LDAP
pGina

victory
alogon

LDAP

LDAP: Lightweight Directory Access Protocol
네트워크상의 다른 호스트의 **디렉토리 서비스에 접근 하기 위한 프로토콜**

TCP/IP 상에서 작동 *https://brunch.co.kr/@wangho/6

LDAP

LDAP: Lightweight Directory Access Protocol
네트워크상의 다른 호스트의 **디렉토리 서비스에 접근 하기 위한 프로토콜**

TCP/IP 상에서 작동 *https://brunch.co.kr/@wangho/6

Q. 디렉토리 서비스란?
- 관리자가 여러 사용자들이 공유 자원에 접근할 수 있도록 도와줌
- DBMS에 비해 복잡한 갱신은 어렵지만, '읽기'에 최적화 되어 있음
- X.500(디렉토리 관련 표준)에 정의

Q. 프로토콜이란?
- 표준!
- HTTP가 HTML 문서를 주고 받는 표준인 것처럼, LDAP이 디렉토리 서비스를 위한 표준

LDAP

요약:
네트워크에서 '디렉토리'란 어떤 자원이 네트워크 상의 어디에 있는지 알려주는 것!

- DNS (Domain Name System)도 네트워크 주소 ⇔ 도메인 이름의 디렉토리 시스템

LDAP

요약:
네트워크에서 '디렉토리'란 어떤 자원이 네트워크 상의 어디에 있는지 알려주는 것!

- DNS (Domain Name System)도 네트워크 주소 ⇔ 도메인 이름의 디렉토리 시스템

- 그러니까 보통 LDAP을 유저권한 관리에 많이 쓰긴하지만, 유저관리에만 쓰는게 아니라
  디렉토리 안에 연락처, 유저, 파일, code 뭐든지간에 일단 넣을 수는 있고
  insert나 update보다는 빠른 검색에 특화되어 있는것!

LDAP

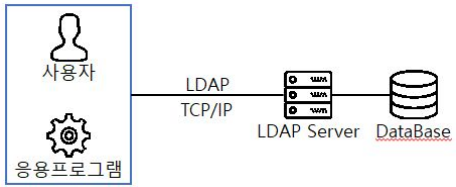
요약:
네트워크에서 '디렉토리'란 어떤 자원이 네트워크 상의 어디에 있는지 알려주는 것!

- DNS (Domain Name System)도 네트워크 주소 ⇔ 도메인 이름의 디렉토리 시스템

- 그러니까 보통 LDAP을 유저권한 관리에 많이 쓰긴하지만, 유저관리에만 쓰는게 아니라
  디렉토리 안에 연락처, 유저, 파일, code 뭐든지간에 일단 넣을 수는 있고
  insert나 update보다는 빠른 검색에 특화되어 있는것!

LDAP 디렉토리는 많은 서버 사이에 분포될 수 있고 주기적으로 동

LDAP 디렉토리는 추상적 계층의 **단순한 트리 구조** (DIT)



Directory Information Tree

DIT는 LDAP 디렉토리를 구성하는 트리 구조

각 노드를 'entry'라고 함

- DBMS에서 하나의 tuple이랑 대응됨 (하나의 row)
- 각 entry는 그 위치를 나타내는 DN (Distinguished Name)으로 구분

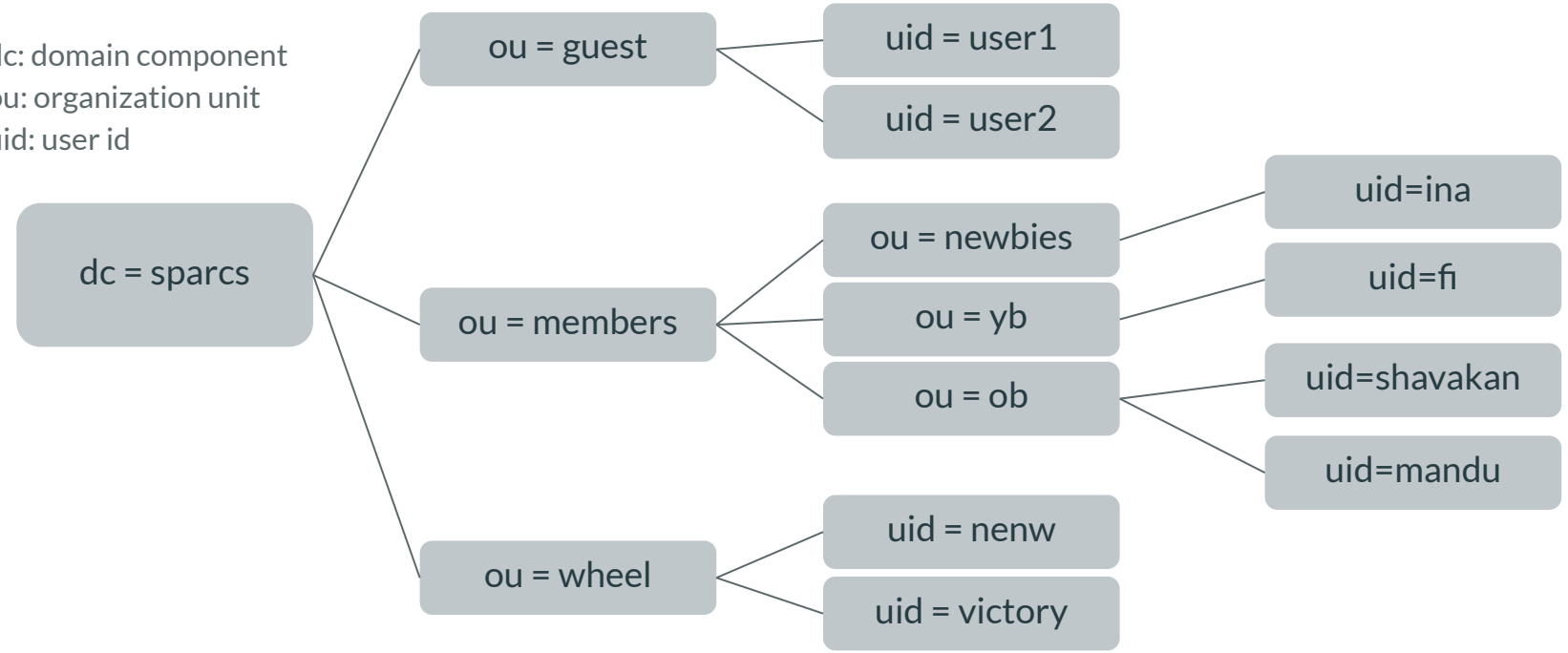
DN은 속성, 속성값의 나열로 이루어져 있음

- 속성의 종류: c = country, cn=common name, ou=organization unit, dc=domain component ...

DIT example

victory's DN(절대경로): uid=victory, ou=wheel, dc=sparcs, dc=org
RDN(상대경로)

dc: domain component
ou: organization unit
uid: user id



Attribute, ObjectClass, Schema

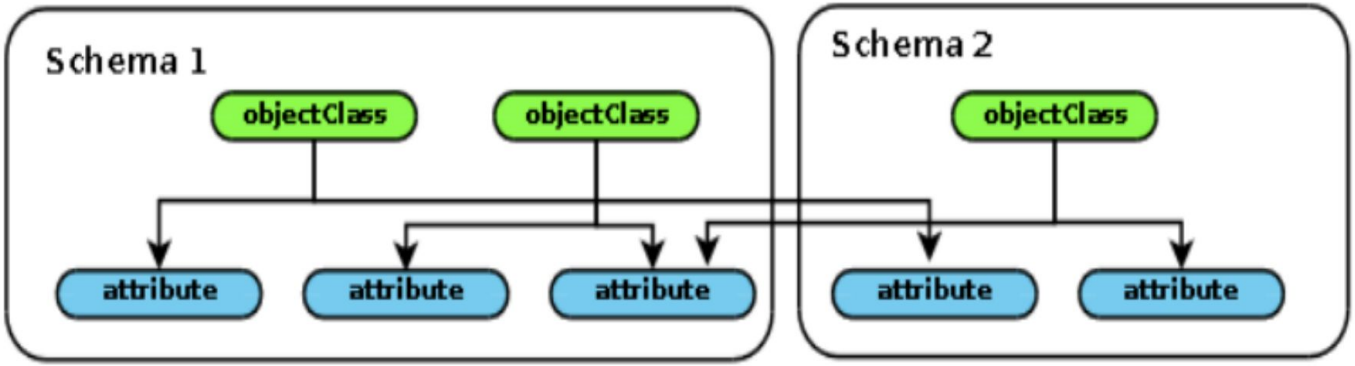
Attribute: 각 객체가 가지는 속성들

ObjectClass: (=entry) Schema에서 정의되는 attribute의 collection

Schema: 어떤 objectClass(entry)가 어떤 attribute을 가질지 정해줌!

- /etc/ldap/schema 에 정의되어 있으며, 사용자가 변경 가능

* ldapexplorer.com/en/manual/107060000-ldap-object-classes.htm



LDAP 실습 - 설치

1. AWS EC2 인스턴스 준비 (보안 그룹에서 389번 포트 오픈)
2. sudo apt update
3. sudo apt -y install slapd ldap-utils

잘 설치되었는지 확인 방법

1. sudo service slapd status로 동작 확인
2. sudo slapcat

LDAP 실습 - 환경설정

실행명령: sudo dpkg-reconfigure slapd

1. No
2. 기본값 유지 (default: ap-northeast-2.compute.internal)
3. 기본값 유지 (default: ap-northeast-2.compute.internal)
4. 비밀번호 설정
5. HDB
6. No
7. Yes
8. No

LDAP 실습 - 순서

오늘 실습

1. sparcs 라는 organization 추가
2. sparcs 안에 유저 생성
3. 생성된 유저로 LDAP Authentication 확인
4. phpldapadmin으로 생성한 것들 GUI로 확인

LDAP 실습 - organization 생성

1. mkdir ldap (오늘 실습을 진행할 폴더)
2. Entry 추가를 위해서는 .ldif 파일이 필요
   a. LDAP Data Interchange Format
   b. LDAP에서 관리하는 정보를 plain text로 변환해서 보여주는 형식이다.

```
dn: ou=sparcs, dc=ap-northeast-2, dc=compute, dc=internal
ou: sparcs
objectclass: organizationalUnit
```

LDAP 실습 - organization 생성

1. Entry 추가
   - ldapadd -x -D cn=admin,dc=ap-northeast-2,dc=compute,dc=internal -W -f organization.ldif
2. Entry 검색
   - ldapsearch -x -b 'dc=ap-northeast-2,dc=compute,dc=internal'

- ldap 명령어 옵션
  - -x 인증 방식을 간단히 함
  - -W prompt로 비밀번호를 물어봄
  - -f 새로 입력할 ldif 파일
  - -D 수정,추가하는 사용자의 dn(아이디)
  - -c 오류가 나도 멈추지 않음

LDAP 실습 - 유저 생성

1. 마찬가지로 .ldif 파일로 유저 추가

```
dn: uid=alogon,ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal
cn: alogon
objectclass: account
objectclass: posixAccount
uid: alogon
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home
userPassword: alogon
```

2. 유저 생성: ldapadd -x -D cn=admin,dc=ap-northeast-2,dc=compute,dc=internal -W -f user.ldif
3. 유저 확인: ldapsearch -x -b 'dc=ap-northeast-2,dc=compute,dc=internal'

LDAP 실습 - Authentication 확인

1. ldapwhoami -x -w (설정한 비밀번호) -D uid=alogon,ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal
2. ldapwhoami -x -w (설정한 비밀번호) -D uid=alogon,ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal -H ldap://(탄력적 IP 주소):389
3. Authentication 성공

```
dn:uid=alogon,ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal
```

4. Authentication 실패

```
ldap_bind: Invalid credentials (49)
```

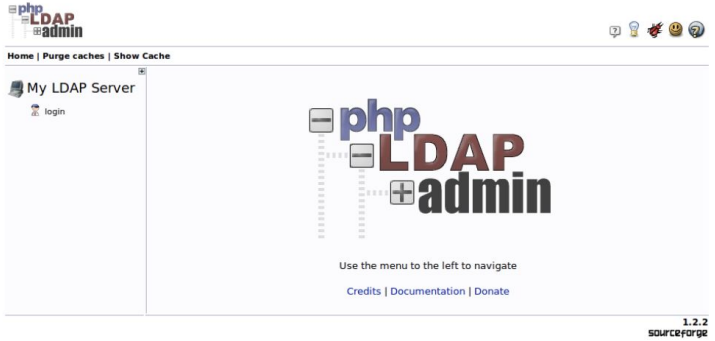
LDAP 실습 - phpldapadmin

1. php를 기반으로 해 LDAP을 GUI환경에서 관리할 수 있게 해 준다.
2. 2002년에 Brignham Young University의 Dave Smith라는 학생이 시작했다.

http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page

LDAP 실습 - phpldapadmin

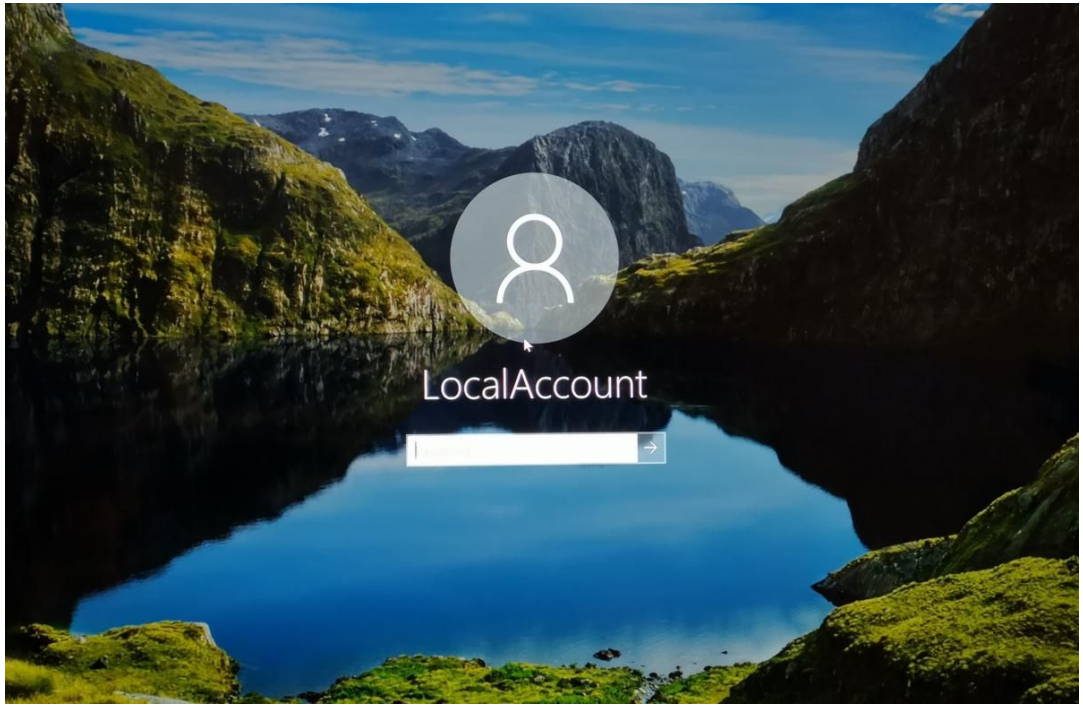
1. sudo apt update
2. sudo apt install phpldapadmin
3. sudo vim /etc/phpldapadmin/config.php
   a. $servers->setValue('server','host','127.0.0.1');
   b. $servers->Value('server','base',array('dc=ap-northeast-2,dc=compute,dc=internal'));
   c. $servers->setValue('login','bind_id','cn=admin,dc=ap-northeast-2,dc=compute,dc=internal');
   d. $config->custom->appearance['hide_template_warning'] = true;
4. EC2-탄력적 IP/phpldapadmin 확인
5. 처음에 설정한 admin 비밀번호로 접근



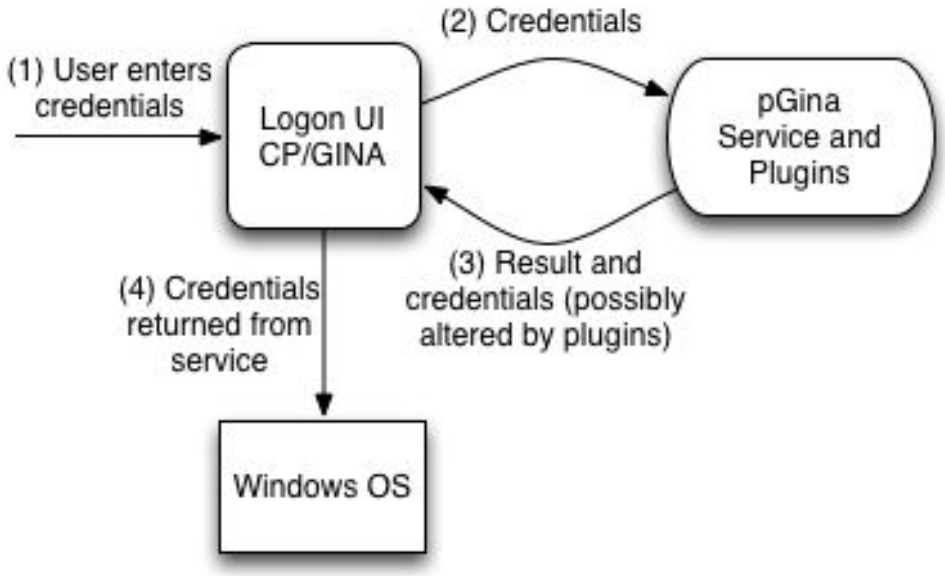
Pgina

- 윈도우 운영체제를 사용하는 머신에서 interactive user authentication과 access management를 할 수 있도록 하는 프로그램 (http://pgina.org/)
- 관리자가 자유롭게 인증방식을 사용할 수 있다.
- 사실 윈도우에서 기본적으로 제공하는 credential provider가 있는데, pGina의 plugin들을 통해 다른 다양한 기능들을 사용할 수 있다

Pgina 사용



Pgina 동작 방식


(1) User enters credentials
Logon UI CP/GINA
(2) Credentials
pGina Service and Plugins
(3) Result and credentials (possibly altered by plugins)
(4) Credentials returned from service
Windows OS

Pgina 사용


Username
A
Password
Service Status: Disconnected
tester
Image
pGina
Large Text