LDAP on Docker

nekonyanneko

2017/03/11

Contents

Part I
Docker install

いつもここから https://www.docker.com/

1 Docker コンテナの作成

以下で Docker コンテナを作成

```
docker run -it centos:6 /bin/bash
```

Part II
LDAP Server

2 LDAP Server のセットアップ

2.1 Docker コンテナの起動

docker プロセスにアタッチ

```
docker start <CONTAINER ID>
docker attach <CONTAINER ID>
```

2.2 LDAP のインストールと設定

ldap ユーザを作成

```
useradd ldap
```

OpenLDAP をインストール

```
yum -y install openldap-servers openldap-clients
```

OpenLDAP サーバーにデータを登録する際の「ldapadd」コマンドや検索用の
「ldapsearch」コマンドは「openldap-clients」パッケージに入っている
そのため、OpenLDAP サーバーのみであっても、「openldap-clients」パッケージ
もインストールしておくこと

初期設定削除

```
rm -rf /etc/openldap/slapd.d/*
rm -rf /var/lib/ldap/*
rm -rf /etc/openldap/slap.d
```

設定ファイルのコピー

```
cp -a /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap /var/lib/ldap/DB_CONFIG
cp -a /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
```

マスターパスワード作成

```
slappasswd
```

ここで出力されたパスワードの Hash 値は控えておく
設定ファイルの編集

```
vi /etc/openldap/slapd.conf
```

```
# スキーマファイル設定
include /etc/openldap/schema/corba.schema
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/duaconf.schema
include /etc/openldap/schema/dyngroup.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/java.schema
include /etc/openldap/schema/misc.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/ppolicy.schema
include /etc/openldap/schema/collective.schema

# 接続プロトコル
allow bind_v2

# 管理ファイル
pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args

# TLS 設定
#TLSCACertificatePath  /etc/openldap/ssl/cacert.pem
#TLSCertificateFile    /etc/openldap/ssl/server.crt
#TLSCertificateKeyFile /etc/openldap/ssl/server.key

# userPassword に関するアクセス権
access to attrs=userPassword
    by self write
    by dn="cn=Manager,dc=example,dc=com" write
    by anonymous auth
    by * none

# その他の属性に対するアクセス権
access to *
    by self write
    by dn="cn=Manager,dc=example,dc=com" write
    by * read

# monitor データベースに対するアクセス権
database monitor
```

```
access to *
    by dn.exact="cn=Manager,dc=example,dc=com" read
    by * none

# データベース設定
database    bdb
suffix      "dc=example,dc=com"
checkpoint  1024 15
rootdn      "cn=Manager,dc=example,dc=com"
rootpw      {SSHA}your.pass.hash
directory   /var/lib/ldap

# index の設定
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
-----------------------------------------------------------------------------
```

設定のテスト

```
slaptest -u -v -f /etc/openldap/slapd.conf
```

config file testing succeeded
/etc/openldap/slapd.d/ の更新

```
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
```

エラーが出るが無視する

```
bdb_db_open: database "dc=example,dc=com": db_open(/var/lib/ldap/id2entry.bdb) failed:
 No such file or directory (2).
backend_startup_one (type=bdb, suffix="dc=example,dc=com"): bi_db_open failed! (2)
slap_startup failed (test would succeed using the -u switch)
```

LDAP 起動

```
service slapd start
chkconfig slapd on
```

2.3 データの登録

基本データの作成

```
mkdir -p /etc/openldap/ldif
vi /etc/openldap/ldif/base.ldif
```

```
-----------------------------------------------------------------------------
# ドメイン
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
```

```
dc: example
o: Example co.,Ltd

# 管理者
dn: cn=Manager,dc=example,dc=com
objectClass: organizationalRole
cn: Manager

# システムユーザー
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

# システムグループ
dn: ou=Group,dc=example,dc=com
objectClass: organizationalUnit
ou: Group

# アドレス帳
dn: ou=Address,dc=example,dc=com
objectClass: organizationalUnit
ou: Address
-----------------------------------------------------------------------------
```

LDAP サーバーに基本データ登録

```
ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f /etc/openldap/ldif/base.ldif
```

パスワード入力を求められるため、「slappasswd」コマンドで入力したパスワード
を入力すること。
情報システム部のグループデータ作成

```
vi /etc/openldap/ldif/group.ldif
```

```
-----------------------------------------------------------------------------
# 情報システム部
dn: cn=system,ou=Group,dc=example,dc=com
objectClass: posixGroup
objectClass: top
cn: system
gidNumber: 1000
-----------------------------------------------------------------------------
```

情報システム部のグループデータ登録

```
ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f /etc/openldap/ldif/group.ldif
```

情報システム部のユーザーデータ作成

```
vi /etc/openldap/ldif/user.ldif
```

```
-----------------------------------------------------------------------------
# 部長：武田 貴彦
```

```
dn: uid=takahiko.takeda,ou=People,dc=example,dc=com
objectClass: shadowAccount
objectClass: posixAccount
objectClass: account
objectClass: top
cn: Takahiko Takeda
uid: takahiko.takeda
uidNumber: 1001
gidNumber: 1000
homeDirectory: /home/takahiko.takeda
loginShell: /bin/bash
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
shadowLastChange: 16175
userPassword: {SSHA}0IBfkSHm6eDVouPuwRlvEBBBofDUNul6

# 開発課 課長：横山 真也
dn: uid=shinya.yokoyama,ou=People,dc=example,dc=com
objectClass: shadowAccount
objectClass: posixAccount
objectClass: account
objectClass: top
cn: Shinya Yokoyama
uid: shinya.yokoyama
uidNumber: 1002
gidNumber: 1000
homeDirectory: /home/shinya.yokoyama
loginShell: /bin/bash
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
shadowLastChange: 16175
userPassword: {SSHA}WjskiArncjkXcoLNsX49TE5+L6qBfeZL

# 運用課 課長：井上 修
dn: uid=osamu.inoue,ou=People,dc=example,dc=com
objectClass: shadowAccount
objectClass: posixAccount
objectClass: account
objectClass: top
cn: Osamu Inoue
uid: osamu.inoue
uidNumber: 1003
gidNumber: 1000
homeDirectory: /home/osamu.inoue
loginShell: /bin/bash
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

```
shadowLastChange: 16175
userPassword: {SSHA}IMy6+0Zvb5mgsrByu0zrD68K9yHtFVR6

# 開発課 社員：石川 直樹
dn: uid=naoki.ishikawa,ou=People,dc=example,dc=com
objectClass: shadowAccount
objectClass: posixAccount
objectClass: account
objectClass: top
cn: Naoki Ishikawa
uid: naoki.ishikawa
uidNumber: 1004
gidNumber: 1000
homeDirectory: /home/naoki.ishikawa
loginShell: /bin/bash
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
shadowLastChange: 16175
userPassword: {SSHA}1ixM0yQBZZlFaReiN778DKGSoo5peemc

# 運用課 社員：田村 和夫
dn: uid=kazuo.tamura,ou=People,dc=example,dc=com
objectClass: shadowAccount
objectClass: posixAccount
objectClass: account
objectClass: top
cn: Kazuo Tamura
uid: kazuo.tamura
uidNumber: 1005
gidNumber: 1000
homeDirectory: /home/kazuo.tamura
loginShell: /bin/bash
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
shadowLastChange: 16175
userPassword: {SSHA}vfmOEDQbUqm43yaqFXIOwxMS9y15mfxt
--------------------------------------------------------------------------------
```

情報システム部のユーザーデータ登録

```
ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f /etc/openldap/ldif/user.ldif
```

3 節

section

3.1　小節

subsection

3.1.1　少々節

subsubsection