Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Installazione di un Identity Provider Shibboleth

Primi passi per l'autenticazione federata

Marco Malavolti - Servizio IDEM GARR AAI

IDEM DAY 2018| Roma, 07/05/2018

IDEM TUTORIALS

https://github.com/ConsortiumGARR/idem-tutorials

Svolgimento del Corso

Il Corso sarà prettamente hands-on:

– Slide (poche e mirate)

– Esercizi su ambiente virtuale

– Verifica collettiva

!!! NON SEMPRE BEST-PRACTICES !!!

Limiti dell'ambiente del corso

– **esempio 1:** Memoria RAM allocata a Jetty

– **esempio 2:** SP, IdP e directory service (LDAP) nello stesso server

– **esempio 3:** Directory Service (LDAP) con lo stesso certificato del virtualhost(Apache) del IdP

Agenda e Logistica

T1: Installazione e configurazione di Shibboleth IdP v3.3.2

T2: IdP configurazione base: connessione con un SP

T3: Configurazione Data Sources multiple

T4: Attribute-Filter

T5: IDEM Entity Registry e Entity Category (R&S e COCO)

1. **Vagrant**:
   a. perfetto per deploy di test
2. **Virtualbox**:
   a. il più diffuso virtualizzatore personale
3. **Ansible**:
   a. automazione
   b. playbook = howto automaticamente testato
   c. ottimo per ambiente di test e produzione

Server di sviluppo usato nel corso

1. Sistema Operativo: **Linux Debian 8 (Jessie) a 64 Bit**
2. Hardware: **1 CPU, 2GB di RAM, 10GB di HDD**
3. Software utilizzati:
   a. `slapd` (openLDAP)
   b. `openjdk-8-jdk` (Java 8)
   c. `apache2` (Web Server)
   d. `mysql-server` (Database server)
   e. `libmysql-java`, `libcommons-dbcp-java`, `libcommons-pool-java`, `libcommons-pool-java` (Librerie Java richieste)
   f. `libapache2-mod-shib2` (Shibboleth SP)
   g. `ntp` (Network Time Protocol)
   h. `jetty 9` (Servlet Container)

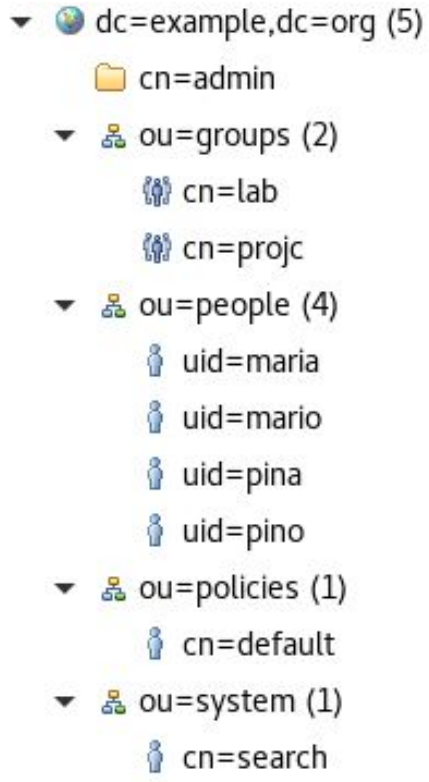
Configurazioni già disponibili sul Server

1. JAVA_HOME=/usr/lib/jvm/default-java/jre

2. Jetty 9 Servlet Container:
   - Opzioni Java (RAM + /dev/urandom)
   - Porta 8080

3. Apache2:
   - Porte 443 e 80 (con redirezione su 443)
   - VirtualHost https://idp.example.org
     i. ProxyPass /idp http://localhost:8080/idp
   - VirtualHost https://sp.example.org
     i. Location /secure
        - AuthType shibboleth
4. slapd:
   - certificati per STARTTLS
   - access list limitata
   - indici
   - schemi "eduperson-201602" e "schac-20150413"

Directory Service (openLDAP)



NO SLAPD.CONF
(Deprecato)

Cominciamo!

1. `vagrant ssh`
2. `sudo su -`
3. `cd ./IdP3-ansible`
4. `git pull`
5. `ansible-playbook playbook.yml -i hosts -e cleanup=true`

STEP 1 - Estrazione e Librerie

```
root@idp:~# cd /opt/
root@idp:/opt# tar xfz shibboleth--identity--provider--3.3.2.tar.gz
root@idp:/opt# cd shibboleth--identity--provider--3.3.2/webapps/WEB-INF/lib
root@idp:/opt/shibboleth--identity--provider--3.3.2/webapps/WEB-INF/lib# ln -s /usr/share/java/commons-dbcp.jar
root@idp:/opt/shibboleth--identity--provider--3.3.2/webapps/WEB-INF/lib# ln -s /usr/share/java/commons-pool.jar
root@idp:/opt/shibboleth--identity--provider--3.3.2/webapps/WEB-INF/lib# ln -s /usr/share/java/jstl1.1.jar
root@idp:/opt/shibboleth--identity--provider--3.3.2/webapps/WEB-INF/lib# ln -s /usr/share/java/mysql.jar
```

STEP 2 - Installazione

```
root@idp:/opt/shibboleth--identity--provider--3.3.2/webapp/WEB-INF/lib# cd ../../../

root@idp:/opt/shibboleth--identity--provider--3.3.2# ./bin/install.sh

Source (Distribution) Directory (press <enter> to accept default):
[/opt/shibboleth-identity-provider-3.3.2]

Installation Directory: [/opt/shibboleth--idp]

Hostname: [idp.example.org]

SAML EntityID: [https://idp.example.org/idp/shibboleth]

Attribute Scope: [example.org]

Backchannel PKCS12 Password:

Re--enter password:

Cookie Encryption Key Password:

Re--enter password:

[...]

BUILD SUCCESSFUL

Total time: 29 seconds
```

STEP 3 - Shibboleth e Jetty

Jetty deve poter scrivere in varie directory di shibboleth:

```
1.  chown -R jetty /opt/shibboleth-idp/logs/
2.  chown -R jetty /opt/shibboleth-idp/metadata/
3.  chown -R jetty /opt/shibboleth-idp/credentials/
4.  chown -R jetty /opt/shibboleth-idp/conf/
5.  chown -R jetty /opt/shibboleth-idp/system/
6.  chown -R jetty /opt/shibboleth-idp/war/
```

Installare il war di shibboleth:

vim /opt/jetty/webapps/idp.xml:

```
<Configure class="org.eclipse.jetty.webapp.WebAppContext">
  <Set name="war"><SystemProperty name="idp.home"/>/war/idp.war</Set>
  <Set name="contextPath">/idp</Set>
  <Set name="extractWAR">false</Set>
  <Set name="copyWebDir">false</Set>
  <Set name="copyWebInf">true</Set>
</Configure>
```

STEP 4 - Shibboleth e openLDAP

File: **/opt/shibboleth-idp/conf/ldap.properties**

Configurazione:

connessione STARTTLS (con certificato del server ldap)
modalità di autenticazione bind&search
filtro di ricerca: `(&(uid={user})(objectClass=inetOrgPerson))`

```
idp.authn.LDAP.authenticator = bindSearchAuthenticator
idp.authn.LDAP.ldapURL = ldap://idp.example.org:389
idp.authn.LDAP.useStartTLS = true
idp.authn.LDAP.sslConfig = certificateTrust
idp.authn.LDAP.trustCertificates = /etc/ssl/certs/idp.example.org--cert.pem
idp.authn.LDAP.baseDN = ou=people,dc=example,dc=org
idp.authn.LDAP.userFilter = (&(uid={user})(objectClass=inetOrgPerson))
idp.authn.LDAP.bindDN = cn=search,ou=system,dc=example,dc=org
idp.authn.LDAP.bindDNCredential = password
```

STEP 5 - Un ID persistente per gli utenti

Abbiamo bisogno di un ID:
persistente, **non riassegnabile**, **opaco** e **relativo all'utente**

SAML NameID	eduPersonTargetedID
è un identificativo presente nel Subject dell'asserzione che l'IdP invia all'SP che lo ha richiamato	è un *attributo* rilasciato dall'IdP che usa il valore presente nel Subjetct dell'asserzione

`<saml2:Subject>`
`  <saml2:NameID [...]>`
`  [...]`
`  </saml2:NameID>`
`  [...]`
`</saml2:Subject>`
	`<saml:AttributeStatement>`
	`  <saml:Attribute Name="eduPersonTargetedID"[...]>`
	`  <saml:AttributeValue [...] </saml:AttributeValue>`
	`  </saml:Attribute>`
	`</saml:AttributeStatement>`

Marco Malavolti - **IDEM GARR AAI** - marco.malavolti@garr.it

STEP 5 - Un ID persistente per gli utenti

Strategie di generazione:

1. computed ma non stored
2. **computed e stored**

File da configurare:

1. **saml-nameid.properties** (strategie di generazione e memorizzazione)
2. **saml-nameid.xml** (abilitazione del persistentId generator)
3. **global.xml** (configurazione del RDMBS dove memorizzare e recuperare il persistentID)

STEP 5 - Un ID persistente per gli utenti

1. *saml-nameid.properties*:

```
idp.persistentId.sourceAttribute = uid
idp.persistentId.salt = SALT
idp.persistentId.generator = shibboleth.StoredPersistentIdGenerator
idp.persistentId.dataSource = MyDataSource
```

2. *saml-nameid.xml*:

```
[...]
<!---- Uncommenting this bean requires configuration in saml--
nameid.properties. ---->
<ref bean="shibboleth.SAML2PersistentGenerator" />
[...]
```


Marco Malavolti - **IDEM GARR AAI** - marco.malavolti@garr.it

STEP 5 - Un ID persistente per gli utenti

3. global.xml:

```
<bean id="MyDataSource" class="org.apache.commons.dbcp.BasicDataSource"
  p:driverClassName="com.mysql.jdbc.Driver"
  p:url="jdbc:mysql://localhost:3306/shibboleth?autoReconnect=true"
  p:username="shibboleth"
  p:password="password"
  p:maxActive="10"
  p:maxIdle="5"
  p:maxWait="15000"
  p:testOnBorrow="true"
  p:validationQuery="select 1"
  p:validationQueryTimeout="5" />

<bean id="shibboleth.JPAStorageService" class="org.opensaml.storage.impl.JPAStorageService"
      p:cleanupInterval="%{idp.storage.cleanupInterval:PT10M}"
      c:factory-ref="shibboleth.JPAStorageService.entityManagerFactory"/>
```

STEP 5 - Un ID persistente per gli utenti

```
<bean id="shibboleth.JPAStorageService.entityManagerFactory"
      class="org.springframework.orm.jpa.LocalContainerEntityManagerFactoryBean">
  <property name="packagesToScan" value="org.opensaml.storage.impl"/>
  <property name="dataSource" ref="MyDataSource"/>
  <property name="jpaVendorAdapter" ref="shibboleth.JPAStorageService.JPAVendorAdapter"/>
  <property name="jpaDialect">
    <bean class="org.springframework.orm.jpa.vendor.HibernateJpaDialect" />
  </property>
</bean>

<bean id="shibboleth.JPAStorageService.JPAVendorAdapter"
      class="org.springframework.orm.jpa.vendor.HibernateJpaVendorAdapter">
  <property name="database" value="MYSQL" />
</bean>
```

STEP 5 - Un ID persistente per gli utenti

RIF.: https://wiki.shibboleth.net/confluence/display/IDP30/PersistentNameIDGenerationConfiguration

Che cosa serve per la memorizzazione dei persistentID?

1. Un database: [shibboleth]
2. Un utente: [shibboleth]
3. Una tabella: [shibpid]

```
cd /root/IdP3--ansible/ ; msyql --u root --p <
roles/mysql/files/shibboleth.sql
```

NOTA: lo script crea anche un'altra tabella (`StorageRecords`) che verrà utilizzata da Shibboleth per la gestione delle sessioni e per la registrazione delle scelte degli utenti sul rilascio dei loro attributi ai Service Provider (consenso informato).

ESERCIZI

1. Installazione (con librerie):
   - `cd /opt ; tar xzf shibboleth-identity-provider-3.*.tar.gz`
   - `cd /opt/shibboleth-identity-provider-3.*/webapp/WEB-INF/lib`
   - `ln -s /usr/share/java/commons-dbcp.jar`
   - `ln -s /usr/share/java/commons-pool.jar`
   - `ln -s /usr/share/java/mysql.jar`
   - `ln -s /usr/share/java/jstl1.1.jar`
   - `cd /opt/shibboleth-identity-provider-3.* ; ./bin/install.sh`
2. Permessi:
   - `cd /opt/shibboleth-idp ; chown -R jetty logs/ metadata/ credentials/ conf/ system/ war/`
3. Caricare i file di configurazione parzialmente compilati:
   - `cd /root/IdP3-ansible; ansible-playbook playbook.yml -i hosts -e '{"pre_t": 1}'`

ESERCIZI

4. Shibboleth e openLDAP:
   - completare il file di configurazione: **`/opt/shibboleth--idp/conf/ldap.properties`**
   - scommentare il corretto "**`idp.authn.LDAP.authenticator`**"

5. `saml-nameid.properties`:
   - completare il file di configurazione: **`/opt/shibboleth--idp/conf/saml--nameid.properties`**
   - vedi commenti in **`idp.persistentId.salt`** e in **`idp.persistentId.dataSource`**

6. `saml-nameid.xml`:
   - completare il file di configurazione: **`/opt/shibboleth--idp/conf/saml--nameid.xml`**
   - rimuovere il commento al giusto **`<bean>`** per abilitare il **`persistentIdGenerator`**

ESERCIZI

7. `global.xml` (configurazione RDBMS per persistentId):
   - completare il file di configurazione: **`/opt/shibboleth--idp/conf/global.xml`**
   - verificare concordanza **`<bean id=... e idp.persistentId.dataSource`**
   - inserire lo stesso valore in **`<property name="dataSource".../>`**
8. Creazione DB:
   - **`mysql --u root --p < /root/IdP3--ansible/roles/mysql/files/shibboleth.sql`**
9. Istruire Jetty al caricamento del WAR di Shibboleth IdP:
   - **`cp /root/IdP3--ansible/roles/shib3idp/files/idp.xml /opt/jetty/webapps`**
10. Riavvio di Jetty:
    - **`service jetty restart`**
11. Visualizzare lo Status di Shibboleth:
    - **`curl --k --s https://localhost/idp/status`**

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

GRAZIE MILLE!

slides

http://bit.ly/2Jxbbvd

Marco Malavolti - Servizio IDEM GARR AAI - (marco.malavolti@garr.it)