Attribútum_feloldás

A felhasználó azonosítása után az IdP még csak a REMOTE_USER változóban megkapott principal azonosítót tudja. A következő lépésben meg kell határozni a felhasználóhoz kapcsolódó attribútumokat. Ezeket az attribútumokat általában valamilyen adatbázisból (LDAP, SQL) kell lekérdezni, de lehetséges konstans, ill. származtatott attribútumokat is használni.

Fontos megjegyezni, hogy az attribútumok csak akkor adódnak át az SP-knek, ha ez az Attribute Release Policy-ban engedélyezve van. Természetesen fel nem oldott attribútumokat nem lehet átadni.

Az attribútum feloldást az IdP konfiguráció `IdPConfig` elemének `resolverConfig` attribútumában megadott XML állományban konfigurálhatjuk. Ez általában a **`resolver.xml`** vagy **`resolver.ldap.xml`** névre hallgat

Működő példa konfiguráció

```
<AttributeResolver xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns="urn:mace:shibboleth:resolver:1.0"
                   xsi:schemaLocation="urn:mace:shibboleth:resolver:1.0 shibboleth-resolver-1.0.xsd">

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonEntitlement">
                <DataConnectorDependency requires="directory"/>
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonAffiliation">
                <DataConnectorDependency requires="directory"/>
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:cn">
                <DataConnectorDependency requires="directory"/>
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:uid">
                <DataConnectorDependency requires="directory"/>
```

```
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonPrincipalName"
smartScope="niif.hu">
                <AttributeDependency requires="urn:mace:dir:attribute-def:uid"/>
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
smartScope="niif.hu">
                <AttributeDependency requires="urn:mace:dir:attribute-def:eduPersonAffiliation"/>
        </SimpleAttributeDefinition>

        <SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonOrgDN" >
                <DataConnectorDependency requires="staticOrgDN"/>
        </SimpleAttributeDefinition>

         <JNDIDirectoryDataConnector id="directory">
                <Search filter="uid%PRINCIPAL%">
                        <Controls searchScope="ONELEVEL_SCOPE" returningObjects="false" />
                </Search>
                <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
                <Property name="java.naming.provider.url"
                        value="ldap://directory.iif.hu:636/ou=users,o=niifi,on=iif,c=hu" />
                <Property name="java.naming.security.protocol" value="ssl" />
                <Property name="java.naming.security.principal"
                        value="uidniif-idp,ou=shib,ou=applications,o=niifi,o=niif,c=hu" />
                <Property name="java.naming.security.credentials" value="XXXXXXXX" />
        </JNDIDirectoryDataConnector>

        <StaticDataConnector id="staticOrgDN">
                <Attribute name="eduPersonOrgDN">
                        <Value>o=niifi,o=niif,c=hu</Value>
                </Attribute>
        </StaticDataConnector>

</AttributeResolver>
```

Attribútum feloldás menete

Az attribútum feloldás abból áll, hogy attribútum definícióhoz adat(bázis) konnektorokat rendelünk. Az adat konnektor feladata az attribútum értékének meghatározása, pl. külső adatforrásokból. Az attribútum definíció azt adja meg, hogy miként kell az értéket a Shibboleth által használt SAML assertionbe tenni.

Adatok kinyerése (DataConnector)

Minden adatforrás rendelkezik egy *id* mezővel, amelynek az összes adatforrásra nézve egyedinek kell lennie.

JNDIDirectoryDataConnector

Ennek segítségével állíthatjuk be a JNDI LDAP kapcsolat paramétereit. Ezen az interfészen keresztül tetszőleges LDAP v3 interfészt biztosító adatforrás lekérdezhető.

Példa:

```
<JNDIDirectoryDataConnector id="directory">
   <Search filter="uid=%PRINCIPAL%">
      <Controls searchScope="ONELEVEL_SCOPE" returningObjects="false" />
   </Search>
   <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
   <Property name="java.naming.provider.url"
         value="ldap://directory.iif.hu:636/ou=users,o=niifi,o=niif,c=hu" />
   <Property name="java.naming.security.protocol" value="ssl" />
   <Property name="java.naming.security.principal"
         value="uid=niif-idp,ou=shib,ou=applications,o=niifi,o=niif,c=hu" />
   <Property name="java.naming.security.credentials" value="XXXXXXXX" />
</JNDIDirectoryDataConnector>
```

Példa beállítások magyarázata (részletes beállítási lehetőségekkel kapcsolatban lásd a Shibboleth Wiki vonatkozó részét!)

- *Search@filter*: az az LDAP filter, amely alapján a REMOTE_USER értékéből megkereshető a felhasználó LDAP entry-je. Ha összetett szűrő szabályt kell mondani, akkor a **&** jelet **&**-vel kell eszképelni.
- *Search/Controls@searchScope*: az LDAP lekérdezés scope-ja. Lehetséges értékek:
  - ONELEVEL_SCOPE
  - OBJECT_SCOPE (base)
  - SUBTREE_SCOPE

- `java.naming.provider.url` *property*: LDAP URL, amely a search base DN-jét is tartalmazza
- `java.naming.provider.protocol` *property*: itt lehet megadni, hogy SSL-t használjon-e az LDAP kapcsolat kiépítésekor. Ha nem akarunk SSL-t használni, akkor ezt a property-t ne adjuk meg! Lásd még: LDAP kliens SSL
- `java.naming.security.principal` *property*: az a DN, amellyel a Shibboleth alkalmazás bind-ol az LDAP szerverhez.
- `java.naming.security.credentials` *property*: az előző DN-hez tartozó jelszó

JDBCDataConnector

E konnektor segítségével tetszőleges JDBC-n keresztül elérhető adatforrásból kinyerhetünk adatokat.

```
<JDBCDataConnector id="studentSystem"
                   dbURL="jdbc:postgresql://test.example.edu/test?user=postgres&password=test"
                   dbDriver="org.postgresql.Driver"
    <Query>select entitlement from foo where name = ?</Query>
</JDBCDataConnector>
```

A "?" karakterrel hivatkozhatunk a REMOTE_USER változóban kapott principal azonosítóra.

A `JDBCDataConnector` részletes paraméterezhetőségéről lásd a Shibboleth wiki vonatkozó részét!

StaticDataConnector

Ennek segítségével rendelhetünk statikus adatokat a felhasználókhoz. Legtöbbször akkor használjuk, ha az IdP-nél történt azonosítás tényéből attribútumokat akarunk származtatni.

```
<StaticDataConnector id="staticOrgDN">
  <Attribute name="eduPersonOrgDN">
    <Value>o=niifi,o=niif,c=hu</Value>
  </Attribute>
</StaticDataConnector>
```

Egy `StaticDataConnector` egyszerre több attribútumot is tud szolgáltatni, ill. egy attribútumnak több értéke is lehet. Bővebben lásd a Shibboleth wiki vonatkozó részét!

Attribútumok előkészítése (AttributeDefinition)

Az attribútum definíciók arra valók, hogy az adatforrásból származó értéket az átvitelt biztosító SAML szabványnak, illetve az attribútumot fogadó SP-nek megfelelő formátumba konvertálják. Ezért minden attribútum definíciónál meg lehet adni függőséget, amelyből az attribútum értéke származik. A függőségnek két fajtája van:

- **DataConnectorDependency**: az attribútum értéke egy már definiált adatforrásból származik.
- **AttributeDependency**: az attribútum értéke egy másik (feloldott) attribútum értékéből származik

Mindkét függőség megadásakor a *requires* XML attribútummal hivatkozhatunk a DataConnector vagy az AttributeDefinition *id*-jére. Ebből következik az is, hogy minden attribútum definíciónak egyedi *id* mezője kell, hogy legyen.

SimpleAttributeDefinition

Ezzel a pluginnal egyszerű műveleteket végezhetünk az adatforrásokból származó értékeken (vagy akár átalakítás nélkül is továbbíthatjuk). Az alábbi attribútumokkal rendelkezik:

- *id*: ezzel lehet rá függőségekben hivatkozni, ill. az attribútum forrásának megállapításához is felhasználható. Az Assertion-ben ennek az értéke szerepel attribútum névként.
- *sourceName*: ezzel lehet explicit módon meghatározni a forrás nevét
- *smartScope*: ha az érték nem scope-olt (azaz nem `valami@valahol` formátumú), akkor az attribútum scope-ja a `smartScope` lesz, ellenkező esetben a scope értéke a "@ utáni rész" lesz (pl.: `valahol`).
  - (Leegyszerűsítve) egy Assertion-ben egy attribútum így adható meg: attribútum név + scope + érték(ek)
- *allowEmpty*: ez a boolean paraméter adja meg, hogy az üres érték elfogadható-e.

  Alapértelmezett értéke `false`, azaz ha nincs érték, akkor az Assertion-be nem kerül bele az attribútum. Ha `true`, akkor érték nélkül kerül bele.

A *sourceName* mezőt nem kötelező megadni, mert a forrás attribútum neve megadható az *id* paraméterben is. A forrás attribútum nevének meghatározása a következő sorrendben történik:

1. Ha meg van adva a *sourceName*, akkor az adat konnektortól ezt az attribútumot kapja meg
2. Ha van olyan - az adat konnektor által nyújtott - attribútum, amely az *id* mezővel teljesen megegyezik, akkor annak az értékét használja

3. Egyébként az adat konnektortól az *id* mezőben megadott paraméter utolsó "**:**" vagy "**/**" jel utáni részének megfelelő attribútumot kérdezi le.

Példa 1.: a * directory* nevű adat konnektortól lekérdezi a "cn" attribútumot, majd ennek értékét az `urn:mace:dir:attribute-def:cn` attribútumban küldi el a másik félnek.

```
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:cn">
    <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>
```

Példa 2.: a *directory* nevű adat konnektortól lekérdezi a *displayName* attribútumot, majd ennek értékét az `urn:mace:dir:attribute-def:<b>cn</b>` (!) attribútumban küldi el a másik félnek.

```
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:cn" sourceName="displayName">
    <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>
```

Példa 3.: a (már korábban feloldott) `urn:mace:dir:attribute-def:uid` attribútumot (amennyiben az nem scope-olt) kiegészíti az "niif.hu" scope-pal, és ezt adja át `urn:mace:dir:attribute-def:eduPersonPrincipalName` néven. Ha viszont az uid értéke pl. `valaki@valahol`, akkor az átadott érték a `valaki` lesz, a scope pedig `valahol`.

```
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:eduPersonPrincipalName" smartScope="niif.hu">
    <AttributeDependency requires="urn:mace:dir:attribute-def:uid"/>
</SimpleAttributeDefinition>
```

Részletes leírást lásd a Shibboleth wiki vonatkozó részében!

CompositeAttributeDefinition

TODO, lásd: https://spaces.internet2.edu/display/SHIB/CompositeAttributeDefinition

RegExpAttributeDefinition

TODO, lásd: https://spaces.internet2.edu/display/SHIB/RegExpAttributeDefinition

ScriptletAttributeDefinition

TODO, lásd: https://spaces.internet2.edu/display/SHIB/ScriptletAttributeDefinition

SAML2PersistentID

TODO, lásd: https://spaces.internet2.edu/display/SHIB/SAML2PersistentIDAttributeDefinition

Tesztelés

A Shibboleth IdP-hez tartozik egy **resolvertest** névre hallgató program, amellyel ellenőrizhetjük az attribútumok feloldását. Használatához először be kell állítani a telepítésnek megfelelően az IDP_HOME és a JAVA_HOME változókat.

Példa: `/usr/local/shibboleth-idp/bin/resolvertest --resolverxml=file:///etc/shibboleth-idp/resolver.ldap.xml --user=bajnokk`

```
<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="ttp://www.w3.org/2001/XMLSchema-instance"
        AttributeName="urn:mace:dir:attribute-def:eduPersonOrgDN"
        AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>o=niifi,o=niif,c=hu</AttributeValue>
</Attribute>

<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        AttributeName="urn:mace:dir:attribute-def:uid"
        AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>bajnokk</AttributeValue>
</Attribute>

<Attribute xmlns="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instanc)"
        AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
        AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue Scope="niif.hu">bajnokk</AttributeValue>
</Attribute>
```

Forrás

- https://spaces.internet2.edu/display/SHIB/NewIdPAttribute

- https://spaces.internet2.edu/display/SHIB/IdPAttributeConfig

---

Változat #3
cziernorbert hozta létre 9 április 2025 16:35:11
cziernorbert frissítette 10 április 2025 09:53:18