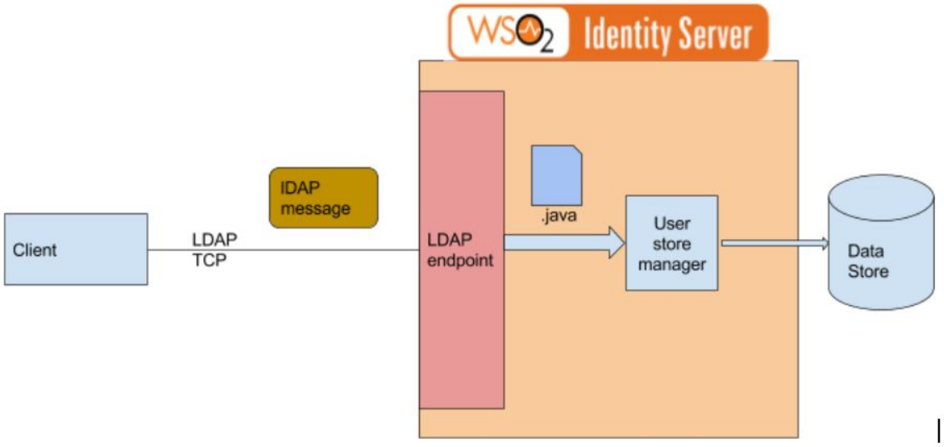
Introduction

LDAP is a core protocol that is used to store user, role, and group information.Identity server already supports connecting to LDAP supported authz systems for authentication and authorization. The idea of this project is to make IS itself act as a LDAP protocol provider.

Identity server does expose a LDAP protocol endpoint by itself such that external ldap clients can connect with IS directly. Here identity server uses userstore manager api to manage users in backend databases such as JDBC,LDAP.



Following the order to setup LDAP endpoint

- Setup Identity.xml file
- Add new claim dialect
- Add apacheds-1.5.7.wso2v5.jar to {IS-HOME}/repository/components/dropins
- Add org.wso2.carbon.identity.inbound.ldap-1.0.0-SNAPSHOT.jar to {IS-HOME}/repository/components/dropins
- Configure the primary user store
- Add user to wso2 IS userstore through ldap protocol
- Delete user from wso2 identity server userstore through ldap protocol

1. Setup Identity.xml file

enable	- If true the LDAP endpoint will start when server starts up.
instanceid	- An id given to the LDAP server instance.
connectionPassword	- The password of the admin. (uid=admin,ou=system)
workingDirectory	- Location where LDAP will store its schema files.
allowAnonymousAccess	- Should allow users to access LDAP server without credentials.Default false.
accessControlEnabled	- Should access control be enabled among partitions. Default true.
saslHostName	- Default host name to be used in SASL (Simple Authentication and Security Layer). This property comes from apacheds implementation itself.
saslPrincipalName	- Default SASL principal name. Again this property also comes from apacheds implementation itself.

```
<LDAPEndPointConfig>
        <enable>true</enable>
        <port>10390</port>
        <instanceId>default</instanceId>
        <connectionPassword>admin</connectionPassword>
        <workingDirectory>.</workingDirectory>
        <allowAnonymousAccess>false</allowAnonymousAccess>
        <accessControlEnabled>true</accessControlEnabled>
        <denormalizeOpAttrsEnabled>false</denormalizeOpAttrsEnabled>
        <maxPDUSize>2000000</maxPDUSize>
        <saslHostName>localhost</saslHostName>
        <saslPrincipalName>ldap/localhost@EXAMPLE.COM</saslPrincipalName>
 </LDAPEndPointConfig>
```

2. Adding new claim dialect

When you are going to adding claim dialect into wso2 identity server there are two ways.
1.Add claim dialect to claim-config.xml file(Using file configuration)
2.Add claim dialect using Identity server ui(Using management console)

- Add claim dialect using claim-config.xml file

Create a claim Dialect

Claim	ClaimURI	DisplayName	AttributeID	Description	MappedLocalClaim
1	http://wso2.org/ldap/claim/givenName	First Name	givenName	First Name	http://wso2.org/claims/givenname
2	http://wso2.org/ldap/claim/nickName	Nick Name	nickName	Nick Name	http://wso2.org/claims/nickname
3	http://wso2.org/ldap/claim/sn	Last Name	sn	Last Name	http://wso2.org/claims/lastname
4	http://wso2.org/ldap/claim/mail	Email	mail	Email Address	http://wso2.org/claims/emailaddress
5	http://wso2.org/ldap/claim/dateOfBirth	DOB	dateOfBirth	Date of Birth	http://wso2.org/claims/dob
6	http://wso2.org/ldap/claim/gender	Gender	gender	Gender	http://wso2.org/claims/gender
7	http://wso2.org/ldap/claim/country	Country	country	Country	http://wso2.org/claims/country
8	http://wso2.org/ldap/claim/streetAddress	Street Address	streetAddress	Street Address	http://wso2.org/claims/streetaddress
9	http://wso2.org/ldap/claim/homePhone	Home Phone	homePhone	Home Phone	http://wso2.org/claims/phoneNumbers.home
10	http://wso2.org/ldap/claim/otherPhone	Other Phone	otherPhone	Other Phone	http://wso2.org/claims/otherphone
11	http://wso2.org/ldap/claim/mobile	Mobile	mobile	Mobile	http://wso2.org/claims/mobile
12	http://wso2.org/ldap/claim/localityName	Locality	localityName	Locality	http://wso2.org/claims/locality
13	http://wso2.org/ldap/claim/stateOrProvinceName	State	stateOrProvinceName	State	http://wso2.org/claims/stateorprovince
14	http://wso2.org/ldap/claim/postalCode	Postalcode	postalCode	Postalcode	http://wso2.org/claims/postalcode
15	http://wso2.org/ldap/claim/PPID		privatePersonalIdentifier	PPID	http://wso2.org/claims/im
16	http://wso2.org/ldap/claim/cn	Full Name	cn	Full Name	http://wso2.org/claims/fullname
17	http://wso2.org/ldap/claim/organizationName	Organization	organizationName	Organization	http://wso2.org/claims/organization
18	http://wso2.org/ldap/claim/telephoneNumber	Telephone	telephoneNumber	Telephone	http://wso2.org/claims/telephone
19	http://wso2.org/ldap/claim/uid	Username	uid	User name	http://wso2.org/claims/username

20	http://wso2.org/ldap/claim/role	Role	role	Role	http://wso2.org/claims/role
21	http://wso2.org/ldap/claim/createdDate	Created Time	createdDate	Created timestamp of the user	http://wso2.org/claims/created
22	http://wso2.org/ldap/claim/im	Meta - Version	im	Meta - Version	http://wso2.org/claims/im
23	http://wso2.org/ldap/claim/lastModifiedDate	Last Modified Time	lastModifiedDate	Last Modified timestamp of the user	http://wso2.org/claims/modified
24	http://wso2.org/ldap/claim/scimId	User ID	scimId	Unique ID of the user	http://wso2.org/claims/userid
25	http://wso2.org/ldap/claim/url	URL	url	URL	http://wso2.org/claims/url
26	http://wso2.org/ldap/claim/homeEmail	Emails - Home Email	homeEmail	Home Email	http://wso2.org/claims/emails.home
27	http://wso2.org/ldap/claim/location	Location	location	Location	http://wso2.org/claims/location
28	http://wso2.org/ldap/claim/workEmail	Emails - Work Email	workEmail	Work Email	http://wso2.org/claims/emails.work

Ex-You can add above information to claim-mgt.xml file according to this way.

```
<Claim>
                  <ClaimURI>http://wso2.org/ldap/claim/givenName</ClaimURI>
                 <DisplayName>First Name</DisplayName>
                 <AttributeID>givenName</AttributeID>
                 <Description>First Name</Description>
                  <Required />
                  <SupportedByDefault />
                  <MappedLocalClaim>http://wso2.org/claims/givenname</MappedLocalClaim>
 </Claim>
```

More details -
https://docs.wso2.com/display/IS530/Adding+Claim+Dialects#AddingClaimDialects-Usingfileconfiguration

Also you can add claim dialect using identity server ui.

- Add claim dialect using identity server ui

More details -
https://docs.wso2.com/display/IS530/Adding+Claim+Dialects

3. Setup bundles

There are two bundles you should use for start ldap endpoint
1.apacheds orbit bundle
2.ldap endpoint bindle

You should copy these two bundles into *<wso2-identityserver>/repository/components/dropins*

As a back end databases you can configure any type of databases which has been supporting to wso2 identity server.
Configuring the Primary User Store
https://docs.wso2.com/display/IS530/Configuring+the+Primary+User+Store

4. Add User

First you should create Sample ldif file. Here you can define more than one users.

sample.ldif

```
dn: uid=test,ou=Users,dc=wso2,dc=org
objectClass: top
objectClass: identityPerson
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: wso2Person
objectClass: scimPerson
cn: cntest
sn: sntest
givenName: testuser
mail: test@wso2.com
mobile: 0711234567
organizationName: wso2
uid: test
userPassword:: YWJjZGU=
country: Srilanka
createdDate: 2017-12-02T17:16:04
lastModifiedDate: 2017-12-02T17:16:04
scimId: e8c029b1-e397-412e-87db-2125bb3ada56
```

Open a new terminal

```
ldapadd -h localhost -p 10390 -D "uid=admin,ou=system" -w admin -f sample.ldif
```

5. Delete User

Open a new terminal

```
ldapdelete -h localhost -p 10390 -D "uid=admin,ou=system" -w admin "uid=test,ou=Users,dc=WSO2,dc=ORG"
```