Shibboleth v systému DSpace

Vlastimil Krejčíř, krejcir@ics.muni.cz

Ústav výpočetní techniky, Masarykova univerzita, Brno

Shibboleth v praxi, NTK Praha

Shibbolizace DSpace

DSpace jako *service provider*, **Shibboleth** jako *SSO*.

Základní informace

- DSpace verze 1.5.x a vyšší
- Apache HTTP server (2.2.x) + Shibboleth modul

Základní zdroje:

`https://mams.melcoe.mq.edu.au/zope/mams/pubs/Installation/dspace15/view`

`https://www.eduid.cz/wiki/cztestfed/howto/sp2/index`

Ve stable verzi (1.6.2) neumí DSpace Shibboleth nativně (přes knihovny v Javě), ale je nutné použít Apache Server jako SP. DSpace pak používá posílané hlavičky.

V budoucích verzích (?) snad nativní podpora.

Základní přehled nastavení

- instalace SP v rámci Apache HTTP serveru
- napojení Apache na Tomcat (*mod_proxy*, *mod_jk*)
- konfigurace serveru Tomcat
- konfigurace DSpace (`dspace.cfg`)

Instalace SP v Apache

- nainstalovat webový server Apache
- nainstalovat software pro Shibboleth (SP)
- default nastavení SP pro Apache nemá nastaveno posílání některých pro DSpace důležitých atributů, které je nutné odkomentovat v souboru `attribute-map.xml`:
  - `mail`
  - `givenName`
  - `sn`

Apache HTTP server + Tomcat

- DSpace běží na serveru Tomcat (nebo podobném)
- pro Shibboleth v DSpace je NUTNÉ napojit Tomcat na Apache
- DSpace jako virtuální server v Apache (http i https)
  - Apache jako klasická reverzní proxy (`mod_proxy`)
  - využití protokolu AJP 1.3 (`mod_jk`)

Výchozí nastavení

- pro následující ukázky konfigurace předpokládejme, že
  - Tomcat i Apache běží na tomtéž lokálním serveru
  - DSpace běží na serveru Tomcat s adresou 127.0.0.1 (localhost) port 8080
  - hlavní aplikace (např. jspui) je v kořenu (tedy `http://localhost:8080/`) – nastavení např. přes `<Context path="" docBase="jspui" />`

Apache jako klasická proxy

```
<VirtualHost dspace.muni.cz:443>
...
ProxyPass /Shibboleth.sso !
<Location /shibboleth-login>
 AuthType shibboleth
 ShibRequireSession On
 ShibUseHeaders On
 Require valid-user
</Location>
<Location />
 ProxyPass http://127.0.0.1:8080/
 ProxyPassReverse http://127.0.0.1:8080/
</Location>
```

Konfigurace přes protokol AJP

Worker je pojmenovaný `tomcat` (viz dále). V Apache nutné nahrát modul `mod_jk`.

```
<VirtualHost dspace.muni.cz:443>
...
JkMount /* tomcat
JkUnMount /Shibboleth.sso/* tomcat
JkUnMount /shibboleth tomcat
JkUnMount /shibboleth-sp/* tomcat
<Location /shibboleth-login>
 AuthType shibboleth
 ShibRequireSession On
 ShibUseHeaders On
 Require valid-user
</Location>
```

Konfigurace přes protokol AJP II

V souboru `${TOMCAT}/conf/workers.properties` nastavit worker:

```
workers.tomcat_home=/opt/tomcat/
worker.list=tomcat
worker.default.port=8009
worker.default.host=localhost
worker.default.type=ajp13
worker.default.lbfactor=1
```

Konfigurace přes protokol AJP III

V souboru `${TOMCAT}/conf/server.xml` nastavit AJP:

```
<Service name="Catalina">
...
<Connector
 port="8009"
 protocol="AJP/1.3"
 redirectPort="443"
 tomcatAuthentication="false"
 address="127.0.0.1"
 URIEncoding="UTF-8" />
```

DSpace a Shibboleth – co to umí?

- nastavení pořadí autentizačních metod (není nutné použít výlučně jednu)
- načtení mailu (povinné), jméno, příjmení
- autoregistrace
- definování rolí dle affiliation (groups)

Nastavení DSpace

- konfigurační soubor `${DSPACE}/config/dspace.cfg`
- direktivy `authentication.shib.*`

Nastavení pořadí autentizace (Shibboleth a default auth):

```
plugin.sequence.org.dspace.authenticate.AuthenticationMethod =
  org.dspace.authenticate.ShibAuthentication,
  org.dspace.authenticate.PasswordAuthentication
```

Nastavení DSpace II

Nastavení základních atributů předávaných serverem (hlavičky) - dle SP `attribute-map.xml`:

- `authentication.shib.email-header = mail`
- `authentication.shib.firstname-header = givenName`
- `authentication.shib.lastname-header = sn`

Nastavení DSpace III

Další nastavení (použití autentizačního systému Tomcatu, nastavení autoregistrace, nastavení session):

- `authentication.shib.email-use-tomcat-remote-user = false`
- `authentication.shib.autoregister = true`
- `webui.session.invalidate = false`

Nastavení DSpace IV

Nastavení rolí – je možné použít *scoped* i *unscoped affiliation*. *Scoped affiliation* se ořezává (`member@muni.cz` → `member`).

- `authentication.shib.role-header = unscoped-affiliation`
- `authentication.shib.role-header.ignore-scope = false`
  - použijeme-li *scoped affiliation*, pak nastavit na `true`
- `webui.session.invalidate = false`
  - doporučeno vývojáři

Nastavení DSpace V

Nastavení default rolí (selže-li načtení *affiliation*):

- `authentication.shib.default-roles = member`

Přiřazení dle role do skupiny (group):

- `authentication.shib.role.member = MEMBER_MUNI`
- `authentication.shib.role.employee = EMPLOYEE_MUNI`

Problémy

- špatné předávání UTF-8 znaků u atributů `sn` a `givenName`
  - jedná se o bug ve stable verzi 1.6.2 (a menší)
  - hlavičky posílané v ISO-8859-1 nejsou konvertovány
  - nutné pro `fname` a `sname` provést v souboru `ShibAuthentication.java`:

    ```
    new String(prom.getBytes("iso-8859-1"),"utf-8");
    ```
- s doporučeným nastavením nefunguje správné přiřazování skupin dle *affiliation*
  - pravděpodobně bug

Děkuji za pozornost.