Shibboleth IdP3.x Workshop

Programm:

Do,16.06.2016
14:00 bis 19:00 Uhr: Implementierungssprint (die Fortgeschrittenen helfen den Anfängern)
19:00 Uhr : Abendessen

Fr, 17.06.2016
09:00 bis 13:00 Uhr:
Migrationsstrategien
Einführung in Spring Web Flow
Intercept Flows (Pre- und Post-Authentication Intercept Flows)
Authentifizierung - Funktionsweise und Konfigurationsmöglichkeiten
Implementierung eigener Authentifizierungsverfahren
2-Faktor-Authentifizierung
13:00 bis 14:00 Uhr: Mittagessen
14:00 bis 18:00 Uhr:
Einführung in Apache Velocity
Anpassung der Webseiten inkl. Lokalisierung
Clustering - Konfigurationsmöglichkeiten
Implementierungen eigener Datenconnectoren

Raum für Notizen, Konfigurationsschnipsel, nützliche URLs u.a.m.

Online-Doku: https://wiki.aai.dfn.de/de:shibidp3

https://shibboleth.net/downloads/identity-provider/3.2.0/shibboleth-identity-provider-3.2.0.zip

https://wiki.aai.dfn.de/de:shibidp3prepare#shibboleth_identity_provider

Installation (https://wiki.aai.dfn.de/de:shibidp3install):

Passwort immer: shibboleth

Hostname: idp.local

Scope: local

Bugfix für Version 3.2.0: https://wiki.aai.dfn.de/de:shibidp3troubleshoot

Konfiguration (https://wiki.aai.dfn.de/de:shibidp3config):

Logging unter Ubuntu (systemd):
journalctl -u tomcat8
"tail -f" ersatz:
journalctl -f -u tomcat8
Es gelten jedoch immer noch die Dateien unter /var/log/tomcat8/ (catalina.out, ...)

https://sp1.local/Shibboleth.sso/Metadata

```
 <MetadataProvider id="LocalMetadata"  xsi:type="FilesystemMetadataProvider" metadataFile="/root
/metadata/sp1-metadata.xml"/>



   <MetadataProvider id="Metadata-SP1"  xsi:type="FilesystemMetadataProvider" metadataFile="/root
/metadata/sp1-metadata.xml"/>
  <MetadataProvider id="Metadata-SP2"  xsi:type="FilesystemMetadataProvider" metadataFile="/root
/metadata/sp2-metadata.xml"/>

cp /root/metadata/* /opt/shibboleth-idp/metadata/
chown tomcat8:tomcat8 /opt/shibboleth-idp/metadata/*

vi /opt/shibboleth-idp/conf/metadata-providers.xmls

   <MetadataProvider id="Metadata-SP1"  xsi:type="FilesystemMetadataProvider" metadataFile="%
{idp.home}/metadata/sp1-metadata.xml"/>
  <MetadataProvider id="Metadata-SP2"  xsi:type="FilesystemMetadataProvider" metadataFile="%
{idp.home}/metadata/sp2-metadata.xml"/>


   <MetadataProvider id="HTTPMetadata"
               xsi:type="FileBackedHTTPMetadataProvider"
               backingFile="%{idp.home}/metadata/sp1-metadata.xml"
               metadataURL="https://sp1.local/Shibboleth.sso/Metadata">
   </MetadataProvider>


# vi conf/metadata-providers.xml
...
<MetadataProvider id="LocalMetadata"  xsi:type="FilesystemMetadataProvider" metadataFile="%
{idp.home}/metadata/local-metadata.xml"/>
...
in /metadata/local-metadata.xml alle Metadaten für die lokalen Metadaten eintragen in einem
<EntitiesDescriptor>-Tag geklammert.


Anbindung LDAP: https://wiki.aai.dfn.de/de:shibidp3config#anbindung_idm_ldap_ad

 /home/shibboleth/jxplorer/jxplorer.sh

 Use a Template: "localhost"

# vi conf/ldap.properties
idp.authn.LDAP.authenticator               = bindSearchAuthenticator
idp.authn.LDAP.ldapURL                     = ldap://idp.local:389
idp.authn.LDAP.useStartTLS                 = false
idp.authn.LDAP.baseDN                      = dc=users,dc=nodomain
idp.authn.LDAP.userFilter                  = (uid={user})
idp.authn.LDAP.bindDN                      = cn=admin,dc=nodomain
idp.authn.LDAP.bindDNCredential                = shibboleth
idp.attribute.resolver.LDAP.returnAttributes    = *


Variante mit directAuthenticator:
```

idp.authn.LDAP.authenticator = directAuthenticator
idp.authn.LDAP.dnFormat = uid=%s,dc=users,dc=nodomain

Freigabe der lokalen IPs für Status-Seite (Nur für Workshop-Beispiel):
 # vi conf/access-control.xml

```
<bean parent="shibboleth.IPRangeAccessControl"
p:allowedRanges="#{ {'127.0.0.0/8', '::1/128'} }" />
```

hier: 127.0.0.0/8 eintragen statt 127.0.0.1/32 ---> dann tut: https://idp.local/idp/status

Folgende Fehlermeldung im idp-process.log derzeit einfach ignorieren (funktioniert trotzdem):
2016-06-16 17:40:00,928 - ERROR [org.apache.velocity:96] - ResourceManager : unable to find resource 'status.vm' in any resource loader.

https://wiki.shibboleth.net/confluence/display/IDP30/Troubleshooting

cp attribute-resolver-full.xml attribute-resolver.xml

Zum Thema Attribute Management: https://www.aai.dfn.de/uploads/media/20150624-AAIWS13-04-attribute.pdf

Exkurs zu Reloadable Services:
Konfiguration unter /conf/services.properties

```
<!-- Release eduPersonAffiliation to two specific SPs. -->
<AttributeFilterPolicy id="example2">
  <PolicyRequirementRule xsi:type="OR">
    <Rule xsi:type="Requester" value="https://sp1.local/shibboleth" />
    <Rule xsi:type="Requester" value="https://sp2.local/shibboleth" />
  </PolicyRequirementRule>

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


  <AttributeRule attributeID="surname">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>

  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>

  <AttributeRule attributeID="mail">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>

  <AttributeRule attributeID="uid">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>

</AttributeFilterPolicy>
```

MetadataProvider in /etc/shibboleth/shibboleth2.xml:
<MetadataProvider type="XML" file="/opt/shibboleth-idp/metadata/idp-metadata.xml"/>
/etc/init.d/shibd restart

Fehlermeldung:
Login Failure: Pool is empty and connection creation failed
Tendenziell: Fehler in conf/ldap.properties
idp.authn.LDAP.ldapURL = ldap://localhost:389 <= Portänderung 10389->389 vergessen?

Noch ein Exkurs
User Consent pro Attribut
/conf/idp.properties
idp.consent.allowPerAttribute = true

++++++++++++++++++++++++++ Workshop 2. Tag ++++++++++++++++++++++++++++++++++
----

https://software.zedat.fu-berlin.de/workshop/
wir werden die Unterlagen noch unter den AAI-Webseiten ablegen

wget "https://wiki.shibboleth.net/confluence/download/attachments/21660022/authn-messages_de.properties"
wget "https://wiki.shibboleth.net/confluence/download/attachments/21660022/consent-messages_de.properties"
wget "https://wiki.shibboleth.net/confluence/download/attachments/21660022/error-messages_de.properties"

Sprachumschaltung auf Loginseite:

https://wiki.shibboleth.net/confluence/display/IDP30/Switching+locale+on+the+login+page

```
<mvc:interceptors>
  <bean id="localeChangeInterceptor"
class="org.springframework.web.servlet.i18n.LocaleChangeInterceptor">
    <property name="paramName" value="lang"/>
  </bean>
</mvc:interceptors>
<bean id="localeResolver" class="org.springframework.web.servlet.i18n.SessionLocaleResolver">
  <property name="defaultLocale" value="en"/>
</bean>
```

vi conf/mvc-beans.xml

Messages schneller neuladen für Live-Editierung (nicht für Produktivbetrieb gedacht):

 # vi conf/services.properties

idp.message.resources = shibboleth.MessageSourceResources
idp.message.cacheSeconds = 1

Webflow Debugging aktivieren:
 # vi conf/logback.xml

```
66a67,68
>     <!-- log spring workflow stuff -->
>     <logger name="org.springframework.webflow" level="{idp.loglevel.webflow:-DEBUG}" />
161c163
<     <root level="${idp.loglevel.root:-INFO}">
---
>     <root level="${idp.loglevel.root:-DEBUG}">
```

```
<logger name="org.springframework.webflow" level="DEBUG" />
```

```
<button type="submit" name="_eventId_authn/External">Mein Verfahre</button>
```

SPENGO / Kerberos-Ticket-Login

Doku:
https://wiki.shibboleth.net/confluence/display/IDP30/SPNEGOAuthnConfiguration

/views/login.vm
anpassen, siehe Minimal-Beispiel im Shib Wiki

/conf/idp.properties
idp.authn.flows= SPNEGO|Password

/conf/authn/spnego-authn-config.xml

```
<!--nach den lokalen Gegebenheiten (Realm, keytab)-->
<util:list id="shibboleth.authn.SPNEGO.Krb5.Realms">
   <bean parent="shibboleth.KerberosRealmSettings"
      p:servicePrincipal="HTTP/idp.example.org@EXAMPLE.ORG"
      p:keytab="/etc/apache2/apache-krb5.keytab" />
</util:list>
```

/conf/authn/general-authn.xml

```
<!--i.d.R. keine Anpassung notwendig (ab IdP 3.2.0)-->
```

Login über Kerberos Credentials, nicht LDAP/AD:

/conf/authn/password-authn-config.xml

```
<import resource="krb5-authn-config.xml" />
<!--(NB: immer nur ein import Statement)-->

<util:list id="shibboleth.authn.Password.Transforms">
  <bean parent="shibboleth.Pair" p:first="^(.+)@EXAMPLE\.ORG$" p:second="$1" />
</util:list>

<!-- wahlweise Username+Password oder Kerberos -->

 <bean id="shibboleth.authn.Password.ExtendedFlows" class="java.lang.String" c:_0="SPNEGO" />
```

```
    <util:list id="shibboleth.authn.Password.ExtendedFlowParameters">
      <value>_shib_idp_SPNEGO_enable_autologin</value>
    </util:list>
```

/conf/authn/krb5-authn-config.xml

```
  <bean id="shibboleth.authn.Krb5.ServicePrincipal" class="java.lang.String"
c:_0="HTTP/idp.example.org@EXAMPLE.ORG" />
  <bean id="shibboleth.authn.Krb5.Keytab" class="java.lang.String" c:_0="/etc/apache2/apache-
krb5.keytab" />

  <alias name="ValidateUsernamePasswordAgainstKerberos" alias="ValidateUsernamePassword"/>
```

/conf/c14n/simple-subject-c14n-config.xml

```
    <!-- Apply any regular expression replacement pairs after authentication. -->
    <util:list id="shibboleth.c14n.simple.Transforms">
      <bean parent="shibboleth.Pair" p:first="^(.+)@EXAMPLE\.ORG$" p:second="$1" />
    </util:list>
```

HIER BITTE LINK FüR SHIBBOLETH + OPENID. Danke :)
https://github.com/uchicago/shibboleth-oidc
Infos zu OpenID Connect: http://openid.net/connect/
sowie https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt63/BT63_AAI_OpenIDConnect_Pempe.pdf

vi conf/intercept/context-check-intercept-config.xml

```
  <!-- IDP3  guest chck -->
   <bean id="shibboleth.context-check.Condition" parent="shibboleth.Conditions.OR">
   <constructor-arg>
      <list>
         <bean parent="shibboleth.Conditions.NOT">
            <constructor-arg>
               <list>
Plain text
                  <bean class="net.shibboleth.idp.profile.logic.SimpleAttributePredicate">
                     <property name="attributeValueMap">
                        <map>
                           <entry key="isIdentified">
                              <list>
                                 <value>false</value>
                              </list>
                           </entry>
                        </map>
                     </property>
                  </bean>
               </list>
            </constructor-arg>
         </bean>
```

```
        <bean parent="shibboleth.Conditions.AND">
          <constructor-arg>
            <list>
              <bean class="net.shibboleth.idp.profile.logic.SimpleAttributePredicate">
                <property name="attributeValueMap">
                  <map>
                    <entry key="isIdentified">
                      <list>
                        <value>false</value>
                      </list>
                    </entry>
                  </map>
                </property>
              </bean>

              <bean parent="shibboleth.Conditions.RelyingPartyId">
                <constructor-arg>
                  <list>
                    <value>https://sp1.example.edu/shibboleth</value>
                    <value>https://sp2.example.edu/shibboleth</value>
                    <value>https://sp3.example.edu/shibboleth</value>
                  </list>
                </constructor-arg>
              </bean>
            </list>
          </constructor-arg>
        </bean>
      </list>
    </constructor-arg>
</bean>
```

vi relaying-party.xm

```
<beanid="shibboleth.DefaultRelyingParty"parent="RelyingParty">
<propertyname="profileConfigurations">
<list>
<beanparent="Shibboleth.SSO"p:postAuthenticationFlows="#{{'attribute-release', 'context-check'}}"/>
’’’’
```

Properties auslagern

```
<bean parent="shibboleth.Conditions.RelyingPartyId">
<constructor-argname="candidates">
<beanparent="shibboleth.CommaDelimStringArray"c:_0="#{ '%{idp.local.services}'.trim() }"/>
</constructor-arg>
</bean>
```

mit

idp.local.services= https://sp1.example.org, https://sp2.example.org