Shibboleth

Installation eines Service Providers (Shibboleth 3)

Stand: 13.05.2019

Schritt1) Installation der erforderlichen Pakete

Vorrausetzung für die Installation von Shibboleth sind die folgenden Pakete:

- unixODBC
- libmemcached

Um Shibboleth zu installieren in den Repositories */etc/yum.repos.de/rehl.source.repo* shibboleth-security eintragen.

```
[shibboleth]
name=Shibboleth (CentOS_7)
# Please report any problems to https://issues.shibboleth.net
type=rpm-md
mirrorlist=https://shibboleth.net/cgi-bin/mirrorlist.cgi/CentOS_7
gpgcheck=1
gpgkey=https://shibboleth.net/downloads/service-provider/RPMS/repomd.xml.key
enabled=1
```

Danach kann Shibboleth mit *#yum install shibboleth* installiert werden. Es wird ein Ordner mit den Konfigurationsdateien unter /etc/shibboleth angelegt.

Schritt 2) Konfiguration der Shibboleth2.xml

Passen Sie die Shibboleth2.xml an Ihren Server an und kopieren Sie den Serverschlüssel und das Zertifikat in den Shibboleth-Ordner.

```
<SPConfig xmlns="urn:mace:shibboleth:3.0:native:sp:config"
    xmlns:conf="urn:mace:shibboleth:3.0:native:sp:config"
    clockSkew="180">
    <OutOfProcess
tranLogFormat="%u|%s|%IDP|%i|%ac|%t|%attr|%n|%b|%E|%S|%SS|%L|%UA|%a" />

<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
    <ApplicationDefaults entityID=https://meinservice.hs-harz.de    REMOTE_USER="uid"
cipherSuites="DEFAULT:!EXP:!LOW:!aNULL:!eNULL:!DES:!IDEA:!SEED:!RC4:!3DES:!kRSA:!SSLv2:!S
SLv3:!TLSv1:!TLSv1.1">
```

```
<Sessions lifetime="28800" timeout="36000" relayState="ss:mem"
          checkAddress="false" handlerSSL="true" cookieProps="https">
  <SSO entityID="https://idp.hs-harz.de/shibboleth">          SAML2          </SSO>

  <!-- SAML and local-only logout. -->          <Logout>SAML2 Local</Logout>
  <!-- Administrative logout. -->
  <LogoutInitiator type="Admin" Location="/Logout/Admin" acl="127.0.0.1 ::1" />
     <!-- Extension service that generates "approximate" metadata based on SP configuration. -->
  <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
   <!-- Status reporting service. -->
  <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
  <!-- Session diagnostic service. -->
  <Handler type="Session" Location="/Session" showAttributeValues="false"/>
  <!-- JSON feed of discovery information. -->
   <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>
</Sessions>

 <Errors supportContact=mail@hs-harz.de   helpLocation="/about.html"
      styleSheet="/shibboleth-sp/main.css"/>


<!--Metadaten vom Server holen-->
<MetadataProvider type="XML" maxRefreshDelay="7200"
backingFilePath="/etc/shibboleth/harz-metadata.xml" url="http://idp.hs-harz.de/harz-
metadata.xml"/>
<!-- oder lokale Datei-->
        <MetadataProvider type="XML" file="harz-metadata.xml"/>

  <!-- Simple file-based resolvers for separate signing/encryption keys. -->
  <CredentialResolver type="File" use="signing"
          key="/path to key" certificate=" path to Zertifikat "/>
  <CredentialResolver type="File" use="encryption"
      key=" path to key " certificate="path to Zertifikat“/>
</ApplicationDefaults>
...
</SPConfig>
```

Quelltext 1: Beispiel einer Shibboleth2.xml

Attribute können in der attribute-map.xml angepasst werden. Beispiel einer angepassten attribute-map.xml für das Attribut uid. Die Attribute die übergeben werden sollen müssen mit der IDP Konfiguration abgestimmt sein.

```
<!--Examples of LDAP-based attributes, uncomment to use these... -->
  <Attribute name="urn:mace:dir:attribute-def:uid" id="uid"/>
   <Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="uid"/>
```

Quelltext 2: Beispieleintrag der UID in der attribute-map.xml

Schritt 3) Metadaten ändern

Melden Sie sich im Rechenzentrum zum Anpassen der Metadaten der HS-Harz-Föderation. Für die Änderungen werden der EntityName, das Zertifikat des Servers und die Attribute, die Sie im Service Provider verarbeiten möchten, benötigt. Die aktualisierte Metadaten-Datei wird eingebunden und kann danach geladen werden.

Schritt 4) Konfiguration des Apache

Danach laden Sie in Ihre Apachekonfiguration das Shibboleth-Modul und richten die Autorisierung ein. Die Autorisierungsklausel kann in der Konfigurationdatei stehen, kann aber auch per .htaccess realisiert werden.

```
# Load the Shibboleth module.
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so <IfModule mod_alias.c>
…
```

```
#Beispiel1: einfachste Form der Autorisierung per Shibboleth
AuthType shibboleth
ShibRequireSession On
require shibboleth
```

```
#Beispiel2: Autorisierung von Nutzern
AuthType shibboleth
ShibRedirectToSSL 443
ShibRequestSetting requireSession 1
#Autorisierung anhand der Nutzernummer
require user m1111 m2222 m3333
```

Quelltext 3: Beispiel der Apachekonfiguration

Schritt 5) Starten des Shib-Daemon

Starten Sie nun den Shib-Daemon mit *#service shibd start* und dann den Apache Daemon.