浙江大学CARSI IdP + CAS部署实践

作者：

浙江大学：单康康

感谢：

北京大学：陈萍、赖清楠、王博

华东师范大学：冯骐

时间：2020.02.05

本文总体流程基于CARSI WIKI（<https://wiki.carsi.edu.cn>），其中重点针对“安装部署CARSI IdP”--“IdP认证对接及属性定义（cas）”阶段，详细介绍浙江大学CARSI IdP + CAS认证对接过程中几个关键点，完整安装配置请参考CARSI WIKI。

浙江大学CARSI IdP + CAS部署流程（手动安装）：

1. 准备IdP安装环境（请参考CARSI WIKI）

2. 手动安装（请参考CARSI WIKI）

**3. IdP认证对接及属性定义（CAS）**

（1）环境配置（请参考CARSI WIKI）

（2）配置web.xml（请参考CARSI WIKI）

（3）配置idp.properties（请参考CARSI WIKI）

（4）配置general-authn.xml（请参考CARSI WIKI）

**（5） 配置/opt/shibboleth-idp/conf/attribute-resolver.xml（属性定义）：**

1）修改eduPersonScopedAffiliation属性映射：

将IdP的eduPersonScopedAffiliation属性映射到CAS服务器中自定义的“用户类型”属性，例如：浙大CAS服务器中“用户类型”属性为“YHLX”，则在attribute-resolver.xml文件中，将eduPersonScopedAffiliation属性定义中的principalAttributeName值改为“YHLX”（因我校急于上线，临时将eduPersonScopedAffiliation属性设为static固定值，暂不影响使用，后期再改）

2）修改eduPersonPrincipalName属性映射：

将IdP的eduPersonPrincipalName属性映射到CAS服务器中自定义的“学工号”属性，例如：浙大CAS服务器中“学工号”属性为“CODE”，则在attribute-resolver.xml文件中，将eduPersonPrincipalName属性定义中的principalAttributeName值改为“CODE”。

3）eduPersonTargetedID属性定义（请参考CARSI WIKI，本文选择相对简单的第二种方式：依据一定的算法每次计算用户的ePTID，释放给所有SP）

4）我校目前attribute-resolver.xml文件完整内容，仅供参考：

<?xml version="1.0" encoding="UTF-8"?>

<AttributeResolver

 xmlns="urn:mace:shibboleth:2.0:resolver"

 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

 xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd">

<AttributeDefinition id="eduPersonScopedAffiliation" xsi:type="Simple">

 <InputDataConnector ref="staticAttributes1" attributeNames="eduPersonScopedAffiliation" />

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

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

</AttributeDefinition>

<DataConnector id="staticAttributes1" xsi:type="Static">

 <Attribute id="eduPersonScopedAffiliation">

 <Value>faculty@zju.edu.cn</Value>

 </Attribute>

</DataConnector>

 <AttributeDefinition id="eduPersonPrincipalName" xsi:type="Scoped" scope="%{idp.scope}" sourceAttributeID="employeename">

 <Dependency ref="employeename" />

 <AttributeEncoder xsi:type="SAML1ScopedString" name="urn:mace:dir:attribute-def:eduPersonPrincipalName" encodeType="false" />

 <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" friendlyName="eduPersonPrincipalName" encodeType="false" />

 </AttributeDefinition>

 <AttributeDefinition xsi:type="SubjectDerivedAttribute" id="employeename" principalAttributeName="CODE"></AttributeDefinition>

<AttributeDefinition id="eduPersonEntitlement" xsi:type="Simple">

 <InputDataConnector ref="staticAttributes" attributeNames="eduPersonEntitlement" />

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

 <AttributeEncoder xsi:type="SAML2String" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" encodeType="false"/>

</AttributeDefinition>

<DataConnector id="staticAttributes" xsi:type="Static">

 <Attribute id="eduPersonEntitlement">

 <Value>urn:mace:dir:entitlement:common-lib-terms</Value>

 </Attribute>

</DataConnector>

<AttributeDefinition id="eduPersonTargetedID" xsi:type="SAML2NameID" nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">

 <InputDataConnector ref="ComputedIDConnector" attributeNames="computedID"/>

 <AttributeEncoder xsi:type="SAML1XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false"/>

 <AttributeEncoder xsi:type="SAML2XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="eduPersonTargetedID" encodeType="false"/>

</AttributeDefinition>

<DataConnector id="ComputedIDConnector" xsi:type="ComputedId" generatedAttributeID="computedID" salt="qmBKO63o8IlYLa/2M1EqLtUdeGAy5MyPeXYtSvAHbtA=" encoding="BASE64">

 <InputAttributeDefinition ref="eduPersonPrincipalName" />

</DataConnector>

</AttributeResolver>

**（6） 配置/opt/shibboleth-idp/conf/attribute-filter.xml（属性释放，请参考CARSI WIKI）：**

我校目前/opt/shibboleth-idp/conf/attribute-filter.xml文件完整内容如下，仅供参考：

<?xml version="1.0" encoding="UTF-8"?>

<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"

 xmlns="urn:mace:shibboleth:2.0:afp"

 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

 xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd">

 <AttributeFilterPolicy id="carsiAttrFilterPolicy">

 <PolicyRequirementRule xsi:type="ANY" />

 <AttributeRule attributeID="eduPersonScopedAffiliation" permitAny="true" />

 <AttributeRule attributeID="eduPersonTargetedID" permitAny="true" />

 </AttributeFilterPolicy>

 <AttributeFilterPolicy id="carsiAttrFilterToSPPolicy">

 <PolicyRequirementRule xsi:type="Requester" value="https://sp.example.org" />

 <AttributeRule attributeID="eduPersonEntitlement" permitAny="true" />

 </AttributeFilterPolicy>

</AttributeFilterPolicyGroup>

4. IdP日志功能（请参考CARSI WIKI）

5. IdP隐私保护配置（请参考CARSI WIKI）

6. IdP测试及上线（请参考CARSI WIKI）

**7. IdP界面定制**

Idp原生界面定制只针对Idp + ldap认证方式，CAS认证方式不需要定制，会直接跳转到学校认证界面。