

# LDAP & pGina

2019 Wheel Seminar

HUBO

# LDAP

- LDAP (Lightweight Directory Access Protocol)
  - '가벼운' '디렉토리' '접근' '방식'

- Directory?

- ~~"/home/hubo.."~~ ~~"C:Windows..."~~
- 폴더라는 껍질 X
  - > '주소록'와 같은 데이터베이스 O (리스트)

이름	수정일	크기	종류
▶ 공용	2017년 6월 5일 오전 12:00	--	폴더
▶ 그림	2018년 11월 5일 오후 10:06	--	폴더
▶ 다운로드	그저께 오후 5:47	--	폴더
▶ 데스크탑	오늘 오전 12:31	--	폴더
▶ 문서	2019년 7월 1일 오후 3:37	--	폴더
▶ 동영상	2019년 2월 2일 오후 11:49	--	폴더
▶ 음악	2018년 12월 30일 오후 5:12	--	폴더
▶ 응용 프로그램	2019년 4월 20일 오후 7:29	--	폴더
▶ anaconda3	2019년 2월 22일 오후 4:11	--	폴더
▶ AndroidStudioProjects	2019년 2월 2일 오전 12:56	--	폴더

- Directory Service

- 기본 개념: Directory 라는 정보를 관리!!
- 그렇다면.. 어떤 '정보'?

di·rec·to·ry | diréktəri, dai- |

명사 {direct(안내하다) + ory(것)} (『복수』 -ries)

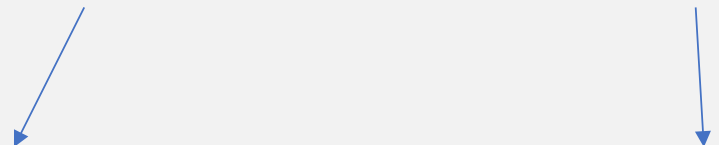
1. 주소 성명록, 인명록, 신사록; ( 빌딩의 ) 입주자 안내판
  - ▶ a telephone *directory*  
전화 번호부
  - ▶ an address *directory*  
주소록.
2. 지도서, 규칙서, (교회의) 예배 규칙서.
3. = [directorate](#).
4. [컴퓨터] 디렉터리: 외부 기억 장치에 들어있는 파일 목록; 특정 파일의 특정 기술서.
5. 《the Directory》[프랑스사] ( 프랑스 혁명 시대의 ) 집정 내각(1795-99).

# LDAP

Directory service:

*'분산 환경에 있는 다중 시스템 및 서비스에 대한 자원 정보 저장소' - IBM*

*+ 해당 자원에 대한 클라이언트 및 서버 어세스 제공*



**네트워크의 사용자, 컴퓨터, 프린터, 도메인, 서버, 사이트 등 => "정보"**

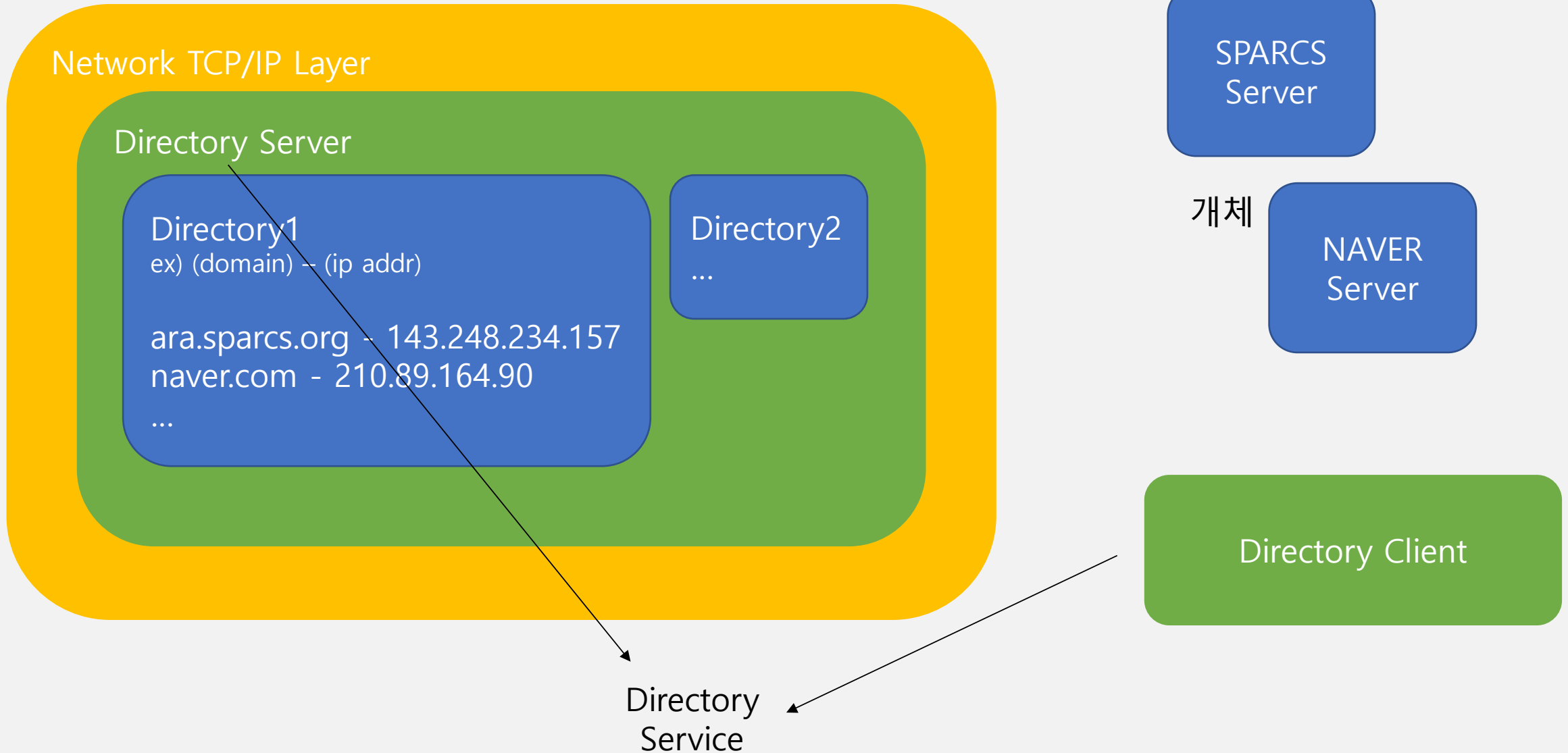
**+ 이 정보들을 제공하는 서버와, 접근하는 클라이언트 => "관리"**

ex) DNS 서버( ara.sparcs.org -> 143.248.234.157 ), SPARCS SSO( ID, passwd -> 로그인/실패 )

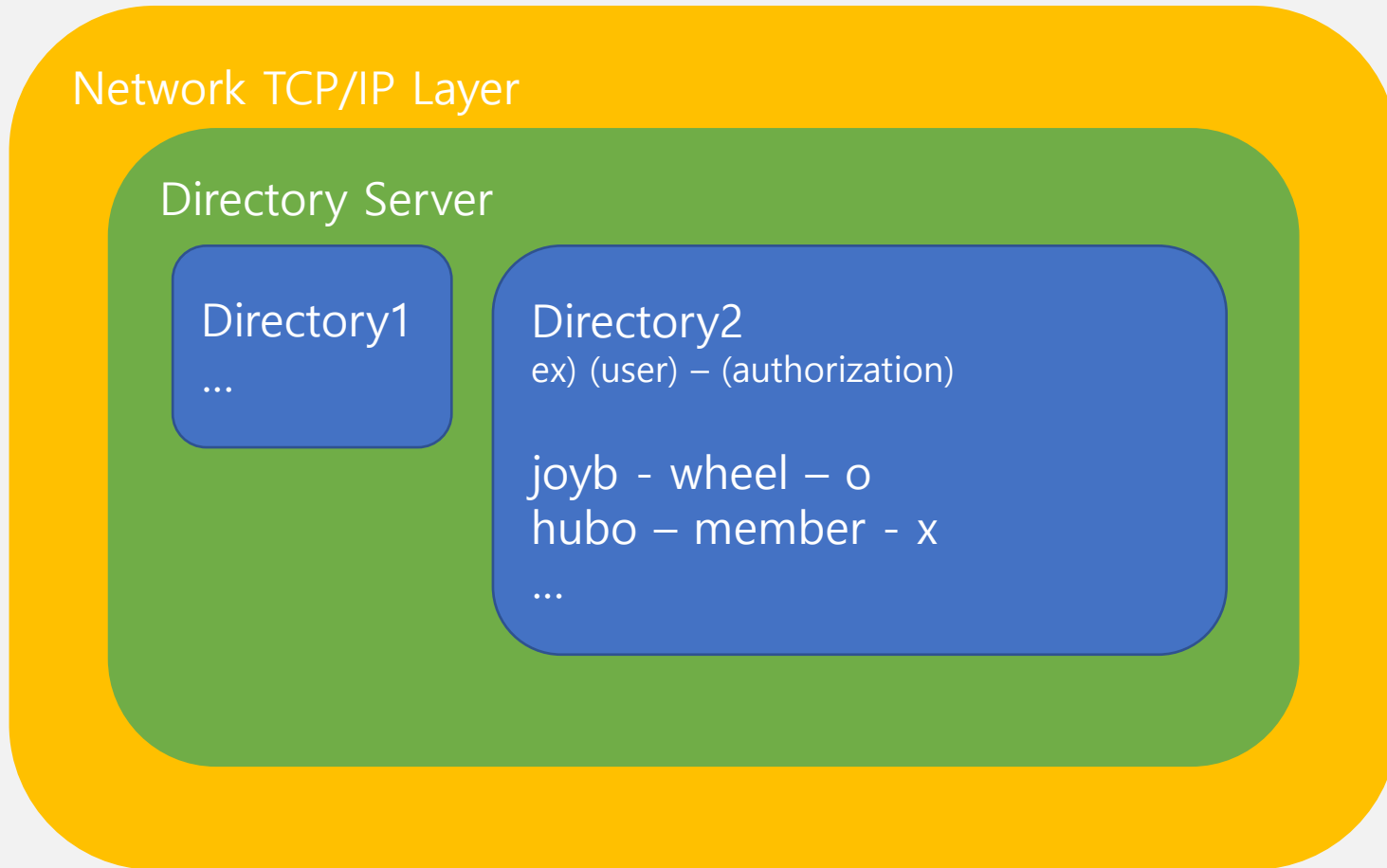
아 복잡해

- 결론: **Directory** 는 **네트워크(TCP/IP Layer)**에, 다른 **네트워크 개체들**에 대한 **정보**를 저장

# LDAP



# LDAP



개체



Hubo:  
member -> wheel

# LDAP

★정리★

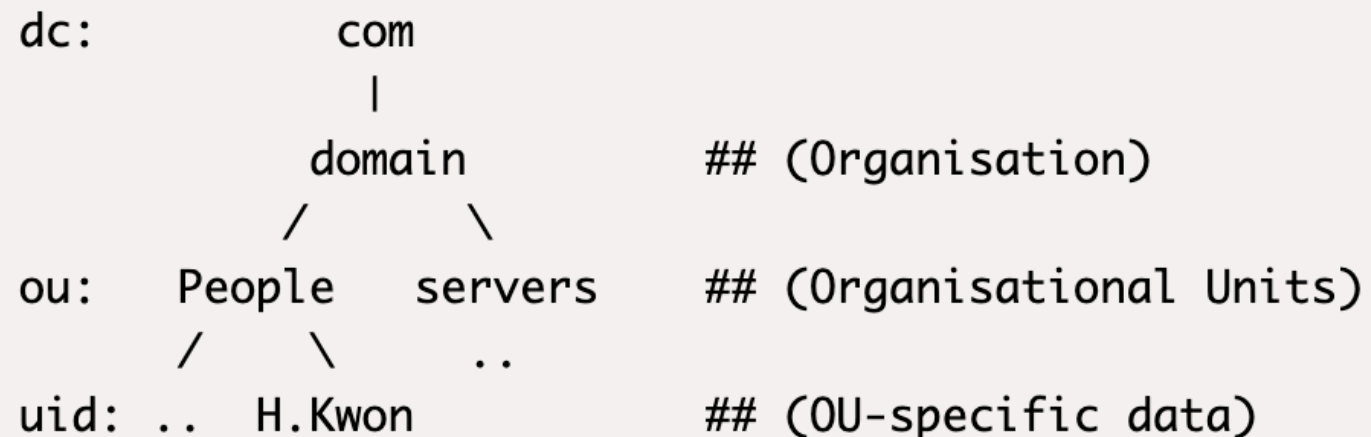
- LDAP
  - Directory service 의 표준 규격
  - 네트워크의 '정보 검색 서비스'
- DB vs LDAP
  - LDAP 은 일종의 DB
  - LDAP 은 'collection of information that's used to describe something'
  - '읽기'가 많이 이뤄지는 환경
- SSO vs LDAP
  - SSO 만들 때 LDAP 사용하기도 함.
  - ID/Passwd 가 맞으면 Access, 아니면 Denied
  - LDAP 은 ID 마다 서로 다른 권한, Manager, Professor, Student, ...
- 종류: Active Directory(windows), **OpenLDAP**(linux, macOS, windows)

# LDAP 의 구조

- DIT (Directory Information Tree)

- dn: uid=HyoungJo Bhang, ou=member, dc=sparcs, dc=org
- dn – 'distinguished name'
- uid – 'user id'
- ou – 'organization unit'
- dc – 'domain component'

ex) h.kwon@sparcs.org



# LDAP 의 구조

- Attribute
  - 각 개체가 가지는 속성 ex) 이름, 전화번호, 학과, ..

- ObjectClass
  - Attribute 의 집합!
  - 오른쪽의 audio \$ busin.. 로 구분!

- Schema
  - LDAP 서버에 정의 -> [old.sparcs.org](http://old.sparcs.org)
  - /etc/ldap/schema 안에 만든다.
  - Attribute 와 ObjectClass 를 정의해놓은 것

```
objectclass ( 2.16.840.1.113730.3.2.2
  NAME 'inetOrgPerson'
  DESC 'RFC2798: Internet Organizational Person'
  SUP organizationalPerson
  STRUCTURAL
  MAY (
    audio $ businessCategory $ carLicense $ departmentNumber $
    displayName $ employeeNumber $ employeeType $ givenName $
    homePhone $ homePostalAddress $ initials $ jpegPhoto $
    labeledURI $ mail $ manager $ mobile $ o $ pager $
    photo $ roomNumber $ secretary $ uid $ userCertificate $
    x500uniqueIdentifier $ preferredLanguage $
    userSMIMECertificate $ userPKCS12 )
)
```



# LDAP 의 구조

```
hubo@old:/etc/ldap/schema$ cat inetorgperson.schema
# inetorgperson.schema -- InetOrgPerson (RFC2798)
# $OpenLDAP$
## This work is part of OpenLDAP Software <http://www.openldap.org/>.
##
## Copyright 1998-2014 The OpenLDAP Foundation.
## All rights reserved.
##
## Redistribution and use in source and binary forms, with or without
## modification, are permitted only as authorized by the OpenLDAP
## Public License.
##
## A copy of this license is available in the file LICENSE in the
## top-level directory of the distribution or, alternatively, at
## <http://www.OpenLDAP.org/license.html>.
#
# InetOrgPerson (RFC2798)
#
# Depends upon
#   Definition of an X.500 Attribute Type and an Object Class to Hold
#   Uniform Resource Identifiers (URIs) [RFC2079]
#   (core.schema)
#
#   A Summary of the X.500(96) User Schema for use with LDAPv3 [RFC2256]
#   (core.schema)
#
#   The COSINE and Internet X.500 Schema [RFC1274] (cosine.schema)
#
# The version of this file as distributed by the OpenLDAP Foundation
# contains text from an IETF RFC explaining the schema. Unfortunately,
# that text is covered by a license that doesn't meet Debian's Free
# Software Guidelines. This is a stripped version of the schema that
# contains only the functional schema definition, not the text of the
```

```
attributetype ( 2.16.840.1.113730.3.1.1
    NAME 'carLicense'
    DESC 'RFC2798: vehicle license or registration plate'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( 2.16.840.1.113730.3.1.2
    NAME 'departmentNumber'
    DESC 'RFC2798: identifies a department within an organization'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

attributetype ( 2.16.840.1.113730.3.1.241
    NAME 'displayName'
    DESC 'RFC2798: preferred name to be used when displaying entries'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

attributetype ( 2.16.840.1.113730.3.1.3
    NAME 'employeeNumber'
    DESC 'RFC2798: numerically identifies an employee within an organization'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

attributetype ( 2.16.840.1.113730.3.1.4
    NAME 'employeeType'
    DESC 'RFC2798: type of employment for a person'
```

# OpenLDAP

- Server – Client
  - old.sparcs.org – hubo or ssal.sparcs.org?
- Server Setup
  - \$ sudo apt-get install slapd ldap-utils
    - slapd: Stand-alone LDAP Daemon
    - Ldap 설정을 위한 비밀번호 입력
  - \$ sudo dpkg-reconfigure slapd
    - No, [sparcs.org](http://sparcs.org), sparcs, 위에 설정한 비번, 비번확인, HDB, No, No, No
  - \$ /etc/init.d/slapd [start, stop, restart]
    - ex) \$ /etc/init.d/slapd restart



# OpenLDAP

- Search

- `$ ldapsearch -x -LLL -b dc=sparcs,dc=org`
  - `-x`: 인증 방식을 간단히
  - `-W`: 비밀번호를 prompt 로 물어봄
  - `-L`: 출력 형식을 간단하게! 1, 2, 3 모두 다름 (LDIF 형식)
  - `-b`: 필터

- dc 사이 띄면 안됨!
  - 하나의 이름이다

```
hubo@hubo-VirtualBox:/etc/ldap/schema$ ldapsearch -x -LLL -b dc=sparcs,dc=org
dn: dc=sparcs,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: sparcs
dc: sparcs

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

hubo@hubo-VirtualBox:/etc/ldap/schema$
```

# OpenLDAP

- Add

- LDIF (LDAP Data Exchange Format): LDAP 의 data 를 plain text 로 만든다.

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

```
dn: cn=hubo, dc=sparcs, dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
cn: hubo
sn: Bhang
uid: hubo
uidNumber: 2000
gidNumber: 100
homeDirectory: /home/hubo
```

\$ ~  
경로에서  
vi add.ldif 를 켜서 저장

# OpenLDAP

- Add

- \$ ldapadd -x -D cn=admin,dc=sparcs,dc=org -W -f add.ldif
  - -x: 인증 방식을 간단히
  - -W: 비밀번호를 prompt 로 물어봄
  - -D: 뒤에 추가하는 사람의 dn!! (admin 사용자)
  - -f: 뒤에 .ldif 파일
  - -c: 오류에도 멈추지 않음
- \$ ldapadd 혹은 \$ ldapmodify -a 둘다 가능

- 다시

- \$ ldapsearch -x -LLL -b dc=sparcs,dc=org

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

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

dn: cn=wheels,dc=sparcs,dc=org
objectClass: posixGroup
cn: wheels
gidNumber: 100

dn: cn=hubo,dc=sparcs,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
cn: hubo
sn: Bhang
uid: hubo
uidNumber: 2000
gidNumber: 100
homeDirectory: /home/hubo

hubo@hubo-VirtualBox:~$
```

# OpenLDAP

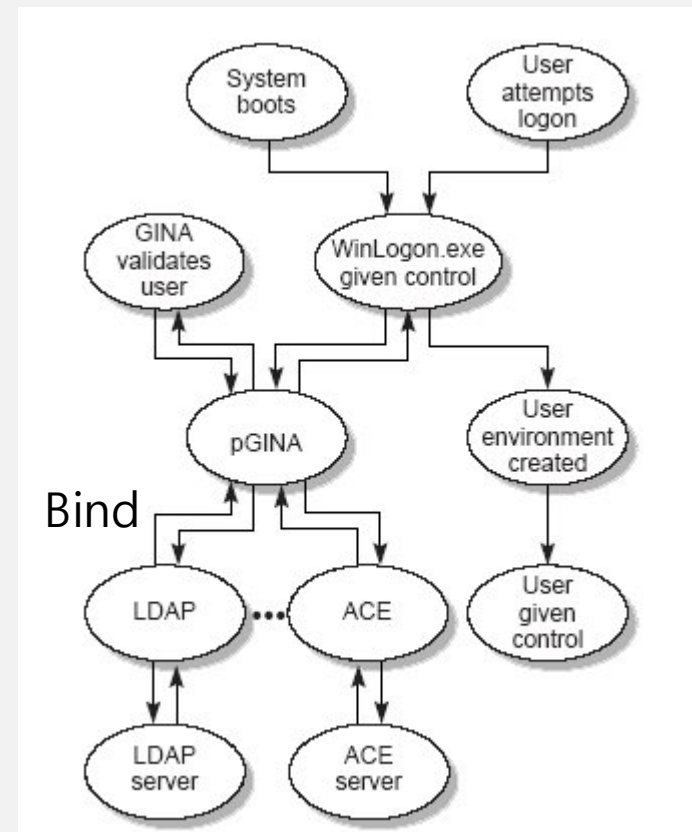
- Client Setup
  - NSS (Name Service Switch)
    - Name Service == Directory Service
    - 복습: 네트워크 상의 정보 저장소. 하나의 서버에 정보를 다 모아두고, 필요한 다른 서버의 요청이 들어오면 보내준다.
    - Name Service 'Switch': nsswitch.conf 라는 파일 자체!
    - 저 파일을 가지고 있으면, 어디서/어떤 순서로 정보를 찾을지를 설정.
    - Local(/etc/passwd, /etc/hosts)인지, DNS 인지, LDAP 인지~
  - \$ sudo apt-get install libnss-ldapd
  - /etc/nsswitch.conf
    - ns switch
  - /etc/nslcd.conf
    - ns LDAP connection daemon

# OpenLDAP

Information Sources	Description
files	A file stored in the client's <code>/etc</code> directory. For example, <code>/etc/passwd</code>
nisplus	An NIS+ table. For example, the <code>hosts</code> table.
nis	A NIS map. For example, the <code>hosts</code> map.
compat	Compat can be used for password and group information to support old-style <code>+</code> or <code>-</code> syntax in <code>/etc/passwd</code> , <code>/etc/shadow</code> , and <code>/etc/group</code> files.
dns	Can be used to specify that host information be obtained from DNS.
ldap	Can be used to specify entries be obtained from the LDAP directory.

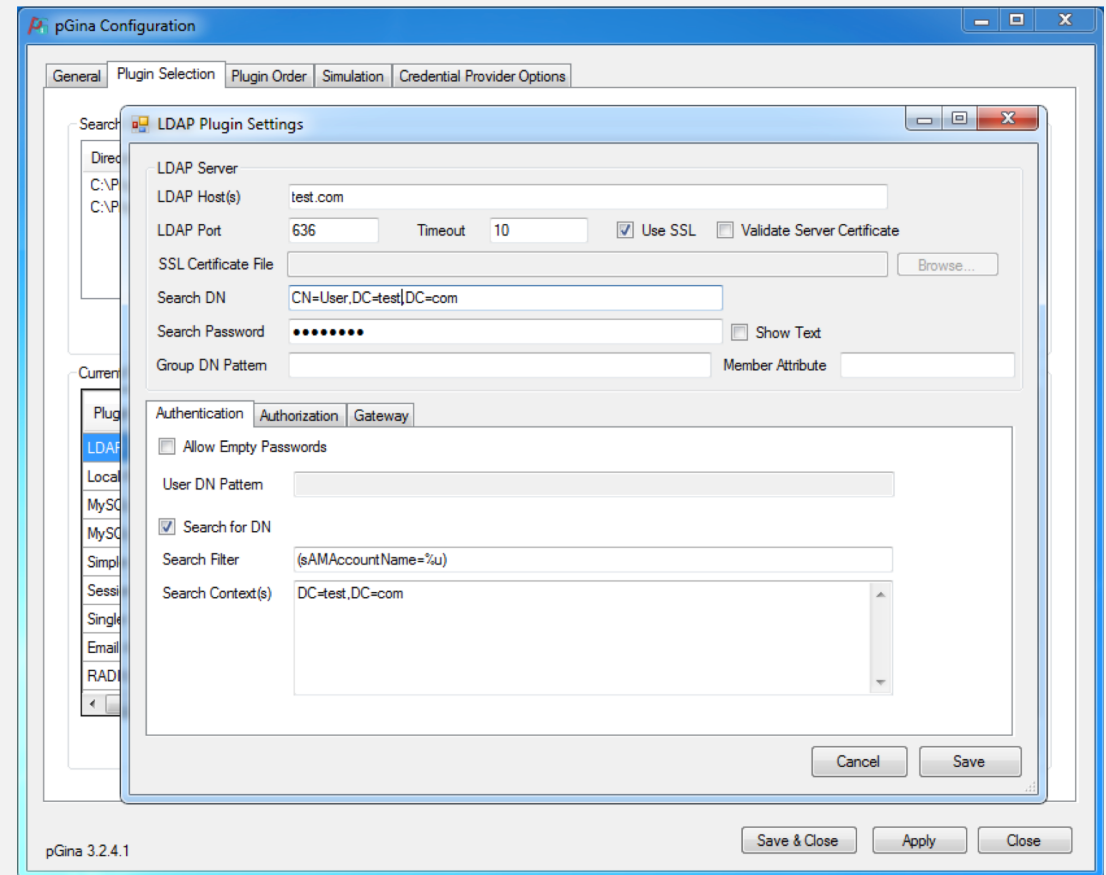
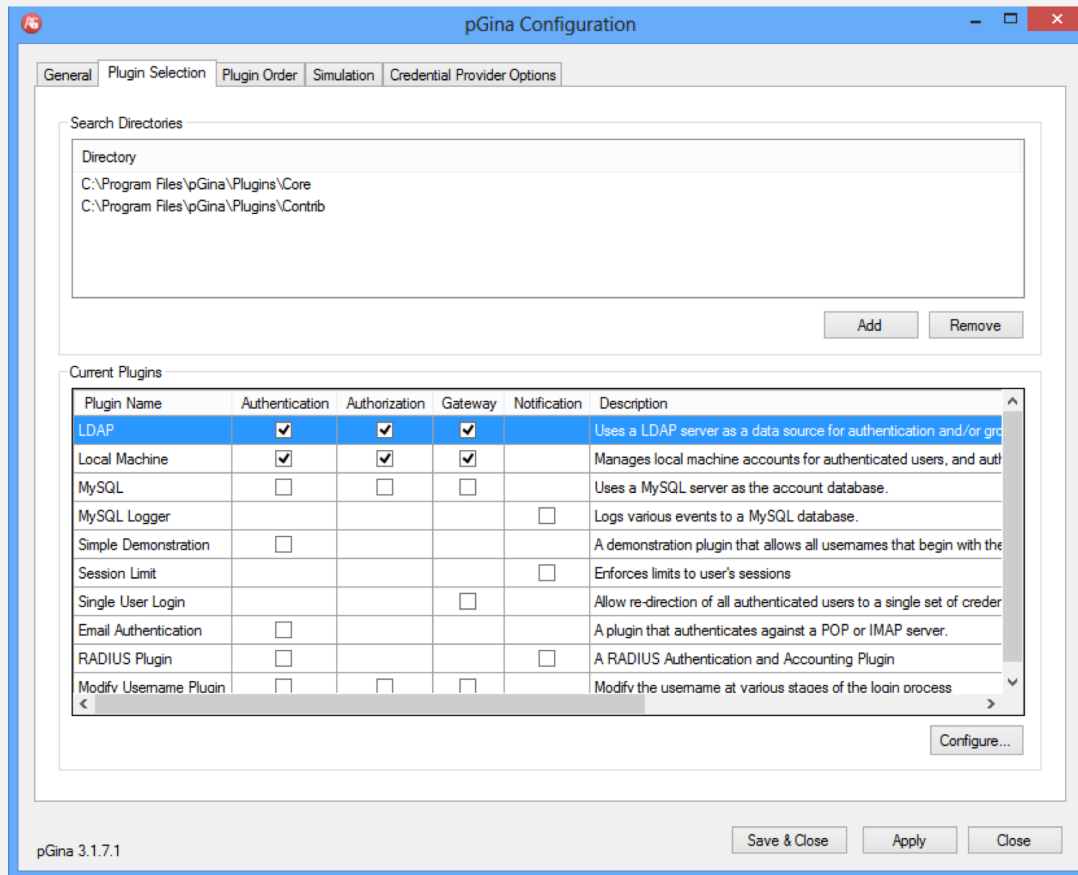
# pGina

- pGina (pluggable Graphical Identification and Authentication)
  - UNIX/macOS 에서 nsswitch 라면, Windows 는 pGina 로 관리.
    - UNIX/Linux/Windows 혼합 환경에 좋다.
    - ex) LDAP 가 이미 존재하거나, MySQL 로 사용자를 관리하고 싶을 때.
  - Windows 는 기존에 authentication(인증)을 위해 GINA/Credential Provider 를 사용
  - GINA 에 plug-in(확장팩)을 추가하면서 pGina 의 configure 에 따라 authentication module 을 불러온다!!
    - LDAP, MySQL, ..





# pGina



# pGina



감사합니다

Q&A

# END

## 정리

- /etc/ldap/schema
- \$ /etc/init.d/slaped [start, stop, restart]
- \$ ldapsearch -x -LLL -b dc=sparcs,dc=org
- \$ ldapadd -x -D cn=admin,dc=sparcs,dc=org -W -f add.ldif
- /etc/nsswitch.conf
- /etc/nslcd.conf

# References

- Directory service: <http://egloos.zum.com/gunsystems/v/6785259>,  
[https://www.ibm.com/support/knowledgecenter/ko/SSEPGG\\_11.1.0/com.ibm.db2.luw.admin.dbobj.doc/doc/c0004944.html](https://www.ibm.com/support/knowledgecenter/ko/SSEPGG_11.1.0/com.ibm.db2.luw.admin.dbobj.doc/doc/c0004944.html)
- LDAP 설명 wiki:  
[https://wiki.gentoo.org/wiki/Centralized\\_authentication\\_using\\_OpenLDAP/ko#LDAP.EB.8A.94\\_.EB.AC.B4.EC.97.87.EC.9D.B8.EA.B9.8C.EC.9A.94.3F](https://wiki.gentoo.org/wiki/Centralized_authentication_using_OpenLDAP/ko#LDAP.EB.8A.94_.EB.AC.B4.EC.97.87.EC.9D.B8.EA.B9.8C.EC.9A.94.3F)
- Coursera: <https://www.coursera.org/lecture/system-administration-it-infrastructure-services/what-is-a-directory-server-8HeT4>
- OpenLDAP: <https://www.openldap.org/>
- Ldapsearch 매개변수 표:  
[https://www.ibm.com/support/knowledgecenter/ko/SSKTMJ\\_9.0.1/admin/conf\\_tableofldapsearchparameters\\_t.html](https://www.ibm.com/support/knowledgecenter/ko/SSKTMJ_9.0.1/admin/conf_tableofldapsearchparameters_t.html)
- pGina: <http://www.informit.com/articles/article.aspx?p=330803&seqNum=2>, <https://github.com/pgina/pgina/wiki/How-pGina-Works>
- Wheel Seminar
  - 18: minguinho
  - 17: akais, yujingaya, victory
  - 16: null, nick
  - 15: potato, kis