Installazione di uno Shibboleth Service Provider 1.3 su Microsoft Windows 2003 Server

Danilo Crecchia

CE.S.I.A.
Università di Modena e Reggioemilia

Milano 01/04/2007

Indice

Prima di cominciare

- Richiesta di partecipazione alla federazione IDEM
- Sulla macchina che ospita il SP:
  - web server IIS 6.0
  - Sincronizzazione dell'orario con quello dell'IdP

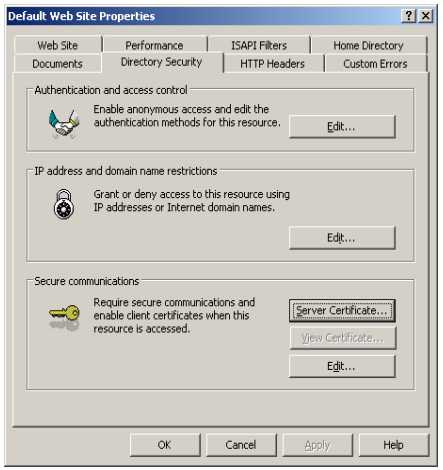
    net time /setsntp:ntp1.inrim.it
- Richiesta di un certificato di tipo SCS
  - ca.garr.it

Installazione SP 1.3

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

Importazione del certificato SSL in IIS

- Il certificato deve contenere al suo interno tutta la catena di certificati PKI
  - http://secure.globalsign.net/cacert/sureserverEDU.pem
  - http://secure.globalsign.net/cacert/ct_root.pem
  - Il loro contenuto deve essere copiato e incollato al di sotto del contenuto del file .crt
- Creazione di una keystore da una coppia chiave/certificato
  - cd \opt\shibboleth-sp\bin
  - openssl pkcs12 -export -in certificato.crt -inkey chiave.key -out iis_cert.pfx
- Importazione della keystore su IIS



Configurazioni generali – shibboleth.xml (1/4)

- Definizione degli attributi per la mappatura del file che gestiscono i log

<SPConfig xmlns="urn:mace:shibboleth:target:config:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mace:shibboleth:target:config:1.0 C:/opt/shibboleth-sp/share/xml/shibboleth/shibboleth-targetconfig-1.0.xsd" logger="**C:/opt/shibboleth-sp/etc/shibboleth/shibboleth.logger**" clockSkew="180">

<Global Logger="**C:/opt/shib-sp/etc/shibboleth/shibd.logger** ">

<Local Logger="**C:/opt/shib-sp/etc/shibboleth/native.logger** " localRelayState="true">

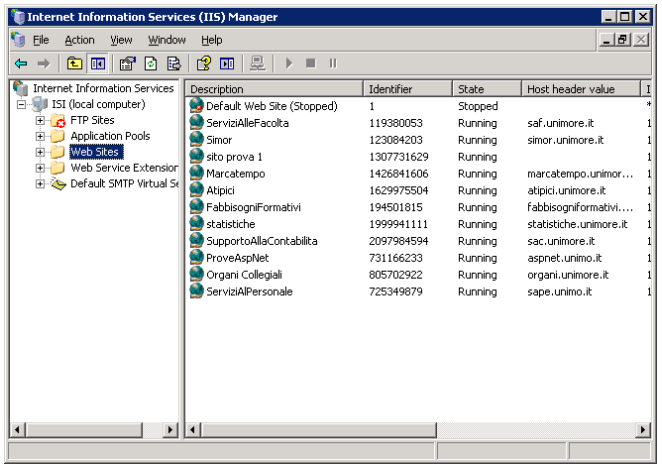
Configurazioni generali – shibboleth.xml (2/4)

- Definizione dell'host e della directory protetta

```
<Host name="sito.uniprova.it" applicationId="sito_uniprova">
    <Path name="shib" 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>
```

- *Definizione dell'entry ISAPI*

```
<Site id="119380053" name="sito.uniprova.it" scheme="https">
    <Alias>sito-b.uniprova.it</Alias>
    <Alias>sito-c.unimprova.it</Alias>
</Site>
```



Configurazioni generali – shibboleth.xml (3/4)

- Definizione dell'entry Applications

<Applications id="default" providerId="**https://sito.uniprova.it/sp**" homeURL="**http://sito.uniprova.it**" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

- *Definizione dell'entry SessionInitiator*

<SessionInitiator isDefault="true" id="default" Location="**/WAYF/IDEM**" Binding="urn:mace:shibboleth:sp:1.3:SessionInit" wayfURL="**https://wayf.idem.garr.it/WAYF**" wayfBinding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" />

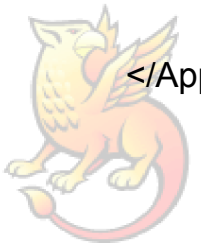
- *Definizione dell'entry CredentialsProvider*

```
<CredentialsProvider type="edu.internet2.middleware.shibboleth.common.Credentials">

    <Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
     <FileResolver Id="defcreds">
            <Key>
                <Path>C:/opt/shibboleth-sp/etc/shibboleth/chiave.key</Path>
            </Key>
            <Certificate>
                <Path>C:/opt/shibboleth-sp/etc/shibboleth/certificato.crt</Path>
            </Certificate>
     </FileResolver>
    </Credentials>

</CredentialsProvider>
```

Configurazioni generali – shibboleth.xml (4/4)

- Caso con più applicazioni che sfruttano il servizio shibboleth sullo stesso server
  - Aggiunta di una entry host per ogni applicativo
  - Aggiunta di una entry host per ogni alias
  - Aggiunta di una entry application per ogni host
- Ogni applicazione avrà la sua sessione specifica

```
<Application id="uniprova1" providerId="https://sito.uniprova1.it">
        <Sessions lifetime="7200" timeout="3600" checkAddress="false" handlerURL="/Shibboleth.sso"
handlerSSL="true" idpHistory="true" idpHistoryDays="7">
                <SessionInitiator isDefault="true" id="default" Location="/WAYF/IDEM"
Binding="urn:mace:shibboleth:sp:1.3:SessionInit" wayfURL="https://wayf.idem.garr.it/WAYF"
wayfBinding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" />
                <md:AssertionConsumerService Location="/SAML/POST" isDefault="true" index="1"
Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" />
                <md:AssertionConsumerService Location="/SAML/Artifact" index="2"
Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01" />
                <md:SingleLogoutService Location="/Logout" Binding="urn:mace:shibboleth:sp:1.3:Logout" />
        </Sessions>
</Application>
```



Configurazioni generali – AAP.xml

- Download dal sito della federazione IDEM
  - http://www.idem.garr.it/docs/conf/AAP.reference.xml
- Copia nella directory
  - c:\opt\shibboleth-sp\etc

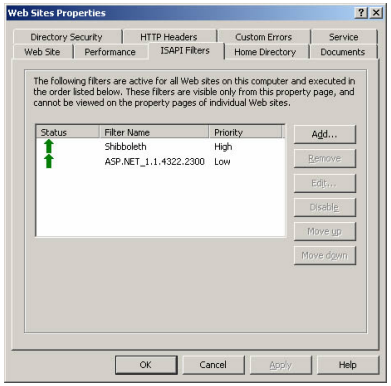
Configurazioni generali – idem-metadata.xml

- Download dell'applicativo wget.exe
  - http://users.ugent.be/~bpuype/wget/
- Realizzazione di una procedura batch da schedulare che permette l'aggiornamento giornaliero del file idem-metadata.xml
  - *wget http://www.idem.garr.it/docs/conf/idem-metadata.xml -P c:\tmp -m -nd –no-check-certificate*
- Controllo well formed e copia nella directory appropriata con l'uso del tool 'siterefresh'
  - siterefresh –url file:c:\tmp\idem-metadata.xml –noverify –out c:\opt\idem-metadata.xml

Configurazione IIS 6.0 (1/2)

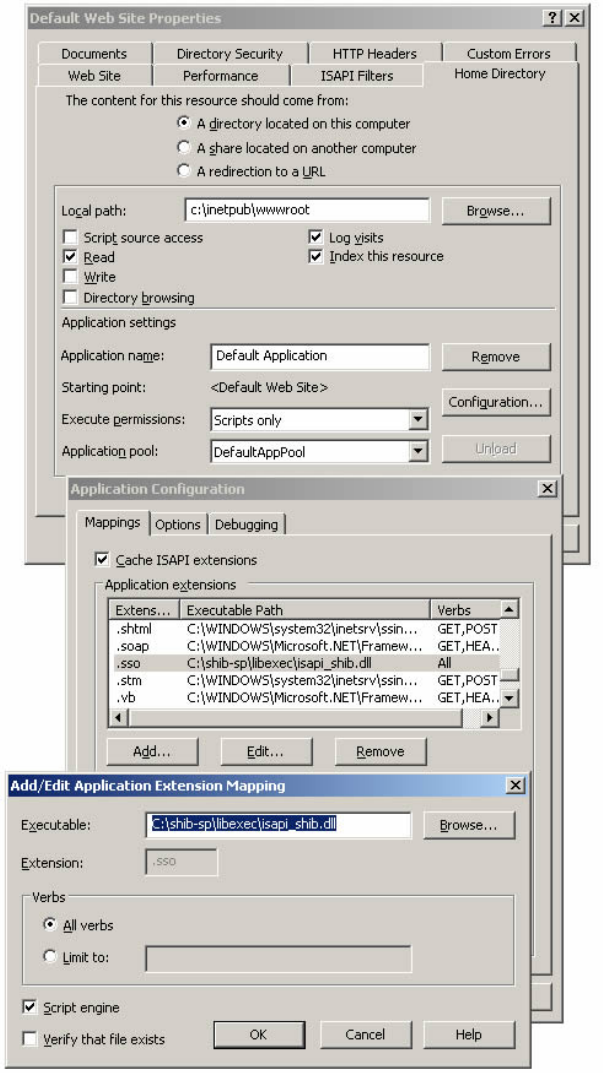
- Riavvio di IIS
  - iisreset
  - Se il server è in produzione è opportuno fare prima un controllo sui file di configurazione con il servizio shibd

    /opt/shibboleth-sp/sbin/shibd -check
- Controllo del corretto caricamento del filtro ISAPI
  - Viene richiesto che il filtro abbia la priorità più alta
  - Se il filtro non è presente nella lista aggiungerlo.
  - L'eseguibile è localizzato in c:\opt\shibboleth-sp\libexec\isapi_shib.dll



Configurazione IIS 6.0 (2/2)

- Test su filtro
  - http://sito.uniprova.it/Shibboleth.sso
  - Se il risultato è una pagina con il testo 'Session Creation Failure‘ il filtro funziona correttamente
- Se con il test viene caricata una pagina con errore http 404
  - Controllare dalle proprietà del sito che I permessi di esecuzione siano su 'script only'
  - Ai file con estensione 'sso' deve essere associato il fitro isapi shibd
  - Sul file isapi_shib.dll dovranno esserci i permessi di lettura ed esecuzione per l'utente IIS_WPG
  - Ripetere il test



Riferimenti

- Configurazione
  - https://spaces.internet2.edu/display/SHIB/ConfiguringShibboleth
- Tutorial
  - http://shib.kuleuven.be/docs/sp/windows2003/install-sp-1.3-windows2003.shtml