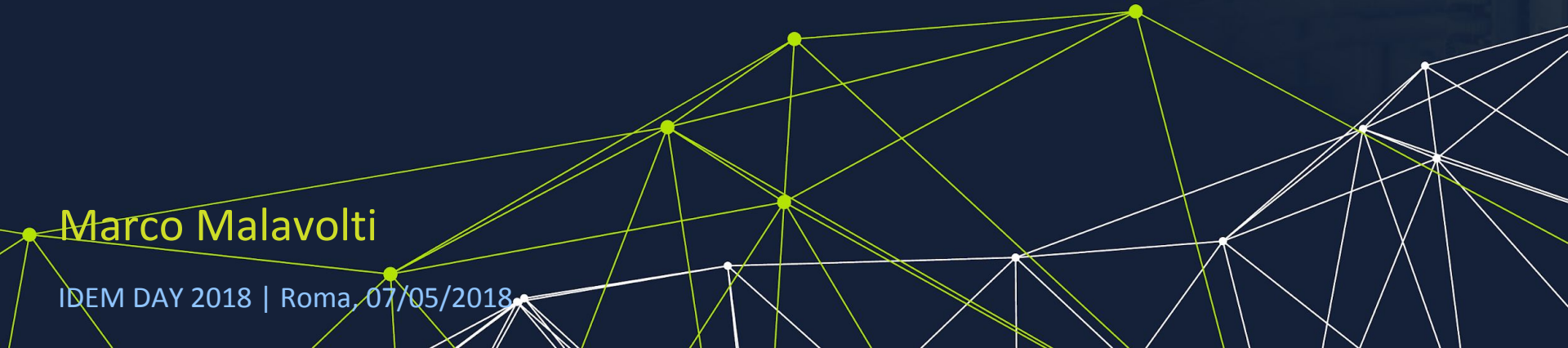
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Attribute Filter

La Gestione del rilascio degli Attributi in Shibboleth



Marco Malavolti

IDEM DAY 2018 | Roma, 07/05/2018

Materiale necessario:

1. **`attribute-resolver*.xml`:**
   Definisce gli attributi e dove recuperarli per abilitarne il supporto sull'IdP

2. **`attribute-filter*.xml`:**
   Definisce le regole per il rilascio degli attributi dall'IdP verso gli SP

3. **`services.xml`:**
   collega Resolvers e Filters tra loro e abilita il tutto

4. **`idp.properties`:**
   valorizza alcune proprietà utili: *scope*

Attributo: eduPersonScopedAffiliation (ePSA)

Nome: **eduPersonScopedAffiliation**

Tipo: **Scoped** (`<affiliazione>@<organizzazione>`) scope

Valori Possibili per `<affiliazione>`: **student**, **staff**, **member**,...
(La loro definizione si trova sul documento "Specifiche alla Compilazione e uso degli attributi nella Federazione IDEM")

Valori possibili per `<organizzazione>`: il dominio dell'organizzazione (quello di norma usato per gli indirizzi mail) **[es.: example.org]**

ePSA: Come ne abilito il supporto?

1. Valorizzo lo scope per il mio IdP sul suo "`idp.properties`":
   `idp.scope = example.org`

   (in questo modo posso usare la proprietà "**`%{idp.scope}`**" nel file `attribute-resolver.xml`)

2. Definisco l'attributo nell'`attribute-resolver.xml` come:

```
<AttributeDefinition scope="%{idp.scope}" xsi:type="Scoped" id="eduPersonScopedAffiliation"
sourceAttributeID="eduPersonAffiliation">
   <Dependency ref="myLDAP" />
   <DisplayName xml:lang="en">Scoped Affiliation</DisplayName>
   <DisplayName xml:lang="it">Affiliazione con ambito</DisplayName>
   <DisplayDescription xml:lang="en">Affiliation Scoped: Type of affiliation with Home Organization with
scope</DisplayDescription>
   <DisplayDescription xml:lang="it">Affiliazione con ambito: ruolo ricoperto con dominio
dell'Organizzazione</DisplayDescription>
   <AttributeEncoder xsi:type="SAML2ScopedString" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
friendlyName="eduPersonScopedAffiliation" encodeType="false" />
</AttributeDefinition>
```

ePSA: Come ne abilito il supporto?

3. Mi assicuro che l'Attribute Resolver in cui ho definito l'ePSA sia presente in `services.xml`:

```
<util:list id ="shibboleth.AttributeResolverResources">
   <value>%{idp.home}/conf/attribute-resolver.xml</value>
</util:list>
```

4. Abilito le modifiche applicate al attribute-resolver.xml:

   curl - sk https://localhost/idp/profile/admin/reload-service?id=**shibboleth.AttributeResolverService**

ePSA: Come ne regolo il rilascio?

1. Genero il mio Attribute Filter "**attribute-filter-custom.xml**":

```
<AttributeFilterPolicyGroup id="ID-UNIVOCO-UTILE-PER-LOGGING"
       xmlns="urn:mace:shibboleth:2.0:afp"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd">

   <!-- Politica di rilascio degli attributi con id="corso" rilascia schacHomeOrganizationType e ePSA
        all'SP con entityID="https://sp.example.org/shibboleth". -->
   <AttributeFilterPolicy id="ID-UNIVOCO-DELLA-POLITICA-DI-RILASCIO">
       <PolicyRequirementRule xsi:type="Requester" value="https://sp.example.org/shibboleth" />

       <!-- L'attributo eduPersonPrincipalName NON viene rilasciato -->
       <AttributeRule attributeID="eduPersonPrincipalName">
           <DenyValueRule xsi:type="ANY" />
       </AttributeRule>

       <!-- L'attributo eduPersonEntitlement viene rilasciato solo col valore stabilito -->
       <AttributeRule attributeID="eduPersonEntitlement">
           <PermitValueRule xsi:type="Value" value="urn:mace:dir:entitlement:common-lib-terms" ignoreCase="true" />
       </AttributeRule>
   </AttributeFilterPolicy>
   ...
```

RuleType

RuleType

RuleType

l'attributeID DEVE essere uguale all'ID usato nell'attribute-resolver.xml

ePSA: Come ne regolo il rilascio?

```
<!-- L'attributo eduPersonScopedAffiliation viene rilasciato qualsiasi sia il valore per lui generato -->
<AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="AND">
        <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true" />
        <Rule xsi:type="OR">
            <Rule xsi:type="Value" value="faculty" ignoreCase="true" />
            <Rule xsi:type="Value" value="student" ignoreCase="true" />
            <Rule xsi:type="Value" value="staff" ignoreCase="true" />
            <Rule xsi:type="Value" value="alum" ignoreCase="true" />
            <Rule xsi:type="Value" value="member" ignoreCase="true" />
            <Rule xsi:type="Value" value="affiliate" ignoreCase="true" />
            <Rule xsi:type="Value" value="employee" ignoreCase="true" />
            <Rule xsi:type="Value" value="library-walk-in" ignoreCase="true" />
        </Rule>
    </PermitValueRule>
</AttributeRule>
</AttributeFilterPolicyGroup>
```

RuleType

RuleType

RuleType

Le *RuleType* sono applicabili sia a <PolicyRequirementRule> che ad <AttributeRule> e possono avere 2 modalità di applicazione: PolicyRule (yes/no) o Matchers (ritorna un intervallo di valori).
I **<PolicyRequirementRule>** usano di solito la "**PolicyRule**", mentre gli **<AttributeRule>** la "**Matchers**"

ePSA: Come ne regolo il rilascio?

2. Mi assicuro che l'Attribute Filter creato/modificato sia presente in `services.xml`:

```
<util:list id ="shibboleth.AttributeFilterResources">
   <value>%{idp.home}/conf/attribute-filter.xml</value>
   <value>%{idp.home}/conf/attribute-filter-custom.xml</value>
</util:list>
```

3. Abilito le modifiche applicate al `attribute-filter.xml`:

   a. Ricaricando solamente il servizio se non ho modificato `services.xml`:
   curl - sk https://localhost/idp/profile/admin/reload-service?id=**shibboleth.AttributeFilterService**

   b. Riavviando interamente l'IdP: `service jetty restart`

ESERCIZIO

Crea il tuo **attribute-filter-custom.xml** e configura:

1. Una regola che neghi alcuni valori

2. Una regola che escluda l'attributo *eduPersonPrincipalName*, ma permetta il *surname*

3. Una regola che rilasci *eduPersonScopedAffiliation* **SOLO SE** è "mario" l'utente

Verificare il funzionamento di ogni nuovo cambiamento prima di procedere al successivo.

Attribute Filter via Web

1. Creare la directory "**/opt/shibboleth-idp/tmp/httpClientCache**":
   a. `mkdir -p /opt/shibboleth-idp/tmp/httpClientCache`
   b. `chown jetty /opt/shibboleth-idp/tmp/httpClientCache`

2. Aggiungere al proprio "services.xml" il <bean> necessario:
   a. `vim /opt/shibboleth-idp/conf/services.xml`

```
<bean id="AF-Custom" class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"
   c:client-ref="shibboleth.FileCachingHttpClient"
   c:url="https://idp.example.org/attribute-filter-custom.xml"
   c:backingFile="%{idp.home}/conf/attribute-filter-custom.xml"/>
...
<util:list id ="shibboleth.AttributeFilterResources">
   <value>%{idp.home}/conf/attribute-filter.xml</value>
   <ref bean="AF-Custom"/>
</util:list>
```

3. Riavviare il servizio:
   a. `service jetty restart`

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

GRAZIE MILLE!

slides

http://bit.ly/2JwNbsk

Marco Malavolti - Servizio IDEM GARR AAI - (marco.malavolti@garr.it)