Shibboleth Service Provider SP

Az alábbi lapon megkíséreljük összefoglalni a legfontosabb lépéseket, melyek általános esetben elegendőek ahhoz, hogy működő Shibboleth SP-t állítsunk üzembe. Fontos, hogy rengeteg olyan igény lehet, amely további speciális beállítások meglétét teszik szükségessé, ezeket ezen a lapon nem részletezzük, ilyen irányú tájékozódáshoz legbiztosabb forrás a http://wiki.shibboleth.net lap.

Telepítés

El?készületek

A Shibboleth SP egy webszerver modul, így szükséges előfeltétel, hogy a gépünkön legyen egy webszerver telepítve, jelenleg Apache és IIS a biztosan támogatott webszerverek. Emellett szükséges, hogy a 443-as port a tűzfalon mindkét irányban engedélyezett legyen, ill. a hosztnév, amelyen a webszerver üzemel, be legyen jegyezve a DNS-be.

Letöltés és telepítés

A legfrissebb változat letölthető https://wiki.shibboleth.net/confluence/display/SP3 címről. Célszerű valamilyen előre csomagolt változattal dolgozni, melyet az adott rendszer csomagkezelőjén keresztül egy mozdulattal feltelepíthetünk minden függőségével együtt.

- Az alábbi parancs a Shibboleth webszerver modul függőségeit is telepíti. Előfordulhat, hogy a telepítés engedélyezni kell a modult és újraindítani az Apache webszervert.

Debian 9 “Stretch” / Ubuntu 16.04 LTS (Xenial)

```
sudo apt install apache2 libapache2-mod-shib2
```

Debian 8 “Stretch” / Ubuntu 14.04 LTS (Trusty)

```
sudo apt-get install apache2 libapache2-mod-shib2
```

Debian 6 “Squeeze” / Debian 7 “Wheezy” / Ubuntu 12.04 LTS (Precise)

Debian 6, Debian 7 és Ubuntu 12.04 rendszerek támogatása lejárt, így a Shibboleth csomag telepítését sem ajánljuk ezekre a rendszerekre!

A Debian Shibboleth csapat által készített új verziók időről időre bekerülnek backports.org tárolóiba is, ezért stable Debiant futtató rendszereken javasolt ezt használni.

A backports.org tárolójának beállításához adjuk hozzá a `/etc/apt/sources.list` fájlhoz a következő sort:

```
deb http://backports.debian.org/debian-backports squeeze-backports main
```

A csomagokat így telepíthetjük:

```
sudo aptitude update
sudo aptitude install -t squeeze-backports libapache2-mod-shib2
```

Ez a Shibboleth webszerver modul függőségeit is telepíti. A Shibboleth használatba vételéhez engedélyezni kell a modult és újra kell indítani az Apache webszervert.

Red Hat / CentOS (RPM) alapú disztribúciók

Shibboleth SP-ből RHEL/CENTOS rendszerekre egyből rendelkezésünkre áll bináris csomag, a fejlesztők ezen platformokon dolgoznak első körben. A telepítés előtt a teendőnk mindössze annyi, hogy a YUM forrásokhoz hozzá kell adni a Shibboleth SP repóját. Ehhez látogassunk el a http://download.opensuse.org/repositories/security://shibboleth/ oldalra, majd a pontos verzió kiválasztása után a security:shibboleth.repo fájl tartalmát másoljuk be a /etc/yum/`/etc/yum.repos.d/CentOS-Base.repo` fájl aljára, majd

```
yum install shibboleth
```

Hibaelhárítás: Can't connect to listener process

Ha a fenti hibába futunk bele, az azt jelenti, hogy a SE linux nem engedi kommunikálni a shibd és a httpd folyamatokat, ezért ezt külön engedélyezni kell. Ehhez készítsünk egy fájlt `shibd.te` néven, melynek tartalma az alábbi legyen:

```
module shibd 1.0;
require {
	type var_run_t;
	type httpd_t;
	type initrc_t;
	class sock_file write;
	class unix_stream_socket connectto;
}
####### # httpd_t ######=
allow httpd_t initrc_t:unix_stream_socket connectto;
```

```
allow httpd_t var_run_t:sock_file write;
```

Ezek után futtassuk le az alábbi parancsokat, melyek a fenti fájlt megfelelően lefordítják, és be is illesztik a létrehozott szabályunkat.

```
# checkmodule -M -m -o shibd.mod shibd.te
checkmodule:  loading policy configuration from shibd.te
checkmodule:  policy configuration loaded
checkmodule:  writing binary representation (version 6) to shibd.mod
# semodule_package -o shibd.pp -m shibd.mod
# semodule -i ./shibd.pp
```

Alapbeállítások

A telepített Shibboleth SP konfigurációs állományait Linux alatt a /etc/shibboleth könyvtárban találjuk. Itt a `shibboleth2.xml` és az `attribute-map.xml` fájlokkal lesz dolgunk.

`shibboleth2.xml`

A telepítéskor alapértelmezetten érkező fájl nagyrészt megfelelő számunkra, az induláshoz csak az alább részletezett módosításokat kell megejtenünk. A változtatandó kódrészletek mind szerepelnek már az eredeti xml-ben is, így a feladat többnyire csak változtatásról, átírásról, bizonyos részek kommentjelek közül történő kiszabadításáról szól.

- Választanunk kell egy entityID-t. Ez általában a védendő szolgáltatást futtató hosztnévből származik: `https://hosztnev/shibboleth`, ezt az azonosítót beírni az `ApplicationDefaults` részbe az alábbi módon (az entityID és a homeURL értékein kívül, ahová a hosztnév írandó be, alapértelmezés szerint mást nem szükséges változtatni):

  ```
  <ApplicationDefaults entityID="https://hosztnév/shibboleth"
                       homeURL="https://hosztnév/shib-error.html"
                       signing="false" encryption="false"
                       id="default" policyId="default"
                       REMOTE_USER="eppn persistent-id targeted-id">
  ```

- Meg kell adni, hogy egy Discovery Service-n keresztül kérjük meg a felhasználót, hogy adja meg, mely IdP-től érkezik, avagy csak IdP-t engedélyezünk számukra. Az első eset nyilvános szolgáltatások esetében indokolt, a második belső, pl. csak intézményi oldalak védésénél szükséges.
  - Discovery Service beállítása

```
<SSO discoveryProtocol="SAMLDS" discoveryURL="https://discovery.eduid.hu">
SAML2 SAML1
</SSO>
```

- Fix IdP beállítása

```
<SSO entityID="https://idp.example.org/idp/shibboleth">
SAML2 SAML1
</SSO>
```

- Meg kell adnunk, hogy milyen metadata forrásból dolgozzon az SP, az alábbi példában az eduID-ban használatos beállítás látható (a hivatkozott href-metadata-signer-2011.crt fájl a http://metadata.eduid.hu címről töltendő le a shibboleth konfigurációs könyvtárába) :

```
<MetadataProvider type="XML" uri="http://metadata.eduid.hu/current/href.xml"
    backingFilePath="href.xml" reloadInterval="7200">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
</MetadataProvider>
```

- Meg kell adni, hogy az SP mely kulcsot és tanúsítványt használja. Ehhez egy self-signed tanúsítványra lesz szükség, amely pl. az alábbi paranccsal generálható:

```
  openssl req -new -newkey rsa:2048 -x509 -days 3652 -nodes -out sp.example.org.crt -
keyout sp.example.org.key
```

  Az xml-ben módosítandó részlet pedig:

```
  <CredentialResolver type="File" key="sp.example.org.key"
certificate="sp.example.org.crt"/>
```

- Végül ugorjunk vissza a fájl első felére, szedjük ki a kommentjeleket a `RequestMapper` rész körül, adjuk meg a kezelendő hosztokat és path-okat. Egy Shibboleth SP példány több, az adott webszerver által kezelt hosztot is kezelni tud, és egy-egy hoszton belül több útvonalat is, ezeket itt meg kell adni. Alább egy példa:

```
<RequestMapper type="Native">
    <RequestMap applicationId="default">
        <Host name="hosztnév" authType="shibboleth" requireSession="false">
                <Path name="secure" authType="shibboleth" requireSession="true" />
        </Host>
    </RequestMap>
</RequestMapper>
```

A péda szerint a hosztnév alatti tartalom nem kíván meg shibbolethes azonosítást, kivéve a `/secure` location. Ha valahol shibbolethes azonosítást kívánunk használni, azt ezen kívül az adott hoszt webszerver konfigjában is jeleznünk kell. Apache-nál az alábbi módon.

```
<Location /secure>
 AuthType shibboleth
 require valid-user
 ShibUseHeaders On
 ShibRequireSession On
</Location>
```

További részletek az authorizációval kapcsolatban:

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPhtaccess

SP adatainak közzététele

A fenti beállítások után egy működő Shibboleth SP-t kapunk eredményül, ugyanakkor ténylegesen csak akkor fog tudni együttműködni a föderációban résztvevő IdP-kkel, ha az SP metaadatait közzétesszük, így azt az IdPk megismerhetik. Ehhez az eduID föderációban a frissen beállított SP adatait a Resource Registry nevű webes adminisztrációs oldalon kell felvinni egy varázsló segítségével, majd a jóváhagyás után várni pár órát, amíg a változások érvénybe lépnek. Ha nincs az intézményi entitások menedzseléséhez jogod ('Access denied'), akkor konzultálj az intézményed eduID kapcsolattartójával, hogy az SP-det szeretnéd a föderációba regisztrálni. Segítséget nyújt az alábbi lista: https://rr.eduid.hu/list

HEXAA integráció

Ha az eduID-ban használatos külső attribútum forrást is szeretnénk az SP-nkhez illeszteni, akkor a shibboleth2.xml fileban a következő példán keresztül lehet megtenni.

```
<AttributeResolver type="Chaining">
   <AttributeResolver type="Query"/>
   <AttributeResolver type="SimpleAggregation" attributeId="eppn"
format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
       <Entity>https://hexaa.eduid.hu/hexaa</Entity>
       <Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="eduPersonEntitlement"/>
```

```
    </AttributeResolver>
</AttributeResolver>
```

Kapcsolódó lapok

- Shibboleth 2 SP telepítése FastCGI alapú webszerver környezetben

---

Változat #1
document-uploader hozta létre 2025-08-07 12:03:17 CEST
document-uploader frissítette 2025-08-07 12:03:17 CEST