Shibboleth

Installation des Shibboleth Service Providers

Die Installation erfolgte auf einer Sunfire X4200 unter CentOS 7.1.

Shibboleth Repository installieren:

```
curl -o /etc/yum.repos.d/security:shibboleth.repo
http://download.opensuse.org/repositories/security://shibboleth/CentOS_7/securit
y:shibboleth.repo
yum install shibboleth
```

Apache Konfiguration

in httpd.conf werden folgende Variablen gesetzt:

```
UseCanonicalName On
ServerName ulblin07.thulb.uni-jena.de
```

Um SSL zu erzwingen, wird alles auf den ssl Port umgeleitet:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

Für den Server müssen Zertifikate installiert werden.

Der SP kann jetzt gestartet werden:

```
systemctl start shibd
```

Das Logfile ist `/var/log/shibboleth/shibd.log`

Über die Statusseite kann geprüft werden, ob der SP am Leben ist:

```
curl -k https://127.0.0.1/Shibboleth.sso/Status
```

Die Statusseite ist normalerweise auf den localhost beschränkt, aber es können weitere Adressen konfiguriert werden, um die Statusseite auch über einen entfernten Browser testen zu können.
Shibbloeth Status Page in /etc/shibboleth/shibboleth2.xml einschränken:

```
<!-- Status reporting service. -->
            <Handler type="Status" Location="/Status" \
acl="127.0.0.1 ::1 [weitere Adressen]"/>
```

Die Statusseite konnte zunächst nicht erreicht werden, weil der Apache nicht auf den Shibboleth Socket zugreifen konnte. In /var/log/audi/audit.log:

```
type=AVC msg=audit(1434979353.414:1915285): avc:  denied  { connectto } for
pid=17526 comm="httpd" path="/run/shibboleth/shibd.sock"
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:system_r:initrc_t:s0
tclass=unix_stream_socket
type=SYSCALL msg=audit(1434979353.414:1915285): arch=c000003e syscall=42
success=no exit=-13 a0=11 a1=7fff7e8a1830 a2=6e a3=3 items=0 ppid=17525
pid=17526 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48
fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd"
subj=system_u:system_r:httpd_t:s0 key=(null)
```

Es musste eine eigene SELinux Policy erstellt werden. Das audit2allow musste dafür zwei mal ausgeführt werden:

```
grep httpd /var/log/audit/audit.log|audit2allow -M  shibsp
semodule -i shisp.pp
grep httpd /var/log/audit/audit.log|audit2allow -M  shibsp1
semodule -i shisp.pp

semodule -l|grep shib
shibsp  1.0
shibsp1 1.0
```

Konfiguration SP

Shibboleth Files und Directories

`/etc/shibboleth` - Hauptseite Konfiguration
`/usr/sbin/shibd` - Shibboleth Daemon
`/var/log/shibboleth` - Logfiles
`/etc/httpd/conf.d/shib.conf` - Shibboleth SP specifische Apache Konfiguration

Punkt 1 ist die Vergabe einer SAML `entityID`. Das ist die ID, über die der SP in der Föderation registriert wird. Das kann eine beliebige ID sein, die Hauptsache eindeutig.

```
<ApplicationDefaults entityID="https://dbttest.thulb.uni-jena.de/shibboleth" \
   REMOTE_USER="eppn persistent-id targeted-id">
```

Der SP muss zu secure Cookies gezwungen werden:

```
 <Sessions lifetime="28800" timeout="3600" relayState="ss:mem" \
   handlerSSL="true"  cookieProps="; path=/; secure; HttpOnly">
```

Letzteres erzwingt, dass Cookies vom SP ausschließlich über eine SSL Verbindung gesendet werden

Die URL zu den Metadaten der Föderation und der Pfad zu dfn-aai.pem (PKI Trust Anchor um die Metadaten verifizieren zu können) muss im MetadataProvider Block definiert werden:
rights

```
 <MetadataProvider type="Chaining">
   <MetadataProvider type="XML"
uri="https://www.aai.dfn.de/fileadmin/metadata/DFN-AAI-Test-metadata.xml" \
   backingFilePath="DFN-AAI-Test-metadata.xml" reloadInterval="7200"
   <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
   <MetadataFilter type="Signature" Certificate="/etc/shibboleth/dfn-aai.pem"/>
 </MetadataProvider>
 </MetadataProvider>
```

Das DFN-AAI-Zertifikat muss natürlich noch heruntergeladen werden:

```
cd /etc/shibboleth
wget --no-check-certificate \
```

```
   https://www.aai.dfn.de/fileadmin/metadata/dfn-aai.pem
```

Die Pfade zum SSL-Key und zum Zertifikat im werden im Block CredentialResolver eingetragen:

```
 <CredentialResolver type="File" key="dbttest.thulb.uni-jena.de_key.pem" \
                certificate="cert-6868828640220023.pem"/>
```

Das ist das gleiche Paar, was im Apache ssl.conf steht, also vom DFN signiert.

Um für die Anwendung das Einloggen von verschiedene Einrichtungen zu ermöglichen, d.h. unterschiedliche Identity Provider anbieten zu können kann ein Discovery Service genutzt werden. Der DFN bietet einen Discovery Service jeweils für die Test und für die Produktions Umgebung an. Nachteil ist, dass bei der Institutionsauswahl alle an der Test- bzw. Produktionsföderation teilnehmenden Einrichtungen zur Auswahl angeboten werden. Möglich ist auch ein Embedded Discovery Service, installiert auf dem eigenen Server, der nur die relevanten Einrichtungen anbietet.
Für die Test DBT nutzen wir den DS der DFN AAI Testföderation:

```
<SSO discoveryProtocol="SAMLDS" \
   discoveryURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf">
   SAML2
</SSO>
```

Shibboleth Konfiguration im Apache

Die Konfiguration erfolgt in /etc/httpd/conf.d/shib.conf (File aus …)

```
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so
ShibCompatValidUser Off
<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>

<IfModule mod_alias.c>
  <Location /shibboleth-sp>
    AuthType None
    Require all granted
  </Location>
  Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
</IfModule>

<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require shib-session
</Location>
```

Die Location Shibboleth.sso kann mit folgenden Parametern aufgerufen werden.

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Metadata
      zeigt die Metadaten

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Session

Angaben zur Session, wenn eine besteht, ansonsten „A valid sessuion was not found“

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Login

Wenn richtig konfiguriert das Login, in unserem Fall die Loginseite des DFN-AAI-Test Discovery Service'

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Logout

Damit loggt man sich aus.

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/DiscoFeed

Die IDPs vom Discovery Service

Die Location /secure erfordert eine Session, der Nutzer wird aufgefordert sich einzuloggen, es erscheint der Login Bildschirm des DFN-AAI-Test DS.

Im /etc/httpd/conf.d/ssl.conf muss noch das Zertifikatspaar und das Chainfile eingetragen werden.

Funktionstest

https://dbttest.thulb.uni-jena.de/secure

→ sollte auf die Seite von DFN-AAI-Test umgeleitet werden, wenn der Server beim DFN AAI registriert ist.

`https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Status`

→ Statusseite funktioniert

`https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Session`

→ A valid session was not found. OK

https://dbttest.thulb.uni-jena.de/Shibboleth.sso/Metadata

→ Funktioniert

tomcat-mir Integration

In ssl.conf die ajp Konfiguration eintragen:

```
ProxyPass /mir ajp://localhost:18322/mir
ProxyPassReverse /mir ajp://localhost:18322/mir
Header always set Strict-Transport-Security "max-age=31556926"
<IfModule mod_proxy.c>
        LogLevel Debug
</IfModule>
<Location /mir/servlets/MCRShibbolethLoginServlet>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require valid-user
</Location>
```

in /etc/httpd/conf.modules.d/00-proxy.conf:

```
ProxyIOBufferSize 65536
```

/mcr/dbt/tomcat-dbtmir/conf/server.xml:

```
<!-- Define an AJP 1.3 Connector on port 8009 →
    <Connector port="18322" protocol="AJP/1.3"
               tomcatAuthentication="false"
               connectionTimeout="20000"
               packetSize="65536"
               URIEncoding="utf-8"
               redirectPort="8443" scheme="https" />
```

Der Eintrag tomcatAuthentication="false" ist notwendig, um die native Webserver Authentication zu nutzen.
Damit die Shibboleth Attribute vom Apache an den Tomcat weitergereicht werden können, müssen diese in Environmetvariablen mit dem Prefix „AJP_“ stehen.
In /etc/shibboleth/shibboleth2.xml muss folgendes ergänzt werden:

```
<ApplicationDefaults entityID="https://dbttest.thulb.uni-jena.de/shibboleth"
                     REMOTE_USER="eppn persistent-id targeted-id"
                     signing="false" encryption="false
                     attributePrefix="AJP_">
```

In /etc/shibboleth/attribute-map.xml stehen die Attribute, die wir vom IDP wollen und bekommen:

```
eduPersonPrincipalName
eduPersonAffiliation
displayName
mail
```

Folgende 2 Attribute liefern die IDPs in der Föderation generell aus:

```
eduPersonScopedAffiliation
eduPersonEntitlement
```