OpenLDAPの設定（IdPv4）

本ページはIdPテスト用のLDAPサーバ構築を行うものですので、別途構築されているLDAPサーバに接続する場合は不要です。次ページより先に進んでください。

OpenLDAPの設定

OpenLDAPは、バージョンによって設定の方法が変わっています。バージョン2.2まではslapd.confに設定内容を定義していましたが、バージョン2.3以降で非推奨となりディレクトリサービス上に設定を格納するようになりました。CentOS 6と7標準のOpenLDAPは2.3以降の、ディレクトリサービス上での設定を基本としています。
以下ではCentOS 7を想定してディレクトリサービス上に設定する方法で記述しています。

---

0. OpenLDAPパッケージの確認

/etc/openldap/schema ディレクトリが存在しない場合は、以下のようにしてOpenLDAPパッケージをインストールしてください。

```
# yum install openldap-clients openldap-servers
```

インストール後、自動起動の設定を行います。

CentOS7の場合

```
# systemctl enable slapd
```

```
# chkconfig --level 345 slapd on
```

---

1. 追加のスキーマファイル

以下のURLには、edupersonスキーマの内容が記載されています。
/etc/openldap/schema 配下に「eduperson.schema」を作成し、スキーマの内容をコピーしてください。
※edupersonスキーマの追加は必須ではありません。
（既に統合認証基盤が構築されており、必要な属性値が存在する場合など）

https://spaces.at.internet2.edu/display/macedir/OpenLDAP+eduPerson

---

2. LDAPサーバのデフォルト設定

ディレクトリサービス上に設定する方法は、slapd.confから変換する方法もありますが、ここではディレクトリサービスのインタフェースを介した手順を説明します。

・LDAPサーバの起動
事前に起動させておく必要があります。

CentOS7の場合

```
# systemctl start slapd
```

```
# service slapd start
```

・データベースの設定

初期登録されている既存のドメイン情報を変更して、使用します。
以下のような内容で、ドメイン情報変更用のldifファイルを作成します。

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to *  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read  by dn.base="cn=olmgr,o=test_o,dc=ac,
c=JP" read  by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: o=test_o,dc=ac,c=JP                ←suffix
-
replace: olcRootDN
olcRootDN: cn=olmgr,o=test_o,dc=ac,c=JP        ←rootdn
-
add: olcRootPW
olcRootPW: {CRYPT}$6$6e4.0f8k69uRYHNq$MxtzkEmGh7sFN7hdumuXyx8PsHqNCs3Mf9sdRcAytz3xs7sbZGathb9G5oc/vrm1zOc7kwVZScy02SJxDGDs60
←rootパスワード（暗号化したもの）
```

ここで設定したolcRootPWは、LDAPのデータベースに対する管理者パスワードです。
また、このパスワードは ldPの設定ファイルにも記述します。(後述)

※暗号化の例：

```
「csildap」というパスワードを暗号化
# slappasswd -h {CRYPT} -c '$6$%s$' -s csildap
{CRYPT}$6$6e4.0f8k69uRYHNq$MxtzkEmGh7sFN7hdumuXyx8PsHqNCs3Mf9sdRcAytz3xs7sbZGathb9G5oc/vrm1zOc7kwVZScy02SJxDGDs60
↑これをドメイン情報変更用ldifのolcRootPWに記載
```

以下のコマンドを実行して、ドメイン情報を変更します。

```
# ldapmodify -Y EXTERNAL -H ldapi:// -f ドメイン情報変更用のldifファイルパス
```

・eduPersonスキーマの登録
スキーマの登録においてもディレクトリサービスのインタフェースを介した手順となります。
ldifファイルより行うため、eduPersonスキーマを使ってldifファイルを作成します。
以下のような内容で、ldifファイル作成に必要な設定ファイルを作成します。

```
include /etc/openldap/schema/eduperson.schema
```

以下のコマンドを実行して、eduPersonスキーマのldifファイルを作成します。

```
# slapcat -f 作成した設定ファイルのパス -F /tmp -n0 -s "cn={0}eduperson,cn=schema,cn=config" > /etc/openldap/schema/eduperson.ldif
```

作成したldifファイルから余分な情報を削除します。
以下の手順に従って、/etc/openldap/schema/eduperson.ldifを編集してください。

```
・ファイル先頭にある {0}eduperson を eduperson に修正
 以下は、修正後の内容です。
 dn: cn=eduperson,cn=schema,cn=config
 objectClass: olcSchemaConfig
 cn: eduperson

・ファイルの後方にある「structuralObjectClass: olcSchemaConfig」以降を全て削除
 以下は、削除対象の項目です。
 structuralObjectClass: olcSchemaConfig
 entryUUID:                ・・・（省略）
 creatorsName:          ・・・（省略）
 createTimestamp:          ・・・（省略）
 entryCSN:                 ・・・（省略）
 modifiersName:          ・・・（省略）
 modifyTimestamp:          ・・・（省略）
```

以下のコマンドを実行して、edupersonスキーマを登録します。

```
# ldapadd -Y EXTERNAL -H ldapi:// -f /etc/openldap/schema/eduperson.ldif
```

---

3. LDAPのテストデータ作成

以下のサンプルを基に、テスト用データを作成し、LDAPへ登録します。
Shibboleth を利用したID/パスワードでの認証に使用されるIDはuid 、パスワードは userPassword になります。
※IDに使用する属性については、ldap.propertiesのidp.authn.LDAP.userFilterの修正で他の属性に変更できます。
　ただし、同様に送信属性値取得の設定がattribute-resolver.xmlもしくはldap.propertiesのidp.attribute.resolver.LDAP.searchFilterで行われており、
　こちらのLDAP検索キーも同様に変更しなければ不整合が起きるので、注意してください。

・test.ldif ファイル作成
 ※環境にもよりますが、文字コードは「UTF-8」で作成してください。

```
dn: o=test_o,dc=ac,c=JP
objectClass: organization
o: test_o

dn: ou=Test Unit1,o=test_o,dc=ac,c=JP
objectClass: organizationalUnit
ou: Test Unit1

dn: ou=Test Unit2,o=test_o,dc=ac,c=JP
objectClass: organizationalUnit
ou: Test Unit2

dn: ou=Test Unit3,o=test_o,dc=ac,c=JP
objectClass: organizationalUnit
ou: Test Unit3

dn: uid=test001,ou=Test Unit1,o=test_o,dc=ac,c=JP
objectClass: eduPerson
objectClass: inetOrgPerson
uid: test001
ou: Test Unit1
ou;lang-ja: テスト001_学部1
sn: test001_sn
sn;lang-ja: テスト001_sn
cn: test001_cn
userPassword: test001
givenName: test001_givenname
givenName;lang-ja: テスト001_givenname
displayName: test001_displayname
displayName;lang-ja: テスト001_displayname
mail: test001_email@nii.ac.jp
eduPersonAffiliation: member
employeeNumber: 0001

dn: uid=test002,ou=Test Unit2,o=test_o,dc=ac,c=JP
objectClass: eduPerson
objectClass: inetOrgPerson
uid: test002
ou: Test Unit2
ou;lang-ja: テスト002_学部2
sn: test002_sn
sn;lang-ja: テスト002_sn
cn: test002_cn
userPassword: test002
givenName: test002_givenname
givenName;lang-ja: テスト002_givenname
displayName: test002_displayname
displayName;lang-ja: テスト002_displayname
mail: test002_email@nii.ac.jp
eduPersonAffiliation: faculty
employeeNumber: 0002

dn: uid=test003,ou=Test Unit3,o=test_o,dc=ac,c=JP
objectClass: eduPerson
objectClass: inetOrgPerson
uid: test003
ou: Test Unit3
ou;lang-ja: テスト003_学部3
sn: test003_sn
sn;lang-ja: テスト003_sn
cn: test003_cn
userPassword: test003
givenName: test003_givenname
givenName;lang-ja: テスト003_givenname
displayName: test003_displayname
displayName;lang-ja: テスト003_displayname
mail: test003_email@nii.ac.jp
eduPersonAffiliation: student
employeeNumber: 0003
```

・LDAPへの登録

```
# ldapadd -x -h localhost -D "cn=olmgr,o=test_o,dc=ac,c=JP" -w csildap -f test.ldif
```

ldapaddコマンドで以下のエラーが出る場合は

```
adding new entry "uid=test001,ou=Test Unit1,o=test_o,dc=ac,c=JP"
ldap_add: Invalid syntax (21)
    additional info: objectClass: value #1 invalid per syntax
```

以下のコマンドでスキーマを読み込んで、さらにtest.ldifのtest001より上の行を削除から、再度お試しください。

```
# ldapadd -Y EXTERNAL -H ldapi:// -f /etc/openldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:// -f /etc/openldap/schema/inetorgperson.ldif
```

TOP NEXT