Installazione Shibboleth Service Provider su Debian-Linux

14 Maggio 2013

Autori: Marco Malavolti, Barbara Monticini

Credits: SWITCH AAI

Indice generale

1 Introduzione

Questo documento ha lo scopo di guidare l'utente nell'installazione di un SP Shibboleth su Debian Linux

2 Software da installare

- openssl;
- ntp;
- apache2
- libapache2-mod-shib2

3 Richiedere il certificato per l'SP

a) In linea con le **specifiche tecniche** della Federazione IDEM è necessario installare sulla porta 443 un certificato rilasciato da una CA riconosciuta. All'interno della comunità GARR è attivo il servizio di rilascio certificati server denominato **TCS** (TERENA Certificate Service). La caratteristica dei certificati TCS è quella di essere emessi da una CA commerciale che nello specifico consiste in **COMODO CA**.

b) L'elenco delle organizzazioni presso le quali il servizio TCS è già attivo è disponibile in https://ca.garr.it/TCS/tab.php

c) Se il servizio non fosse ancora attivo presso la vostra organizzazione è possibile contattare GARR Certification Service per avviare il procedimento di attivazione (e-mail a garr-ca@garr.it)

d) Per generare una richiesta di certificato seguire le istruzioni suggerite nelle pagine di documentazione TCS (https://ca.garr.it/TCS/doc_server.php)

Le richieste di certificato devono essere inviate ai referenti TCS presenti nella vostra organizzazione (denominati Contatti Amministrativi TCS). Per conoscere i nomi dei Contatti Amministrativi nominati all'interno del vostro Ente inviare una mail di richiesta a garr-ca@garr.it

4 Modifica del file hosts

`sudo nano /etc/hosts` aggiungendo alla lista l'IP e il Nome della macchina scelta per ospitare il Service Provider di Shibboleth.

5 Installare apache2, libapache2-mod-shib2, openssl e ntp[1]

a) `sudo apt-get install apache2 libapache2-mod-shib2 openssl ntp`

b) `sudo nano /etc/environment` e aggiungere queste righe in fondo al file:

```
SITE_AVAILABLE=/etc/apache2/sites-available
APACHE=/etc/apache2
SHIB_SP=/etc/shibboleth
```

c) Fare Logout e Login per attuare i cambiamenti all'environment della macchina

d) Verificare che sia attivo apache2 e che faccia comparire la pagina “It Works!” da http://fqdn.del.mio.webserver o da http://127.0.0.1.

[1] per ubuntu 10.04 e superiori

5.1 Installare Shibboleth Service Provider

1) `sudo su -`
2) `cd var/www ; mkdir secure`
3) `nano /etc/apache2/sites-available/default-ssl` e aggiungere quanto segue prima del `<tag>` "`</VirtualHost>`" finale:

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

4) `a2enmod shib2 ; apache2 restart`
5) `cd /etc/shibboleth/`
6) Prelevare la **GARR-CA.pem (preferito)** o il **signer-bundle.pem:**

   `wget https://ca.garr.it/mgt/CAcert.pem ; mv CAcert.pem GARR-CA.pem`

   oppure:

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

   `mv 45-signerbundle signer-bundle.pem`
7) Verificarne l'autenticità:

   `openssl x509 -in GARR-CA.pem -fingerprint -sha1 -noout`

   `openssl x509 -in GARR-CA.pem -fingerprint -md5 -noout`

   confrontando i valori ottenuti con quelli presenti in https://ca.garr.it/mgt/getCA.php.
8) Cambia i permessi al **GARR-CA.pem**:

   `chmod 444 /etc/shibboleth/GARR-CA.pem`

9) Modificare lo "`shibboleth2.xml`":

   `nano /etc/shibboleth/shibboleth2.xml` e modificare le seguenti voci:

   a) Modificare "`sp.example.org`" con "`fqdn.mio.sp`"

   b) Sostituire le linee 43 – 46 con:

```
<SSO entityID="https://fqdn.mio.idp/shibboleth">
   SAML2
</SSO>
```

c) Modificare il tag `<Errors>` come segue:

```
<Errors supportContact="<email.di@supporto.it>"
        logoLocation="/usr/share/shibboleth/logo.jpg"
        styleSheet="/usr/share/shibboleth/main.css"/>
```

d) Modificare il primo example di `<MetadataProvider>` come segue:

```
<MetadataProvider type="XML"
      uri="https://www.idem.garr.it/docs/conf/signed-test-metadata.xml"
      backingFilePath="/etc/shibboleth/idem-signed-test-metadata.xml"
      reloadInterval="7200">


   <MetadataFilter type="Signature" verifyName="false">
      <TrustEngine type="StaticPKIX">
       <CredentialResolver type="File">
        <Certificate format="PEM">
         <Path>/etc/shibboleth/GARR-CA.pem</Path>
        </Certificate>
       </CredentialResolver>
      </TrustEngine>
    </MetadataFilter>



<!--
   <MetadataFilter type="Signature" certificate="signer-bundle.pem"/>
-->
</MetadataProvider>
```

(Se viene scelto il MetadataFilter che utilizza la "`signer-bundle.pem`" ogni 3 anni tale certificato scadrà e lo si dovrà aggiornare, mentre se viene scelto quello che utilizza la "`GARR-CA.pem`" non si incontreranno tali problemi)

10) Creare 1 certificato e 1 chiave autofirmati per l'SP eseguendo il comando:

`/usr/sbin/shib-keygen`

11) `nano /etc/apache2/ports.conf` e rimuovere le righe (per una maggiore sicurezza):

```
nameVirtualHost *:80

Listen 80
```

12) `nano /etc/apache2/sites-available/default-ssl` e modificare come segue:

```
<Directory />
     Options FollowSymLinks
     AllowOverride None
</Directory>
```

diventa:

```
<Directory />
     Options None
     AllowOverride None
     Order deny,allow
     Deny from all
</Directory>
```

`LogLevel warn` ==> **`LogLevel info`**

```
<Directory /var/www/>
     Options Indexes FollowSymLinks MultiViews
     AllowOverride None
     Order allow,deny
     Allow from all
</Directory>
```

diventa:

```
<Directory /var/www/>
     Options None
     AllowOverride None
     Order allow,deny
     Allow from all
     RedirectMatch ^/$ /secure/
</Directory>
```

Facoltativo:

sotto a "`SSLEngine on`" inserire:

```
SSLProtocol all -SSLv2
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:!MEDIUM
```

13) `mkdir /etc/shibboleth/cert-from-CA` e inserire al suo interno il certificato e la chiave privata ricevuti dalla CA

14) rinominarli in "`ssl-cert.pem`" e "`ssl-key.pem`"

15) `nano /etc/apache2/sites-available/default-ssl` e modificare come segue:

```
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
```

diventa:

```
SSLCertificateFile /etc/shibboleth/cert-from-CA/ssl-cert.pem
```

`SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key`

diventa:

`SSLCertificateKeyFile /etc/shibboleth/cert-from-CA/ssl-key.pem`

16) `cd /etc/shibboleth/cert-from-CA`

17) `wget https://ca.garr.it/mgt/Terena-chain.pem`

18) `nano /etc/apache2/sites-available/default-ssl` e modificare come segue:

`#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt`

diventa:

`SSLCertificateChainFile /etc/shibboleth/cert-from-CA/Terena-chain.pem`

19) Modificare i permessi della cartella "`/etc/shibboleth`" per concedere all'utente "`_shibd`" di scrivervi dentro:

```
chown -R _shibd:root /etc/shibboleth/
```

20) `a2enmod ssl ; a2ensite default-ssl ; /etc/init.d/apache2 restart ; /etc/init.d/shibd restart`

21) Inviare i propri Metadata, raggiungibili alla URL: **https://fqdn.del.mio.sp/Shibboleth.sso/Metadata** a idem-help@garr.it

6 Configurazione dello Shibboleth SP per l'utilizzo del DS

1) Seguire attentamente le istruzioni inviate da idem-help@garr.it e quindi:

   `nano /etc/shibboleth/shibboleth2.xml` e modificare come segue:

```
<SSO entityID="https://<fqdn.idp>/idp/shibboleth">
     SAML2 SAML1
</SSO>
```

deve diventare:

```
<SSO discoveryProtocol="SAMLDS"
     discoveryURL="https://ds.idem-test.garr.it/discovery/WAYF">
     SAML2 SAML1
</SSO>
```

2) Riavviare l'IdP e provare ad accedere, via https, al vostro SP.
   Comparirà il Discovery Service al cui interno si troverà anche il proprio IdP.

7 Riconoscimento attributi LDAP

Aprire il file "`/etc/shibboleth/attribute-map.xml`" e rimuovere il commento al blocco sotto a "`<!--Examples of LDAP-based attributes, uncomment to use these... -->`"