Guida all'Installazione dello Shibboleth Service Provider su Window Server 2003

v 1.0

12 Ottobre 2011

Autori: Marco Malavolti, Danilo Crecchia e Daniela Nasi

Credits: Switch AAI

1 Richiesta del Certificato a GARR CA

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**.

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

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

c) 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

2 Sincronizzazione della Data e dell'Ora

- Aprire il Prompt dei Comandi e digitare: `net time /setsntp:ntp.unimo.it`

3 Installazione di IIS 6.0

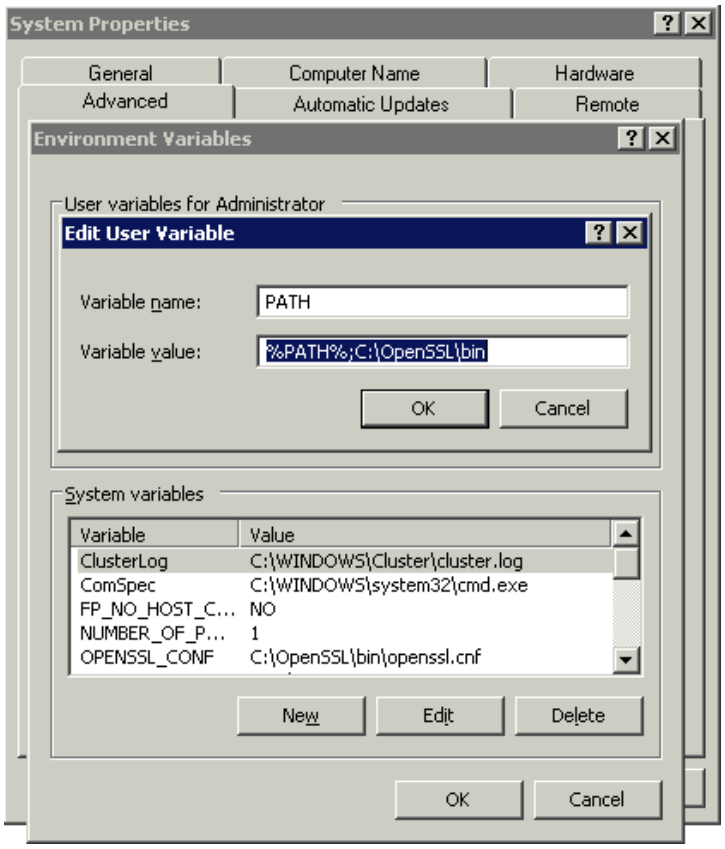
- Aprire "*Installazione Applicazioni*" dal Pannello di Controllo
- Accedere all' "*Installazione componenti di Windows*"
- Spuntare "*Server applicazioni*" e procedere con l'installazione

4 Installazione di Shibboleth Service Provider

- Scaricare il pacchetto adatto alla propria architettura da qui: http://shibboleth.internet2.edu/downloads.html
- Installare il pacchetto lasciando attivate tutte le impostazioni predefinite.
- Riavviare il server come richiesto dall'installazione.

5 Installazione di OpenSSL su Windows

- Scaricare il pacchetto adatto alla propria architettura da qui: http://ww.slproweb.com/products/Win32OpenSSL.html e installarlo nella cartella `C:/OpenSSL` e lasciando tutte le impostazioni predefinite.
- Scaricate e installate anche il Visual C++ 2008 Redistributables se non lo avete per il corretto funzionamento dell'OpenSSL.
- Impostare la variabile PATH nelle Variabili di Ambiente come segue:



- Da ora in poi potete usare OpenSSL come comando nel Prompt dei Comandi

6 Configurazione di IIS 6.0

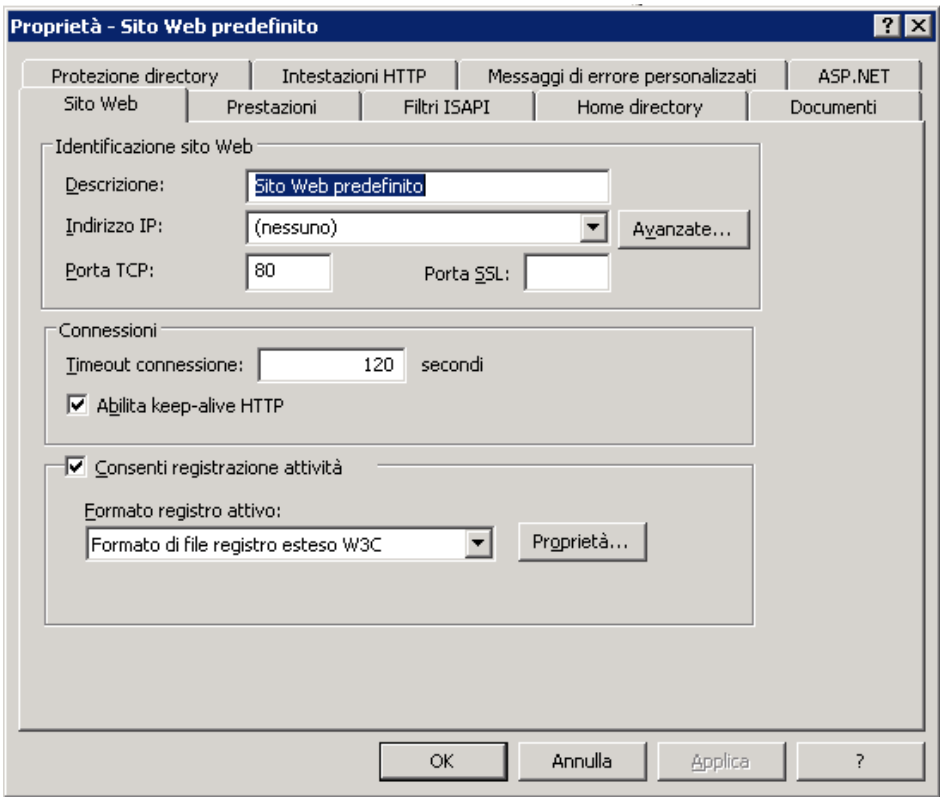
- Verificare che l'IIS sia attivo aprendo: http://localhost
  (deve mostrare la pagina "In fase di allestimento")
- Controllare di avere il file "`hosts`" dentro a

  "`%systemroot%\system32\drivers\etc`"

  e modificarlo per mappare il proprio IP sul nome della macchina ospitante il SP
- Testare si produca la medesima situazione avventuta per il localhost anche sul http://miosp.test.uni.it che ovviamente andrà modificato col vostro nome-macchina
- Scaricare dentro la cartella `C:\opt\shibboleth-sp\etc\shibboleth\` il file signer_bundle.pem
- Scaricare dentro la cartella C:\opt\shibboleth-sp\etc\shibboleth\ il file signed-metadata.xml
- Creare il KEYSTORE.pfx necessario per l'HTTPS del proprio SP digitanto nel prompt dei Comandi:

```
cd C:\MyCerts
openssl pkcs12 -export -in SP-cert.pem -inkey SP-key.pem -out KEYSTORE.pfx
```

- Inserire la password per l'esportazione e vi ritroverete il file KEYSTORE.pfx
- Creare 1 cartella "`secure`" dentro a "`C:\inetpub\wwwroot`" e spostatevi dentro i file "`iistart.htm`" e "`pagerror.gif`"
- Aprire "Gestione Internet Information Service (IIS)" dal Pannello di Controllo
- Espandere la cartella "Siti Web" → Tasto destro sul Sito Web Predefinito → Proprietà



- Dalla scheda "**Home Directory**" impostare il percorso locale come "`C:\inetpub\wwwroot`" e, senza cliccare su OK che chiuderebbe la finestra, spostarsi dentro la scheda "**Sito Web**" e:
    1. immettere una descrizione al sito (es.: Shibboleth Service Provider)
    2. impostare l'indirizzo IP della macchina che ospita l'SP
    3. Verificare che vi siano la Porta TCP: 80 e la Porta SSL: 443
    4. Cliccare su OK
- Tasto destro su "**Siti Web**" e nella scheda "**Home Directory**" cliccare sul bottone "Configurazione" sotto "Impostazioni applicazione" → Aggiungi... → Eseguibile: `C:\opt\shibboleth-sp\lib\shibboleth\isapi_shib.dll` e Estensione: `.sso` → togliere la spunta a "Verifica esistenza del file" → OK
- Spostarsi sulla scheda "Filtri ISAPI"
- Cliccare sul bottone Aggiungi → Dare un nome al filtro e come percorso "`C:/opt/shibboleth-sp/lib/shibboleth/isapi_shib.dll`" e dare OK → Applica → OK
- Espandere la cartella "**Siti Web**" → Tasto destro sul Sito Web Predefinito → Proprietà → scheda "Protezione directory" → cliccare sul bottone "Certificato server..." e importare il KEYSTORE.pfx preparato precedentemente.
- Riavviare *IIS* (selezionare "NomeMacchina (computer locale)" → tasto destro → tutte le attività → Riavvia IIS) e il servizio "*Shibboleth 2 Daemon (Default)*"
- Verificare se il sito rimane accessibile anche da https.

7 Configurazione di Shibboleth Service Provider

- Aprire con un editor di testo il file C:/opt/shibboleth-sp/etc/shibboleth/shibboleth2.xml
- Tutti gli "sp.example.org" ==> "miosp.uni.it"
- Tutti gli "idp.example.org" ==> "mioidp.uni.it"
- Decommentare l'Example del <MetadataProvider> e modificarlo come il seguente:

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

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

</MetadataProvider>
```

- Riavviare l'IIS e lo Shibboleth 2 Daemon
- Accedere a https://miosp.uni.it/Shibboleth.sso/Metadata e inviare il file scaricato a idem-help@garr.it

8 Configurazione di Shibboleth SP per WAYF del GARR

- Aprire con un editor di testo il file C:/opt/shibboleth-sp/etc/shibboleth/shibboleth2.xml

- In <Session> commentare la seguente porzione di codice:

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

E aggiungervi sotto:

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

- In <Metadata> modificare come segue:

```
<!-- Chains together all your metadata sources. -->
<MetadataProvider type="Chaining">
   <!-- Example of remotely supplied batch of signed metadata. -->
   <MetadataProvider type="XML"
```

```
      uri="https://www.idem.garr.it/docs/conf/signed-test-metadata.xml"
      validate="true"
      backingFilePath="signed-metadata.xml"
      reloadInterval="7200">
    <MetadataFilter type="Signature" verifyName="false">
      <TrustEngine type="StaticPKIX">
        <CredentialResolver type="File">
          <Certificate format="PEM">
            <Path>C:/opt/shibboleth-sp/etc/shibboleth/GARR-CA.pem</Path>
          </Certificate>
        </CredentialResolver>
      </TrustEngine>
    </MetadataFilter>
  </MetadataProvider>
</MetadataProvider>

<!-- Chain the two built-in trust engines together. -->
<TrustEngine type="Chaining">
      <TrustEngine type="ExplicitKey"/>
       <TrustEngine type="PKIX"/>
</TrustEngine>
```

- Scaricare https://ca.garr.it/mgt/CAcert.pem in
  `C:/opt/shibboleth-sp/etc/shibboleth`
- Verificare i fingerprint del certificato scaricato con:

  1. `openssl x509 -in CAcert.pem -fingerprint -sha1 -noout`
  2. `openssl x509 -in CAcert.pem -fingerprint -md5 -noout`

  e confrontando i loro valori con quelli in https://ca.garr.it/mgt/getCA.php
- Rinominare **CAcert.pem** in **GARR-CA.pem** (Se vi crea problemi, eliminate eventuali blocchi di Windows al Certificato: Tasto Destro su GARR-CA.pem → Annulla Blocco)
- Il Certificato deve essere leggibile da tutti, ma non modificabile.
- Ora aprite il vostro sito `https://sp.lab.test.it/secure` e vi dovrebbe comparire il Discovery WAYF.