OpenLDAP 運用ガイド

更新日: 2012 年 4 月 10 日

作成日: 2012 年 3 月 27 日

リビジョン: 1.0

目次

1. はじめに 1

2. LDAP サーバー構成設計 2
- 2.1 基本構成 2
- 2.2 マルチマスター構成 2

3. 構築前の準備 4
- 3.1 対象環境 4
- 3.2 設定パラメーター 4
  - 3.2.1 LDAP base suffix 4
  - 3.2.2 LDAP 管理者、複製者 それぞれのパスワード 5

4. 認証サーバー環境の構築 (OpenLDAP) 6
- 4.1 マスターサーバー 1（ldap01）の設定 6
  - 4.1.1 /opt/osstech/etc/openldap/slapd.conf 6
- 4.2 マスターサーバー 2（ldap02）の設定 8
  - 4.2.1 /opt/osstech/etc/openldap/slapd.conf 8

5. OpenLDAP の TLS 設定 9
- 5.1 自己証明書の作成 9
- 5.2 証明書と秘密鍵の設定 (マスターサーバー 1) 11
- 5.3 証明書と秘密鍵の設定 (マスターサーバー 2) 12
- 5.4 slapd.conf の設定 12

6. チューニングパラメーター 14
- 6.1 索引設定 14
- 6.2 キャッシュ設定 14
- 6.3 BDB 設定 15
- 6.4 同時接続数 16

7. 初期データーの登録 17
  - 7.1.1 複製確認 18

8. LDAP クライアントの設定 20
- 8.1 RHEL 5 20
- 8.2 RHEL 6 23

9. ログの取得 28
- 9.1 syslog の設定 28
- 9.2 slapd.conf の loglevel 設定 28

10. LDAP 情報のバックアップ、リストア 30
- 10.1 バックアップ 30
- 10.2 LDAP データベースのリカバリー 30
- 10.3 LDAP 情報の復旧方法 31
  - 10.3.1 データ再同期による情報の復旧 31
  - 10.3.2 バックアップファイルによる情報の復旧 32

11. SLAMD によるパフォーマンス測定 33

11.1 環境 33
11.2 環境構築 33
11.2.1 SLAMD サーバーの設定 33
11.2.2 SLAMD クライアントの設定 35
11.3 SLAMD による測定 35
12. LDAP GUI クライアントの紹介 36
13. 各種設定ファイル 37
13.1 マスターサーバー 1、2 共通設定 37
13.1.1 /opt/osstech/etc/openldap/slapd.conf 37
13.2 LDAP クライアント設定（RHEL 5） 39
13.2.1 /etc/openldap/ldap.conf 39
13.2.2 /etc/ldap.conf 40
13.2.3 /etc/nsswitch.conf 40
13.2.4 /etc/pam.d/system-auth 40
13.3 LDAP クライアント設定（RHEL 6） 41
13.3.1 /etc/openldap/ldap.conf 41
13.3.2 /etc/pam_ldap.conf 41
13.3.3 /etc/nslcd.conf 41
13.3.4 /etc/nsswitch.conf 42
13.3.5 /etc/pam.d/system-auth 42

1. はじめに

本ドキュメントは、弊社提供の OpenLDAP パッケージ導入後の認証サーバー環境（マルチマスター構成）の運用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。

本ドキュメントに関する記載内容について、疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

また、本ドキュメントでは必要に応じて以下のような略語を使います。

- Red Hat Enterprise Linux5 を　RHEL5 と表記します。
- Red Hat Enterprise Linux6 を　RHEL6 と表記します。

2. LDAP サーバー構成設計

OpenLDAP を利用した LDAP マルチマスター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。

2.1 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。

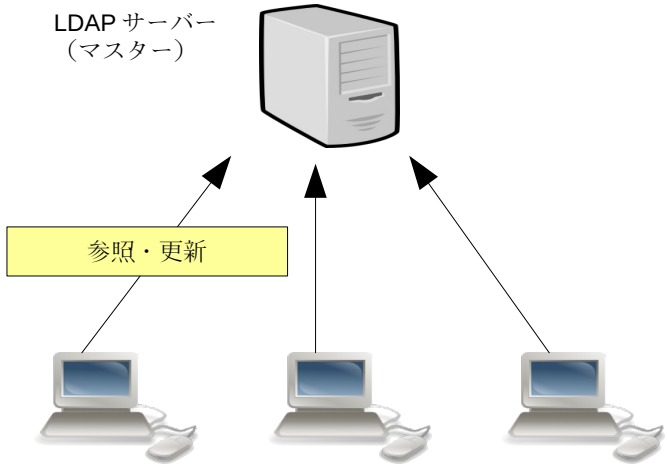


図 2.1.: 基本構成

2.2 マルチマスター構成

LDAP サーバーの冗長性をあげるために、マスター 2 台で構成する方法です。 2 台の LDAP サーバーがそれぞれマスタサーバーとして機能します。

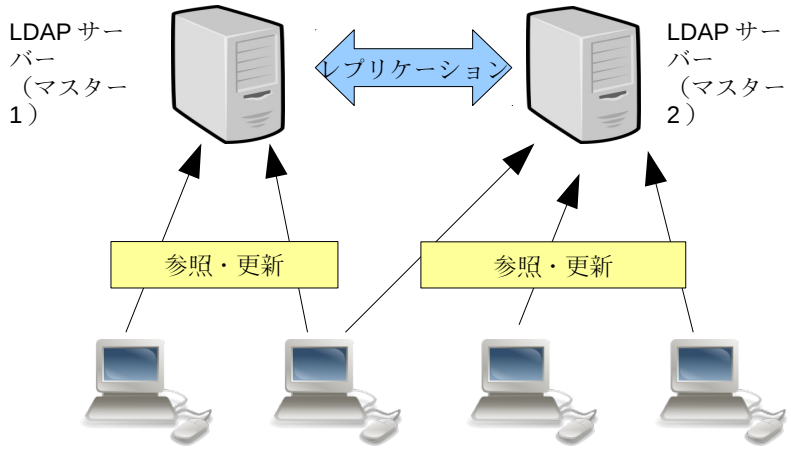


図 2.2.: マルチマスタ構成

3. 構築前の準備

3.1 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
  - RHEL 5 (x86/x86_64)　もしくは　RHEL 6 (x86_64)
    - SELinux
      - 無効
    - ファイアウォール
      - 無効

- ディレクトリサーバー
  - osstech-openldap-2.4

- マスターサーバー 1
  - ホスト名
    - ldap01.example.co.jp

- マスターサーバー 2
  - ホスト名
    - ldap02.example.co.jp

3.2 設定パラメーター

設定に入る前に以下のパラメーターを決定します。

3.2.1 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。

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

3.2.2 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。同様にマルチマスター構成で複製を行うユーザー、パスワードも決定します。

本書では以下のパラメーターを使って解説します。

パラメーター	解説例
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	replica-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）

4. 認証サーバー環境の構築 (OpenLDAP)

マスターサーバー間の LDAP エントリーの複製は 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ーなどについては以下のガイド等を参照ください。

- OpenLDAP2.4 管理者ガイド

  http://www.openldap.org/doc/admin24/index.html

- RHEL 5 導入ガイド

  http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/index.html

- RHEL 6 導入ガイド

  http://docs.redhat.com/docs/ja-JP/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/index.html

4.1 マスターサーバー 1（ldap01）の設定

まずマスターサーバー 1 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 /opt/osstech/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ーは以下となります。

- suffix　パラメーター

  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　パラメーター

  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　パラメーター

  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　パラメーター

  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 =wx
        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
```

- syncrepl　パラメーター

  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（複製対象エントリー）、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。

```
serverID 1 ldap://ldap01.example.co.jp/
serverID 2 ldap://ldap02.example.co.jp/

syncrepl rid=1
       provider=ldap://ldap01.example.co.jp/
       type=refreshAndPersist
       retry="5 10 30 +"
       keepalive=600:5:60
       searchbase="dc=example,dc=co,dc=jp"
       scope=sub
```

```
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"

syncrepl rid=2
        provider=ldap://ldap02.example.co.jp/
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=600:5:60
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"
```

- mirrormode　パラメーター

  マルチマスター(Active-Active)構成を有効にするために、mirrormode を設定します。

```
    mirrormode on
```

4.2 マスターサーバー 2（ldap02）の設定

次にもう 1 台の LDAP サーバー構築について解説します。

4.2.1 /opt/osstech/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。設定内容はマスターサーバー 1（ldap01）と全く同じです。

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 ldap01.example.co.jp.key \
-out ldap01.example.co.jp.pem \
-days 3650 \
-subj "/C=JP/ST=Tokyo/L=Shinagawa-ku/O=OSSTECH/OU=development/CN=ldap01.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 1 用の自己署名証明書ファイル ldap01.example.co.jp.pem、秘密鍵ファイル ldap01.example.co.jp.key が生成されます。

```
Generating a 2048 bit RSA private key
..............................+++
.....................................................................+++
writing new private key to 'ldap01.example.co.jp.key'
```

同様にして、マスターサーバー 2 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)をマスターサーバー 2 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 1 で実施して構いません）

```
# openssl req \
-x509 \
-newkey rsa:2048 \
-nodes \
-keyout ldap02.example.co.jp.key \
-out ldap02.example.co.jp.pem \
-days 3650 \
-subj "/C=JP/ST=Tokyo/L=Shinagawa-ku/O=OSSTECH/OU=development/CN=ldap02.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 ldap01.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 ldap01.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=ldap01.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 ldap01.example.co.jp.pem
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=JP, ST=Tokyo, L=Shinagawa-ku, O=OSSTECH, OU=development,
CN=ldap01.example.co.jp
        Validity
            Not Before: Feb 27 01:08:03 2012 GMT
            Not After : Mar 28 01:08:03 2012 GMT
        Subject: C=JP, ST=Tokyo, L=Shinagawa-ku, O=OSSTECH, OU=development,
CN=ldap01.example.co.jp
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            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 1)

マスターサーバー 1 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。マスターサーバー 2 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 ldap01.example.co.jp.pem  >> /etc/openldap/cacerts/CA.pem
# cat ldap02.example.co.jp.pem >> /etc/openldap/cacerts/CA.pem
# scp /etc/openldap/cacerts/CA.pem ldap02:/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 ldap01.example.co.jp.pem /etc/openldap/cacerts
```

```
# cp ldap01.example.co.jp.key /etc/openldap/private
```

/opt/osstech/etc/openldap/slapd.conf の
TLSCACertificateFile、TLSCertificateFile、TLSCertificateKeyFile パラメーターにマスターサーバー 1 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/ldap01.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/ldap01.example.co.jp.key
```

5.3 証明書と秘密鍵の設定 (マスターサーバー 2)

マスターサーバー 2 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 ldap01.example.co.jp.pem  >> /etc/openldap/cacerts/CA.pem
# cat ldap02.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 ldap02.example.co.jp.pem /etc/openldap/cacerts
# cp ldap02.example.co.jp.key /etc/openldap/private
```

/etc/openldap/slapd.conf の TLSCACertificateFile、TLSCertificateFile、TLSCertificateKeyFile パラメーター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/ldap02.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/lap02.example.co.jp.key
```

5.4 slapd.conf の設定

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　パラメーター

  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（複製対象エントリー）、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。

```
serverID 1 ldaps://ldap01.example.co.jp/     ← ldaps に変更
serverID 2 ldaps://ldap02.example.co.jp/     ← ldaps に変更

syncrepl rid=1
        provider=ldaps://ldap01.example.co.jp/     ← ldaps に変更
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=600:5:60
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"

syncrepl rid=2
        provider=ldaps://ldap02.example.co.jp/     ← ldaps に変更
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=600:5:60
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"
```

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。

- レプリケーションのための索引設定

```
index objectClass                       eq,pres
index entryCSN,entryUUID                eq
```

- その他の索引の設定例

```
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、エントリー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。

/opt/osstech/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。

```
# /opt/osstech/sbin/slapindex
```

slapindex コマンドを実行すると、/opt/osstech/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/opt/osstech/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 -hR ldap:ldap /opt/osstech/var/lib/ldap/*
```

6.2 キャッシュ設定

OpenLDAP の slapd は、LDAP のエントリー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 [エントリー数]
  - 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ー数を指定します。このキャッシュ内のエントリーは、利用時にエントリーの解析処理が不要なため、非常に高速に処理されます。
- idlcachesize [エントリー数]
  - 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ー数を指定します。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。RHEL 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 または 4096 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、
/opt/osstech/var/lib/sv/slapd/env/OPENFILELIMIT ファイルに設定する必要があります。

```
# echo '16384' >>/opt/osstech/var/lib/sv/slapd/env/OPENFILELIMIT
```

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. 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。

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: dc=example,dc=co,dc=jp
objectClass: dcObject
objectClass: organization
o: Example Corp.
dc: example

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 master-pass
  （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 osstech-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。

7.1.1 複製確認

ここまでで LDAP の基本設定が終了し、マスター 1、マスター 2 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 ldap01 > ldap01.ldif
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h ldap02 > ldap02.ldif
# diff -u ldap01.ldif ldap02.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/opt/osstech/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 osstech-ldap restart
```

- 接続確認

```
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -LLL -h ldap01
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -LLL -h ldap02
```

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 osstech-ldap on
```

以上でマルチマスター構成の認証サーバー構築は終了です。

8. 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。

8.1 RHEL 5

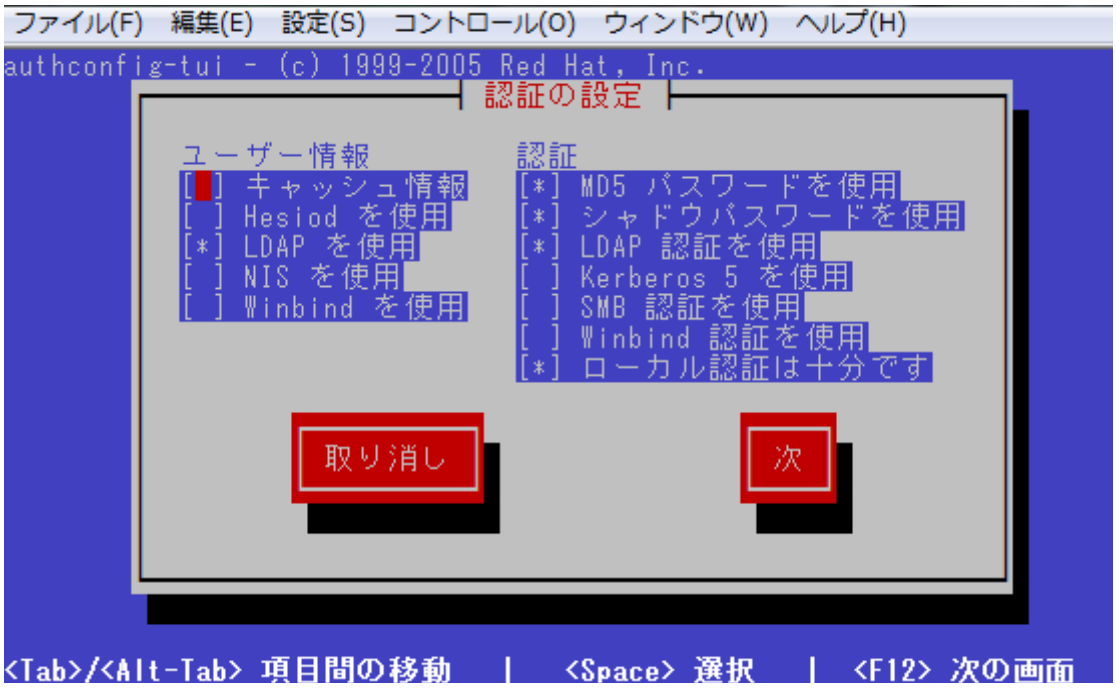
設定が必要なファイルは、次の 4 ファイルです。

- /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-tui コマンドを使用します。

```
# authconfig-tui
```

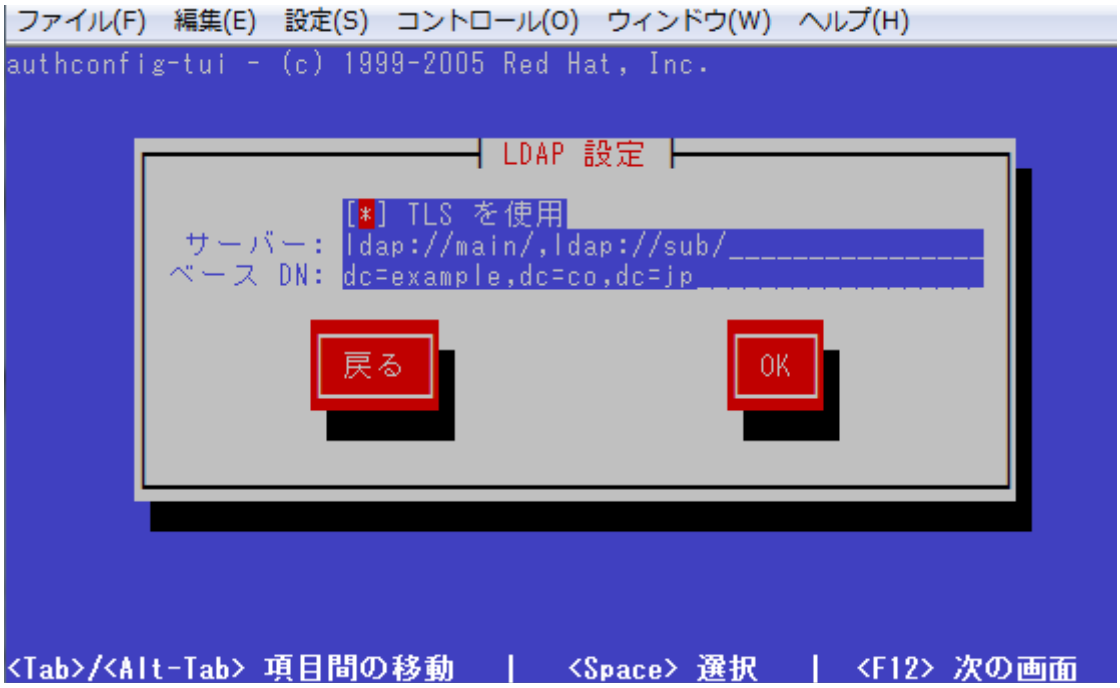
最初の画面で「ユーザー情報」の「LDAP を使用」、「認証」の「LDAP 認証を使用」、「ローカル認証は十分です」にチェックがあるか確認します。チェックがなければチェックをつけます。



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。

TLS を利用する場合、[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。　　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。



authconfig-tui コマンドを実行すると以下のパラメーターが設定されます。

- /etc/openldap/ldap.conf
  - URI　パラメーター

    LDAP サーバーの URI が設定されます。

    ```
    URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
    ```

  - BASE　パラメーター

    参照するベース DN が設定されます。

    ```
    BASE dc=example,dc=co,dc=jp
    ```

  - TLS_CACERTDIR　パラメーター

    デフォルトで参照する証明書ディレクトリが設定されます。

    ```
    TLS_CACERTDIR /etc/openldap/cacerts
    ```

- /etc/ldap.conf
  - uri　パラメーター

    LDAP サーバーの URI が設定されます。

    ```
    uri ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
    ```

- base　パラメーター

  参照するベース DN が設定されます。

  ```
  base dc=example,dc=co,dc=jp
  ```

- ssl　パラメーター

  [TLS を使用]にチェックを入れた場合に設定されます。

  ```
  ssl start_tls
  ```

8.2 RHEL 6

RHEL 6 では nss_ldap の代わりに、次の 2 つのモジュールが必要です。

- pam_ldap
- nss-pam-ldapd

また、nss-pam-ldapd で必要とされる次のパッケージも一緒にインストールします。

- nscd

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/pam_ldap.conf
  - pam_ldap モジュール用の設定ファイル
- /etc/nslcd.conf
  - nscd , nss-pam-ldapd 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-tui コマンドを使用します。

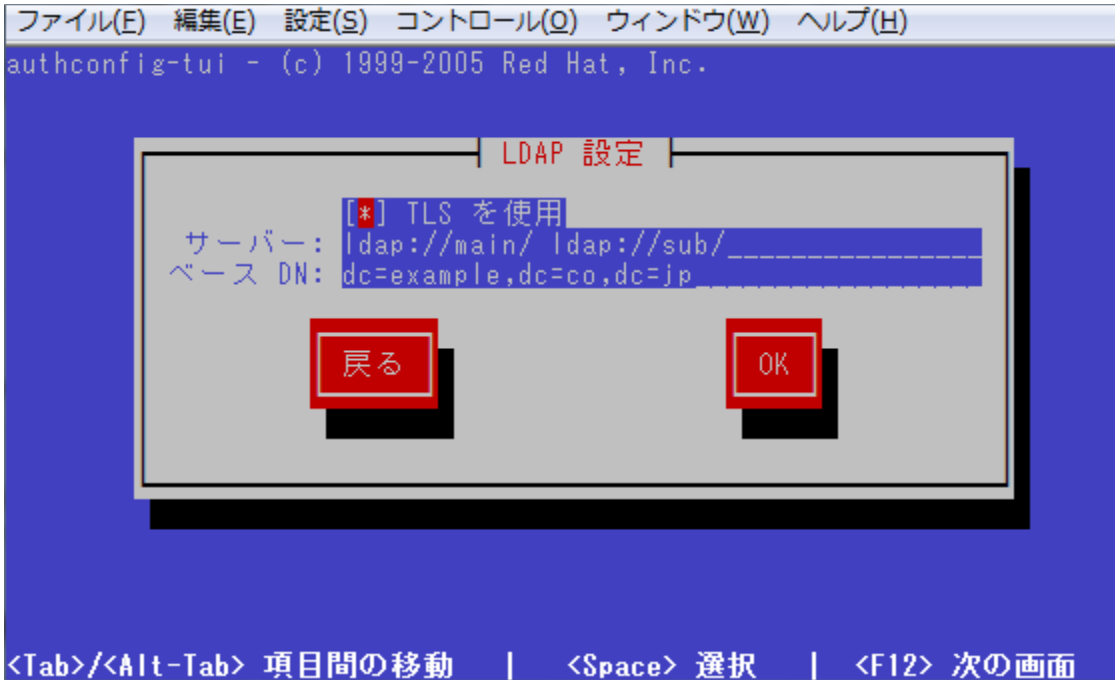
```
# authconfig-tui
```

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。

TLS を利用する場合、[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。　　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。



authconfig-tui コマンドを実行すると以下のパラメーターが設定されます。

- /etc/openldap/ldap.conf
  - URI　パラメーター

    LDAP サーバーの URI が設定されます。

    ```
    URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
    ```

  - BASE　パラメーター

    参照するベース DN が設定されます。

    ```
    BASE dc=example,dc=co,dc=jp
    ```

  - TLS_CACERTDIR　パラメーター

    デフォルトで参照する証明書ディレクトリが設定されます。

    ```
    TLS_CACERTDIR /etc/openldap/cacerts
    ```

- /etc/pam_ldap.conf
  - host　パラメーター

    ローカルホストの設定がコメントアウトされます。

    ```
    #host 127.0.0.1
    ```

- base　パラメーター

  参照するベース DN が設定されます。

  ```
  base dc=example,dc=co,dc=jp
  ```

- uri　パラメーター

  LDAP サーバーの URI が設定されます。

  ```
  URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
  ```

- tls_cacertdir　パラメーター

  デフォルトで参照する証明書ディレクトリが設定されます。

  ```
  tls_cacertdir /etc/openldap/cacerts
  ```

- ssl　パラメーター

  [TLS を使用]にチェックを入れた場合に設定されます。

  ```
  ssl start_tls
  ```

- pam_password　パラメーター

  [MD5　パスワードを使用]にチェックを入れた場合に設定されます。

  ```
  pas_password md5
  ```

- /etc/nslcd.conf
  - uri　パラメーター

    LDAP サーバーの URI が設定されます。

    ```
    URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
    ```

  - base　パラメーター

    参照するベース DN が設定されます。

    ```
    base dc=example,dc=co,dc=jp
    ```

  - ssl　パラメーター

    [TLS を使用]にチェックを入れた場合に設定されます。

    ```
    ssl start_tls
    ```

- tls_cacertdir　パラメーター

  デフォルトで参照する証明書ディレクトリが設定されます。

```
tls_cacertdir /etc/openldap/cacerts
```

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/rsyslog.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 rsyslog restart
```

9.2 slapd.conf の loglevel 設定

LDAP サーバーのログは、/opt/osstech/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ーのログ
1024 (0x400)	shell	shell バックエンドのログ
2048 (0x800)	parse	エントリー解析のログ
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製品付属のバックアップスクリプトで取得することができます。

- バックアップ対象
  - LDAP に登録されている全データ
- バックアップファイルの保存ディレクトリ
  - /var/backup/ldap
- バックアップファイル名
  - dc=example,dc=co,dc=jp.ldif.gz
- 保存ファイル数
  - 30 世代

LDAP の設定ファイルなどはバックアップ対象に含まれてませんので、必要に応じてバックアップを行って下さい。

このバックアップスクリプトはインストールの時に cron で毎朝 5 時半に実行されるよう設定されます。

- /etc/cron.d/slapdbbackup

  実行時間や頻度を変更したい場合は、この設定ファイルを変更して下さい。

```
30 5 * * * root test -x /opt/osstech/share/openldap/bin/slapdbbackup && /opt/oss
tech/bin/setuidgid -s ldap /opt/osstech/share/openldap/bin/slapdbbackup
```

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、両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。

```
# /opt/osstech/sbin/slapd_db_verify /opt/osstech/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。

```
# /opt/osstech/sbin/slapd_db_recover -v -h /opt/osstech/var/lib/ldap
```

インデックスを再構築します。

```
# /opt/osstech/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 -hR ldap:ldap /opt/osstech/var/lib/ldap
```

LDAP サーバーを起動します。

```
# /sbin/service osstech-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/opt/osstech/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以下の方法で復旧させてください。

10.3.1 データ再同期による情報の復旧

2 台のマスターサーバーどちらかに障害が発生し、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 osstech-ldap stop
# rm -f /opt/osstech/var/lib/ldap/*
# service osstech-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で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 ldap01 > ldap01.ldif
# ldapsearch -x -W -D “cn=Manager,dc=example,dc=co,dc=jp” -h ldap02 > ldap02.ldif
# diff -u ldap01.ldif ldap02.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。

LDAP データが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（データ量によります）。

10.3.2 バックアップファイルによる情報の復旧

両方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。

まず最初に、両サーバーの LDAP サービスを停止して下さい。

```
# service osstech-ldap stop
```

マスターサーバー 1 にて次の手順で LDAP データーの復旧を行います。

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（/var/backup/ldap/dc=example,dc=co,dc=jp.ldif)を利用します。

```
# rm -f /opt/osstech/var/lib/ldap/*
# /opt/osstech/sbin/slapadd -vwql /var/backup/ldap/dc=example,dc=co,dc=jp.ldif
# chown -hR ldap:ldap /opt/osstech/var/lib/ldap
# service osstech-ldap start
```

再構築し終わりましたら、マスターサーバー 2 も　10.3.1 データ再同期による情報の復旧　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-2.0.1
    - http://slamd.com/
- OpenLDAP サーバー
    - openldap-2.4.25-42

11.2 環境構築

11.2.1 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://www.oracle.com/technetwork/java/javase/downloads/index.html

```
# chmod 755 ./jdk-6u31-linux-x64-rpm.bin
# ./jdk-6u31-linux-x64-rpm.bin
```

SLAMD のサイトからダウンロードした slamd-2.0.1.zip を展開します。

```
# unzip slamd-2.0.1.zip
```

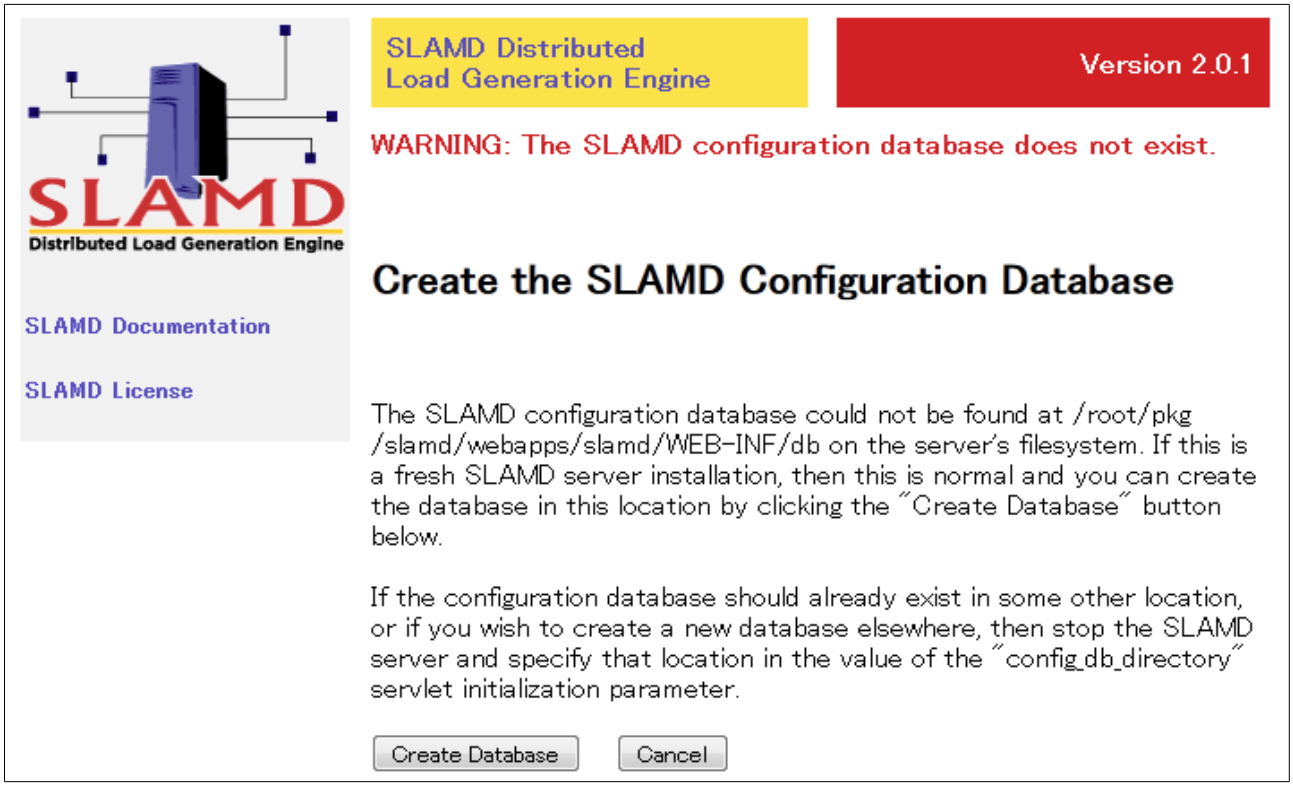
SLAMD サーバーを起動します。

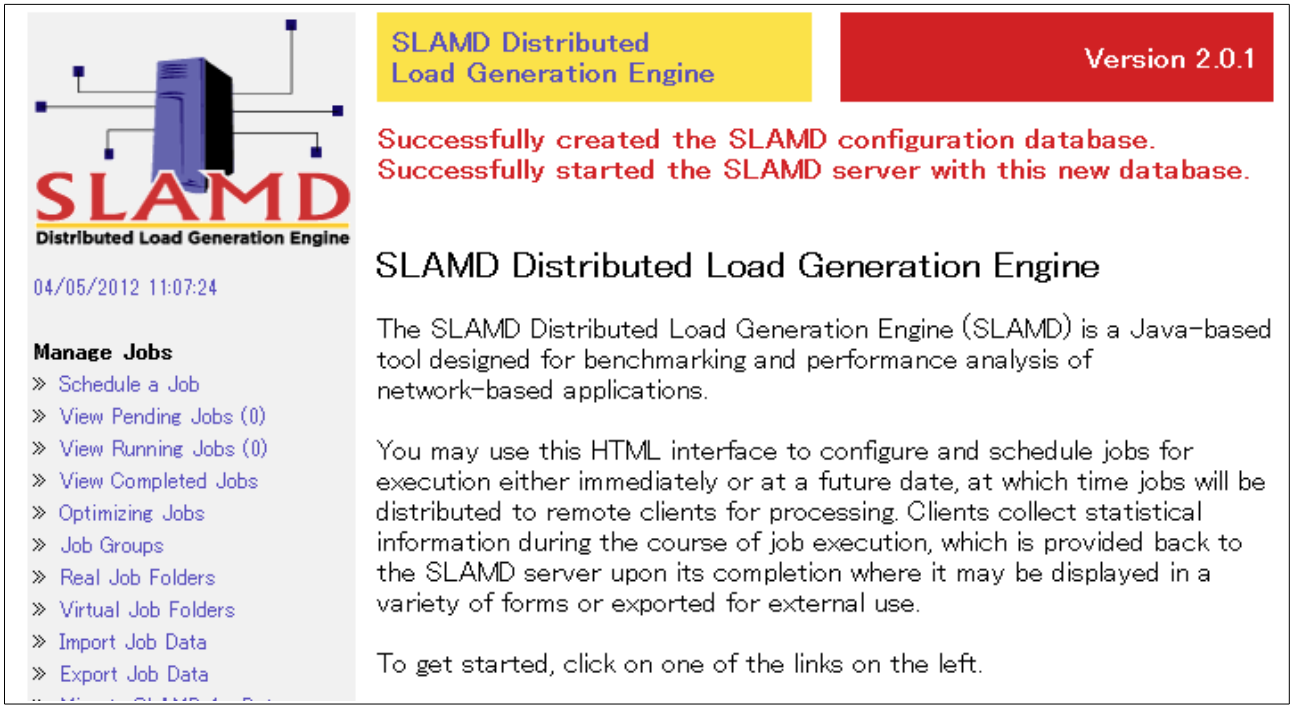
```
# cd slamd/bin
# ./startup.sh
```

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

「create database」のリンクをクリックして管理画面に移動します。





11.2.2 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-2.0.1.zip を展開したディレクトリに含まれている slamd_client-2.0.1.zip を展開します。

```
# cd slamd
# unzizp slamd_client-2.0.1.zip
```

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。

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 a 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 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.openchannelsoftware.com/projects/LDAP_Browser_Editor
- 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/
- Apache Directory Studio
  - Eclipse ベースの LDAP クライアント
  - http://directory.apache.org/studio/

13. 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。

13.1 マスターサーバー 1、2 共通設定

13.1.1 /opt/osstech/etc/openldap/slapd.conf

```
include         /opt/osstech/etc/openldap/schema/corba.schema
include         /opt/osstech/etc/openldap/schema/core.schema
include         /opt/osstech/etc/openldap/schema/cosine.schema
include         /opt/osstech/etc/openldap/schema/duaconf.schema
include         /opt/osstech/etc/openldap/schema/dyngroup.schema
include         /opt/osstech/etc/openldap/schema/inetorgperson.schema
include         /opt/osstech/etc/openldap/schema/java.schema
include         /opt/osstech/etc/openldap/schema/misc.schema
include         /opt/osstech/etc/openldap/schema/nis.schema
include         /opt/osstech/etc/openldap/schema/openldap.schema
include         /opt/osstech/etc/openldap/schema/ppolicy.schema
include         /opt/osstech/etc/openldap/schema/collective.schema

pidfile         /opt/osstech/var/run/openldap/slapd.pid
argsfile        /opt/osstech/var/run/openldap/slapd.args
loglevel 256
threads 4
tool-threads 4
timelimit 30
idletimeout 10
sizelimit unlimited
TLSCACertificateFile /etc/openldap/cacerts/CA.pem
TLSCertificateFile /etc/openldap/cacerts/ldap01.example.co.jp.pem
TLSCertificateKeyFile /etc/openldap/private/ldap01.example.co.jp.key
password-hash {SSHA}
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 =wx
        by * none
access to *
        by * read
modulepath /opt/osstech/lib64/openldap2.4
moduleload ppolicy
moduleload syncprov
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       /opt/osstech/var/lib/ldap
mode 0640
lastmod on
checkpoint 512 5
cachesize 500
idlcachesize 1500
dbconfig set_data_dir .
dbconfig set_lg_dir .
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,pres
index ou, sn, uid                eq
index cn                        eq,sub
index displayName, mail         eq
index uidNumber, gidNumber       eq
```

```
index entryCSN, entryUUID        eq
overlay syncprov
syncprov-sessionlog              128

serverID 1 ldaps://ldap01.example.co.jp/
serverID 2 ldaps://ldap02.example.co.jp/
syncrepl rid=1
        provider=ldaps://ldap01.example.co.jp/
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=600:5:60
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"
syncrepl rid=2
        provider=ldap://ldap02.example.co.jp/
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=600:5:60
        searchbase="dc=example,dc=co,dc=jp"
        scope=sub
        schemachecking=off
        binddn="cn=replica,dc=example,dc=co,dc=jp"
        bindmethod=simple
        credentials="replica-pass"
mirrormode on
```

13.2 LDAP クライアント設定（RHEL 5）

13.2.1 /etc/openldap/ldap.conf

```
URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
BASE dc=example,dc=co,dc=jp
```

```
TLS_CACERTDIR /etc/openldap/cacerts
```

13.2.2 /etc/ldap.conf

```
base dc=example,dc=co,dc=jp
uri ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
pam_password md5
```

13.2.3 /etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
hosts:      files dns
bootparams: nisplus [NOTFOUND=return] files
ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
netgroup:   files ldap
publickey:  nisplus
automount:  files ldap
aliases:    files nisplus
```

13.2.4 /etc/pam.d/system-auth

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
```

```
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
```

13.3 LDAP クライアント設定（RHEL 6）

13.3.1 /etc/openldap/ldap.conf

```
URI ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
BASE dc=example,dc=co,dc=jp
TLS_CACERTDIR /etc/openldap/cacerts
```

13.3.2 /etc/pam_ldap.conf

```
base dc=example,dc=co,dc=jp
uri ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
pam_password md5
```

13.3.3 /etc/nslcd.conf

```
uri ldaps://ldap01.example.co.jp/ ldaps://ldap02.example.co.jp/
base dc=example,dc=co,dc=jp
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
```

13.3.4 /etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
hosts:      files dns
bootparams: nisplus [NOTFOUND=return] files
ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
netgroup:   files ldap
publickey:  nisplus
automount:  files ldap
aliases:    files nisplus
```

13.3.5 /etc/pam.d/system-auth

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
```

```
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
```