Installazione di un Identity Provider

Giacomo Tenaglia

CNR Bologna

5 Marzo 2007

Installazione di un Identity Provider

Introduzione

- Implementazione ufficiale di Internet2.
- Servlet Java.
- Backend LDAP per autenticazione e attributi.
- Schema `eduPerson` di Internet2.

Configurazione di sistema

OS:

- Debian GNU/Linux Etch.
- Kernel 2.6.18.

Applicazioni fondamentali:

- Apache v2.2.3
- Java v.1.5
- Tomcat v5.5

Applicazioni accessorie:

- NTP v4.2.2
- OpenLDAP v2.3.30
- OpenSSL v0.9.8c

Certificati SSL

Generazione richieste certificato per un servizio:

- `openssl genrsa -out service.key`
- `openssl req -new -nodes -out service.req.pem -key service.key`

Firma di un certificato richiesto (da parte della CA):

- `openssl ca -out service.crt.pem -infiles service.req.pem`

Estrazione delle parte encoded dal certificato:

- `mv service.crt.pem service.tmp.pem`
- `openssl x509 -in service.tmp.pem -out service.crt.pem`
- `rm service.tmp.pem`

OpenLDAP: configurazione

Schema `eduPerson` per gli utenti:

- `wget http://middleware.internet2.edu/dir/schema/ldifs/OpenLDAP_eduPerson-200412.tar.gz`
- `tar xzvf OpenLDAP_eduPerson-200412.tar.gz`
- `cp eduperson-200412.ldif /etc/ldap/schema/eduperson-200412.schema`
- `chmod 644 /etc/ldap/schema/eduperson-200412.schema`

Alla configurazione di `slapd` va aggiunta la riga:

[file:///etc/ldap/slapd.conf]

```
include         /etc/ldap/schema/eduperson-200412.schema
```

OpenLDAP: aggiunta utenti

LDIF di un utente di prova:

[file://user.ldif]

```
# user01,People,test,shib
dn: uid=user01,ou=People,dc=test,dc=shib
uid: user01
cn: Test
sn: User01
mail: user01@denil.bo.cnr.it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: eduPerson
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/false
userPassword : pippo
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/user01
gecos: Test User01,,,
```

Aggiunta utente (se necessario creazione della ou=People):

- `ldapadd -x -W -D cn=admin,dc=test,dc=shib -f users.ldif`

OpenLDAP: SSL

Configurazione relativa ai certificati:

[file:///etc/ldap/slapd.conf]

```
TLSCACertificateFile    /etc/ldap/ssl/cacert.pem
TLSCertificateFile      /etc/ldap/ssl/ldap.crt.pem
TLSCertificateKeyFile   /etc/ldap/ssl/ldap.key
TLSCipherSuite          ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
TLSVerifyClient         never
```

Configurazione di `slapd` per supporto SSL:

[file:///etc/default/slapd]

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:///"
```

Apache

Redirezione richieste Shibboleth su Tomcat:

[file:///etc/apache2/mods-available/proxy_ajp.conf]

```
<Location /shibboleth-idp>
    ProxyPass ajp://idp.test.shib:8009/shibboleth-idp
    ProxyPassReverse ajp://idp.test.shib:8009/shibboleth-idp
</Location>
```

Protezione SSO Handler di Shibboleth via `mod_authnz_ldap`:

[file:///etc/apache2/sites-available/idp]

```
<Location /shibboleth-idp/SSO>
        AuthName "Autenticazione su LDAP/SSL"
        AuthType Basic
        AuthBasicProvider ldap
        AuthLDAPURL ldaps://idp.test.shib/ou=People,dc=test,dc=shib?uid?sub?(uid=*)
        AuthzLDAPAuthoritative Off
        require valid-user
</Location>
```

Uso di SSL con `mod_authnz_ldap`:

[file:///etc/apache2/mods-enabled/authnz_ldap.conf]

```
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/ssl/cacert.pem
LDAPTrustedMode SSL
```

Apache: SSL

Handler per il SSO su SSL:

[file:///etc/apache2/sites-available/idp]

```
<VirtualHost _default_:443>

DocumentRoot "/var/www/"
ServerName idp.test.shib:443
ServerAdmin giacomo.tenaglia@area.bo.cnr.it
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/apache2/ssl/www.crt.pem
SSLCertificateKeyFile /etc/apache2/ssl/www.key
SSLCertificateChainFile /etc/apache2/ssl/cacert.pem
SSLCACertificateFile /etc/apache2/ssl/cacert.pem

<Location /shibboleth-idp/SSO>
    AuthName "Autenticazione su LDAP/SSL"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL ldaps://idp.test.shib/ou=People,dc=test,dc=shib?uid?sub?(uid=*)
    AuthzLDAPAuthoritative Off
    require valid-user
</Location>

</VirtualHost>
```

Apache: SSL (2)

Virtualhost su SSL per l'AA (certificati lato client):

[file:///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/apache2/ssl/www.crt.pem
SSLCertificateKeyFile /etc/apache2/ssl/www.key
SSLCertificateChainFile /etc/apache2/ssl/cacert.pem
SSLCACertificateFile /etc/apache2/ssl/cacert.pem
ErrorLog /var/log/apache2/ssl_error.log
TransferLog /var/log/apache2/ssl_access.log

</VirtualHost>
```

Configurazione connector AJP con Apache:

[file:///etc/tomcat5.5/server.xml]

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" address="192.168.254.1"
    enableLookups="false" redirectPort="8443"
    protocol="AJP/1.3" tomcatAuthentication="false" />
```

Disabilitazione uso di security manager (Debian-specific):

[file:///etc/default/tomcat5]

```
TOMCAT5_SECURITY=no
```

IdP: installazione

Implementazione ufficiale di Internet2:

- `wget http://shibboleth.internet2.edu/downloads/shibboleth-idp-1.3.2.tar.gz`
- `tar xzvf shibboleth-idp-1.3.2.tar.gz`
- `cd shibboleth-1.3.2-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`

IdP: configurazione generale

Dati generali dell'IdP:

[file:///usr/local/shibboleth-idp/etc/idp.xml]

```
<IdPConfig
xmlns="urn:mace:shibboleth:idp:config:1.0"
xmlns:cred="urn:mace:shibboleth:credentials:1.0"
xmlns:name="urn:mace:shibboleth:namemapper:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:mace:shibboleth:idp:config:1.0 ../schemas/shibboleth-idpconfig-1.0.xsd"
AAUrl="https://idp.test.shib:8443/shibboleth-idp/AA"
resolverConfig="file:/usr/local/shibboleth-idp/etc/resolver.xml"
defaultRelyingParty="urn:mace:test.shib:federation"
providerId="https://idp.test.shib/shibboleth">
```

Certificati per firmare le assertions SAML:

[file:///usr/local/shibboleth-idp/etc/idp.xml]

```
<RelyingParty name="urn:mace:test.shib:federation" signingCredential="idp_cred">
    <NameID nameMapping="shm"/>
</RelyingParty>

<Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
    <FileResolver Id="idp_cred">
        <Key><Path>file:/usr/local/shibboleth-idp/etc/idp.key</Path></Key>
        <Certificate><Path>file:/usr/local/shibboleth-idp/etc/idp.crt.pem</Path></Certificate>
    </FileResolver>
</Credentials>
```

IdP: configurazione attributi utenti

Definizione degli attributi da prelevare dalla sorgente:

[file:///usr/local/shibboleth-idp/etc/resolver.xml]

```
<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:uid">
    <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>

<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:cn">
    <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>

<SimpleAttributeDefinition id="urn:mace:dir:attribute-def:mail">
    <DataConnectorDependency requires="directory"/>
</SimpleAttributeDefinition>
```

Sorgente LDAP su SSL:

[file:///usr/local/shibboleth-idp/etc/resolver.xml]

```
<JNDIDirectoryDataConnector id="directory">
    <Search filter="uid=%PRINCIPAL%">
        <Controls searchScope="SUBTREE_SCOPE" returningObjects="false" />
    </Search>
    <Property name="java.naming.factory.initial" value="com.sun.jndi.ldap.LdapCtxFactory" />
    <Property name="java.naming.provider.url"
          value="ldap://idp.test.shib/ou=People,dc=test,dc=shib" />
    <Property name="java.naming.security.protocol" value="ssl" />
</JNDIDirectoryDataConnector>
```

IdP: attributi via LDAP su SSL

Creazione keystore con certificato della CA e del server LDAP:

- `cd /usr/local/shibboleth-idp/etc/`
- `keytool -import -keystore ./keystore.jks -alias ca -file  /ssl/cacert.pem`
- `keytool -import -keystore ./keystore.jks -alias idp-ldap -file  /ssl/ldap.crt.pem`

Modifica di `resolvertest` per utilizzo del keystorea appena creato, aggiungendo all'ultima riga:

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

Uso del keystore da Tomcat:

[file:///etc/default/tomcat5.5]

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

IdP: politica di rilascio attributi

Definizione di una semplice politica:

[file:///usr/local/shibboleth-idp/etc/arps/arp.site.xml]

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeReleasePolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="urn:mace:shibboleth:arp:1.0"
    xsi:schemaLocation="urn:mace:shibboleth:arp:1.0 shibboleth-arp-1.0.xsd" >

    <Description>Test ARP.</Description>
    <Rule>
        <Target>
            <AnyTarget/>
        </Target>
        <Attribute name="urn:mace:dir:attribute-def:uid">
            <AnyValue release="permit"/>
        </Attribute>
        <Attribute name="urn:mace:dir:attribute-def:mail">
            <AnyValue release="permit"/>
        </Attribute>
    </Rule>
</AttributeReleasePolicy>
```

Test installazione

- Apache SSL
  `https://idp.test.shib`
- Tomcat
  `http://idp.test.shib:8180/`
- Connector AJP
  `https://idp.test.shib/shibboleth-idp/login.jsp`
- LDAP
  `ldaps://idp.test.shib`
- Autenticazione LDAP (404 se acceduto direttamente)
  `https://idp.test.shib/shibboleth-idp/SSO`
- Attributi su LDAP

```
export IDP_HOME=/usr/local/shibboleth-idp/

$IDP_HOME/bin/resolvertest -user=user01 -file=file:///$IDP_HOME/etc/resolver.xml
```

Note

Non è specificato il SSO Handler:

- Apache Basic Auth ha limiti (logout).
- SSO intra-istituzione: CAS, Pubcookie, ...

HW consigliato:

- Test: PIII/1GHz, 512MB RAM, 150MB storage.
- Produzione: Xeon/Opteron, 2GB RAM, Gigabit ethernet.
- SMP: non aumenta le prestazioni in modo spettacolare.

Riferimenti

- OpenSSL CA:
  `http://www.eclectica.ca/howto/ssl-cert-howto.php`
- LDAP:
  `http://www.bo.cnr.it/corsi-di-informatica/seminarioldap`
- Shibboleth Wiki:
  `https://spaces.internet2.edu/display/SHIB/InstallingShibboleth`