LDAP

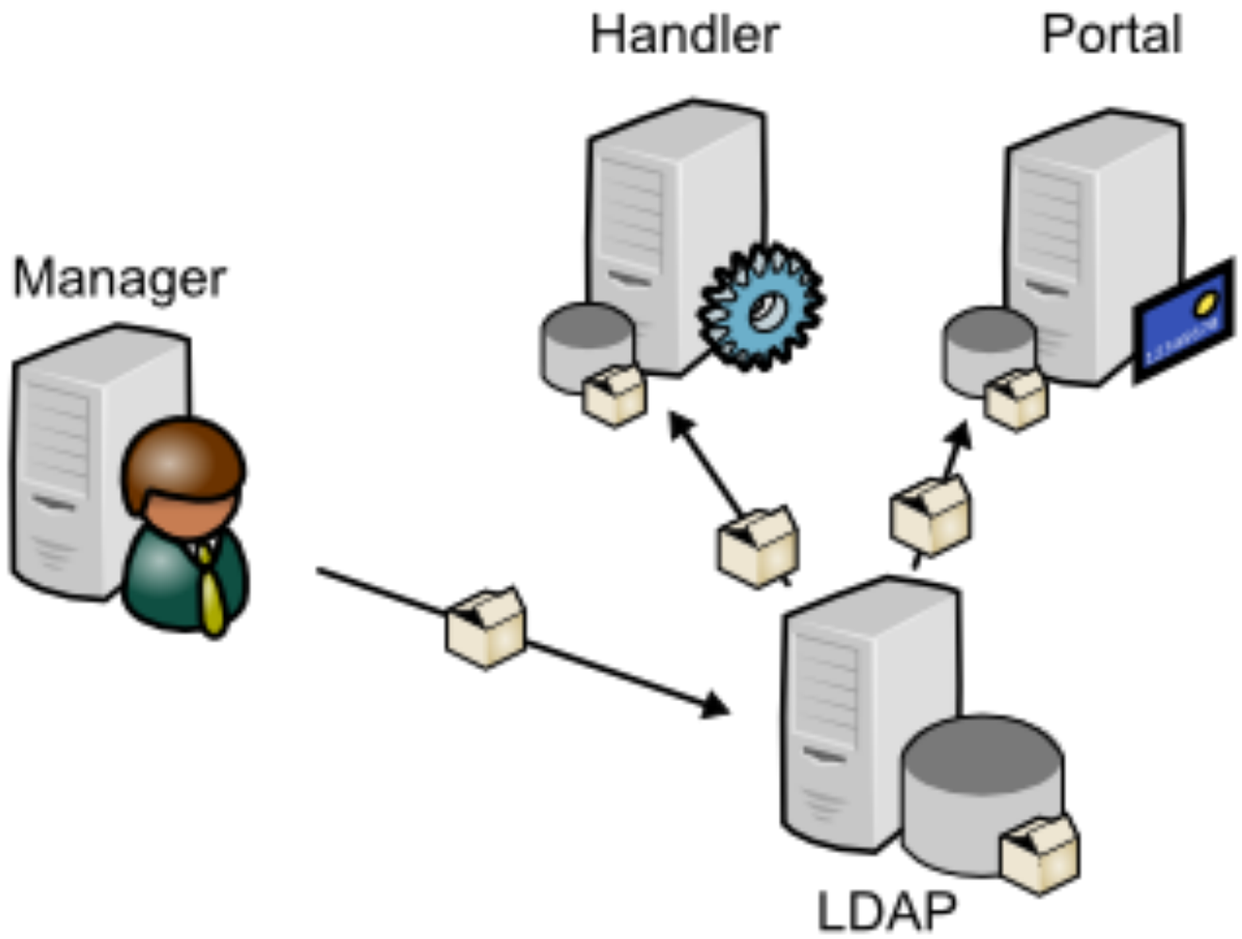
potato, kis

LDAP

- Lightweight Directory Access Protocol
- 다른 호스트의 디렉토리 서비스에 접근하기 위한 프로토콜이다.
- TCP/IP 상에서 작동한다.
- 사용자 DB를 공유한다고 생각하면 쉽다. (다른 종류의 정보도 공유할 수 있지만 이 세미나에서는 사용자 정보를 다룬다.)

LDAP

- Manager가 LDAP 서버에 정보를 입력한다.
- LDAP 클라이언트에서 LDAP 서버에 저장되어있는 사용자 정보를 이용한다.



디렉토리 서비스

- 네트워크 리소스를 관리하는데 사용한다.
- 네트워크 리소스와 사용자에 대한 정보를 갖고 있다.
- DBMS에 비해 복잡한 갱신이 어렵다. 대신 읽기에 최적화 되어 있다.
- X.500에 정의되어 있다.

Directory Information Tree

- DIT(Directory Information Tree)는 LDAP을 이루는 트리 구조다.

- 트리의 각 노드는 ‘Entry’라고 부른다. 하나의 entry는 DBMS에서의 하나의 tuple이라고 볼 수 있다.

- 각 entry는 DN(Distinguished Name)으로 구분된다. DN는 그 위치를 함께 나타낸다.

- DN은 오른쪽에서 왼쪽으로 확장된다.

- 속성값(Attribute name)은 줄여 쓰는 것이 일반적이다.

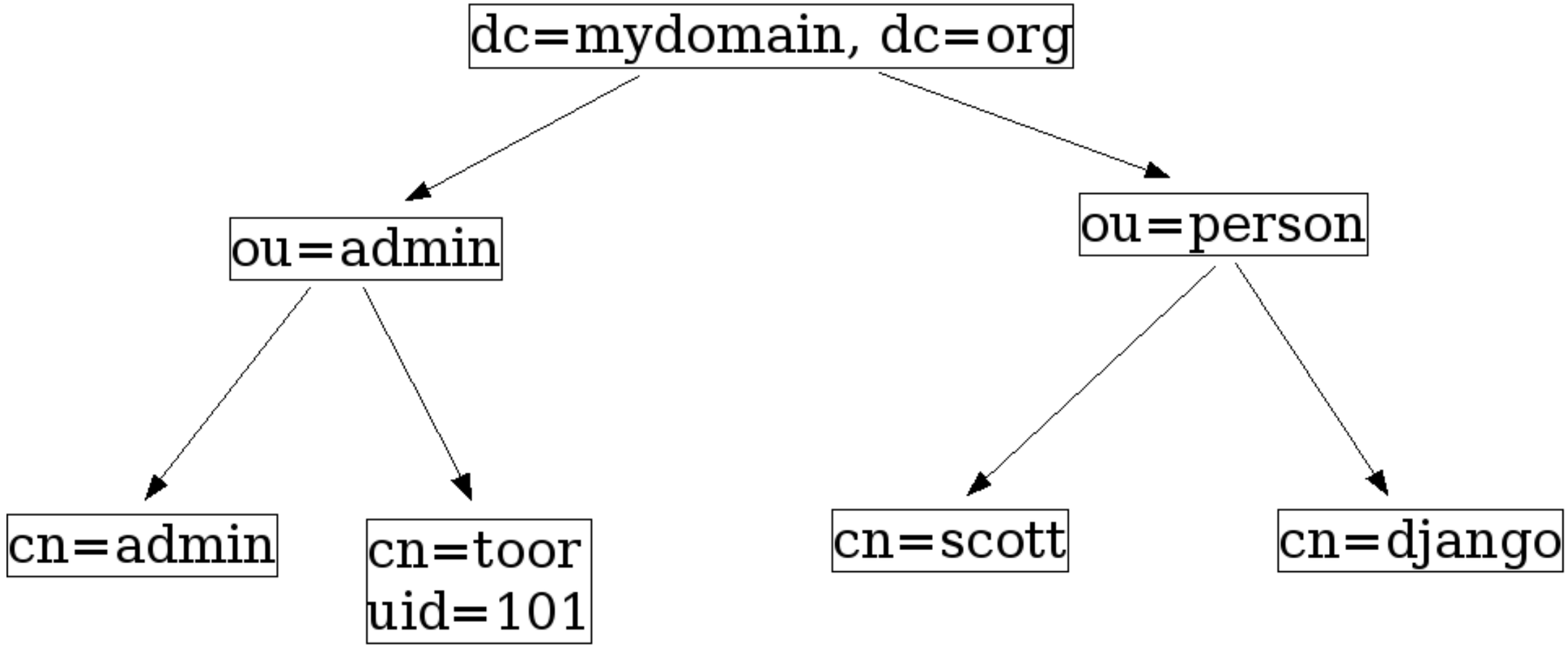
  예) c = country, cn = common name, ou = organization unit,
  dc = domain component …

DIT 예시

Exemple de DIT

o=mydomain, c=fr notation X500

dc=mydomain.org
dc=mydomain, dc=org notation rfc 2247



LDIF

- LDAP Data Interchange Format

- LDAP에서 관리하는 정보를 plain text로 변환해서 보여주는 형식이다.

DIT 예시

- slapd-config DIT by LDIF

```
dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcBackend={0}hdb,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}hdb,cn=config
```

Schema

- entry가 가질 수 있는 attributes를 정의한다.
- ojbectClass에서 사용할 schema를 정한다.
- programming language에서 class와 비슷한 개념이다.
- 사용자에 맞는 schema를 만들어서 사용할 수 있다.

```
dn: cn=wseminar,dc=wseminar4,dc=sparcs,dc=org
objectClass: posixGroup
cn: wseminar
gidNumber: 100

dn: cn=potato,dc=wseminar4,dc=sparcs,dc=org
objectClass: inetOrgPerson
uid: potato
uid: 1
sn: po
givenName: tato
cn: potato
```

LDAP Server

OpenLDAP 설치

- slapd(Stand-alnone LDAP daemon)와 ldap-utils를 설치한다.
  (slapd는 2.4.23 버전이 설치된다.)

```
sudo apt-get install slapd ldap-utils
```

slapd 끄고 켜기

```
sudo /etc/init.d/slapd stop

sudo /etc/init.d/slapd start

sudo /etc/init.d/slapd restart
```

설정

```
sudo dpkg-reconfigure slapd
```

- 설정 순서

-> NO

-> wseminar#.sparcs.org (# = 각자 주소)

-> wseminar#

-> 비밀번호, 비밀번호 확인

-> HDB, NO, NO, NO

ldapsearch

- 속성

-x : 인증 방식을 간단히 한다. (기본값은 SASL)

-W : prompt로 비밀번호를 물어본다. -x속성과 함께 사용된다.

-L : 표현 형식을 바꾼다.

-b : 검색의 시작 지점을 설정한다. (트리에서 해당 노드 밑으로 검색한다.)

가장 마지막(filter) : 해당하는 속성값을 불러온다. 생략하면 모든 속성값을 불러온다.

자세한건 man ldapsearch 참고

ldapsearch 사용 예시

```
ldapsearch -x -LLL -b dc=wseminar#,dc=sparcs,dc=org
```

```
potato@wseminar4:~$ ldapsearch -x -LLL -b dc=wseminar4,dc=sparcs,dc=org
dn: dc=wseminar4,dc=sparcs,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: wseminar4
dc: wseminar4

dn: cn=admin,dc=wseminar4,dc=sparcs,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
```

- ldap server 설정 보기

```
sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b cn=config
```

ldapmodify, ldapadd

- ldapadd는 ldapmodify에 -a 속성을 붙인 것과 같다.
  (ldapadd = ldapmodify -a)

- 속성

-x : 인증 방식을 간단히 한다. (기본값은 SASL)

-W : prompt로 비밀번호를 물어본다. -x속성과 함께 사용된다.

-f : 뒤에 .ldif 파일이 온다.

-D : 뒤에 수정, 추가하는 사용자의 dn이 온다.

-c : 오류가 나도 멈추지 않고 계속한다.

자세한건 man ldapadd 참고

ldapmodify, ldapadd 사용 예시

- .lidf 파일을 만든다.

```
vi ~/add.ldif
```

add.ldif

```
dn: cn=wseminar,dc=wseminar#,dc=sparcs,dc=org    <- 자기 서버 주소
objectClass: posixGroup
cn:wseminar                                      <- dn에 쓴 cn 그대로
gidNumber: 100

dn: cn=potato2,dc=wseminar#,dc=sparcs,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
uid: potato2
sn: tato2                                        <- sn : 성
givenName: po                                    <- givenName : 이름
cn: potato2
uidNumber: 10000                                 <- 안겹치게
gidNumber: 100                                   <- 위에 쓴 그 gidNumber
userPassword: potatopw
homeDirectory: /home/potato2
```

ldapmodify, ldapadd 사용 예시

```
ldapadd -x -D cn=admin,dc=wseminar4,dc=sparcs,dc=org -W -f add.ldif

ldapsearch -x -LLL -b dc=wseminar4,dc=sparcs,dc=org
```

```
dn: cn=wseminar,dc=wseminar4,dc=sparcs,dc=org
objectClass: posixGroup
cn: wseminar
gidNumber: 100

dn: cn=potato2,dc=wseminar4,dc=sparcs,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
uid: potato2
sn: tato2
givenName: po
cn: potato2
uidNumber: 10000
gidNumber: 100
homeDirectory: /home/potato2
```

phpLDAPadmin

- php를 기반으로 해 LDAP을 GUI환경에서 관리할 수 있게 해 준다.
- 2002년에 Brignham Young University의 Dave Smith라는 학생이 시작했다.
- 최신 버전은 1.2.3이다.
- 그러나 어째서인지 apt-get install로 설치되는 버전은 1.2.0.5이다. 실습은 이 버전으로 진행한다.
- http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page

phpldapadmin 설치

```
sudo apt-get install phpldapadmin
```

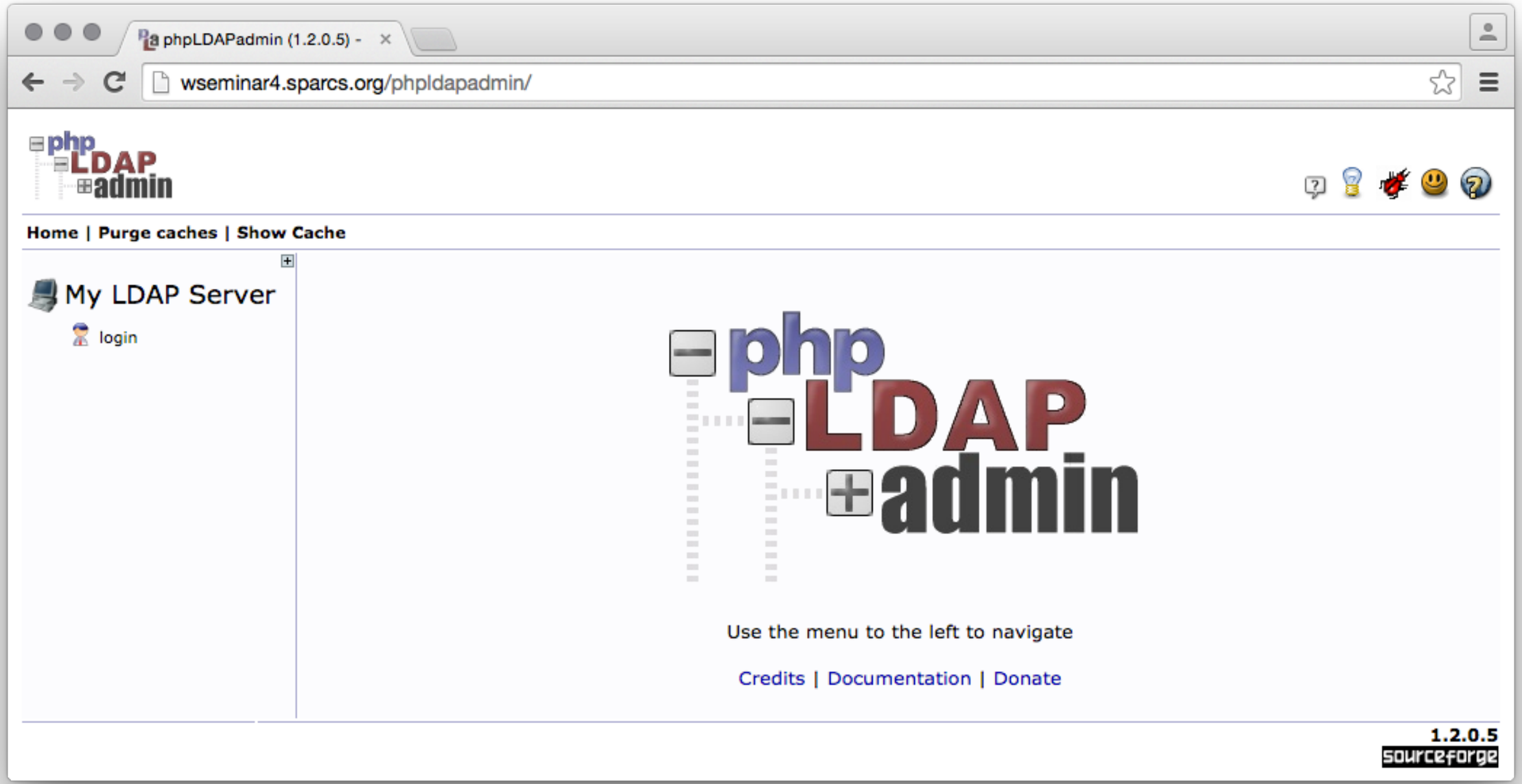
phpldapadmin 설정

```
sudo vi /etc/phpldapadmin/config.php
```

```
276.$servers->setValue('server','host','wseminar#.sparcs.org');


283.$servers->
   setValue('server','base',array('dc=wseminar#,dc=sparcs,dc=org'));


306.$servers->
   setValue('login','bind_id','cn=admin,dc=wseminar#,dc=sparcs,dc=org');
```

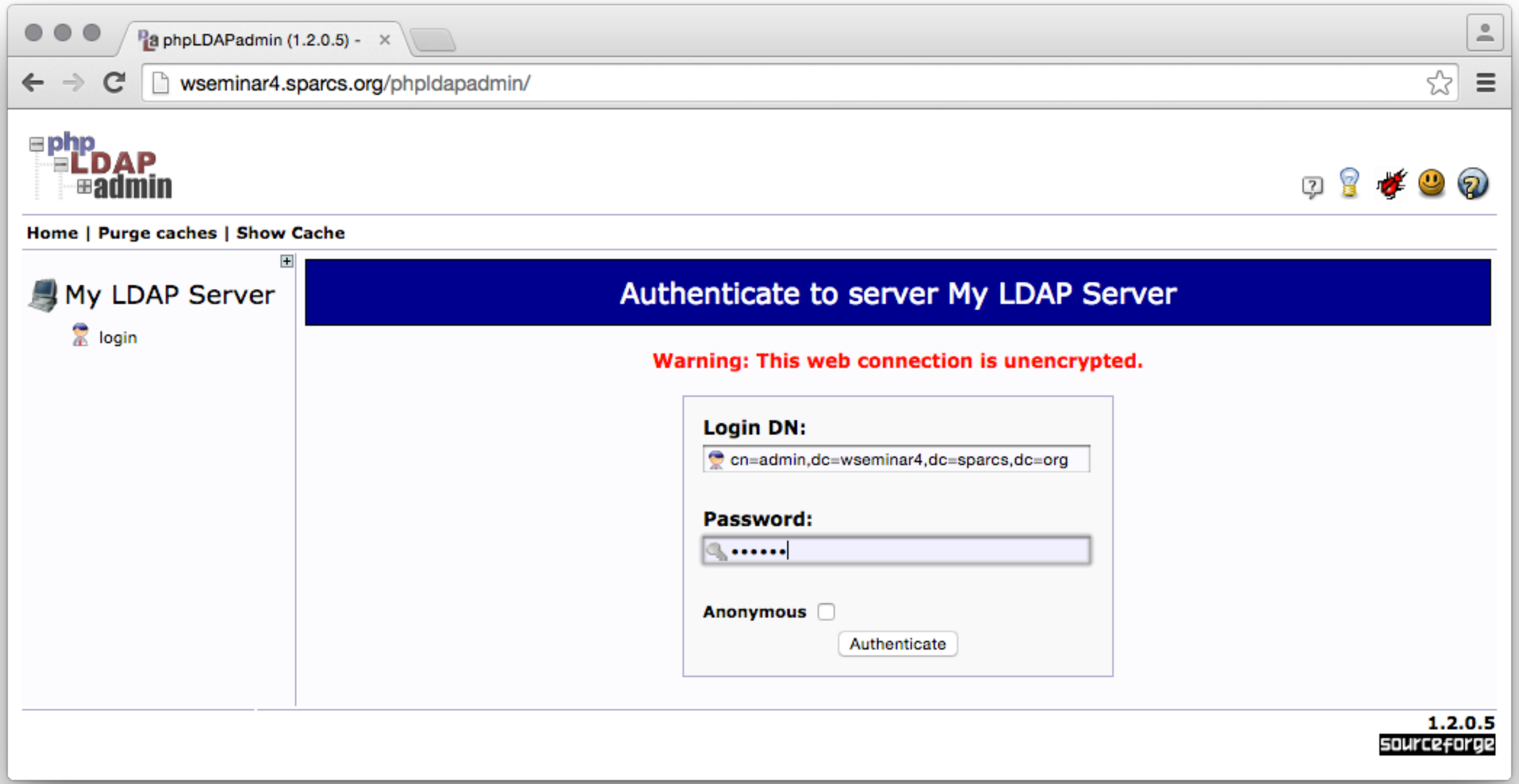
phpldapadmin 접속

- http://wseminar#.sparcs.org/phpldapadmin <- 접속



phpldapadmin 로그인

- 비밀번호는 아까 파란 화면에서 설정했던 비밀번호를 사용한다.



phpLDAPadmin

- 왼쪽에 보이는 트리는 `ldapsearch` 명령어로 검색한 내용과 동일하다.

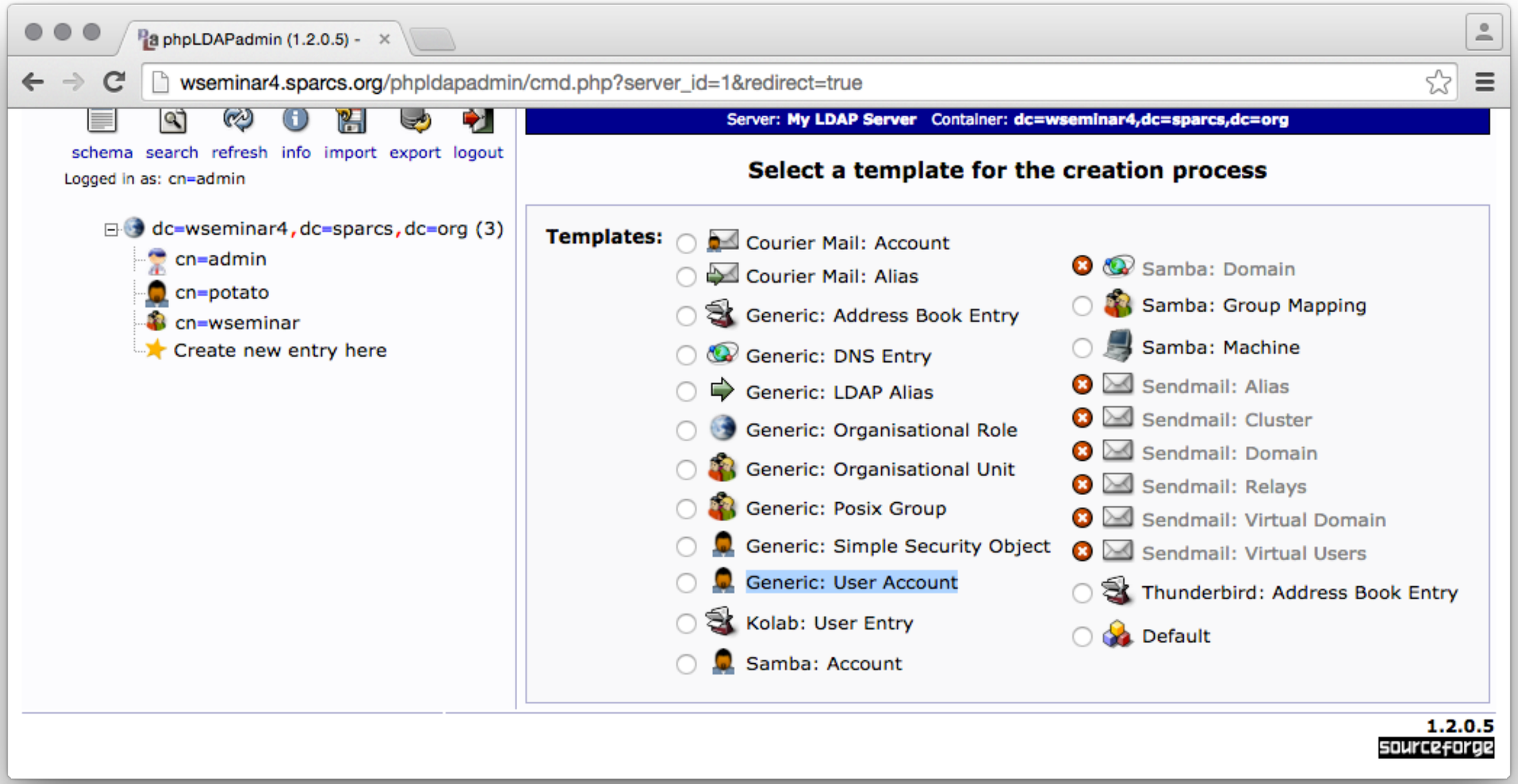
```
potato@wseminar4:~$ ldapsearch -x -LLL -b dc=wseminar4,dc=sparcs,dc=org dn
dn: dc=wseminar4,dc=sparcs,dc=org

dn: cn=admin,dc=wseminar4,dc=sparcs,dc=org

dn: cn=wseminar,dc=wseminar4,dc=sparcs,dc=org

dn: cn=potato,dc=wseminar4,dc=sparcs,dc=org
```

phpLDAPadmin에서 계정 추가하기

- ‘Create new entry here’ 클릭

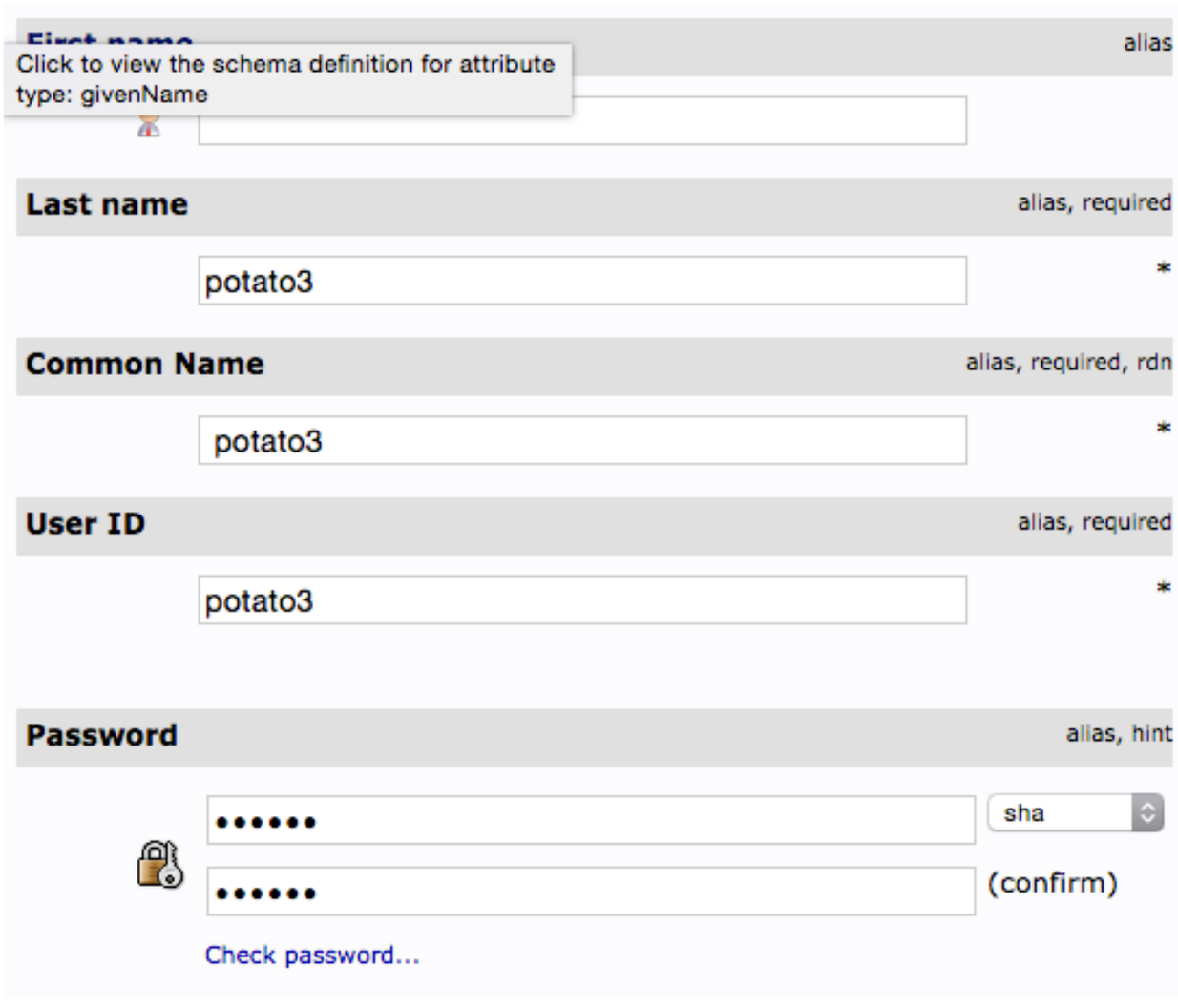
phpLDAPadmin에서 계정 추가하기

- ‘Generic: User Account’ 클릭

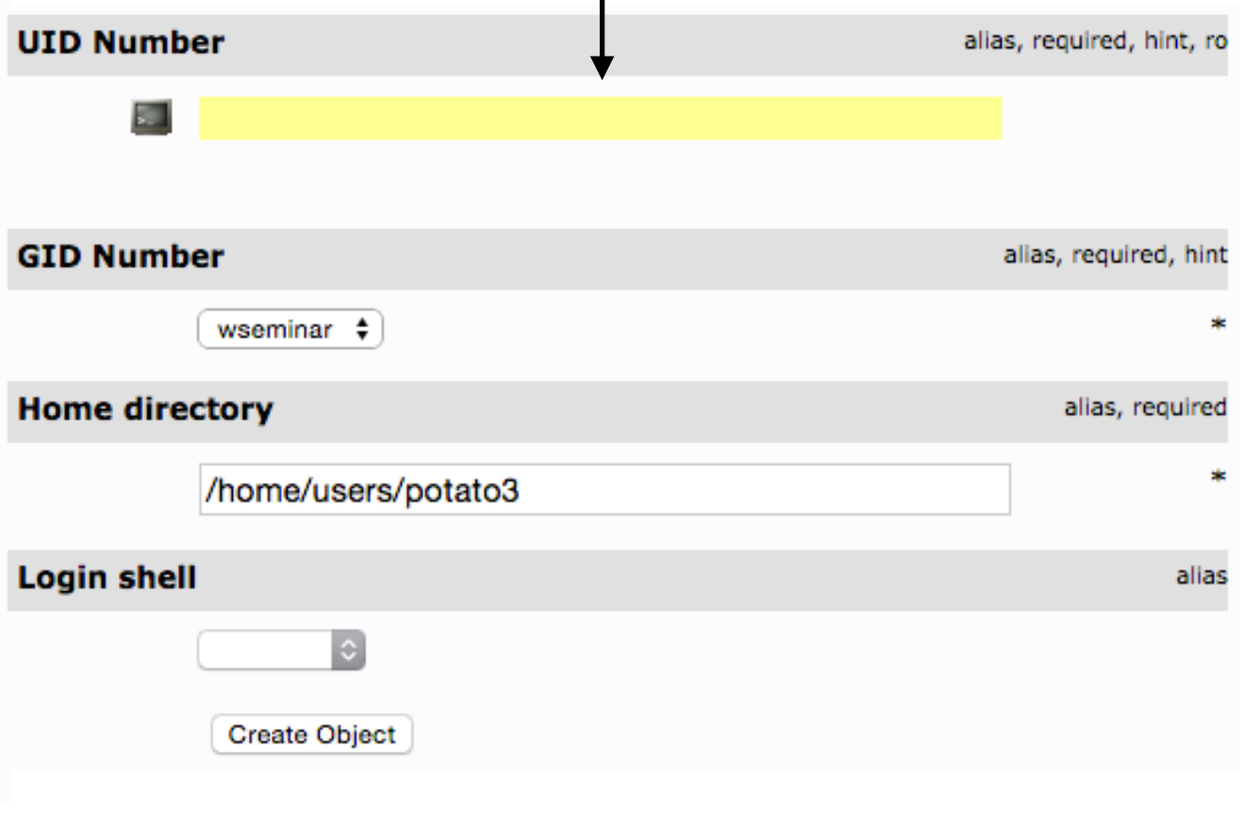


phpLDAPadmin에서 계정 추가하기

- 내용 입력하기

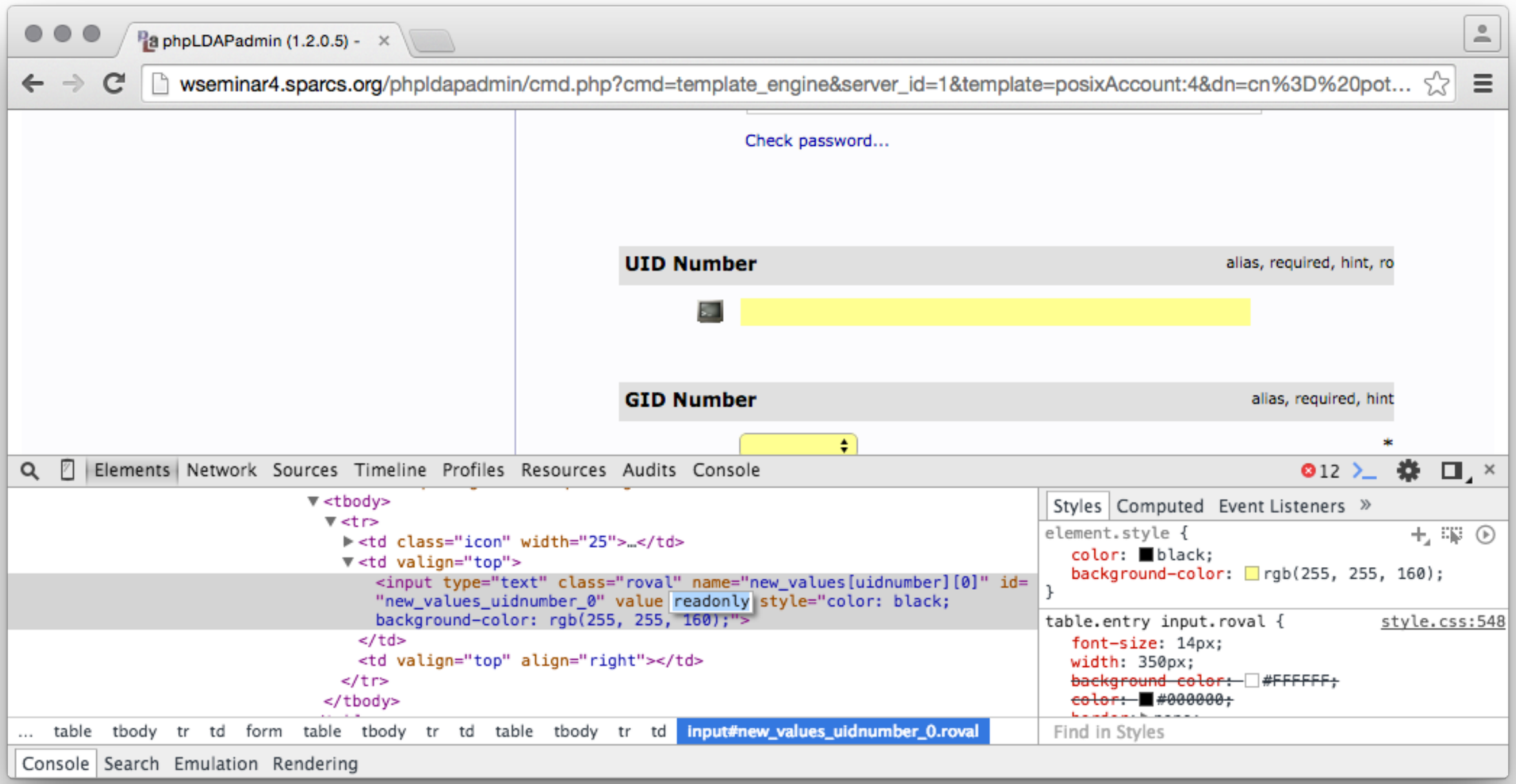


그런데 UID Number가 readonly 상태이다.



버그 수정

- ‘UID Number’가 readonly 상태인 것은 일종의 버그로 ‘우클릭 -> 요소검사 -> readonly 속성 삭제’를 하면 해결 가능하다.



버그 수정

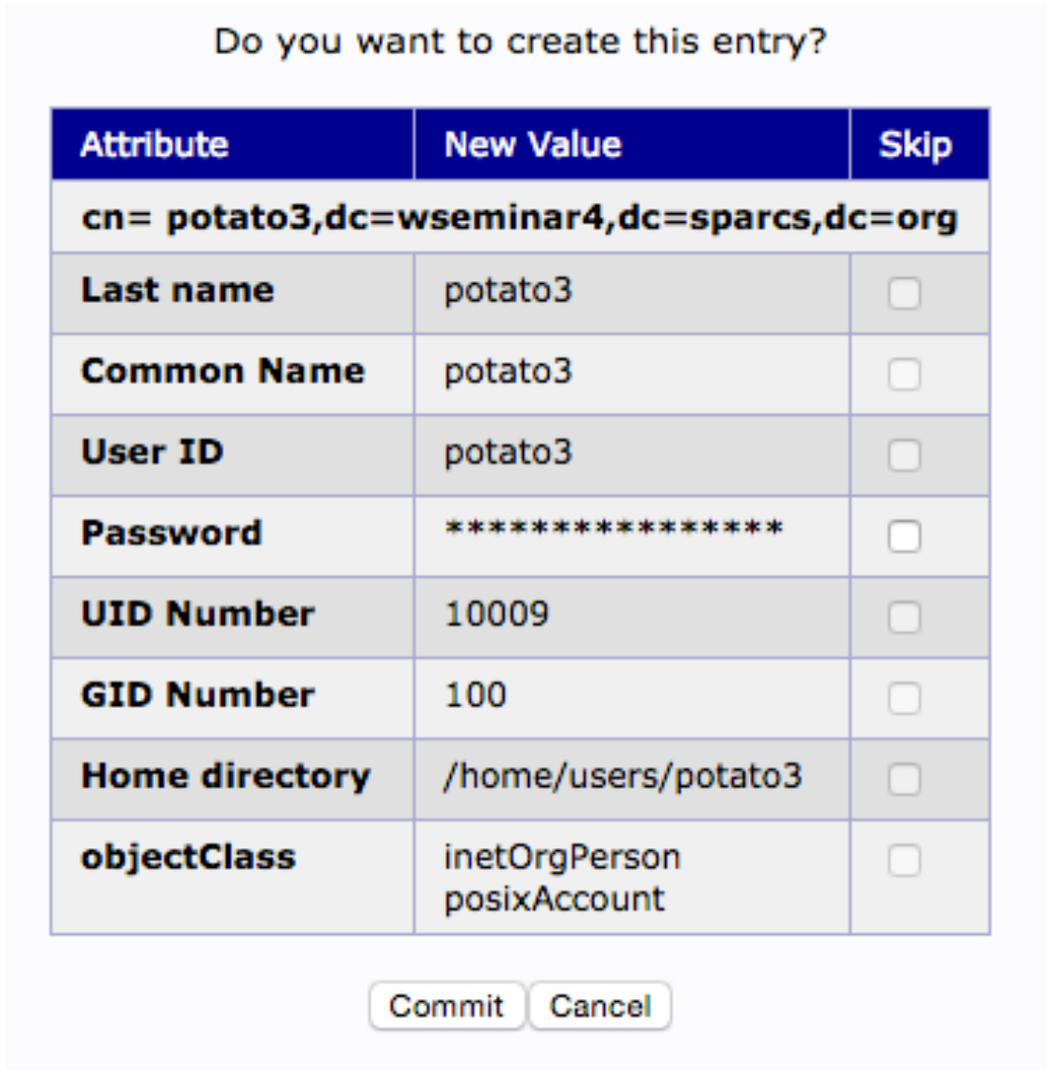
- 이 버그를 영구적으로 해결하는 방법은 다음과 같다.

```
sudo vi /etc/phpldapadmin/templates/creation/posixAccount.xml
```

```
<attribute id="uidNumber">
        <display>UID Number</display>
        <icon>terminal.png</icon>
        <order>6</order>
        <page>1</page>
<!--    <readonly>1</readonly> -->
        <value>=php.GetNextNumber(/;uidNumber)</value>
</attribute>
```

phpLDAPadmin에서 계정 추가하기

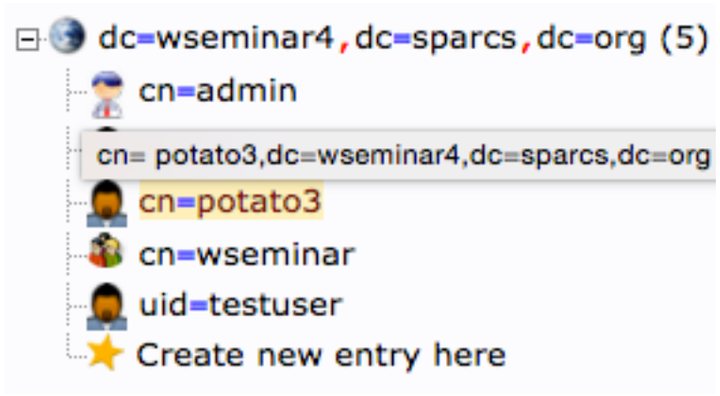
- ‘Create Object’ 버튼 클릭 후 확인창에서 ‘Commit’을 클릭한다.


Do you want to create this entry?

Attribute	New Value	Skip
cn= potato3,dc=wseminar4,dc=sparcs,dc=org		
Last name	potato3	☐
Common Name	potato3	☐
User ID	potato3	☐
Password	**********	☐
UID Number	10009	☐
GID Number	100	☐
Home directory	/home/users/potato3	☐
objectClass	inetOrgPerson posixAccount	☐

Commit Cancel

phpLDAPadmin에서 계정 추가하기

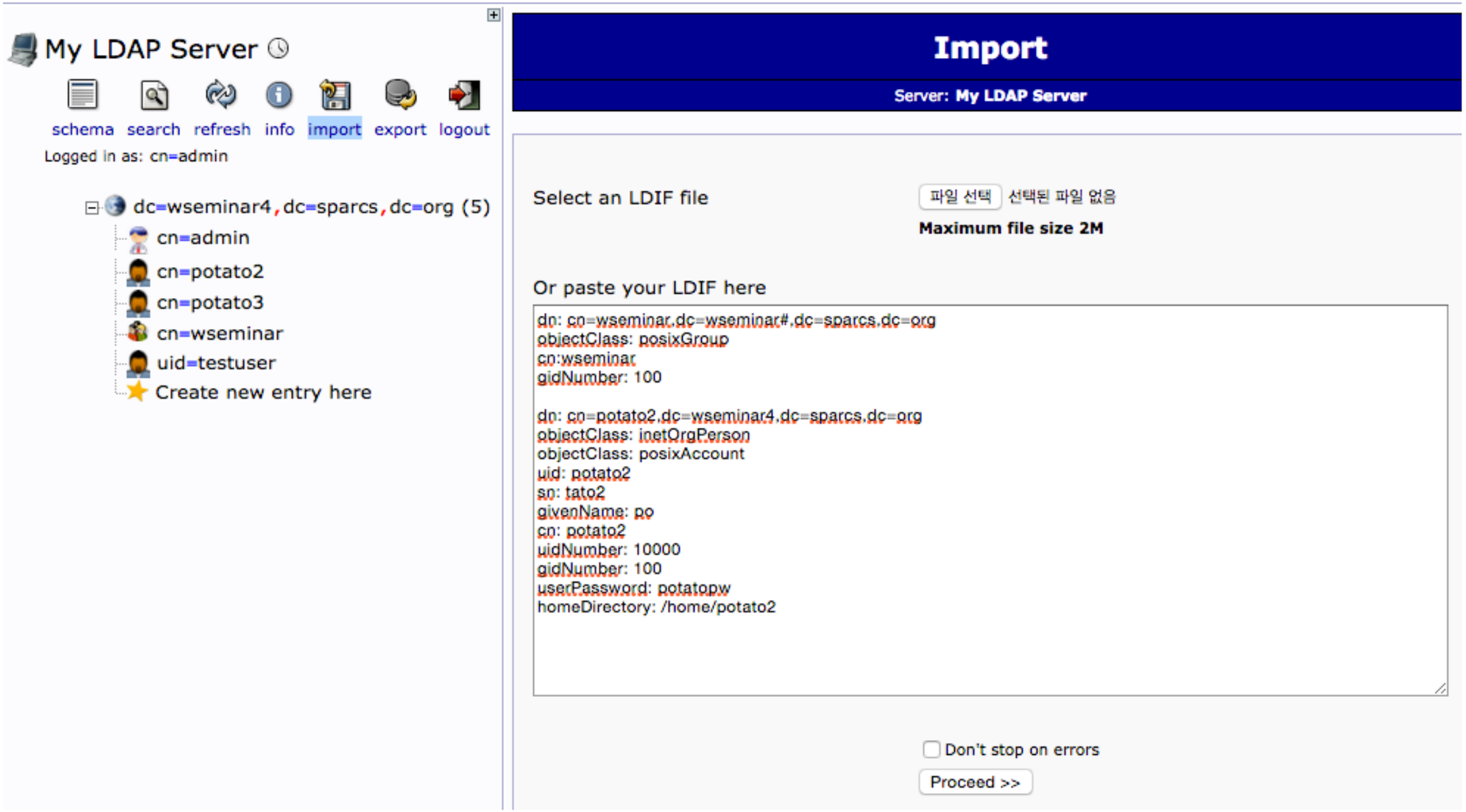


- 새로운 계정이 추가된 것을 확인한다.

```
potato@wseminar4:~$ ldapsearch -x -LLL -b dc=wseminar4,dc=sparcs,dc=org dn
dn: dc=wseminar4,dc=sparcs,dc=org

dn: cn=admin,dc=wseminar4,dc=sparcs,dc=org

dn: cn=wseminar,dc=wseminar4,dc=sparcs,dc=org

dn: uid=testuser,dc=wseminar4,dc=sparcs,dc=org

dn: cn=potato2,dc=wseminar4,dc=sparcs,dc=org

dn: cn=potato3,dc=wseminar4,dc=sparcs,dc=org
```

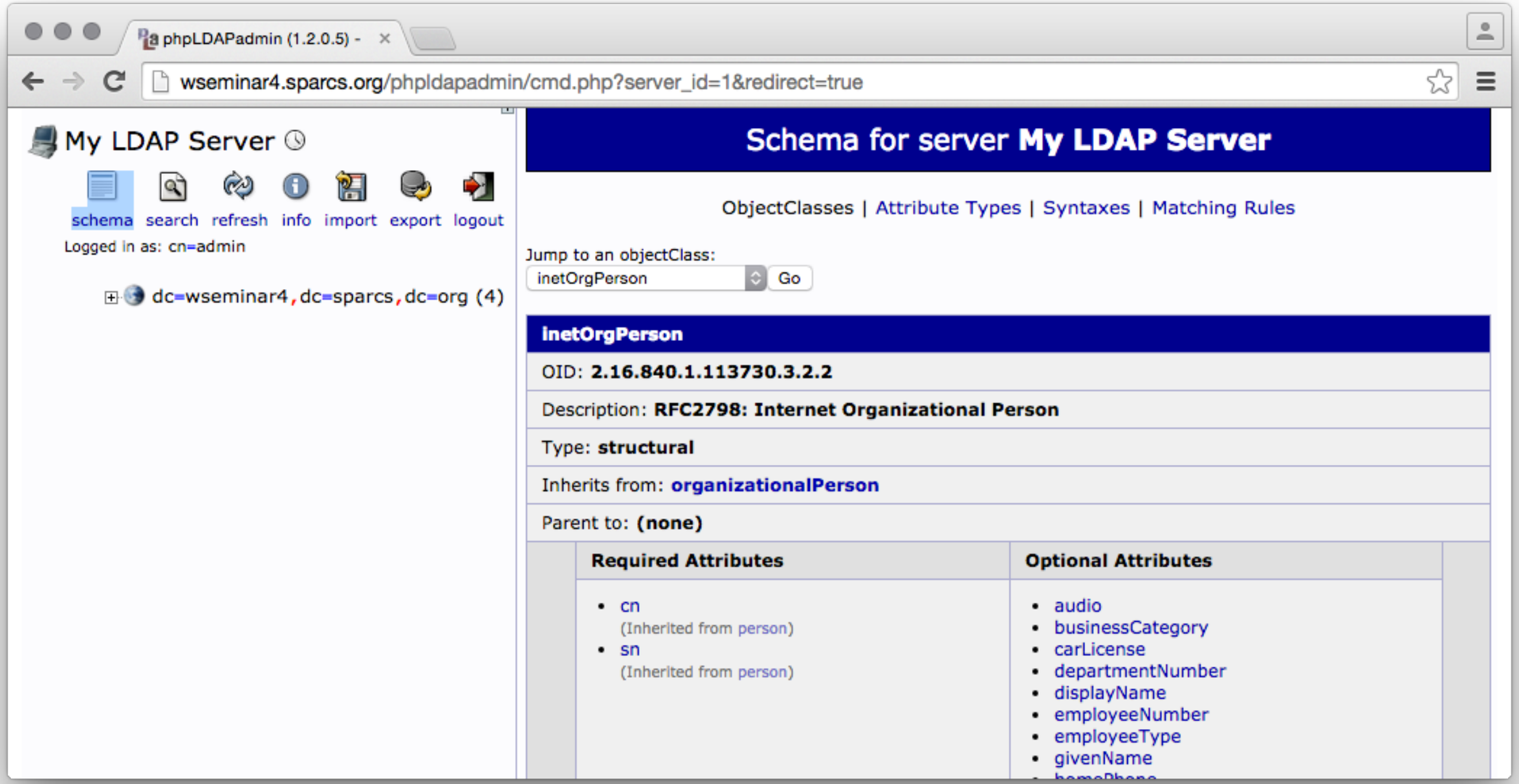
phpLDAPadmin import

- import 기능을 사용하면 GUI로도 .ldif 파일을 사용할 수 있다.



Schema 구경하기

- GUI로 보면 어떤 건지 쉽게 알 수 있다.



LDAP Client

NSS, PAM 설치

```
sudo apd-get install libnss-ldapd libpam-ldapd
```

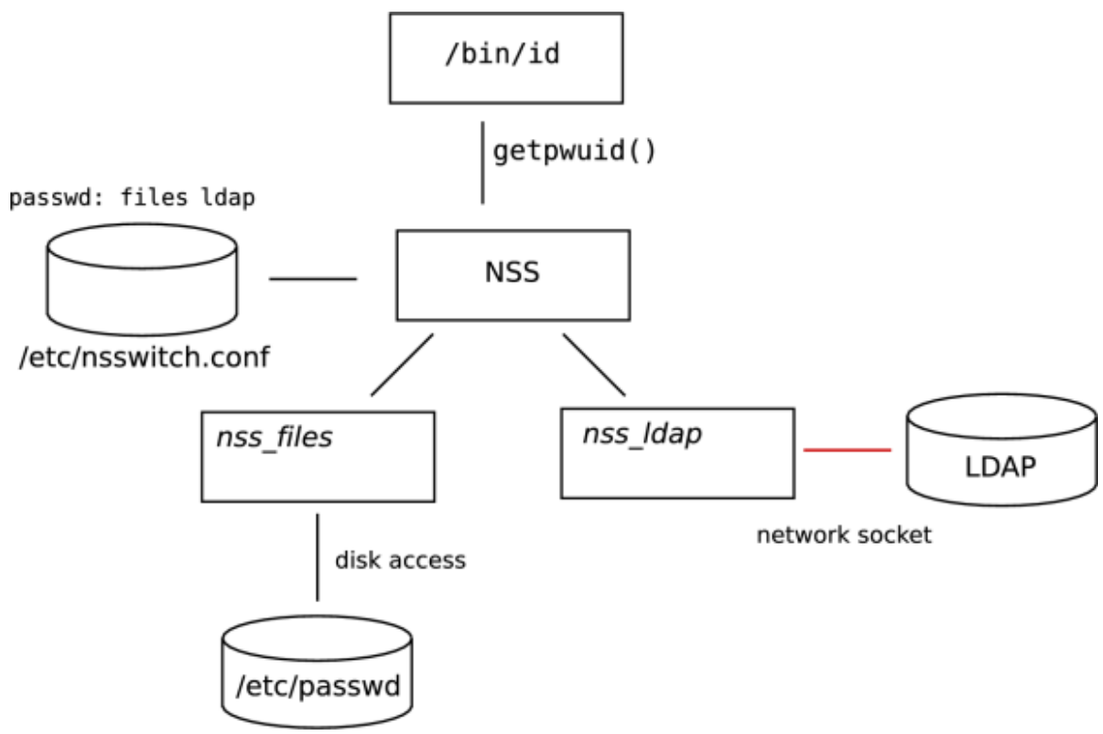
- ldap server 는 wsemianr4.sparcs.org

- 설정은 group, hosts, networks, passwd, shadow - 체크(스페이스바)

NSS

- Name Service Switch
- LDAP을 포함한 Name Service에 관련된 데이터를 어디서 받아올지 설정한다.

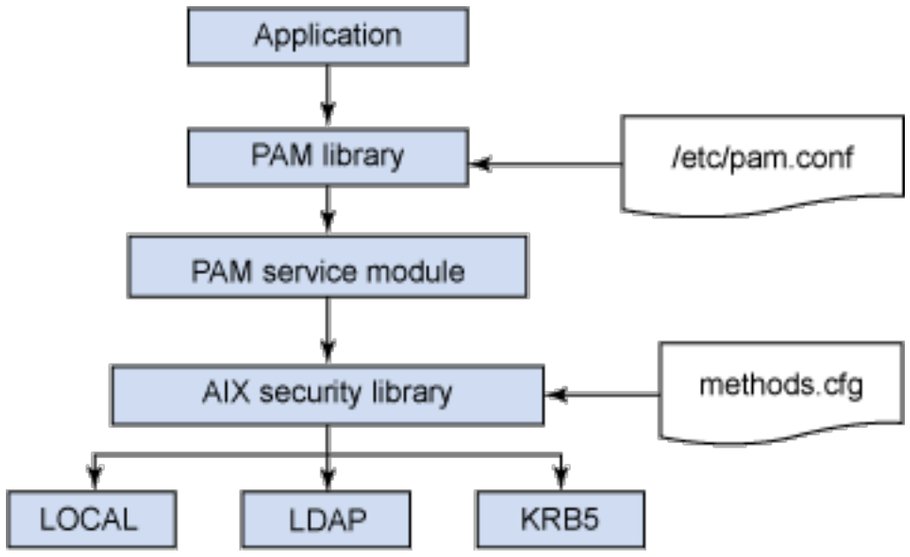
  예) ‘우리의 사용자 계정은 /etc/passwd 파일에도 있지만 LDAP 서버에도 있다는 사실을 잊지 말라고~’ 라고 여러분의 컴퓨터에게 알려준다.



PAM

- Pluggable authentication module
- low-level의 인증을 통합적으로 관리한다.
- 초창기에는 /etc/passwd 파일로 모든 사용자 인증을 관리했다.
- 그러던 어느날 새로운(더 안전한) 인증 방식을 도입하려고 하니 기존에 /etc/passwd 파일을 사용하던 모든 프로그램이 수정되어야 한다는 사실을 알게 됐다.
- ‘우리는 이런 비극을 반복해서는 안된다.’
- ‘인증만 따로 담당하는 놈을 하나 만들자.’

-> PAM 탄생



NSS 끄고 켜기

- nscd : Name Service Caching Daemon

```
sudo /etc/init.d/nscd [stop | start | restart]
```

- nslcd : Name Service LDAP Connection Daemon

```
sudo /etc/init.d/nslcd [stop | start | restart]
```

NSS 설정

sudo vi /etc/nslcd.conf

```
10. uri ldap://wseminar4.sparcs.org      <- 수정(이번에는 'wseminar4'로 추가)
13. base dc=wseminar4,dc=sparcs,dc=org   <- 수정(이번에는 'wseminar4'로 추가)
```

sudo vi /etc/nsswitch.conf

```
passwd:         files ldap              <- 수정(만약 'ldap'이 추가되어있지 않다면)
group:          files ldap              <- 수정(만약 'ldap'이 추가되어있지 않다면)
shadow:         files ldap              <- 수정(만약 'ldap'이 추가되어있지 않다면)

hosts:          files dns ldap          <- 수정(만약 'ldap'이 추가되어있지 않다면)
networks:       files ldap              <- 수정(만약 'ldap'이 추가되어있지 않다면)

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

확인

```
getent passwd
```

```
george:x:1003:1003:,,,:/home/george:/bin/bash
coearth:x:1004:1004:,,,:/home/coearth:/bin/bash
ftp:x:108:110:ftp daemon,,,:/srv/ftp:/bin/false
messagebus:x:109:111::/var/run/dbus:/bin/false
avahi:x:110:112:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
bind:x:103:105::/var/cache/bind:/bin/false
potato:x:1000:1000:,,,:/home/potato:/bin/bash
openldap:x:111:114:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
testuser:x:10005:100:Test User:/home/testuser:/bin/bash
potato2:*:10000:100:potato2:/home/potato2:
```

- 새로운 사용자가 생겼다.

확인

- putty에서 새롭게 추가된 계정으로 로그인 해보자.

- user name : testuser, password : testuser

- user name : potato2, password: potatopw

실습

- phpLDAPamin을 사용하거나, 새로 .ldif 파일을 작성해 새로운 사용자를 추가해 보자.

  (새로운 사용자가 가져야 하는 속성은 add.ldif 파일을 참고한다.)

- LDAP 서버를 본인의 서버로 바꾸어 추가된 사용자로 로그인 해 본다.

덧

- 우리는 이렇게 시작해서 결국 크고 아름다운 LDAP서버를 운영하게 된다.
- 하지만 어느날 이 커다란 서버를 다른 서버로 옮겨야 하는 상황이 온다.
- 이 때 사용자 정보가 약 2500개 쯤 된다고 하자.
- 이 데이터를 전부 .ldif 파일로 만들어 옮기거나, phpLDAPadmin에서 일일이 옮기고 싶지는 않을 것이다.
- 그래서 만들어진 것이 MigrationTools이다.

MigrationTools

- 설치 : `sudo apt-get install migrationtools`
- 설정 : `sudo vi /etc/migrationtools/migrate_common.ph`

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = “wseminar#.sparcs.org”;

# Default base
$DEFAULT_BASE = “dc=wseminar#,dc=sparcs,dc=org”;
```

- default DNS domain, base를 수정한다.

DB를 통째로 옮기기

```
sh /usr/share/migrationtools/migrate_all_online.sh

    1. dc=wseminar4,dc=sparcs,dc=org
    2. wseminar#
    3. cn=admin,dc=wseminar#,dc=sparcs,dc=org
    4. cn=admin,dc=wseminar#,dc=sparcs,dc=org
    5. [password]
    6. No
```

- 단, 먼저 slapd가 실행되어있어야 한다.