Shibboleth IdP

Francesco Malvezzi

Università di Modena e Reggio nell'Emilia

30 marzo 2009

Introduzione

In questa sezione installeremo Shibboleth-IdP 2.1 su un server GNU/Debian lenny.
La nostra scelta:

- tomcat5.5
- apache2.2 con mod_ajp

Alternativa solo tomcat

Vantaggi:

- un solo servizio;
- fine delle idiosincrasie di openssl.

Svantaggi:

- minore flessibilità;
- il bind a una porta privilegiata (443) richiede qualche modifica agli script di default;
- bisogna usare i keystore (difficile inserire una chiave privata).

Alternativa tomcat con apache portable runtime

Vantaggi:

- un solo servizio;
- “optimal performance”;

Svantaggi:

- minore flessibilità;
- il bind a una porta privilegiata (443) richiede qualche modifica agli script di default;
- ricompilazione – difficile gestione.

Pacchetti da installare.

- openssl;
- ntp;
- apache2;
- sun-java6-jdk (non-free);
- tomcat5.5.

Attivare proxy_ajp

- Aggiungere in coda alle location in /etc/apache2/sites-available/default-ssl

```
<Location /idp>
ProxyPass ajp://localhost:8009/idp
ProxyPassReverse ajp://localhost:8009/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.

Creare il sito per lo Attribute Authority in Apache

- Copiare /etc/apache2/sites-available/default-ssl in /etc/apache2/sites-available/default-ssl2;
- correggere le occorrenze della porta 443 in 8443;
- modificare la destinazione dei log;
- deselezionare la direttiva “Client authentication”:

```
SSLVerifyClient optional_no_ca
        SSLVerifyDepth  10
```

Rendere attive le modifiche in Apache

Aggiungere al file /etc/apache2/ports:

```
<IfModule mod_ssl.c>
    Listen 8443
</IfModule>
```

Eseguire:

```
a2enmod ssl
a2enmod proxy_ajp
a2ensite default-ssl
a2ensite default-ssl2
/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="127.0.0.1"
enableLookups="false" redirectPort="443"
protocol="AJP/1.3" tomcatAuthentication="false" />
```

Aggiungere in /etc/default/tomcat5.5

```
JAVA_OPTS="-Djava.awt.headless=true -Xmx512M -XX:MaxPermSize=512M"
TOMCAT5_SECURITY=no
```

Installazione - 1

Implementazione ufficiale di Internet2:

```
wget http://shibboleth.internet2.edu/downloads/shibboleth/idp/2.1.2/sh
wget http://shibboleth.internet2.edu/downloads/shibboleth/idp/2.1.2/sh
gpg --keyserver hkp://subkeys.pgp.net --recv-keys 47905D15 146B2514
gpgv --keyring .gnupg/pubring.gpg shibboleth-identityprovider-2.1.2-bi
jar xf shibboleth-identityprovider-2.1.2-bin.zip
cd shibboleth-identityprovider-2.1.2
```

Sovrascrittura classi obsolete:

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

Installazione:

```
export JAVA_HOME=/usr/lib/jvm/java-6-sun
export CATALINA_HOME=/var/lib/tomcat5.5
sh install.sh
chown tomcat55:nogroup /opt/shibboleth-idp/logs/
chown tomcat55:nogroup /opt/shibboleth-idp/metadata/
chown tomcat55:nogroup /opt/shibboleth-idp/credential/
```

Installazione - 2

Creazione di un Context Deployment Fragment

```
cat > $CATALINA_HOME/conf/Catalina/localhost/idp.xml
<Context docBase="/opt/shibboleth-idp/war/idp.war"
         privileged="true"
         antiResourceLocking="false"
         antiJARLocking="false"
         unpackWAR="false"
         swallowOutput="true" />
CTRL + D
```

Un test:

```
https://idem-idp.dmz-ext.unimo.it/idp/profile/Status
```

Deve dare `OK`.

Configurazione – panoramica

I file di configurazione rilevanti per lo IdP sono:

relying-party.xml Impostazioni generali del server: profili SAML, certificati digitali, metadati;

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

attribute-filter.xml Poliche di rilascio degli attributi: definisce quali attributi rilasciare a quali SP;

handler.xml enumerazione degli handler esposti;

login.config configurazione del login (JAAS).

Configurazione – i file dei certificati

idp.key e idp.crt chiave privata e certificato x509 generate durante l'installazione;

idp.jks keystore con chiave, certificato e password generate durante l'installazione. È un file inutile se tomcat è dietro un proxy inverso;

cacerts keystore principale di java (in $JAVA_HOME/jre/lib/security). Deve contenere le CA delle risorse cui shibboleth accede: metadati, data sources, backend di autenticazione ecc. . . (passphrase "changeit").

Configurazione – il minimo indispensabile

- Editare `handler.xml` per cancellare lo endpoint `RemoteUser`. Abilitare lo endpoint `UsernamePassword`.
- Modificare secondo le proprie esigenze `login.config`

Digressione – TestShib two

Per un test più serio, che include la verifica del passaggio degli attributi di default, è disponibile TestShib 2:
`http://www.testshib.org/testshib-two/index.jsp`

Attributi – importazione da ldap

https://spaces.internet2.edu/display/SHIB2/IdPAddAttribute

Esempio:

```
<resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory"
xmlns="urn:mace:shibboleth:2.0:resolver:dc"
        ldapURL="ldap://ldap.example.org"
        baseDN="ou=people,dc=example,dc=org"
        principal="uid=myservice,ou=system"
        principalCredential="myServicePassword"
        useStartTLS="true">
        <FilterTemplate>
            <![CDATA[
                (uid=$requestContext.principalName)
            ]]>
        </FilterTemplate>
    </resolver:DataConnector>
```

Attributi – definizione

Nel file attribute-resolver.xml
Esempio:

```
 <resolver:AttributeDefinition id="uid" xsi:type="Simple"
xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        sourceAttributeID="uid">
        <resolver:Dependency ref="myLDAP" />
        <resolver:AttributeEncoder xsi:type="SAML1String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:mace:dir:attribute-def:uid" />
        <resolver:AttributeEncoder xsi:type="SAML2String"
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
            name="urn:oid:0.9.2342.19200300.100.1.1"
friendlyName="uid" />
    </resolver:AttributeDefinition>
```

Un attributo speciale – eduPersonTargetID - 1

Installare mysql:

```
apt-get install libmysql-java
ln -s /usr/share/java/mysql-connector-java.jar /usr/share/tomcat5.5/common/lib/
ln -s /usr/share/java/mysql-connector-java.jar $IDP_HOME/lib/
```

Creare il database:

```
mysql> create database userdb;
Query OK, 1 row affected (0.00 sec)

mysql> grant all privileges on userdb.* to 'idp_user'@'localhost'
identified by 'some_passwd';
Query OK, 0 rows affected (0.00 sec)

CREATE TABLE shibpid
(
    localEntity VARCHAR(255) NOT NULL,
    peerEntity VARCHAR(255) NOT NULL,
    principalName VARCHAR(255) NOT  NULL,
    localId VARCHAR(255) NOT NULL,
    persistentId VARCHAR(255) NOT NULL,
    peerProvidedId VARCHAR(255) NULL,
    creationDate TIMESTAMP NOT NULL,
    deactivationDate TIMESTAMP NULL,
    KEY persistentId (persistentId),
    KEY persistentId_2 (persistentId, deactivationDate),
    KEY localEntity (localEntity(16), peerEntity(16),localId),
    KEY localEntity_2 (localEntity(16), peerEntity(16), localId, deactivationDate)
 )
);
```

Un attributo speciale – eduPersonTargetID - 2

Rilasciare eduPersonTargetedID (attribute-resolver.xml):

```
<resolver:AttributeDefinition id="eduPersonTargetedID" xsi:type="SAML2NameID"
 xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        sourceAttributeID="persistentID">
        <resolver:Dependency ref="myStoredID" />
        <resolver:AttributeEncoder xsi:type="SAML1XMLObject" xmlns="urn:mace:shibboleth:2.0:at
                name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" />
        <resolver:AttributeEncoder xsi:type="SAML2XMLObject" xmlns="urn:mace:shibboleth:2.0:at
                name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="eduPersonTargetedID" />
    </resolver:AttributeDefinition>

 <resolver:DataConnector xsi:type="StoredId"
    xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                           id="myStoredID"
                           sourceAttributeID="commonName"
    generatedAttributeID="persistentID"
    salt="c3AuZXVyb3BraS5vcmc6ODAyNjAiBggrBgEFBQcwAoYWaHR0cDo">
      <resolver:Dependency ref="ldap1" />
      <resolver:Dependency ref="commonName" />
      <ApplicationManagedConnection
 jdbcDriver="com.mysql.jdbc.Driver" jdbcURL="jdbc:mysql://localhost:3306/userdb"
 jdbcUserName="idp_user" jdbcPassword="some_passwd" />
    </resolver:DataConnector>
```

Test degli attributi

Usare aacli.sh, ad esempio:

```
sudo sh bin/aacli.sh --configDir=conf --principal=francesco
        --requester=https://idem-sp.unimore.it/sp
--issuer=https://idem-idp.unimore.it/idp/shibboleth
```

Per aderire ad IDEM

- accertarsi di presentarsi con un certificato digitale accettato;
- inserire in `idem-metadata.xml` il proprio frammento di metadata (`$IDP_HOME\metadata\idp-metadata.xml`);
- modificare `relying-party.xml` per scaricare i metadati di Idem:

```
<MetadataProvider id="URLMD-idem" xsi:type="FileBackedHTTPMetadataProvider"
 xmlns="urn:mace:shibboleth:2.0:metadata"
 metadataURL="https://www.idem.garr.it/docs/conf/signed-metadata.xml"
 backingFile="/opt/shibboleth-idp/metadata/idem-metadata.xml">
            <MetadataFilter xsi:type="ChainingFilter"
            xmlns="urn:mace:shibboleth:2.0:metadata">
                <MetadataFilter xsi:type="SignatureValidation"
                                xmlns="urn:mace:shibboleth:2.0:metadata"
                                trustEngineRef="shibboleth.MetadataTrustEngine"
                                requireSignedMetadata="true" />
            </MetadataFilter>
        </MetadataProvider>
```

Riferimenti

- Istruzioni ufficiali di Internet2: https://spaces.internet2.edu/display/SHIB2/IdPInstall
- Ancora Internet2: https://spaces.internet2.edu/display/SHIB2/IdPApacheTomcatPrepare
- 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
- Istruzioni dello SWITCH: https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.1/idp/install-idp-2.1-debian.html