OpenLDAP 導入手順書

更新日: 2009 年 10 月 28 日

作成日: 2008 年 3 月 6 日

リビジョン: 1.7

目次

1. 要旨

本書は OpenLDAP による認証サーバー環境（LDAP マスター、スレーブ構成）の構築に関するガイドです。

一般的なコマンドの使用方法等については、各ソフトウェアのマニュアルなどに従ってください。また、smbldap-tools については弊社提供の別文書を参照ください。

1.1 対象環境

本書の対象環境は以下となります。各項目については適宜実際に構築される環境に合わせてください。

- OS
  - Red Hat Enterprise Linux 4 (x86/x86_64)
    - インストールタイプ
      - 「デフォルトのソフトウェアをインストール」を選択（カスタマイズなし）
    - SELinux
      - 無効
    - ファイアウォール
      - 無効
- ディレクトリサーバー
  - openldap-2.3.43-1.4_OSSTECH
- マスターサーバー
  - ホスト名
    - master.example.co.jp
  - IP アドレス
    - 10.1.0.10/24
- スレーブサーバー
  - ホスト名
    - slave.example.co.jp
  - IP アドレス
    - 10.1.0.11/24

- 導入パッケージの保存場所
  - /root/RPMS/

1.2 設定パラメータ

設定に入る前に以下のパラメータを決定します。

1.2.1 LDAP base suffix

LDAP ベース・サフィックスを決定します。これはユーザーが任意に設定することができますが、通常ピリオド（.）で区切られた DNS ドメイン名を dc=で区切って使用します。 ここで dc は Domain Component を意味しています。dc 以外の ou:Organization Unit や c:country,o:organization は指定しないでください。
（dc 以外を利用すると smbldap-tools が動作しないことがあります）

- 間違った例
  - dc=example.co.jp (dc=で区切られていない)

1.2.2 LDAP 管理者、複製者 それぞれのパスワード

LDAP サーバーの管理権限を持つユーザー、パスワードを決定します。同様にスレーブサーバーへの複製を行うユーザー、パスワードも決定します。

1.2.3 ドメイン名

smbldap-tools を使用し、LDAP ユーザーの管理を行う際に必要となります。Samba をファイルサーバーとして利用しない場合には重要ではありません。今後 Samba をファイルサーバーとして利用する可能性がある場合はドメイン名の変更が不要となるように決定してください。（構築後に変更するには十分注意が必要な為）

本書では以下のパラメータを使って解説します。

パラメータ	解説例	ユーザ設定
LDAP base suffix	dc=example,dc=co,dc=jp	
LDAP 管理ユーザー	Manager	
LDAP 管理者パスワード	master-pass （本来パスワードは英大文字・小文字・数字を取り混ぜてもっと複雑にすべきです）	
LDAP 複製ユーザー	replica	
LDAP 複製者パスワード	secret （本来パスワードは英大文字・小文字・数字を取り混ぜてもっと複雑にすべきです）	
Windows ドメイン名	LDAPTEST	

2. パッケージ導入

ここでは、OS のインストールが終了しており、弊社パッケージの入手まで終了していると仮定し解説します。

弊社パッケージは以下に保存されています。

```
/root/RPMS/cent4_openldap23/openldap-2.3.43-1.4_OSSTECH.el4.i386.rpm
/root/RPMS/cent4_openldap23/openldap-clients-2.3.43-1.4_OSSTECH.el4.i386.rpm
/root/RPMS/cent4_openldap23/openldap-devel-2.3.43-1.4_OSSTECH.el4.i386.rpm
/root/RPMS/cent4_openldap23/openldap-servers-2.3.43-1.4_OSSTECH.el4.i386.rpm
/root/RPMS/cent4_openldap23/openldap-servers-sql-2.3.43-1.4_OSSTECH.el4.i386.rpm
/root/RPMS/cent4_openldap23/compat-openldap-2.3.43_2.2.29-1.2_OSSTECH.el4.i386.rpm

/root/RPMS/smbldap-tools/smbldap-tools-0.9.2-1.14_OSSTECH.i386.rpm
/root/RPMS/smbldap-tools/perl-Crypt-SmbHash-0.12-1.2.1_OSSTECH.noarch.rpm
/root/RPMS/smbldap-tools/perl-IO-Socket-SSL-0.999-1.1_OSSTECH.noarch.rpm
/root/RPMS/smbldap-tools/perl-Net-SSLeay-1.25-3.1_OSSTECH.i386.rpm
```

個々のパッケージを導入する際には注意する箇所があります。

2.1 openldap

以下のパッケージは openldap-devel をインストールする際に必要となるパッケージです。openldap のパッケージをインストールする前に予めこのパッケージをインストールイメージ（CD もしくは DVD）よりインストールしておいてください。

```
cyrus-sasl-devel-2.1.19-14.i386.rpm
```

また、以下のパッケージは今回利用しませんので、保存ディレクトリから削除してください。

```
openldap-servers-sql-2.3.43-1.4_OSSTECH.el4.i386.rpm
```

以下のコマンドにて openldap を弊社パッケージにします。

```
# cd /root/RPMS/cent4_openldap23
# rpm -Uvh *
```

2.2 smbldap-tools

以下のパッケージは smbldap-tools、perl-Crypt-SmbHash をインストールする際に必要となるパッケージです。smbldap-tools、perl-Crypt-SmbHash のパッケージをインストールする前に予めこのパッケージをインストールイメージ（CD もしくは DVD）よりインストールしておいてください。

```
perl-Digest-SHA1-2.07-5.i386.rpm
perl-LDAP-0.31-5.noarch.rpm
perl-Convert-ASN1-0.18-3.noarch.rpm
perl-XML-SAX-0.12-7.noarch.rpm
perl-XML-NamespaceSupport-1.08-6.noarch.rpm
```

また、以下のパッケージは smbldap-tools にて TLS を使用するために必要となります。

```
perl-IO-Socket-SSL-0.999-1.1_OSSTECH.noarch.rpm
perl-Net-SSLeay-1.25-3.1_OSSTECH.i386.rpm
```

以下のコマンドにて smbldap-tools、perl-Crypt-SmbHash、perl-IO-Socket-SSL、perl-Net-SSLeay を弊社パッケージにします。

```
# cd /root/RPMS/smbldap-tools
# rpm -ivh *
```

以上にて弊社パッケージの導入は完了です。

3. LDAP サーバー構成設計

OpenLDAP を利用した LDAP サーバーの構成例を紹介しますので、運用に適した形態を選択してください。

3.1 基本構成

LDAP サーバーが 1 台の基本構成です。データーの更新・参照を全て受け持ちますので冗長性がありません。

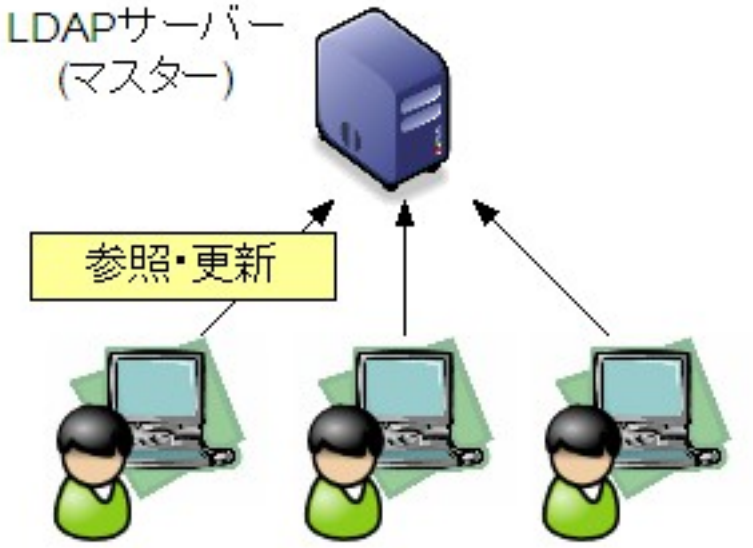

図 3.1.: 基本構成

3.2 マスター・スレーブ構成

LDAP サーバーの冗長性をあげるために、マスター・スレーブの 2 台で構成する方法です。 スレーブサーバーのデーターは複製機能によって自動で更新されます。

OpenLDAP では単一のマスターサーバーしか構成できないため、更新処理はマスターサーバーに対して行う必要があります。そのため、マスターサーバーが停止すると更新処理を行うことができなくなります。

更新処理の冗長性も向上したい場合には、各サーバーにクラスタソフトウェアを導入し、マスターサーバーの障害発生時にはサーバーを切り替えて、LDAP のマスターが稼動できるようにする必要があります。

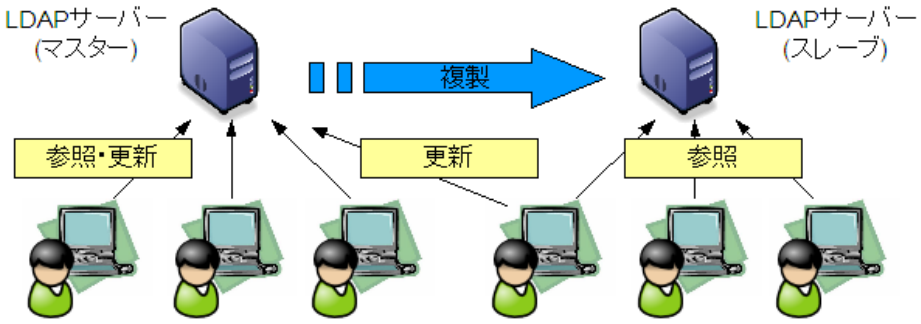

図 3.2.: マスター・スレーブ構成

3.3 スレーブサーバーの追加

LDAP 要求の増加や、拠点の分散などに合わせて、LDAP のスレーブサーバーを追加することができます。

この構成でも更新処理はマスターサーバーに集中しますので、データーの更新を適切に管理する必要があります。

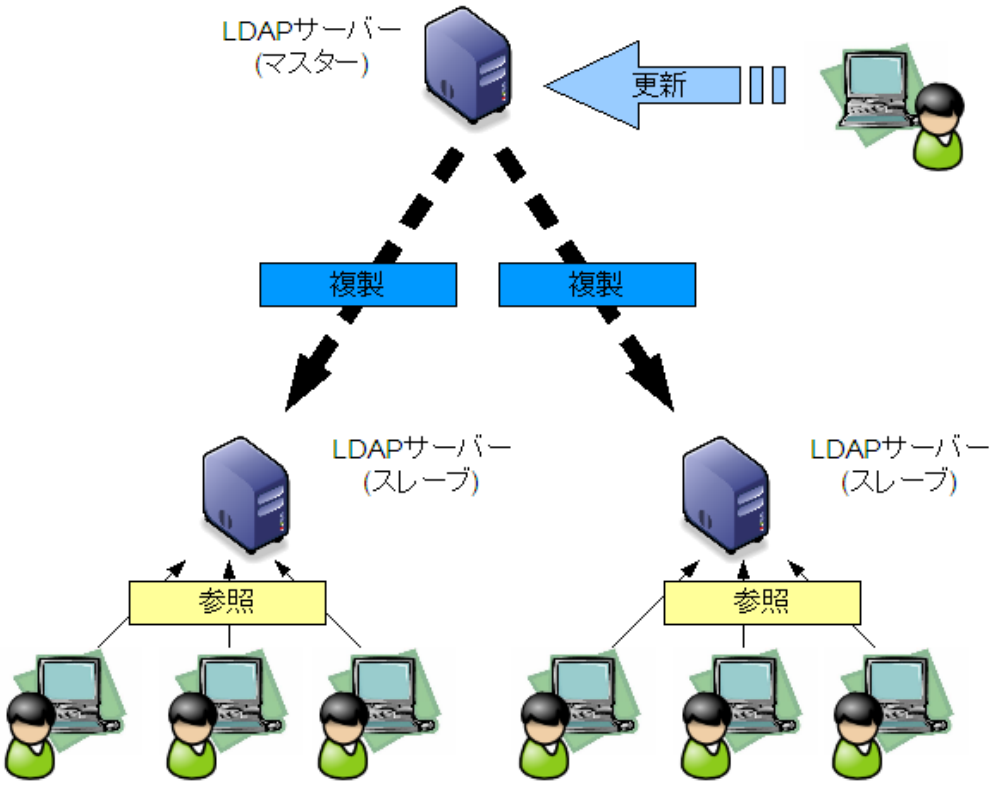

図 3.3.: スレーブサーバーの追加

4. 認証サーバー環境の構築 (OpenLDAP)

マスターサーバーからスレーブサーバーへの LDAP エントリの複製は syncrepl 方式で行います。

本ドキュメントで解説していないパラメータなどについては以下のガイド等を参照ください。

- OpenLDAP 管理者ガイド

  http://www5f.biglobe.ne.jp/~inachi/openldap/admin23/index-ja.html

- Red Hat Enterprise Linux 4 リファレンスガイド

  http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/ja/ref-guide/

4.1 マスターサーバーの設定

まずマスターサーバーの構築について解説します。対象となる設定ファイルは以下の通りです。

4.1.1 /etc/openldap/slapd.conf

このファイルは OpenLDAP の LDAP サービスを提供する slapd デーモンの設定ファイルです。設定が必要なパラメータは以下となります。

- include /etc/openldap/schema/samba.schema

  smbldap-tools を利用するために、samba のスキーマ設定が必要となりますので、以下のスキーマ設定を追加します。

```
include /etc/openldap/schema/samba.schema
```

- suffix　パラメータ

  あらかじめ決定した LDAP base suffix を指定します。

```
suffix "dc=example,dc=co,dc=jp"
```

- rootdn　パラメータ

  あらかじめ決定した LDAP 管理ユーザーの DN(Distinguished Name：識別名)を指定します。

```
rootdn "cn=Manager,dc=example,dc=co,dc=jp"
```

- rootpw　パラメータ

  あらかじめ決定した LDAP 管理者のパスワードを指定します。

```
rootpw master-pass
```

- access　パラメータ

  LDAP 情報のアクセス権限を決定します。

  LDAP 管理ユーザー、LDAP 複製ユーザーの DN の変更のみ実施してください。

```
access to *
        by dn="cn=replica,dc=example,dc=co,dc=jp" read
        by * break
access to *
        by dn="cn=Manager,dc=example,dc=co,dc=jp" write
        by * break
access to attrs=userPassword
        by anonymous auth
        by self =w
        by * none
access to *
        by * read
```

- overlay syncprov、syncprov-sessionlog パラメーター

  複製機能を有効にするために、syncprov 機能を設定します。

```
overlay syncprov
syncprov-sessionlog 128
```

4.1.2　LDAP クライアントの設定

OS のユーザー情報や認証を LDAP 経由で実施するために、OS を LDAP クライアントとして設定します。

設定が必要なファイルは、次の 4 ファイルです。

- /etc/openldap/ldap.conf
  - OpenLDAP のコマンド用の設定ファイル
- /etc/ldap.conf
  - nss_ldap, pam_ldap モジュール用の設定ファイル
- /etc/nsswitch.conf
  - ネームサービススイッチの設定ファイル
- /etc/pam.d/system-auth
  - PAM 認証設定ファイル

これらのファイルの設定には authconfig コマンドを使用します。(RHEL5 以降では authconfig-tui コマンドです。)

```
# authconfig
```

最初の画面で「ユーザー情報」の「LDAP を使用」、「認証」の「LDAP 認証を使用」、「ローカル認証は十分です」にチェックがあるか確認します。チェックがなければチェックをつけます。

次の画面で LDAP サーバーのホスト名と、LDAP の「ベース DN」として base suffix を指定します。ホスト名は「利用する LDAP サーバーを「 , 」 （カンマ）区切りで指定することで、LDAP 問い合わせの冗長化を設定することができます。

複数の LDAP サーバーを指定した場合、指定した順番で、lDAP サーバーに問い合わせをしますのでマスターサーバーから記入します。

4.2 スレーブサーバーの設定

次にスレーブサーバーの構築について解説します。

4.2.1 /etc/openldap/slapd.conf

このファイルは OpenLDAP の LDAP サービスを提供する slapd デーモンの設定ファイルです。設定が必要なパラメータは以下となります。

- include /etc/openldap/schema/samba.schema

  smbldap-tools を利用するために、samba のスキーマ設定が必要となりますので、以下のスキーマ設定を追加します。

  ```
  include /etc/openldap/schema/samba.schema
  ```

- suffix　パラメータ

  あらかじめ決定した LDAP base suffix を指定します。

  ```
  suffix "dc=example,dc=co,dc=jp"
  ```

- rootdn　パラメータ

  あらかじめ決定した LDAP 管理ユーザーの DN(Distinguished Name：識別名)を指定します。

  ```
  rootdn "cn=Manager,dc=example,dc=co,dc=jp"
  ```

- rootpw　パラメータ

  あらかじめ決定した LDAP 管理者のパスワードを指定します。

```
rootpw master-pass
```

- access　パラメータ

  LDAP 情報のアクセス権限を決定します。

  LDAP 管理ユーザー、LDAP 複製ユーザーの DN の変更のみ実施してください。

```
access to *
        by * break
access to attrs=userPassword
        by anonymous auth
        by * none
access to *
        by * read
```

- syncrepl　パラメータ

  LDAP 情報の複製を行う為の設定項目を決定します。provider（マスターサーバーの URI:必ずホスト名で）、searchbase（複製対象エントリ）、binddn（マスターサーバーへ bind する複製者）、credentials（複製者のパスワード）の変更のみ実施してください。

```
syncrepl rid=1
        provider="ldap://master.example.co.jp/"
        type=refreshAndPersist
        retry="5 10 30 +"
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials=secret
```

- updateref　パラメータ

  マスターサーバーの URI を指定します。

```
updateref "ldap://master.example.co.jp/"
```

4.2.2 slapd.conf 以外の設定ファイル

/etc/openldap/slapd.conf　以外の設定ファイルは以下です。設定内容はマスターサーバーと 1 点を除いて変わりありません。

- /etc/openldap/ldap.conf
  - ldap クライアントとしての設定ファイル
- /etc/ldap.conf
  - ldap クライアントとしての設定ファイル(nss_ldap 用)
- /etc/nsswitch.conf
  - システムデータベースとネームサービススイッチの設定ファイル
- /etc/pam.d/system-auth
  - PAM 認証設定ファイル

マスターサーバー時同様に、最終章の設定ファイルよりユーザーが変更する場合は以下のコマンドを使用します。

```
# authconfig
```

最初の画面の設定内容はマスターサーバーの設定と同じです。

次に LDAP サーバーの IP アドレス、LDAP base suffix を入力します。 優先的に参照するサーバーを自サーバー(スレーブサーバー)とするため、スレーブサーバーの IP アドレスから記入します。


root@main:~
ファイル(F) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
authconfig 4.6.10 - (c) 1999-2005 Red Hat, Inc.
LDAP 設定
[*] TLS を使用
サーバー: sub.main
ベース DN: dc=example,dc=co,dc=jp
戻る
OK
<Tab>/<Alt-Tab> 項目間の移動 | <Space> 選択 | <F12> 次の画面

5. OpenLDAP の TLS 設定

LDAP は通信を平文で行うため、ネットワークを盗聴される可能性があります。そこで、LDAP の通信を TLS(Transport Layer Security)によって暗号化することができます。

LDAP の暗号化には、LDAPS による通信と StartTLS による通信の２種類があります。

LDAPS では通信ポートとして LDAP の 389 番ではなく 636 番を利用し、常に暗号化通信を行います。一方、StartTLS を利用した場合、通信ポートとして LDAP の 389 番を利用しますが、通信の最初にネゴシエーションを行い、TLS に対応している場合は暗号化通信を行います。

5.1 自己証明書の作成

LDAP サーバーへのアクセスを TLS (SSL) にするため、証明書の作成とインストールについて解説します。本書では、プライベートな環境での利用を想定しているため、公的な認証局 (CA, Certificate Authority) の利用ではなく、自己署名を利用した証明書についての解説となります。

自己署名の証明書を生成するには openssl コマンドの req サブコマンドに -x509 オプションを指定します。以下は、マスターサーバー 用の自己署名証明書ファイルと秘密鍵ファイルを生成するコマンドラインです。秘密鍵の含まれるファイルの内容は第三者に漏洩しないよう注意を要します。

```
# openssl req \
-x509 \
-newkey rsa:2048 \
-nodes \
-keyout master.example.co.jp.key \
-out master.example.co.jp.pem \
-days 3650 \
-subj "/C=JP/ST=Tokyo/L=Shinagawa-ku/O=OSSTECH/OU=development/CN=master.example.co.jp"
```

実行すると以下のメッセージが表示され、マスターサーバー 用の自己署名証明書ファイル master.example.co.jp.pem、秘密鍵ファイル master.example.co.jp.key が生成されます。

```
Generating a 2048 bit RSA private key
..............................+++
.....................................................................+++
writing new private key to 'master.example.co.jp.key'
```

同様にして、スレーブサーバー 用の自己署名証明書と秘密鍵を生成します。その際は一般名(CN の部分)をスレーブサーバーのホスト名にします。また、証明書、秘密鍵のファイル名も変更します。（生成はマスターサーバーで実施して構いません）

```
# openssl req \
```

```
-x509 \
-newkey rsa:2048 \
-nodes \
-keyout slave.example.co.jp.key \
-out slave.example.co.jp.pem \
-days 3650 \
-subj "/C=JP/ST=Tokyo/L=Shinagawa-ku/O=OSSTECH/OU=development/CN=slave.example.co.jp"
```

openssl コマンドに与えた引数の意味は次の通りです:

- req
  - 公開鍵への署名要求 (CSR) を生成するためのサブコマンド。
- -x509
  - 署名要求を生成せずに、自己署名の証明書を生成を指示。
- -newkey rsa:2048
  - 鍵ペアの生成を指示、および鍵の種類 (RSA) と鍵長 (2048 ビット) の指定。
- -nodes
  - 秘密鍵を暗号化せずに保存。
- -keyout master.example.co.jp.key
  - 生成する秘密鍵の出力先のファイル名。（ファイル名は任意）
- -out master.example.co.jp.pem
  - 生成する自己署名証明書の出力先のファイル名。（ファイル名は任意）
- -days 3650
  - 生成する自己署名証明書の有効期間。(日数)
  - 通常、省略すると 30 日となる。
- -subj "*…省略…*/CN=master.example.co.jp"
  - 証明書に記載されるサイトの識別名 (DN, Ditinguished Name)。
  - 一般名 (CN, Common Name) の値はホスト名にする必要がある。
  - プライベートでの利用であるため、一般名以外の値は重要ではない。

証明書の内容は openssl コマンドの x509 サブコマンドで確認することができます。下記の実行例のように、証明書の発行者が「Issuer」の欄に、証明対象が「Subject」の欄で示され、証明書の有効期間は「Validity」欄の「Not Before」の日時から「Not After」の日時までとなります (日本時間ではなく協定世界時で表示される点に注意)。

```
# openssl x509 -noout -text -in master.example.co.jp.pem
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=JP, ST=Tokyo, L=Shinagawa-ku, O=OSSTECH, OU=development,
CN=master.example.co.jp
        Validity
            Not Before: Feb 27 01:08:03 2008 GMT
            Not After : Mar 28 01:08:03 2008 GMT
        Subject: C=JP, ST=Tokyo, L=Shinagawa-ku, O=OSSTECH, OU=development,
CN=master.example.co.jp
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
…以下省略…
```

5.2 証明書と秘密鍵の設定 (マスターサーバー)

マスターサーバーに証明書と秘密鍵をインストールします。以下、カレントディレクトリに生成した証明書と秘密鍵があるものとします。

最初に、インストール先のディレクトリを適宜作成します。秘密鍵のインストール先ディレクトリ (/etc/openldap/private) のパーミッションとグループにご注意ください。スレーブサーバー側も同様に用意します。

```
# mkdir /etc/openldap/private
# chmod 750 /etc/openldap/private
# chgrp ldap /etc/openldap/private
```

すべての証明書を認証局の証明書として /etc/openldap/cacerts にインストールします(CA.pem というファイル名は任意)。順番は関係ありません。

```
# cat master.example.co.jp.pem  >> /etc/openldap/cacerts/CA.pem
# cat slave.example.co.jp.pem >> /etc/openldap/cacerts/CA.pem
# scp /etc/openldap/cacerts/CA.pem slave:/etc/openldap/cacerts/CA.pem
```

自ホストの証明書を /etc/openldap/cacerts に、自ホストの秘密鍵を /etc/openldap/private にインストールします。

```
# cp master.example.co.jp.pem /etc/openldap/cacerts
# cp master.example.co.jp.key /etc/openldap/private
```

/etc/openldap/slapd.conf の TLSCACertificateFile、TLSCertificateFile、TLSCertificateKeyFile パラメータにマスターサーバーの自己証明書並びに秘密鍵を指定します。

```
TLSCACertificateFile /etc/openldap/cacerts/CA.pem
TLSCertificateFile /etc/openldap/cacerts/master.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/master.example.co.jp.key
```

5.3 証明書と秘密鍵の設定 (スレーブサーバー)

スレーブサーバーに証明書と秘密鍵をインストールします。以降の説明では生成した証明書と秘密鍵がカレントディレクトリにあるものとします。

最初に、インストール先のディレクトリを適宜作成します。秘密鍵のインストール先ディレクトリ (/etc/openldap/private) のパーミッションとグループにご注意ください。

```
# mkdir /etc/openldap/private
# chmod 750 /etc/openldap/private
# chgrp ldap /etc/openldap/private
```

すべての証明書を認証局の証明書として /etc/openldap/cacerts にインストールします(CA.pem というファイル名は任意のファイル名をつけることができます)。順番は関係ありません。

```
# cat master.example.co.jp.pem  >> /etc/openldap/cacerts/CA.pem
# cat lave.example.co.jp.pem >> /etc/openldap/cacerts/CA.pem
```

自ホストの証明書を /etc/openldap/cacerts に、自ホストの秘密鍵を /etc/openldap/private にインストールします。

```
# cp slave.example.co.jp.pem /etc/openldap/cacerts
# cp slave.example.co.jp.key /etc/openldap/private
```

/etc/openldap/slapd.conf の TLSCACertificateFile、TLSCertificateFile、TLSCertificateKeyFile パラメータに自己証明書並びに秘密鍵を指定します。

```
TLSCACertificateFile /etc/openldap/cacerts/CA.pem
TLSCertificateFile /etc/openldap/cacerts/slave.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/slave.example.co.jp.key
```

5.4 slapd.conf の設定(スレーブサーバー)

TLS 接続を設定し、LDAPS 接続に変更した場合、複製機能で利用する通信も LDAPS 経由に変更する必要があります。そのため、slapd.conf の URI を指定している箇所を ldap から ldaps に変更する必要があります。

- syncrepl　パラメータ

  LDAP 情報の複製を行う為の設定項目を決定します。provider（マスターサーバーの URI:必ずホスト名で）、searchbase（複製対象エントリ）、binddn（マスターサーバーへ bind する複製者）、credentials（複製者のパスワード）の変更のみ実施してください。

```
syncrepl rid=1
        provider="ldaps://master.example.co.jp/"       ← ldaps に変更
        type=refreshAndPersist
        retry="5 10 30 +"
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials=secret
```

- updateref　パラメータ

  マスターサーバーの URI を指定します。

```
updateref "ldaps://master.example.co.jp/"       ← ldaps に変更
```

5.5 LDAP クライアントの設定

5.5.1 マスターサーバー

TLS を利用する場合、authconfig コマンドの LDAP サーバーを設定する画面で、[TLS を使用]にチェックを入れ、LDAP サーバーのホスト名、LDAP base suffix を入力します。 設定する LDAP サーバーのホスト名は、自サーバーを優先するために、自サーバーから指定します。

また、ホスト名は証明書に指定した一般名 (CN, Common Name) にする必要があります。

5.5.2 スレーブサーバー

TLS を利用する場合、authconfig コマンドの LDAP サーバーを設定する画面で、[TLS を使用]にチェックを入れ、LDAP サーバーのホスト名、LDAP base suffix を入力します。ここでもマスターサーバー同様に自サーバーから記入します。

マスターサーバー同様、authconfig コマンドでは以下のパラメーターが設定されませんので、手動にて修正してください。

- URI　パラメータ

  LDAP サーバーの URI を指定します。

  ```
  URI ldaps://slave.example.co.jp/ ldaps://master.example.co.jp/
  ```

- TLS_CACERT　パラメータ

  生成した認証局の証明書を指定します。

  ```
  TLS_CACERT /etc/openldap/cacerts/CA.pem
  ```

- /etc/ldap.conf
  - uri　パラメータ

    LDAP サーバーの URI を指定します。

    ```
    uri ldaps://slave.example.co.jp/ ldaps://master.example.co.jp/
    ```

  - tls_cacertfile　パラメータ

    生成した認証局の証明書を指定します。

    ```
    tls_cacertfile /etc/openldap/cacerts/CA.pem
    ```

6. チューニングパラメーター

6.1 索引設定

検索時に索引を利用可能にするため、属性ごとに索引を設定することができます。

- 索引の設定例

```
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uid                               eq,pres,sub
```

索引を設定すると、検索時の性能が向上しますが、エントリの更新時に索引の更新も必要となるため、更新の性能は低下します。

したがって、不要な索引は設定しないように気をつける必要があります。

/etc/openldap/slapd.conf の索引設定を変更した場合、slapindex コマンドで索引を再作成する必要があります。索引の再作成の際には、slapd を停止して、次のコマンドを実行します。

```
# /usr/sbin/slapindex
```

slapindex コマンドを実行すると、/var/lib/ldap 配下の各索引のファイルが更新されますが、root ユーザーで slapindex を実行すると、ファイルの所有者が root に変更され、slapd の再起動時に問題となります。

したがって、slapindex が完了したら、chown コマンドで/var/lib/ldap 配下のファイルの所有者を ldap ユーザーに変更することを忘れないでください。

```
# chown -R ldap:ldap /var/lib/ldap/*
```

6.2 キャッシュ設定

OpenLDAP の slapd は、LDAP のエントリをキャッシュとして保持します。キャッシュのチューニングとして、次のパラメーターを設定することができます。

```
checkpoint 512 5
cachesize 500
idlcachesize 1500
```

それぞれのパラメーターは次の意味を表します。

- checkpoint [キロバイト] [分]
  - 指定したサイズのデーターがデーターベースのキャッシュに書き込まれるか、指定した時間が経過したときに、チェックポイント処理によってデータベースのキャッシュがディス

クに書き込まれ、チェックポイントがトランザクションログに記録されます。

- cachesize [エントリ数]
  - slapd がメモリ上に解析済みの状態で保持するキャッシュのエントリ数を指定します。このキャッシュ内のエントリは、利用時にエントリの解析処理が不要なため、非常に高速に処理されます。
- idlcachesize [エントリ数]
  - インデックスキャッシュとしてメモリに保持可能なエントリ数を指定します。検索時にインデックスを利用する際の性能に影響します。

6.3 BDB 設定

OpenLDAP がデーターを格納する BDB のチューニングのために、次のパラメーターを設定することができます。

- BDB のパラメーター設定例

```
dbconfig set_cachesize 0 8388608 0
dbconfig set_lk_max_objects 5000
dbconfig set_lk_max_locks 5000
dbconfig set_lk_max_lockers 5000
dbconfig set_flags DB_LOG_AUTOREMOVE
dbconfig set_lg_regionmax 1048576
dbconfig set_lg_max 104857600
dbconfig set_lg_bsize 20971520
```

それぞれのパラメーターは次の意味を表します。

- set_cachesize [ギガバイト] [バイト] [セグメント数]
  - メモリにキャッシュするデーターのサイズをギガバイト単位で指定します。
  - メモリにキャッシュするデーターのサイズをバイト単位で指定します。
  - キャッシュの領域を構成するセグメント数を指定します。 0、または 1 を指定した場合、キャッシュ領域全体が 1 つのセグメントで構成されます。
  - ギガバイトとバイトの合計サイズが、BDB のキャッシュとして利用され、最大 4 ギガバイトまで指定することができます。
- set_lk_max_objects [数値]
  - BDB で同期ロックのために利用可能とするオブジェクト数の最大値を指定します。
- set_lk_max_locks [数値]
  - BDB でロックを利用可能なロック数の最大値を指定します。
- set_lk_max_lockers [数値]
  - BDB でロックを実行するオブジェクトの最大値を指定します。

- set_flags [パラメーター]
  - BDB に様々な機能を設定します。
    - DB_LOG_AUTOREMOVE
      - BDB が不要になったログファイルを自動で削除します。
- set_lg_regionmax [バイト]
  - データーベースに利用されるファイル名をキャッシュするためのメモリサイズを指定します。
- set_lg_max [バイト]
  - 1 つあたりのログファイルの最大サイズをバイト単位で指定します。
- set_lg_bsize [バイト]
  - ログ情報をキャッシュしておくためのメモリサイズをバイト単位で指定します。

6.4 同時接続数

OpenLDAP では、slapd に接続できる同時接続数がコンパイル時に決定されます。RHEL4/CentOS4 標準の openldap パッケージでは、最大同時接続数はデフォルトの 1024 に設定されています。弊社提供パッケージでは、最大同時接続数を 16384 に拡大してあります。

弊社 openldap パッケージで最大同時接続数を設定するには、/etc/sysconfig/ldap ファイルで ulimit コマンドを実行するように設定する必要があります。

```
# echo 'ulimit -n 16384' >>/etc/sysconfig/ldap
```

LDAP クライアントから LDAP サーバーに接続されたセッションは、クライアント側から明示的に切断されなければ、接続したままとなります。そのため、多数のセッションが接続されたままになってしまう場合には、slapd.conf の idletimeout パラメーターで、アイドル状態のセッションを自動的に切断するように設定することができます。

idletimeout パラメーターは、秒で指定し、0 を指定した場合は自動での切断が行われません。またデフォルト値は 0 となっています。

7. ユーザー登録環境の構築 (smbldap-tools)

ユーザー登録に smbldap-tools を利用するため、smbldap-tools の設定が必要になります。

7.1 マスターサーバー側の設定

ここではマスターサーバー側の設定について解説します。まずはドメイン SID(Security Identifier)を確認します。

マスターサーバーで以下のコマンドを実施します。

```
# service ldap start
# net getlocalsid
```

すると以下のようにドメインの SID が表示されます。（SID の値は環境ごとに変わります）

```
SID for domain MASTER is: S-1-5-21-2888749833-2609368007-2065259343
```

これで、ドメイン SID は S-1-5-21-2888749833-2609368007-2065259343 と決定しました。

7.1.1 /etc/smbldap-tools/smbldap.conf

このファイルはユーザー/グループ アカウント管理ツール (smbldap-tools) の設定ファイルです。最終章の設定ファイルよりユーザーが変更する箇所は以下となります。

- SID パラメータ

  net getlocalsid コマンドで表示されたドメイン SID を指定します。

```
SID="S-1-5-21-2888749833-2609368007-2065259343"
```

- sambaDomain パラメータ

  あらかじめ決定した Windows ドメイン名を指定します。

```
sambaDomain="LDAPTEST"
```

- slaveLDAP パラメータ

  参照先 LDAP サーバーのホスト名を指定します。（自サーバーのホスト名）

```
slaveLDAP="master.example.co.jp"
```

- masterLDAP パラメータ

  マスターサーバーのホスト名を指定します。（自サーバーのホスト名）

```
slaveLDAP="master.example.co.jp"
```

- cafile パラメータ

生成した認証局の証明書を指定します。

```
cafile="/etc/openldap/cacerts/CA.pem"
```

- suffix　パラメータ

  あらかじめ決定した LDAP base suffix を指定します。

```
suffix="dc=example,dc=co,dc=jp"
```

7.1.2　/etc/smbldap-tools/smbldap_bind.conf

OpenLDAP への bind するユーザー/パスワード の設定ファイルです。最終章の設定ファイルよりユーザーが変更する箇所は以下となります。

- slaveDN、masterDN　パラメータ

  あらかじめ決定した LDAP 管理ユーザーの DN を指定します。これは/etc/openldap/slapd.conf に指定した rootdn パラメータと同一とします。

```
slaveDN="cn=Manager,dc=example,dc=co,dc=jp"
masterDN="cn=Manager,dc=example,dc=co,dc=jp"
```

- slavePw、masterPw　パラメータ

  あらかじめ決定した LDAP 管理ユーザーの DN を指定します。これは/etc/openldap/slapd.conf に指定した rootdn パラメータと同一とします。

```
slavePw=master-pass
masterPw=master-pass
```

7.2　スレーブサーバー側の設定

ここではスレーブサーバー側の設定について解説します。

7.2.1　/etc/smbldap-tools/smbldap.conf

このファイルはユーザー/グループ アカウント管理ツール (smbldap-tools) の設定ファイルです。このファイルでマスターサーバー側と違う設定箇所は slaveLDAP　パラメータのみです。マスターサーバー側のファイルをコピー後以下の設定を変更してください。

- slaveLDAP　パラメータ

  参照先 LDAP サーバーのホスト名を指定します。（自サーバーのホスト名）

```
slaveLDAP="slave.example.co.jp"
```

7.2.2 ドメイン SID の設定

先ほどのドメイン SID 値を以下のコマンドでスレーブサーバーに設定します。これによりサーバーが同じドメイン SID を持つこととなります。

```
# net setlocalsid S-1-5-21-2888749833-2609368007-2065259343
```

設定後、以下のコマンドにてドメイン SID が設定されているか確認します。

```
# net getlocalsid
SID for domain MASTER is: S-1-5-21-2888749833-2609368007-2065259343
```

8. 初期データーの登録

ここまでで一通りの設定は終了しました。

以下のコマンドをマスターサーバーで実行し、LDAP サーバへ初期データを投入します。（引数の-a には Samba の管理者アカウント名を指定します。今回は Samba は利用しませんが指定しないと root ユーザーとなる為に一般的な管理者 Administrator を指定します。-b も samba にて利用します。ゲスト接続時に使用するアカウントとなります。）

```
# smbldap-populate -a Administrator -b Guest -l 998 -m 512
```

エラーが発生し、正常にデータ投入できない場合は、smbldap.conf の設定をよく確認してください。LDAP の設定を誤ってしまいデータを初期化するときは以下のようにいったん LDAP データを削除します。

```
# service ldap stop
# rm /var/lib/ldap/*
# service ldap start
```

上記で LDAP のデータは消えてしまうので再度、smbldap-populate コマンドを実行して下さい。

次に LDAP に LDAP 管理ユーザー、複製ユーザーを登録します。この登録には LDIF（LDAP Data Interchange Format）という形式のファイルを利用します。add.ldif というファイルを以下の内容で作成します。

```
dn: cn=Manager,dc=example,dc=co,dc=jp
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: Manager
description: LDAP administrator
userPassword: {SSHA}m/K5p7bFcRmDE5Isel0L7O0yV8WImYjL

dn: cn=replica,dc=example,dc=co,dc=jp
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: replica
description: LDAP replication user
userPassword: {SSHA}KIPfZ6KBnO2Dkv/sq/khPaHLNjdLvJVX
```

ここで変更する箇所は以下となります。

あらかじめ決定した LDAP 管理ユーザーの DN を指定します。

```
dn: cn=Manager,dc=example,dc=co,dc=jp
```

LDAP 管理ユーザーのユーザー名を指定します。

```
cn: Manager
```

LDAP 管理者のパスワードをハッシュしたものを指定します。

```
userPassword: {SSHA}m/K5p7bFcRmDE5Isel0L7O0yV8WImYjL
```

先ほど決定した LDAP 複製ユーザーの DN を指定します。

```
dn: cn=replica,dc=example,dc=co,dc=jp
```

LDAP 複製ユーザーのユーザー名を指定します。

```
cn: replica
```

LDAP 複製者のパスワードをハッシュしたものを指定します。

```
userPassword: {SSHA}KIPfZ6KBnO2Dkv/sq/khPaHLNjdLvJVX
```

ハッシュパスワードは以下のコマンドより生成します。

```
# slappasswd -s secret
  （デフォルトのフォーマットが SSHA となっています）
```

マスタサーバー、スレーブサーバー共に LDAP を再起動します。LDAP サーバー起動後に、マスターサーバーで以下のコマンドを実施し、用意した add.ldif ファイルを LDAP のデータベース内に登録します。

```
# service ldap restart
# ldapadd -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -f add.ldif
```

パスワードを入力を求められるので、Manager ユーザーのパスワードを 2 度入力します。エラーが表示されないか確認してください。ここで、-D オプションで指定しているユーザーは、LDAP 管理ユーザーの DN を指定します。

8.1.1 複製確認

ここまでで LDAP の基本設定が終了し、マスター、スレーブ共に LDAP サーバーが起動している状態です。ここで両サーバーの情報に差異がないか以下のコマンドで確認します。（コマンドを実行するのはどちらのサーバーでも構いません）

```
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h 10.0.1.11 > slave.ldif
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h 10.0.1.10 > master.ldif
```

```
# diff -u master.ldif slave.ldif
```

パスワードを入力を求められるので、Manager ユーザーのパスワードを 2 度入力します。ここで、-D オプションには、LDAP 管理ユーザーの DN を指定します。

上記で差異がないことが確認できたら、両サーバーの/etc/openldap/slapd.conf より rootpw の行を削除します。削除後、もう一度 ldap を再起動し、LDAP の接続などが問題なく動作しているか確認します。

- openldap の起動

```
# service ldap restart
```

- 接続確認

```
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -LLL -h 10.0.1.11
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -LLL -h 10.0.1.10
```

パスワードを入力を求められるので、Manager ユーザーのパスワードを 2 度入力します。ここで、-D オプションには、LDAP 管理ユーザーの DN を指定します。

また、OS 起動時に LDAP サーバーのプロセスを起動する為に、chkconfig コマンドを実行します。
（両サーバーで実施してください）

```
# chkconfig ldap on
```

以上でマスター、スレーブ構成の認証サーバー構築は終了です。

9. ログの取得

LDAP サーバーのログを取得したい場合、次の設定を行います。

9.1 syslog の設定

LDAP サーバー(slapd)は、デフォルトで facility の local4 として syslog メッセージを出力します。したがって、syslog の設定で local4 のメッセージを記録可能にする必要があります。

LDAP サーバーのログを/var/log/ldap.log ファイルに記録するために、/etc/syslog.conf に以下の設定を追加します。ファイル名の先頭についているハイフン「-」は、ログ出力の負荷を軽減するため、ログの書き出しごとにディスクを sync することを防ぐための設定です。

```
local4.*       -/var/log/ldap.log
```

syslog を再起動します。

```
# /sbin/service syslog restart
```

9.2 slapd.conf の loglevel 設定

LDAP サーバーのログは、/etc/openldap/slapd.conf の loglevel パラメーターに設定したログ対象に該当するログメッセージが出力されます。

loglevel パラメーターには、数値、もしくはキーワードを指定することができます。数値で指定する場合は、10 進数、もしくは 16 進数で指定します。また、複数のログ対象を記録したい場合は、複数のパラメーターを指定することができます。

指定できる値を以下に示します。

※注意：OpenLDAP のログ出力はデバッグを目的に実装されており、ログ出力を有効にすると(例えば、デフォルトのログレベル”256”に設定する)LDAP サーバーへの負荷が増加してしまいます。そのため、性能を優先させる場合はログレベル”none”を設定することを推奨します。

数値 (10 進数 / 16 進数)	キーワード	意味
1 (0x1)	trace	関数呼び出しのトレース
2 (0x2)	packets	パケット処理のログ
4 (0x4)	args	詳細なトレース
8 (0x8)	conns	コネクション管理のログ
16 (0x10)	BER	送受信したパケットのログ
32 (0x20)	filter	検索フィルターの処理のログ

64 (0x40)	config	設定ファイルの解析ログ
128 (0x80)	ACL	アクセスコントロールのログ
256 (0x100)	stats	接続状況のログ
512 (0x200)	stats2	クライアントに対して送信したエントリのログ
1024 (0x400)	shell	shell バックエンドのログ
2048 (0x800)	parse	エントリ解析のログ
4096 (0x1000)	cache	未使用
8192 (0x2000)	index	未使用
16384 (0x4000)	sync	同期処理のログ
32768 (0x8000)	none	ログレベルに関係なく取得されるログメッセージ以外は記録されない
-1	any	全てのログ

10. LDAP 情報のバックアップ、リストア

10.1 バックアップ

LDAP 情報のバックアップは main サーバー側で cron デーモンを使用し、毎日 ldapsearch コマンドにて LDIF を作成することで対応します。 最終章にバックアップスクリプトのサンプルを掲載しております。

10.2 LDAP データベースのリカバリー

LDAP サーバーで以下のような症状が発生した場合、LDAP データベース(Berkley DB)に不整合が発生している可能性があります。

- slapd が起動しない
- LDAP 検索が実行できない

このような状況になった場合は、以下の手順でデータベースのリカバリーを試みます。なお、マスターサーバー/スレーブサーバーとも手順は同じです。

まず、データベースファイルの整合性を確認します。

```
# /usr/sbin/slapd_db_verify /var/lib/ldap/*.bdb
```

エラーメッセージが表示された場合は、以下の手順でデータベースリカバリーを行います。

```
# /usr/sbin/slapd_db_recover -v -h /var/lib/ldap
```

インデックスを再構築します。

```
# /usr/sbin/slapindex -v
```

LDAP データベースファイルの所有者とグループを ldap に変更します。

```
# chown ldap:ldap /var/lib/ldap/*
```

LDAP サーバーを起動します。

```
# /sbin/service ldap restart
```

LDAP サーバーが起動し、各種 LDAP 操作コマンドが正常に実行できる場合はリカバリーに成功しています。

この手順を実施しても復旧不可能な場合は、次節の「10.3LDAP 情報の復旧方法」を実施してください。

10.3 LDAP 情報の復旧方法

LDAP サーバーのデータは/var/lib/ldap に db ファイルとして保存されています。しかし、利用の仕方によってはこのデータは壊れてしまうことがございます。壊れてしまった場合はマスター、スレーブそれぞれ以下の方法で復旧させてください。

10.3.1 スレーブ側の復旧

スレーブ側のサーバーに障害が発生し、再度 LDAP データを再同期させるには以下の手順を実施してください。

```
# service ldap stop
# rm -f /var/lib/ldap/*
# service ldap start
```

手順としては以上となります。データが正常に複製されているかどうかは以下のコマンドマスター、スレーブそれぞれの情報を取得しデータの比較をしてください。

```
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h 10.0.1.11 > slave.ldif
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h 10.0.1.10 > master.ldif
# diff -u master.ldif slave.ldif
```

パスワードを入力を求められるので、Manager ユーザーのパスワードを 2 度入力します。ここで、-D オプションには、LDAP 管理ユーザーの DN を指定します。

スレーブへ全て反映されるのには少々時間がかかる場合があります（データー量によります）。

10.3.2 マスター側の復旧

マスター側のサーバーに障害が発生した場合の復旧手順は以下となります。

```
# service ldap stop
# rm -f /var/lib/ldap/*
```

ldap を再起動する前に、main サーバーの/etc/openldap/slapd.conf に rootpw の行を設定します。

```
# service ldap start
# ldapadd -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -f /opt/samba-
ldap_backup/20080312.ldif
```

パスワードを入力を求められるので、Manager ユーザーのパスワードを 2 度入力します。エラーが表示されないか確認してください。ここで、-D オプションで指定しているユーザーは、LDAP 管理ユーザーの DN を指定します。

ここで登録する LDIF ファイルは、バックアップしている LDIF ファイル（/opt/samba-ldap_backup/日付.ldif)、動作中であるスレーブサーバーのデータファイル（ldapsearch をスレーブサーバーに対して実施）どちらのデーターを利用しても構いません。新しい方をご利用ください。

マスター側が再構築し終わりましたら、念のため、スレーブ側も　10.3.1 スレーブ側の復旧　の手順通り、再構築を実施してください。

11. SLAMD によるパフォーマンス測定

LDAP サーバーのパフォーマンス測定を行うために、SLAMD と呼ばれるパフォーマンス測定ツールを利用することができます。本章では SLAMD の基本的な利用方法について説明します。

11.1 環境

SLAMD は、複数のクライアントから LDAP サーバーに負荷を発生させることができます。そのため、負荷発生用のクライアントと、LDAP サーバーが別々に必要になります。

- SLAMD サーバー
  - slamd-1.8.2
    - http://slamd.com/
- OpenLDAP サーバー
  - openldap-2.3.27-8

11.2 環境構築

11.2.1 OpenLDAP サーバーの設定

SLAMD のサイトからダウンロードした slamd-1.8.2.tar.gz を展開します。

```
# tar xfz slamd-1.8.2.tar.gz
```

OpenLDAP 用の設定ファイルをコピーします。

```
# cp slamd/config/slamd.openldap.conf /etc/openldap/
```

/etc/openldap/slapd.conf の最後に次の設定を追加します。

```
include /etc/openldap/slamd.openldap.conf
```

LDAP サーバーを再起動します。

```
# /sbin/service ldap restart
```

SLAMD 用のエントリを LDAP に登録します。SLAMD 用エントリとして、o=SLAMD,dc=example,dc=com を作成するものとして説明します。

- slamd.ldif

```
dn: o=SLAMD,dc=example,dc=com
objectClass: organization
```

```
o: SLAMD
```

slamd.ldif のエントリを ldapadd コマンドで追加します。

```
# ldapadd -x -W -D “cn=Manager,dc=example,dc=com” -f slamd.ldif
```

11.2.2 SLAMD サーバーの設定

Sun のサイトから、Linux 用 JDK をダウンロードし、インストールします。

http://java.sun.com/javase/downloads/?intcmp=1281

```
# chmod 755 ./jdk-6u5-linux-i586-rpm.bin
# ./jdk-6u5-linux-i586-rpm.bin
```

SLAMD のサイトからダウンロードした slamd-1.8.2.tar.gz を展開します。

```
# tar xfz slamd-1.8.2.tar.gz
```

起動スクリプトなどを設定します。

slamd/bin/startup.sh 、 slamd/bin/shutdown.sh の先頭付近にある次の行を削除します。

```
echo ”PLEASE EDIT THE $0 SCRIPT TO SPECIFY YOUR ENVIRONMENT CONFIGURATION”
exit 1
```

JAVA_HOME を、次の設定に変更します。

```
JAVA_HOME=/usr/java/jdk1.6.0_05/
```

SLAMD サーバーを起動します。

```
# cd slamd/bin
# ./startup.sh
```

Web ブラウザで SLAMD サーバーの Web 管理画面にアクセスします。

http://localhost:8080/slamd

最初は何も設定されていないため、「here」のリンクをクリックして設定画面に移動します。

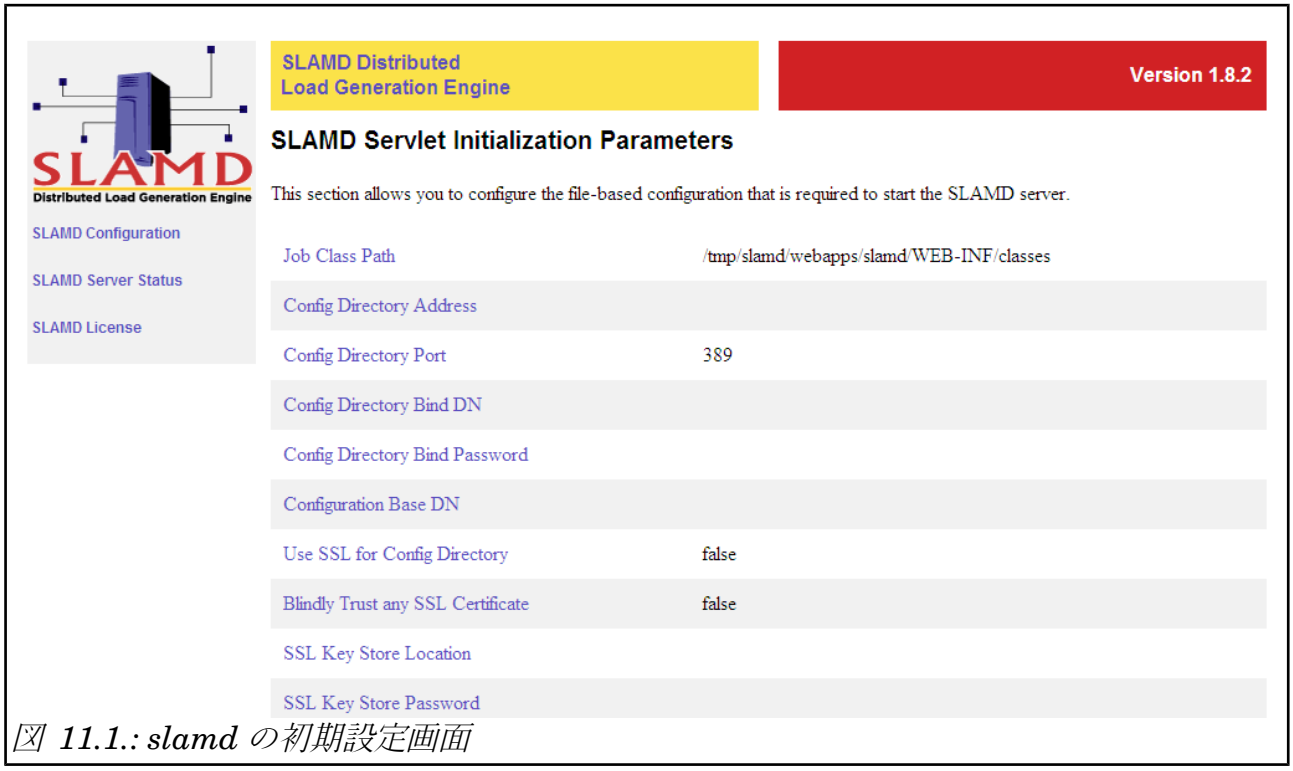

図 11.1.: slamd の初期設定画面

上記画面中の以下の項目を設定します。

- Config Directory Address
  - 10.1.0.10
- Config Directory Bind DN
  - cn=Manager,dc=example,dc=com
- Config Directory Bind Password
  - ********
- Configuration Base DN
  - o=SLAMD,dc=example,dc=com

画面右下の「Add SLAMD Config」をクリックすると、OpenLDAP サーバーに SLAMD の設定が登録されます。

準備が完了したら、「SLAMD Server Status」の画面の「Start SLAMD」をクリックして、SLAMD を開始します。

11.2.3 SLAMD クライアントの設定

負荷を実行する SLAMD クライアント、および SLAMD クライアントを管理する SLAMD クライアン

トマネージャーを設定します。

slamd-1.8.2.tar.gz を展開したディレクトリに含まれている slamd_client-1.8.2.tar.gz を展開します。

```
# cd slamd
# tar xfz slamd_client-1.8.2.tar.gz
```

クライアント用の設定ファイル slamd/slamd_client/slamd_client.conf を設定します。

先頭付近にある次の行を削除します。

```
echo "PLEASE EDIT slamd_client.conf TO SPECIFY YOUR ENVIRONMENT CONFIGURATION"
exit 1
```

JAVA_HOME を設定します。

```
JAVA_HOME=/usr/java/jdk1.6.0_05/
```

SLAMD_ADDRESS を設定します。

```
SLAMD_ADDRESS=127.0.0.1
```

SLAMD クライアントと、SLAMD クライアントマネージャーを起動します。

```
# cd slamd/slamd_client
# ./start_client.sh &
# ./start_client_manager.sh &
```

11.3 SLAMD による測定

左側メニューの「Schedule Job」をクリックし、測定を行うジョブを選択し、ジョブを登録します。

登録されたジョブが完了すると、左側メニューの「View Completed Jobs」から結果を確認することができます。

12. LDAP を活用したシングル・サインオン

本章では LDAP を活用したシングル・サインオンの利用例を紹介します。

12.1 Apache + mod_auth_tkt

Web サーバーを Apache で構成する場合、Apache の mod_auth_tkt モジュールを利用することで、LDAP 認証を利用したシングルサインオンを実現することができます。

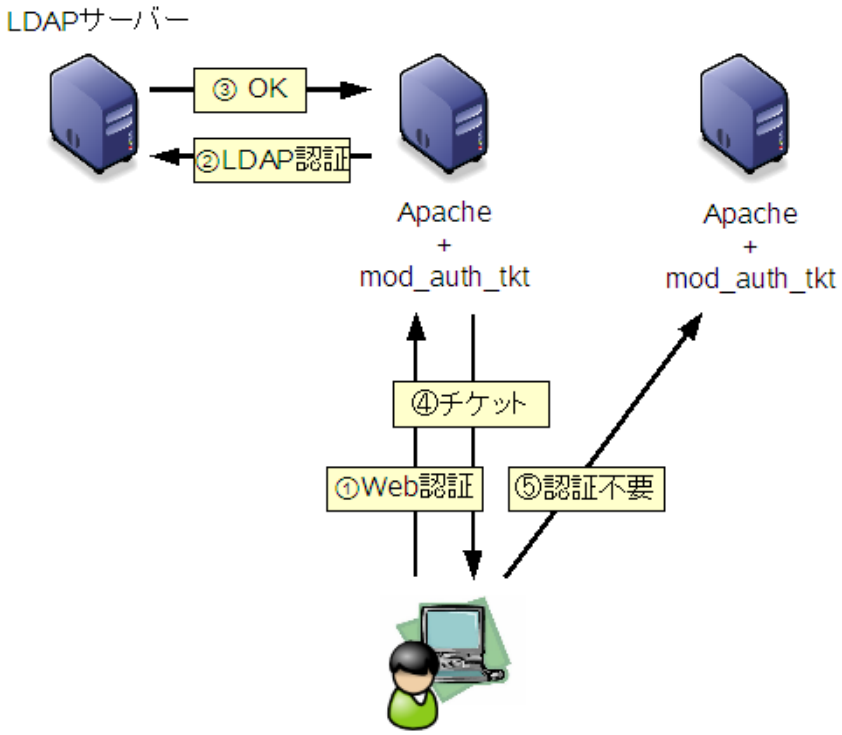

図 12.1.: Apache + mod_auth_tkt によるシングルサインオン

12.2 SAML によるシングル・サインオン

SAML は、OASIS で標準化されたシングル・サインオンのための XML 標準仕様です。

Web サイトを SAML 対応で構築することで、認証情報を複数のドメイン間で共有することが可能になります。SAML は HTTP、SOAP で通信を行います。

以下は、SAML によるシングル・サインオンの構成例です。HTTP 経由で送られる SAML の認証要求を適切にハンドリングすることで、組織内の認証サーバーによる認証を利用することが可能になります。

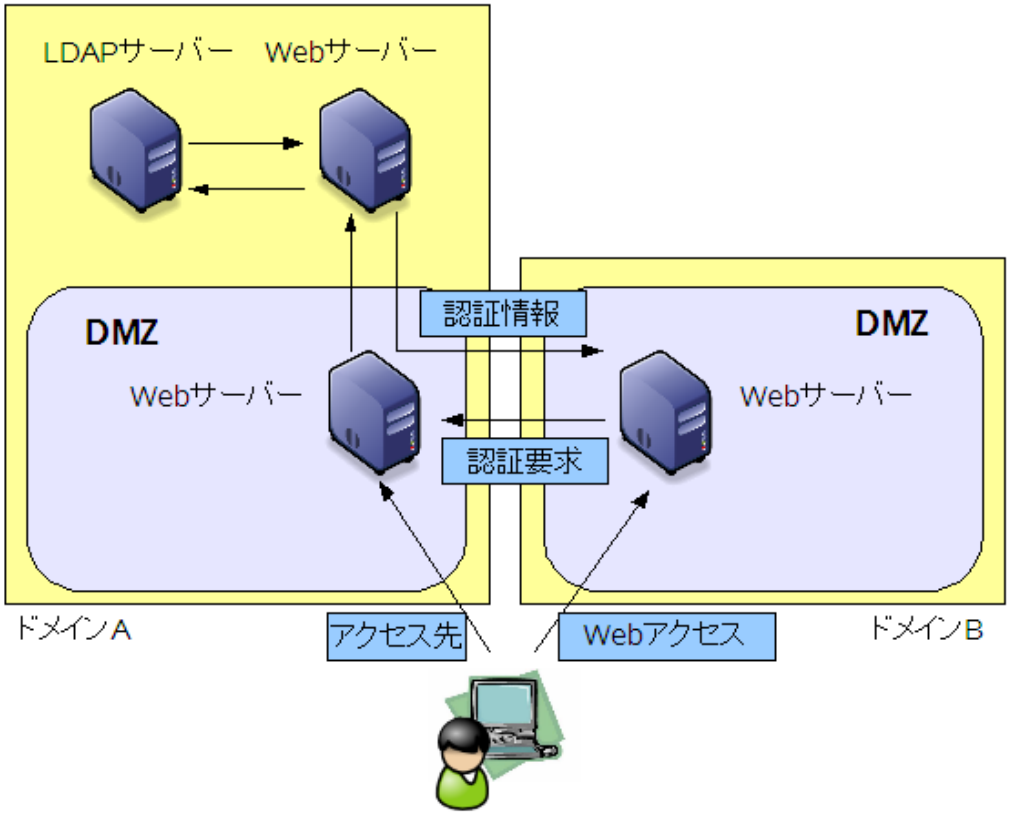

図 12.2.: SAML によるシングル・サインオンの構成例(pull モデル)

13. LDAP GUI クライアントの紹介

- LDAP Browser Editor
  - Java ベースの LDAP クライアント
  - http://www-unix.mcs.anl.gov/~gawor/ldap/
- phpldapadmin
  - PHP による Web ブラウザ経由の LDAP クライアント
  - http://sourceforge.net/projects/phpldapadmin
- LDAP Explorer
  - Windows アプリケーション
  - http://sourceforge.net/projects/ldaptool
- Softerra LDAP Browser
  - Windows アプリケーション
  - 更新不可。更新可能な GUI ツールは、LDAP Administrator(有償)にて提供
  - http://www.ldapadministrator.com/download.htm
- JXplorer
  - Java アプリケーション
  - http://www.jxplorer.org/

14. 各種設定ファイル

今回の設定内容を掲載します。コメント類のいくつかは省略してあります。

14.1 master.example.co.jp、slave.example.co.jp 共通設定

14.1.1 /etc/smbldap-tools/smbldap_bind.conf

```
slaveDN="cn=Manager,dc=example,dc=co,dc=jp"
slavePw=master-pass
masterDN="cn=Manager,dc=example,dc=co,dc=jp"
masterPw=master-pass
```

14.1.2 /etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
hosts:      files dns
bootparams: files
ethers:     files
netmasks:   files
networks:   files
protocols:  files ldap
rpc:        files
services:   files ldap
netgroup:   files ldap
publickey:  files
automount:  files ldap
aliases:    files
```

14.1.3 /etc/pam.d/system-auth

```
auth        required      /lib/security/$ISA/pam_env.so
auth        sufficient    /lib/security/$ISA/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/$ISA/pam_ldap.so use_first_pass
auth        required      /lib/security/$ISA/pam_deny.so
account     required      /lib/security/$ISA/pam_unix.so broken_shadow
account     sufficient    /lib/security/$ISA/pam_localuser.so
```

```
account     sufficient    /lib/security/$ISA/pam_succeed_if.so uid < 100 quiet
account     [default=bad success=ok user_unknown=ignore] /lib/security/$ISA/pam_ldap.so
account     required      /lib/security/$ISA/pam_permit.so
password    requisite     /lib/security/$ISA/pam_cracklib.so retry=3
password    sufficient    /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password    sufficient    /lib/security/$ISA/pam_ldap.so use_authtok
password    required      /lib/security/$ISA/pam_deny.so
session     required      /lib/security/$ISA/pam_limits.so
session     required      /lib/security/$ISA/pam_unix.so
session     optional      /lib/security/$ISA/pam_ldap.so
```

14.2 master.example.co.jp

14.2.1 /etc/smbldap-tools/smbldap.conf

```
SID="S-1-5-21-2888749833-2609368007-2065259343"
sambaDomain="LDAPTEST"
slaveLDAP="master.example.co.jp"
slavePort="389"
masterLDAP="master.example.co.jp"
masterPort="389"
ldapTLS="1"
verify="require"
cafile="/etc/openldap/cacerts/CA.pem"
clientcert=""
clientkey=""
suffix="dc=example,dc=co,dc=jp"
usersdn="ou=Users,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
hash_encrypt="SSHA"
crypt_salt_format="%s"
userLoginShell="/bin/bash"
```

```
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"
userSmbHome="\\PDC-SRV\%U"
userProfile="\\PDC-SRV\profiles\%U"
userHomeDrive="H:"
userScript="logon.bat"
mailDomain="example.co.jp"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
encoding="UTF-8"
OracleSES="0"
```

14.2.2 /etc/ldap.conf

```
base dc=example,dc=co,dc=jp
uri ldap://master.example.co.jp/ ldap://slave.example.co.jp/
ldap_version 3
timelimit 30
bind_timelimit 5
bind_policy soft
idle_timelimit 5
pam_password md5
tls_cacertfile /etc/openldap/cacerts/CA.pem
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
```

14.2.3 /etc/openldap/slapd.conf

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/nis.schema
```

```
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/samba.schema
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
threads 16
loglevel 0
timelimit 30
idletimeout 10
sizelimit unlimited
TLSCACertificateFile /etc/openldap/cacerts/CA.pem
TLSCertificateFile /etc/openldap/cacerts/master.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/master.example.co.jp.key
access to *
        by dn="cn=replica,dc=example,dc=co,dc=jp" read
        by * break
access to *
        by dn="cn=Manager,dc=example,dc=co,dc=jp" write
        by * break
access to attrs=userPassword
        by anonymous auth
        by self =w
        by * none
access to *
        by * read
database        bdb
suffix          "dc=example,dc=co,dc=jp"
rootdn          "cn=Manager,dc=example,dc=co,dc=jp"
rootpw master-pass（設定当初必要、後に削除）
directory       /var/lib/ldap
mode 0640
lastmod on
checkpoint 512 5
cachesize 500
idlcachesize 1500
dbconfig set_cachesize 0 8388608 0
```

```
dbconfig set_lk_max_objects 5000
dbconfig set_lk_max_locks 5000
dbconfig set_lk_max_lockers 5000
dbconfig set_flags DB_LOG_AUTOREMOVE
dbconfig set_lg_regionmax 1048576
dbconfig set_lg_max 104857600
dbconfig set_lg_bsize 20971520
index objectClass               eq
index ou                        eq
index cn                        eq,sub
index sn                        eq
index uid                       eq
index displayName               eq
index mail                      eq
index uidNumber                 eq
index gidNumber                 eq
index memberUID                 eq
index entryCSN                  eq
index entryUUID                 eq
overlay syncprov
syncprov-sessionlog             128
```

14.2.4 /etc/openldap/ldap.conf

```
URI     ldaps://master.example.co.jp/ ldaps://slave.example.co.jp/
SIZELIMIT       0
TIMELIMIT       0
BASE dc=example,dc=co,dc=jp
TLS_CACERT /etc/openldap/cacerts/CA.pem
TLS_CACERTDIR /etc/openldap/cacerts
```

14.2.5 バックアップスクリプト

```
#!/bin/bash
sedai=2
DATE=$(date +'%Y%m%d')
if [ ! -d /opt/samba-ldap_backup ]; then
        mkdir /opt/samba-ldap_backup
```

```
fi
slapd_conf="/etc/openldap/slapd.conf"
smbldap_bind_conf="/etc/smbldap-tools/smbldap_bind.conf"
ldap_bind_dn="`sed -n 's/^rootdn[ \t]*\("\)*\([^"]*[^ \t"]\).*$/\2/p' "$slapd_conf"`"
ldap_bind_secret="`sed -n 's/^masterPw=[ \t]*\("\)*\([^"]*[^ \t"]\).*$/\2/p'
"$smbldap_bind_conf"`"
ldap_uri="`sed -n 's/^updateref[ \t]*\("\)*\([^"]*[^ \t"]\).*$/\2/p' "$slapd_conf"`"
if [ x"$ldap_uri" = x"" ]; then
    ldap_uri="ldap://127.0.0.1"
fi
ldapsearch \
    -LLL \
    -H "$ldap_uri" \
    -x -D "$ldap_bind_dn" -w "$ldap_bind_secret" \
> /opt/samba-ldap_backup/$DATE.ldif
st=$?
if [ $st != 0 ]; then
        echo "" >> /var/log/messages
        echo "######$DATE BACKUP ERROR#####" >> /var/log/messages
        echo "" >> /var/log/messages
        exit
fi
ldif=$(ls /opt/samba-ldap_backup/*ldif | wc | awk '{print $1}')
count=$sedai
while [ $ldif -gt $count ];
do
        delfile=$(ls /opt/samba-ldap_backup/*ldif | sort -n )
        delfile=$(echo $delfile | awk '{print $1}')
        /bin/rm -f $delfile
        let count=count+1
done
exit 0
```

14.3 slave.example.co.jp

14.3.1 /etc/smbldap-tools/smbldap.conf

```
SID="S-1-5-21-2888749833-2609368007-2065259343"
```

```
sambaDomain="LDAPTEST"
slaveLDAP="slave.example.co.jp"
slavePort="389"
masterLDAP="master.example.co.jp"
masterPort="389"
ldapTLS="1"
verify="require"
cafile="/etc/openldap/cacerts/CA.pem"
clientcert=""
clientkey=""
suffix="dc=example,dc=co,dc=jp"
usersdn="ou=Users,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
hash_encrypt="SSHA"
crypt_salt_format="%s"
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"
userSmbHome="\\PDC-SRV\%U"
userProfile="\\PDC-SRV\profiles\%U"
userHomeDrive="H:"
userScript="logon.bat"
mailDomain="example.co.jp"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

```
encoding="UTF-8"
OracleSES="0"
```

14.3.2 /etc/ldap.conf

```
base dc=example,dc=co,dc=jp
uri ldap://slave.example.co.jp/ ldap://master.example.co.jp/
ldap_version 3
timelimit 30
bind_timelimit 5
bind_policy soft
idle_timelimit 5
pam_password md5
tls_cacertfile /etc/openldap/cacerts/CA.pem
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
```

14.3.3 /etc/openldap/slapd.conf

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/samba.schema
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
threads 16
loglevel 256
timelimit 30
idletimeout 10
sizelimit unlimited
TLSCACertificateFile /etc/openldap/cacerts/CA.pem
TLSCertificateFile /etc/openldap/cacerts/slave.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/slave.example.co.jp.key
access to *
        by dn="cn=Manager,dc=example,dc=co,dc=jp" write
        by * break
```

```
access to attrs=userPassword
        by anonymous auth
        by * none
access to *
        by * read
database        bdb
suffix          "dc=example,dc=co,dc=jp"
rootdn          "cn=Manager,dc=example,dc=co,dc=jp"
rootpw master-pass（設定当初必要、後に削除）
directory       /var/lib/ldap
mode 0640
lastmod on
checkpoint 512 5
cachesize 500
idlcachesize 1000
dbconfig set_cachesize 0 8388608 0
dbconfig set_lk_max_objects 5000
dbconfig set_lk_max_locks 5000
dbconfig set_lk_max_lockers 5000
dbconfig set_flags DB_LOG_AUTOREMOVE
dbconfig set_lg_regionmax 1048576
dbconfig set_lg_max 104857600
dbconfig set_lg_bsize 20971520
index objectClass               eq
index ou                        eq
index cn                        eq,sub
index sn                        eq
index uid                       eq
index displayName               eq
index mail                      eq
index uidNumber                 eq
index gidNumber                 eq
index memberUID                 eq
index entryCSN                  eq
index entryUUID                 eq
syncrepl rid=1
```

```
        provider="ldaps://master.example.co.jp/"
        type=refreshAndPersist
        retry="5 10 30 +"
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials=secret
updateref "ldaps://master.example.co.jp/"
```

14.3.4 /etc/openldap/ldap.conf

```
URI     ldaps://slave.example.co.jp/ ldaps://master.example.co.jp/
SIZELIMIT       0
TIMELIMIT       0
BASE dc=example,dc=co,dc=jp
TLS_CACERT /etc/openldap/cacerts/CA.pem
TLS_CACERTDIR /etc/openldap/cacerts
```