

Shib2PersistentId

Perzisztens azonosító használata Shibboleth2 IdP esetén

Ez az oldal a Shibboleth `storedId` plugin telepítését írja le MySQL adatbázis motorral.

Adatbázis driver telepítése

A MySQL JDBC driver a következő URL-ről érhető el: <http://dev.mysql.com/downloads/#connector-j>.
Letöltés után a kitömörített drivercsomagból a .jar végű fájlt kell bemásolni a `/usr/share/tomcat6/lib` könyvtár alá.

Táblaszerkezet

```
CREATE TABLE `shibpid` (  
  `localEntity` varchar(200) NOT NULL,  
  `peerEntity` varchar(200) NOT NULL,  
  `principalName` varchar(200) NOT NULL,  
  `localId` varchar(200) NOT NULL,  
  `persistentId` varchar(200) NOT NULL,  
  `peerProvidedId` varchar(200) default NULL,  
  `creationDate` timestamp NOT NULL default CURRENT_TIMESTAMP on update CURRENT_TIMESTAMP,  
  `deactivationDate` timestamp NULL default NULL,  
  KEY `i_shibpid_pid` (`persistentId`),
```

```
KEY `i_shibpid_pid_date` (`persistentId`,`deactivationDate`),
KEY `i_shibpid_lid` (`localEntity`,`peerEntity`,`localId`),
KEY `i_shibpid_lid_date` (`localEntity`,`peerEntity`,`localId`,`deactivationDate`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8
```

Perzisztens attribútum feloldása

Az attribute-resolver.xml konfigurációs fájlban vegyük fel a következő DataConnectort illetve PrincipalConnectort:

```
<resolver:DataConnector xsi:type="StoredId"
  xmlns="urn:mace:shibboleth:2.0:resolver:dc"
  id="persistentIdConnector"
  sourceAttributeID="uid"
  generatedAttributeID="persistentId"
  salt="valami-random-sztring">
  <resolver:Dependency ref="myLDAP" />
  <ApplicationManagedConnection jdbcDriver="com.mysql.jdbc.Driver"
    jdbcURL="jdbc:mysql://localhost/installfest"
    jdbcUserName="root"
    jdbcPassword="" />
</resolver:DataConnector>

<resolver:PrincipalConnector xsi:type="StoredId"
  xmlns="urn:mace:shibboleth:2.0:resolver:pc" id="saml2Persistent"
  nameIDFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
  storedIdDataConnectorRef="persistentIdConnector" />
```

Amennyiben alkalmazáserver oldali kapcsolatkezelést szeretnénk használni, a [következő leírás](#) hasznos lehet.

Definiáljuk a persistentId attribútumot (a transientId ELŐTT! - különben a transientId -t választja ki az idp...):

```
<resolver:AttributeDefinition id="persistentId" xsi:type="Simple"
  xmlns="urn:mace:shibboleth:2.0:resolver:ad">
  <resolver:Dependency ref="persistentIdConnector" />
  <resolver:AttributeEncoder xsi:type="SAML2StringNameID"
```

```
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
nameFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
</resolver:AttributeDefinition>
```

Perzisztens attribútum kódolása a SAML válaszbba

Az `attribute_filter.xml` -ben meg kell adni hogy a frissen létrehozott `persistentId` attribútumot kiadja az SP-nek:

```
<AttributeFilterPolicy id="releaseNameIDToAnyone">
  <PolicyRequirementRule xsi:type="basic:ANY" />

  <AttributeRule attributeID="transientId">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
  <AttributeRule attributeID="persistentId">
    <PermitValueRule xsi:type="basic:ANY" />
  </AttributeRule>
</AttributeFilterPolicy>
```

Változat #3

cziernorbert hozta létre 9 április 2025 16:34:51

cziernorbert frissítette 10 április 2025 09:52:59