OpenSSO

OpenSSO telepítése

Az OpenSSO szerver letölthető a projekt oldaláról. Telepítéshez servlet-api támogató alkalmazásszerver szükséges. (Tomcat-et nem ajánlják a futtatásra, inkább érdemes nagyobb alkalmazásszervereken futtatni, pl. Glassfish vagy Oracle AS)

Az alkalmazásszerver konfigurációjában a Heap size-ot 1G méretűre kell állítani (-Xmx1G), különben a telepítés hibát dob. Valamint érdemes a JVM hotspotot -server módban futtatni. (/path/to/glassfish/domains/domain/config/domain.xml)

Glassfish V2UR1 alatt így zajlik a telepítés:

```
$ /path/to/asadmin deploy --name opensso --contextroot opensso /path/to/opensso.war
```

Ezután webes felületen történik a konfigurálás: meg kell adni az admin felhasználó nevét, jelszavát, a konfigurációs címtár paramétereit (érdemes a beágyazott címtárat használni), a felhasználókat tároló címtár paramétereit (host, port, admin bind paraméterek és DIT gyökér).

Sikeres telepítés esetén a webes felületen állíthatjuk be ízlésünk szerint a kért szolgáltatásokat.

Realm-ek

Az OpenSSO egyszerre képes több szervezetet kiszolgálni, ezeknek a konfigurációját külön-külön 'realm'-ekben kezeli. Minden realmhez megadhatóak az authentikációs modulok, a felhasználói adatokat tartalmazó címtár elérésének paraméterei, egyedileg szerkeszthetők a hozzáférési szabályok, és a federációs konfiguráció is teljesen külön van minden szervezetnél.

Hosztolt IDP beállítása

Legegyszerűbben a nyitóoldalon elhelyezett gyorslinkekkel hozhatunk létre új IDP-t ('Create hosted Identity Provider'). Ekkor meg kell adni a realm-et, és hogy melyik Circle-of-trust részévé kívánjuk tenni az IDP-t. Ha még nem hoztunk létre COT-ot, akkor azt megtehetjük itt.

Ezután a 'Federation' fül alatt találjuk az összes beállítási paramétert. A hosztolt IDP minden beállítását elvégezhetjük adminfelületről: aláíró és titkosító kulcsok (ezeket keystore-ból veszi, amit

a keytool parancssal menedzselhetünk parancssorból), támogatott NameID formátumok, attríbutum mappelés akár saját osztállyal, és persze a támogatott SAML2 bindingok - Redirect, POST, Artifact - paraméterei.

A beállított metaadatok XML formátumban a http://host:port/opensso/saml2/jsp/exportmetadata.jsp URL-en lesznek elérhetőek. (az exportmetadata.jsp a következő paramétereket tudja fogadni: realm, entityID)

Amennyiben digitálisan aláírt metaadatra van szükségünk, azt az adminkonzolból tudjuk csak exportálni, illetve ezen patch segítségével az exportmetadata.jsp -ből is a signMetadata=true paraméter megadásával (https://opensso.dev.java.net/issues/show_bug.cgi?id=2680)

Új SP hozzáadása

Szintén a taszkok között található link új távoli SP hozzáadására ('Register remote Service Provider'). Itt a SAML2 metaadat URL-jét kell megadni, vagy feltölteni azt. Ezen kívül egy listában megadható, hogy milyen attribútum-leképzést igényel az SP. Természetesen az SP-t is hozzá kell adni egy COT-hoz.

Miután felvettük az SP-t, néhány attribútumot a Federation fülön átállíthatunk utólag is.

Interoperabilitás

- OpenSSO IdP - Shibboleth2 SP
- OpenSSO SP - Shibboleth2 IdP
- OpenSSO IdP - SimpleSAMLphp SAML2 SP

Problémák

Hibás metaadat hozzáadása (vannak hibák, amiket az import parancs nem vesz észre) után a hozzáadott entity-t nem lehet törölni sem, ilyenkor a teljes federation fül működésképtelenné válik. Megoldás: újraindítás és a famadm delete-entity parancs használata. Ha ez sem megy, akkor a konfigurációs címtárból ki kell törölni az entity-t.

Az SP metaadatának tartalmazni kell a NameID attribútumot, az IDP anélkül nem képes a federációra. Ezt a ManageNameIDService után, és az AssertionConsumerService elé kell beírni, pl. így

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:51 CEST
cziernorbert frissítette 2026-04-14 13:23:04 CEST