OSSTech OpenLDAP 2.4 インストールガイド

オープンソース・ソリューション・テクノロジ (株)

更新日　　2021 年 12 月 24 日

目次

1 はじめに

本ドキュメントは、弊社提供の OpenLDAP パッケージを導入・設定するための手順書です。

OpenLDAP パッケージのインストール・設定の際に、必ず本ドキュメントの内容を確認してから、作業を実施してください。

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、サポート ID を記載いただいたうえで、弊社サポート窓口までお問い合わせください。

2 OpenLDAP 2.4 パッケージのインストール

2.1 システム要件

2.1.1 ソフトウェア要件

以下のいずれかの OS 環境が必要です。

- Red Hat Enterprise Linux 8.0 (x86-64) 以降
- Red Hat Enterprise Linux 7.2 (x86-64) 以降
- CentOS 8.0 (x86-64) 以降
- CentOS 7.2 (x86-64) 以降
- Amazon Linux 2 (x86-64)
- AlmaLinux 8 (x86-64)
- Rocky Linux 8 (x86-64)

2.1.2 ハードウェア要件

ソフトウェア要件に記載の OS が動作する以下のハードウェア環境が必要です。

- CPU: AMD64, Intel 64 (x86-64) および互換 CPU
- メモリ: 4GB 以上 (8GB 以上推奨、登録する LDAP エントリー数等に依存)
- ディスク
  - ソフトウェア: /opt/osstech 配下 1GB 以上
  - データ : /var/opt/osstech 配下 1GB 以上推奨 (データ数に依存)
  - ログ : /var/log/osstech 配下 10GB 以上推奨 (ログ保存量に依存)

2.2 パッケージ構成

OSSTech 版 OpenLDAP パッケージは、以下のパッケージにより構成されています。

- OSSTech ソフトウェア製品基本パッケージ
  - osstech-base
  - osstech-support
- OpenLDAP 2.4 パッケージ
  - osstech-openldap
  - osstech-openldap-clients
  - osstech-openldap-servers

  - osstech-openldap2.4-libs
  - osstech-openldap-python-scripts
  - osstech-openldap-servers-perl
- Berkeley DB パッケージ (RHEL8 環境では含まれません)
  - osstech-db5.3
  - osstech-db5.3-utils

2.3 Red Hat Enterprise Linux 版パッケージのインストール

以下の OS 環境でのパッケージのインストール方法について記載します。

- Red Hat Enterprise Linux 8 / CentOS 8 / AlmaLinux 8 / Rocky Linux 8
- Red Hat Enterprise Linux 7 / CentOS 7
- Amazon Linux 2

2.3.1 準備

パッケージのインストールは root ユーザーのみに許可されています。su コマンド、もしくは、sudo コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（画面には表示されません）
```

続いて、OpenLDAP パッケージ一式をインストール先ホストの任意のディレクトリに展開します。

本ドキュメントの実行例では、 /srv/osstech/software/RPMS に展開したことを前提として記述します。

2.3.2 依存パッケージ

弊社提供の OpenLDAP 2.4 で必要とされる OS 同梱パッケージは、以下となります。

- ksh
- libtool-ltdl
- openssl
- python3
- perl
- lz4

osstech-openldap-python-scripts パッケージをインストールする際には python3 パッケージも追加で必要となります。

- osstech-openldap-python-scripts パッケージには OpenLDAP のログの各リクエストの経過時間等を JSON 形式に変換する slapdstatslog2json スクリプトなどが含まれます。

2.3.3 パッケージのインストール

弊社提供の OpenLDAP 2.4 パッケージは /opt/osstech ディレクトリ配下に新規インストールされます。

/srv/osstech/software/RPMS に弊社提供のパッケージ一式がコピーされていることを確認します。

```
# cd /srv/osstech/software/RPMS
# tar xfz osstech-openldap-2.4.58-176.el8.tar.gz
# cd osstech-openldap-2.4.58-176.el8
# ls
doc  install.sh  x86_64
```

install.sh コマンドを実行することで、インストールに必要な依存パッケージのダウンロード、インストール、および、弊社 OpenLDAP パッケージ一式がインストールされます。依存パッケージは、通常 OS で設定されている yum レポジトリからネットワーク経由で取得しますが、yum コマンドでパッケージの取得ができないサーバー環境の場合、事前に OS メディア等で依存パッケージを入手し、rpm コマンドで依存パッケージのインストールを完了しておいてください。

```
# ./install.sh
```

install.sh コマンドを実行すると、インストール処理が実行され、依存パッケージ、および OpenLDAP パッケージのインストールが行われます。

以下の出力が得られれば、パッケージのインストールは完了です。

```
完了しました! (もしくは Complete!)
```

以上で、 OpenLDAP 2.4 パッケージのインストールは完了です。

3 OpenLDAP 2.4 パッケージのアップデート

パッケージのアップデート作業は root ユーザーで行ないます。

```
$ su -
Password: root のパスワードを入力（画面には表示されません）
```

パッケージのアップデート前に OpenLDAP の各種設定ファイルのバックアップを行ないます。cp コマンドなどでファイルのバックアップを取得してください。

バックアップ対象ディレクトリ	ディレクトリに含まれるデータ
/opt/osstech/etc/openldap	OpenLDAP の設定ファイル、スキーマファイルなど

3.1 シングル構成時アップデート手順

1 台構成の OpenLDAP サーバーをアップデートする時は、下記の手順で実施してください。

OpenLDAP サービスを停止します。

```
# systemctl stop osstech-slapd
```

slapcat コマンドを利用して、登録されている LDAP エントリーの LDIF 形式のバックアップを取得します。「-l」オプションにファイル名を指定することで、バックアップファイルの名前を指定することができます。

```
# sudo -u ldap /opt/osstech/sbin/slapcat -l backup-20210601.ldif
```

続いて、弊社提供の更新版の OpenLDAP パッケージ一式をインストール先ホストの任意のディレクトリに展開します。本ドキュメントでは/srv/osstech/software/RPMS 配下に展開する前提で説明します。

```
# cd /srv/osstech/software/RPMS
# tar xfz osstech-openldap-2.4.58-176.el8.tar.gz
# cd osstech-openldap-2.4.58-176.el8
# ls
doc  install.sh  x86_64
```

展開されたディレクトリに含まれる install.sh コマンドにて、弊社パッケージのアップデートを行うことができます。

また、必要に応じて、依存パッケージのインストールも実施します。(依存パッケージは yum レポジトリより取得します。)

もし、アップデート対象のサーバーが yum コマンドでパッケージを取得できない環境の場合、事前に OS メディア等で依存パッケージを入手し、rpm コマンドなどでサーバーにインストールを行ってください。

```
# ./install.sh
```

install.sh コマンドを実行すると、インストール処理が実行され、依存パッケージ、および OpenLDAP パッケージのインストールが行われます。

以下の出力が得られればパッケージのアップデートは完了です。

```
完了しました! (もしくは Complete!)
```

OpenLDAP サービスを起動します。

```
# systemctl start osstech-slapd
```

以上でアップデートは終了です。

3.2 マルチマスター構成時アップデート手順

2 台以上のマルチマスター構成時の OpenLDAP 2.4 パッケージのアップデート手順は次の手順で実施してください。

本ドキュメントでは、2 台のマルチマスター構成の OpenLDAP サーバーを例に記載します。LDAP 1 号機のホスト名を ldap1、LDAP 2 号機のホスト名を ldap2 として説明します。

3.2.1 LDAP 1 号機のアップデート手順

ldap1 の OpenLDAP サービスを停止します。

```
[root@ldap1]# systemctl stop osstech-slapd
```

slapcat コマンドを利用して、登録されている LDAP エントリーの LDIF 形式のバックアップを取得します。「-l」オプションにファイル名を指定することで、バックアップファイルの名前を指定することができます。

```
[root@ldap1]# sudo -u ldap /opt/osstech/sbin/slapcat -l backup-20210601.ldif
```

続いて、弊社提供の更新版の OpenLDAP パッケージ一式をインストール先ホストの任意のディレクトリに展開します。本ドキュメントでは/srv/osstech/software/RPMS 配下に展開する前提で説明します。

```
[root@ldap1]# cd /srv/osstech/software/RPMS
[root@ldap1]# tar xfz osstech-openldap-2.4.58-176.el8.tar.gz
[root@ldap1]# cd osstech-openldap-2.4.58-176.el8
# ls
doc  install.sh  x86_64
```

展開されたディレクトリに含まれる install.sh コマンドにて、弊社パッケージのアップデートを行うことができます。

また、必要に応じて、依存パッケージのインストールも実施します。(依存パッケージは yum レポジトリより取得します。)

もし、アップデート対象のサーバーが yum コマンドでパッケージを取得できない環境の場合、事前に OS メディア等で依存パッケージを入手し、rpm コマンドなどでサーバーにインストールを行ってください。

```
[root@ldap1]# ./install.sh
```

install.sh コマンドを実行すると、インストール処理が実行され、依存パッケージ、および OpenLDAP パッケージのインストールが行われます。

以下の出力が得られれば、LDAP 1 号機のパッケージのアップデートは完了です。

```
完了しました! (もしくは Complete!)
```

OpenLDAP サービスを起動します。

```
[root@ldap1]# systemctl start osstech-slapd
```

LDAP 1 号機のアップデートの完了後、LDAP の同期確認を行ないます。 LDAP 1 号機と、LDAP 2 号機で、contextCSN が同じ値になっていることを確認します。

```
[root@ldap1]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D <管理者 DN> \
  -b <ルート suffix> \
  -s base \
  contextCSN \
;
contextCSN: 20200925023414.129432Z#000000#001#000000

[root@ldap2]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
```

```
  -D <管理者 DN> \
  -b <ルート suffix> \
  -s base \
  contextCSN \
;
contextCSN: 20200925023414.129432Z#000000#001#000000
```

contextCSN の値が同じであれば、同期に問題はありませんので、続いて LDAP 2 号機のアップデート作業を行ないます。

3.2.2 LDAP 2 号機のアップデート手順

ldap2 の OpenLDAP サービスを停止します。

```
[root@ldap2]# systemctl stop osstech-slapd
```

続いて、弊社提供の更新版の OpenLDAP パッケージ一式をインストール先ホストの任意のディレクトリに展開します。本ドキュメントでは/srv/osstech/software/RPMS 配下に展開する前提で説明します。

```
[root@ldap2]# cd /srv/osstech/software/RPMS
[root@ldap2]# tar xfz osstech-openldap-2.4.58-176.el8.tar.gz
[root@ldap2]# cd osstech-openldap-2.4.58-176.el8
[root@ldap2]# ls
doc  install.sh  x86_64
```

展開されたディレクトリに含まれる install.sh コマンドにて、弊社パッケージのアップデートを行うことができます。

また、必要に応じて、依存パッケージのインストールも実施します。(依存パッケージは yum レポジトリより取得します。)

もし、アップデート対象のサーバーが yum コマンドでパッケージを取得できない環境の場合、事前に OS メディア等で依存パッケージを入手し、rpm コマンドなどでサーバーにインストールを行ってください。

```
[root@ldap2]# ./install.sh
```

install.sh コマンドを実行すると、インストール処理が実行され、依存パッケージ、および OpenLDAP パッケージのインストールが行われます。

以下の出力が得られれば、LDAP 2 号機のパッケージのアップデートは完了です。

```
完了しました！（もしくは Complete!）
```

OpenLDAP サービスを起動します。

```
[root@ldap2]# systemctl start osstech-slapd
```

LDAP 2 号機のアップデートの完了後、LDAP の同期確認を行ないます。 LDAP 1 号機と、LDAP 2 号機で、contextCSN が同じ値になっていることを確認します。

```
[root@ldap1]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D <管理者 DN> \
  -b <ルート suffix> \
  -s base \
  contextCSN \
;
contextCSN: 20200925023414.129432Z#000000#001#000000
```

```
[root@ldap2]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D <管理者 DN> \
  -b <ルート suffix> \
  -s base \
  contextCSN \
;
contextCSN: 20200925023414.129432Z#000000#001#000000
```

contextCSN の値が同じであれば、同期に問題はありませんので、アップデート作業は完了です。

3.3 パッケージアップデート時の切り戻し

パッケージをアップデート後、何からの理由で以前のバージョンに戻したい場合、次の手順で行ないます。

以前のパッケージ一式を展開したディレクトリ内の x86_64 ディレクトリに移動します。

```
[root@ldap]# cd /srv/osstech/software/RPMS
[root@ldap]# tar xfz osstech-openldap-2.4.58-171.el8.tar.gz
[root@ldap]# cd osstech-openldap-2.4.58-171.el8
[root@ldap]# ls
doc  install.sh  x86_64
[root@ldap]# cd x86_64
```

現在インストール済みの OpenLDAP パッケージを確認します。

```
[root@ldap]# rpm -qa |grep osstech-openldap
osstech-openldap-2.4.58-176.el8.x86_64
osstech-openldap2.4-libs-2.4.58-176.el8.x86_64
osstech-openldap-servers-2.4.58-176.el8.x86_64
osstech-openldap-clients-2.4.58-176.el8.x86_64
```

以前のパッケージのうち、インストール済みのパッケージの古いバージョンを指定して、rpm コマンドの–oldpackage オプションを付けてインストールを行ないます。

```
[root@ldap]# rpm -Uhv --oldpackage \
osstech-openldap-2.4.58-172.el8.x86_64.rpm \
osstech-openldap2.4-libs-2.4.58-172.el8.x86_64.rpm \
osstech-openldap-servers-2.4.58-172.el8.x86_64.rpm \
osstech-openldap-clients-2.4.58-172.el8.x86_64.rpm
```

パッケージのインストール完了後、osstech-slapd サービスの再起動を行ない、サービスが正常稼働することを確認します。

```
[root@ldap]# systemctl restart osstech-slapd
```

4 OpenLDAP 2.4 パッケージの構成

弊社製 OpenLDAP 2.4 パッケージは/opt/osstech ディレクトリ配下にインストールされます。

分類	ファイル
LDAP デーモン	/opt/osstech/sbin/slapd
LDAP クライアントユーティリティ	/opt/osstech/bin/ldapsearch など
管理者用 LDAP ユーティリティ	/opt/osstech/sbin/slapadd など
OpenLDAP サーバー設定ファイル	/opt/osstech/etc/openldap/slapd.conf
OpenLDAP クライアント設定ファイル	/opt/osstech/etc/openldap/ldap.conf
スキーマファイル	/opt/osstech/etc/openldap/schema 配下
LDAP データ格納ディレクトリ	/opt/osstech/var/lib/ldap
LDAP バックアップ設定	/opt/osstech/etc/openldap/slapdbbackup.conf
ログ設定	/opt/osstech/etc/rsyslog.d/slapd.conf
ログローテート設定	/opt/osstech/etc/logrotate.d/syslog
BDB ユーティリティ	/opt/osstech/sbin/slapd_db_recover など

5 LDAP サーバー構築の事前準備

5.1 LDAP サーバー構成

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。

認証サービスとしての利用の場合、冗長性を考慮して、2 台のマルチマスター構成を推奨します。

5.1.1 スタンドアロン構成

OpenLDAP が 1 台だけの基本構成です。1 台でデータの更新・参照を全て受け持ちます。冗長性がありませんので、障害時やシステムのアップデート時などに LDAP サービスを停止する状況が生じます。

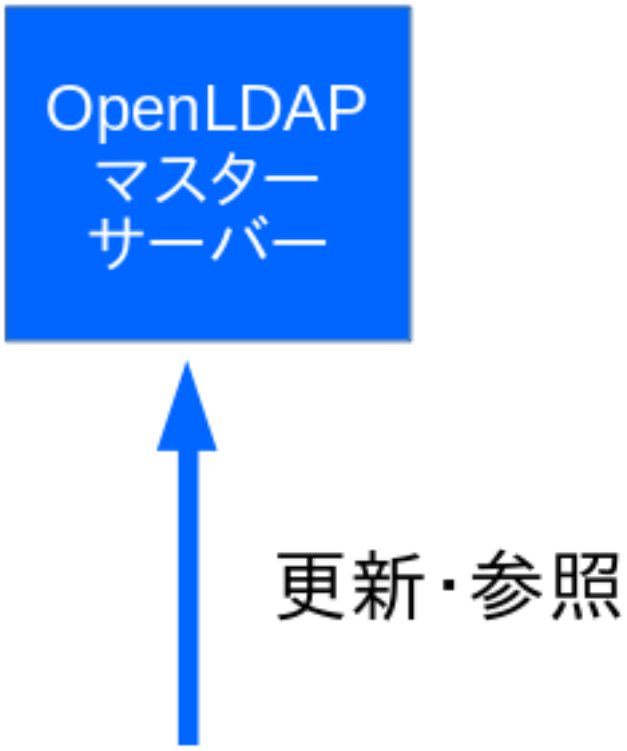

図 1　LDAP サーバー スタンドアロン構成

5.1.2 マルチマスター構成

LDAP サーバーの冗長性を向上させるため、複数の LDAP サーバーを用意して、LDAP データを双方向に複製 (レプリケーション) する構成です。2 台の OpenLDAP サーバーがそれぞれマスターサーバーとして機能します。

障害時の接続先切替の自動化のため、ロードバランサと組み合わせて構成することで高い冗長性を確保することが可能です。

注意: LDAP に対する更新処理は、どちらか一方のマスターサーバーに対してのみ行う構成とすることを推奨します。同一エントリに対して同時に複数台のサーバーに更新が行われると、いずれかの更新内容が欠落する可能性があります。

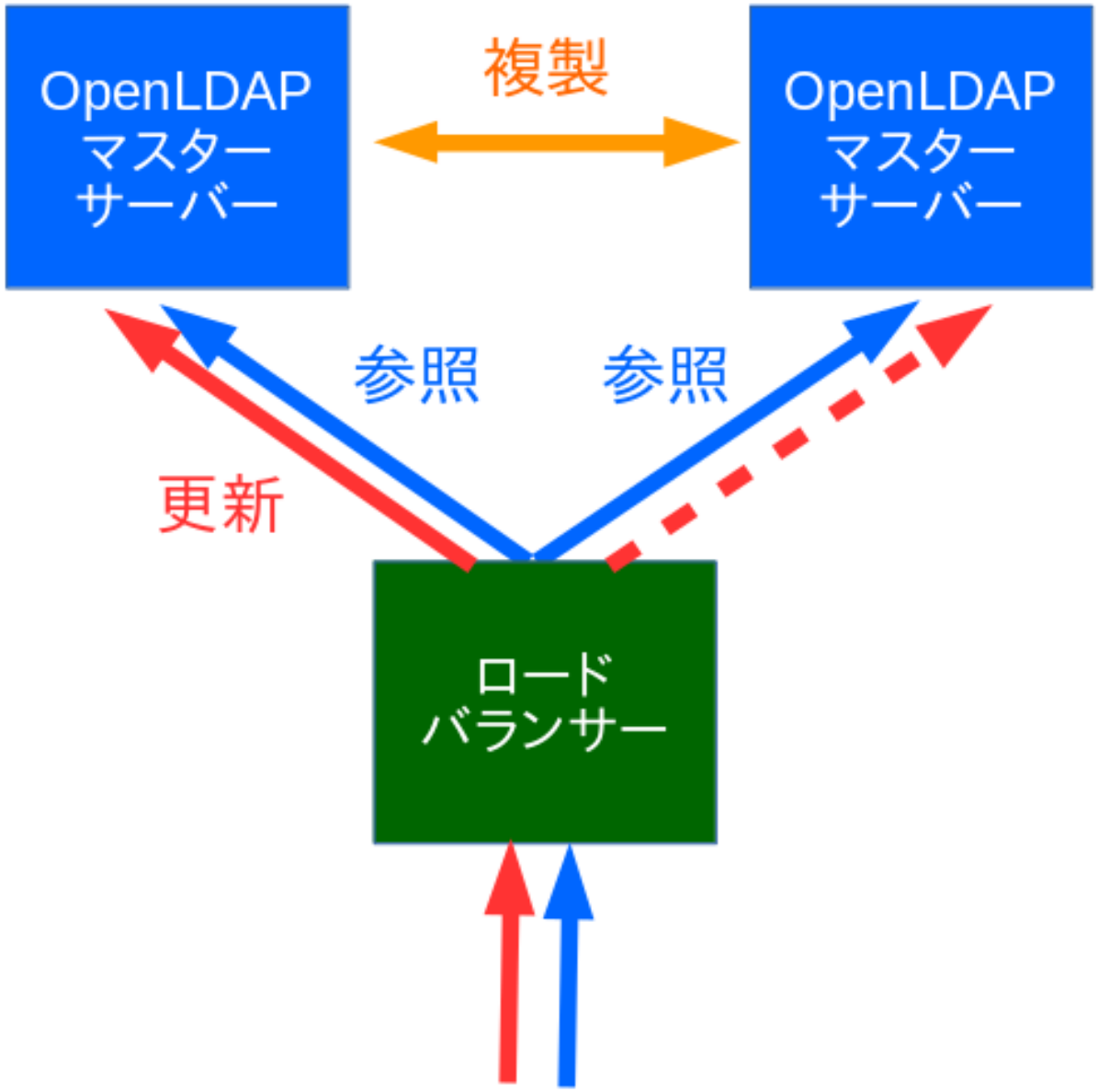

図 2　LDAP サーバー マルチマスター構成

5.1.3 マスター・スレーブ構成

データの更新・参照が可能な LDAP マスターサーバーと、参照のみが可能な LDAP スレーブサーバーを組み合わせて構成します。LDAP スレーブサーバーは負荷に合わせて台数を増やすことで、システム全体の参照性能の向上に繋がります。

- LDAP マスターサーバーは、LDAP プロバイダーサーバーと呼ばれることもあります。
- LDAP スレーブサーバーは、LDAP コンシューマーサーバーと呼ばれることもあります。

LDAP マスターサーバーをマルチマスターで構成し、必要に応じて LDAP スレーブサーバーを追加することで、更新系の冗長化と、参照系のスケールアウトに対応します。

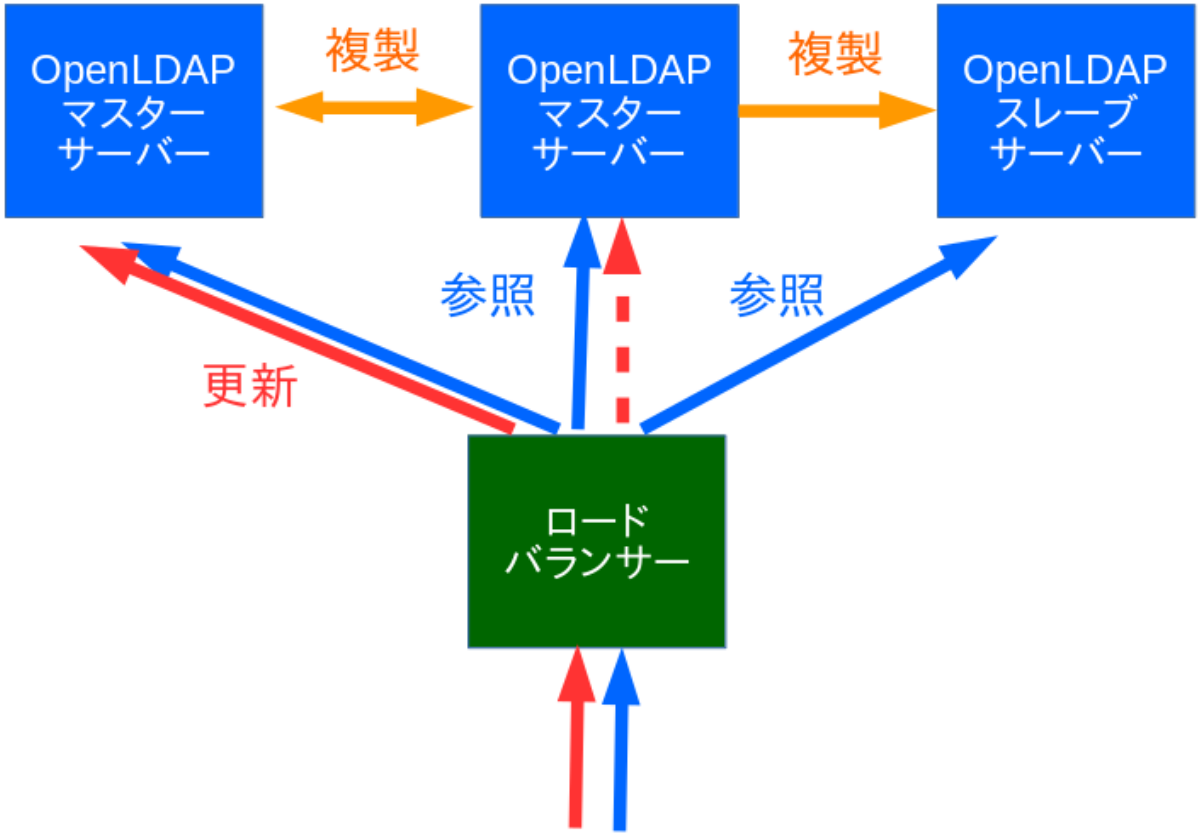

図 3　LDAP サーバー マスター・スレーブ構成

5.2 対象環境

本ドキュメントの想定する LDAP サーバーの構築環境は次の通りです。

- OS
  - Red Hat Enterprise Linux 8 / CentOS 8 / AlmaLinux 8 (x86-64)
  - Red Hat Enterprise Linux 7 / CentOS 7 (x86-64)
- ソフトウェア
  - OSSTech 版 OpenLDAP 2.4
- ホスト名
  - LDAP 1 号機: ldap1.example.com
  - LDAP 2 号機: ldap2.example.com

2 台の LDAP サーバーによるマルチマスター構成で構築します。

5.3 基本設計パラメーター

構築作業を行う前に、以下のパラメーターを決定します。

5.3.1 LDAP DIT サフィックス

LDAP DIT のサフィックス (ベース DN) を決定します。これは管理者が任意に設定することができますが、一般的には組織の DNS ドメイン名を分解し、「dc=」とカンマ「,」で区切った名前を使用します。

「dc」とは、「Domain Component」を意味しています。

- 例
  - 組織の DNS ドメイン名: example.com
  - LDAP DIT サフィックス: dc=example,dc=com

5.3.2 LDAP 管理者/複製処理用パスワード

OpenLDAP サーバーの各種処理を実行するための LDAP エントリとそのパスワードを決定します。本ドキュメントでは、以下のパラメーターを使って説明します。

パラメーター	設定例
LDAP DIT サフィックスの DN	dc=example,dc=com
LDAP 管理者エントリの DN	cn=admin,dc=example,dc=com
LDAP 管理者エントリのパスワード	admin-pass ※ 1
LDAP 複製処理用エントリの DN	cn=replica,dc=example,dc=com
LDAP 複製処理用エントリのパスワード	replica-pass ※ 1

※ 1:運用システムでは、十分安全なパスワードを選択してください

6 LDAP サーバー環境の構築

本ドキュメントでは、次の要件の LDAP サーバーを構成します。

- LDAP(389/TCP)、および LDAPS(636/TCP) によるサービス提供
- syncrepl 方式による LDAP データの複製

6.1 OS 環境の設定

各 LDAP サーバーで、下記の OS 環境の設定を行ないます。

6.1.1 時刻同期の設定

OpenLDAP のエントリの管理は時刻を利用します。LDAP サーバーの時刻については NTP による時刻合わせを実施してください。

Red Hat Enterprise Linux (CentOS) では、chrony もしくは、ntpd による時刻同期の設定を行ってください。

6.1.2 ファイアウォールの設定

外部から LDAP サーバーへの通信を許可するため、LDAP 用のポート設定を行ないます。下記は、外部から LDAP(389/TCP)、および、LDAPS(636/TCP) への通信を許可するための標準的な設定です。

```
# firewall-cmd --permanent --add-service=ldap
# firewall-cmd --permanent --add-service=ldaps
# firewall-cmd --reload
```

6.2 LDAP サーバー設定

設定は /opt/osstech/etc/openldap/slapd.conf ファイルに行ないます。

slapd.conf 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。

OpenLDAP のマルチマスター構成のために、設定が必要な基本的なパラメーターは次の通りです。

- database
- suffix
- rootdn
- rootpw
- database

- access
- overlay syncprov, syncprov-sessionlog, syncprov-checkpoint
- serverId
- syncrepl
- mirrormode

OSSTech 版 OpenLDAP では、テンプレートとなる設定内容を/opt/osstech/etc/openldap/slapd.conf ファイルに設定済みとなっていますので、各パラメーターを用途に合わせて変更してご利用ください。

6.2.1 database パラメーター

slapd.conf ファイルは、database パラメータごとに 1 つの LDAP ツリーを格納するための設定を行ないます。通常は、1 台の LDAP サーバーに 1 つの LDAP ツリーを格納しますが、複数の database 設定を行うことで、複数の LDAP ツリーを格納することも可能です。

database パラメーターには、データベースの種類を示す次のような値を指定することが可能です。(よく利用されるものを抜粋しています)

- wt
  - 一般的な LDAP エントリを格納するための WiredTiger バックエンドを意味します。WiredTiger データベースと呼ばれる更新性能が大幅に向上したバックエンドを利用できます。
  - 運用において以下の制約事項があります。
    - slapd 起動中に slapcat コマンドで直接 LDAP データを参照することはできません。
    - DN を変更するコマンド (MODRDN) において、対象のエントリのツリー配下にエントリが含まれる場合、DN を変更することができません。
- bdb
  - 一般的な LDAP エントリを格納するための Berkeley DB バックエンドを意味します。従来から利用されてきた実績のあるデータベース形式です。
- monitor
  - LDAP の利用状況の統計情報などを格納するためのバックエンドの利用を意味します。
- null
  - データの格納を行わず特別な用途で利用します。

設定例

```
database wt
```

各バックエンドのパラメーターについては、後述します。

6.2.2 suffix パラメーター

LDAP ツリーのトップを意味するルートサフィックスの DN を指定します。

```
suffix "dc=example,dc=com"
```

この LDAP サーバーの各エントリは、このサフィックス配下に登録されることになります。

6.2.3 rootdn パラメーター

LDAP 管理処理用エントリの DN を指定します。root ユーザーが直接 LDAP の操作を行うことを許可するため、以下の DN を指定してください。下記以外の通常の DN を管理者として指定する場合、suffix パラメーターに指定したエントリ配下の DN を指定する必要があります。

```
rootdn "gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
```

rootdn パラメーターに指定したユーザーは、LDAP サーバーの全てのエントリを管理・更新する権限を持ち、アクセス制限やアカウントロックも除外される特別なアカウントとなります。

6.2.4 rootpw パラメーター

rootdn に通常の DN を指定した場合に LDAP 管理処理用エントリのパスワードを指定することができます。

```
rootpw root-pass
```

rootpw パラメーターには、LDAP 管理処理用エントリのパスワードを平文パスワード、もしくはハッシュ化済みパスワードで指定することができます。

しかし、設定ファイルに平文で管理者のパスワードを記載することは望ましくないため、初期エントリの登録後、rootpw の平文パスワードの設定は削除することを推奨します。

6.2.5 access パラメーター

LDAP DIT へのアクセス権限を設定します。

本ドキュメントでは基本的なアクセス権の設定として、以下の要件を満たす設定とします。

- 管理者アカウントは、全ての LDAP エントリの管理が可能
- 複製処理用アカウントは、全ての LDAP エントリの参照が可能
- ユーザーが LDAP の認証が可能
- 認証を行っていないユーザーは LDAP エントリの参照が不可能

なお、rootdn に指定されたエントリは “manage” と同等の権限が自動的に付与されます。

本要件を満たすアクセス権の設定は、以下の内容となります。

```
access to *
    by dn="cn=admin,dc=example,dc=com" manage
    by dn="cn=replica,dc=example,dc=com" read
    by * break

access to attrs=userPassword
    by anonymous auth
    by * none

access to *
    by * none
```

userPassword 属性の「by anonymous auth」の権限は、認証 (BIND) の処理のために必ず必要となります。

6.2.6 マルチマスター複製用設定

マルチマスター構成で設定を行う際、1 台の LDAP サーバーはデータを更新し複製先にデータを複製するマスターサーバーとしての機能と、他の複製元からデータを受け取り自サーバーのデータを更新するスレーブサーバーとしての機能を 1 台のサーバー上で行ないます。

LDAP マスターサーバー (複製元) としての複製機能を有効にするために、syncprov 機能を以下の内容で設定します。

```
overlay syncprov
syncprov-checkpoint 128 5
syncprov-sessionlog 128
```

各パラメーターは次の意味を持ちます。

- syncprov-checkpoint [**操作数**] [**時間 (分)**]
  - メモリ上で保持している contextCSN を定期的にファイルに書き戻すタイミングを指定します。指定した「操作数」の更新が行なわれるか、「時間 (分)」が経過するとチェックポイント動作として、ファイルへの書き戻しが発生します。
  - デフォルトではチェックポイントは行なわれません。
- syncprov-sessionlog
  - LDAP データベースを更新した操作履歴としてメモリ上に保存しておく操作の数です。他のノードからの LDAP の同期の際に参照されます。

LDAP スレーブサーバー (複製先) として、マスターサーバーから LDAP データを同期するために syncrepl パ

ラメーター、および関連パラメーターを設定します。

- serverID パラメーターは、複製を行うサーバー内でサーバーごとに一意の数値を指定します。
- mirrormode パラメーターは、マルチマスター構成を有効とするために「on」の値を指定します。

syncrepl 設定には、以下のパラメーターの設定が必要となります。

パラメーター	設定値
rid	1 台の LDAP サーバー内で、syncrepl パラメーターごとに一意の数値
provider	接続先 LDAP マスターサーバーの URI
type	複製方法 (refreshAndPersist)
retry	LDAP マスターサーバーへの接続が切断された場合のリトライ間隔
keepalive	LDAP マスターサーバーへの接続の keepalive 設定
searchbase	複製対象とする LDAP DIT のツリーの最上位エントリ
scope	searchbase からの複製範囲 (通常は sub)
schemachecking	複製時のエントリのスキーマチェックの有無 (通常は off)
binddn	複製時の接続アカウントの DN
bindmethod	複製時の接続時の認証方式 (通常は simple)
credentials	複製時の接続アカウントのパスワード (平文指定のみ)

LDAP 1 号機の複製機能の設定例は次の通りです。

```
serverID 1

syncrepl rid=1
    provider=ldap://ldap2.example.com/
    type=refreshAndPersist
    retry="5 10 30 +"
    keepalive=600:5:60
    searchbase="dc=example,dc=com"
    scope=sub
    schemachecking=off
    binddn="cn=replica,dc=example,dc=com"
    bindmethod=simple
    credentials="replica-pass"

mirrormode on
```

LDAP 2 号機の複製機能の設定例は次の通りです。

```
serverID 2

syncrepl rid=1
    provider=ldap://ldap1.example.com/
    type=refreshAndPersist
    retry="5 10 30 +"
    keepalive=600:5:60
    searchbase="dc=example,dc=com"
    scope=sub
    schemachecking=off
    binddn="cn=replica,dc=example,dc=com"
    bindmethod=simple
    credentials="replica-pass"

mirrormode on
```

複製設定以外の設定については、LDAP 1 号機と LDAP 2 号機での設定内容は通常同じものとなります。

6.2.7 LDAP スレーブサーバーの複製設定

マルチマスターサーバーではなく、LDAP スレーブサーバーとして構成する場合、mirrormode パラメーターの代わりに updateref パラメーターを設定します。

LDAP スレーブサーバーは、クライアントから更新要求を受け取った際、自サーバーでデータの更新を行うことができないため、更新を行うことができる LDAP サーバーの接続先情報をクライアントに返します。この情報のことを「updateref」と呼びます。

updateref を受け取ったクライアントは、その接続先に改めて更新リクエストを送信し直す必要があります。

例えば LDAP 3 号機として LDAP スレーブサーバーを設定する場合、syncprov 関連の設定は不要で、複製設定として次の内容のパラメーターを設定します。

```
serverID 3

syncrepl rid=1
    provider=ldap://ldap1.example.com/
    type=refreshAndPersist
    retry="5 10 30 +"
    keepalive=600:5:60
    searchbase="dc=example,dc=com"
    scope=sub
    schemachecking=off
    binddn="cn=replica,dc=example,dc=com"
    bindmethod=simple
    credentials="replica-pass"

updateref ldap://ldap1.example.com/
```


6.2.8 WiredTiger バックエンド (wt) の設定

WiredTiger バックエンドを利用する場合の設定例は次の通りです。

```
database wt
suffix "dc=example,dc=com"
rootdn "gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
directory /opt/osstech/var/lib/ldap
wtconfig cache_size=256M
wtconfig log=(enabled)
wtconfig checkpoint=(log_size=0,wait=3600)
idlcache on
```

- wtconfig cache_size
  - WiredTiger データベース内で利用する内部キャッシュサイズを指定します。通常は 256M で十分です。
- wtcoonfig log
  - enabled を指定することでトランザクションログの取得を有効にします。slapd の異常終了時にもトランザクションログにより、更新内容を LDAP データベースに反映することが可能となります。
- wtconfig checkpoint
  - チェックポイントを取得するたびに、トランザクションログの内容をファイルに書き出し、不要になったトランザクションログファイルを自動的に削除します。
  - wait に指定した秒数ごとにチェックポイントが取得されます。
  - log_size に指定したバイト数を更新するたびにチェックポイントを取得します。0 を指定した場合は、更新サイズによるチェックポイントは行ないません。
- idlcache
  - 検索性能を向上するためのキャッシュデータを利用する場合 on を設定します。デフォルトは off です。

6.2.9 Berkeley DB バックエンド (bdb) の設定

Berkeley DB バックエンドを利用する場合の設定例は次の通りです。

```
database bdb
suffix "dc=example,dc=com"
rootdn "gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
directory /opt/osstech/var/lib/ldap
dbconfig set_data_dir .
dbconfig set_lg_dir .
dbconfig set_cachesize 1 0 1
dbconfig set_lk_max_objects 5000
dbconfig set_lk_max_locks 5000
dbconfig set_lk_max_lockers 5000
dbconfig set_flags DB_LOG_AUTOREMOVE
```

各パラメーターの意味は次の通りです。

- 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のサイズをギガバイトとバイト単位で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。
  - 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、slapd の起動時に確保されます。最大 4 ギガバイトまで指定することができます。
  - セグメント数 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。
- 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 が不要になったトランザクションログファイルを自動で削除します。
- set_lg_regionmax［**バイト**］
  - データ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**］
  - トランザクションログファイルの 1 つあたりの最大サイズをバイト単位で指定します。
- set_lg_bsize［**バイト**］
  - トランザクション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。

6.2.10 monitor バックエンドの設定

LDAP サーバーの利用状況や、各種統計情報を取得するために、monitor バックエンドを設定することができます。

monitor バックエンドの設定例は次の通りです。

```
database monitor

access to *
        by dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn="cn=admin,dc=example,dc=com" read
```

monitor データベースには自動的に情報が集計されますので、アクセスを許可するユーザー (DN) に read 権を与えてください。

6.2.11 null バックエンドの設定

null バックエンドは LDAP のエントリとしては何も提供しないバックエンドですが、rootdn パラメーターに管理者ユーザーを設定することで、特定の suffix に依存しない管理者ユーザーを作成することができます。

この機能は、一部の商用 LDAP サービスからの移行時に役に立つことがあります。

```
database null
suffix ""
rootdn "cn=Directory Manager"
rootpw {SSHA}xxxxxxxxxxxxxxx
```

6.3 LDAP サーバーの TLS 対応

LDAP は通信を平文で行うため、ネットワーク上を流れる情報を盗聴されると、LDAP 通信の内容が漏洩・改竄される可能性があります。本章では LDAP の通信を TLS(Transport Layer Security) によって暗号化する方法を説明します。

LDAP の暗号化通信には、LDAPS による通信と LDAP + 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/TCP ではなく 636/TCP を利用し、常に暗号化通信を行ないます。一方、StartTLS を利用する場合、通信ポートとして LDAP の 389/TCP を利用しますが、通信の最初でネゴシエーションを行ない、LDAP サーバーが TLS に対応している場合は暗号化通信を行ないます。

6.3.1 自己証明書の作成

LDAP サーバーの TLS 対応のために、サーバー証明書の設置が必要となります。本書では、自己署名を利用した証明書の設置方法について説明しますが、公的な認証局によるサーバー証明書を利用することも可能です。

自己署名の証明書を生成するためには、 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、ldap1、及び、ldap2 の両サーバーで使用可能な自己証明書ファイルと秘密鍵ファイルを生成するコマンドです。ldap1 か ldap2 にて、このコマンドを実行してください。

```
# (
  cat /etc/pki/tls/openssl.cnf
  echo '[v3_ca]'
  echo 'subjectAltName=@altnames'
  echo '[altnames]'
  echo 'DNS.1=ldap.example.com'
  echo 'DNS.2=ldap1.example.com'
  echo 'DNS.3=ldap2.example.com'
) | openssl req \
    -config /dev/stdin \
```



```
    -new \
    -subj '/CN=ldap.example.com' \
    -x509 \
    -out ldap.example.com.crt \
    -days 7300 \
    -sha256 \
    -newkey rsa:4096 \
    -keyout ldap.example.com.key \
    -nodes \
;
```

上記コマンドを実行すると以下のメッセージが表示され、自己署名証明書ファイル ldapexample.com.crt、秘密鍵ファイル ldap.example.com.key が生成されます。

```
Generating a 4096 bit RSA private key
...
writing new private key to 'ldap.example.com.key'
-----
```

作成された証明書と秘密鍵は ldap1、 ldap2 の以下の場所に保存します。

- /opt/osstech/etc/openldap/certs/ldap.example.com.crt
- /opt/osstech/etc/openldap/private/ldap.example.com.key

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、自己署名の証明書の生成を指示
- -newkey rsa:4096
  - 鍵ペアの生成を指示、および鍵の種類 (RSA) と鍵長 (4096 ビット) の指定
- -nodes
  - 秘密鍵を暗号化せずに保存
- -keyout ldap.example.com.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 ldap.example.com.crt
  - 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 7300
  - 生成する自己署名証明書の有効期間 (日数)
  - 省略すると 30 日となります。
- -subj "/CN=ldap.example.com
  - 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ります。
- 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ありません。

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。

以下の実行例のように、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してください)。

```
$ openssl x509 -noout -text -in ldap.example.com.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            8f:9b:33:9e:e2:81:ed:9d
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=ldap.example.com
        Validity
            Not Before: Oct 29 07:05:09 2018 GMT
            Not After : Oct 24 07:05:09 2038 GMT
       Subject: CN=ldap.example.com
       Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
... 省略...
          X509v3 Subject Alternative Name:
              DNS:ldap.example.com, DNS:ldap01.example.com, DNS:ldap02.example.com
... 省略...
```

なお、弊社製品には、自己証明書を簡単に作成するためのスクリプトが含まれております。下記の手順にて、自己証明書を作成することが可能です。

弊社製品に含まれる osstech-support パッケージをインストールします。

```
# rpm -ih osstech-support-3.0-xxx.el7.x86_64.rpm
```

openssl-selfcert スクリプトにより、自己証明書を作成します。コマンドの引数には、作成する証明書の subjectAltName に含めたいホスト名を全て指定してください。先頭に指定したホスト名が自己証明書の CN の値として設定されます。

```
$ /opt/osstech/bin/openssl-selfcert \
  ldap.example.com \
  ldap1.example.com \
  ldap2.example.com \
;
... 省略...
```

```
writing new private key to 'ldap.example.com.key'
-----
-r-------- 1 alice users 2069 10月 29 07:35 ldap.example.com.crt
-r-------- 1 alice users 3272 10月 29 07:35 ldap.example.com.key
```

6.3.2 サーバー証明書と秘密鍵の設定

前述の手順で作成したサーバー証明書と秘密鍵を LDAP 1 号機と LDAP 2 号機に設置します。今回は両方のノードで利用できるサーバー証明書を準備したため、同じ手順を 2 台で行ないます。

以下の場所に、サーバー証明書と秘密鍵が設置されていることを確認します。

- /opt/osstech/etc/openldap/certs/ldap.example.com.crt
- /opt/osstech/etc/openldap/private/ldap.example.com.key

秘密鍵ファイルは、一般ユーザーが参照できず、ldap ユーザーが参照できるようにパーミッションを設定します。

```
# chmod 640 /opt/osstech/etc/openldap/private/ldap.example.com.key
# chown root:ldap /opt/osstech/etc/openldap/private/ldap.example.com.key
```

続いて、/opt/osstech/etc/openldap/slapd.conf ファイルの証明書関連のパラメーターを設定します。

```
TLSCACertificateFile /opt/osstech/etc/openldap/certs/ldap.example.com.crt
TLSCertificateFile   /opt/osstech/etc/openldap/certs/ldap.example.com.crt
TLSCertificateKeyFile /opt/osstech/etc/openldap/private/ldap.example.com.key
```

TLSCACertificateFile は認証局の証明書、TLSCertificateFile にサーバー証明書を設定しますが、今回の手順の場合、両者に同じファイルを指定します。

6.3.3 複数台構成の場合のサーバー証明書設定

LDAP サーバーの複数台構成で syncrepl 機能による複製を行う場合、複製の通信を LDAP(StartTLS) や LDAPS で通信を行うためには、複製通信のためにサーバー証明書が適切に設定されている必要があります。

商用サービスや UPKI などで発行された公的なサーバー証明書を利用する場合、それぞれの LDAP サーバーで TLSCertificateFile と TLSCertificateKeyFile を設定することで、複製の通信も暗号化することができます。

自己署名証明書を利用する場合、syncrepl パラメーターを設定する側に、接続先の LDAP サーバーの自己署名証明書を、TLSCACertificateFile に指定するサーバー証明書ファイルに含める必要があります。

例えば、LDAP 1 号機と LDAP 2 号機のマルチマスター構成の場合、LDAP 1 号機のサーバー証明書ファイルを LDAP 2 号機の TLSCACertificateFile に設定し、LDAP 2 号機のサーバー証明書ファイルを LDAP 1 号機の

TLSCACertificateFile に設定することになります。

このようにサーバー証明書ファイルを適切に配置・設定後、syncrepl パラメーターの provider 設定を LDAPS に変更します。

- LDAP 1 号機の provider 設定

```
syncrepl
... 省略...
    provider=ldaps://ldap2.example.com/
... 省略...
```

- LDAP 2 号機の provider 設定

```
syncrepl
... 省略...
    provider=ldaps://ldap1.example.com/
... 省略...
```

6.3.4 TLS プロトコルの指定

TLS を設定する場合、セキュリティ的に脆弱なプロトコルの利用を避けるため、SSL 3.0 の通信は無効にすることが強く推奨されており、OpenLDAP でも利用するプロトコルレベルを設定することができます。

OpenLDAP で TLS 1.0 以前の通信プロトコルを無効化するためには、slapd.conf に以下の設定を追加します。

```
TLSProtocolMin 3.2
```

上記の設定で、TLS 1.1 以降の通信が許可され、TLS 1.0 までしか対応していないクライアントとの TLS 通信は拒否されます。

なお指定できる値とプロトコルバージョンの関係は次の通りです。

プロトコル	設定値
SSL 3.0	3.0
TLS 1.0	3.1
TLS 1.1	3.2
TLS 1.2	3.3

6.3.5 利用可能な暗号方式の設定

TLS 通信を利用する場合に利用可能な暗号化方式を許可するために、TLSCipherSuite パラメーターを利用することができます。昔から利用されている暗号化方式には現代においては十分安全とはいえない方式もあるため、脆弱な暗号化方式を取り除いて利用を許可しておくことが望まれます。

弊社では、slapd.conf の TLSCipherSuite パラメーターとして、以下の設定を行うことを推奨しています。

```
TLSCipherSuite ALL:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:
!DES-CBC3-SHA:!KRB5:!PSK:!IDEA:!SEED:!RC4:!MD5:!EXPORT:!LOW:!aNULL:!eNULL
```

※上記設定は、改行せずに 1 行で設定してください

6.4 チューニングパラメーター

6.4.1 インデックス設定

LDAP の検索時にインデックスを利用可能にするため、属性ごとにインデックスを設定することができます。OpenLDAP では、最大 127 個の属性に対して、インデックスを設定することが可能です。

- レプリケーションのためのインデックス設定例

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

- その他のインデックスの設定例

```
index ou,cn,mail,sn,givenName  eq,pres,sub
index uid                      eq,pres,sub
```

インデックスを設定すると、設定内容に一致する検索条件を満たす場合の検索性能が向上しますが、エントリの更新時にインデックスの更新処理も必要となるため、更新処理の性能が低下し、検索性能にも影響を与えることがあります。従って、利用されないインデックスは設定しないように注意しましょう。

LDAP エントリ投入後に slapd.conf のインデックス設定を変更した場合、slapindex コマンドでインデックスを再作成する必要があります。

インデックスの再作成は、slapd を停止した状態で、slapindex コマンドを実行します。

```
# systemctl stop osstech-slapd
# sudo -u ldap /opt/osstech/sbin/slapindex
# systemctl start osstech-slapd
```

slapindex コマンドを実行すると、/opt/osstech/var/lib/ldap 配下の各インデックスのファイルが更新されます。

このときにファイルの所有者が root に変更され、そのままでは slapd の起動が出来なくなります。そのため、slapindex コマンド実行後は、必ず chown コマンドで/opt/osstech/var/lib/ldap 配下のファイルの所有者を ldap ユーザーに変更してください。

運用開始後、LDAP のログに 「bdb_substring_candidates: (属性名) not indexed」や「bdb_equality_candidates: (属性名) not indexed」といったメッセージが記録される場合、検索リクエストに指定されているフィルタに適したインデックスが設定されていないことを意味します。このような場合、各属性の「eq」や「sub」といったインデックスを追加することで、検索性能を改善できることがあります。

6.4.2 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。エントリをキャッシュすることで、ディスクへのアクセスやエントリの解析処理が軽減されるため、認証・参照系の操作に対するレスポンスが向上します。

キャッシュ関連として、次のパラメーターを設定することができます。

```
cachesize 10000
idlcachesize 30000
checkpoint 512 5
```

- `cachesize [エントリ数]`
  - slapd がメモリ上にエントリをキャッシュとして保持できる最大数を指定します。このキャッシュ内のエントリは、参照時にエントリ内容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。
- `checkpoint [キロバイト] [分]`
  - 指定したサイズのデータがデータ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戻され、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。

6.5 slapd.conf ファイルの設定例

これまでに説明した各パラメーターを設定した slapd.conf の設定例を示します。

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

```
include /opt/osstech/etc/openldap/schema/inetorgperson.schema
include /opt/osstech/etc/openldap/schema/ldapns.schema
include /opt/osstech/etc/openldap/schema/ns-mail.schema
include /opt/osstech/etc/openldap/schema/ppolicy.schema

moduleload ppolicy

pidfile /opt/osstech/var/run/openldap/slapd.pid
argsfile /opt/osstech/var/run/openldap/slapd.args

loglevel stats

threads 32
tool-threads 4
timelimit 30
sizelimit unlimited

TLSCACertificateFile /opt/osstech/etc/openldap/certs/ca.crt
TLSCertificateFile /opt/osstech/etc/openldap/certs/ldap1.crt
TLSCertificateKeyFile /opt/osstech/etc/openldap/private/ldap1.key
TLSProtocolMin 3.2
TLSCipherSuite ALL:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!DES-CBC3-SHA:
!KRB5:!PSK:!IDEA:!SEED:!RC4:!MD5:!EXPORT:!LOW:!aNULL:!eNULL (1 行で)

password-hash {CRYPT}
password-crypt-salt-format "$6$%.16s"

access to dn.subtree=""
        by * read

database wt
suffix "dc=example,dc=com"
rootdn gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
directory /opt/osstech/var/lib/ldap
wtconfig cache_size=256M

index objectClass               eq
index modifyTimestamp           eq
index ou                        eq
index cn                        eq,sub
index sn                        eq
index uid                       eq
index displayName               eq
index mail                      eq
index mailAlternateAddress      eq
index uidNumber                 eq
index gidNumber                 eq
index memberUID                 eq
index uniqueMember              eq
index member                    eq
index entryCSN                  eq
index entryUUID                 eq
```



```
limits dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
        time=unlimited
        size=unlimited

limits dn="cn=admin,dc=example,dc=com"
        time=unlimited
        size=unlimited

limits dn="cn=replica,dc=example,dc=com"
        time=unlimited
        size=unlimited

access to *
        by dn="cn=replica,dc=example,dc=com" read
        by * break

access to *
        by dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
        by dn="cn=admin,dc=example,dc=com" manage
        by * break

access to attrs=userPassword
        by anonymous auth
        by * none

access to *
        by * read

overlay syncprov
syncprov-checkpoint 128 5
syncprov-sessionlog 128

serverID 1

syncrepl rid=001
        provider="ldaps://ldap2.example.com"
        type=refreshAndPersist
        retry="5 10 30 +"
        keepalive=300:5:10
        searchbase="dc=example,dc=com"
        scope=sub
        schemachecking=off
        bindmethod=simple
        binddn="cn=replica,dc=example,dc=com"
        credentials="replica-pass"

mirrormode on

database monitor

access to *
```



```
        by dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn="cn=admin,dc=example,dc=com" read
```

作成した slapd.conf ファイルは、以下の権限で配置します。

オーナー	グループ	権限
root	ldap	0640

7 初期データの登録

slapd.conf ファイルの設定が完了後、管理者は LDAP に初期データを登録します。

初期データには、LDAP 管理処理用エントリと、複製処理用エントリを登録します。また、ユーザー用の OU やグループ用の OU など、LDAP ツリーに必要な各種エントリを合わせて登録することも可能です。

初期データは、LDIF(LDAP Data Interchange Format) 形式のテキストファイルとして作成します。

初期データとして、init.ldif ファイルとして、以下の内容で作成します。

```
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: Example Corp.
dc: example

dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP admin
userPassword: {CRYPT}$6$e49HFO/c$zqek.sFAMjpzOyogpjgkEtwMY6OgeQzG/Ykmwl80DpH
WLxiz..kFZ77CaU3N6dvzHiruLeQHLMIJYmT69qcOR0

dn: cn=replica,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: replica
description: LDAP replica
userPassword: {CRYPT}$6$TPngEmepG9n/5TcX$2u0DIAg.HpqzVBG9x5p7EkwTuO6/tIMFI47
7Zwk4hQWtI9WktgThF81rrevJJI2MeQFlqMO.k66hnqH7fRwOR0

dn: ou=users,dc=example,dc=com
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups
```

上記はサンプルとしての内容ですが、導入環境に合わせて、次の各項目の値を変更します。

- LDAP suffix の値
  - 各 DN に指定されている「dc=example,dc=com」の値を適切な suffix に変更してください
- 管理者用エントリの DN と RDN の値
  -「dn: cn=admin,dc=example,dc=com」と「cn: admin」の部分を適切な値に変更してください。

- 複製処理用エントリの DN と RDN の値
  - 「dn: cn=replica,dc=example,dc=com」と「cn: replica」の部分を適切な値に変更してください。

7.1 パスワード (userPassword) のハッシュ化

各ユーザーエントリに設定している userPassword 属性には、そのユーザーで認証する際のパスワードを設定します。パスワードは平文でも設定できますが脆弱なため、適切にハッシュ化したパスワードを指定する必要があります。

OpenLDAP で利用可能な主なパスワードのハッシュ化方式と特徴について説明します。

ハッシュ化方式	特徴
PBKDF2	ソルト付き、SHA-2(512〜256 ビット)、ストレッチング (10000 回)
CRYPT	ソルト付き、SHA-2(512 ビット) など、ストレッチング (5000 回)
SSHA512	ソルト付き、SHA-2(512 ビット)
SSHA	ソルト付き SHA-1 160 ビット (脆弱なため利用しないことが望ましい)

現在は、強度、利用時の負荷、汎用性などを勘案して、CRYPT(SHA512) 方式での userPassword のハッシュ化方式の利用を推奨します。

- ソルト
  - 複数のユーザーが同一のパスワードを利用している場合、パスワードをハッシュ化すると、変換後のハッシュ化済みパスワード文字列も同一となり、同一のパスワードを利用していることが推測可能となります。ハッシュ化済みパスワード文字列の安全性を高めるために、パスワードごとにソルトと呼ばれる何文字かのランダムな文字を付与することで、ハッシュ化済みパスワード文字列が同一とならない仕組みを提供します。
- ストレッチング
  - ハッシュ化済みパスワード文字列が漏洩した場合に、総当りなどでのオフライン解析に対する強度を高めるため、ハッシュ操作を何度も行うストレッチングという処理が行われます。ストレッチングを行うことでパスワードの解析に必要な時間が数千倍以上必要となるためオフライン解析に対する安全性が高まります。
  - デフォルトでは PBKDF2 では 10000 回、CRYPT では 5000 回のストレッチングが行われます。
  - ストレッチングは通常の認証時にも行われ、CPU の利用率が高まるため、CPU リソースを十分に用意することを推奨します。現代の環境ではストレッチングを行っているハッシュ方式を利用しても、LDAP の認証にかかる時間は 1 秒未満です。
- CRYPT 方式
  - CRYPT 方式は、ハッシュ化の処理を OS のライブラリを利用して行なうため、他のシステムとの互換性が高い方式となります。

- 歴史的経緯により、CRYPT 形式ではいくつかのハッシュ化方式を選択できる仕組みとなっていますが、現在の推奨は CRYPT(SHA512) となります。

userPassword 属性はハッシュ化方式と、パスワードをハッシュ化した値を BASE64 エンコードした文字列を組み合わせた次の形式で表されます。

```
{ハッシュ化方式}[ハッシュ化パスワードの BASE64 エンコーディング]
```

このハッシュ化パスワード形式を生成するために slappasswd コマンドを利用することができます。

```
# /opt/osstech/sbin/slappasswd
New password:  <平文でパスワードを入力>
Re-enter new password: <平文でパスワードを再入力>
{SSHA}rjq7rNnDQCkdcpt/pwmKsg/zIsarHQpP
```

デフォルトでは SSHA(ソルト付き SHA-1) 形式のハッシュ化パスワードが生成されます。

-s オプションを指定することで、コマンドの引数としてパスワード文字列を指定することができますが、シェルの履歴に残るため、本番環境では利用しないでください。

```
# /opt/osstech/sbin/slappasswd -s replica-pass
{SSHA}BIYEBUNC/J4RKWwpi4g7NoEqensvfYJq
```

slappasswd コマンドに-h オプションを指定することで、ハッシュ方式を指定することができます。指定できる値としては主に次のものがあります。

指定値	ハッシュ方式
{PBKDF2}	PBKDF2 方式
{CRYPT}	CRYPT 方式
{SSHA512}	Salt 付き SHA-2 512 ビット
{SSHA}	Salt 付き SHA-1

以下は、{PBKDF2}方式で生成する場合の設定例です。

```
# /opt/osstech/sbin/slappasswd -h '{PBKDF2}'
New password:  <平文でパスワードを入力>
Re-enter new password: <平文でパスワードを再入力>
{PBKDF2}10000$mOF7eiKjObtNGj07F9WokA$4NM.BawhBqmqUBvKCQiuxCgCCdQ
```

CRYPT 方式で指定する場合、-c オプションでソルトとして指定する値によって、CRYPT の処理内で利用す

るハッシュ化方式を選択することができます。

以下は CRYPT 方式を SHA-2 512 ビットでハッシュ化する場合のコマンドの実行例です。-c オプションに指定した値のうち、「6」の部分が、SHA-2 512 ビットを意味し、「.16s」n の部分がソルト長が 16 文字を意味するキーワードです。

```
# /opt/osstech/sbin/slappasswd -h '{CRYPT}' -c '$6$%.16s' -s replica-pass
{CRYPT}$6$.16s$s29MjivUhIuZ2Ml3ixuE....
```

7.2 LDIF の登録

作成した LDIF の登録手段は 2 つあります。

1. slapadd コマンドによる登録
2. ldapadd コマンドによる登録

7.2.1 slapadd コマンドによる初期データの登録

slapadd コマンドは、データベースファイルに直接データを登録することができます。

root ユーザーのみ実行可能ですが、データベースファイルに直接データを登録するため、LDAP にデータが登録されていない状態でのみ利用します。

また、LDAP サービスを経由したデータのチェックなどが行なわれないため、データの記載順序などが正しくない場合、LDAP データとして不整合な状態が発生することもあるため、LDIF を作成する際に注意が必要です。

```
# /opt/osstech/sbin/slapadd -l init.ldif
```

slapadd コマンドで LDAP データを登録すると、各データファイルのオーナーが root ユーザーで作成され、slapd が起動しなくなるため、各データファイルのオーナーを変更してから、LDAP サービスを起動します。

```
# chown -hR ldap:ldap /opt/osstech/var/lib/ldap/*
# systemctl start osstech-slapd
```

7.2.2 ldapadd コマンドによる初期データの登録

ldapadd コマンドは、LDAP サービス経由で LDAP にデータを登録することができます。また、別サーバーの LDAP に対して登録を行うことも可能です。

そのため、初期データの登録の際には、まず LDAP サービスを起動します。

```
# systemctl start osstech-slapd
```

ldapadd コマンドに LDIF ファイルを指定して、初期データを登録します。

```
# /opt/osstech/bin/ldapadd -Y EXTERNAL -H ldapi:/// -f init.ldif

adding new entry "dc=example,dc=com"

adding new entry "cn=admin,dc=example,dc=com"

adding new entry "cn=replica,dc=example,dc=com"

adding new entry "ou=Users,dc=example,dc=com"

adding new entry "ou=Groups,dc=example,dc=com"
```

7.3 登録したデータの確認

LDAP に登録済みのデータは ldapsearch コマンドで確認することができます。初期データの登録後、cn=admin ユーザーによる LDAP 操作が可能となります。

```
# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
;
Enter LDAP Password: ******* (cn=admin のパスワード)
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# example.com
dn: dc=example,dc=com
objectClass: organization
objectClass: dcObject
dc: example
o: example

... 省略 ...
```

7.3.1 ldapsearch コマンドの便利な利用方法

ldapsearch コマンドで LDAP エントリを LDIF 形式で取得したい場合、“-LLL” オプションを指定します。

```
# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
  -LLL \
;
```

OpenLDAP サーバーに LDAP エントリを登録すると、各エントリに管理用の内部属性も付与されて管理されます。内部属性を参照したい場合、ldapsearch コマンドの取得対象属性に「+」を指定します。

```
# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
  + \
;
```

ldapsearch コマンドで LDAP エントリを取得する際、1 行の内容が長い場合に、自動的に改行が行なわれます。LDIF 形式でエントリを扱いたい場合などに、自動的に改行されたくない場合、“-o ldif-wrap=no” オプションを指定します。

```
# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
  -o ldif-wrap=no \
  -LLL \
;
```

7.4 LDAP データの更新・削除

登録済みの LDAP データを更新する場合、更新用の LDIF ファイルを作成します。

以下の LDIF は、sn 属性の値を「山田」に変更する場合の LDIF です。

```
dn: uid=user1,ou=Users,dc=example,dc=com
changetype: modify
replace: sn
```

```
sn: 山田
```

複数の属性を一度に変更する場合は、「-」で区切ります。

```
dn: uid=user1,ou=Users,dc=example,dc=com
changetype: modify
replace: sn
sn: 山田
-
replace: givenName
givenName: 太郎
```

新しく属性を登録する場合は「add」を使います。 以下の LDIF は新しく description 属性を追加する場合の例です。

```
dn: uid=user1,ou=Users,dc=example,dc=com
changetype: modify
add: description
description: このアカウントはテスト用です。
```

登録済みの属性を削除する場合は 「delete」を使います。

```
dn: uid=user1,ou=Users,dc=example,dc=com
changetype: modify
delete: description
```

ldapmodify コマンドで、作成した LDIF の内容を LDAP に反映します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f modify.ldif \
;
```

7.5 複製確認

複数台の LDAP サーバーで構成されている場合、以下の手順で複製が正しく動作していることの確認を行ないます。

LDAP 1 号機で、以下の手順にて contextCSN の値を取得します。


```
[root@ldap1]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
  -s base \
  contextCSN \
;
Enter LDAP Password: ********
contextCSN: 20200618055623.591253Z#000000#001#000000
contextCSN: 20200702045400.385038Z#000000#002#000000
```

LDAP 2 号機で、以下の手順にて contextCSN の値を取得します。

```
[root@ldap2]# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
  -s base \
  contextCSN \
;
Enter LDAP Password: ********
contextCSN: 20200618055623.591253Z#000000#001#000000
contextCSN: 20200702045400.385038Z#000000#002#000000
```

contextCSN は、その LDAP サーバー経由で更新された最新の更新状態を記録するエントリです。contextCSN に含まれる「#001」や「#002」が、slapd.conf ファイルで設定されている serverID を意味します。

上記の取得例では、LDAP 1 号機経由で更新された最新エントリの情報が、「20200618055623.591253Z#000000#001#000000」となり、2020 年 6 月 18 日 5 時 56 分 23 秒 (UTC) に更新されたことを意味します。

また、同じ値が LDAP 2 号機の contextCSN として登録されていることより、LDAP 1 号機から LDAP 2 号機への複製が正しく反映されていることが分かります。

一方、LDAP 2 号機経由で更新された最新エントリの情報が「20200702045400.385038Z#000000#002#000000」となり、2020 年 7 月 2 日 4 時 54 分 00 秒 (UTC) に更新されたことを意味します。

こちらも同じ値が LDAP 1 号機の contextCSN に含まれていることより、LDAP 2 号機から LDAP 1 号機への複製が正しく反映されていることが分かります。

LDAP サーバー構築直後は、LDAP 2 号機に対してエントリの更新を行っていないことも多いため、LDAP 2 号機のエントリを直接更新し、LDAP 1 号機にエントリが複製され、contextCSN も更新されることを確認してください。

8 LDAP サーバーの様々な設定

8.1 ldap.conf ファイルの設定

OSSTech 版 OpenLDAP をインストールすると、/opt/osstech/etc/openldap/ldap.conf ファイルが作成されます。

このファイルは OSSTech 版 OpenLDAP のクライアントツール (ldapsearch や ldapadd など) が動作する際に参照され、デフォルト設定などが反映されます。

例えば、下記の設定を行った場合、/opt/osstech/bin/ldapsearch コマンドなどの-b オプションと-H オプションを指定しなくても、デフォルト値として “-b dc=example,dc=com -H ldap://localhost” が指定された場合と同じ結果が得られます。

```
BASE dc=example,dc=com
URI ldap://localhost
```

以下のコマンドで man データを参照することで、ldap.conf ファイルに指定可能なパラメーターの確認が可能です。

```
$ /opt/osstech/bin/osstech-man ldap.conf
```

なお、OS 同梱版の OpenLDAP パッケージでは、/etc/openldap/ldap.conf ファイルが用意されていますが、このファイルの設定内容は、/usr/bin/ldapsearch コマンドや、/usr/lib64/libldap 系のライブラリなどが参照します。

8.2 Listen ポート設定

OSSTech 版 OpenLDAP の初期状態では、slapd が LISTEN するアドレスは 0.0.0.0(IPv4)、::/0(IPv6) に設定され、全てのネットワークインタフェースからのリクエストを受け付けます。

特定のネットワークインタフェースに限定して slapd を LISTEN したい場合は、slapd の起動時の-h オプションで LISTEN するインタフェースのアドレスやホスト名を指定する必要があります。

/opt/osstech/etc/openldap/service/slapd/env/SERVICES ファイルに-h オプションに渡したい文字列を設定することができます。

```
# echo "ldap://127.0.0.1/ ldaps://127.0.0.1/" > \
/opt/osstech/etc/openldap/service/slapd/env/SERVICES
```

上記コマンドを実行後、slapd を再起動することで設定が反映されます。

```
# systemctl restart osstech-slapd
```

SERVICES ファイルに何も設定されていないデフォルト状態では、LDAP サーバーのサービス URL として、次の URL が設定されます。(※ ldaps:///については、サーバー証明書が設定されている場合です)

```
ldapi:/// ldap:/// ldaps:///
```

8.3 IPv6 無効化

slapd の起動時に「-4」オプションを付与することで、IPv6 を無効化することができます。OSSTech 版 OpenLDAP では、以下のコマンドで起動オプションを設定することができます。

```
# echo "-4" > /opt/osstech/etc/openldap/service/slapd/env/OPTIONS
```

起動後に、slapd を再起動して設定を反映します。

```
# systemctl restart osstech-slapd
```

8.4 サービス起動・停止のタイムアウト設定変更

OSSTech 版 OpenLDAP は、OS の systemd 経由で起動・停止が行なわれます。

起動や停止を開始してから一定時間が経過しても処理が完了しない場合、systemd が自動的にタイムアウトを判断し、起動・停止処理を中断します。

デフォルトでは 90 秒のタイムアウトが設定されていますが、他に導入されているシステムの影響などで起動・停止処理が 90 秒以上かかる場合には、以下の手順でタイムアウト時間を変更することが可能です。

```
# systemctl edit osstech-slapd.service
```

上記コマンドでエディタが起動しますので、次の内容を追加して保存・終了してください。(下記の例では起動時間のタイムアウトを 300 秒に変更しています)

```
[Service]
TimeoutStartSec=300
TimeoutStopSec=300
```

この手順により、/etc/systemd/system/osstech-slapd.service.d/override.conf ファイルが作成され、OSSTech 版 OpenLDAP の起動・停止のタイムアウト時間が変更されます。

8.5 root ユーザーによる LDAP データ操作

LDAP サーバーのデータ操作で ldapsearch や ldapadd などのコマンドを利用する際、LDAP サーバーに登録されたユーザーの DN を指定して接続し認証を行うことで、LDAP に接続することができます。

この認証の際に、LDAP のユーザーの DN の代わりに、同一サーバー上の root ユーザーであることを利用して認証する方法を設定して利用することが可能です。

root ユーザーで接続する場合、認証方式として SASL による EXTERNAL 認証を利用し、ldapi プロトコルにより同一サーバー上の LDAP サービスに接続します。

この接続方式で接続した root ユーザーに対して、検索や更新を許可するために、slapd.conf のアクセス制限設定、および、リミット制限に以下の設定を追加します。

```
limits dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
       time=unlimited
       size=unlimited
```

```
access to *
       by dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
       by * break
```

以上の設定を反映した LDAP サーバーに対して、同一サーバー上から root ユーザーで ldapsearch や ldapadd などを実行する際に、「-Y EXTERNAL」と「-H ldapi:///」オプションを付与することで、パスワード入力が不要な root ユーザーでの接続を行うことができます。

```
# /opt/osstech/bin/ldapsearch -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com -LLL
# /opt/osstech/bin/ldapmodify -Y EXTERNAL -H ldapi:/// -f modify.ldif
```

9 パスワードポリシー

OpenLDAP には ppolicy オーバーレイによるパスワードポリシー機能が用意されています。パスワードポリシーを設定すると、以下の操作時にパスワードポリシーが適用されます。

- LDAP の認証 (BIND) 時
- パスワード変更時の新しいパスワードに対するチェック

OpenLDAP を参照するクライアントがパスワードポリシー機能に対応していれば、これらのクライアント上でもパスワードポリシー機能を有効に活用することができます。

本章では OpenLDAP のパスワードポリシーの設定方法について解説します。

9.1 パスワードポリシーの設定

OpenLDAP のパスワードポリシーは、slapd.conf ファイルに ppolicy オーバーレイを設定することで有効になります。

1. パスワードポリシー用スキーマファイルの有効化

slapd.conf ファイルに以下のスキーマ設定行が記述されていることを確認します。記述がない場合は、スキーマ取り込み行の末尾に追記します。

```
include /opt/osstech/etc/openldap/schema/ppolicy.schema
```

2. ppolicy オーバーレイモジュールのロード

パスワードポリシー機能 (ppolicy) を有効化するため、モジュールをロードする設定を追記します。

```
moduleload ppolicy
```

3. パスワードポリシー機能の有効化

slapd.conf ファイルの database セクション内に以下の内容を追記します。

```
overlay ppolicy
ppolicy_default "cn=default,ou=policies,dc=example,dc=com"
```

「ppolicy_default」は、特別なパスワードポリシーが設定されていない全てのエントリに適用されるデフォルト

のパスワードポリシーとなります。指定したエントリが存在しなければ無視され、デフォルトのパスワードポリシーは設定されません。

設定完了後、slapd を再起動します。

```
# systemctl restart osstech-slapd
```

複数台構成の場合、パスワードポリシーの設定は各ノードごとに行う必要があります。パスワードポリシーを有効にし ppolicy.schema に含まれる属性が LDAP に登録されている場合、複製先のノードでも ppolicy スキーマが有効になっている必要があります。

したがって、通常は複製先のノードのパスワードポリシーを有効に設定してから、最後に複製元となるノードのパスワードポリシーを有効にします。

9.2 パスワードポリシーエントリの登録

パスワードポリシー機能では、以下の 3 種類のポリシーの設定方法があり、次の順番で優先されます。

1. ユーザーエントリに直接設定されているパスワードポリシー
2. ユーザーエントリから指定されるパスワードポリシーエントリ
3. 全ユーザーに適用されるデフォルトのパスワードポリシー (デフォルトパスワードポリシーと呼びます)

デフォルトパスワードポリシーが設定されている場合でも、ユーザーエントリに個別に設定されているポリシーが優先されます。

9.2.1 デフォルトパスワードポリシーの登録

デフォルトパスワードポリシーとして、以下の形式の LDIF ファイルを作成します。以下の LDIF ファイル (本説明では default_policy.ldif とします) の各設定値は設定例です。各属性の詳細については「OpenLDAP パスワードポリシーパラメーター詳細」で説明します。

```
dn: ou=policies,dc=example,dc=com
objectClass: organizationalUnit
ou: policies

dn: cn=default,ou=policies,dc=example,dc=com
objectClass: pwdPolicy
objectClass: organizationalRole
cn: default
pwdAttribute: userPassword
pwdMinLength: 8
pwdCheckQuality: 2
pwdMaxAge: 7776000
```

```
pwdMinAge: 180
pwdExpireWarning: 1209600
pwdLockout: TRUE
pwdMaxFailure: 5
pwdLockoutDuration: 90
pwdFailureCountInterval: 180
pwdInHistory: 3
pwdMustChange: TRUE
```

パスワードポリシーエントリの DN は、slapd.conf ファイルの「ppolicy_default」パラメーターで指定した DN と同じものにします。

ldapadd コマンドで作成したパスワードポリシーを LDAP に登録します。

```
# /opt/osstech/bin/ldapadd \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f default_policy.ldif \
;
```

LDIF ファイルの登録が完了すると、デフォルトパスワードポリシーが有効となります。

ただし、slapd.conf ファイルの rootdn に指定された管理用エントリのみは、パスワードポリシーは適用されませんので注意してください。

9.2.2 ユーザーごとの共有パスワードポリシーの設定

デフォルトパスワードポリシー以外に、特定のユーザーにあるパスワードポリシーを適用したい場合、共有パスワードポリシーのエントリを作成し、特定ユーザーのみ参照させることができます。

共有パスワードポリシーのエントリを LDIF ファイルで作成します。本章の説明では subpolicy.ldif とします。

```
dn: cn=subpolicy,ou=policies,dc=example,dc=com
objectClass: pwdPolicy
objectClass: organizationalRole
cn: DefaultPolicy
pwdAttribute: userPassword
pwdMinLength: 8
pwdCheckQuality: 2
pwdMaxAge: 7776000
pwdMinAge: 180
pwdExpireWarning: 1209600
pwdLockout: TRUE
pwdMaxFailure: 5
pwdLockoutDuration: 90
pwdFailureCountInterval: 180
```



```
pwdInHistory: 3
pwdMustChange: TRUE
```

ldapadd コマンドで作成した LDIF ファイルを登録します。

```
# /opt/osstech/bin/ldapadd \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f subpolicy.ldif \
;
```

続いて、ユーザーがこのパスワードポリシーを参照するため、ユーザーのエントリ内容を変更するための LDIF(policy_change.ldif) を作成します。下記の LDIF の dn の値は実際にこのポリシーを適用するユーザーの dn を指定してください。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
add: pwdPolicySubentry
pwdPolicySubentry: cn=subpolicy,ou=policies,dc=example,dc=com
```

ldapmodify コマンドで、ユーザーのエントリに反映します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f policy_change.ldif \
;
```

以上で、subpolicy エントリに設定されているパスワードポリシーが該当ユーザーに適用されます。

該当ユーザーにデフォルトパスワードポリシーを適用したい場合には、今回追加した「pwdPolicySubentry」属性を削除してください。

9.2.3 ユーザーパスワードポリシーの設定

ユーザーごとに固有のパスワードポリシーを設定したい場合、ユーザーエントリに直接パスワードポリシーを設定することができます。

以下のようにユーザーエントリにパスワードポリシーを設定するための LDIF ファイルを作成します。LDIF ファイルの dn の値として、該当ユーザーの dn を指定してください。

また、「pwdPolicysubentry」属性の値として、ユーザー自身の dn の値を指定してください。つまり、適用す

るパスワードポリシーの参照先を自身のエントリとして設定します。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
add: objectClass
objectClass: pwdPolicy
-
add: pwdPolicySubentry
pwdPolicySubentry: uid=username,ou=Users,dc=example,dc=com
-
add: pwdAttribute
pwdAttribute: userPassword
-
add: pwdMinLength
pwdMinLength: 8
-
add: pwdCheckQuality
pwdCheckQuality: 2
-
add: pwdMaxAge
pwdMaxAge: 7776000
-
add: pwdMinAge
pwdMinAge: 180
-
add: pwdExpireWarning
pwdExpireWarning: 1209600
-
add:pwdLockout
pwdLockout: TRUE
-
add:pwdMaxFailure
pwdMaxFailure: 5
-
add: pwdLockoutDuration
pwdLockoutDuration: 90
-
add: pwdFailureCountInterval
pwdFailureCountInterval: 180
-
add: pwdInHistory
pwdInHistory: 3
```

作成した LDIF ファイルを ldapmodify コマンドで LDAP に反映します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f userpolicy.ldif \
```

```
;
```

以上で、該当ユーザーにパスワードポリシーが適用されます。該当ユーザーのパスワードポリシーをデフォルトパスワードポリシーに変更したい場合は、「pwdPolicySubentry」属性を削除してください。

なお、ユーザーエントリに設定したパスワードポリシー内容の変更は LDAP 管理者によって実行する必要があります。ユーザー自身でパスワードポリシーの内容を変更することはできません。

9.3 パスワードポリシーの変更

設定済みのパスワードポリシーを変更したい場合、LDAP に登録されているパスワードポリシーエントリの内容を更新する必要があります。変更手順として、LDIF ファイルを用意して ldapmodify コマンドで変更する方法を説明します。

変更例として、連続認証失敗時のアカウントロックに関連するパラメーターの変更手順を説明します。新しいパスワードポリシーでは連続 5 回認証に失敗した場合に、30 分間アカウントロックを行うためのポリシーに変更します。

以下が実際の変更のための LDIF ファイル (change_ppolicy.ldif) です。dn の値には変更を行ないたいパスワードポリシーの dn の値や、ユーザーの dn の値を指定してください。

```
dn: cn=default,ou=policies,dc=example,dc=com
changetype: modify
replace:pwdLockout
pwdLockout: TRUE
-
replace:pwdMaxFailure
pwdMaxFailure: 5
-
replace: pwdLockoutDuration
pwdLockoutDuration: 1800
```

ldapmodify コマンドでパスワードポリシーの変更を行ないます。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f change_ppolicy.ldif \
;
```

9.4 パスワードポリシーを適用しないユーザー

ppolicy 機能でデフォルトパスワードポリシーを設定すると、rootdn のユーザー以外の全てのユーザーのパスワードポリシーが適用されます。例えば、管理用エントリや、複製用エントリなどデフォルトパスワードポリシーを適用しないエントリには、存在しないパスワードポリシーを指定することでパスワードポリシーを無効化します。

各管理用ユーザーごとに、以下の内容の LDIF ファイル (none_policy.ldif) を作成します。dn の値は対象となる各ユーザーの dn の値を指定してください。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
add: pwdPolicySubentry
pwdPolicySubentry: cn=none,ou=policies,dc=example,dc=com
```

なお「pwdPolicySubentry」に指定されている「cn=none,ou=policies,dc=example,dc=com」というエントリは LDAP に登録する必要はありません。

ldapmodify コマンドを実行し、各ユーザーのパスワードポリシーを適用します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f none_policy.ldif \
;
```

なお、OSS テクノロジの標準 LDAP サーバー構成では、パスワードの有効期限切れによる接続エラーを避けるため、以下の各エントリのパスワードポリシーを無効化することを推奨しています。

- LDAP サーバー管理者エントリ
  - 「cn=admin」など
- LDAP サーバー管理用エントリ
  - 複製用の「cn=replica」など
- 各アプリケーションからの LDAP 接続用エントリ
  - 「cn=unicornidm」など

9.5 OpenLDAP パスワードポリシーパラメーター詳細

9.5.1 アカウントロック

パスワードポリシーのアカウントロックに関連したパラメーターを説明します。

9.5.1.1 pwdLockout

「TRUE」を設定すると、認証に連続で失敗した際にアカウントをロックし、一定期間認証に成功しない状態にします。デフォルトではアカウントロックが行なわれている際にもアカウントがロックされていることを示すメッセージはクライアントに返しません。後述の「ppolicy_lockout オプション」に関する注意事項も参照してください。

デフォルト値は「FALSE」(アカウントをロックしない) です。

9.5.1.2 pwdMaxFailure

認証に連続して失敗した際に、アカウントロックが発動するまでの失敗回数を指定します。「0」を指定した場合、認証に何回失敗してもアカウントはロックされません。

デフォルト値は「0」です。

9.5.1.3 pwdFailureCountInterval

アカウントロックのための認証失敗回数を判定する有効期間 (秒) を設定します。

アカウントロックが有効な場合、ユーザーが認証に失敗するたびにそのユーザーのエントリに pwdFailureTime 属性として認証に失敗した時刻のエントリが追加されます。pwdFailureTime に記録される時刻は秒単位であるため、一秒間に記録できる認証失敗回数は 1 回に制限されます。

アカウントロックの判定は、認証時から pwdFailureCountInterval(秒) 前までの間に、pwdFailureTime 属性が何回記録されているかを確認し、pwdMaxFailure の回数以上が記録されている場合に、アカウントロックが有効なフラグを設定し、アカウントロック状態に遷移します。

また、pwdFailureCountInterval の値が「0」の場合は、有効期間が無限大として扱われ、最後の認証成功以降今までに認証失敗した履歴が全てカウントされます。

認証に失敗した後に、認証に成功すると pwdFailureTime 属性が削除され、認証失敗回数がリセットされます。

デフォルト値は「0」です。

9.5.1.4 pwdMaxRecordedFailure

以前の OpenLDAP では、認証に成功するまで pwdFailureTime 属性が無限に追加され、特定のエントリに大量の pwdFailureTime 属性が保存されることでシステムの動作に影響を及ぼすことがありました。そこで、pwdMaxRecordedFailure オプションが導入され、1 つのユーザーエントリに保存される pwdFailure 属性の最大の数が制限できるようになりました。

pwdMaxRecordedFailure の値が設定されていない場合の、デフォルト値は「5」です。また、pwdMaxFailure

より小さい値が設定されている場合、pwdMaxFailure の値が pwdMaxRecordedFailure の値として扱われます。

9.5.1.5 pwdLockoutDuration

アカウントがロックされてから、アカウントロックが解除されるまでの時間 (秒) を指定します。pwdLockoutDuration の値が「0」、もしくは設定されていない場合、アカウントロックは自動的に解除されず、管理者がアカウントロックを明示的に解除する必要があります。

9.5.2 パスワード有効期限

パスワードポリシーのパスワード有効期限関連パラメーターを説明します。

9.5.2.1 pwdMaxAge

パスワードの有効期間 (秒) を指定します。「0」を指定した場合はパスワードの有効期間は無期限となります。

デフォルト値は「0」です。

pwdMaxAge に 1 以上の値を設定すると、ユーザーが最後にパスワードを変更した時刻がユーザーエントリ内の pwdChangedTime 属性に記録されます。pwdChangedTime 属性に記録された時刻に、pwdMaxAge(秒) を足した時刻までがパスワードが有効な期間として扱われます。

pwdChangedTime 属性は以下の条件でユーザーエントリに記録されます。

- pwdMaxAge 属性に 1 以上の値を設定した後に、userPassword 属性を含むユーザーエントリを登録した場合
- pwdMaxAge 属性に 1 以上の値を設定した後に、既に登録されているユーザーエントリのパスワードを変更した場合

pwdMaxAge を 1 以上に設定する前から LDAP に登録されていたユーザーエントリについては、以下のいずれかの操作を実行するまで pwdChangedTime 属性が登録されず、パスワードの有効期限が適用されません。

- ユーザーのパスワードを変更する
- ユーザーエントリに pwdChangedTime 属性を追加する

pwdChangedTime 属性を明示的にユーザーエントリに追加する手順を説明します。

pwdChangedTime 属性を変更するための LDIF ファイルを作成します。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
replace: pwdChangedTime
```

```
pwdChangedTime: 20190724150133Z
```

pwdChangedTime は、GeneralizedTime 型と呼ばれる形式で UTC の時刻 (JST-9) で構成された文字列で、最後の文字が「Z」で終わります。

続いて、ldapmodify コマンドで LDIF データを登録します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -e relax \
  -f pwdchanged.ldif \
;
```

この操作に関して、以下の 2 点の注意が必要です。

- pwdChangedTime 属性は OpenLDAP の内部属性のため、-D オプションに指定する管理者に対して manage 権限が付与されている必要があります。slapd.conf ファイルの rootdn に指定したユーザー、もしくは ACL 設定で「manage」権が指定されているユーザーのみが pwdChangedTime 属性変更可能です。「write」権で内部属性を更新することはできません。
- ldapmodify オプションに「-e relax」オプションが必要です。

9.5.2.2 pwdMinAge

パスワードの変更禁止期間 (秒) を指定します。「0」を指定した場合は変更禁止期間は設けられません。パスワードの変更禁止期間を設けることで、ユーザーがパスワード変更をすぐに繰り返すことを防ぐことができ、パスワード変更履歴機能を回避することが難しくなります。

デフォルト値は「0」です。

本パラメーターに「1」以上の値を設定すると、最後にパスワードを変更した時刻がユーザーエントリ内の pwdChangedTime 属性に記録されます。pwdChangedTime 属性の役割は pwdMaxAge 属性を設定した場合と同じです。

9.5.2.3 pwdExpireWarning

パスワードの期限切れの事前警告期間 (秒) を指定します。「0」を指定した場合は警告は表示されません。警告メッセージは期限切れ 1 日前まで表示されます。

デフォルト値は「0」です。

本機能は BIND 成功時に LDAP クライアントにメッセージを返す機能ですが、実際にユーザーに事前警告

メッセージを表示するかどうかは LDAP クライアントの実装に依存します。

9.5.2.4 pwdGraceAuthnLimit

期限切れパスワードによる認証 (BIND) の最大猶予回数を指定します。「0」を指定した場合、猶予は設けられません。パスワードの期限が切れた後に BIND がこの回数以上失敗すると、BIND 不可 (Password expired) となります。

デフォルト値は 0 です。

9.5.3 パスワード変更時の強度検査

パスワード変更時の強度検査に関連したパラメーターを説明します。

9.5.3.1 pwdCheckQuality

パスワードの強度検査の有効化・無効化を指定します。設定値として以下の値を指定できます。

- 0: 検査しない (デフォルト値)
- 1: 検査する。検査が不可能な場合には検査せずに受け入れる
- 2: 検査する。検査が不可能な場合にはエラーとする

パスワードの変更手順としては、次の 2 種類があります。

1. クライアント側で「userPassword 属性」の値を作成し ldapmodify などで属性の値を直接更新する方法
2. クライアント側から「Password modify operation」により平文パスワードを送信し、サーバー側でハッシュ化して userPassword 属性に格納する方法

「検査が不可能な場合」とは、1 の手順を用いてクライアント側でパスワード文字列をハッシュ化済みの場合に発生します。この場合、サーバー側では元のパスワード文字列を得られないため、パスワードの強度を検査することができません。

9.5.3.2 pwdMinLength

パスワードの最小文字数を指定します。「0」を指定した場合、最小文字数の制限は行なわれません。「pwdCheckQuality」パラメーターの値が「2」または「1」の場合のみ有効となります。

デフォルト値は「0」です。

9.5.3.3 pwdMaxLength

パスワードの最大文字数を指定します。値を設定しない場合、最大文字数の制限は行なわれません。「pwdCheckQuality」パラメーターの値が「2」または「1」の場合のみ有効となります。

デフォルト値は指定無しです。

本パラメーターは osstech-openldap-2.4.57-178 以降のバージョンにて利用可能です。

9.5.3.4 pwdInHistory

パスワード履歴保持数を指定します。ユーザーが登録したパスワードは各ユーザーエントリの pwdHistory 属性に pwdInHistory に指定した数まで保存され、パスワード履歴としてチェックされます。「0」を指定した場合はパスワード履歴を記録しません。

デフォルト値は「0」です。

9.5.3.5 pwdCheckModule

OSSTech 版 OpenLDAP には拡張されたパスワード品質チェックモジュールが同梱されており、以下の手順で利用可能となります。

1. LDAP DIT のパスワードポリシーエントリに以下の属性を追加します。(pwdCheckModule と pwdCheckQuality 属性は、既存で設定済みであれば置き換えてください)

```
objectClass: pwdPolicyChecker
pwdCheckModule: ppolicy-pwdcheck.la
pwdCheckQuality: 2
```

2. ppolicy-pwdcheck 用の環境変数を設定します。(任意)

```
# echo 2 >/opt/osstech/var/lib/sv/slapd/env/PPOLICY_PWDCHECK_COMPLEX
# systemctl restart osstech-slapd
```

パスワード品質チェックモジュールは、slapd 起動時の環境変数で制御することができます。以下の環境変数名が用意されていますので、上記の手順で「/opt/osstech/var/lib/sv/slapd/env」配下に環境変数名のファイルを作成し、値をファイル内に設定してください。

- 環境変数名: PPOLICY_PWDCHECK_INTERNAL
  - 既定値：1 (有効)

  - 内蔵のパスワード品質チェック機能を利用するかどうかを設定します。 0 に設定すると無効化、それ以外の数値で有効化されます。
- 環境変数名: PPOLICY_PWDCHECK_LENGTH
  - 既定値：6
  - パスワードの長さに要求される最短の長さを設定します。これより短い長さのパスワードは拒否されます。
- 環境変数名:PPOLICY_PWDCHECK_COMPLEX
  - 既定値： 3
  - パスワードに含まれる文字種の数に求められる最小の数を設定します。これより少ない数の文字種しか含まないパスワードは拒否されます。英文字の大文字・小文字は別の種類として扱われます。
- 環境変数名: PPOLICY_PWDCHECK_ALPHABET
  - 既定値：0
  - パスワードに含まれる英文字の数に求められる最小の数を設定します。これより少ない数の英文字しか含まないパスワードは拒否されます。
- 環境変数名: PPOLICY_PWDCHECK_UPPER
  - 既定値：0
  - パスワードに含まれる英大文字の数に求められる最小の数を設定します。これより少ない数の英大文字しか含まないパスワードは拒否されます。
- 環境変数名:PPOLICY_PWDCHECK_LOWER
  - 既定値： 0
  - パスワードに含まれる英小文字の数に求められる最小の数を設定します。これより少ない数の英小大文字しか含まないパスワードは拒否されます。
- 環境変数名:PPOLICY_PWDCHECK_DIGIT
  - 既定値： 0
  - パスワードに含まれる数字の数に求められる最小の数を設定します。これより少ない数の数字しか含まないパスワードは拒否されます。
- 環境変数名: PPOLICY_PWDCHECK_SYMBOL
  - 既定値：0
  - パスワードに含まれる記号の数に求められる最小の数を設定します。これより少ない数の記号しか含まないパスワードは拒否されます。
- 環境変数名: PPOLICY_PWDCHECK_HAS_NO_ID
  - 既定値 : 0
  - 0 より大きい整数値を設定した場合、ユーザー名が含まれるパスワードは拒否されます。パスワード変更対象のユーザーの DN の RDN がユーザー名としてチェックに使われます。パスワードに含まれるユーザー名の大文字・小文字は区別されずチェックされます。
- 環境変数名: PPOLICY_PWDCHECK_COMMAND
  - 既定値 : なし
  - 上記機能で実現できないパスワードの品質をチェックするための外部コマンドを設定したい場合に利用します。指定したコマンドからの応答をもとに指定された新しいパスワードの許可・拒否を判定します。コマンドにコマンドライン引数を渡すことはできません。

* コマンドへの入力
  - 標準入力にパスワード変更対象の LDAP エントリの識別名 (DN) と改行文字、新しいパスワードと改行文字を渡します。
* コマンドからの出力
  - パスワードの強度に問題が無い場合は「OK」あるいは、「OK:任意の文字列」を返してください。
  - 問題がある場合はそれ以外の任意の文字列 (問題の内容) を返してください。コマンドの終了コードは無視されます。

9.5.4 その他

その他のパラメーターについて説明します。

9.5.4.1 pwdAllowUserChange

ユーザーによるパスワード変更の許可・禁止を指定します。設定値には「TRUE」か「FALSE」を指定します。「TRUE」はユーザーによるパスワード変更を許可することを意味します。

デフォルト値は「TRUE」です。

9.5.4.2 pwdMustChange

管理者によるパスワードリセット後、最初の BIND 直後にパスワードの変更を必須とするかどうか指定します。設定値として「TRUE」か「FALSE」を指定できます。「TRUE」を設定した場合、パスワード変更が要求されます。

デフォルト値は「FALSE」です。

9.5.4.3 pwdSafeModify

パスワード変更時に変更前のパスワードの入力が必要か不要か指定します。設定値として「TRUE」か「FALSE」を指定できます。「TRUE」を設定した場合、変更前のパスワードの入力が要求されます。

デフォルト値は「FALSE」です。

9.6 アカウントロックの運用について

ユーザーの認証時に失敗が繰り返される場合、適切にアカウントロックを行うことでパスワードの総当り攻撃を防ぐ効果が得られます。ただし、アカウントロックの状態をクライアントに返却することは、攻撃者に不要な情報を与えることにつながるため、認証時にユーザー名やパスワードを間違えている状態とアカウントロックされている状態がクライアントに区別がつかないことが望ましいといえます。

9.6.1 ppolicy_use_lockout オプション

slapd.conf ファイルで pplicy_use_lockout オプションを「on」に設定すると、BIND 時にアカウントロックが行なわれた場合に LDAP クライアントにアカウントロックのエラーを返す動作を有効化します。このエラーによりアカウントロックされていることが明確になるため、指定されたユーザー (DN) が存在することにより、悪意のある攻撃社がユーザーの存在確認に利用することができます。したがって、不特定多数からの接続を受け付ける環境などでセキュリティを重視する場合には、本パラメーターは有効にしないでください。

本番運用前に、アカウントロック動作が正しく動作していることを確認する場合には有用なパラメーターです。

9.6.2 アカウントロック状態の確認方法

slapd.conf ファイルに「ppolicy_use_lockout」オプションを記述した場合でも、Linux ホストへのログイン時にはアカウントロックに関するメッセージは表示されません。これはサーバーのセキュリティを向上させるための仕様となっています。

アカウントロックが行なわれているかどうか確認したい場合、ldapsearch コマンドで該当ユーザーのエントリで認証し、「-e ppolicy」オプションを付与します。該当ユーザーのアカウントがロックされている場合、次の実行例のように「Account locked」のメッセージが付与されます。

```
# /opt/osstech/bin/ldapsearch \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -e ppolicy \
;
Enter LDAP Password: ******** (正しいパスワード)
ldap_bind: Invalid credentials(49); Account locked
```

9.6.3 他のパスワードポリシーに抵触している状態でのアカウントロック

パスワードの有効期限が切れている状態で pwdMaxFailure で指定した回数だけ不正なパスワードを入力するとアカウントロック状態となります。認証失敗回数については、以下の挙動となります。

- パスワードの有効期限が切れた状態で、かつ、アカウントロックされていない状態の場合、正しいパスワードを入力すると認証失敗回数はリセットされます。
- パスワードの有効期限が切れた状態で、かつ、アカウントロックされている状態の場合、正しいパスワードを入力しても認証失敗回数はリセットされません。

9.7 アカウントロックの解除

認証に連続して失敗しアカウントがロックされた場合に、ロックを解除する方法を説明します。

アカウントロックの解除方法として、以下の 3 つの方法があります。

1. 一定時間経過後に自動的にアカウントロックを解除する
2. ユーザーのパスワードを変更する
3. ユーザーエントリに含まれるアカウントロック状態の属性を削除する

9.7.1 一定時間経過後に自動的にアカウントロックを解除する

「pwdLockoutDuration」属性にアカウントロック解除までの時間を設定します。

9.7.2 ユーザーのパスワードを変更する

管理者がユーザーのパスワードを変更することで、自動的にアカウントロックが解除されます。パスワード変更には ldappasswd コマンドなどを利用します。

9.7.3 ユーザーエントリに含まれるアカウントロック状態の属性を削除する

アカウントがロックされると、該当ユーザーのエントリに「pwdAccountLockedTime」という属性が保存されます。この属性にはアカウントがロックされた時刻が記録されています。この属性を削除することで、強制的にアカウントロックを解除することができます。削除の手順は以下の通りです。

該当ユーザーの pwdAccountLockedTime 属性を削除する内容の LDIF ファイルを作成します。dn の値には、該当ユーザーの dn を指定してください。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
delete: pwdAccountLockedTime
```

ldapmodify コマンドで作成した LDIF を適用します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -f LDIF ファイル \
;
Enter LDAP Password: *******  ← admin のパスワード
```

以上の操作でアカウントロックが解除されます。

逆に、ユーザーエントリに pwdAccountLockedTime 属性を登録することで、特定のユーザーを意図的にアカウントロックすることも可能です。pwdAccountLockedTime にはアカウントロックされた時刻を Generalized-Time 型 (UTC) で保存します。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
add: pwdAccountLockedTime
pwdAccontLockedTime: 20190724173701Z
```

9.7.4 認証失敗回数のリセット方法

pwdAccountLockedTime 属性を削除することでアカウントロックの状態は解除されますが、認証失敗回数を保持する pwdFailureTime 属性は削除されていません。そのため、pwdAccountLockedTime 属性を削除した直後に、ユーザーが認証に失敗すると、認証失敗回数の上限を超えるため、再びアカウントがロックされます。

認証失敗回数をリセットするためには、次のいずれかの操作を行ないます。

1. 一定時間経過後に認証失敗回数をリセットする
2. アカウントロック解除後に正しいパスワードで認証に成功する
3. pwdFailureTime 属性を削除する

9.7.4.1 一定時間経過後に認証失敗回数をリセットする

アカウントロックのリセット後にも「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許す場合は、「pwdFailureCountInterval」属性を設定します。この属性には認証失敗回数がリセットされるまでの期間 (秒) を指定します。そのため、以下のような基準から設定値を決定します。

- pwdLockoutDuration 属性で指定した時間と同じか、それよりも短い時間
  - 一定時間経過後に自動的にアカウントロックが解除された後に、「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許可するため
- アカウントロック発生 →管理者により強制的アカウントロック解除」に要する時間よりも短い時間
  - 管理者による強制的アカウントロック解除後に、「pwdMaxFailure」で指定した認証失敗回数分のパスワード入力ミスを許可するため

9.7.4.2 アカウントロック解除後に正しいパスワードで認証に成功する

該当ユーザーの DN を使って正しいパスワードで認証 (BIND) に成功すると、pwdFailureTime 属性が自動的に削除され、認証失敗回数がリセットされます。

9.7.4.3 pwdFailureTime 属性を削除する

管理者により pwdFailureTime 属性を削除することで認証失敗回数をリセットできます。この属性は rootdn に指定されたアカウントか、manage 権限を持つアカウントからのみ削除が可能です。また、削除時に relax rules control を指定する必要があります。

relax rules control の指定方法として、次の 2 つの方法があります。

1. -e relax オプションで操作する場合

次の内容の LDIF ファイルを作成します。dn には、該当ユーザーの dn を指定してください。

```
dn: uid=username,ou=Users,dc=example,dc=com
changetype: modify
delete: pwdFailureTime
```

ldapmodify コマンドで LDIF を適用します。接続用 DN には rootdn のユーザーか、manage 権を有する管理者の DN を指定し、オプションとして「-e relax」を指定します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -e relax \
  -f LDIF ファイル \
;
```

2. LDIF に relax rules control を指定する場合

次の内容の LDIF ファイルを作成します。dn には、該当ユーザーの dn を指定してください。

```
dn: uid=username,ou=Users,dc=example,dc=com
control: 1.3.6.1.4.1.4203.666.5.12
changetype: modify
delete: pwdFailureTime
```

ldapmodify コマンドで LDIF を適用します。接続用 DN には rootdn のユーザーか、manage 権を有する管理者の DN を指定します。

```
# /opt/osstech/bin/ldapmodify \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
```

```
  -f LDIF ファイル \
;
```

9.7.5 パスワードポリシーレスポンス詳細

OpenLDAP でパスワードポリシーを有効化した場合に、OpenLDAP サーバーが返すレスポンスについて説明します。

OpenLDAP の ppolicy が返す応答コントロールの LDAP Control Type は「1.3.6.1.4.1.42.2.27.8.5.1」となります。パスワードポリシーに抵触して BIND に失敗した場合のレスポンスはいずれも「Invalid credentials(49)」となります。以下の表に、各パスワードポリシーに違反した場合の LDAP Control Value を記します。

エラーの原因	応答コントロール
認証成功時	無し
パスワード間違いによる認証失敗	無し
パスワード有効期限切れ	error: passwordExpired(0)
アカウントロックアウト	error: accountLocked(1)
次回ログイン時のパスワード変更必要	error:changeAfterReset(2)

9.7.6 ppolicy_hash_cleartext オプション

パスワード変更時に、LDAP の Password modify extended operation(ldappasswd の方式) に従ってパスワード変更を行うと、LDAP サーバー側で slapd.conf ファイルの password-hash パラメーターに設定されたハッシュアルゴリズムでハッシュ化して userPassword 属性にパスワードを格納します。

一方、LDAP の add や modify といった通常の LDAP 更新リクエストにより userPassword を変更する場合、LDAP サーバー側はパスワード情報が平文パスワードであってもそのまま userPassword 属性に保存します。このように平文パスワードを指定して add や modify が行なわれた場合に、LDAP サーバー側で特別にパスワードのみを自動的にハッシュ化して保存するためのオプションが ppolicy_hash_cleartext パラメーターです。

```
ppolicy_hash_cleartext on
```

上記のようにこのパラメーターを on にすることで平文パスワードを自動的に password-hash パラメーターに指定されたハッシュアルゴリズムで変換して userPassword 属性に保存する機能が有効になります。

ただし、この動作は LDAP の仕様上は認められていないため、平文パスワードを送信したクライアントは、userPassword 属性に平文パスワードが入っていることを想定して動作している可能性があり、アプリケーションの動作に不具合が発生する可能性もあります。したがって、本オプションを利用する場合は、on に設定後、パスワード更新処理関連において十分な動作検証を実施してから利用してください。

10 OpenLDAP psync モジュール

psync モジュールは、OSS テクノロジが開発した OpenLDAP と Active Directory のユーザーのパスワードを自動的に同期するためのモジュールです。ユーザー名キーとして、OpenLDAP 側でのパスワード変更、Active Directory 側でのパスワード変更を同期します。

本モジュールの実装上の制約として、LDAP スレーブサーバーが存在する場合、本モジュールを適切に利用することはできません。必ず LDAP マスターサーバーのみの構成でご利用ください。

10.1 事前準備

本モジュールを利用する際に、Active Directory サーバーにモジュール等を追加する必要はありませんが、Active Directory サーバーに LDAP サーバーから LDAPS(636/TCP) ポート経由でパスワード更新を行うため、LDAPS 通信を許可するために Active Directory サーバーにサーバー証明書の設定、もしくは証明書機関の導入が必要となります。

10.2 psync モジュールの設定

psync モジュールは OSSTech 版 OpenLDAP の rpm パッケージに含まれています。次の手順で設定を行ってください。

psync はパスワードの同期処理で LDAP の userPassword 属性を更新する際に、global ディレクティブに設定された password-hash パラメーターに従って動作します。password-hash パラメーターが設定されていない場合、デフォルトとして'{SSHA}'(Salt 付き SHA-1) としてハッシュ化が行なわれます。

psync モジュールには、以下のパラメーターが用意されています。

- psync-uri
  - Active Directory サーバーの LDAP URI を指定します。必ず ldaps:// の URI を指定します。
- psync-binddn
  - Active Directory に接続する際の管理者の DN を指定します。
- psync-credentials
  - psync-binddn に指定した DN のパスワードを平文で指定します。
- psync-searchbase
  - Active Directory 上の同期対象ユーザーを検索する際の LDAP の search base を指定します。
- psync-userkey(オプション)
  - OpenLDAP 上の同期対象のユーザーを検索する際のユーザーの RDN の属性名を指定します。
  - デフォルト値は「uid」です。

上記の各パラメーターは同期対象ユーザーが格納されている database ディレクティブ内に記載します。

slapd.conf ファイルの各設定値の設定例を示します。

```
moduleload psync
overlay psync
...
database bdb
...
psync-uri ldaps://ad1.example.com/
psync-binddn "cn=Administrator,cn=Users,dc=example,dc=com"
psync-credentials "adminpassword"
psync-searchbase "CN=Users,dc=example,dc=com"
```

psync モジュールを syncprov モジュールと同時に利用する場合、複製処理の関係で、overlay syncprov の設定よりも後に overlay psync を記載してください。また、他の overlay もある場合、一番最後に overlay psync を記載してください。

10.3 Active Directory サーバーのサーバー証明書の配置

psync モジュールでは、OpenLDAP 側でパスワード変更が発生した際に、Active Directory サーバーの LDAPS(636/TCP) ポートに LDAP プロトコルでパスワード変更要求を行ないます。この際に TLS 接続のため、Active Directory のサーバー証明書の検証が行なわれます。

したがって、Active Directory サーバーのサーバー証明書を/etc/openldap/ldap.conf の TLS_CACERTDIR のディレクトリに配置するか、もしくは TLS_CACERT に指定されたファイルにサーバー証明書の内容を含める必要があります。

```
TLS_CACERTDIR /etc/openldap/certs
```

10.4 ログ設定

psync モジュールのログは、loglevel に 0x10000 を追加することで slapd から syslog に記録が行なわれます。

```
loglevel stats 0x10000
```

11 LDAP サーバーの運用

11.1 サービスの起動・停止

11.1.1 LDAP サービス起動手順

root ユーザーで LDAP サーバーにログインし、ターミナルで次のコマンドを実行してください。

```
# systemctl start osstech-slapd
```

次のコマンドで Active の欄が「active(running)」となることを確認します。

```
# systemctl status osstech-slapd
● osstech-slapd.service - OSSTech OpenLDAP Server
   Loaded: loaded (/usr/lib/systemd/system/osstech-slapd.service; enabled;
vendor preset: disabled)
   Active: active (running) since 水 2019-07-24 15:46:53 JST; 10s ago
 Main PID: 12387 (slapd)
```

11.1.2 LDAP サービス停止手順

root ユーザーで LDAP サーバーにログインし、ターミナルで次のコマンドを実行してください。

```
# systemctl stop osstech-slapd
```

次のコマンドで Active の欄が「inactive(dead)」になることを確認します。

```
# systemctl status osstech-slapd
● osstech-slapd.service - OSSTech OpenLDAP Server
   Loaded: loaded (/usr/lib/systemd/system/osstech-slapd.service; enabled;
vendor preset: disabled)
   Active: inactive (dead) since 水 2019-07-24 15:49:07 JST; 4s ago
```

11.1.3 LDAP サービス再起動手順

root ユーザーで LDAP サーバーにログインし、ターミナルで次のコマンドを実行してください。

```
# systemctl restart osstech-slapd
```

Active の欄が「active(running)」になることを確認します。

```
# systemctl status osstech-slapd
● osstech-slapd.service - OSSTech OpenLDAP Server
   Loaded: loaded (/usr/lib/systemd/system/osstech-slapd.service; enabled;
vendor preset: disabled)
   Active: active (running) since 水 2019-07-24 15:50:40 JST; 5s ago
```

11.1.4 LDAP サービス実行状況確認手順

root ユーザーで LDAP サーバーにログインし、ターミナルで次のコマンドを実行してください。

```
# systemctl status osstech-slapd
```

LDAP サービスが起動している場合、Active の欄に「active(running)」のメッセージが表示されます。

```
# systemctl status osstech-slapd
● osstech-slapd.service - OSSTech OpenLDAP Server
   Loaded: loaded (/usr/lib/systemd/system/osstech-slapd.service; enabled;
vendor preset: disabled)
   Active: active (running) since 水 2019-07-24 15:46:53 JST; 10s ago
 Main PID: 12387 (slapd)
```

また、LDAP サービス稼働中に pgrep コマンドで確認すると、slapd プロセスが次の形式で表示されます。

```
# pgrep -a slapd
889 /opt/osstech/sbin/slapd -d none -f /opt/osstech/etc/openldap/slapd.conf ...
```

LDAP サービスが停止している場合、Active の欄に「inactive(dead)」のメッセージが表示されます。

```
# systemctl status osstech-slapd
● osstech-slapd.service - OSSTech OpenLDAP Server
   Loaded: loaded (/usr/lib/systemd/system/osstech-slapd.service; enabled;
vendor preset: disabled)
   Active: inactive (dead) since 水 2019-07-24 15:49:07 JST; 4s ago
```

11.1.5 LDAP サービスの自動起動設定

OS 起動時に LDAP サービスが自動で起動するために、以下のコマンドを実行します。

```
# systemctl enable osstech-slapd
```

自動起動が設定されているか確認したい時は、以下のコマンドを実行します。

```
# systemctl is-enabled osstech-slapd
enabled
```

- 「enabled」 … 自動起動が有効
- 「disabled」… 自動起動が無効

自動起動を無効にしたいときは、以下のコマンドを実行します。

```
# systemctl disable osstech-slapd
```

11.2 ユーザーエントリのパスワード変更

LDAP に登録されている管理用/複製処理用のエントリや、別システムからの接続用のエントリのパスワードを変更する場合、ldappasswd コマンドで行ないます。

```
# /opt/osstech/bin/ldappasswd \
  -H ldaps://<ホスト名> \
  -x \
  -W \
  -D <管理用エントリの DN> \
  -S \
  <変更対象エントリの DN> \
New password: <変更対象エントリの新しいパスワードを入力>
Re-enter new password: <変更対象エントリの新しいパスワードを入力>
Enter LDAP Password: <管理用エントリのパスワードを入力>
```

「管理用エントリの DN」にパスワードの更新権を持つ LDAP 管理用エントリ (例: cn=admin,dc=example,dc=com) を指定します。

「変更対象エントリの DN」部分にパスワード変更対象エントリの DN を指定します。

11.3 ログ設定

OpenLDAP は、slapd.conf の loglevel パラメーターに基づき、ログメッセージを syslog 経由で出力します。ログレベルは、loglevel パラメーターに以下のキーワードの組み合わせで設定します。

ログレベル	意味
trace	関数呼び出しのトレース
args	詳細なトレース
conns	コネクション管理のログ

ログレベル	意味
filter	検索フィルター処理のログ
config	設定ファイルの解析ログ
ACL	アクセスコントロールのログ
stats	接続状況、リクエストのログ
stats2	クライアントに対して送信したエントリのログ
parse	エントリ解析のログ
sync	複製処理のログ
none	ログレベルに関係なく記録される重要なログ以外は記録しない
any	全てのログを記録する

複数のログの対象を記録したい場合は、複数のキーワードを空白区切りで指定します。ただし、OpenLDAP の stats 以外のログに関しては、デバッグログに近いレベルで多くのログが出力され、LDAP サービスの性能低下につながるため、通常は設定する必要はありません。

OpenLDAP の slapd はデフォルトで facility の local4 として syslog にログを出力しますが、OSSTech 版 OpenLDAP のログファイルの出力先は/opt/osstech/etc/rsyslog.d/slapd.conf ファイルに設定されており、デフォルトでは「/var/log/osstech/ldap.log」となっています。

```
if $programname == 'slapd' then \
-/var/log/osstech/ldap.log
& stop
```

ログファイルの保存先を変更した場合は、rsyslogd を再起動してください。

```
# systemctl restart rsyslog
```

11.3.1 ログローテート設定

OSSTech 版 OpenLDAP のログファイルのログローテート設定は、osstech-base パッケージが提供する/opt/osstech/etc/logrotate.d/syslog ファイルにより設定されています。

標準では以下のローテート内容が設定されています。

パラメーター	設定値
世代数	100 世代
取得タイミング	毎日 AM3 時頃

/opt/osstech/etc/logrotate.d/syslog ファイルを更新すると、次回のログローテート時から反映されます。

11.3.2 LDAP ログの見方

OpenLDAP の「stats」レベルのログは、次の形式で記録され、LDAP にアクセスするクライアントの情報を取得することができます。

```
conn=1002 fd=13 ACCEPT from IP=127.0.0.1:57671 (IP=0.0.0.0:389)
conn=1002 op=0 BIND dn="cn=admin,dc=example,dc=com" method=128
conn=1002 op=0 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE ssf=0
conn=1002 op=0 RESULT tag=97 err=0 text=
conn=1002 op=1 ADD dn="cn=user1,dc=example,dc=com"
```

以下のような情報を含みます。

- LDAP 接続の識別子 (conn=<ID>)
- LDAP クライアントの IP アドレス (ACCEPT from IP=<IP **アドレス**>:<**ポート番号**>)
- LDAP クライアントの接続ユーザーの DN (BIND dn="<DN>")
- LDAP 操作 (リクエストと結果) の識別子 (op=<ID>)
- LDAP 操作の種別
  - 接続 (ACCEPT)
  - 認証 (BIND)
  - 検索 (SRCH)
  - 追加 (ADD)
  - 変更 (MOD)
  - 削除 (DEL)
  - そのほか
- LDAP 操作の結果と LDAP エラーコード (RESULT ... err=<**エラーコード**>)
  - LDAP エラーコード 0 は成功を意味する。
  - 検索結果の場合はエントリ数も含む。(SEARCH RESULT ... nentries=<**エントリ数**>)

通常時でも次のようなログが記録されることがあります。これ以外のログメッセージの場合はサポートにお問合せください。

- connection_read(<**番号**>): no connection!
  - LDAP サーバーがリクエストを受信しようとした際に LDAP クライアントが既に LDAP 接続を切断していたことを示します。
  - LDAP クライアントが正式な手順で切断処理を行なっていない場合に発生することがあります。
  - 通常は問題ありません。

以下のログは発生頻度や負荷状況などによりますが、パフォーマンス劣化が生じている可能性があります。発生頻度が少なくクライアント側のサービスの応答・動作に影響がなければ通常は無視して構いません。

- `deferring operation: too many executing`
  - 複数の LDAP クライアントから短時間に大量の LDAP リクエストを受けた結果、リクエストを処理するスレッドが不足して処理が待たされたときに記録されます。
  - スレッドに空きができれば該当リクエストの処理が通常どおり行なわれます。
- `deferring operation: awaiting write`
  - 直前のリクエストの処理結果がクライアントに返されるのを待つためにリクエストの処理が遅延されています。
- `bdb_equality_candidates: <`**属性名**`> not indexed`
  - LDAP 検索のフィルターに指定された属性がインデックスを持たない場合に記録されます。
- `=> <`**内部処理内容**`> failed: DB_LOCK_DEADLOCK: Locker killed to resolve a deadlock`
  - OpenLDAP サーバーのバックエンドデータベース Berkeley DB (BDB) がデッドロックを検知し、それを解消するためにデッドロック状態のスレッドを停止したことを示します。
  - 通常、この後に LDAP アクセスログ `conn=<`**接続** `ID> op=<`**操作** `ID>: <`**操作内容**`> failure` が続きます。
  - 停止されたスレッドが受け持っていた操作は新たなスレッドで再試行され, 操作が成功するまで繰り返されます。(操作をキャンセルするわけではありません)

11.3.3 LDAP ログの監視

OpenLDAP では、エラーメッセージが系統立てられておらず、各メッセージにログ監視の抽出に利用できるキーワードが含まれていません。

一方、loglevel stats(256) で運用している場合、操作リクエストのログには下記の特定のキーワードが含まれるため、これらのキーワードを含まないようなメッセージが出力されている場合に、エラーメッセージの可能性があります。

```
ACCEPT,BIND,SRCH,SEARCH,ADD,MOD,DEL,MODRDN,RESULT,PASSMOD,STARTTLS,closed
```

そのため、メッセージ監視の際は上記のキーワードを含まないメッセージを監視することを推奨します。

11.3.4 ログメッセージの Rate Limit 設定について

RHEL7 以降の環境では、一定期間に大量のログメッセージが記録された場合、ログ出力を省略する Rate Limit 設定が行なわれています。

LDAP サーバーでは、多数のクライアントからのアクセスによって、認証や検索時に大量のログが記録される場合がありますので、ログメッセージの欠落を防ぐため Rate Limit 設定を無効化しておくことを推奨します。

OSSTech 版 OpenLDAP パッケージをインストールすると、Rate Limit 設定が無効化されるように下記の設定が行なわれています。

11.3.4.1 journald の Rate Limit 設定

弊社提供の OpenLDAP パッケージを導入した場合、osstech-base パッケージに含まれる/etc/systemd/journald.conf.d/osstech.conf ファイルに、journald の Rate Limit を無効化する設定が含まれています。

```
[Journal]
RateLimitInterval=0
```

11.3.5 rsyslog の Rate Limit 設定 (RHEL7 のみ)

弊社提供の OpenLDAP パッケージを導入した場合、osstech-base パッケージに含まれる/etc/rsyslog.d/osstech.conf ファイルに、rsyslogd の Rate Limit を無効化する設定が含まれています。

```
$SystemLogRateLimitInterval 0
$imjournalRatelimitInterval 0
```

11.4 バックアップ

OSSTech 版 OpenLDAP 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自動的に取得することができます。

項目	設定値
バックアップ対象	LDAP サーバーの DIT に登録されている全データ
保存ディレクトリ	/var/opt/osstech/backup/ldap
バックアップファイル名	dc=example,dc=com.ldif.gz (ファイル名は LDAP の DIT に基づく)
バックアップ頻度	毎日 AM 5 時 30 分
バックアップ世代数	30 世代

OpenLDAP の設定ファイルなどはバックアップ対象に含まれていませんので、別途必要に応じてバックアップを実施してください。

LDAP のバックアップスクリプトは、osstech-openldap-servers パッケージインストール時に、cron で毎日 AM 5 時 30 分に実行されるように、/opt/osstech/etc/cron.d/slapdbbackup ファイルとして設定されます。

バックアップ取得の時間を変更したい場合は、この設定ファイルを変更してください。

```
SHELL=/bin/sh
30 5 * * * ldap test -x /opt/osstech/sbin/slapdbbackup &&
/opt/osstech/sbin/slapdbbackup (1 行で)
```

バックアップの世代数を変更したい場合、/opt/osstech/etc/openldap/slapdbbackup.conf ファイルの「backup_maxage」の数値を変更してください。

```
backup_maxage="30"
```

11.4.1 WiredTiger バックエンドでのバックアップ取得

WiredTiger バックエンドでは LDAP サーバー稼働中に slapcat コマンドによるオンラインでの LDIF の取得ができません。そのため、OSSTech 提供のバックアップスクリプトでは、WiredTiger バックエンド利用の際には、slapcat コマンドの代わりに ldapsearch コマンドによる全エントリの取得を行ないます。

バックアップのために ldapsearch コマンドでエントリを取得する際に、ldap ユーザー権限で ldapi:/// 経由で LDAP データにアクセスします。

そのため、WiredTiger バックエンド利用時に自動的にバックアップを取得するため、以下の limit 設定とアクセス権の設定を slapd.conf ファイルに追加してください。

```
limits dn="gidNumber=55+uidNumber=55,cn=peercred,cn=external,cn=auth"
       time=unlimited
       size=unlimited
```

```
access to *
       by dn="gidNumber=55+uidNumber=55,cn=peercred,cn=external,cn=auth" read
       by * break
```

なお、上記設定の uidNumber と gidNumber に指定した数値「55」は、LDAP サーバーの OS に登録された ldap ユーザーの UID / GID の値を指定してください。それぞれの値の確認は id コマンドで可能です。

```
# id ldap
uid=55(ldap) gid=55(ldap) groups=55(ldap)
```

11.5 リストア

OpenLDAP 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、障害などによりデータファイルが破損することがあります。

データファイルが破損してしまった場合は、以下の方法で復旧してください。

11.5.1 BDB バックエンドの整合性復旧

BDB バックエンドを利用している際に、slapd プロセスが異常終了した場合など、正常な終了処理が行えなかった場合に、データファイルの内容が一部破損し、データファイルを自動的に復旧できないことがあります。

slapd サービスが起動できない場合など、正常に LDAP サービスが稼働しない場合、障害が発生しているサーバー上で次の手順により復旧を試してください。

最初に出た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の復旧を行ないます。

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

インデックスの再構築を行ないます。

```
# sudo -u ldap /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
```

OpenLDAP サービスを起動します。

```
# systemctl start osstech-slapd
```

OpenLDAP 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、復旧に成功しています。この手順を実施しても復旧不可能な場合は、次の手順を実施してください

11.5.2 データ複製による LDAP データのリストア

複数台のサーバー構成時、障害が発生した LDAP サーバーとは別に、正常に稼働している LDAP マスターサーバーが残っている場合、複製機能を利用して障害が発生した LDAP サーバーのデータを復旧することができます。

複製機能を正しく設定している状態であれば、以下の手順で LDAP データを再同期することで最新の LDAP データにリストアすることができます。

障害が発生したサーバーの LDAP サービスを停止します。

```
# systemctl stop osstech-slapd
```

現在のデータのバックアップを取得しておきます。

```
# cp -rp /opt/osstech/var/lib/ldap /opt/osstech/var/lib/ldap-`date +%Y%m%d`
```

障害が発生したサーバーのデータファイルを削除し、LDAP サービスを起動します。

```
# rm -rf /opt/osstech/var/lib/ldap/*
# systemctl start osstech-slapd
```

リストア手順は以上となります。

正常な LDAP サーバーとリストアした LDAP サーバーのエントリを比較することで、複製が完了していることを確認してください。

```
# /opt/osstech/bin/ldapsearch \
  -h ldap1 \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
>ldap1.ldif
Enter LDAP Password: ********
# /opt/osstech/bin/ldapsearch \
  -h ldap2 \
  -x \
  -W \
  -D cn=admin,dc=example,dc=com \
  -b dc=example,dc=com \
>ldap2.ldif
Enter LDAP Password: ********
# diff -u ldap1.ldif ldap2.ldif
```

ldapsearch コマンドの「-D オプション」には、LDAP 管理用エントリの DN を指定します。

パスワード入力を求められますので、-D オプションに指定した管理用エントリのパスワードを入力します。

LDAP データの複製が完了するまで、エントリ数によっては多少時間がかかる場合があります。

11.5.3 バックアップファイルからのフルリストア

マルチマスター構成の両方のサーバーに障害が発生しデータが復旧できない場合や、シングル構成の場合には、バックアップファイルからのフルリストアによる LDAP データの復旧を行ないます。

まず最初に全 LDAP サーバーの LDAP サービスを停止します。

```
# systemctl stop osstech-slapd
```

LDAP マスター 1 号機にて、以下の手順で LDAP データの復旧を行ないます。

念の為、現在の LDAP データを別ディレクトリに移動します。

```
# cp -rp /opt/osstech/var/lib/ldap /opt/osstech/var/lib/ldap-`date +%Y%m%d`
# rm -rf /opt/osstech/var/lib/ldap/*
```

復旧に利用する LDIF ファイルは、バックアップとして取得している LDIF ファイル (/opt/osstech/var/backup/ldap/<LDAP suffix>.ldif.gz) を利用します。

```
# zcat /opt/osstech/var/backup/ldap/dc=example,dc=com.ldif.gz \
  |/opt/osstech/sbin/slapadd -vw
# chown -hR ldap: /opt/osstech/var/lib/ldap
# systemctl start osstech-slapd
```

LDAP サービスの再起動が完了したら、シングル構成の場合は復旧作業は完了です。

マルチマスター構成の場合は、LDAP マスター 2 号機を「データ複製による LDAP データのリストア」の手順に従い復旧を行ないます。

LDAP スレーブサーバーについても、LDAP マスターサーバーの復旧完了後、「データ複製による LDAP データのリストア」の手順に従い復旧することができます。

11.6 証明書ファイルの更新

証明書ファイルの更新時、TLSCertificateFile(サーバー証明書)、TLSCertificateKeyFile(秘密鍵ファイル) に設定されている証明書ファイルを新しいファイルに更新してください。

```
TLSCertificateFile /opt/osstech/etc/openldap/certs/ldap1.crt
TLSCertificateKeyFile /opt/osstech/etc/openldap/private/ldap1.key
```

中間 CA 証明書が更新される場合は、TLSCACertificateFile パラメーターに指定されているファイルも更新してください。

```
TLSCACertificateFile /opt/osstech/etc/openldap/certs/ca.crt
```

ファイルの更新後、LDAP サービスを起動して証明書ファイルの更新は完了です。

```
# systemctl restart osstech-slapd
```

なお、複数台構成の場合、複製の通信に利用するため、複製先 (複製元) のサーバーのサーバー証明書を設定していることがあります。

この場合、複製の関連先に設定されているサーバー証明書を新しいファイルに更新し、LDAP サービスの再起動を実施してください。

11.7 各種コマンド、設定ファイルの man データの確認

OSSTech 版 OpenLDAP パッケージに含まれる各コマンドや設定ファイルの man データの参照は osstech-man コマンドで行ないます。

```
$ /opt/osstech/bin/osstech-man <参照したいコマンド等>
```

例えば、ldapsearch コマンドの man データの確認は次のコマンドで行ないます。

```
$ /opt/osstech/bin/osstech-man ldapsearch
```

11.8 LDAP 運用時の便利なコマンド

OSSTech 版 OpenLDAP では、LDAP の運用に役立つ次のコマンドを提供しています。

- ldifdiff
- ldifunwrap
- ldifunbase64
- ldifsort
- ldifsortattr

11.8.1 ldifdiff コマンド

ldifdiff コマンドは、LDIF ファイルのエントリや属性の順序を無視して、2 つの LDIF ファイルを比較します。

LDIF ファイルと LDIF ファイルに含まれているエントリの内容を比較したい場合、通常は含まれているエントリの出力順序は定まっていないため、diff コマンドでは内容を簡単に比較することができません。

そこで、ldifdiff コマンドを利用することで、LDIF のエントリ単位での比較が可能となります。

```
# /opt/osstech/bin/ldifdiff 1.ldif 2.ldif
```

11.8.2 ldifunwrap コマンド

ldifunwrap コマンドは、ldapsearch による LDIF 取得時に “-o ldif-wrap=no” オプションを付け忘れて自動的に改行が行なわれた LDIF ファイルに対して、改行を取り除く処理が可能です。

```
# /opt/osstech/bin/ldifunwrap backup.ldif > backup_new.ldif
```

11.8.3 ldifunbase64 コマンド

ldifunbase64 コマンドは、LDIF ファイル中に含まれる BASE64 化された値を、デコードして出力します。

LDAP では ASCII 以外の文字を格納する際に、値を BASE64 でエンコードして格納します。そして、ldapsearch コマンドは、BASE64 でエンコードされたデータをそのまま出力します。(属性名の後が “::” になります)

下記の実行例では、sn と givenName の値が BASE64 でエンコードされています。

```
# /opt/osstech/bin/ldapsearch -x cn=yamada
dn: cn=yamada,ou=Users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
cn: yamada
sn:: 5bGx55Sw
givenName:: 5aSq6YOO
```

BASE64 化された値をデコードするには、base64 コマンドの-d オプションを使うことができます。

```
# echo 5bGx55Sw | base64 -d
山田
```

しかし LDIF 中に大量に現れる BASE64 文字列を一つずつ変換するのは大変なため、代わりに ldifunbase64 コマンドにより一括で変換することが可能です。

また、このコマンドで変換した結果は、LDIF の仕様に基づいたままの出力結果ですので、そのまま ldapmodify などのコマンドに LDIF ファイルとして利用することができます。

```
# /opt/osstech/bin/ldapsearch -x cn=yamada | /opt/osstech/bin/ldifunbase64
dn: cn=yamada,ou=Users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
cn: yamada
sn: 山田
givenName: 太郎
```

11.8.4 ldifsort コマンド

ldifsort コマンドは LDIF 中の DN の値をキーに、LDIF のエントリを並べ替えます。

LDAP では出力されるエントリの順番は不定のため、ldapsearch コマンドで取得した LDIF の結果はソートされていません。(上位のツリーが先に出力されるというツリー構造に従った順番は維持されます)

DN の値に従って LDIF のエントリを並び替えたい場合に ldifsort コマンドを使うことができます。

```
# /opt/osstech/bin/ldifsort allentry.ldif
```

11.8.5 ldifsortattr コマンド

ldifsortattr コマンドは、LDIF 内のエントリごとに属性名のアルファベット順に従って、並べ替えます。

LDAP では、1 エントリ内のデータに含まれる属性名の順序は不定です。そのため、ldapsearch コマンドでエントリを取得すると、エントリごとに属性名の並びはばらばらになります。

そこで、ldifsortattr コマンドを使って、エントリ内の属性を順番に並べ替えることができます。

```
# /opt/osstech/bin/ldifsortattr allentry.ldif
```