Configure Shibboleth IdP with Active Directory

1.Configure AD in the /opt/shibboleth-idp/conf/ldap.properties file.

```
idp.authn.LDAP.authenticator            = adAuthenticator

idp.authn.LDAP.ldapURL                  = ldap://ip address:389

idp.authn.LDAP.useStartTLS              = false

idp.authn.LDAP.useSSL                   = false

idp.authn.LDAP.returnAttributes         = passwordExpirationTime,loginGraceRemaining
idp.authn.LDAP.baseDN                   = ou=staff,dc=xyz,dc=org

idp.authn.LDAP.subtreeSearch            = true

idp.authn.LDAP.userFilter               = (sAMAccountName={user})

idp.authn.LDAP.bindDN                   = testuser@xyz.org

idp.authn.LDAP.bindDNCredential         = *********

idp.attribute.resolver.LDAP.searchFilter  =(samaccountname=$resolutionContext.principal)

idp.attribute.resolver.LDAP.returnAttributes   = sn,displayName,mail,samaccountname
```

2.Configure AD attributes in the /opt/shibboleth-idp/conf/attribute-resolver.xml file.

```
<resolver:AttributeDefinition id="sAMAccountName" xsi:type="ad:Simple"
sourceAttributeID="sAMAccountName">

 <resolver:Dependency ref="myLDAP" />

 <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-
def:samaccountname" encodeType="false" />

<resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:1.2.840.113556.1.4.221" encodeType="false" />

 </resolver:AttributeDefinition>



<resolver:AttributeDefinition xsi:type="ad:Script"  id="eduPersonScopedAffiliation">

 <resolver:Dependency ref="myLDAP" />

<resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-
def:eduPersonScopedAffiliation" />

<resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" friendlyName="eduPersonScopedAffiliation" />

   <ad:Script><![CDATA[
```

```
    if (typeof memberOf != "undefined" && memberOf != null ){
      for ( i = 0; memberOf != null && i < memberOf.getValues().size(); i++ ){
        value = memberOf.getValues().get(i);

        if (value.indexOf("OU=student ") > -1){
          eduPersonScopedAffiliation.getValues().add("student@%{idp.scope}");
        }
        if (value.indexOf("CN= staffs ") > -1){
          eduPersonScopedAffiliation.getValues().add("staff@%{idp.scope}");
        }
      }
    }
  ]]>
</ad:Script>
```

2.Release AD attributes in the /opt/shibboleth-idp/conf/attribute-filter.xml file.

```
<AttributeFilterPolicy id="example1">
    <PolicyRequirementRule xsi:type="ANY" />
    <AttributeRule attributeID="eduPersonScopedAffiliation">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="sAMAccountName">
      <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```