

Shib3IdpAttrib

Shibboleth 3 IdP attribútum feloldás beállítása

Vonatkozó állományok:

- `{idp.home}/conf/attribute-resolver.xml`
- `{idp.home}/conf/idp.properties`

Az alábbiakban LDAP címtárat használunk forrás adatbázisként az attribútumok feloldásához. Az `{idp.home}/conf/ldap.properties` állományban beállított kapcsolódási paraméterek az attribútum feloldáshoz is használhatók.

Az `{idp.home}/conf/attribute-resolver-ldap.xml` állomány jó kiindulási pont, cseréljük le erre az `{idp.home}/conf/attribute-resolver.xml` állományt.

```
cd /opt/shibboleth-idp/conf # vagy ahová az IdP telepítésre került
cp attribute-resolver.xml attribute-resolver-simple.xml # másolat készítése
cp attribute-resolver-ldap.xml attribute-resolver.xml
```

Szerkesszük az alábbiak szerint az `{idp.home}/conf/attribute-resolver.xml` állományt. A *mail* attribútumot már tartalmazza a beállító állomány. Az alábbi példában az *sn* és *givenName* attribútumokat vesszük fel.

```
<!-- ===== -->
<!--   Attribute Definitions           -->
<!-- ===== -->

<!-- ... további tartalom ... -->

<!--
In the rest of the world, the email address is the standard identifier,
despite the problems with that practice. Consider making the EPPN value
the same as your official email addresses whenever possible.
-->

<resolver:AttributeDefinition id="mail" xsi:type="ad:Simple" sourceAttributeID="mail">
  <resolver:Dependency ref="myLDAP" />
  <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:mail"
```

```

encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.3"
friendlyName="mail" encodeType="false" />
</resolver:AttributeDefinition>

<resolver:AttributeDefinition id="sn" xsi:type="ad:Simple" sourceAttributeID="sn">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:sn"
encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.4" friendlyName="sn"
encodeType="false" />
</resolver:AttributeDefinition>

<resolver:AttributeDefinition id="givenName" xsi:type="ad:Simple" sourceAttributeID="givenName">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:givenName"
encodeType="false" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.42"
friendlyName="givenName" encodeType="false" />
</resolver:AttributeDefinition>

<!-- ===== -->
<!--   Data Connectors           -->
<!-- ===== -->

<!-- ... további tartalom ... -->

```

- A **18, 24.** sorban adjuk meg az attribútum nevét, valamint, hogy egyszerű attribútumról van szó, nem szükséges átalakítani.
- A **19, 25.** sor hivatkozik a használandó LDAP kapcsolatra.
- A **21, 27.** sorbeli SAML2String előállításához szükséges oid megegyezik az attribútum LDAP sémabeli oid-jával.

Dokumentáció:

- <https://wiki.shibboleth.net/confluence/display/IDP30/AttributeResolverConfiguration>

Változat #3

cziernorbert hozta létre 9 április 2025 16:35:31

cziernorbert frissítette 10 április 2025 09:53:36