Shib2IdpAttrib

Az attribútum feloldást az `IDP_HOME/conf` könyvtárban található **`attribute-resolver.xml`** névre hallgató fájlban konfigurálhatjuk. A fájl szerkezetét tekintve **négy részből** áll.

Attribute-resolver alapbeállítások

Ezeket általában nem kell állítgatni, megfelelőek az alapbeállítások

```
<AttributeResolver xmlns="urn:mace:shibboleth:2.0:resolver"
xmlns:resolver="urn:mace:shibboleth:2.0:resolver"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:pc="urn:mace:shibboleth:2.0:resolver:pc"
    xmlns:ad="urn:mace:shibboleth:2.0:resolver:ad" xmlns:dc="urn:mace:shibboleth:2.0:resolver:dc"
    xmlns:enc="urn:mace:shibboleth:2.0:attribute:encoder" xmlns:sec="urn:mace:shibboleth:2.0:security"
    xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver classpath:/schema/shibboleth-2.0-attribute-
resolver.xsd
                        urn:mace:shibboleth:2.0:resolver:pc classpath:/schema/shibboleth-2.0-attribute-resolver-pc.xsd
                        urn:mace:shibboleth:2.0:resolver:ad classpath:/schema/shibboleth-2.0-attribute-resolver-ad.xsd
                        urn:mace:shibboleth:2.0:resolver:dc classpath:/schema/shibboleth-2.0-attribute-resolver-dc.xsd
                        urn:mace:shibboleth:2.0:attribute:encoder classpath:/schema/shibboleth-2.0-attribute-
encoder.xsd
                        urn:mace:shibboleth:2.0:security classpath:/schema/shibboleth-2.0-security.xsd">

    <!-- ... -->
</AttributeResolver>
```

Attribútumok definiálása

Az attribútum-definíciós szakasz igazából egyfajta egységesítése és előkészítése különböző forrásokból kinyerhető és később továbbítható adatoknak. Egy attribútum definiálásakor meg kell adni az alapként szolgáló `<AttributeDefinition>` elemet három attribútumával:

```
<resolver:AttributeDefinition id="cn" xsi:type="simple:Simple"
        xmlns="urn:mace:shibboleth:2.0:resolver:ad">
```

- **id** - az attribútum egyedi neve (nagyon fontos a jó névválasztás :)
- **xsi:type** - értéke lehet `Simple` vagy `Scoped`, de mivel a második nem szabványos, így törekedni kellene a `Simple` használatára
- **xmlns** - alapértelmezett értéke: `urn:mace:shibboleth:2.0:resolver:ad`

Az `<AttributeDefinition>` elemen belül meg kell adni az attribútum függőségét és az attribútum kódolási tulajdonságait

Attribútumok függősége

Egy attribútum függhet bármilyen más, az attribute-resolver.xml fájlban definiált elemtől, legyen az másik `<AttributeDefinition>`, vagy `<DataConnector>`. Egy attributum több más elemtől is függhet. Az egyetlen attribútuma a forrás elem azonosítója.

`<resolver:Dependency ref="ID_DEPENDENCY1" />`

Attribútumok kódolási tulajdonságai

Egy attribútumhoz többféle kódolási mechanizmust megadhatunk, melyek meghatározzák, hogy az attribútum kiadásakor milyen formátum(ok)ban lesz elérhető az aktuális attribútum értéke. Ha nem adunk meg kódolási mechanizmust, alapértelmezetten `SAML2String` alapon kódol. Egy kódolás megadása az `<AttributeEncoder>` elem segítségével történik. A szükséges attribútumok

- **xsi:type** - értéke a kódolás típusa
- **xmlns** - alapértelmezett értéke: `urn:mace:shibboleth:2.0:resolver:encoder`
- **name** - a megadott típuson belüli azonosító
- **friendlyName** - :)

Példa

```
<resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
                           name="oid:1.3.6.1.4.1.5923.1.1.1.7"
                           friendlyName="commonName" />
```

Kapcsolódások adattárakhoz

Ahhoz, hogy megkaphassuk az egyes attribútumokhoz tartozó értéket, valamilyen adattárból (adatbázis, címtár) kell őket kinyernünk, hiszen ekkor még csak a sikeres azonosítás után tartunk, és csak a felhasználói nevet tudjuk, amivel az azonosítás megtörtént. **Fontos**, hogy az egyes kapcsolódások definiálásakor erre a felhasználói névre a **`$requestContext.principalName`** néven hivatkozhatunk, amely kiindulópontként szolgálhat lekérdezéseinkhez.

Kapcsolódás címtárhoz

1. Konnektor definiálása

Új adatbáziskapcsolat létrehozásához definiálnunk kell a konnektort `<DataConnector xsi:type="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc">` az alábbi attribútumokkal

Attribútumok, melyeket kötelező megadni

- **id** - egyedi azonosító, mellyel az attribútum definicióknál elérhetjük a konnektort
- **ldapURL** - a címtár elérési útja. Több is megadható vesszőkkel elválasztva, ekkor a megadott sorrend alapján addig próbálkozik, amíg valahol nem tud csatlakozni
- **baseDN** - a címtárban való kereséshez tartozó BaseDN
- **principal** - a címtár bind-olására használandó felhasználói név
- **principalCredential** - a címtár bind-olására használandó felhasználói névhez tartozó jelszó

```
<resolver:DataConnector xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                        id="UNIQUE_ID"
                        ldapURL="LDAP_URL"
                        baseDN="BASE_DN"
                        principal="PRINCIPAL_NAME"
                        principalCredential="PRINCIPAL_CREDENTIAL">

    <!-- Ide kerülnek majd az további konfigurációs beállítások a következő lépések alapján -->

</resolver:DataConnector>
```

2. Az LDAP lekérdezés definiálása

```
<resolver:DataConnector xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                        id="UNIQUE_ID"
                        ldapURL="LDAP_URL"
                        baseDN="BASE_DN"
                        principal="PRINCIPAL_NAME"
                        principalCredential="PRINCIPAL_CREDENTIAL">

    <FilterTemplate>
        <![CDATA[
            (uid=${requestContext.principalName})
        ]]>
```

```
    </FilterTemplate>

    <!-- Ide kerülhet a lekérdezési eredmény mezőneveinek és értékeinek felüldefiniálása -->

</resolver:DataConnector>
```

Kapcsolódás relációs adatbázisokhoz

1. Konnektor definiálása

Új adatbáziskapcsolat létrehozásához definiálnunk kell a konnektort `<DataConnector xsi:type="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc">` az alábbi attribútumokkal

Attribútumok, melyeket kötelező megadni

- **id** - egyedi azonosító, mellyel az attribútum definicióknál elérhetjük a konnektort

Attribútumok, melyeket opcionálisan megadhatók

- **readOnlyConnection** - logikai érték, mely meghatározza, hogy az adatbázis csak olvasható, vagy esetleg írható is. Alapértelmezés szerint `true`, azaz csak olvasható
- **queryUsesStoredProcedure** - logikai érték, mely meghatározza, hogy az 5. lépésnél bemutatott módon definiált SQL lekérdezések használhatnak-e előre meghatározott eljárásokat. Alapértelmezés szerint nem, azaz `false`
- **cacheResults** - logikai érték, mely meghatározza, hogy a lekérdezés eredménye eltárolható-e a felhasználó munkamenetének lejártáig. Alapértelmezés szerint igen, azaz `true`

```
<resolver:DataConnector xsi:typ="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                        id="UNIQUE_ID">

    <!-- Ide kerülnek majd az további konfigurációs beállítások a következő lépések alapján -->

</resolver:DataConnector>
```

2. Függőségek definiálása

Opcionális

3. Másodlagos adatkapcsolat definiálása

Opcionális

4/a. Idp által natívan vezérelt adatbáziskapcsolatok beállítása

Az Idp alkalmazás által vezérelt kapcsolathoz definiálnunk kell egy `<ApplicationManagedConnection>` elemet az alábbi (mind kötelezően megadandó) attribútumokkal

- **jdbcDriver** - a JDBC meghajtó teljes elérési útvonala
- **jdbcURL** - URL, melyen elérjük az adatbázist
- **jdbcUserName** - adatbázis eléréséhez tartozó felhasználó
- **jdbcPassword** - a fenti felhasználóhoz tartozó jelszó

Példa MySQL adatbázis eléréséhez

```
<resolver:DataConnector xsi:type="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                    id="UNIQUE_ID">

    <!-- Ide kerülhetnek a függőségek a másodlagos adatkapcsolatokkal kapcsolatos beállítások -->

    <ApplicationManagedConnection jdbcDriver="com.mysql.jdbc.Driver"
                                  jdbcURL="jdbc:mysql://localhost:3306/DATABASE_NAME?autoReconnect=true"
                                  jdbcUserName="DATABASE_USER"
                                  jdbcPassword="DATABASE_USER_PASSWORD" />

    <!-- Ide kerülnek majd az további konfigurációs beállítások a következő lépések alapján -->

</resolver:DataConnector>
```

4/b. Konténer által vezérelt adatbáziskapcsolatok beállítása

5. SQL lekérdezés definiálása

```
<resolver:DataConnector xsi:type="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                    id="UNIQUE_ID">

    <!-- Ide kerülhetnek a függőségek a másodlagos adatkapcsolatokkal kapcsolatos beállítások -->

    <ContainerManagedConnection resourceName="RESOURCE_NAME" />

    <QueryTemplate>
        <![CDATA[
            SELECT * FROM PEOPLE WHERE userid='$requestContext.principalName'
        ]]>
    </QueryTemplate>

    <!-- Ide kerülhet a lekérdezési eredmény mezőneveinek és értékeinek felüldefiniálása -->
```

```
</resolver:DataConnector>
```

6. Lekérdezési eredmény mezőneveinek és értékeinek felüldefiniálása

Opcionális

Alapértelmezés szerint a lekérdezések eredményét mezőnevenként és a hozzákapcsolódó értékként egy-egy attribútumba szervezi a konnektor, melyet lehetőségünk van felüldefiniálni, ehhez a `<Column>` elemet használhatjuk az alábbi atttribútumokkal

Kötelező megadni

*__columnName__ - az lekérdezés eredményének mezője, mellyel kapcsolatban módosításokat hajtanánk végre

Az alábbiak közül minimum egyet kötelező megadni

- **attributeID** - az attribútum azonosítója, melyhez hozzárendeljük az eredményt
- **type** - az eredmény típusa. A következők közül választhatunk: BigDecimal, Boolean, Byte, ByteArray, Date, Double, Float, Integer, Long, Object, Short, String, Time, Timestamp, URL

```
<resolver:DataConnector xsi:type="RelationalDatabase" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                        id="UNIQUE_ID">

    <!-- Ide kerülhetnek a függőségek a másodlagos adatkapcsolatokkal kapcsolatos beállítások ill. a
kapcsolatvezérló beállítások -->



    <QueryTemplate>
        <![CDATA[
            SELECT * FROM people WHERE userid='$requestContext.principalName'
        ]]>
    </QueryTemplate>

    <Column columnName="firstname" attributeID="fname" />
    <Column columnName="personid" type="String" />

</resolver:DataConnector>
```

7. Összegzés

Működő példa a fentieket összegezve

```
<!-- ###### ###### ###### ### -->
<!-- Data Connectors -->
<!-- ###### ###### ###### ### -->

<resolver:DataConnector id="vhoMySQLsurname" xsi:type="RelationalDatabase"
xmlns="urn:mace:shibboleth:2.0:resolver:dc">

    <ApplicationManagedConnection
        jdbcDriver="com.mysql.jdbc.Driver"
        jdbcURL="jdbc:mysql://localhost:3306/VHOtools?autoReconnect=true"
        jdbcUserName="DATABASE_USER"
        jdbcPassword="DATABASE_USER_PASSWORD" />

    <QueryTemplate>
      <![CDATA[
          SELECT uniqueID FROM vho_Users WHERE username = '$requestContext.principalName'
      ]]>
    </QueryTemplate>

    <Column columnName="uniqueID" attributeID="uid" />

</resolver:DataConnector>
```

Principal Connectors

Ezt sem kell babrálni :)

```
<!-- ###### ###### ###### ### -->
<!-- Principal Connectors -->
<!-- ###### ###### ###### ### -->

<resolver:PrincipalConnector xsi:type="Transient" xmlns="urn:mace:shibboleth:2.0:resolver:pc"
id="shibTransient"
                    nameIDFormat="urn:mace:shibboleth:1.0:nameIdentifier" />
<resolver:PrincipalConnector xsi:type="Transient" xmlns="urn:mace:shibboleth:2.0:resolver:pc"
id="saml1Unspec"
```

```
                    nameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" />
<resolver:PrincipalConnector xsi:type="Transient" xmlns="urn:mace:shibboleth:2.0:resolver:pc"
id="saml2Transient"
                    nameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
```

Attribútum

Változat #3
cziernorbert hozta létre 9 április 2025 16:37:11
cziernorbert frissítette 10 április 2025 09:55:06