Installazione Shibboleth Service Provider su Debian-Linux

28 Gennaio 2015

Autori: Marco Malavolti

Credits: Shibboleth, 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
- php5

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. (Es.: 127.0.1.1 sp-test.example.org sp-test)

5 Installare apache2, libapache2-mod-shib2, openssl, php5 e ntp[1]

a) Installare i pacchetti necessari:
   - `sudo apt-get install apache2 libapache2-mod-shib2 openssl php5 ntp`

b) Verificare che compaia "**It Works!**" da *http://sp-test.example.org* o da *http://127.0.1.1*.

[1] per ubuntu 10.04 e superiori

5.1 Installare Shibboleth Service Provider

1) Acquisire i permessi di ROOT e creare la cartella "`secure`":
   - `sudo su -`
   - `cd /var/www`
   - `mkdir secure`
2) Inserire il seguente file **/var/www/secure/index.php**:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
   <html>
      <head>
        <title></title>
        <meta name="GENERATOR" content="Quanta Plus">
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
      </head>
      <body>
         <p>
           <a href="https://sp-test.example.it/privacy.html">Politica della
      Privacy</a>
         </p>
      <?php
         foreach ($_SERVER as $key => $value){
            print $key." = ".$value."<br>";
         }

         /*foreach ($_ENV as $key => $value){
            print $key." = ".$value."<br>";
         }

         foreach ($_COOKIE as $key => $value){
            print $key." = ".$value."<br>";
         }*/

      ?>

      </body>
   </html>
```

3) Modificare `/etc/apache2/sites-available/default-ssl` aggiungendo quanto segue prima del "`</VirtualHost>`" finale:

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

4) Attivare il modulo shib2 e riavviare Apache2:
   - `a2enmod shib2`
   - `service apache2 restart`
5) Prelevare l' **idem_signer_2019.pem:**
   - `wget https://www.idem.garr.it/documenti/doc_download/321-idem-metadata-signer-2019 -O /etc/shibboleth/idem_signer_2019.pem`
6) Cambia i permessi al **idem_signer_2019.pem**:
   - `chmod 444 /etc/shibboleth/idem_signer_2019.pem`
7) Modificare le voci seguenti del file "`shibboleth2.xml`":
   a) Modificare "`sp.example.org`" con il proprio FQDN (es. "`sp-test.example.org`")
   b) Sostituire come segue:

```
<SSO entityID="https://idp.example.org/shibboleth"
     discoveryProtocol="SAMLDS"
     discoveryURL="https://ds.example.org/DS/WAYF">
               SAML2 SAML1
</SSO>
```

deve diventare:

```
<SSO discoveryProtocol="SAMLDS"
     discoveryURL="https://wayf.idem-test.garr.it/WAYF">
     SAML2 SAML1
</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) Inserire il seguente `<MetadataProvider>`:

```
<MetadataProvider type="XML"
      uri="http://www.garr.it/idem-metadata/idem-test-metadata-sha256.xml"
      backingFilePath="idem-test-metadata-sha256.xml"
      reloadInterval="7200">

   <MetadataFilter type="Signature" certificate="idem_signer_2019.pem"/>

</MetadataProvider>
```

e) Aggiungere le **necessarie** informazioni MDUI del proprio SP nel file **/etc/shibboleth/shibboleth2.xml** ,senza aggiungere tabulazioni o spazi, seguendo le indicazioni del template fornito QUI:

```
            <!-- Extension service that generates "approximate" metadata based
on SP configuration. -->
            <Handler type="MetadataGenerator" Location="/Metadata"
signing="false">
<mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
   <mdui:DisplayName xml:lang="en">ENG DisplayName SP</mdui:DisplayName>
   <mdui:DisplayName xml:lang="it">ITA DisplayName SP</mdui:DisplayName>
   <mdui:Description xml:lang="en">ENG Description SP</mdui:Description>
   <mdui:Description xml:lang="it">ITA Description SP</mdui:Description>
   <mdui:InformationURL xml:lang="en">ENG_PAGE_INFO_URL</mdui:InformationURL>
   <mdui:InformationURL xml:lang="it">ITA_PAGE_INFO_URL</mdui:InformationURL>
   <mdui:Logo height="16" width="16"
xml:lang="en">ENG_LOGO_URL_HTTPS_16x16</mdui:Logo>
   <mdui:Logo height="16" width="16"
xml:lang="it">ITA_LOGO_URL_HTTPS_16x16</mdui:Logo>
   <mdui:Logo height="60" width="80"
xml:lang="en">ENG_LOGO_URL_HTTPS_80x60</mdui:Logo>
   <mdui:Logo height="60" width="80"
xml:lang="it">ITA_LOGO_URL_HTTPS_80x60</mdui:Logo>
</mdui:UIInfo>

<md:AttributeConsumingService index="1">
   <md:ServiceName xml:lang="en">ENG DisplayName SP</md:ServiceName>
   <md:ServiceName xml:lang="it">ITA DisplayName SP</md:ServiceName>
   <md:ServiceDescription xml:lang="en">ENG Description
SP</md:ServiceDescription>
   <md:ServiceDescription xml:lang="it">ITA Description
SP</md:ServiceDescription>
   <!-- example for the desiderd attribute: mail -->
   <md:RequestedAttribute FriendlyName="mail"
      Name="urn:oid:0.9.2342.19200300.100.1.3"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

   <!-- example for the required attribute: eduPersonPrincipalName -->
   <md:RequestedAttribute FriendlyName="eppn"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
```

```
      isRequired="true" />
</md:AttributeConsumingService>

<md:Organization>
   <md:OrganizationName xml:lang="en">ENG Org Name</md:OrganizationName>
   <md:OrganizationName xml:lang="it">ITA Org Name</md:OrganizationName>
   <md:OrganizationDisplayName xml:lang="en">ENG Org
DisplayName</md:OrganizationDisplayName>
   <md:OrganizationDisplayName xml:lang="it">ITA Org
DisplayName</md:OrganizationDisplayName>
   <md:OrganizationURL xml:lang="en">ENG_PAGE_ORG_URL</md:OrganizationURL>
   <md:OrganizationURL xml:lang="it">ITA_PAGE_ORG_URL</md:OrganizationURL>
</md:Organization>

<md:ContactPerson contactType="technical">
   <md:GivenName>System</md:GivenName>
   <md:SurName>Support</md:SurName>
   <md:EmailAddress>mailto:system.support@domainOrg.it</md:EmailAddress>
</md:ContactPerson>
            </Handler>
```

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

   `/usr/sbin/shib-keygen`

9) Verificare che le modifiche effettuate siano corrette eseguendo il comando:
   - `shibd -t /etc/shibboleth/shibboleth2.xml`

10) Modificare il file `/etc/apache2/ports.conf` e rimuovere/commentare le seguenti righe per impedire l'accesso in HTTP:

```
nameVirtualHost *:80

Listen 80
```

11) Modificare il file `/etc/apache2/sites-available/default-ssl` 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 -SSLv3
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:!MEDIUM
```

12) Creare la cartella `/etc/shibboleth/cert-from-CA` e inserire al suo interno il certificato e la chiave privata ricevuti dalla CA per le pagine HTTPS del Service Provider.

13) Rinominarli in '`ssl-cert.pem`' e '`ssl-key.pem`'

14) Modificare il file `/etc/apache2/sites-available/default-ssl` 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
```

15) Scaricare la catena TERENA:
    - `cd /etc/shibboleth/cert-from-CA`
    - `wget https://ca.garr.it/mgt/Terena-chain.pem`
16) Modificare il file `/etc/apache2/sites-available/default-ssl` come segue:

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

diventa:

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

17) Abilitare il Service Provider a riconoscere gli attributi rilasciati da un 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... -->`"
18) Attivare il modulo "**ssl**" e il sito HTTPS di Apache eseguendo i seguenti comandi:
    - `a2enmod ssl`
    - `a2ensite default-ssl`
    - `service apache2 restart`
    - `service shibd restart`
19) Registrate i vostri Metadati, ottenibili alla URL
    "**https://fqdn.del.mio.sp/Shibboleth.sso/Metadata**"

    sull **IDEM Entity Registry**: https://registry.idem.garr.it

20) In caso di problemi rivolgersi a idem-help@garr.it.