LDAP / pGINA

By Klien (kyuho lee)

LDAP 의 정의

Lightweight

Directory

Access

Protocol

- 네트워크상의 다른 호스트 의 디렉토리 서비스에 접근하기 위한 프로토콜

프로토콜 이란?

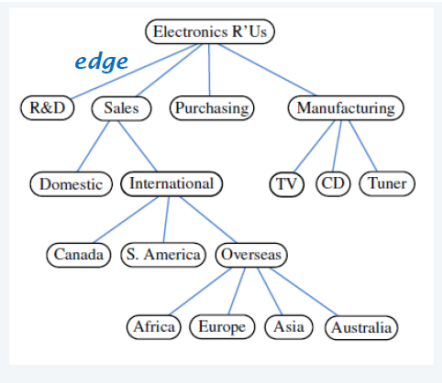
- HTTP 처럼 정보전달을 위한 표준 방식이다.
  - HTTP 는 HTML 페이지를 전달하기 위한 방식
  - LDAP 는 다른 호스트의 디렉토리 안에 있는 정보를 전달하기 위한 방식
- TCP/IP 라는 기본적인 정보교환 프로토콜을 기반으로 세워져 있다 (HTTP와 같은 기반)

디렉토리 서비스란?

- 관리자가 여러 사용자들이 공유 자원에 접근할수 있도록 도와주는 서비스
- Key-valye 패어 식으로 보통 정보를 저장한다
- 정보를 확인하는 빈도가 정보를 수정하는 빈도보다 높다
- ex) 전화번호부, 주소, 유저와 패스워드, DNS!!
  - DNS는 도메인 네임의 디렉토리 시스템이다....
- 그래서 DB보다는 갱신 방법이 어렵다
- X.500 이라는 디렉토리 표준에 정의 됌.

DIT - LDAP 의 기본 디렉토리 트리구조

- 트리: Set of nodes storing elements heierachically



DIT - LDAP 의 기본 디렉토리 트리구조

- DIT 에서의 node: entry 라고 불림
  - DB에서의 튜플과 같다
  - 각 entry는 몇가지의 attribute 들로 이루어져 있다
    - Key - value 페어 형식
    - ex) cn=kyuho (cn 이 key)
  - 하지만 entry 에 임의의 attribute를 집어넣을순 없다
  - 각 entry는 DB처럼 schema를 설정해줄수 있다 → objectClass라고 한다
    - 즉 objectClass 는 attribute의 집합이다

DIT - LDAP 의 기본 디렉토리 트리구조

RDN: entry의 이름! 유일하다 (여기서는
uid=klien
)

DN: DIT entry의 부모 의 RDN들을 나열한 체인 → entry 의 위치를 특정 가능

objectClass: 어떤 schema?

그 밑의 attribute들은 objectClass 에 의해서 정의된다.

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

cn: kyuho

objectclass: account

objectclass: posixAccount

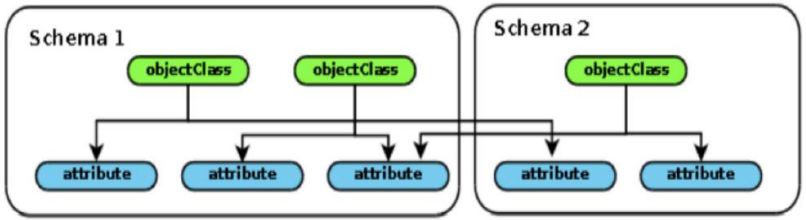
uid: klien

uidNumber: 2000

gidNumber: 2000

homeDirectory: /home

userPassword: kyuholee2



DIT - LDAP 의 기본 디렉토리 트리구조

- 각 entry는 순수하게 organizational한 목적으로도 사용 가능
  - 우리가 아는 파일 시스템의 dir 역할
  - 그런 이유로 organizational unit이라는 object class도 존제
- 복잡한 트리구조는 지원하지 않음으로 최대한 간결한 형식으로 구성
- Attribute들도 따로 schema가 존재 / attribute의 형식 만들기
- Objectclass에서 꼭 필요한 attribute랑 있으면 좋은 attribute로 구별 가능 (MUST 옵션 , MAY 옵션)

LDAP 실습

LDAP 설치

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

설치 확인

1. Sudo service slapd status
2. Sudo slapcat

LDAP 실습

환경설정

sudo dpkg-reconfigure slapd

1. No
2. Ap-northeast-2.compute.internal (default)
3. Ap-northeast-2.compute.internal (default)
4. Password / confirm
5. No
6. Yes
7. No

LDAP 실습

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

1. Sparcs organization생성

1. 실습용 dir 생성
2. Entry 추가를 위해 .ldif 파일 생성
    a. LDAP Data Interchange Format
    b. LDAP entry를 text로 표현

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

1. Sparcs organization생성

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

- 명령어 옵션
    - -x 인증 방식 간편화
    - -W prompt로 비번 물어보기
    - -f 입력 파일명
    - -D 파일 수정/추가자 이름 (creator name)
    - -c 오류가 나도 안멈춤

2. Organization 유저 생성

1. Ldif 파일 추가
2. 유저생성 (entry 추가): ldapadd -x -D cn=admin,dc=ap-northeast-2,dc=compute,dc=internal -W -f user.ldif
3. 유저검색: ldapsearch -x -b 'ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal'

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

cn: kyuho (이름)

objectclass: account

objectclass: posixAccount

uid: klien(아이디)

uidNumber: 2000

gidNumber: 2000

homeDirectory: /home

userPassword: kyuholee2(비번)

3. Authentication 확인

1. ldapwhoami -x -w (설정한 비밀번호) -D uid=(아이디),ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal
2. ldapwhoami -x -w (설정한 비밀번호) -D uid=(아이디),ou=sparcs,dc=ap-northeast-2,dc=compute,dc=internal -H ldap://(탄력적 IP 주소):389
3. 성공시 dn 체인이 표시된다!

4. Phpldapadmin 사용

1. LDAP용 GUI!
2. 2002년에 Brignham Young University의 Dave Smith라는 학생이 시작했고 한다…
3. 소스: http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page

4. Phpldapadmin 사용

1. Sudo apt update
2. Sudo apt install phpldapadmin
    a. 실행전에 꼭 80번포트에서 돌아가는 어플이 없도록 확인
    b. 아파치 서버가 안켜진다...
3. sudo vim /etc/phpldapadmin/config.php
    a. $servers->setValue('server','host','127.0.0.1');
    b. $servers->setValue('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;(위쪽에 있다)
4. (EC2 ip)/phpldapadmin으로 접속
5. 비번은 설정한대로!