Costruire uno Shibboleth IdP per IDEM

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 IdP su Debian Etch;
- configurare Shibboleth per partecipare alla federazione IDEM.

La scelta di Debian/Etch come IdP non è l'unica possibile: Shibboleth-IdP si installa con un script `ant` cross-platform. Esistono alternative anche per l'uso di Apache2/Tomcat5.5. Questa configurazione resta però la più rodata e meglio documentata.

Alcune questioni che non saranno trattate

È al di fuori delle finalità di questa trattazione (prerequisiti):

- Identity management (come raccogliere, gestire e mantenere aggiornate le identità degli utenti);
- LDAP (configurazione e connessione sicura – LDAPS o StartTLS);
- Certificati digitali (come ottenere i certificati SCS è spiegato a: `http://ca.garr.it/SCS/istruzioni.php`).

Prima di ogni altra cosa

Ottenere un certificato SCS per il proprio IdP.
Il certificato deve essere SCS, perché solo SCS è la CA accettata da IDEM.
Suggerimenti: `http://ca.garr.it/`

Pacchetti da installare.

- openssl;
- ntp;
- apache2;
- sun-java5-jdk;
- tomcat5.5.

Attivare proxy_ajp

- Creare /etc/apache2/mods-available/proxy_ajp.conf

```
<Location /shibboleth-idp>
ProxyPass ajp://idp.uniprova.it:8009/shibboleth-idp
ProxyPassReverse ajp://idp.uniprova.it:8009/shibboleth-idp
</Location>
```

- Modificare: /etc/apache2/mods-enable/proxy.conf

```
<Proxy *>
AddDefaultCharset off
Order deny,allow
</Proxy>
```

Cioé commentare le righe di `deny` e lasciare invariato il resto.

Attivare StartTLS con LDAP

Modificare: /etc/apache2/mods-available/authnz_ldap.conf[1]

```
LDAPTrustedMode TLS
LDAPTrustedGlobalCert CA_BASE64 /etc/ssl/certs/scs-chain.pem
```

in cui `scs-chain.pem` sono i certificati:

- GTE CyberTrust Global Root
- Cybertrust Educational CA

uno accodato all'altro.
`http://ca.garr.it/SCS/istruzioni.php`

[1] NB: Se il server LDAP ha un certificato sotto una CA diversa da SCS, sostituire a scs-chain.pem i certificati di questa CA; se la comunicazione avviene senza cifratura, saltare questa slide.

Creare il sito idp in apache – 1

Creare il file: /etc/apache2/sites-available/idp

```
<VirtualHost _default_:443>
DocumentRoot "/var/www/"
ServerName idp.unitest.it:443
ServerAdmin root@localhost
ErrorLog /var/log/apache2/ssl_error.log
TransferLog /var/log/apache2/ssl_access.log
SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLCertificateFile /etc/ssl/certs/idp.pem
SSLCertificateKeyFile /etc/ssl/private/idp.key
SSLCertificateChainFile /etc/ssl/certs/scs-chain.pem
SSLCACertificateFile /etc/ssl/certs/scs-chain.pem
<Location /shibboleth-idp/SSO>
AuthName "Autenticazione su LDAP/StartTLS"
AuthType Basic
AuthBasicProvider ldap
AuthLDAPURL ldap://ldap1.unitest.it/ou=people,dc=unitest,dc=it?uid?sub?(uid=*) TLS
AuthzLDAPAuthoritative Off
require valid-user
</Location>
</VirtualHost>
```

Creare il sito idp in apache – 2

continua /etc/apache2/sites-available/idp

```
# workaround for apache2 POST bug
<VirtualHost _default_:8443>
SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA: \\
   +HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLVerifyClient require
SSLVerifyDepth 10
SSLOptions +StdEnvVars +ExportCertData
SSLCertificateFile /etc/ssl/certs/idp.pem
SSLCertificateKeyFile /etc/ssl/private/idp.key
SSLCertificateChainFile /etc/ssl/certs/scs-chain.pem
SSLCACertificateFile /etc/ssl/certs/scs-chain.pem
ErrorLog /var/log/apache2/ssl_error.log
TransferLog /var/log/apache2/ssl_access.log
</VirtualHost>
```

Rendere attive le modifiche in Apache

Modificare il file /etc/apache2/sites-enabled/000-default:

```
NameVirtualHost *:80
<VirtualHost *:80>
```

Aggiungere in /etc/apache2/ports:

```
Listen 80
Listen 443
Listen 8443
```

Eseguire:

```
a2enmod ssl
a2enmod proxy_ajp
a2enmod authnz_ldap
a2ensite idp
/etc/init.d/apache2 force-reload
```

Configurazione connector AJP con Apache nel file: `/etc/tomcat5.5/server.xml`

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="qui_lo_ip_dell_host"
enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" tomcatAuthentication="false" />
```

Aggiungere in /etc/default/tomcat5

```
TOMCAT5_SECURITY=no
```

Provare quanto fatto finora

- - Installare (poi cancellare) il pacchetto `tomcat5.5-webapps`;
  - aggiungere (poi rimuovere) a `proxy_ajp.conf`:
    ```
    <Location /jsp-examples>
    ProxyPass ajp://idp.unimore.it:8009/jsp-examples
    ProxyPassReverse ajp://idp.unimore.it:8009/jsp-examples
    </Location>
    ```
  - riavviare apache.
- `https://idp.uniprova.it`: pagina di benvenuto di Apache, certificato valido;
- `https://idp.uniprova.it:8443`: richiesta di certificato utente oppure errorcode -122227 (Firefox);
- `https://idp.uniprova.it/shibboleth-idp/SSO`: appare popup di autenticazione. Dopo l'autenticazione errore;[2]
- `http://idp.uniprova.it:8180`: pagina di benvenuto di Apache Tomcat/5.5;
- `https://idp.uniprova.it/jsp-examples/`: pagina di benvenuto di Apache Tomcat/5.5;

[2] Anche dopo l'installazione di Shibboleth l'accesso diretto allo SSO darà errore tipo: "Invalid data from Service Provider: no target URL received."

Installazione

Implementazione ufficiale di Internet2:

```
wget http://shibboleth.internet2.edu/downloads \
 /shibboleth-idp-1.3.3.tar.gz
tar xzvf shibboleth-idp-1.3.3.tar.gz
cd shibboleth-1.3.3-install/
```

Sovrascrittura classi obsolete:

```
cp ./endorsed/*.jar /usr/share/tomcat5.5/common/endorsed/
```

Installazione usando ant:

```
export JAVA_HOME=/usr/lib/jvm/java-1.5.0-sun
export CATALINA_HOME=/var/lib/tomcat5.5
./ant
chown tomcat55:nogroup /usr/local/shibboleth-idp/logs/
chmod 755 /usr/local/shibboleth-idp/bin/*
chown tomcat55:nogroup /var/lib/tomcat5.5/webapps/shibboleth-idp.war
```

Configurazione – panoramica

I file di configurazione rilevanti per lo IdP sono:

idp.xml File di configurazione generale: modificare gli indirizzi del server, i certificati digitali, il nome del file con i metadata;

resolver.xml Risoluzione degli attributi: definizione del servizio a cui richiederli (LDAP, db con driver jdbc), definizione degli attributi da estrarre e loro denominazione;

arps.site.xml Poliche di rilascio degli attributi: definisce quali attributi rilasciare a quali SP;

idem-metadata.xml Definizione dei partecipanti alla Federazione: elenca tutti gli IdP e gli SP con i rispettivi nomi DNS e i percorsi degli indirizzi per lo scambio degli attributi e il Single Sign On. Contiene anche i certificati digitali della CA.

Configurazione – i file

Un esempio dei file di configurazione dello IdP:

idp.xml `http://www.idem.garr.it/docs/conf/idp.reference.xml`

resolver.xml `http://www.idem.garr.it/docs/conf/resolver.reference.xml`

arps.site.xml `http://www.idem.garr.it/docs/conf/arp.site.reference.xml`

idem-metadata.xml `http://www.idem.garr.it/docs/conf/idem-metadata.xml`

Il passaggio degli attributi

Creazione keystore con certificato della CA e del server LDAP:

```
cd /usr/local/shibboleth-idp/etc/
keytool -import -keystore ./keystore.jks -alias ca -file scs-chain.pem
keytool -import -keystore ./keystore.jks -alias idp-ldap -file europki.pem
```

Modificare di `resolvertest` per usare il keystore appena creato, aggiungere all'ultima riga:

```
-Djavax.net.ssl.trustStore=/usr/local/shibboleth-idp/etc/keystore.jks
```

Uso del keystore da Tomcat: `/etc/default/tomcat5.5`

```
CATALINA_OPTS="-Djavax.net.ssl.trustStore=/usr/local/shibboleth-idp/etc/keystore.jks"
```

Test:

```
$IDP_HOME/bin/resolvertest --user=malvezzi \\
--idpXml=file:///$IDP_HOME/etc/idp.xml \\
--requester=https://www.dispense.unimore.it
```

Aderire ad IDEM

Inserire i dati dello IdP

- nel `idem-metadata.xml`;
- nel WAYF.

Istruzioni: `http://www.idem.garr.it/`
Contatto: Barbara Monticini (`monticini@fi.infn.it`).

Provare subito

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

Panoramica:

Invece dell'apparizione del popup di autenticazione inviato da Apache, si potrebbe avere piacere a mostrare una form di login.
Vantaggi:

- personalizzare la pagina secondo le esigenze della propria azienda;
- aggiungere delle istruzioni.

N.B.: Facoltativo!

Passi da compiere

Passi di svolgere:

- Disattivare la protezione dell'handler di SSO da Apache (commentare la sezione <Location /shibboleth-idp/SSO> in /etc/apache2/sites-available/idp);
- Aggiungere al file /etc/tomcat5.5/server.xml la configurazione del proprio server LDAP per permettere l'autenticazione;
- Modificare al file di deploy di shibboleth (web.xml) per fare apparire i file della form di login.

server.xml

Aggiungere al file /etc/tomcat5.5/server.xml:

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
       connectionURL="ldaps://ldap1.unitest.it"
    connectionName="cn=adminshib,dc=unitest,dc=it"
    connectionPassword="test"
    userBase="dc=unitest,dc=it"
    userSubtree="true"
    userSearch="(uid={0})"
    userRoleName="objectClass"
    debug="99"
    />
```

- userSearch="(uid=0)" nel caso che gli utenti usino come username lo uid;
- ConnectionName e ConnectionPassword devono essere presenti;
- userRoleName="objectClass" associa ad ogni utente il ruolo "person" (presente come objectClass).

web.xml – 1

Aggiungere al file /var/lib/tomcat5.5/webapps/shibboleth-idp/WEB-INF/web.xml, nel blocco <web-app>

```
<!-- Define a security constraint on this application -->
 <security-constraint>
   <!-- the list of URL patterns that needs to be protected -->
   <web-resource-collection>
     <web-resource-name>SSO servlet</web-resource-name>
     <url-pattern>/SSO</url-pattern>
   </web-resource-collection>
   <auth-constraint>
     <!-- allow all roles, a role has to be specified from Tomcat v5.5.15 and higher -->
     <role-name>*</role-name>
   </auth-constraint>
   <!-- force all data to use SSL for transport -->
   <user-data-constraint>
     <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   </user-data-constraint>
 </security-constraint>
```

web.xml – 2

File:
/var/lib/tomcat5.5/webapps/shibboleth-idp/WEB-INF/web.xml

```
<!-- Login configuration using form-based authentication -->
<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>Shibboleth form-based authentication</realm-name>
  <form-login-config>
    <form-login-page>/login.jsp</form-login-page>
    <form-error-page>/login-error.jsp</form-error-page>
  </form-login-config>
</login-config>
<!-- Security roles referenced by this web application -->
<security-role>
  <description>All Users</description>
  <role-name>person</role-name>
</security-role>
```

Riferimenti

- https://spaces.internet2.edu/display/SHIB/InstallingShibboleth
- tutorial di Giacomo Tenaglia, 2 aprile 2007 (http://www.garr.it/meeting_aai/slide_sem/2idp.pdf)
- Seminario su Shibboleth 28-29/11/07 di Giacomo Tenaglia ad UniPD http://dreams.stat.unipd.it/?Gruppi_di_lavoro:Seminario_su_Shibboleth_28-29%2F11%2F07
- https://spaces.internet2.edu/display/SHIB/IdPUserAuthnConfig