Shibboleth SP per IDEM con Debian

Francesco Malvezzi

Ce.S.I.A.
Università di Modena e Reggio nell'Emilia

1 aprile 2008

Introduzione

Lo scopo di questo tutorial è:

- installare un Shibboleth SP su Debian Etch;
- configurare Shibboleth per partecipare alla federazione IDEM.

Prima di ogni altra cosa

Ottenere un certificato SCS per il proprio SP.
Il certificato deve essere SCS, perché solo SCS è la CA accettata da IDEM.
Istruzioni: `http://ca.garr.it/SCS/istruzioni.php`
Altri prerequisiti:

- web server Apache2.2
- ntp

Installazione del servizio.

Download del modulo:

```
apt-get install libapache2_mod_shib
```

Creazione di una cartella protetta: /etc/apache2/sites-available/shib_sp[1]

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

Abilitazione del modulo:

```
a2enmod shib
a2ensite shib_sp
/etc/init.d/apache2 force-reload
```

[1] Ricordarsi di creare la cartella “secure”.

File di configurazione

File di configurazione di reference:

- shibboleth.xml (`http://www.idem.garr.it/docs/conf/shibboleth.reference.xml`) – per una prova si può cambiare solo `Host name`[2] e `Credentials`;
- AAP.xml (`http://www.idem.garr.it/docs/conf/AAP.reference.xml`) – per una prova si può usare invariato;
- idem-metadata.xml (`http://www.idem.garr.it/docs/conf/idem-metadata.xml`) – lasciare invariato.

Test della correttezza sintattica del servizio:

```
shibd -t /etc/shibboleth/shibboleth.xml
```

[2] Cioé ricerca/sotituisci di sp.uniprova.it con il nome host del server reale

Aderire ad IDEM

Fare inserire i dati dello SP nel file `idem-metadata.xml`;
Istruzioni: `http://www.idem.garr.it/`
Contatto: `idem-idp@garr.it`
Se avete delle credenziali valide per un IdP potete già provare lo SP[3]!

[3] Ad esempio abilitare il php e creare il file index.php <?php print_r($_SERVER) ?>

Provare subito

- SP di prova GARR
  `https://sp-test.garr.it/secure`
- SP di prova UniMORE
  `https://omissis.unimore.it/secure`

AAP.xml

Con il file *AAP.xml* si accettano gli attributi passati dallo IdP.
Ogni attributo deve essere accettato esplicitamente.
Si stabilisce una connessione tra:

Name Il nome dell'attributo come proviene dell'IdP: ad es.: `eduPersonScopedAffiliation`;

Header il nome della variabile d'ambiente che gli sviluppatori potranno interrogare per avere dati sull'utente autenticato, ad es: `Shib-EP-Affiliation`;

Alias l'etichetta con cui riferirsi a questo attributo nell'authz (XML-based o HtAccessControl) – può essere assente.

I log

I log di Shibboleth sono:

/var/log/shibboleth/shibd.log funzionamento del demone, dialogo con lo IdP, scambio degli attributi;

/var/log/shibboleth/transaction.log log forensico: tiene traccia delle transazioni effettuate con lo IdP; il valore del NameIdentifier permette di collegare le entry di questo log con quelle dello IdP (shib-access.log);

/var/log/apache2/native.log autorizzazione;

Affinché sia popolato, il file di destinazione del Native logger deve essere creato e deve avere i permessi corretti:

```
touch /var/log/apache2/native.log
chown www-data /var/log/apache2/native.log
```

Lazy sessions

Talvolta può essere necessario non obbligare l'utente all'autenticazione Shibboleth. Ad esempio possono coesistere due autenticazioni (Shibboleth ed una locale) tra cui l'utente può scegliere.
Sono necessarie due modifiche:

sessioni pigre	sessioni strette
<Location /secure> AuthType shibboleth Require shibboleth </Location>	<Location /secure> AuthType shibboleth ShibRequireSession On require valid-user </Location>

- in `shibboleth.xml` settare a `false` il requireSession della directory da proteggere:

```
<Path name="secure" authType="shibboleth" \
 requireSession="false"/>
```

Lazy sessions – 2

E per permettere l'autenticazione Shibboleth in una lazy session?
Ridirigere l'utente al concatenamento:

- hostname dello SP;
- indirizzo del WAYF (nel caso IDEM: /WAYF/IDEM);
- stringa fissa: "?target="
- indirizzo completo cui ridirigere l'utente dopo l'autenticazione (url-encoded)

Esempio:

```
https://omissis.unimore.it/Shibboleth.sso/WAYF/IDEM? \
 target=https%3A%2F%2Fomissis.unimore.it%2Fsecure
```

Mantenere aggiornati i metadati

Mettere nel cron:

```
cd /tmp
wget --ca-certificate /etc/ssl/certs/scs-chain.pem \
 https://www.idem.garr.it/docs/conf/idem-metadata.xml
siterefresh --url idem-metadata.xml --noverify \
 --out /etc/shibboleth
mv -rf idem-metadata.xml
```

Riferimenti

- Controllo accesso in XML – presentazione di Danilo Crecchia;
- Applicazioni multiple sullo stesso server (nomi differenti oppure configurazioni differenti) – presentazione di Danilo Crecchia.
- tutorial di Giacomo Tenaglia, 2 aprile 2007 (`http://www.garr.it/meeting_aai/slide_sem/3sp.pdf`)