Installazione di un Service Provider

Giacomo Tenaglia

CNR Bologna

5 Marzo 2007

Installazione di un Service Provider

Introduzione

- Implementazione ufficiale di Internet2.
- Protezione risorse su Apache: `mod_shib` .
- Demone per interazione con IdP: `shibd` .
- C/C++.

Configurazione di sistema

OS:

- Debian GNU/Linux Etch.
- Kernel 2.6.18.

Applicazioni fondamentali:

- Apache v2.2.3

Applicazioni accessorie:

- NTP v4.2.2
- 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`

SP: installazione

Implementazione ufficiale di Internet2:

- Sorgenti:
  `http://shibboleth.internet2.edu/downloads/`
- RPM:
  `http://shibboleth.internet2.edu/downloads/RPMS/`
- Pacchetti Debian (K.U.Leuven):
  `http://shib.kuleuven.be/debian-repository/`

Installazione dei pacchetti Debian:

[file:///etc/apt/sources.list]

```
deb http://shib.kuleuven.be/debian-repository binary/
```

- `apt-get update`
- `apt-get install shibboleth-sp`

SP: configurazione Apache

Abilitazione di `mod_shib`:

[file:///etc/apache2/mods-available/shib.load]

```
LoadModule mod_shib /usr/lib/shibboleth-sp/mod_shib_22.so
```

Configurazione di `mod_shib`:

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

```
ShibSchemaDir /usr/share/xml/shibboleth
ShibConfig /etc/shibboleth/shibboleth.xml

#
# Used for example logo and style sheet in error templates.
#
<IfModule mod_alias.c>
    Alias /shibboleth-sp/main.css /usr/share/doc/shibboleth-sp/main.css
    Alias /shibboleth-sp/logo.jpg /usr/share/doc/shibboleth-sp/logo.jpg
</IfModule>
```

Protezione di una directory:

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

```
<Location /secure>
    AuthType shibboleth
    ShibRequireSession On
    require valid-user
</Location>
```

SP: configurazione Shibd

Configurazione dell'Applications Id di default:

[file:///etc/shibboleth/shibboleth.xml]

```
<Applications id="default" providerId="https://sp.test.shib/sp"
    homeURL="https://sp.test.shib"
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
```

Configurazione dei certificati:

[file:///etc/shibboleth/shibboleth.xml]

```
<CredentialsProvider type="edu.internet2.middleware.shibboleth.common.Credentials">
    <Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
        <FileResolver Id="defcreds">
            <Key>
                <Path>/etc/shibboleth/sp.key</Path>
            </Key>
            <Certificate>
                <Path>/etc/shibboleth/sp.crt.pem</Path>
            </Certificate>
        </FileResolver>
```

SP: configurazione politica accettazione attributi

Definizione una semplice politica:

[file:///etc/shibboleth/AAP.xml]

```
<AttributeRule Name="urn:mace:dir:attribute-def:uid" Scoped="true" Header="REMOTE_USER"
    Alias="user">
    <AnySite>
        <Value Type="regexp">^[^@]+$</Value>
    </AnySite>
</AttributeRule>

<AttributeRule Name="urn:mace:dir:attribute-def:cn" Header="Shib-Person-commonName">
    <AnySite>
        <AnyValue/>
    </AnySite>
</AttributeRule>

<AttributeRule Name="urn:mace:dir:attribute-def:mail" Header="Shib-InetOrgPerson-mail">
    <AnySite>
        <AnyValue/>
    </AnySite>
</AttributeRule>
```

Test installazione

- Apache SSL
  `https://sp.test.shib`
- Configurazione shibd
  `shibd -t /etc/shibboleth/shibboleth.xml`
- Apache e `mod_shib`
  `https://sp.test.shib/secure/`

Riferimenti

- Guida installazione:
  `https://spaces.internet2.edu/display/SHIB/InstallingShibboleth`
- Proteggere risorse:
  `https://spaces.internet2.edu/display/SHIB/SPProtectionConfig`
- Shibboleth-enabled SP:
  `https://wiki.internet2.edu/confluence/display/seas/Home`