Shibboleth SP

installazione e configurazione di base per SSO

Nunzio Napolitano – IDEM CTS –Università degli Studi di Napoli PARTHENOPE

Agenda

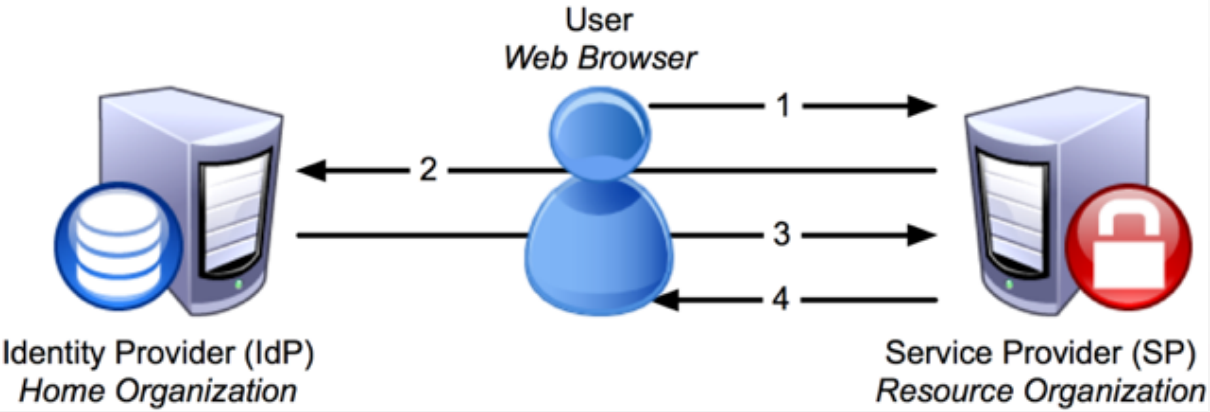
Intro sui service provider

Installazione

Configurazione

Protezione di una risorsa web

Quadro di insieme

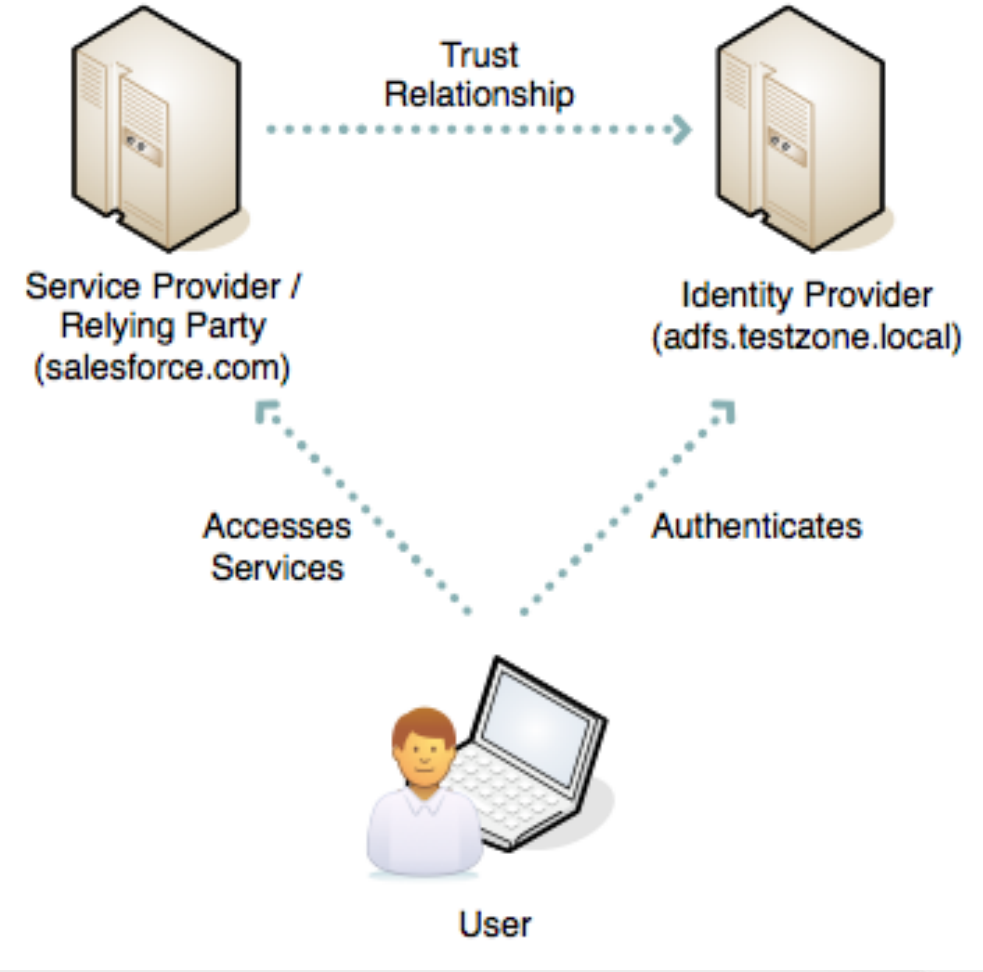


1.The SP detects the user attempting to **access restricted content** within the resource.
2.The SP generates an **authentication request**, then sends the request, and the user, to the user's IdP.
3.The **IdP authenticates** the user, then sends the **authentication response**, and the user, back to the SP.
4.The **SP verifies the IdP's response** and sends the request through to the resource

https://wiki.shibboleth.net/confluence/display/SHIB2/NewUnderstandingShibboleth

Trust Relationship

La fiducia reciproca fra IdP ed SP si ottiene attraverso i **metadati**



Framework SAML

Shibboleth SP - modulo di Apache/IIS, utilizzabile con tutti i linguaggi di programmazione supportati dal webserver.

SimpleSAMLphp - implementazione PHP nativa Integrabile direttamente nella nostra applicazione (PHP)

Elenco dei software

http://en.wikipedia.org/wiki/SAML-based_products_and_services

Estensioni SAML

Le applicazioni più note hanno dei plug-in SAML già disponibili

https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled

https://rnd.feide.no/federated-software/

Agenda

Intro sui service provider

Installazione

Configurazione

Proteggere risorsa web

Istruzioni operative

Visualizzazione pagine web

- *Browser* (si può usare quello Host oppure quello della VM)

Configurazione shibboleth/apache/etc..

- Copia dei file da terminale (`sudo -i`)
- Edit dei file (gedit, vi,etc)

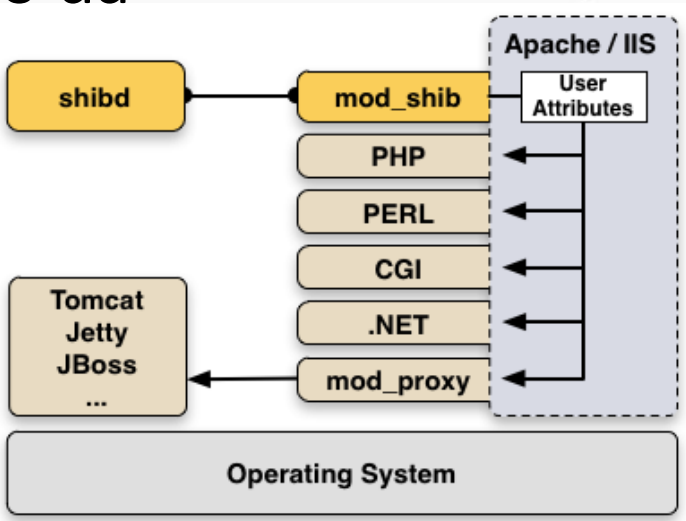
Materiale per configurazione in

`/home/testuser/CORSO_IDEM`

Shibboleth SP

Shibboleth Service Provider è composto da

- mod_shib (Apache /IIS)
- Demone SHIBD



<u>Caratteristiche</u>

- Proteggere <u>l'accesso</u> con «Require»
- Attributi utente accessibili nell'ambiente del web server da tutte le applicazioni (PHP, Perl, .Net, ASP, CGI, ...) es. $_SERVER['mail'].
- Servlet container, (es. Tomcat) devono operare con Apache or IIS come front-end

Installazione

- pacchetti per Debian/Ubuntu

```
Sudo apt-get install apache2 libapache2-mod-shib2
openssl php5 ntp
```

- distribuzioni RPM based

```
http://download.opensuse.org/repositories/security://
shibboleth/
```

Struttura delle directory

- Modulo Apache
  - `/etc/apache2/mod-available/shib2.load`
  - `/usr/lib/apache2/modules/mod_shib2.so`
- Demone
  - `/usr/bin/`
  - `/usr/lib/x86_64-linux-gnu/shibboleth/*`
  - `/usr/sbin/shib-keygen`
  - `/usr/sbin/shibd`
- CFG
  - `/etc/shibboleth/*`
- Elenco files

  `Comando : dpkg -L libapache2-mod-shib2`

  http://packages.ubuntu.com/trusty/amd64/libapache2-mod-shib2/filelist

Agenda

Intro sui service provider

Installazione

Configurazione

Proteggere risorsa web

Agenda

Configurazione -shibd

- Metadati – *Firma e verifica*
- Set *entityID*
- Set *SSO*
- Set *metadata provider*

I nostri metadati

La carta di identità del nostro SP

https://sp1.local/Shibboleth.sso/Metadata

Configurazione - certificati

Salvare i certificati per la **VERIFICA** dei metadati

- Federazione IDEM

  ```
  Wget
  https://www.idem.garr.it/documenti/doc_download/321-idem-metadata-signer-2019
  -O /etc/shibboleth/metadata-signer.crt
  ```

- Questo corso

  ```
  Wget https://sp.lab.unimo.it/metadata-signer.crt
  -O /etc/shibboleth/metadata-signer.crt
  ```

Configurazione - certificati

Creare i certificati per la **FIRMA** dei metadati

- Generazione certificati

  /usr/sbin/shib-keygen

  /etc/shibboleth/sp-cert.pem

  /etc/shibboleth/sp-key.pem

- Solo per il corso

```
Cp /home/testuser/CORSO_IDEM/1_SESSIONE/shibboleth/sp-
*.pem  /etc/shibboleth
```

Configurazione – shibboleth2.xml -1/3

Editing di /etc/shibboleth/shibboleth2.xml

entityID

Sostituire

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
REMOTE_USER="eppn persistent-id targeted-id">
```

con

```
<ApplicationDefaults entityID="https://sp1.local/shibboleth"
REMOTE_USER="eppn persistent-id targeted-id">
```

Configurazione – shibboleth2.xml -2/3

Editing di /etc/shibboleth/shibboleth2.xml

SSO (caso singolo IdP)

Sostituire

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

Con

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

Configurazione – shibboleth2.xml -3/3

Editing di /etc/shibboleth/shibboleth2.xml

MetadataProvider

Inserire il seguente <MetadataProvider>:

```
<MetadataProvider type="XML"
uri="https://sp.lab.unimo.it/rr3/signedmetadata/federation/fed-corso/metadata.xml"
backingFilePath="/etc/shibboleth/signed-test-metadata.xml"
reloadInterval="7200">
<MetadataFilter type="Signature" certificate="metadata-signer.crt"/>
</MetadataProvider>
```

Configurazione -check

- Verifichiamo la configurazione

```
Shibd –t
```

- Riavviamo il servizio

```
Services shibd restart
```

- Attiviamo il modulo shib2

```
a2enmod shib2
service apache2 restart
```

I nostri metadati

Rivediamo i nostri metadata

https://sp1.local/Shibboleth.sso/Metatada

Analizziamo i vari TAG

```
<Request Initiator>
<Assertion cunsumer service>
```

Agenda

Intro sui service provider

Installazione

Configurazione

Proteggere risorsa web

Protezione di una risorsa Locale

Pagina da proteggere

https://sp1.local/intranet/intranet.html

Configurazione - Apache

- configurazione della Location da proteggere

  Modificare /etc/apache2/sites-available/service _provider.conf

```
<Location /intranet>
 AuthType shibboleth
 ShibRequestSetting requireSession true
 Require shib-session
</Location>
```

- Attivare il modulo shib2

```
service apache2 restart
```

Protezione di una risorsa Locale

VERIFICA

https://sp1.local/intranet/intranet.html

Sistemiamo le cose……

Lanciamo lo script di update per allineare tutte le VM

```
cd /home/testuser
./CORSO_IDEM/1_SESSIONE/update_stato_1.sh
```

Speriamo vi sia piaciuto….

…..e tutto abbia funzionato!!!