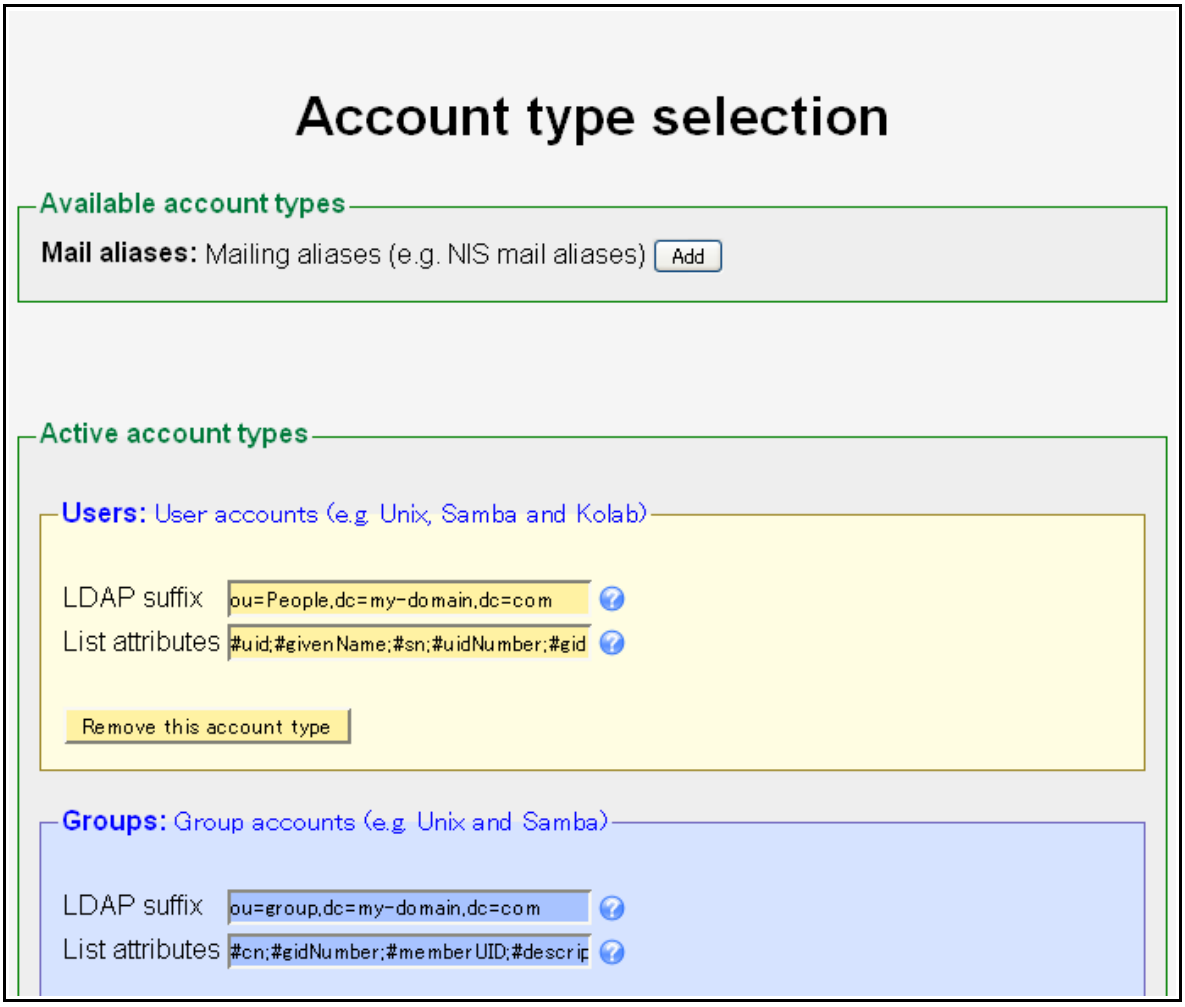
画面 5: Module Selection

画面 5 では、ユーザ、グループなどの LDAP エントリの属性を定義しています。デフォルト設定では Samba 3.0 との連携用の設定となっています。運用環境で Samba 3.0 との連携を行わない場合には、各エントリから、「Samba3」のモジュールを削除します。モジュールの削除は、「Samba3」を選択し、「=>」ボタンをクリックすることで設定できます。

- Users: Samba 3(sambaSamAccount)の削除
- Groups:Samba 3(sambaGroupMapping)の削除
- Hosts: Samba 3(sambaSamAccount)の削除

各モジュールの設定が完了したら、画面下部の「OK」ボタンをクリックし、画面 4 に戻ります。

次に「Account types and modules」の「Edit account types」をクリックし、画面 6 を表示させます。



画面 6: Account types の設定

Users、Groups、Hosts、Samba domains の各項目の LDAP suffix を、運用環境の LDAP suffix に合わせます。本ドキュメントの環境では、以下の設定を行うことになります。

- Users: ou=People,dc=example,dc=jp
- Groups: ou=group,dc=example,dc=jp
- Hosts: ou=machines,dc=example,dc=jp
- Samba domains: ou=domains,dc=example,dc=jp

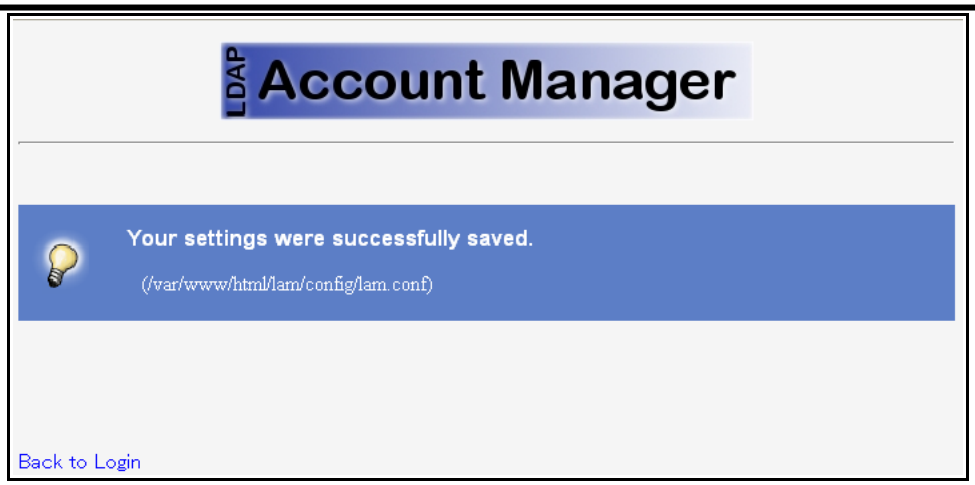
各項目の「List attributes」は、通常変更する必要はありません。
以上の設定を終えたら、画面 6 の下部にある「OK」ボタンをクリックします。

続いて画面 4 に戻りますので、各項目について、以下の通り設定します。

- Server settings
  - Server address: ldap://localhost:389 (デフォルト値のまま)
  - Tree suffix: dc=example,dc=jp (運用環境の slapd.conf の suffix に合わせます)
  - Cache timeout： 5 分 (LAM が保持する LDAP のキャッシュを更新する間隔です。)
- Account types and modules:
  - 「Edit account types」をクリックします。詳細については既に説明しました。

- Unix
  - Users: LAM でユーザ作成時に割り当てる UID の最小値と最大値を指定します。
  - Hosts: LAM で Samba 用マシンアカウント作成時に割り当てる UID の最小値と最大値を設定します。Samba を使用しない場合には利用されません。Users に割り当てている範囲と重ならないように設定します。
  - Password hash type: ユーザのパスワードの暗号化方式を指定します。通常はデフォルトの「SSHA」で問題ありません。
- Samba3
  - Time zone:「GMT+09」を選択します。(Samba3 用の設定を削除している場合は表示されません。)
- Unix
  - Groups:グループ作成時に割り当てる GID の最小値と最大値を設定します。
- List settings
  - LDAP のエントリを表示する際に、一度に表示するエントリ数です。最大 100 エントリの表示まで選択することが可能です。
- Language settings
  - Default language：日本語(日本)を選択します。
- Script settings
  - Server list:lamdaemon によるスクリプト実行を行う場合に、対象となるサーバを指定します。lamdaemon 利用の詳細については、/var/www/html/lam/docs/README.lamdaemon.txt を参照してください。
  - Path to external script: lamdaemon で quota の設定やホームディレクトリ作成用に特別なスクリプトを利用する場合にスクリプトのパスを設定します。
  - Rights for the home directory: lamdaemon によるホームディレクトリの作成時に、ホームディレクトリに設定するパーミッションを設定します。
- Security settings
  - List of valid users: LAM にログインすることを許可するユーザの DN を設定します。本ドキュメントでは設定例として、slapd.conf に設定した”cn=Manager,dc=example,dc=jp”のエントリを設定します。
  - New password: 現在ログインしている LDAP の基本設定画面にログインするためのパスワードを変更する場合に、新しいパスワードを入力します。本ドキュメントでは、デフォルトで設定されている”lam”を “secret”に変更します。

以上の設定を終えたら、画面下部の「OK」ボタンをクリックします。正常に変更が完了すれば、画面 6 が表示されます。



画面 7: lam.conf の設定変更に成功

画面下部の「Back to Login」をクリックし、LAM のログイン画面に戻ります。

上記の画面 7 が表示されずエラーが表示される場合には、lam.conf ファイルの所有者が apache ユーザになっているか確認してください。

5.LAM の利用

基本設定が完了したら、LAM を利用することができます。

http://localhost/lam/index.html

にアクセスして、LAM のログイン画面(画面 8)を表示します。

画面 8: LAM のログイン画面

LAM の基本設定で設定したユーザ(cn=Manager,dc=example,dc=jp)名が「ユーザ名」の選択肢に表示されていますので、基本設定で設定したパスワードを入力し、「ログイン」ボタンをクリックします。

初回ログイン時には、LDAP にエントリが作成されていないため、画面 9 が表示されますので、「作成」ボタンをクリックします。

画面 9: LDAP エントリの作成

LDAP エントリの作成に成功すると、画面 10 が表示されます。

画面 10: LDAP エントリの作成に成功

作成された LDAP エントリを確認するために、「ツリービュー」をクリックします。

画面 11: ツリービューによる表示

6.ユーザ・グループ管理操作

6.1.グループの作成

LAM でグループエントリを作成したい場合、画面上部の「グループ」をクリックします。

画面 11: グループ管理

最初はグループエントリが存在しないため、「グループが見つかりません!」のメッセージが表示されます。そこで、「新しいグループ」ボタンをクリックし、グループの作成を行います。

画面 13: グループの新規作成

画面 13 のように、「ページ unix の必須属性を全て設定してください」と表示されますので、画面左部分の「unix」のボタンをクリックします。

画面 14: グループの作成

画面 14 が表示されますので、「グループ名」を入力します。GID 番号は自動的に割り振られますので、通常は変更する必要はありません。グループ名を入力し終えたら、画面左部の「メイン」をクリックします。

メインページに戻ると、画面 15 のように「アカウント作成」のボタンが有効になっていますので、「アカウント作成」をクリックします。

画面 15: グループアカウントの作成

アカウントの作成に成功すると、画面 16 が表示されます。さらにグループを作成する場合は、「他のアカウントを作成」ボタンをクリックします。グループ一覧を表示したい場合は、「アカウント一覧に戻る」をクリックします。

画面 16: グループアカウントの作成に成功

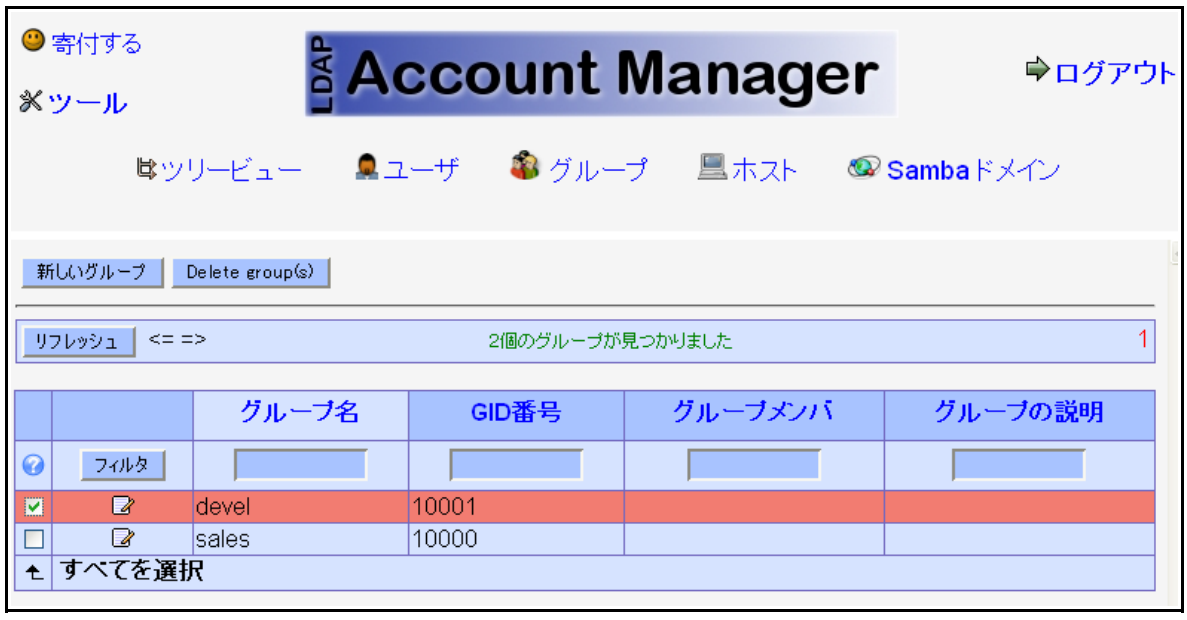
グループアカウントの一覧画面に戻ると、画面 17 のように作成したグループの情報が表示されます。

画面 17: グループアカウントの一覧

6.2.グループの削除

LDAP に登録されているグループを削除したい場合、グループアカウント一覧の画面で、削除したいグループのチェックボックスにチェックを付けて、「Delete group(s)」ボタンをクリックします。

画面 18 では、「devel」グループの削除を行うために、チェックボックスにチェックをつけています。



画面 18: 削除するグループの選択

「Delete group(s)」ボタンをクリックすると、画面 19 の確認画面が表示されますので、「削除」か「中止」のどちらかを選択します。

画面 19: グループエントリの削除

削除を選択すると、LDAP から該当するグループエントリが削除され、画面 20 が表示されます。

画面 20: LDAP からグループエントリを削除

画面 20 が表示されると、グループエントリの削除が完了するため、「一覧に戻る」をクリックして、グループの削除処理を終了します。

6.3.ユーザの作成

LDAP にユーザエントリを作成したい場合には、画面上部の「ユーザ」をクリックします。LDAP エントリにまだユーザエントリが作成されていない場合、画面 21 が表示されます。

画面 21: ユーザエントリの一覧

ユーザアカウントを作成したい場合、「新しいユーザ」ボタンをクリックすると、画面 22 が表示されます。

画面 22: ユーザアカウント情報の入力

Personal、unix の必須属性を設定するために、最初に「ページを選択」内の「Personal」ボタンをクリックします。

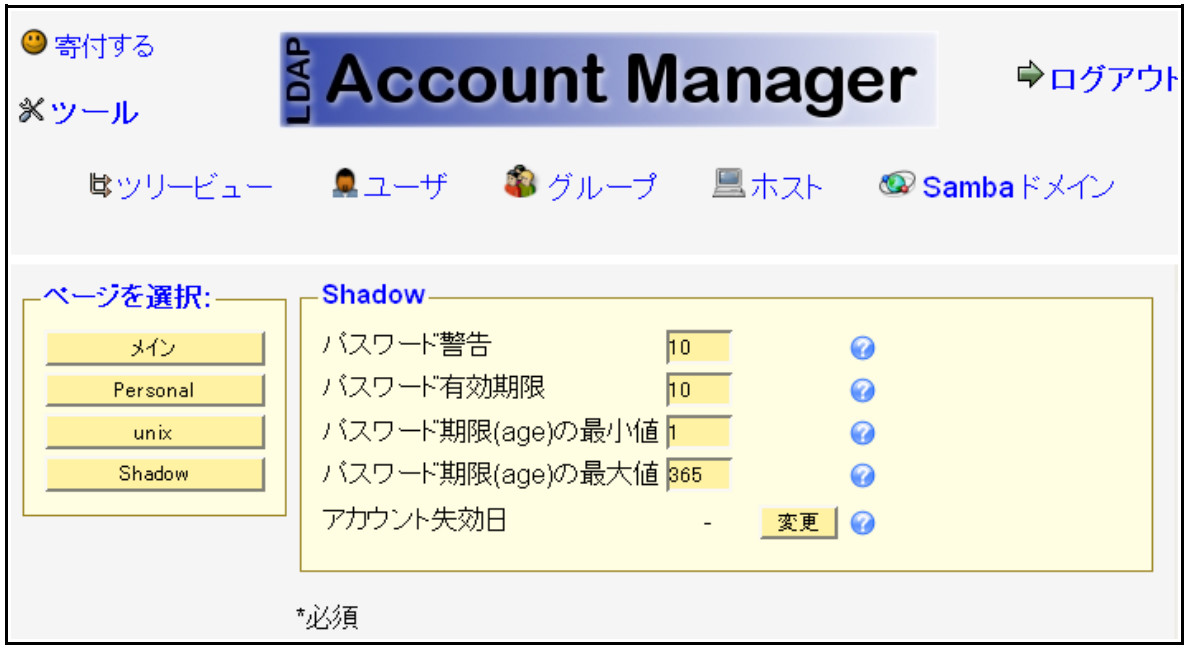
画面 23: Personal 属性の入力

Personal 属性の入力項目のうち、必須項目は、「姓」のみですので、それ以外の項目の入力については任意で選択し入力してください。Personal 属性の入力が完了したら、「ページを選択」の「unix」ボタンをクリックしてください。

画面 24: unix 属性の設定

画面 24 が表示されますので、ユーザアカウントに設定する内容を、それぞれの項目に入力してください。なお、UID 番号が入力されなかった場合は、自動的に割り当てられます。

それぞれの項目の入力が終了したら、「ページを選択」のうち、「Shadow」か「メイン」をクリックします。「Shadow」では画面 25 で表示されているように、パスワードの有効期限などの属性を設定することができます。なお、Shadow 属性の設定は必須ではありません。



画面 25: Shadow 属性の設定

ユーザ作成に関する全ての必須属性の入力が完了すると、「メイン」ページの「アカウント作成」ボタンが有効になります(画面 26)。入力した内容でユーザアカウントを LDAP エントリに作成する場合、「アカウント作成」ボタンをクリックします。

画面 26: ユーザアカウントの作成

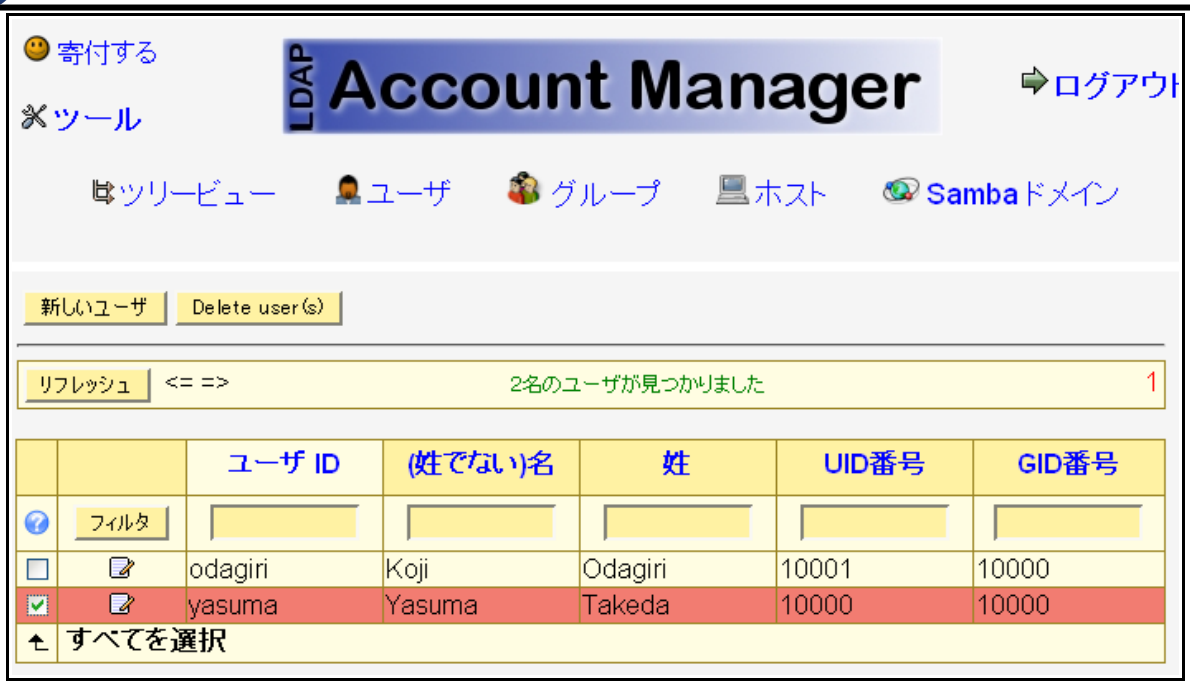
LDAP に正常にユーザーアカウントを作成できた場合、画面 27 が表示されます。

画面 27: ユーザアカウント登録の完了

さらにユーザアカウントの作成を続ける場合には、「他のアカウントを作成」を選択します。ユーザアカウントの作成を終了する場合には、「アカウント一覧に戻る」を選択します。

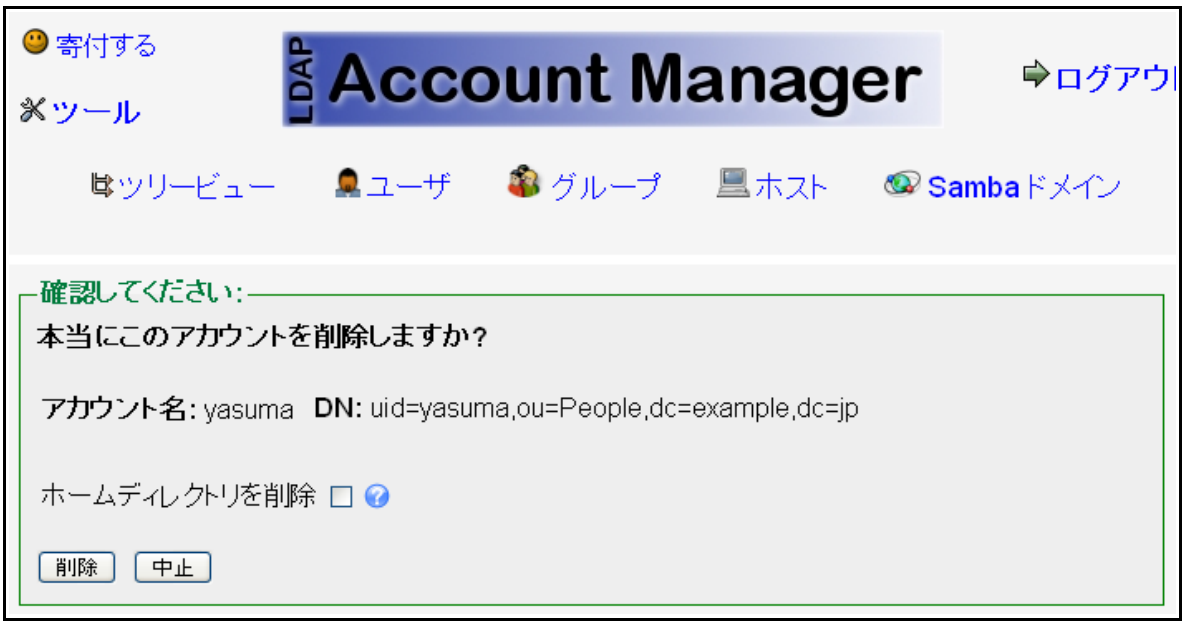
6.4.ユーザの削除

LDAP に登録されているユーザアカウントのエントリを作成したい場合、ユーザ一覧表示の画面から、削除したいユーザのチェックボックスにチェックを付け、「Delete user(s)」ボタンをクリックします。



画面 28: ユーザ一覧から削除するユーザを選択

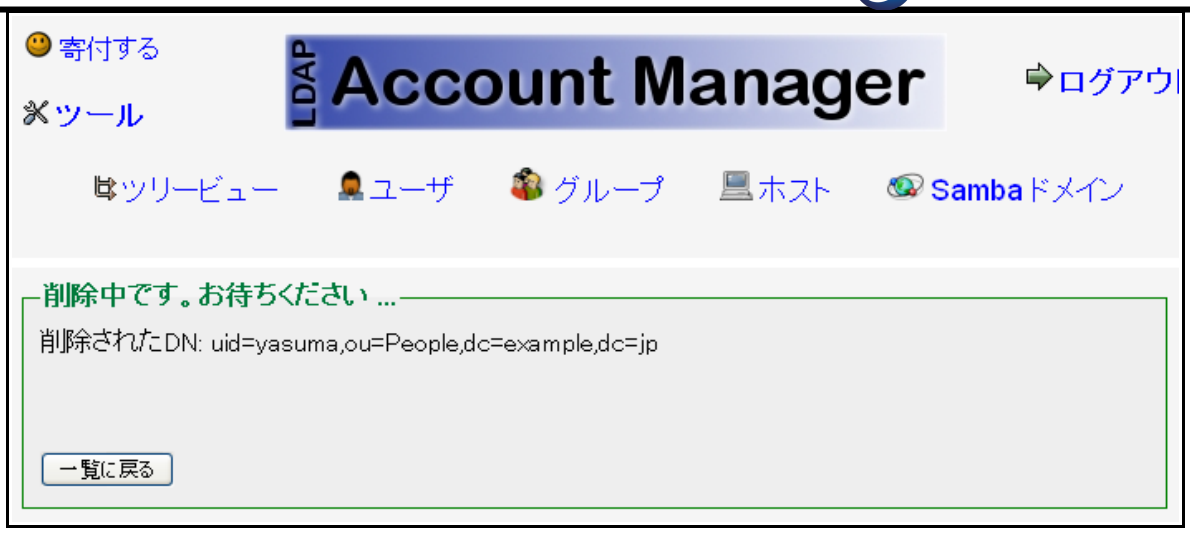
画面 28 では、ユーザ ID「yasuma」のユーザを選択しています。
「Delete user(s)」をクリックすると、画面 29 の確認画面が表示されます。



画面 29: ユーザエントリ削除の確認

LDAP からユーザエントリを削除する場合には、「削除」ボタンをクリックしてください。またあわせて、ユーザのホームディレクトリを削除する場合、「ホームディレクトリを削除」のチェックボックスにチェックを入れてください。

正常にユーザエントリが削除されると、画面 30 が表示されますので、「一覧に戻る」をクリックして、ユーザ一覧の画面に戻ってください。



画面 30: ユーザアカウントの削除に成功

6.5.ユーザ情報の変更

ユーザ情報を変更したい場合、「ツリービュー」から該当するユーザを選択します。画面 31 は、「uid=yasuma」ユーザを選択しています。

画面 31: ユーザ情報の詳細表示

画面 31 の右側部分に選択したユーザアカウントに設定されている各エントリの内容が表示されていますので、変更したい項目を修正し、画面下部にある「保存」ボタンをクリックして、変更内容を保存します。

「保存」ボタンをクリックすると、変更箇所が画面 32 のように表示されますので、問題なければ、「更新」ボタンをクリックします。

画面 32: 変更内容の確認

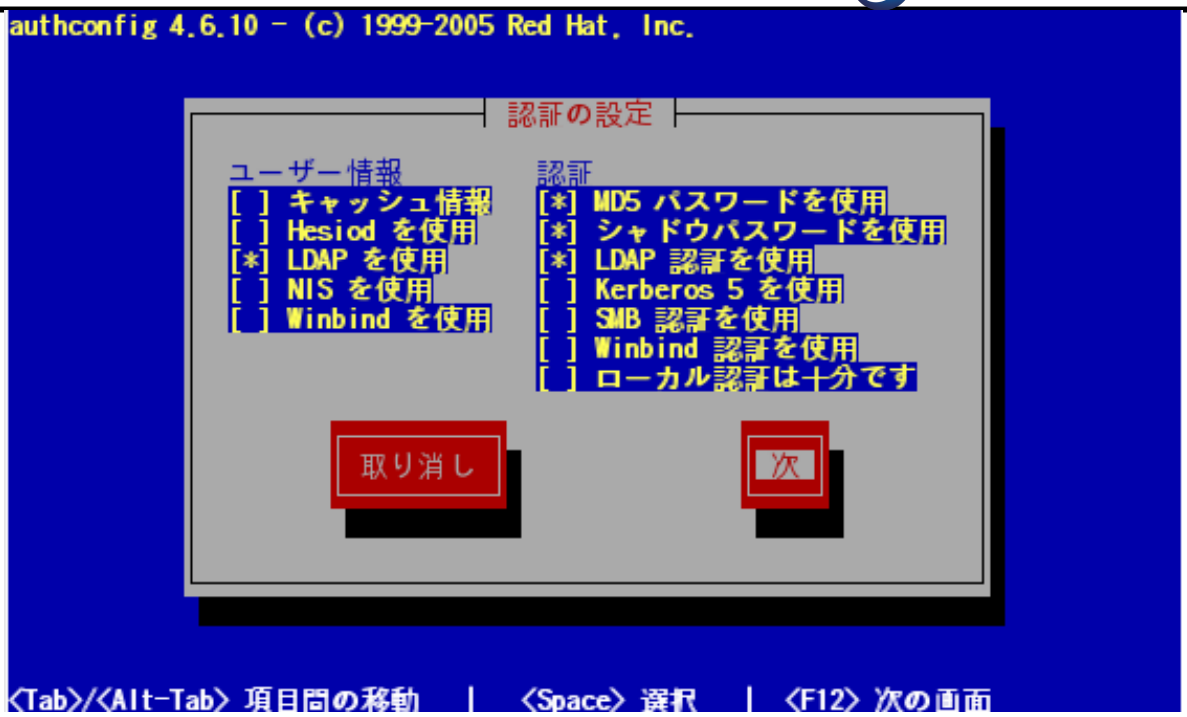
7.RedHat Enterprise Linux 4, CentOS 4 での LDAP 基本設定

LAM で作成した LDAP エントリを利用するためには、OS で LDAP のエントリを参照する設定が必要になります。RedHat Enterprise Linux 4、および CentOS4 では、authconfig コマンドで LDAP 参照の設定を行うことができます。

端末上で、root 権限で authconfig コマンドを実行します。

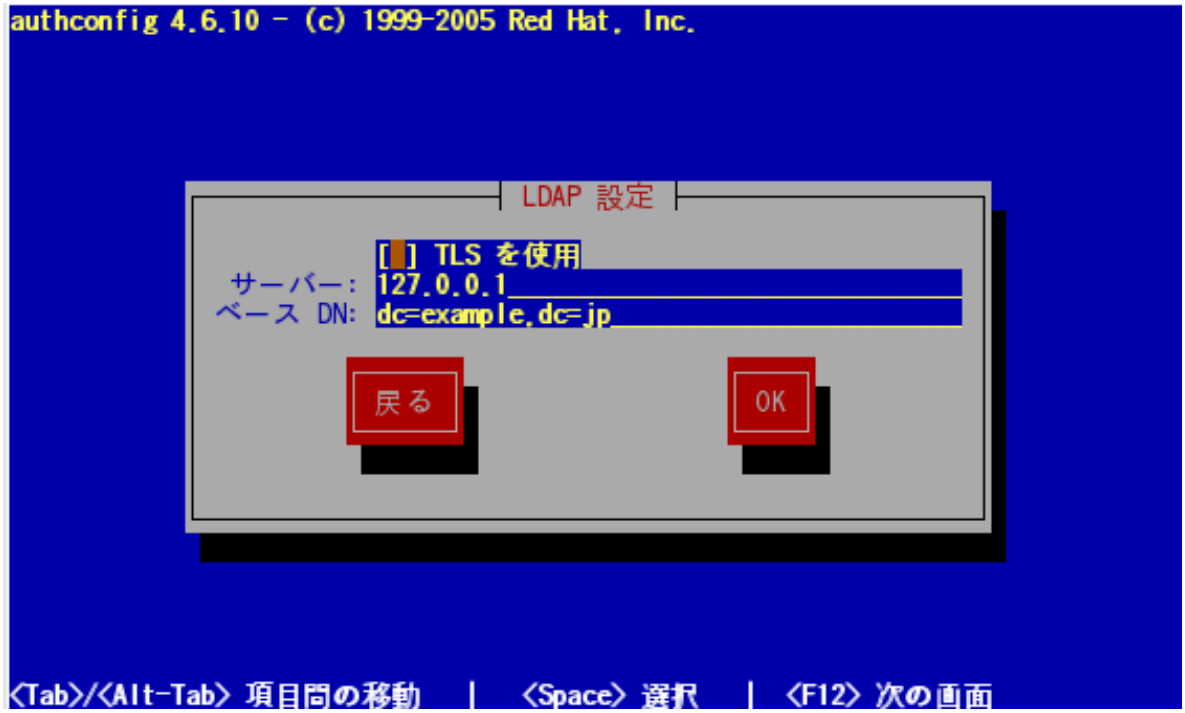
```
# authconfig
```

画面 33 の設定画面で、「ユーザ情報」として「LDAP を使用」、「認証」として、「LDAP 認証を使用」にチェックを付け、「次」を選択します。



画面 33: LDAP 利用のための設定

画面 34 では、TLS 使用の有無、LDAP サーバの IP アドレス、および、LDAP のベース DN を指定します。本ドキュメントの環境では、ベース DN として、”dc=example,dc=jp”を設定することになります(画面 34)。



画面 34: LDAP サーバへの接続設定