LDAP, pGina

leesia

What is LDAP?

- Lightweight Directory Access Protocol
- 말 그대로, 디렉토리 서비스 접근을 위한 프로토콜
- 디렉토리는 무엇인지 대충 안다
- 그렇다면 디렉토리 서비스란 무엇일까, 디렉토리와 어떻게 다른가?

What is directory service?

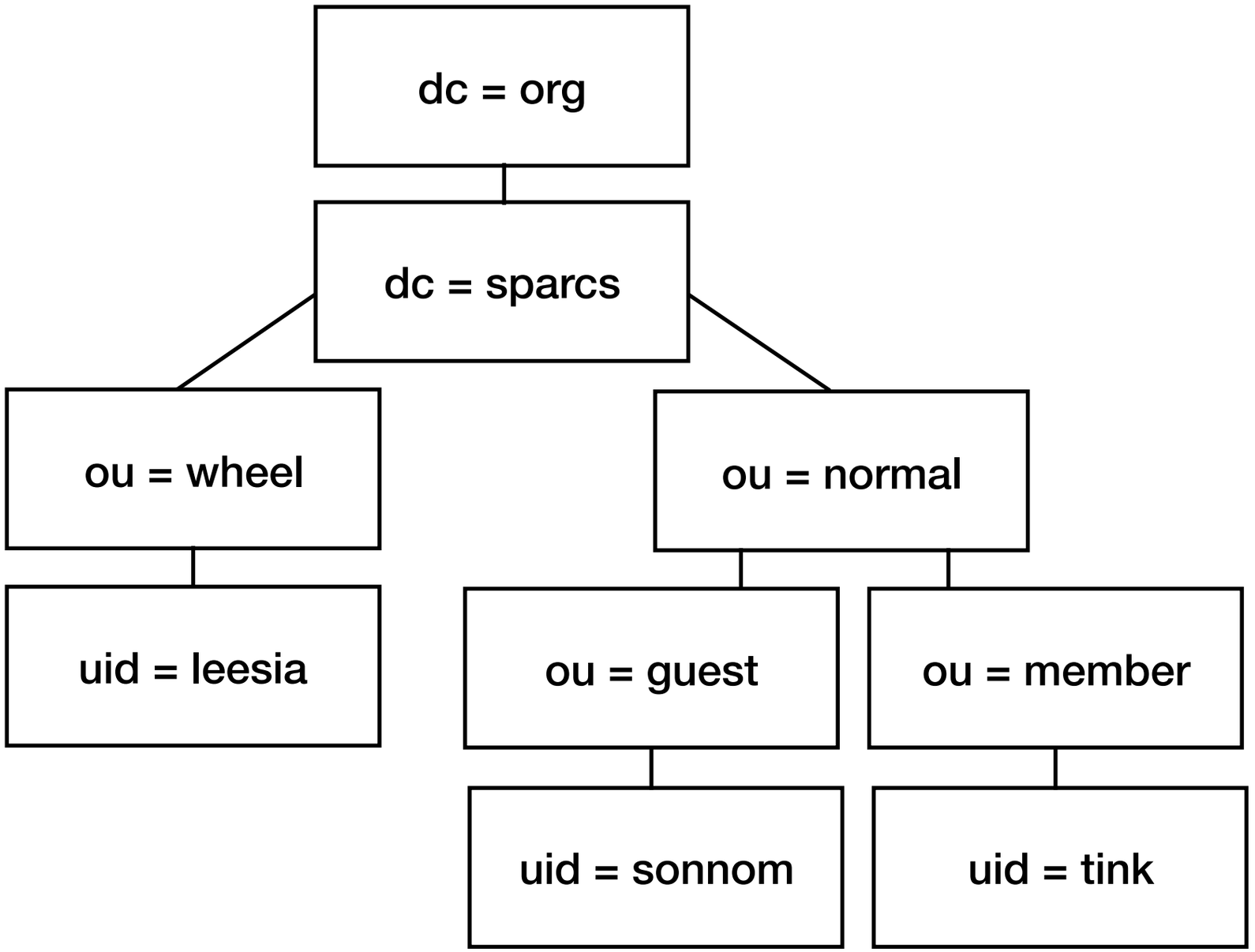
- 디렉토리 서비스는 컴퓨터 네트워크의 사용자와 네트워크 자원에 대한 정보를 저장하고 조직하는 프로그램이다.

- ex) aria의 ssh 서비스를 스팍스 사람들에게 제공하고 싶다.
  - 다양한 사용자가 존재 : leesia, nenw, tink, …
  - aria에는 다양한 자원이 존재 : cpu, 메모리, gpu, ….
  - 이러한 사용자들의 정보와 자원에 대한 정보를 저장해서, 사용자들이 자원에 접근할 수 있도록 해준다!

What is directory service?

- 따라서 디렉토리 서비스는 그 특성상 쓰기 작업보다 읽기 작업에 더 특화되어 있다.
  ex) 유저 추가는 매 학기 신입분들이 뽑힐 때만 쓰기 작업이 일어날 테지만, 읽기 작업은 유저가 매번 aria에 접속할 때마다 일어난다.

Directory service structure : Directory Information Tree



박스 하나하나를 엔트리라 한다

Directory service structure

- 모든 엔트리들은 각각의 Objectclass를 갖는다. 이는 객체 지향 언어에서의 class의 개념과 완전히 동일하다.

- 각각의 Objectclass는 여러 개의 attribute를 가진다.

Directory service structure

- DNS hierarchy와 거의 비슷하다
  1. cn (common name) : leaf entries (end objects)
     ex) users, groups
  2. dc (domain component) : LDAP hierarchy 상의 container entries

Practice: Install slapd

- Let’s make an EC2 instance
- $ sudo apt update
- $ sudo apt -y install slapd ldap-utils

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Install slapd

- $ sudo slapcat

```
ubuntu@ip-172-31-37-140:~$ sudo slapcat
dn: dc=ap-northeast-2,dc=compute,dc=internal
objectClass: top
objectClass: dcObject
objectClass: organization
o: ap-northeast-2.compute.internal
dc: ap-northeast-2
structuralObjectClass: organization
entryUUID: 9af32996-bbc6-1039-95b3-67314b7d5f2d
creatorsName: cn=admin,dc=ap-northeast-2,dc=compute,dc=internal
createTimestamp: 201912260058427
entryCSN: 20191226005842.505287Z#000000#000#000000
modifiersName: cn=admin,dc=ap-northeast-2,dc=compute,dc=internal
modifyTimestamp: 201912260058427

dn: cn=admin,dc=ap-northeast-2,dc=compute,dc=internal
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9OGQxV3RCMld4NURTL1FzL3oyd05CcTRDU2hXR0FTaVM=
structuralObjectClass: organizationalRole
entryUUID: 9af4cd6e-bbc6-1039-95b4-67314b7d5f2d
creatorsName: cn=admin,dc=ap-northeast-2,dc=compute,dc=internal
createTimestamp: 201912260058427
entryCSN: 20191226005842.516069Z#000000#000#000000
modifiersName: cn=admin,dc=ap-northeast-2,dc=compute,dc=internal
modifyTimestamp: 201912260058427
```

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Add population

- 다음을 추가해보자
  1. A node called People (store users)
  2. A user called ‘ldaptest’

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Add population

- $ sudo vim top.ldif

```
dn: ou=people,  dc=ap-northeast-2,dc=compute,dc=internal
ou: people
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: ap-northeast-2.compute.internal

dn: ou=contacts,ou=people,  dc=ap-northeast-2,dc=compute,dc=internal
ou: contacts
ou: people
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: ap-northeast-2.compute.internal

dn: ou=group,  dc=ap-northeast-2,dc=compute,dc=internal
ou: group
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: ap-northeast-2.compute.internal
```

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Add population

```
ldapadd -x -D 'cn=admin,dc=ap-northeast-2,dc=compute,dc=internal' -W -f top.ldif
```

```
Enter LDAP Password:
adding new entry "ou=people,  dc=ap-northeast-2,dc=compute,dc=internal"
adding new entry "ou=contacts,ou=people,  dc=ap-northeast-2,dc=compute,dc=internal"
adding new entry "ou=group,  dc=ap-northeast-2,dc=compute,dc=internal"
```

```
ldapsearch -x -b 'dc=ap-northeast-2,dc=compute,dc=internal'
```

-x: simple authentication
-b: base dn for search

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Add population

- $ sudo vim people.ldif

```
dn: uid=ldaptest,ou=people,dc=ap-northeast-2,dc=compute,dc=internal
cn: ldaptest
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home
loginShell: /bin/bash
shadowLastChange: 11192
shadowMin: -1
shadowMax: 99999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 134538308
uid: ldaptest
userPassword: haha
```

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Add population

```
ldapadd -x -D 'cn=admin,dc=ap-northeast-2,dc=compute,dc=internal' -W -f people.ldif
```

```
Enter LDAP Password:
adding new entry "uid=ldaptest,ou=people,dc=ap-northeast-2,dc=compute,dc=internal"
```

```
ldapsearch -x -b "dc=ap-northeast-2,dc=compute,dc=internal" "(objectclass=*)"
```

https://help.ubuntu.com/lts/serverguide/openldap-server.html

Practice: Authentication

When we enter the right password in “@secret”

```
ldapwhoami -x -w  “@secret" -D uid=ldaptest,ou=people,dc=ap-northeast-2,dc=compute,dc=internal

dn:uid=ldaptest1,ou=people,dc=ap-northeast-2,dc=compute,dc=internal
```

When we enter the invalid password

```
ldapwhoami -x -w  “@secret" -D uid=ldaptest,ou=people,dc=ap-northeast-2,dc=compute,dc=internal

ldap_bind: Invalid credentials (49)
```

Authentication in client

```
ldapwhoami -x -w haha -D uid=ldaptest1,ou=people,dc=ap-northeast-2,dc=compute,dc=internal -H ldap://13.125.206.157:389
```

Practice: Authentication in client

```
ldapwhoami -x -w haha -D uid=ldaptest1,ou=people,dc=ap-northeast-2,dc=compute,dc=internal -H ldap://13.125.206.157:389
```

```
dn:uid=ldaptest1,ou=people,dc=ap-northeast-2,dc=compute,dc=internal
```

What is pGina?

What is pGina?

What is pGina?

- 윈도우 운영체제를 사용하는 머신에서 interactive user authentication과 access management를 할 수 있도록 하는 프로그램 (http://pgina.org/)

- 사실 윈도우에서 기본적으로 제공하는 credential provider가 있는데, pGina의 plugin들을 통해 다른 다양한 기능들을 사용할 수 있다

How pGina works?

- pGina는 두 가지 component를 가진다
  - the Credential Provider (or GINA)
  - the pGina service

- pGina CP는 단순히 유저 정보를 받아서 이를 pGina service로 넘겨주기만 한다

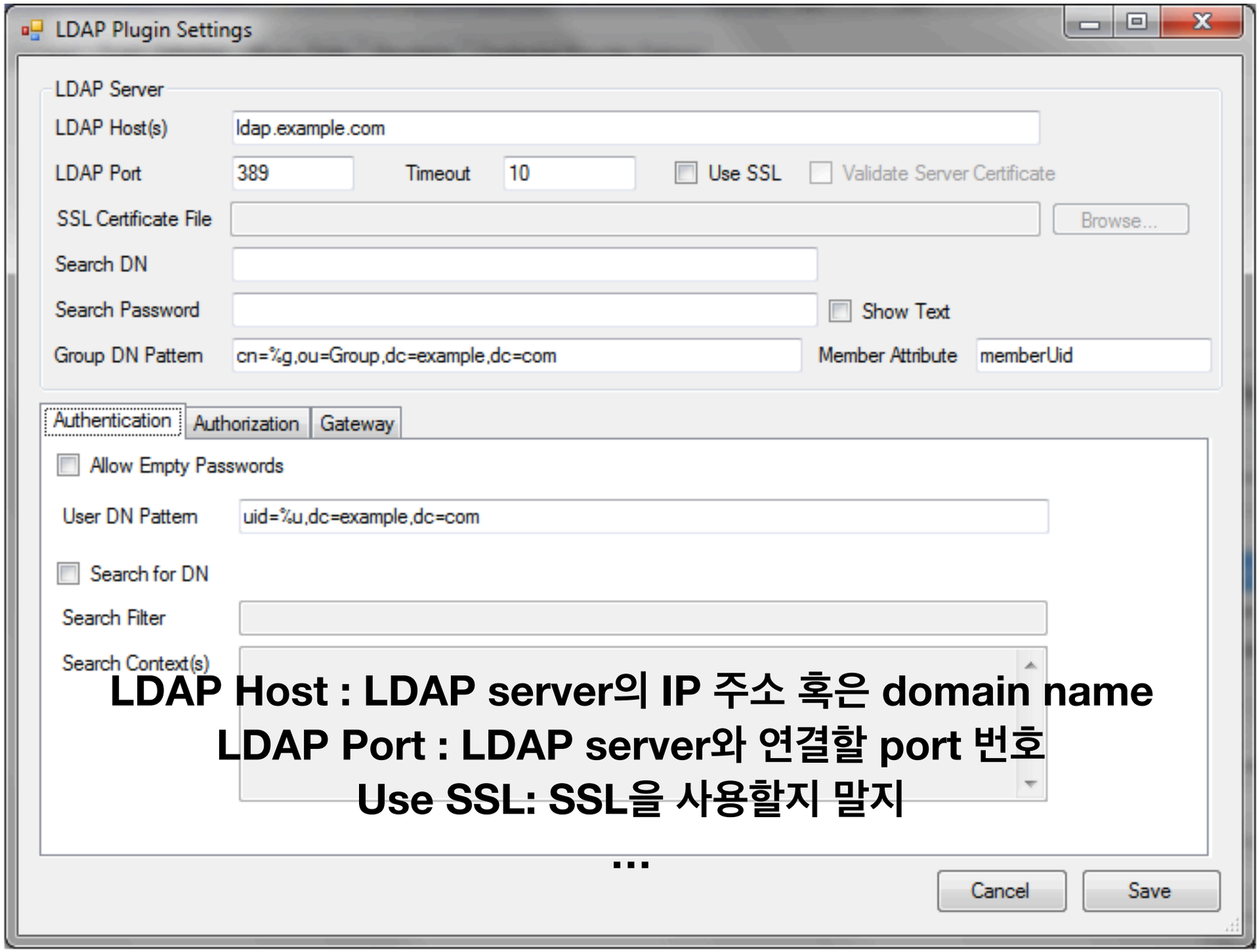
- pGina service 상의 plugin들이 authentication과 authorization을 진행한다

How we can use pGina?

- Connect pGina with LDAP server!!

- LDAP plugin이 존재한다. (http://pgina.org/docs/v3.1/ldap.html)

How we can use pGina?



LDAP Host : LDAP server의 IP 주소 혹은 domain name

LDAP Port : LDAP server와 연결할 port 번호

Use SSL: SSL을 사용할지 말지

...