

Managing Objects in OpenLDAP

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the common objects stored in an LDAP database.
2. Use LDAP Data Interchange Format (LDIF) files to create organizational units, groups, and users in OpenLDAP.

Additional resources used during the episode can be obtained using the download link on the overview episode.

-
- Managing Objects in OpenLDAP
 - Object Types
 - Creating Objects with LDIF Files
 - Creating Objects with phpLDAPadmin
 - LDAP Object Types
 - Fully customizable
 - Defined by the schema
 - Examples
 - User accounts
 - Groups
 - Email accounts / Aliases
 - DNS records
 - Organizational Units
 - Objects are containers of attributes
 - **CN**: commonName
 - **O**: organizationName
 - **OU**: organizationalUnitName
 - **DC**: domainComponent
 - **UID**: userid
 - LDIF Files
 - LDAP Data Interchange Format (LDIF)
 - Text files that contain changes to the LDAP database
 - Create/Add
 - Modify
 - Delete
 - Follows a particular format based on attributes
 - Create OUs using LDIF files
 1. Create an LDIF file and populate with user attributes
 - `nano ou.ldif`
 2. Import the file
 - `ldapadd -x -D cn=admin,dc=lab,dc=itpro,dc=tv -W -f ou.ldif`
 - `-x` Use simple authentication
 - `-D` Distinguished name to bind to
 - `-W` Prompt for password
 - `-f` File to import
 - Create user accounts using LDIF files
 1. Generate a password
 - `slappasswd`
 - `password123`

2. Create an LDIF file and populate with user attributes

- nano user.ldif

3. Import the file

- ldapadd -x -D cn=admin,dc=lab,dc=itpro,dc=tv -W -f user.ldif

• Creating objects with phpLDAPAdmin

- phpLDAPAdmin
 - <http://phpldapadmin.sourceforge.net/>
 - Simple UI for managing objects
- Accessible via `http://server_name/phpldapadmin`

Example ou.ldif

```
dn: ou=users,dc=lab,dc=itpro,dc=tv
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=lab,dc=itpro,dc=tv
objectClass: organizationalUnit
ou: groups
```

Example user.ldif

```
dn: uid=donpezet,ou=users,dc=lab,dc=itpro,dc=tv
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Don
sn: Pezet
userPassword: {SSHA}4kVuir9Wv/D1ztUdKvr49qibkE6aeL6F
loginShell: /bin/bash
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/donpezet

dn: cn=donpezet,ou=groups,dc=lab,dc=itpro,dc=tv
objectClass: posixGroup
cn: donpezet
gidNumber: 10001
memberUid: donpezet
```