Installazione di uno Shibboleth SP 2 su Microsoft Windows 2003/2008 Server

Danilo Crecchia

S.I.A.
Università di Modena e Reggio Emilia

Roma 30/03/2009

Indice

Prima di cominciare

- Sulla macchina che ospita il SP:
  - web server IIS 6.0 o IIS 7.0
  - Sincronizzazione dell'orario con quello dell'IdP

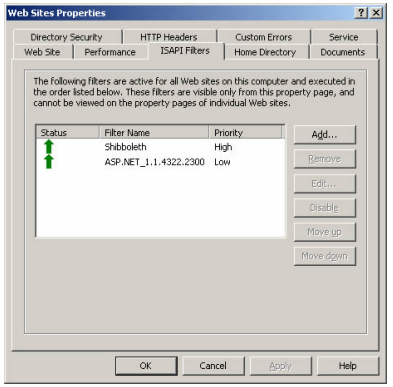
    net time /setsntp:ntp1.inrim.it

Installazione SP 2.0

- Download del pacchetto autoinstallante
  - http://shibboleth.internet2.edu/downloads/shibboleth/cppsp/latest/win32/
- Installazione
  - Servizio shibd sulla porta 1600
  - Filtro ISAPI
  - Tool
    - openssl
    - shibd

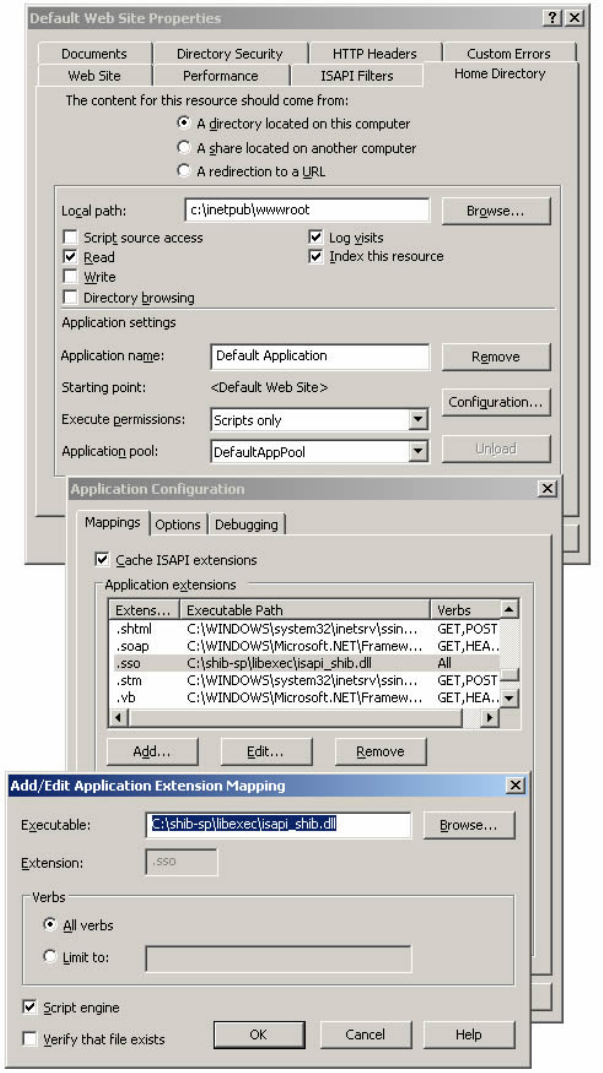
Configurazione IIS 6.0

- Controllo del corretto caricamento del filtro ISAPI
  - L'eseguibile è localizzato in c:\opt\shibboleth-sp\libexec\isapi_shib.dll
  - Viene richiesto che il filtro abbia la priorità più alta



Configurazione IIS 6.0

- Problemi con il filtro
  - Controllare dalle proprietà del sito che I permessi di esecuzione siano su 'script only'
  - Controllare che all'estensione .sso sia associato il filtro isapi_shib.dll
  - Sul file isapi_shib.dll dovranno esserci i permessi di lettura ed esecuzione per l'utente IIS_WPG
  - Se il file native.log non viene creato aggiungere I permessi di scrittura per la cartella /opt/shibboleth-sp/var/log/shibboleth
  - Richiamare dal browser Shibboleth.sso http://esempio1.test.it/Shibboleth.sso
  - Riavvio di IIS



Configurazione IIS 7.0

- 

Aggiunta del filro isapi_shib.dll
- 

Mapping dell'estensione .sso
- 

Aggiunta del permesso sull'estensione Shibboleth ISAPI
- Restart IIS

Configurazioni generali – shibboleth2.xml (1/6)

- Dopo ogni modifica il servizio shibd deve essere riavviato
- Definizione degli host e della/e directory protetta/e

```
<InProcess logger="native.logger">
    <ISAPI normalizeRequest="true">
        <Site id="1" name="esempio1.test.it" />
        <Site id="2" name="esempio2.test.it">
            <Alias>esempio2.test2.it</Alias>
        </Site>
    </ISAPI>
</InProcess>
```



```
<RequestMap applicationId="default">
    <Host name="esempio1.test.it">
        <Path name="secure" authType="shibboleth" requireSession="true" />
    </Host>
    <Host name="esempio2.test.it">
        <Path name="secure" authType="shibboleth" requireSession="true" />
    </Host>
    <Host name="esempio2.test2.it">
        <Path name="secure" authType="shibboleth" requireSession="true" />
    </Host>
</RequestMap>
```

Configurazioni generali – shibboleth2.xml (2/6)

- Gestione delle autorizzazioni

```
<Host name="esempio1.test.it">
    <Path name="secure" authType="shibboleth" requireSession="true" />
    <AccessControl>
        <AND>
            <OR>
                    <Rule require="scopedAffiliation">staff@uniprova.it</Rule>
                    <Rule require=”scopedAffiliation”>staff@unitest.it</Rule>
             </OR>
             <NOT>
                    <Rule require=”PersonalName”>pirata@unitest.it</Rule>
             </NOT>
         </AND>
    </AccessControl>
</Host>
```

Configurazioni generali – shibboleth2.xml (3/6)

- Application defaults

```
<ApplicationDefaults id="default" policyId="default"
        entityID="https://esempio1.test.it/shibboleth"
        homeURL="https://esempio1.test.it/welcome/"
        REMOTE_USER="eppn persistent-id targeted-id"
        signing="false" encryption="false"
>
[…]
```

Configurazioni generali – shibboleth2.xml (4/6)

- Definizione del Session Initiator

Caso IdP

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="Intranet"
        relayState="cookie" entityID="https://idp.test.it/idp/shibboleth">
    <SessionInitiator type="SAML2" defaultACSIndex="1"
        template="/opt/shibboleth-sp/etc/shibboleth/bindingTemplate.html"/>
    <SessionInitiator type="Shib1" defaultACSIndex="5"/>
</SessionInitiator>
```

Caso WAYF

```
<SessionInitiator type="Chaining" Location="/WAYF" id="WAYF" relayState="cookie">
    <SessionInitiator type="SAML2" defaultACSIndex="1" template="bindingTemplate.html"/>
    <SessionInitiator type="Shib1" defaultACSIndex="5"/>
    <SessionInitiator type="WAYF" defaultACSIndex="5" URL="https://wayf.example.org/WAYF"/>
</SessionInitiator>
```

Configurazioni generali – shibboleth.xml (5/6)

- Download del metadata dalla rete

```
<MetadataProvider type="XML" uri="https://shibboleth.test.it/metadata.xml"
 backingFilePath="c:\opt\shibboleth-sp\shibboleth\etc\metadata.xml" reloadInterval="7200">
        <SignatureMetadataFilter certificate="c:\opt\shibboleth-sp\etc\shibboleth\garrcert.pem"/>
 </MetadataProvider>
```

- Credenziali

```
<CredentialResolver type="File"
      key="C:\opt\shibboleth-sp\etc\shibboleth\chiave.key"
      certificate="C:\opt\shibboleth-sp\etc\shibboleth\chiave.crt"/>
```

Configurazioni generali – shibboleth2.xml (6/6)

- Application Override
  - Viene utilizzato nel caso in cui ci siano 'host che richiedono configurazioni diverse da quelle dell'ApplicationDefaults

```
<ApplicationOverride id="other-app" entityID="http://esempio2.test.it/shibboleth">

  <Sessions lifetime="28800" timeout="3600" checkAddress="false"
    handlerURL="/Shibboleth.sso" handlerSSL="false"
    exportLocation="http://localhost/Shibboleth.sso/GetAssertion" exportACL="127.0.0.1"
    idpHistory="false" idpHistoryDays="7">

        <SessionInitiator type="Chaining" Location="/Login" isDefault="true"
          id="Intranet" relayState="cookie" entityID="https://idp.test.it/shibboleth
          forceAuthn="true">
        <SessionInitiator type="SAML2" defaultACSIndex="1" acsByIndex="false"
         template="bindingTemplate.html" />
       <SessionInitiator type="Shib1" defaultACSIndex="5" />
      </SessionInitiator>

   </Sessions>
</ApplicationOverride>
```

- Per associare all'host queste configurazioni valorizzare l'attributo ApplicationId con l'id dell'ApplicationOverride

Metadata

- Download del metadata associato all'host

  http://esempio1.test.it/Shibboleth.sso/Metadata

- Nel caso l'host abbia degli alias

  Ci sono due modi:

  1) Aggiunta di un ApplicationOverride
     <ApplicationOverride id="other-app" entityID="https://esempio1.test2.it/shibboleth">
     - In questo caso deve essere scaricato un metadata anche per l'alias

  2) Copia, nel metadata scaricato di tutte le entry <md:AssertionConsumerService>
     - Le entry copiate vengono accodate a quelle già presenti e solo per queste viene sostituito il nome dell'host con quello dell'alias

- Invio del metadata all'amministratore del Idp

Riferimenti

- http://shibboleth.internet2.edu/