Openspace pass 1 rum 1

Shibboleth for dummies

Börja med idp-installeraren, den ger en bra grund att stå på.

Bygga attribut
Alla attribut byggs i attribute-resolver.xml.
Finns inte attributet du vill släppa får du bygga det.
Idp-installeraren lägger in alla standardattribut från ldapscheman inetOrgPerson, eduPerson och norEduPerson.
Resolver för ett enkelt attribut ser ut så här:

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

    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
        friendlyName="eduPersonEntitlement" />
</resolver:AttributeDefinition>
```

För att bygga specialattribut som behövs för t.ex. Nya så skall det se ut ungefär så här om du har de entitlementen bland alla andra.
Ska man bara släppa en delmängd av värdena som finns i data källan så kan man antingen bygga en script-resolver eller lägga in en regel i attributfiltret.
Tänk på att syntax skiljer sig en del mellan java7 och java8. Detta exempel är baserat på java7.

```
<resolver:AttributeDefinition  xsi:type="Script"
        xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        id="nyaEduPersonEntitlement"
        sourceAttributeID="eduPersonEntitlement">
    <resolver:Dependency ref="myLDAP" />
    <resolver:AttributeEncoder xsi:type="enc:SAML1String" name="urn:mace:dir:attribute-def:
eduPersonEntitlement" />

    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
        friendlyName="eduPersonEntitlement" />
    <Script>
        <![CDATA[
            importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);

            nyaEduPersonEntitlement = new BasicAttribute("nyaEduPersonEntitlement");

            if (typeof eduPersonEntitlement != "undefined" && eduPersonEntitlement != null ) {
                for ( i = 0; eduPersonEntitlement != null && i < eduPersonEntitlement.getValues().size(); i++ )
{
                    if (eduPersonEntitlement.getValues().get(i).indexOf("urn:mace:swami.se:gmai:nya-dw") === 0)
{
                        nyaEduPersonEntitlement.getValues().add(eduPersonEntitlement.getValues().get(i));
                    }
                }
            }
        ]]>
    </Script>
</resolver:AttributeDefinition>
```

Släppa attribut
Regler för att släppa attribut till andra entiteter definieras i attribute-filter.xml.
För att släppa alla attribubtvärden som kommer från datakällan, bygg attributet vid behov:

```
<AttributeFilterPolicy id="afp-nya-sp">
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://expert.antagning.se/ecs-sp"
/>
    <AttributeRule attributeID="cn">
      <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="nyaEduPersonEntitlement">
      <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
</AttributeFilterPolicy>
```

För att släppa en delmängd:

```
<AttributeFilterPolicy id="afp-nya-sp">
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://expert.antagning.se/ecs-sp"
/>
    <AttributeRule attributeID="cn">
      <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="eduPersonEntitlement">
      <PermitValueRule xsi:type="basic:AND">
        <basic:Rule xsi:type="basic:AttributeValueRegex" regex="^urn:mace:swami.se:gmai:nya-dw:.*" />
        <basic:Rule xsi:type="basic:NOT">
          <basic:Rule xsi:type="basic:AttributeValueString" value="urn:mace:swami.se:gmai:nya-dw:roleadmin" />
        </basic:Rule>
      </PermitValueRule>
    </AttributeRule>
</AttributeFilterPolicy>
```

Lägga in andra entiteter
Metadata för andra entiteter läggs in i metadata-providers.xml.
Idp-installeraren lägger till flödet swamid-2.0.xml som innehåller alla SWAMIDs produktions entiteter samt eduGAIN.

Ett block för metadata som finns åtkomligt via http(s) ser ut så här, detta exemper har med taggen RetainedRole för att endast ladda metadata för SPs.

```
<MetadataProvider id="URLMD" xsi:type="FileBackedHTTPMetadataProvider" xmlns="urn:mace:shibboleth:2.0:metadata"
                metadataURL="METADATAURL"
                backingFile="/opt/shibboleth-idp/metadata/METADATAFIL.xml">
        <MetadataFilter xsi:type="EntityRoleWhiteList">
                <RetainedRole>md:SPSSODescriptor</RetainedRole>
        </MetadataFilter>
</MetadataProvider>
```

För statisk metadata som bara finns i fil så ser det ut så här:

```
    <MetadataProvider id="LocalMetadata"  xsi:type="FilesystemMetadataProvider" metadataFile="
PATH_TO_YOUR_METADATA"/>
```

Common practice

- Köra XMLint för at verifiera config.
- Rekomendation är att IDP:n bör ha minst 1Gb minne.

Attribute resolver / släppa attribut till vald SP

Kod-exempel från Simon

[…]

```
  <AttributeFilterPolicy id="afp-nya-sp">
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://expert.antagning.se/ecs-sp"/>
    <AttributeRule attributeID="cn">
      <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
      <PermitValueRule xsi:type="basic:ANY"/>
    </AttributeRule>
    <AttributeRule attributeID="eduPersonEntitlement">
      <PermitValueRule xsi:type="basic:AND">
        <basic:Rule xsi:type="basic:AttributeValueRegex" regex="^urn:mace:swami.se:gmai:nya-dw:.*" />
        <basic:Rule xsi:type="basic:NOT">
          <basic:Rule xsi:type="basic:AttributeValueString" value="urn:mace:swami.se:gmai:nya-dw:roleadmin" />
    </basic:Rule>
   </PermitValueRule>
  </AttributeRule>
 </AttributeFilterPolicy>
```

[…]

SWAMID rekomenderar att använda entitets-kategorier för att släppa attribut. Då slipper man specialbehandla varje SP.

Entity Categories

Metadata filen som kommer när man sätter upp en SP.

Vad skall/behöver ändras ?

Anders: Så lite som möjligt, Skicka in det som spottas ur med nedanstående ändringar.

- mdui:DisplayName
- mdui:Description
- mm bör läggas till.