LDAP 서버 설치 및 관리 (OpenLDAP, PAM auth)

2014 SPARCS WHEEL SEMINAR

CHOCHO 조현성

LDAP이란?

Lightweight Directory Access Protocol

TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜

경량 DAP!

- DAP는 OSI 프로토콜 스택에서 작동 + 컴퓨팅 자원을 많이 사용하는 무거운 프로토콜

Directory Services

OS의 디렉터리 안에 있는 정보를 저장, 정리, 제공하는 소프트웨어 시스템

- Directory: “파일 시스템을 관리하고, 각 파일이 있는 장소를 쉽게 찾도록 디스크의 요소를 분할/검색하는 정보를 포함하는 레코드의 집합“
  - Ex. 전화번호부: Name → Number
  - 사전: Word → Definition
  - DNA: Domain name → IP address

유저, 시스템, 네트워크, 서비스, 어플리케이션 등의 정보를 공유하여 intranet 및 internet applications 발전에 기여

X.500

전자 디렉터리 서비스를 전달하는 일련의 네트워크 표준

다음과 같은 프로토콜을 정의:

- **DAP (Directory Access Protocol)**
- DSP (Directory System Protocol)
- DISP (Directory Information Shadowing Protocol)
- DOP (Directory Operational Bindings Management Protocol)

LDAP

X.500의 경량판 DAP.

+	-
타 서비스간 통합인증에 용이	Transaction과 같은 개념 X
- 관리: 유지보수 비용 감소	→ 게시판처럼 내용 수정이 잦은 곳에서 쓰기 어려움
- 관리: 더욱 수월한 보안 문제 대응	통합인증과 같은 서비스에 적용하면 보안상 리스크가 큼
- 사용자: 재가입에 대한 피로도 감소	
쓰기보다 읽기에 특화된 DB → 간단한 조건으로 빠른 검색 가능	
한번에 한 개의 정보를 찾는데 적합 (사용자 로그인 처리, 직원 정보 조회 등등)	

LDAP의 사용

Centralization of user and group information

Authenticate users locally

Authenticate users in a web application

Create a shared address directory for mail agents

LDAP의 구조

DIT (Directory Information Tree)

- 계층적 구조 (hierarchical architecture)
- Entry
  - 트리 구조에서의 **노드 (Node)**
  - 하나의 데이터를 나타냄
  - DN(distinguished name)으로 구분
    - 자신의 위치와 고유성을 나타냄

Entry

속성 (attribute) 들을 가지고,

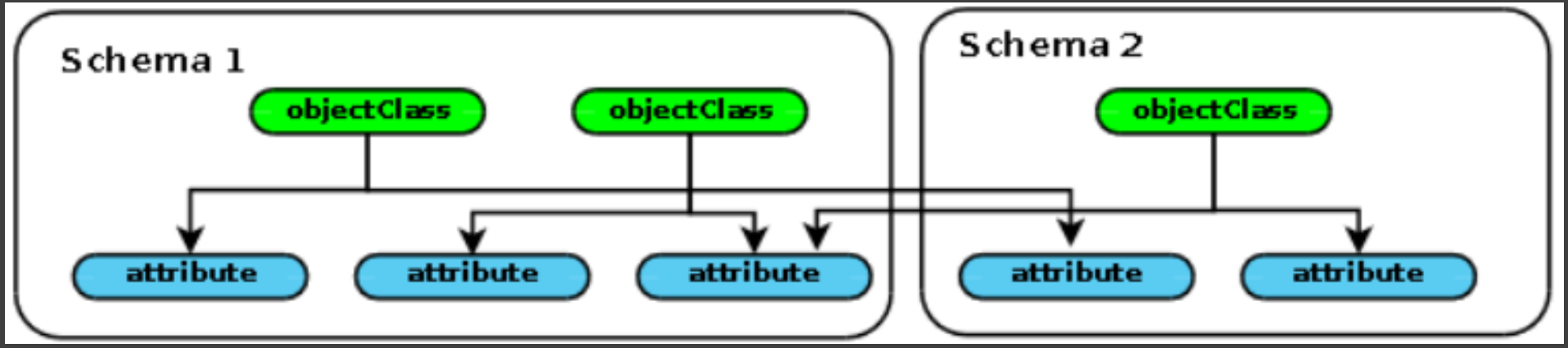
속성값 (attribute value) 들은 하나 이상의 값을 가질 수 있다

DN은 간결하게 축약하여 표시

Schema, objectClass, & attribute

objectClass: Schema에서 정의되는 attribute들의 collection

이러한 schema들은 /etc/ldap/schema에 정의되어있다 (나중에 설치하면서 살펴보자)



주로 사용되는 엔트리

cn (Common Name) : HYUNSUNG CHO 와 같은 일반적인 이름

sn (Sir Name) : 우리나라 성에 해당

ou (Organization Unit) : 그룹에 해당

dc (Domain Component) : 도메인의 요소

- ara.kaist.ac.kr 의 dc 는 kaist.ac.kr 또는 ara.kaist.ac.kr

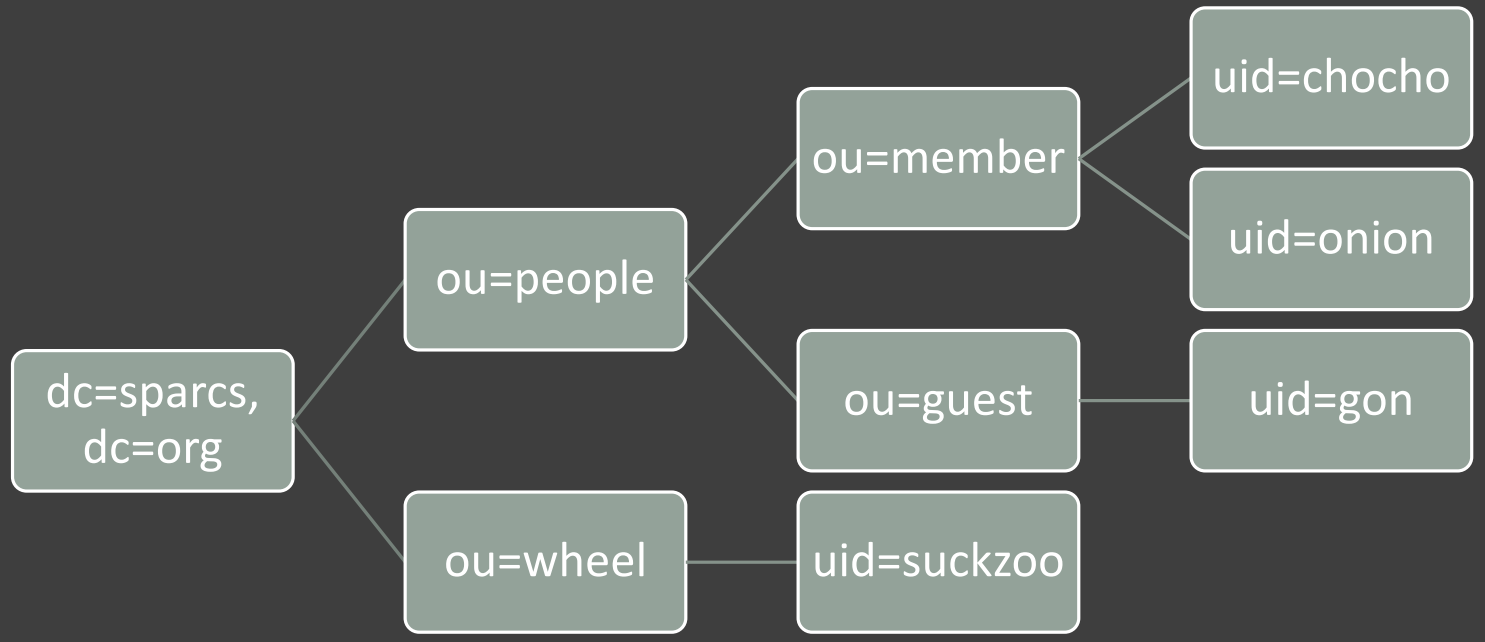
dn (Distinguished Name) : 고유의 이름

o : organization

c : country

uid : user id

Directory Information Tree



DN : “uid=chocho,ou=member,ou=people,dc=sparcs,dc=org”
RDN : “ou=wheel”, “uid=onion”

OpenLDAP

LDAP의 오픈소스 implementation

Linux 뿐만 아니라 다른 OS도 지원

frontend 와 backend 로 나눠짐

- frontend : network access와 protocol processing을 관리
- backend : data storage를 관리

Available Backends

현재 OpenLDAP 에서는 크게 세 부분으로 나뉘어진 16개의 backend가 지원된다.

Data Storage Backends (직접 데이터를 저장)

- back-bdb, hdb, ldif, mdb, ndb

Proxy Backends (다른 data storage 시스템으로 연결하는 게이트웨이 역할)

- back-ldap, meta, passwd, relay, sql

Dynamic Backends (그때그때 데이터를 생성하는 방식)

- back-config, dnssrv, monitor, null, perl, shell, sock

참조: http://en.wikipedia.org/wiki/OpenLDAP

Overall Concept

Installation

slapd : stand-alone LDAP daemon 을 설치해야 한다

$ sudo apt-get install slapd ldap-utils

Administrative credentials:
credentials for ***rootDN***

Post-install Inspection

/etc/ldap/slapd.d를 살펴보자

$ sudo ldapsearch –Q –LLL –Y EXTERNAL –H ldapi:/// -b cn=config dn

를 하면 slapd-config DIT가 어떻게 생겼는지 볼 수 있다

Post-install Inspection: Explanation of entries

cn=config: global settings

cn=module{0},cn=config: a dynamically loaded module

cn=schema,cn=config: contains hard-coded system-level schema

cn={0}core,cn=schema,cn=config: the hard-coded core schema

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

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

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

olcBackend={0}hdb,cn=config: the 'hdb' backend storage type

olcDatabase={-1}frontend,cn=config: frontend database, default settings for other databases

olcDatabase={0}config,cn=config: slapd configuration database (cn=config)

olcDatabase={1}hdb,cn=config: your database instance (dc=examle,dc=com)

Post-install Inspection

Default 값으로 dc=nodomain이 설정되어 있다

$ ldapsearch –x –LLL –H ldap:/// -b dc=nodomain dn 으로 확인

$ sudo dpkg-reconfigure slapd 로 바꿔주자

$ ldapsearch –x –LLL –H ldap:// -b dc=wseminar4,dc=sparcs,dc=org dn 로 재확인

Modifying/Populating your Database – (1) Add

Database에 추가해보자

1. a node called *People* (to store users)
2. a node called *Groups* (to store groups)
3. a group called *wheel*
4. A user called *'yourid'*

Modifying/Populating your Database – (1) Add

$ vi add_content.ldif

```
dn: ou=Groups,dc=wseminar4,dc=sparcs,dc=org
objectClass: organizationalUnit
ou: Groups

dn: cn=wheel,ou=Groups,dc=wseminar4,dc=sparcs,dc=org
objectClass: posixGroup
cn: wheel
gidNumber: 5000

dn: uid=chocho,ou=People,dc=wseminar4,dc=sparcs,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: chocholdap
sn: Cho
givenName: Hyunsung
cn: Hyunsung Cho
displayName: Hyunsung Cho
uidNumber: 10000
gidNumber: 5000
userPassword: chocholdap
gecos: Hyunsung Cho
loginShell: /bin/bash
homeDirectory: /home/chocho
```

LDIF (LDAP Data Interchange Format)

LDAP은 원래 binary protocol!

LDIF가 LDAP content를 다음과 같은 형태의 텍스트로 바꿔줌

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

LDIF – 데이터 변경 형식

dn: cn=Hyunsung Cho, ou=people, dc=sparcs, dc=org

changetype: modify

replace:cn

cn: Chocho Cho

<DN of the entry>
Changetype: [modify | add | delete]
(if changetype is modify)[replace | add | delete]:
<attribute>

Modifying/Populating your Database – (1) Add

LDAP에 추가하기

- $ ldapadd –x –D cn=admin, dc=wseminar4,dc=sparcs,dc=org –W –f add_content.ldif

```
chocho@wseminar4:~$ sudo ldapadd -x -D cn=admin,dc=wseminar4,dc=sparcs,dc=org -W -f add_content.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=wseminar4,dc=sparcs,dc=org"

adding new entry "ou=Groups,dc=wseminar4,dc=sparcs,dc=org"

adding new entry "cn=wheel,ou=Groups,dc=wseminar4,dc=sparcs,dc=org"

adding new entry "uid=chocho,ou=People,dc=wseminar4,dc=sparcs,dc=org"
```

-D : 뒤에 사용자의 entry dn을 적는다. ID와 비슷한 개념이다.

-W : 이 명령어를 사용시 비밀번호를 물어본다.

-f : 뒤에 ldif 파일을 받게 한다.

Modifying/Populating your Database – (1) Add

ldapsearch를 사용해서 제대로 추가되었는지 확인

- $ ldapsearch –x –LLL –b dc=wseminar4,dc=sparcs,dc=org ‘uid=chocho’ cn gidNumber

```
chocho@wseminar4:~$ ldapsearch -x -LLL -b dc=wseminar4,dc=sparcs,dc=org 'uid=chocho' cn gidNumber
dn: uid=chocho,ou=People,dc=wseminar4,dc=sparcs,dc=org
cn: Hyunsung Cho
gidNumber: 5000
```

- *-x:* "simple" binding; will not use the default SASL method
- *-LLL:* disable printing extraneous information
- *uid=chocho:* a "filter" to find the john user
- *cn gidNumber:* requests certain attributes to be displayed (the default is to show all attributes)

More about “ldapsearch”

Filter

- Equality (완전매칭) : “uid=chocho”
- Substring (부분 문자열 매칭) : “uid=ch*”
- Approximate (유사한 단어 매칭) : “uid~=choch”
- Less than, greater than (사전순서상의 크기로 매칭) : “uid>=chocho”
- And: “&(uid=chocho)(gidNumber=1000)”
- Or: |
- Not: !

MigrationTools

DB의 양이 많으면 일일이 ldif 파일로 옮겨 적기 귀찮으니까 쓰는 툴

$ sudo apt-get install migrationtools

$ vi /etc/migrationtools/migrate_common.ph #Edit default domain & base

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = “wseminar4.sparcs.org”;
# Default base
$DEFAULT_BASE = “dc=wseminar4,dc=sparcs,dc=org”;
```

MigrationTools 이용해서 전체 DB 옮기기

($ sudo service slapd start)

$ cd /usr/share/migrationtools

$ sh ./migrate_all_online.sh

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

MigrationTools: 기존 계정 Import 하기

/usr/share/migrationtools 폴더를 보면 여러 스크립트들이 있다

이 스크립트와 piping 을 이용해서 간단하게 import가 가능하다

ex.) authentication을 import 해보자

$ cd /usr/share/migrationtools

$ ./migrate_passwd.pl /etc/passwd >passwd.ldif

※ 시스템 계정은 공유하면 안되니 passwd.ldif 에서 미리 지우도록 한다.

$ ldapadd –h localhost –x –W –D “cn=admin,dc=wseminar4,dc=sparcs,dc=org” –c –f passwd.ldif

Modifying the slapd Configuration DB

ldapmodify를 이용해 *{1}hdb,cn=config* DB에 “Index”를 추가해보자

$ vi uid_index.ldif

```
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: uid eq,pres,sub
```

$ sudo ldapmodify –Q –Y EXTERNAL –H ldapi:/// -f uid_index.ldif

$ sudo ldapsearch –Q –LLL –Y EXTERNAL –H ldapi:/// -b \ #Confirm the change
> cn=config ‘(olcDatabase={1}hdb)’ olcDbIndex

Logging

직접 slapd-config DB를 바꿔서 Activity log를 출력할 수 있다

$ vi logging.ldif

```
dn: cn=config
changetype: modify
add: olcLogLevel
olcLogLevel: stats
```

$ sudo ldapmodify –Q –Y EXTERNAL –H ldapi:/// -f logging.ldif

Logging

너무 많은 메시지가 출력되면 rsyslog의 configuration을 수정

/etc/rsyslog.conf 에 다음을 추가:

```
# Disable rate limiting
# (default is 200 messages in 5 seconds; below we make the 5 become 0)
$ SystemLogRateLimitInterval 0
```

$ sudo service rsyslog restart

Access Control Lists (ACL)

ldapsearch로 ACL 검색!

ex) DB의 ACL 엔트리 검색:

- $ sudo ldapsearch –Q –LLL –Y EXTERNAL –H ldapi:/// -b \
  > cn=config ‘(olcDatabase={1}hdb)’ olcAccess

```
chocho@wseminar4:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
> cn=config '(olcDatabase={1}hdb)' olcAccess
dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymou
 s auth by dn="cn=admin,dc=wseminar4,dc=sparcs,dc=org" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=wseminar4,dc=sparcs,dc=org
 " write by * read
```

Access Control Lists (ACL)

```
chocho@wseminar4:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
> cn=config '(olcAccess=*)' olcAccess olcSuffix
[sudo] password for chocho:
dn: olcDatabase={-1}frontend,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
 ,cn=auth manage by * break
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read

dn: olcDatabase={0}config,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
 ,cn=auth manage by * break

dn: olcDatabase={1}hdb,cn=config
olcSuffix: dc=wseminar4,dc=sparcs,dc=org
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymou
 s auth by dn="cn=admin,dc=wseminar4,dc=sparcs,dc=org" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=wseminar4,dc=sparcs,dc=org
 " write by * read
```

LDAP Authentication

LDAP server를 만들었으니 client도 만들어보자!

NSS와 PAM 두 개로 나누어 설정

NSS란?

Name Service Switch

Does the name lookups to an LDAP directory server

/etc/nsswitch.conf 파일을 보자

NSS Setup

원래는 libnss-ldap 패키지를 사용하는 것이 일반적이었으나

여러 단점들을 보완하여 사용하기도 더욱 간편한 libnss-ldapd가 나왔다

NSS Installation Using libnss-ldapd

$ sudo apt-get install libnss-ldapd

LDAP server의 URI와 base DN 설정
(wseminar4.sparcs.org OR dc=‘’’wseminar4’’’,dc=‘’’sparcs’’’,dc=‘’’org’’’)

잘 동작하는지 확인하려면?

$ sudo getent passwd

* libnss-ldap로 설정하는 법은 여기 → https://wiki.debian.org/LDAP/NSS

NSS Installation Using libnss-ldap

$ sudo apt-get install libnss-ldapd

$ vi /etc/libnss-ldap.conf

```
# Your LDAP server. Must be resolvable without usint LDAP.
uri ldap://wseminar4.sparcs.org

# The distinguished name of the search base.
base dc=wseminar4,dc=sparcs,dc=org
```

NSS Installation Using libnss-ldap

$ vi /etc/nsswitch.conf

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns ldap
networks:       files ldap

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

netgroup:       nis
```

How to Debug

/etc/init.d/nscd stop

/etc/init.d/nslcd start

nslcd –d

nscd = name service caching daemon

nslcd = local LDAP name service daemon

PAM 이란?

Pluggable Authentication Module

Does authentication to an LDAP server

모든 서비스에 대해 일일이 인증할 필요 없게
중앙 집중적으로 인증을 도와주는 모듈

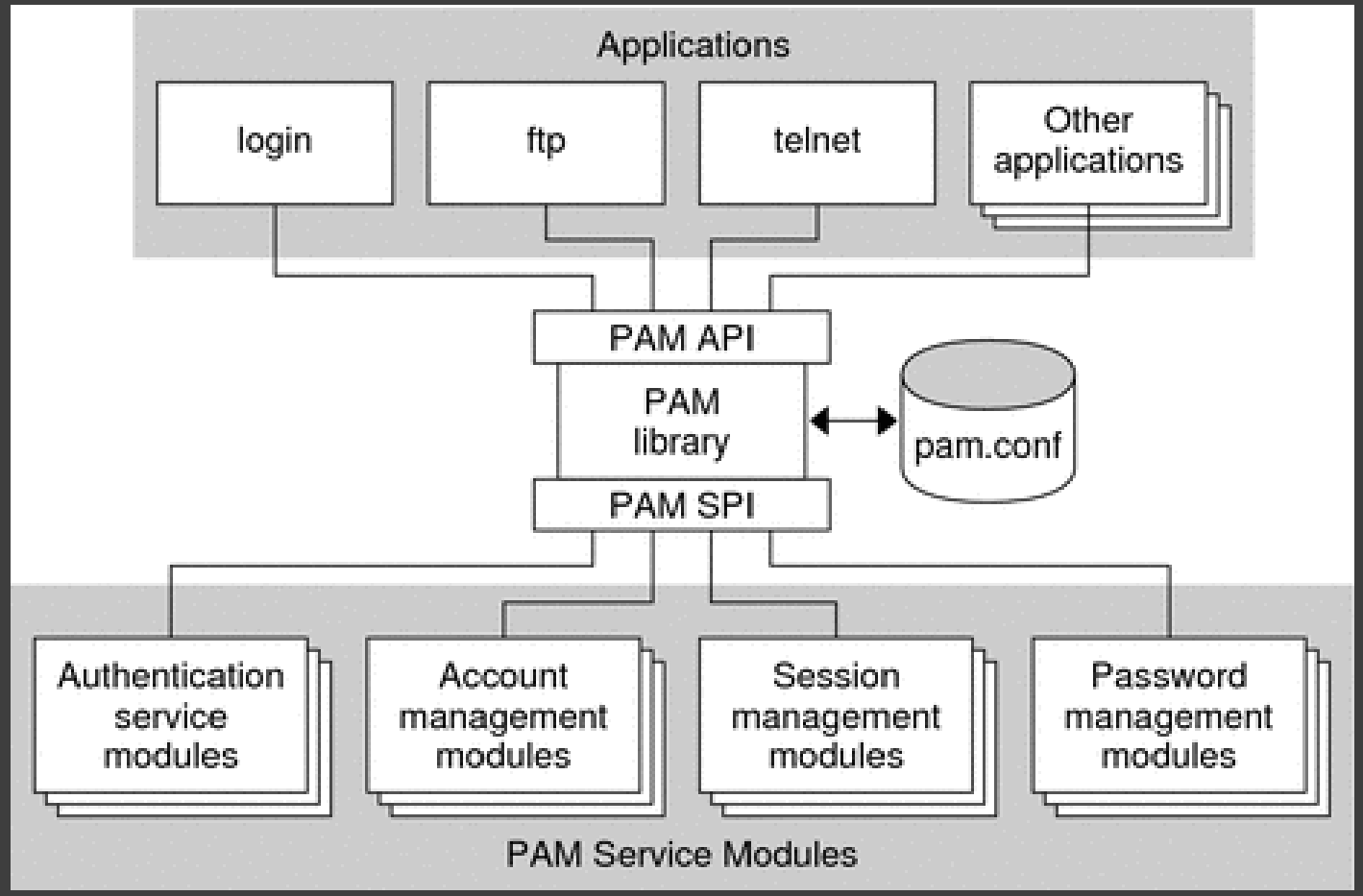
인증 방법에 대한 함수를 포함한 라이브러리 제공

서비스 인증 설정 파일: /etc/pam.d/*
PAM 인증 모듈: /lib/security/*
PAM 인증 모듈의 설정파일: /etc/security/*

PAM 의 원리

1. 사용자가 특정 서비스에 접근할 때 그 서비스는 PAM에게 인증을 요청
2. PAM은 요청한 서비스의 설정 파일(/etc/pam.d/서비스)를 확인
3. 설정에 맞게 인증을 수행
4. 결과를 서비스에 반항
5. 서비스는 인증 결과 (True/False)를 바탕으로 서비스를 제공/거절

PAM Architecture



PAM Authentication

1. libpam-ldap 패키지를 이용해 pam_ldap 모듈을 사용
   - user가 저장된 directory에 따라 로그인이 제한됨
   - LDAP directory로의 access right이 덜 필요함
   - doesn’t expose password hashes
2. LDAP 서버에서 NSS를 사용해 client로 보내진 password hashes를 사용
   - getent shadow 를 사용해 password hashes를 return 할 수 있음 (root권한으로 접근했을 때만)

PAM Installation Using libpam-ldapd

NSS처럼 libpam-ldap 와 libpam-ldapd 두 가지가 있다

libpam-ldapd 와 libnss-ldapd 로 업데이트 되면서
따로 돌아가던 NSS와 PAM이
같은 backend (nslcd) 와 configuration file (/etc/nslcd.conf) 를 공유

더 간편한 libpam-ldapd 를 쓰자
$ sudo apt-get install libpam-ldapd

libpam-ldap 또는 pam_unix 로 설정하는 법은 여기 → https://wiki.debian.org/LDAP/PAM

Testing

$ sudo getent passwd 로 LDAP server와 client가 잘 연결 되었는지 확인해보자

LDAP server에서 DB에 추가했던 아이디로 client 서버에 로그인이 되는지 확인

References

http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol - LDAP

http://en.wikipedia.org/wiki/OpenLDAP - OpenLDAP

http://en.wikipedia.org/wiki/Pluggable_authentication_module - PAM

https://wiki.debian.org/LDAP - LDAP 설치/설정

https://help.ubuntu.com/14.04/serverguide/openldap-server.html - LDAP 설치/설정

2009-2012 LDAP 휠 세미나 (casper, harry, logue, chaos)

끝