Magic

Middleware for collaborative Applications and Global vIrtual Communities

Federación de identidades

IdP, SP, DS

Carlos González| RedCLARA | 25-05-16 | Magic Project

Sobre esta presentación

- Centrada en Shibboleth
- Basada en el “Curso técnico de federación de identidad para la educación y la investigación” disponible en cursos.redclara.net (versión previa de shib)

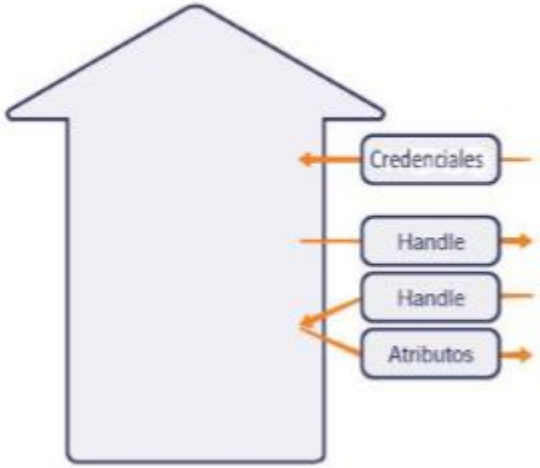
Shibboleth

Magic
Middleware for collaborative Applications and Global virtual Communities

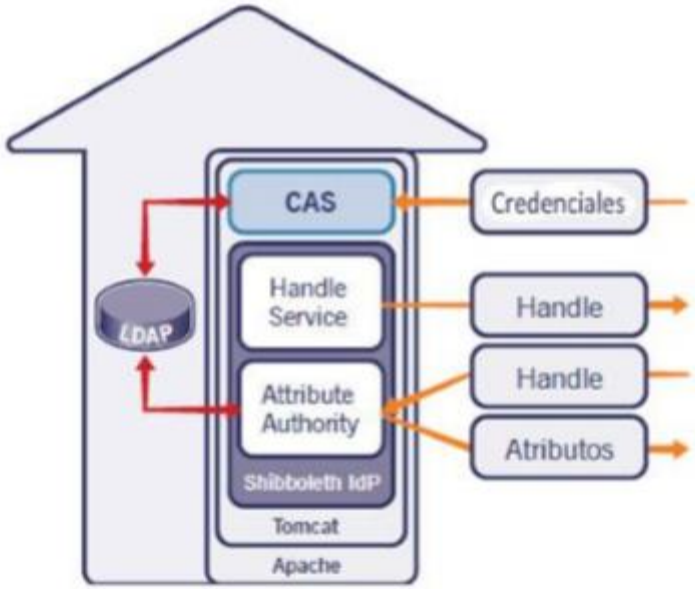
- Middleware creado por Internet2
- Autorización y autenticación
- SSO
- Permite utilizar una única identidad para varios sistemas, en diferentes institutionces
- Provee IdP, SP, DS, Agregación de Metadatos
- Jueces 12: 1-15
- Shibboleth vs SimpleSAMLphp

IdP

Magic
Middleware for collaborative Applications and Global virtual Communities

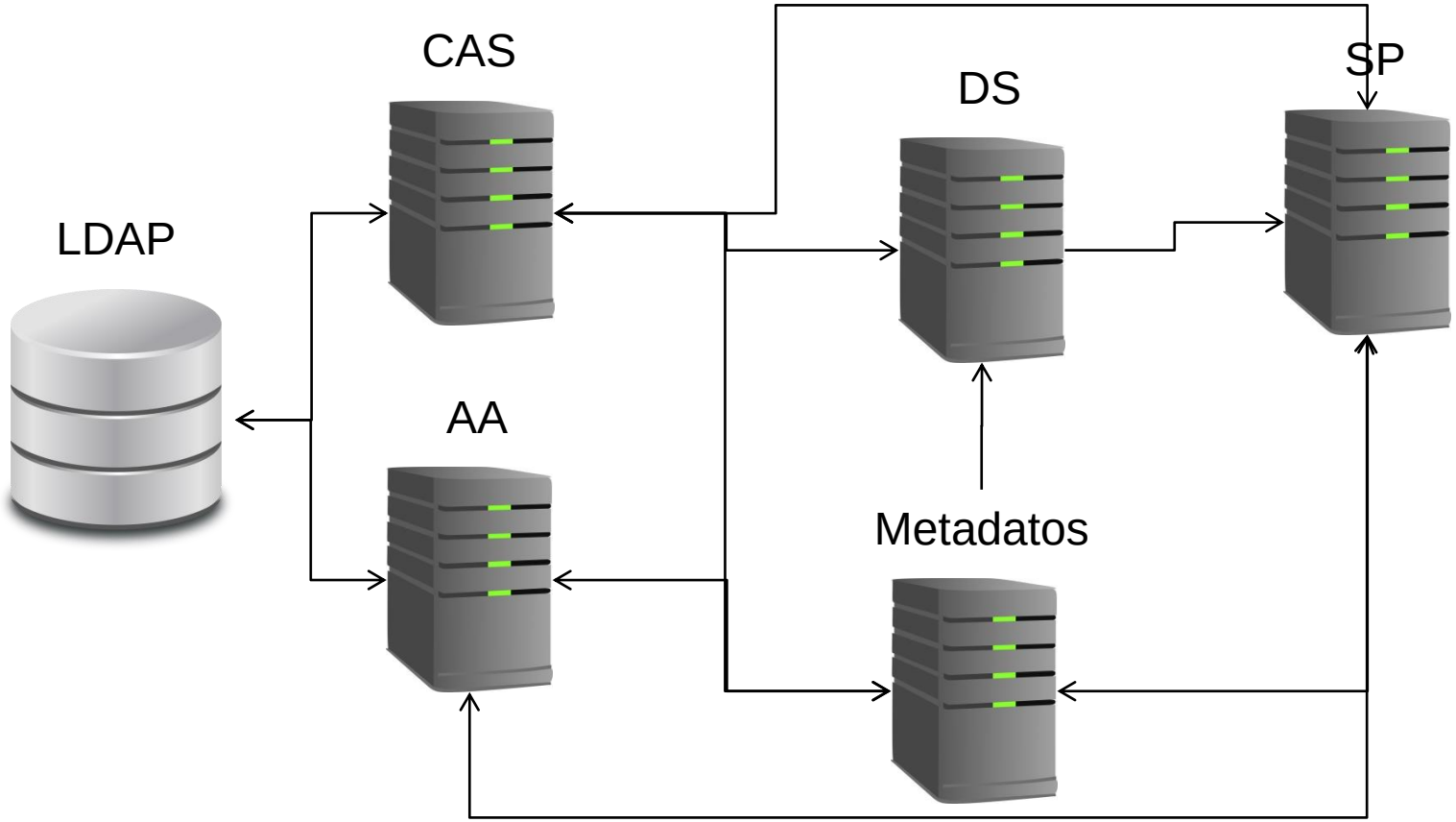


IdP


CAS
Credenciales
Handle Service
Handle
LDAP
Handle
Attribute Authority
Atributos
Shibboleth IdP
Tomcat
Apache

Requisitos para desplegar un IdP

- Primero, sobre despliegue general:



Requisitos para desplegar un IdP

- Oracle Java u OpenJDK 7 y 8
- Servlet container:
  - Tomcat 7
  - Jetty 8
- “Only Tomcat 8 and Jetty 9.2 - Jetty 9.3 are officially supported by the project at this time.”
- **“recommended container implementation is Jetty”**
- Se recomienda Linux, OS X y Windows
- Certificado digital !!!

Instalación – qué se requiere antes

Magic
Middleware for collaborative Applications and Global virtual Communities

- entityID
- Subdominio para los atributos “scoped”
- Metadatos de los SP

Instalación – con qué ayuda Shibboleth

- El proceso de instalación sugerirá:
  - El entityID (que puede ser cambiado)
  - Pares de autofirmados de llaves/certificados para:
    - Firmar mensajes
    - Asegurar conexiones de servicios web
    - Encripción de datos por otros sistemas para ser desencriptados por el IdP
  - Una clave secreta para asegurar los cookies
  - Los metadatos de ejemplo, iniciales, del IdP
  - Un conjunto inicial de archivos de configuración

Instalación

- Cree una máquina virtual
- Instale lo previamente requerido (Java, Jetty…)
- Descargue la versión más reciente de shibboleth IdP (https://shibboleth.net/downloads/identity-provider/latest)
- Desempaquete los archivos
- Vaya al directorio que se creó al desempaquetar
- Ejecute **./bin/install.sh**
- Despliegue el archivo que se crea en *war/idp.war*
- Pruebe que es un master instalando IdP: **bin/status.sh**
- Importante, para reconstruir el war: **bin/build.sh**

Configuración

- Configure la autenticación (para el ejemplo, vía LDAP):
  - Configure la autenticación por password () en *authn/general-authn.xml*

    Otras son RemoteUser, X509…
  - Configure la autenticación vía LDAP en *authn/password-authn-config.xml*:

    ```
    <import resource="ldap-authn-config.xml" />
    ```

    Remueva los otros import (o coméntelos)
  - Configure los archivos para autenticarse contra LDAP en *conf/authn/ldap-authn-config.xml*
    - Siga los pasos en *https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration*

Configuración

- Cargue los metadatos de los SP (o de la federación)

```
  <MetadataProvider id="ICMD"
xsi:type="FileBackedHTTPMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata"
        metadataURL="http://md.incommon.org/InCommon/InCommon-
metadata.xml"
        backingFile="%{idp.home}/metadata/InCommon-metadata.xml"
        minRefreshDelay="PT5M"
        maxRefreshDelay="PT1H"
        refreshDelayFactor="0.75">
```

Si los metadatos están firmados, informar sobre el certificado:

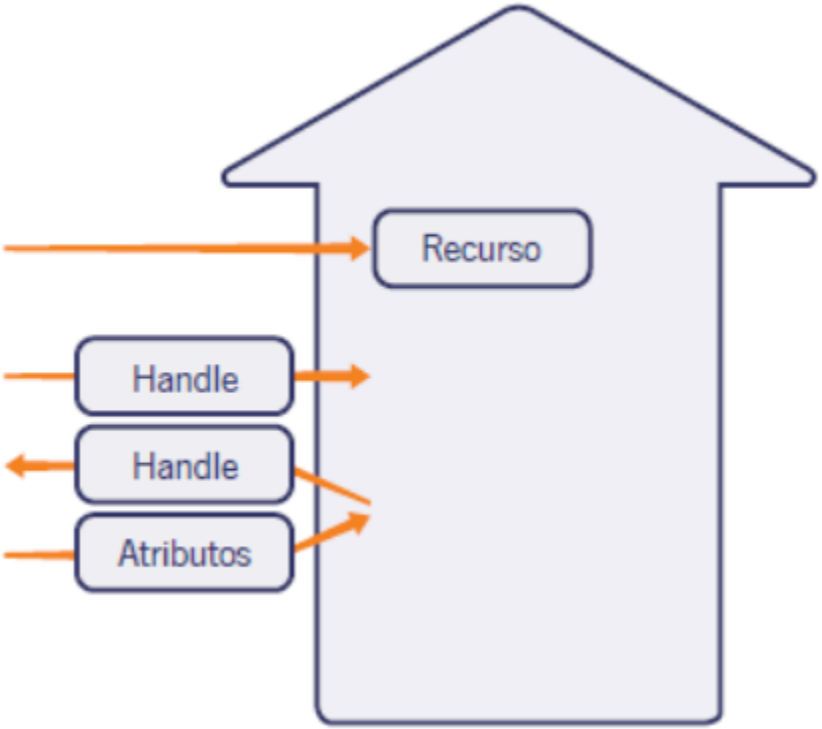
```
<MetadataFilter xsi:type="SignatureValidation"
requireSignedRoot="true"
         certificateFile="%{idp.home}/credentials/inc-md-cert.pem" />
```

Recursos

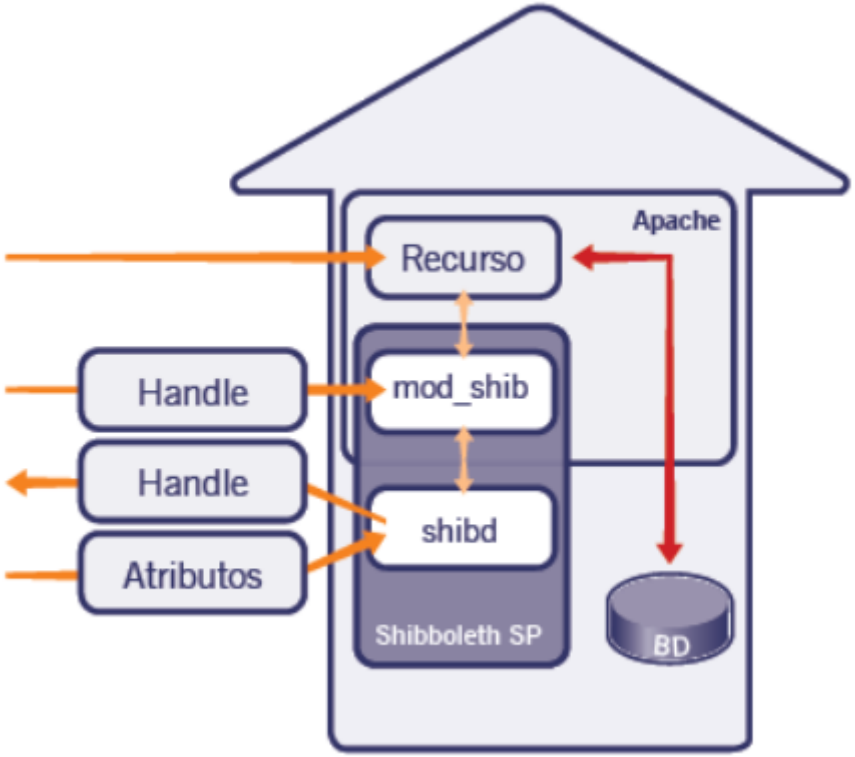
- Instalación:
  - https://wiki.shibboleth.net/confluence/display/IDP30/Installation
- Configuración de los metadatos:
  - https://spaces.internet2.edu/display/InCFederation/Shibboleth+Metadata+Config
- Configuración LDAP:
  - *https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration*

SP

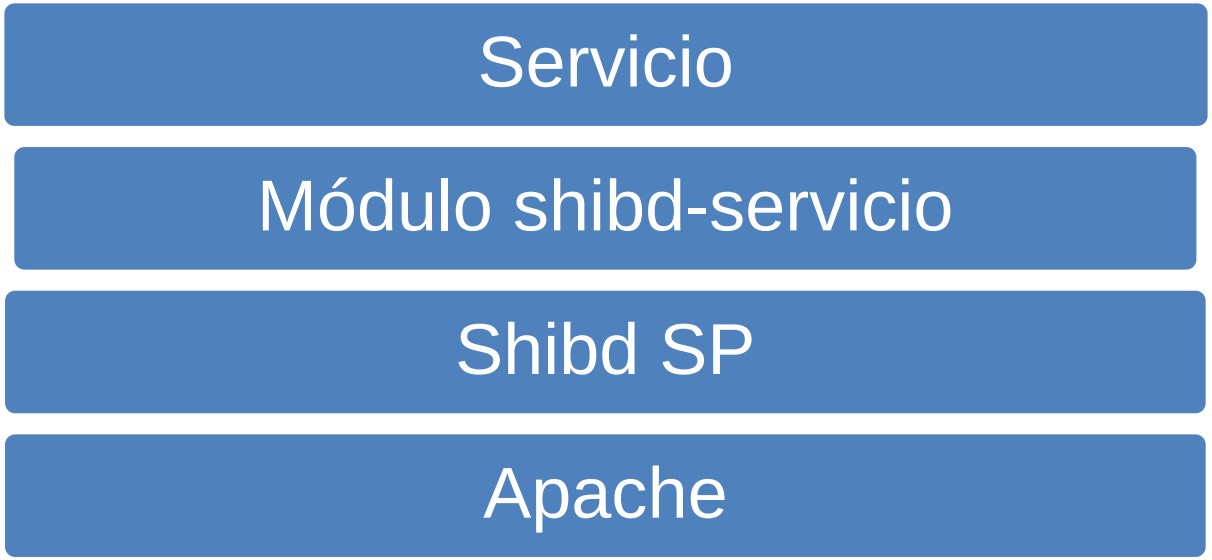
Magic
Middleware for collaborative Applications and Global virtual Communities



SP


Apache
Recurso
mod_shib
shibd
Handle
Handle
Atributos
Shibboleth SP
BD

Primero, algo de arquitectura



Instalando el SP

- Instalar shibboleth vía yum o apt-get
- Esto instala el módulo de apache
- https://localhost/Shibboleth.sso/Status

Probando

- Proteja un directorio

```
<Location /secure>
AuthType shibboleth
ShibRequestSetting requireSession 1
Require valid-user
</secure>
```

- En el directorio protegido cree un archivo para mostrar las variables existentes en la sesión

```
<?php print_r($_SERVER) ?>
```

Configurando el SP

- Adicione el IdP en MetadataProvider

```
<MetadataProvider type="XML" url="https://federation.org/metadata.xml
" backingFilePath="fedmetadata.xml">
    <MetadataFilter type="Signature" certificate="fedsigner.pem"/>
</MetadataProvider>
```

Recursos

- Instalando el SP para Linux
  - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxInstall

DS (WAYF)

Magic
Middleware for collaborative Applications and Global virtual Communities

- Discojuice
- UNINETT
- Múltiples formas de despliegue:
  - Embebido
  - Como un servicio standalone

Discojuice

Magic
Middleware for collaborative Applications and Global virtual Communities

```
<!-- JQuery hosted by Google -->
<script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js" type="text/javascript"></script>

<!-- DiscoJuice hosted by UNINETT at discojuice.org -->
<script type="text/javascript" src="https://cdn.discojuice.org/discojuice-stable.min.js"></script>
<link rel="stylesheet" type="text/css" href="https://cdn.discojuice.org/css/discojuice.css" />
<script type="text/javascript">
        DiscoJuice.Hosted.setup(
                {
                        "target": "a.signin",
                        "title": "Example showcase service",
                        "spentityid": "https://bridge.uninett.no/saml2/entityid",
                        "responseurl": "http://bridge.uninett.no/response.html",
                        "redirectURL": "http://bridge.uninett.no/login?idp=",
                        "feeds": ["edugain", "kalmar", "feide"]
                }
        );
</script>
```