Shib2IdpARP

Az attribútumok kiadását az `IDP_HOME/conf` könyvtárban található **`attribute-filter.xml`** névre hallgató fájlban konfigurálhatjuk.

Attribute-filter alapbeállítások

Ezeket általában nem kell állítgatni, megfelelőek az alapbeállítások

```
<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy" xmlns="urn:mace:shibboleth:2.0:afp"
    xmlns:basic="urn:mace:shibboleth:2.0:afp:mf:basic"
xmlns:saml="urn:mace:shibboleth:2.0:afp:mf:saml"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:mace:shibboleth:2.0:afp classpath:/schema/shibboleth-2.0-afp.xsd
                        urn:mace:shibboleth:2.0:afp:mf:basic classpath:/schema/shibboleth-2.0-
afp-mf-basic.xsd
                        urn:mace:shibboleth:2.0:afp:mf:saml classpath:/schema/shibboleth-2.0-
afp-mf-saml.xsd">

   <!-- ... -->

</AttributeFilterPolicyGroup>
```

Kiadási szabálycsoportok megadása

Egy kiadási szabálycsoportot a `<AttributeFilterPolicy>` elemmel definiálhatunk, melynek kötelező aleleme egy `<PolicyRequirementRule xsi:type="MATCHING_RULE_TYPE">` elem, amely meghatározza, hogy a szabály mely attribútumok esetén aktivizálódjon. A működése kifejezetten egyszerű, a kiadási szabály akkor lesz aktív, mikor a `PolicyRequirementRule` elem attribútumában meghatározott egyezési feltétel igaz értéket ad.

Egy kiadási szabálycsoport (attribute filters) meghatározhatja egy sor attribútum számára, hogy mikor, milyen feltételek teljesülése mellett adhatók ki értékeik.

Egy kiadási szabály megadása

Egy attribútumra vonatkozó szabályt a `<AttributeRule>` elemmel határozunk meg, melynek kötelező attrubútuma annak az attribútumnak az azonosítója, melyre a szabályokat vonatkoztatni szeretnénk, és egy elem, amely meghatározza, hogy milyen illeszkedés esetében aktív a szabály.

Példa I.

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

Egy attribútumra vonatkozó szabályban természetesen további finomításokat megadhatunk.

Példa II.

```
    <AttributeRule attributeID="eduPersonAffiliation">
        <PermitValueRule xsi:type="basic:OR">
            <Rule xsi:type="basic:AttributeValueString" value="faculty" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="student" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="staff" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="alum" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="member" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="affiliate" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="employee" ignoreCase="true"/>
            <Rule xsi:type="basic:AttributeValueString" value="library-walk-in"
ignoreCase="true"/>
        </PermitValueRule>
    </AttributeRule>
```

Magyarázat: a kiadási szabály, akkor adja ki az `eduPersonAffiliation` attribútumot, amennyiben annak értéke egyezik a felsoroltak valamelyikével (`OR` szabály - tehát elég, hogy egyikkel egyezzen).

Az alábbi listában található egyezési szabályok alkalmazhatók egy-egy `<PermitValueRule>` megadásakor:

- ANY - Always evaluates to true

- AND - Evaluates to true if all contained rules are true
- OR - Evaluated to true if any contained rule is true
- NOT - Evaluates to true if the contained rule evaluates to false
- AttributeRequesterString - Evaluates to true if the attribute requester's entity ID matches a given string
- AttributeIssuerString - Evaluates to true if the attribute issuer's entity ID matches a given string
- PrincipalNameString - Evaluates to true if the user's principal name matches a given string
- AuthenticationMethodString - Evaluates to true if the method used to authenticate the user matches a given string
- AttributeValueString - Evaluates to true if the value of a given attribute matches a given string
- AttributeScopeString - Evaluates to the true if the scope of a value of a given attribute matches a given string
- AttributeRequesterRegex - Evaluates to true if the attribute requester's entity ID matches a given regular expression
- AttributeIssuerRegex - Evaluates to true if the attribute issuer's entity ID matches a given regular expression
- PrincipalNameRegex - Evaluates to true if the user's principal name matches a given regular expression
- AuthenticationMethodRegex - Evaluates to true if the method used to authenticate the user matches a given regular expression
- AttributeValueRegex - Evaluates to true if the value of a given attribute matches a given regular expression
- AttributeScopeRegex - Evaluates to the true if the scope of a value of a given attribute matches a given regular expression
- Script - Evaluates a scriptlet to determine if the rule evaluates to true
- AttributeRequesterInEntityGroup - Evaluates to true if the attribute requester is defined within a given entity group in SAML metadata
- AttributeIssuerInEntityGroup - Evaluates to true if the attribute issuer is defined within a given entity group in SAML metadata
- AttributeScopeMatchesShibMDScope - Evaluates to true the scope of an attribute value matches the scope defined in the attribute issuer's metadata.

Változat #1
document-uploader hozta létre 2025-08-07 12:06:28 CEST
document-uploader frissítette 2025-08-07 12:06:28 CEST