

ZEPPELIN w/ LDAP

우아한형제들
데이터서비스팀

한동훈



왜 LDAP 인가?

- 사내 AD 계정과 연동 가능.
- Shiro.ini 고치기 귀찮아...
- Google business 계정과 연동하여 LDAP 구성 가능
 - <https://support.google.com/a/answer/106368?hl=en>
- 그룹 관리의 용이성.
- Kerberos 와 LDAP 은 찰떡 공합
 - HDFS / HIVE 등의 Kerberos 인증에 LDAP 을 연동시킬 수 있다.



Ubuntu + OpenLDAP + phpLdapAdmin

- OpenLDAP

- <https://help.ubuntu.com/lts/serverguide/openldap-server.html>
- `sudo apt-get install slapd ldap-utils`
- `sudo dpkg-reconfigure -plow slapd`
 - Reconfigures Domain name, Organization Name, admin passwords.
 - example.com for this example.

- phpLdapAdmin

- `sudo apt-get install phpldapadmin`
- Edit `/etc/apache2/conf-available/phpldapadmin.conf` for domain name other than example.com

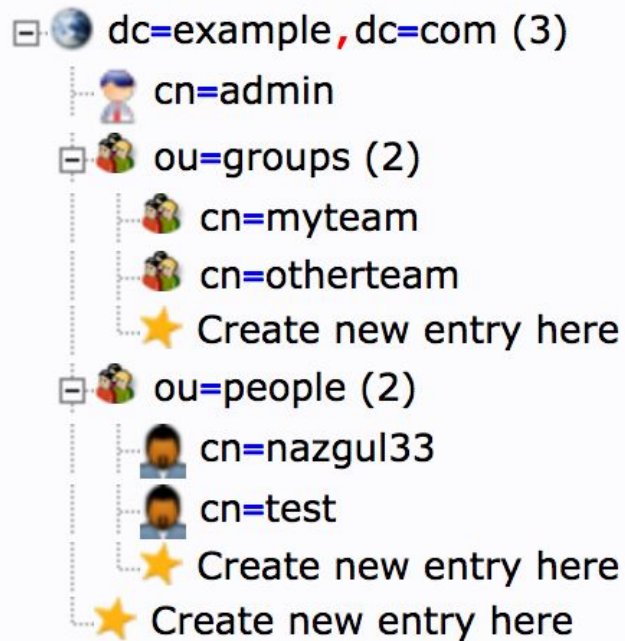




phpldapadmin 으로 그룹 및 계정 추가

- Add Organization Units
 - people
 - groups
 - system
- Add groups to ou=groups,dc=example,dc=com
 - Create a child entry (myteam, otherteam)
 - Generic: Posix Group
- Add people to ou=people,dc=example,dc=com
 - Create a child entry (nazgul33, mytest1, test)
 - Generic : User Account
- Add system account for zeppelin in ou=system,dc=example,dc.com
 - Create a child entry (zeppelin)
 - Generic : User Account

phpldapadmin 으로 그룹 및 계정 추가



phpLdapAdmin : 그룹에 유저 추가

- click group name in left pane.
- click “Add new attribute” in right pane
- choose “memberUid”
- add a uid
- click “Update Object”

cn=myteam

Server: My LDAP Server Distinguished Name: cn=myteam,ou=groups,dc=example,dc=com
Template: Default

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Add Attribute

memberUid

nazgul33

cn

required, rdn

myteam

*

(add value)

(rename)

gidNumber

required

500

objectClass

required

posixGroup

(structural)

top

(add value)

Update Object



phpLdapAdmin : 그룹에 유저 추가

cn=myteam

Server: **My LDAP Server** Distinguished Name: **cn=myteam,ou=groups,dc=example,dc=com**
Template: **Default**

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

An attribute (memberUid) was modified and is highlighted below.

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

cn required, rdn

myteam *

(add value)

(rename)

gidNumber required

500

memberUid

nazgul33

(add value)

(modify group members)

objectClass required

posixGroup (structural)

top

(add value)

Update Object

- next addition is easier.
- try “modify group members”

Modify group cn=myteam

Server: **My LDAP Server** Distinguished Name: **cn=myteam,ou=groups,dc=example,dc=com**
Template: **Default**

There are **1** members in group **cn=myteam**:

Available members

Group members

mytest1
test

nazgul33

Add selected >>

Add all >>

<< Remove selected

<< Remove all

Save changes



ZEPPELIN 설정 0.6.1 : zeppelin/conf/shiro.ini

[main]

ldapRealm = org.apache.zeppelin.server.LdapGroupRealm

ldapRealm.contextFactory.environment[ldap.searchBase] = ou=people,dc=example,dc=com

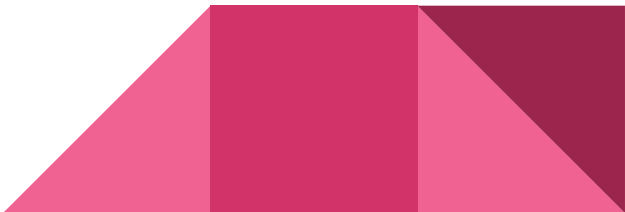
ldapRealm.contextFactory.url = ldap://localhost:389

ldapRealm.userDnTemplate = cn={0},ou=people,dc=example,dc=com

ldapRealm.contextFactory.authenticationMechanism = SIMPLE

securityManager.realms = \$ldapRealm

No support for LDAP groups





ZEPPELIN 설정 : 0.7.0 :

zeppelin/conf/shiro.ini

[main]

ldapADGCRealm = org.apache.zeppelin.realm.LdapRealm

ldapADGCRealm.contextFactory.systemUsername = cn=zeppelin,ou=system,dc=example,DC=com

ldapADGCRealm.contextFactory.systemPassword = XXXXXXXX

ldapADGCRealm.userDnTemplate=cn={0},ou=people,dc=example,dc=com

ldapADGCRealm.searchBase = dc=example,dc=com

ldapADGCRealm.userSearchBase = ou=people,dc=example,dc=com

ldapADGCRealm.groupSearchBase = ou=groups,dc=example,dc=com

ldapADGCRealm.contextFactory.url = ldap://localhost:389

ldapADGCRealm.contextFactory.authenticationMechanism = simple

ldapADGCRealm.userObjectClass = posixAccount

ldapADGCRealm.groupObjectClass = posixGroup

ldapADGCRealm.authorizationEnabled = true

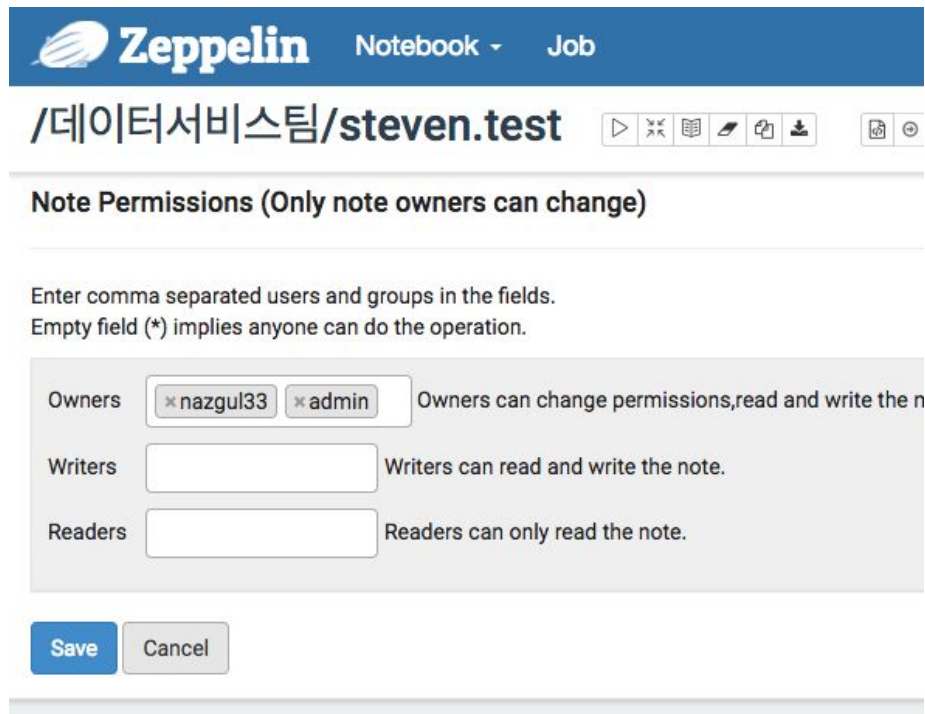
ldapADGCRealm.memberAttribute = memberUid

ldapADGCRealm.memberAttributeValueTemplate=cn={0},ou=people,dc=example,dc=com

ldapADGCRealm.rolesByGroup = myteam:admin,otherteam:user <- mapping between LDAP GROUP / SHIRO ROLE

securityManager.realms = \$ldapADGCRealm

ZEPPELIN notebook permission



The screenshot shows the Zeppelin Notebook interface. At the top, there's a blue header with the Zeppelin logo, 'Notebook', and 'Job'. Below the header, the path '/데이터서비스팀/steven.test' is displayed. A toolbar with various icons is visible. The main section is titled 'Note Permissions (Only note owners can change)'. It includes instructions: 'Enter comma separated users and groups in the fields. Empty field (*) implies anyone can do the operation.' There are three input fields: 'Owners' (containing 'nazgul33' and 'admin'), 'Writers' (empty), and 'Readers' (empty). Each field has a description of its permissions. At the bottom, there are 'Save' and 'Cancel' buttons.

Zeppelin Notebook Job

/데이터서비스팀/steven.test

Note Permissions (Only note owners can change)

Enter comma separated users and groups in the fields.
Empty field (*) implies anyone can do the operation.

Owners: nazgul33, admin Owners can change permissions, read and write the note.

Writers: Writers can read and write the note.

Readers: Readers can only read the note.

Save Cancel

- admin is the shido role mapped to LDAP group.
- type 3 letters to let Zeppelin show role names starting with those.
- Add roles to Writers or Readers and see what happens.