Daniele Albrizio (Università di Trieste)

Generazione e rilascio Attributi: Resolver e Filter

Vediamo

- attribute-resolver.xml
  - attributo statico
  - attributo scoped
  - attributo mapped
  - attributo templated
  - attributo scripted
- Riavvio del servizio per la risoluzione degli attributi

Attributi Statici

Attributi non presenti nel backend (ldap/AD)

- schacHomeOrganization
- schacHomeOrganizationType

Attribute definition

```
<resolver:AttributeDefinition id="schacHomeOrganization" xsi:type="ad:Simple"
                              sourceAttributeID="schacHomeOrganization">
  <resolver:Dependency ref="staticAttributes" />
  <resolver:AttributeEncoder xsi:type="enc:SAML2String"
                             name="urn:oid:1.3.6.1.4.1.25178.1.2.9"
                             friendlyName="schacHomeOrganization" />
</resolver:AttributeDefinition>
```

Data Connector

```
<resolver:DataConnector id="staticAttributes" xsi:type="dc:Static">

    <dc:Attribute id="schacHomeOrganization">
        <dc:Value>units.it</dc:Value>
    </dc:Attribute>

    <dc:Attribute id="schacHomeOrganizationType">
<dc:Value>urn:schac:homeOrganizationType:int:university</dc:Value>
    </dc:Attribute>

</resolver:DataConnector>
```

Scoped Attribute

Scoped Attribute: eduPersonScopedAffiliation

staff@units.it

faculty@units.it

member@units.it

Lo scope degli attributi DEVE essere dichiarato nei metadati dell'IdP

Si può esprimere con la variabile %{idp.scope} di idp.properties

Scoped Attribute

```
<resolver:AttributeDefinition xsi:type="ad:Scoped"
                              id="eduPersonScopedAffiliation"
                              scope="units.it"
                              sourceAttributeID="affiliation">
    <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
                               name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
                               friendlyName="eduPersonScopedAffiliation" />
</resolver:AttributeDefinition>
```

Mapped

```
<resolver:AttributeDefinition id="mappedGroup" xsi:type="ad:Mapped"
sourceAttributeID="memberOf">
    <resolver:Dependency ref="myLDAP" />
    <ad:DefaultValue passThru="true"/>
    <ad:ValueMap>
        <ad:ReturnValue>return1</ad:ReturnValue>
        <ad:SourceValue ignoreCase="true">fred</ad:SourceValue>
    </ad:ValueMap>
    <ad:ValueMap>
        <ad:ReturnValue>return1</ad:ReturnValue>
        <ad:SourceValue>source2</ad:SourceValue>
        <ad:SourceValue>source3</ad:SourceValue>
    </ad:ValueMap>
    <ad:ValueMap>
        <ad:ReturnValue>some_string_to_add_before_value:$1</ad:ReturnValue>
        <ad:SourceValue>(.+)</ad:SourceValue>
    </ad:ValueMap>
</resolver:AttributeDefinition>
```

Templated Attribute

```
<resolver:AttributeDefinition id="displayName" xsi:type="ad:Template">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="enc:SAML2String"
                name="urn:oid:2.16.840.1.113730.3.1.241"
                friendlyName="displayName" encodeType="false" />
        <ad:Template>
          <![CDATA[
              <-=| ${givenName} ${sn} |=->
          ]]>
        </ad:Template>
        <ad:SourceAttribute>sn</ad:SourceAttribute>
        <ad:SourceAttribute>givenName</ad:SourceAttribute>
</resolver:AttributeDefinition>
```

Scripted Attribute

```
<resolver:AttributeDefinition xsi:type="ad:Simple" id="addMail" sourceAttributeID="addM">
        <resolver:Dependency ref="addM" />
</resolver:AttributeDefinition>

<resolver:AttributeDefinition id="addM" xsi:type="ad:Script" dependencyOnly="true">
    <ad:ScriptFile>/opt/shibboleth-idp/conf/scripts/addMail.js</ad:ScriptFile>
</resolver:AttributeDefinition>
```

Reloadable Services

curl -sk https://localhost/idp/profile/admin/reload-service?id=shibboleth.Attribute**Resolver**Service | html2text

Esercizio

- Nel file attribute-resolver.xml configurare
  - 2 attributi statici schacHomeOrganization e schacHomeOrganizationType
  - 1 attributo scoped eduPersonScopedAffiliation
  - 1 attributo mapped mappedGroup
  - 1 attributo templated displayName
  - 1 attributo custom scripted
- Riavviare il servizio per la risoluzione degli attributi

Vediamo

- attribute-filter.xml
  - AttributeFilterPolicy
  - PolicyRequirementRule
  - PermitValue
  - DenyValue
- Consent
- Aggiungengere un file come risorsa filtro nell'IdP
- Riavviare il servizio del filtraggio degli attributi

Filtri sui valori degli attr.

```
<AttributeRule attributeID="Group">
    <PermitValueRule xsi:type="Value" value="Docente" ignoreCase="true" />
    <PermitValueRule xsi:type="Value" value="Tecnico" ignoreCase="true" />
    <PermitValueRule xsi:type="Value" value="Amministrativo"
ignoreCase="true" />
    <DenyValueRule xsi:type="Value" value="servizio" ignoreCase="true" />
</AttributeRule>
```

Per permettere qualsiasi valore:

```
<PermitValueRule xsi:type="ANY" />
```

Filtri sui valori degli attr.

```
<AttributeFilterPolicy>
  <PolicyRequirementRule xsi:type="InEntityGroup" groupID="http://edugain.org/" />
      <AttributeRule attributeID="eduPersonAffiliation">
        <PermitValueRule 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" />
        </PermitValueRule>
      </AttributeRule>
</AttributeFilterPolicy>
```

Filtri

Solo se richiesto nei metadati dell'SP

```
<AttributeRule attributeID="surname">
   <PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="true"/>
</AttributeRule>
```

Rilascia a tutti qualsiasi valore

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

R&S Entity Category

```
<AttributeFilterPolicy id="REFEDSResearchAndScholarship">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>
    ...
```

R&S Entity Category

```
<!-- Minimal subset of the "R and S" attribute bundle. -->
<!-- If ePPN values could be reassigned you MUST also release
eduPersonTargetedID -->

<AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="eduPersonTargetedID">
        <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
</AttributeRule>
<AttributeRule attributeID="email">
        <PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
</AttributeRule>
```

R&S Entity Category

```
<!-- Other attributes only if requested (could also be released unconditionally) -->

  <AttributeRule attributeID="givenName">
      <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="surname">
      <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
      <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>

</AttributeFilterPolicy>
```

Consent

- memorizzazione di default nei cookie client side ClientPersistentStorageService (possibile anche su DB)
- logging del consenso al rilascio degli attributi nell'audit log
  - Chiedi sempre
  - Chiedi se cambiano le informazioni
  - Non chiedere più

Consent

- Visualizzazione dei Terms of Use (privacy policy) dell'IdP e dell'SP (metadati)
- Visualizzazione della descrizione del servizio e del logo associato se presenti nei metadati

Consent

messages/consent-messages_en.properties
messages/consent-messages_it.properties
messages/consent-messages.properties
-> consent-messages_it.properties

idp.properties:#idp.consent.allowDoNotRemember = true
idp.properties:#idp.consent.allowGlobal = true
idp.properties:#idp.consent.allowPerAttribute = false
idp.properties:#idp.consent.compareValues = false
idp.properties:#idp.consent.storageRecordLifetime = P1Y

Consent

Loghi e descrizioni rendono piacevole e scorrevole e confidente l’esperienza utente.

Lato IdP valorizzare sempre:

- negli attributi Friendly name e Description internazionalizzati
- nei metadati mdui:logo con url HTTPS stando attenti alle dimensioni

Ulteriori Sorgenti Filtri

Nel file services.xml:

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

Poi bisogna riavviare l’IdP.

Reloadable Services

curl -sk https://localhost/idp/profile/admin/reload-service?id=shibboleth.Attribute**Filter**Service | html2text

Esercizio

- Nel file attribute-filter.xml configurare
  - 1 filtro che permetta tutti i valori
  - 1 filtro che permetta alcuni valori
  - 1 filtro che escluda l'attributo
  - 1 filtro che escluda alcuni valori
- Ordinare alfabeticamente gli attributi presentati da consent in intercept/consent-intercept-config.xml
- Aggiungengere un file come risorsa filtro nell'IdP
- Riavviare Shibboleth

Licenza d’uso

I loghi Garr e Idem sono dei rispettivi proprietari.
Per tutti gli altri contenuti...

Quest'opera è stata rilasciata sotto la licenza Creative Commons Attribuzione-Condividi allo stesso modo 2.5.Per leggere una copia della licenza visita il sito web http://creativecommons.org/licenses/publicdomain/ o spedisci una lettera a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Sorgenti Filtri – Sperimentale

Nel file services.xml:

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

<bean id="FileBacked_RR_Garr_ARP"
class="net.shibboleth.ext.spring.resource.FileBackedHTTPResource"
            c:client-ref="shibboleth.FileCachingHttpClient"
c:url="https://registry.idem.garr.it/rr3/arp/format3exp/aHR0cHM6Ly9pZGVtZmVy
by51bml0cy5pdC9pZHAvc2hpYmJvbGV0aA~~/arp.xml"
                        c:backingFile="%{idp.home}/conf/cache/RrgarrARP.xml"/>
```

Nel file services.properties:

```
idp.service.attribute.filter.checkInterval = PT15M
```