LDAPまとめ

Chihiro Ito(伊藤 智博)
twitter:chirokings
http://chirokings.blogspot.com/
http://www.chirokings.com/

LDAPとは

Lightweight Directory Access Protocol

ITU-T

X.500 DAP

高機能
運用コスト高
開発コスト高

軽量化

IETF

LDAP

90%の機能
10%のコスト

- プロトコルスタックの簡素化（OSI階層モデル->TCP/IP）
- 機能の簡略化（豊富な機能->9つの操作）
- データ表現形式の簡素化（複雑な構造->簡素）

RFC1777

ver.2

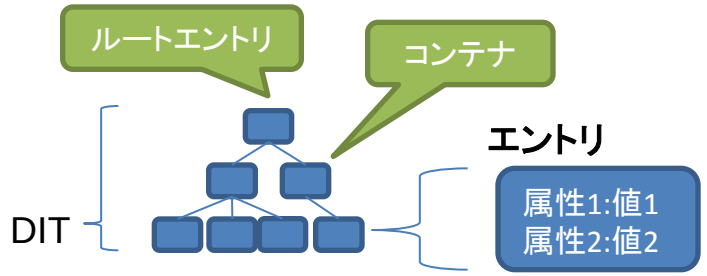
RFC2251-2256

ver.3

SASL,TLS認証
Unicode
パフォーマンス向上

LDAPの9機能

操作	説明
バインド	LDAPセッションの開始
アンバインド	LDAPセッションの終了
検索	検索条件に一致するエントリの検索
追加	新規エントリの追加
更新	エントリの属性値の追加・更新・削除
削除	エントリの削除
改名	エントリ識別名(DN)の変更
比較	エントリ内の属性値の比較
放棄	要求中のLDAP操作の放棄



(Directory Information Tree)

属性

必須属性
オプション属性
名前属性

属性1 ： 値1

属性名　属性値

オブジェクトクラスの型

形式	説明
構造型	STRUCTURAL 1つ以上必要
抽象型	ABSTRACT 直接使用できない
補助型	AUXILIARY 単独では使用できない

主な属性名

属性名	説明
cn	一般名(common name)
sn	名字(surname)
gn	名前(given name)
o	組織名(organization name)
ou	組織単位名(organizational unit name)
dc	ドメイン要素(domain component)

Open LDAP

ライセンス
OpenLDAP Public License

ソースからのインストール方法
./configure
make depend
make
make install

ログ
syslogのlocal4ファシリティ

利用ポート
LDAP:TCP389
LDAPS:TCP636

クライアント側設定ファイル
NSS用：/etc/ldap.conf
Ldap系コマンド用：/etc/openldap/ldap.conf

configureオプション例(ver.2.4.25)

オプション	説明	デフォルト
--prefix=パス [以下PREFIX]	インストール先ディレクトリ	/usr/local
--enable-syslog	syslog利用の有効化	yes
--enable-ipv6	IPv6の有効化	auto
--with-cyrus-sasl	SASL認証機能の有効化	auto
--with-threads	スレッド機能の有効化	auto
--with-tls	TLS/SSL機能の有効化	auto
--exec-prefix=パス [以下EPREFIX]	アーキテクチャ依存のファイルのインストール先	prefixと同じ
--bindir=パス	クライアントコマンドのインストール先	EPREFIX/bin
--sbindir=パス	システム管理コマンドのインストールパス	EPREFIX/sbin
--sysconfdir=パス	設定ファイルの格納場所	PREFIX/etc
--libdir=パス	ライブラリの格納場所	EPREFIX/lib
--includedir=パス	C言語のインクルードファイルの格納場所	PREFIX/include

slapd起動オプション

-4	IPv4でのみ接続を待ち受ける
-6	IPv6でのみ接続を待ち受ける
-d <level>	デバッグレベルを指定
-f <file>	設定ファイルを指定
-u <user>	指定したユーザ権限で動作
-g <group>	指定したグループ権限で動作
-s <level>	Syslogのファシリティを指定
-r <dir>	指定したディレクトリにchrootして動作

- ver.1 ミシガン大学の最終リリース
- ver.2 LDAP v.3対応 IPv6
- ver.2.1 いくつかのバックエンドを実装 SASL
- ver.2.2 レプリケーション オーバーレイ
- ver.2.3 back-configバックエンド
- ver.2.4 N-way Multi Master

インストール方法毎のファイルの格納先

	ソース（prefixからのパス）	パッケージ
デーモン	./libexec/slapd	/usr/sbin/slapd
設定ファイル	./etc/openldap/slapd.conf	/etc/openldap/slapd.conf
DB	/usr/local/var/openldap-data	/var/lib/ldap

レプリケーション

slurpd

失敗すると拒絶ファイルを作成

replog.スレーブサーバ名:ポート.rej

slurpdをワンショットモード(-o)で起動して取り込む

マスターサーバ

LDIF形式

slapd → 書き出し → 変更情報 ← 参照 ← slurpd → 同期 → slapd

スレーブサーバ

slapd.conf
replogfile 更新情報のファイルパス
replica host=スレーブサーバ名
bindmethod=simple
binddn="cn=Slave,dv=xxx,dc=net"
credentials=xxx

一致

slapd.conf
updatedn "cn=Slave,dv=xxx,dc=net"
updateref ldap://master.xxx.net

updatedn:同期により更新を許可するdn
updateref:行進用給仕に紹介するマスター

同期の保証が難しく、
管理が複雑に。

syncrepl

OpenLDAP 2.2から

オーバーレイsyncprovを有効にするだけ

コンシューマが増えると負荷が増える

refreshOnly:定期的に接続
refreshAndPersist:常に接続

コンシューマだけ設定を行う

プロバイダ
slapd

更新確認

同期
LDAP content syncronization protocol

コンシューマ
slapd

slapd.conf(2.2)
sessionlog 123 100
slapd.conf(2.3)
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
index entryCSN, entryUUID eq

slapd.conf
syncrepl rid=100
provider=ldap://provide.xxx.net:389
bindmethodd=simple
binddn="cn=Slave,dc=xxx,dc=net"
credentials="xxx"
type=refreshAndPersist
searchbase="dc=xxx,dc=net"

知識参照

下位知識参照(紹介オブジェクト)

エントリ
dn: ou=sub,dc=xxx,dc=net
objectClass: referral
objectClass: extensiibleObject
ou: sub
ref: ldap://slave.xxx.net/ou=sub,dc=xxx,dc=net

上位知識参照

slapd.conf
referral ldap://master.xxx.net/

パフォーマンスチューニング

spald

LDAPサーバ側

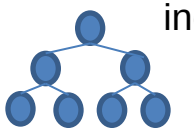
キャッシュ

spald.conf
cachesize キャッシュするエントリ数
idlcachesize キャッシュするインデックス数

idlcachesize > cachesize × 3 が望ましい

索引

slapd.confに書いて
slapindexで作成



index 属性名 種類

index objectClass eq
index uidNumber,gidNumber eq

directoryディレクティブに指定/エントリ名.bdb

syncrepl時にentryCSN,entryUUIDにeqを
つけると同期性能アップ

名称	種類
存在	pres
等価	eq
近似	approx
部分文字列	sub
前方一致	subinitial
後方一致	subfinal
部分一致	subany

nscd

LDAPクライアント側

クライアント側で使用
設定ファイル：/etc/nscd.conf

Berkeley DB

バックエンドDB

DB_CONFIG

設定項目	説明
set_cachesize	共有メモリに確保されるDBキャッシュサイズ
set_lg_bsize	TransactionLog書込みバッファサイズ(Byte)
set_lg_max	TransactionLogファイルのサイズ(Byte)
set_lg_regionmax	TransactionLogの管理領域サイズ(Byte)

BerkeleyDBのコマンド

コマンド	説明
db_stat -m	メモリキャッシュ情報の取得
db_stat -t	トランザクション情報を取得
db_verify	DB構造を検証
db_recover	DBを整合性のある状態に回復
db_archive	不要になったログファイルを表示/削除
db_printlog	DBログを可読可能に変換
db_dump	DBファイルをdb_loadで処理する形式に出力
db_load	テキストファイルからDBファイルを作成
db_checkpoint	DBのチェックポイント処理
db_upgrade	DBファイルを新BerkeleyDB用に更新

セキュリティ

簡易認証

暗号化パスワードを設定する

slappasswd -h {MD5} -s xxxxxx
{MD5}kajjhkjdfasdhlfk==

slapd.conf
rootpw {MD5}kajjhkjdfasdhlfk==

SASL認証

サーバでsaslユーザとエントリを関連付け
コマンドでパスワードを設定

saslpasswd -u xxx.net penguin

登録したアカウントを確認
sasldblistusers

slapd.conf
sasl-host ldap.xxx.net
sasl-realm xxx.net
sasl-regexp “uid=(.*),cn=xxx.net,cn=DIGEST-MD5,cn=auth” “uid=$1,dc=xxx,dc=net”

SSL/TLS

証明書と鍵を作って設定してSSL/TLSを起動
クライアント側も指定が必要

slapd.conf
TLSCertificateFile LDAPサーバの証明書
TLSCertificateKeyFile LDAPサーバのプライベートキー
TLSCACertificateFile CAの証明書

起動オプション
slapd -h ‘ldap:// ldaps://’

ldap.conf
ssl on
TLS_CACERT CAの証明書

start_tlsなら
ssl start_tls

SSL/TLSクライアント認証

slapd.conf
TLSVerifyClient demand

もしくはtrue,hand

ACL

access to 検索条件
by 対象ユーザ 権限

slapd.conf
defaultaccess search

例

access to *
by self write
by anonymous auth
by user read

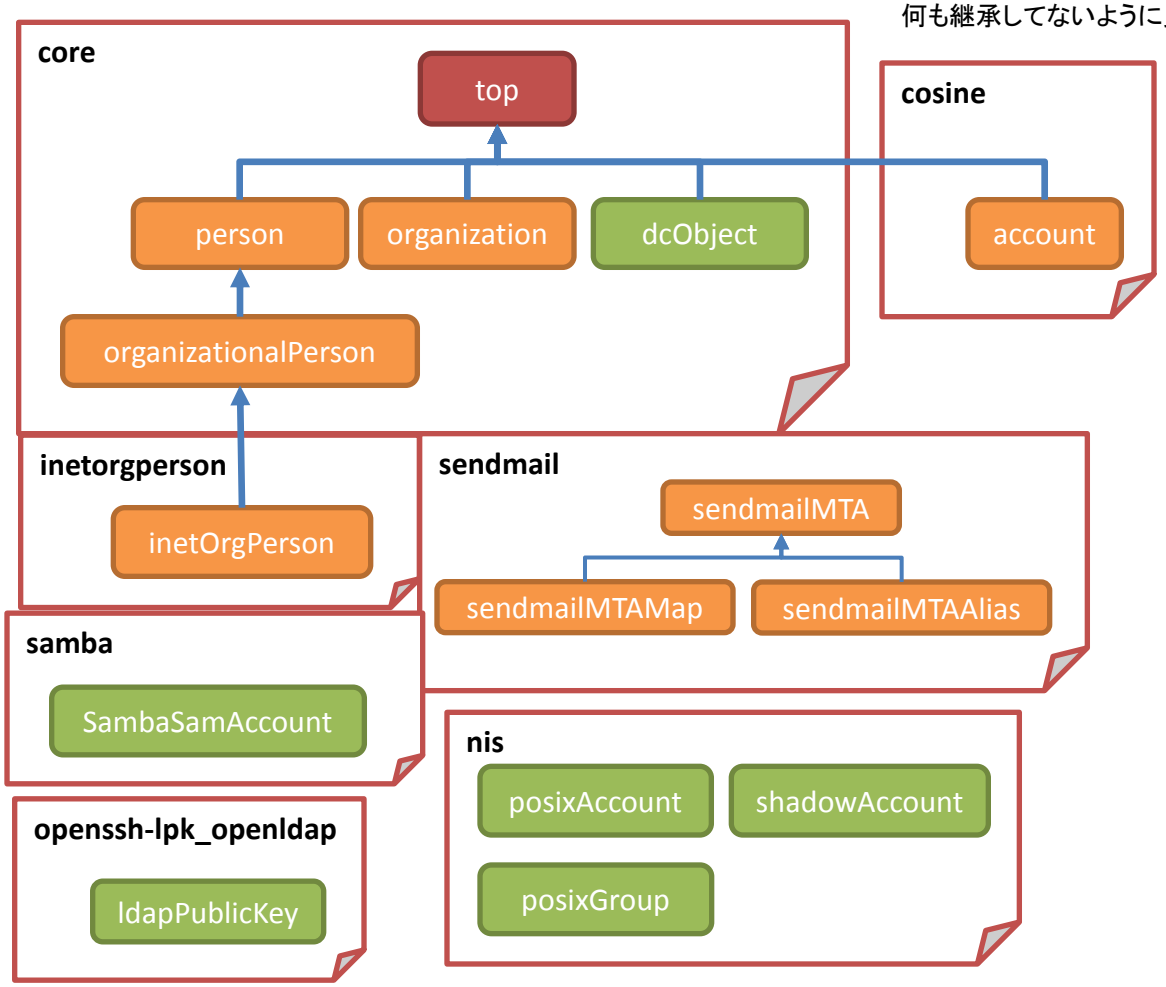
検索条件	説明
*	ディレクトリ内すべてのエントリ
dn=DNの値	指定したエントリ
attrs=属性名	指定した属性
fiilter=検索フィルタ	検索フィルタに一致するエントリ

対象ユーザ	説明
*	匿名接続を含めた全接続ユーザ
anonymous	認証されていないユーザ
users	認証されたユーザ
self	対象エントリに対応するユーザ
dn=値（正規表現可）	指定したDNに対応するユーザ

権限	説明
none	アクセス不可
auth	認証するアクセス権
compare	auth+比較権限
search	compare+検索権限
read	search+読取権限
write	read+書込み権限

定義ファイル

何も継承してないように見えるのはtopを継承



.schemaファイル

補助型オブジェクトクラス

構造型オブジェクトクラス

抽象型オブジェクトクラス

OID:Object IDentifier
IANAが管理

共通項目	説明
OID	オブジェクトクラスの識別子
NAME	オブジェクトクラスの名称
DESC	コメント

オブジェクトクラス項目	説明
SUP	スーパークラスと形式
MUST	必須属性（$区切り）
MAY	オプション属性（$区切り）

属性項目	説明
EQUALITY	同値照合
ORDERING	順照合
SUBSTR	部分文字列照合
SYNTAX	属性型

ldapコマンド

- LDAPクライアントコマンド
- LDAPプロトコルで接続

共通オプション

オプション	説明
-H ホスト	参照する URI を指定します。
-p ポート番号	接続するための TCP ポートを明示します。
-D DN	バインドするDNを指定
-Z	StartTLSを利用(成功しなければ通常通)
-ZZ	StartTLSを利用(成功しなければ終了)
-x	簡易認証を使用
-W	簡易認証パスワードを対話的に入力
-w パスワード	簡易認証のパスワードを指定
-U ユーザ	SASLユーザを指定

ldapadd,ldapmodify

オプション	説明
-n	実行はせずテストを行う
-f ファイル	LDIFファイルを指定

ldapdelete

オプション	説明
-r	指定したエントリ以下を再帰的に削除

ldapmodrdn

オプション	説明
-r	古いDNの値を削除
-n	実行はせずテストを行う
-f ファイル	LDIFファイルを指定

ldapsearch

オプション	説明
-L	結果をLDIF形式で表示
-LL	-Lからコメントを非表示
-LLL	-LLからLDIFバージョンを非表示
-P 2|3	プロトコルのバージョンを指定
-b DN	ベースDNを指定
-h URI	検索するLDAPサーバを指定
-k	Kerberos認証を使用
-s スコープ	検索スコープを指定
-z 数	表示される最大エントリ数を指定

検索スコープ

対象	base	one	sub	child
自ノード	○	○	○	×
子ノード	×	○	○	○
子孫ノード	×	×	○	○

検索条件の例

(cn=A*)
(&(sn=Koike)(o=network))
(|(o=network)(o=develop))
(&(|(o=develop)(o=web))(sn=Hata))

LDIFの例 RFC2849

dn: 更新対象DN
changetype: modify
add: 追加する属性名
追加する属性値: 値
-
dn: 削除対象のDN
changetype: modify
delete: 削除する属性名
-
dn: 更新対象のDN
changetype: modify
replace: 修正する属性名
修正する属性名: 値

コメントは「#」
バイナリはBASE64エンコードして「属性名::属性値」

```
ldapadd -x -D 'cn=Manager,dc=example,dc=net' -W -f sample.ldif
ldapsearch -x -D 'cn=Manager,dc=example,dc=net' -W -LLL -b 'dc=example,dc=net' '(objectClass=person)' cn
ldapmodrdn -x -D 'cn=Manager,dc=example,dc=net' -W 'cn=Taro Sato,ou=People,dc=example,dc=net' 'cn=Taro Tanaka'
ldapdelete -x -D 'cn=Manager,dc=example,dc=net' -W 'cn=Taro Sato,ou=People,dc=example,dc=net'
```

slapコマンド

- データベースに直接アクセス
- slapdが起動していなくてもアクセス可能

基本的に共通なオプション（抜粋）

オプション	説明
-v	冗長モードにします。
-d デバッグレベル	指定のレベル *level* のデバッグメッセージを出力するようにします。
-f 設定ファイル	代替のslapd.confファイルを指定します。

slapcatとslapaddの共通なオプション（抜粋）

オプション	説明
-c	継続(エラー無視)モードにします。
-n DB番号	設定ファイルに定義されている dbnum 番目のデータベースから出力を生成します。この -n オプションは -b オプションと一緒に使えません。
-l LDIF	LDIF を標準出力にではなく指定したファイルに書き出します。

slapcatオプション（抜粋）

オプション	説明
-b サフィックス	サフィックスを指定

slaptestオプション（抜粋）

オプション	説明
-u	dry-run モードにします(データベースがオープンできなくても設定が正しければエラーになりません)。

slappasswdオプション（抜粋）

オプション	説明
-h	ハッシュの種類
-s secret	指定のパスワード secret をハッシュ化します。

参考

- http://ja.wikipedia.org/wiki/LDAP
- http://www.openldap.org/
- http://ja.wikipedia.org/wiki/OpenLDAP