

Shibboleth IdP v3.2.1

davide.vagheti@garr.it

- Hands-on:
 - Slide (poche e mirate)
 - Esercizi su ambiente virtuale
 - Verifica collettiva

NON SEMPRE BEST-PRACTICES

- limiti dell'ambiente del corso
 - esempio1: ram allocata a Tomcat
 - esempio2: SP, IdP e directory nello stesso server
 - esempio3: directory con lo stesso certificato del virtualhost del IdP

- T1: Installazione e configurazione di Shibboleth IdP v3.2.1
- T2: IdP configurazione base: connessione con un SP
- T3: Configurazione Data Sources multiple
- T4: Trasformazione Attributi
- T5: Configurazione filtri
- T6: IDEM Entity Registry

T1,T2: 1h e 15min T3-T6: 45min

- vagrant:
 - perfetto per deploy di test
- virtualbox:
 - il piu' diffuso virtualizzatore personale
- ansible:
 - automazione
 - playbook = howto automaticamente testato
 - ok per ambiente di test e per produzione

- SO: Ubuntu 14.04 32bit
- Pacchetti:
 - slapd
 - tomcat7
 - openjdk-7-jdk
 - apache2
 - mysql-server
 - libmysql-java (mysql-java-connector)
 - libapache2-mod-shib2 (Shibboleth SP 2.5)
 - ntp

Gia' configurati:

- tomcat7
 - JAVA_HOME
 - opzioni JAVA (/dev/urandom e RAM);
 - in ascolto solo AJP (8009)
- apache2
 - solo 443
 - VirtualHost <https://idp.example.org>
 - ProxyPass /idp ajp:...
 - VirtualHost <https://sp.example.org>
 - Location /secure
 - AuthType shibboleth
- slapd
 - certificati per STARTTLS
 - access list limitata
 - indici
 - schema eduPerson versione 201602

Directory Information Tree



(NO slapd.conf)

- cn=config
- dc=example,dc=org
 - ou=groups
 - cn=lab
 - cn=projc
 - ou=people
 - uid=mario
 - uid=maria
 - uid=pino
 - uid=pina
 - ou=system
 - cn=search

Iniziamo...

Aggiorniamo



```
vagrant ssh
```

```
sudo su
```

```
cd IdP3-ansible
```

```
git pull
```

```
ansible-playbook playbook.yml -i  
hosts -e cleanup=true
```

Untar e install.sh



```
root@idp:~# cd /opt/  
root@idp:/opt# tar xfz shibboleth-identity-provider-3.2.1.tar.gz  
root@idp:/opt# cd shibboleth-identity-provider-3.2.1/  
root@idp:/opt/shibboleth-identity-provider-3.2.1# ./bin/install.sh  
Source (Distribution) Directory: [/opt/shibboleth-identity-provider-  
3.2.1]
```

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

```
Hostname: [sp.example.org]
```

```
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
```

Tomcat e Shibboleth



Tomcat deve poter scrivere in varie directory di shibboleth:

```
chown -R tomcat7 /opt/shibboleth/idp/conf
chown -R tomcat7 /opt/shibboleth/idp/logs
chown -R tomcat7 /opt/shibboleth/idp/metadata
chown -R tomcat7 /opt/shibboleth/idp/credentials
```

Installare il war di shibboleth:

```
vim /etc/tomcat7/Catalina/localhost/idp.xml
```

```
<Context
docBase="/percorso/installazione/shibboleth/war/i
dp.war"
    privileged="true"
    antiResourceLocking="false"
    swallowOutput="true">
    <Manager pathname="" />
</Context>
```

Shibboleth e LDAP



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

Configurazione:

- connessione STARTTLS
- (certificato del server ldap)
- modalita' di autenticazione bind&search
- filtro di ricerca: uid e 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
```

Un ID per i nostri utenti



SAML 2 NameID o eduPersonTargetedId:

- il primo e' nel subject dell'asserzione:

```
<saml2:Subject>  
  <saml2:NameID [...]>  
  [...]  
</saml2:NameID>  
  [...]  
</saml2:Subject>
```

- il secondo e' un attributo:

```
<saml:AttributeStatement>  
  <saml:Attribute Name="eduPersonTargetedId" [...]>  
    <saml:AttributeValue [...] </saml:AttributeValue>  
  </saml:Attribute>  
</saml:AttributeStatement>
```

Una storia lunga:

<https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers>

<https://www.terena.org/mail-archives/refeds/msg05282.html>

<http://saml2int.org/profile/current/>

Abbiamo bisogno di un id:

- persistent, non-reassignable, opaque, targeted;

Strategie di generazione:

- computed ma non stored;
- **computed e stored;**

File da configurare:

- saml-nameid.properties
 - strategie di generazione e memorizzazione
- saml-nameid.xml
 - abilitazione del persistentId generator
- global.xml
 - configurazione del RDMBS dove memorizzare e recuperare il persistentId

saml-nameid.properties

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

saml-nameid.xml

```
[...]
    <util:list id="shibboleth.SAML2NameIDGenerators">
        <ref
bean="shibboleth.SAML2TransientGenerator" />
        <!-- Uncommenting this bean requires
configuration in saml-nameid.properties. -->
        <ref
bean="shibboleth.SAML2PersistentGenerator" /> [...]
```

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"/>

<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>
```

Configurazione del RDBMS



Rif.:

<https://wiki.shibboleth.net/confluence/display/IDP30/PersistentNameIDGenerationConfiguration>

Cosa ci serve:

- un DB: [shibboleth]
- un utente: [shibboleth]
- una tabella: [storedId]

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

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

- **installazione:**

- `cd /opt; untar... ; cd /opt/shibboleth/idp; ./bin/install.sh`
- valori: `hostname=idp.example.org; password=password`

- **permessi:**

- `tomcat7 owner di conf, logs, metadata, credentials (ricorsivo)`

- **caricare i file di configurazione parzialmente compilati:**

- `cd /root/IdP3-ansible; ansible-playbook playbook.yml -i hosts -e '{"pre_t": 1}'`

- **shibboleth e ldap:**

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

- **saml-nameid.properties:**

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

- **saml-nameid.xml**

- completare il file di configurazione: `/opt/shibboleth-idp/conf/saml-nameid.xml`
- **scommentare il bean per abilitare il** `persistentIdGenerator`

- **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".../>`

- **creazione DB:**

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

- **riavvio tomcat:** `/etc/init.d/tomcat7 restart`

- **Shibboleth IdP status:**

- `curl -k -s https://localhost/idp/status`