Guida Shibboleth IdP2.2.0 apache+tomcat

a cura di Fabio Dono, Servizio IDEM GARR AAI, idem-help@garr.it, ultima modifica 26/11/2010

TOC

- 1 Introduzione
- 2 Pacchetti necessari
  - 2.1 OpenSSL
  - 2.2 NTP
  - 2.3 Apache 2.2 con mod_ssl e mod_proxy_ajp
  - 2.4 gnupg e gpgv
- 3 Java
  - 3.1 Installare manualmente Java 6 in /opt
- 4 Tomcat 6
  - 4.1 Installazione Tomcat 6 manuale
- 5 IdP Shibboleth 2.2.0
  - 5.1 Installazione IdP Shibboleth
  - 5.2 MySQL Server 5.0
    - 5.2.1 Creare Utenti e DataBase
    - 5.2.2 Installazione del java mysql connector
- 6 Certificati X.509
- 7 Autenticazione Utenti
  - 7.1 Configurazione JAAS
- 8 Configurare Tomcat
- 9 Configurare Apache
  - 9.1 mod_ssl
- 10 Configurare l' IdP Shibboleth
  - 10.1 Configurare l' IdP
    - 10.1.1 Configurazione delle Credenziali
    - 10.1.2 Metadata Trust
    - 10.1.3 Attribute-resolver e Attribute-filter
    - 10.1.4 Configurazione dell' Authentication Handler
    - 10.1.5 Configurazione urlIdP Status
  - 10.2 Re-installare Shibboleth
  - 10.3 Avviare Tomcat
- 11 Log

Introduzione

Comandi da shell

Output

```
Contenuto default di un file.
Modifiche generiche da apportare.
Modifiche specifiche da apportare.
```

Pacchetti necessari

OpenSSL

Versione 0.9.8, pacchetto: openssl.
OpenSSL verra' usato per gestire i certificati.

NTP

Pacchetto: ntp-server
Shibboleth richiede necessariamente di avere l'orologio correttamente sincronizzato. Dopo averlo installato ricordare di configurarlo con un server NTP raggiungibile nella propria rete.

Apache 2.2 con mod_ssl e mod_proxy_ajp

Pacchetto: apache2.

gnupg e gpgv

Pacchetto: gnupg and gpgv
Necessario per verificare la firma del software installato

Java

Controllare se la versione di java6 e' l'ultimo update disponibile

```
java -version
java version "1.6.0_22"
```

se si, questa parte potra' essere saltata

Installare manualmente Java 6 in /opt

-Scaricare Java SE Development Kit (JDK) 6 versione Linux da http://java.sun.com

-Installare Java 6 in /opt rimuovendo anche i link simbolici eventualmente presenti:

```
cd /opt
chmod 750 jdk-6u22-linux-i586.bin
./jdk-6u22-linux-i586.bin
test -d /opt/java && rm /opt/java
ln -s /opt/jdk1.6.0_22 /opt/java
```

-Usare update-alternatives per includere gli eseguibili di Java nei path.

```
export JAVA_HOME=/opt/java
/usr/sbin/update-alternatives --install /usr/bin/java \
java $JAVA_HOME/bin/java 200
/usr/sbin/update-alternatives --install /usr/bin/javac \
javac $JAVA_HOME/bin/javac 200
/usr/sbin/update-alternatives --install /usr/bin/jar \
jar $JAVA_HOME/bin/jar 200
/usr/sbin/update-alternatives --install /usr/bin/keytool \
keytool $JAVA_HOME/bin/keytool 200
```

-Includere o sostituire in /etc/profiles le seguenti righe

```
[...]
JAVA_HOME=/opt/java
export JAVA_HOME
```

Tomcat 6

Tomcat 6.0.17 o superiori (al momento Tomcat 7 non e' ancora stato testato con shibboleth) e' strettamente necessario per completare l'installazione di un IdP Shibboleth v2.x. Dal momento che Debian spesso non e' aggiornato all'ultimo update di Tomcat, si procedera' scaricando l'ultima versione 6.x da http://tomcat.apache.org/download-60.cgi

Installazione Tomcat 6 manuale

1. Scaricare l'ultima versione di Tomcat 6.0.x in /opt
2. **cd /opt**
   tar -xzf apache-tomcat-6.0.29.tar.gz
3. Creare i link simbolici per le directory di configurazione e logs
   ln -s /opt/apache-tomcat-6.0.29 /opt/tomcat
   ln -s /opt/tomcat/conf /etc/tomcat
   ln -s /opt/tomcat/logs /var/log/tomcat
4. Rimuovere eventuali file non necessari da /opt/tomcat/bin:
   cd /opt/tomcat/bin
   rm *.bat
5. Rimuovere le web application non necessarie da /opt/tomcat/webapps:
   cd /opt/tomcat/webapps
   rm -rf docs examples host-manager manager
6. Creare una directory per le librerie endorsed (/opt/tomcat/endorsed):
   cd /opt/tomcat
   mkdir /opt/tomcat/endorsed
7. Creare un link simbolico a catalina.sh (usato per avviare tomcat):
   ln -s /opt/tomcat/bin/catalina.sh /etc/init.d/tomcat
8. Configurare la memoria fisica del server da allocare per la JVM, tenendo conto che la memoria minima allocabile per Xmx e' 512MB e per il parametro di memoria massima XX:MaxPermSize e' opportuno impostare la meta' della memoria fisica disponibile oppure 256MB come valore minimo:
   vim /opt/tomcat/bin/catalina.sh oppure il vostro editor preferito (vim?) per editare il file ed aggiungere la riga in rosso mancante

```
#
# $Id: catalina.sh ... $
# -----------------------------------------------------------------------------
JAVA_OPTS="-Xmx512M -XX:MaxPermSize=256"
# OS specific support.  $var _must_ be set to either true or false.
```

9. Update rc.d per eseguire automaticamente Tomcat con runlevels di default:
update-rc.d tomcat defaults

IdP Shibboleth 2.2.0

Installazione IdP Shibboleth

1. Scaricare Shibboleth da http://shibboleth.internet2.edu/downloads/shibboleth/idp/ :
   cd /opt
   wget http://shibboleth.internet2.edu/downloads/shibboleth/idp/2.2.0/shibboleth-identityprovider-2.2.0-bin.zip
   wget http://shibboleth.internet2.edu/downloads/shibboleth/idp/2.2.0/shibboleth-identityprovider-2.2.0-bin.zip.asc
2. Scaricare le chiavi PGP e verificare la firma dei file scaricati:
   wget http://shibboleth.internet2.edu/downloads/KEYS
   gpg --import KEYS
   gpgv --keyring ~/.gnupg/pubring.gpg shibboleth-identityprovider-2.2.0-bin.zip.asc
   gpgv: Signature made [...] using DSA key ID A1EAE3E8
   gpgv: Good signature from [...]
   rm KEYS
3. Estrarre shibboleth-identityprovider-2.2.0-bin.zip nella cartella /opt/shibboleth-identityprovider-2.2.0 e rendere eseguibile il file install.sh:

```
cd /opt
jar -xf shibboleth-identityprovider-2.2.0-bin.zip
cd /opt/shibboleth-identityprovider-2.2.0
chmod u+x install.sh
```

4. Effettuare le modifiche necessarie per consentire certificati autofirmati di 3 anni:

```
cd /opt
wget https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.2/idp/ant-extensions-13Apr2008.jar
mv ant-extensions-13Apr2008.jar ./shibboleth-identityprovider-2.2.0/src/installer/lib/
```

5. Modificare il file /opt/shibboleth-identityprovider-2.2.0/src/installer/resources/build.xml :

```
vim /opt/shibboleth-identityprovider-2.2.0/src/installer/resources/build.xml
```

Cercare la riga

```
<selfSignedCert hostname="${idp.hostname}"
```

e cambiarla in

```
<selfSignedCert hostname="${idp.hostname}" years="3"
```

6. Copiare le librerie endorsed di Shibboleth IdP nella directory endorsed $CATALINA_HOME/endorsed (che nel nostro caso sara' $CATALINA_HOME=/opt /tomcat):

```
cd /opt/shibboleth-identityprovider-2.2.0
cp ./endorsed/*.jar /opt/tomcat/endorsed/
```

7. Eseguire install.sh:

```
chmod 755 install.sh
./install.sh
Buildfile: src/installer/resources/build.xml

install:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Be sure you have read the installation/upgrade instructions on the Shibboleth website before proceeding.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Where should the Shibboleth Identity Provider software be installed? [/opt/shibboleth-idp]
/opt/shibboleth-idp
What is the fully qualified hostname of the Shibboleth Identity Provider server? [idp.example.org]
idp-shib.uniexample.it
A keystore is about to be generated for you. Please enter a password that will be used to protect it.
P4sSw0rd P3r Pr0t3gg3re Il K3ySt0r3
Updating property file: /opt/shibboleth-identityprovider-2.2.0/src/installer/resources/install.properties
Created dir: /opt/shibboleth-idp
Created dir: /opt/shibboleth-idp/bin
Created dir: /opt/shibboleth-idp/conf
Created dir: /opt/shibboleth-idp/credentials
Created dir: /opt/shibboleth-idp/lib
Created dir: /opt/shibboleth-idp/lib/endorsed
Created dir: /opt/shibboleth-idp/logs
Created dir: /opt/shibboleth-idp/metadata
Created dir: /opt/shibboleth-idp/war
Generating signing and encryption key, certificate, and keystore.
Copying 5 files to /opt/shibboleth-idp/bin
Copying 8 files to /opt/shibboleth-idp/conf
Copying 1 file to /opt/shibboleth-idp/metadata
Copying 49 files to /opt/shibboleth-idp/lib
Copying 5 files to /opt/shibboleth-idp/lib/endorsed
Copying 1 file to /opt/shibboleth-identityprovider-2.2.0/src/installer
Building war: /opt/shibboleth-identityprovider-2.2.0/src/installer/idp.war
Copying 1 file to /opt/shibboleth-idp/war
Deleting: /opt/shibboleth-identityprovider-2.2.0/src/installer/web.xml
Deleting: /opt/shibboleth-identityprovider-2.2.0/src/installer/idp.war
```

```
BUILD SUCCESSFUL
Total time: 22 seconds
```

8. Creare i Link simbolici a shibboleth:
   ```
   ln -s /opt/shibboleth-idp/conf /etc/shibboleth
   ln -s /opt/shibboleth-idp/logs /var/log/shibboleth
   ```
9. Impostare la variabile d'ambiente per la home di shibboleth:
   ```
   export IDP_HOME=/opt/shibboleth-idp
   ```
10. Aggiungere ad /etc/profile :
    ```
    vim /etc/profile
    IDP_HOME=/opt/shibboleth-idp
    export IDP_HOME
    ```
11. Creare una directory per i content descriptor:
    ```
    cd /opt/tomcat
    mkdir -p conf/Catalina/localhost
    vim /opt/tomcat/conf/Catalina/localhost/idp.xml
    ```
    Creare un content descriptor in /opt/tomcat/conf/Catalina/localhost/idp.xml copiando quanto segue

```
<Context
    docBase="/opt/shibboleth-idp/war/idp.war"
    privileged="true"
    antiResourceLocking="false"
    antiJARLocking="false"
    unpackWAR="false"
    swallowOutput="true" />
```

MySQL Server 5.0

1. Installare il pacchetto MySQL server v5.0:
   ```
   apt-get install mysql-server-5.0
   ```
   N.B. con la configurazione di default MySQL 5 e' in ascolto solo su localhost su IPv4.
2. Impostare la password per root in MySQL:
   ```
   /usr/bin/mysqladmin -u root password 'PaSSw0Rd r00t'
   ```

Creare Utenti e DataBase

Creazione DB:

```
mysql -u root -p
Enter password:

mysql> SET NAMES 'utf8';
SET CHARACTER SET utf8;
CHARSET utf8;
CREATE DATABASE IF NOT EXISTS shibboleth CHARACTER SET=utf8;
USE shibboleth;
```

Creare la tabella per il persistent id:

```
CREATE TABLE IF NOT EXISTS shibpid (
  localEntity TEXT NOT NULL,
  peerEntity TEXT NOT NULL,
  principalName VARCHAR(255) NOT NULL default '',
  localId VARCHAR(255) NOT NULL,
  persistentId VARCHAR(36) NOT NULL,
  peerProvidedId VARCHAR(255) default NULL,
  creationDate timestamp NOT NULL default CURRENT_TIMESTAMP
  on update CURRENT_TIMESTAMP,
  deactivationDate timestamp NULL default 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)
```

```
) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

Visualizzare la tabella appena creata:

```
DESCRIBE shibpid;
```

```
+------------------+--------------+------+-----+-------------------+-------+
| Field            | Type         | Null | Key | Default           | Extra |
+------------------+--------------+------+-----+-------------------+-------+
| localEntity      | text         | NO   | MUL |                   |       |
| peerEntity       | text         | NO   |     |                   |       |
| principalName    | varchar(255) | NO   |     |                   |       |
| localId          | varchar(255) | NO   |     |                   |       |
| persistentId     | varchar(36)  | NO   | MUL |                   |       |
| peerProvidedId   | varchar(255) | YES  |     | NULL              |       |
| creationDate     | timestamp    | NO   |     | CURRENT_TIMESTAMP |       |
| deactivationDate | timestamp    | YES  |     | NULL              |       |
+------------------+--------------+------+-----+-------------------+-------+
8 rows in set (0.00 sec)
```

Creare un utente shibboleth con privilegi limitati:

```
USE mysql;
INSERT INTO user (Host,User,Password,Select_priv,
 Insert_priv,Update_priv,Delete_priv,Create_tmp_table_priv,
 Lock_tables_priv,Execute_priv) VALUES
  ('localhost','shibboleth',PASSWORD('demo'),
   'Y','Y','Y','Y','Y','Y','Y','Y');
FLUSH PRIVILEGES;
GRANT ALL ON shibboleth.* TO 'shibboleth'@'localhost'
IDENTIFIED BY 'demo';
FLUSH PRIVILEGES;
QUIT
```

Controllare se l'utente *shibboleth* e' stato creato con la password *demo*

```
mysql -u shibboleth -p
Enter password
demo
Welcome to the MySQL monitor. Commands end with ; or \g.
[...]
```

Installazione del java mysql connector

1. Download del connector da uno dei mirror http://dev.mysql.com/downloads/connector/j/ con `wget` in /opt
2. Estrarne il contenuto:
   ```
   cd /opt
   tar -xvzf mysql-connector-java-5.1.13.tar.gz
   ```
3. Copiare il file .jar con i relativi connector nella cartella lib dell'idp:
   ```
   cp mysql-connector-java-5.1.13/mysql-connector-java-5.1.13-bin.jar \
   /opt/shibboleth-identityprovider-2.2.0/lib/
   ```

Certificati X.509

Ottenere un certificato di una CA riconosciuta per l'endpoint sulla porta 443.

Autenticazione Utenti

Configurazione JAAS

1. Editare il file login.config incollando quanto segue e personalizzandolo con i dati dell' ldap

```
vim $IDP_HOME/conf/login.config
```

```
ShibUserPassAuth {
// Example LDAP authentication
// See: https://spaces.internet2.edu/display/SHIB2/IdPAuthUserPass
   edu.vt.middleware.ldap.jaas.LdapLoginModule required
      host="ldap.example.org"
      port="389"
      ssl="false"
      tls="false"
      base="ou=people,dc=example,dc=org"
      subtreeSearch="true"
      userField="uid"
      ServiceUser="cn=administrator,dc=example,dc=org"
      serviceCredential="password";
// Example Kerberos authentication, requires Sun's JVM
// See: https://spaces.internet2.edu/display/SHIB2/IdPAuthUserPass
/*
   com.sun.security.auth.module.Krb5LoginModule required
      keyTab="/path/to/idp/keytab/file";
*/
};
```

2. Far si che la JVM usi il file di configurazione JAAS appena modificato, aggiungendo in `/etc/java-6-sun/security/java.security` le seguenti linee:

```
#
# Default login configuration file
#
login.config.url.1=file:/opt/shibboleth-idp/conf/login.config
```

Configurare Tomcat

1. Modificare /opt/tomcat/conf/server.xml e configurare il Connector AJP 1.3 sulla porta 8009:

```
<!-- 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" />
```

Configurare Apache

Le configurazioni di Apache si trovano nella directory `/etc/apache2/sites-available/`

mod_ssl

1. Copiare i certificati precedentemente ottenuti nelle cartelle:

```
cp idpcertificato.key /etc/ssl/private/
cp idpcertificato.crt /etc/ssl/certs/
cd /etc/ssl/certs/
wget https://www.idem.garr.it/index.php/it/documenti/doc_download/CAcert.pem
```

2. Aggiungere al fondo del file /etc/apache2/apache2.conf :

```
ServerTokens Prod
```

3. Configurare il Virtual Host modificando le linee evidenziate:

```
vim /etc/apache2/sites-available/aai-logon
```

```
<IfModule mod_ssl.c>
<Virtual Host _default_:443>
ServerName               idp-shib.uniexample.it:443
SSLEngine On
SSLCipherSuite           ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:!SSLv2:+EXP
SSLProtocol              all -SSLv2
SSLCertificateFile       /etc/ssl/certs/idpcertificato.crt
SSLCertificateKeyFile    /etc/ssl/private/idpcertificato.key
```

```
SSLCertificateChainFile  /etc/ssl/certs/CAcert.pem
SSLOptions               +StdEnvVars
[...]
```

4. Configurare il Virtual Host (porta 8443) modificando le linee evidenziate:

vim /etc/apache2/sites-available/aai-aa

```
<IfModule mod_ssl.c>
<VirtualHost _default_:8443>
ServerName               idp-shib.uniexample.it:8443
SSLEngine On
SSLCipherSuite           ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:!SSLv2:+EXP
SSLProtocol              all -SSLv2
SSLCertificateFile       /opt/shibboleth-idp/credentials/idp.crt
SSLCertificateKeyFile    /opt/shibboleth-idp/credentials/idp.key
SSLVerifyClient          optional_no_ca
SSLVerifyDepth           10
SSLOptions               -StdEnvVars +ExportCertData
[...]
```

5. Abilitare i virtual hosts (aai-logon e aai-aa):

a2ensite aai-logon aai-aa

```
Enabling site aai-logon.
Enabling site aai-aa.
Run '/etc/init.d/apache2 reload' to activate new configuration!
```

6. Abilitare il modulo ssl.

a2enmod ssl

```
Module ssl installed; run /etc/init.d/apache2 force-reload to enable.
```

7. Abilitare il modulo proxy ajp, il modulo mod_proxy verra' anch'esso abilitato.

a2enmod proxy_ajp

```
Enabling proxy as a dependency
Module proxy installed; run /etc/init.d/apache2 force-reload to enable.
Module proxy_ajp installed; run /etc/init.d/apache2 force-reload to enable.
```

8. Controllare se le porte 443 e 8443 siano aperte nel file /etc/apache2/ports.conf

```
Listen 443
Listen 8443
```

9. Riavviare apache:

apache2ctl -t

```
Syntax OK
```

apache2ctl -k restart

Configurare l' IdP Shibboleth

Configurare l' IdP

Configurazione delle Credenziali

Le credenziali che Shibboleth usa sono nella directory /opt/shibboleth-idp/credentials/ directory. L'installer genera automaticamente un certificato autofirmato che verra' poi usato nella federazione IDEM. Tale certificato e' incluso nel frammento di metadati /opt/shibboleth-idp/metadata/idp-metadata.xml.

1. Impostare owner e permessi:

```
cd /opt/shibboleth-idp/credentials
chown root idp.key
chgrp root idp.{key,crt}
chmod 440 idp.key
chmod 644 idp.crt
```

Metadata Trust

wget https://www.idem.garr.it/index.php/it/documenti/doc_download/45-signerbundle

mv 45-signerbundle /opt/shibboleth-idp/credentials/idem.crt

Eseguire il backup del file relying-party.xml esistente

mv /opt/shibboleth-idp/conf/relying-party.xml /opt/shibboleth-idp/conf/relying-party.xml.bak

Scaricare il file relying-party.xml di esempio:

cd /opt/shibboleth-idp/conf

wget https://www.idem.garr.it/index.php/it/documenti/doc_download/136-relying-partyxml-guida-idp-220

e modificare opportunamente i punti indicanti:

https://idp2.idem.garr.it/idp/shibboleth

Attribute-resolver e Attribute-filter

Modificare il file `/opt/shibboleth-idp/conf/attribute-resolver.xml`

```
[...]
   <resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
       ldapURL=" ldap://ldap.example.uniexample.it"
       baseDN="dc=uniexample,dc=it"
       principal="cn=admin,dc=garr,dc=it"
       principalCredential="secret-password">
       <FilterTemplate>
           <![CDATA[
               (uid=$requestContext.principalName)
           ]]>
       </FilterTemplate>
   </resolver:DataConnector>
[...]
 <resolver:DataConnector xsi:type="StoredId" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
                         id="myStoredID"
                         sourceAttributeID="uid"
                         generatedAttributeID="persistentID"
                         salt="InserireStringaRandom">
       <resolver:Dependency ref="myLDAP" />
       <ApplicationManagedConnection
               jdbcDriver="com.mysql.jdbc.Driver" jdbcURL="jdbc:mysql://localhost:3306/shibboleth"
               jdbcUserName="shibboleth" jdbcPassword="demo" />
 </resolver:DataConnector>
[...]
```

Configurare eduPersonTargetedID

```
 <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:attribute:encoder"
        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:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
        friendlyName="eduPersonTargetedID" />
 </resolver:AttributeDefinition></font>
[...]
```

Configurare eduPersonScopedAffiliation

```
[...]
 <resolver:AttributeDefinition id="eduPersonScopedAffiliation"
        xsi:type="Scoped" xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        scope="uniexample.it" sourceAttributeID="eduPersonAffiliation">
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1ScopedString"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
```

```
        name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation" />
     <resolver:AttributeEncoder xsi:type="SAML2ScopedString"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
        friendlyName="eduPersonScopedAffiliation" />
 </resolver:AttributeDefinition>
[...]
```

Configurare eduPersonAffiliation

```
[...]
 <resolver:AttributeDefinition id="eduPersonAffiliation"
        xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"
        sourceAttributeID="eduPersonAffiliation">
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1String"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:mace:dir:attribute-def:eduPersonAffiliation" />
     <resolver:AttributeEncoder xsi:type="SAML2String"
        xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
        friendlyName="eduPersonAffiliation" />
 </resolver:AttributeDefinition>
[...]
```

Modificare infine il file `/opt/shibboleth-idp/conf/attribute-filter.xml` in base agli attributi presenti in `attribute-resolver.xml`

Configurazione dell' Authentication Handler

Modificare il file `/opt/shibboleth-idp/conf/handler.xm`
E decommentare la parte dopo `< !-- Username/password login handler -- >`

```
 <!--  Username/password login handler -->
    <LoginHandler xsi:type="UsernamePassword"
                  jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config">
        <AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthenticationMethod>
    </LoginHandler>
```

Configurazione urlIdP Status

Modificare `/opt/shibboleth-identityprovider-2.2.0/src/main/webapp/WEB-INF/web.xml`

```
[...]
<! -- Servlet for displaying IdP status. -- >
<servlet>
   <servlet-name>Status</servlet-name>
   <servlet-class>edu.internet2.middleware.shibboleth.idp.StatusServlet</servlet-class>

   <init-param>
       <param-name>AllowedIPs</param-name>
       <param-value>127.0.0.1/32 ::1/128 130.59.0.0/16 2001:620::/48 #range di ip consentito#</param-value>
    </init-param>

    <load-on-startup>2</load-on-startup>
</servlet>
[...]
```

Re-installare Shibboleth

Dopo aver modificato alcuni file di configurazione presenti nella directory di installazione `/opt/shibboleth-identityprovider-2.2.0/` e' necessario eseguire nuovamente l'installazione di modo che Shibboleth faccia un nuovo deploy della webapp **idp.war**

Quando verra' chiesto se sovrascrivere la configurazione gia' esistente rispondere No.

```
cd /opt/shibboleth-identityprovider-2.2.0/
./install.sh
```

```
Buildfile: src/installer/resources/build.xml

install:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Be sure you have read the installation/upgrade instructions on the
Shibboleth website before proceeding.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Where should the Shibboleth Identity Provider software be installed?
[/opt/shibboleth-idp]

The directory '/opt/shibboleth-idp' already exists. Would you like to
overwrite this Shibboleth configuration? (yes, [no])
no
```

Avviare Tomcat

Ora avviando Tomcat dal suo eseguibile Catalina tutto dovrebbe funzionare:

```
sh /opt/tomcat/bin/catalina.sh start
Using CATALINA_BASE: /opt/tomcat
Using CATALINA_HOME: /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME: /usr/lib/jvm/java-6-sun
Using CLASSPATH: /opt/tomcat/bin/bootstrap.jar
```

Log

Ricordare inoltre di controllare i log di catalina in `/var/log/tomcat/catalina.out`
Ed i log di shibboleth in `/var/log/shibboleth/idp-process.log`
I log dell'idp contengono importanti "warning" che possono aiutare a carpire la salute del vostro idp appena installato.