Configuración de un LDAP con SWB para control de Usuarios

Prerrequisitos

Los pasos descritos en el siguiente manual requieren los siguientes puntos:

- Una instancia de SWB completamente funcional y un usuario con privilegios de SuperUsuario
- Acceso vía FTP y SSH al servidor con los permisos necesarios para realizar cambios a la configuración del Application Server así como reinicios de este
- Conexión entre el servidor con la instancia de SWB y el Directorio Activo vía protocolo LDAP v3
- Conocimientos para realizar la configuración del Application Server ocupado para la publicación de SWB

Procedimiento

IMPORTANTE: Este manual no está diseñado para la configuración de LDAP para el acceso a la administración de SWB, solamente para los portales que se contengan en nuestra instancia

Configurar los parámetros de conexión entre SWB y el Directorio Activo

Esto se realiza en el archivo genericLDAP.properties que se encuentra ubicado en la carpeta /WEB-INF/classes dentro de la instalación de SWB.
La configuración se realiza en base las los parámetros específicos de su LDAP, a continuación se muestran en rojo ejemplos de los parámetros a configurar y en verde alguna información extendida de estos:

NOTA: Se recomienda el uso de alguna herramienta como JXplorer (http://jxplorer.org/) o similar para realizar pruebas de conexión entre el servidor de SWB y el Servidor de Directorio Activo, asegurando que la conexión y los parámetros ocupados son correctos, (host base dn = base dc; user dn = principal ; password= password)

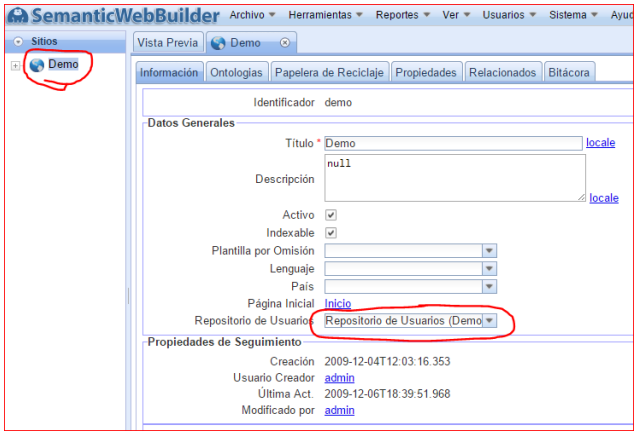
Los parámetros mencionados son solamente ejemplo pudiendo variar los nombres según nuestras configuraciones LDAP.

Dependiendo de la configuración de nuestro LDAP la conexión se podría realizar con un usuario de LDAP en lugar del usuario “principal”

```
#ExternalRepositoryBridge Class
class=org.semanticwb.security.auth.SWB4GenericLDAPBridge (clase de SWB que se ocupara para la conexión)
#factory of connections to LDAP
factory=com.sun.jndi.ldap.LdapCtxFactory
#URL to LDAP Server
url=ldap://localhost   (url del servidor DA, el puerto por defecto usado es el 389)
#UID of Object to browse and seek LDAP
principal= CN=Jorge Luis Lopez,OU=Dirección General,OU=Corporativo,DC=DominioPropio,DC=com,DC=mx
(CN = Common Name, OU = Organizational Unit, DC = Domain Component)
#Credential of Object to browse and seek LDAP
credential=1axd!DDF (Password)
#URI to the base container
base=DC= DominioPropio,DC=com,DC=mx  (Domino base)
#name of the field considered as PK
seekField= AccountName (Campo llave de búsqueda)
#name of the objectclass to recognaize an object as a user
userObjectClass= person (Clase objeto para buscar usuarios)
#name of the First Name field
fieldFirstName=givenName  (Nombre)
#name of the Last Name field
fieldLastName=sn  (Primer apellido)
#name of the Second Last Name field
fieldMiddleName=mn  (Segundo apellido)
#name of the eMail field
fieldEmail=mail (Correo electrónico)
#name of the language field or |langString for a default value
valueLanguage=|es
```

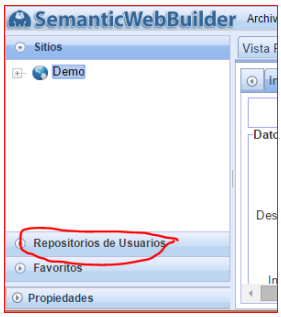
Configurar el repositorio del sitio en SWB al que le activaremos el LDAP

Este procedimiento se debe realizar para cada repositorio de sitio que deseamos valide los usuarios por medio del LDAP. Para ver el repositorio que tenemos asignado a nuestro sitio, damos doble clic en nuestro sitio, esto nos abrirá la ventana de información mostrando lo siguiente:

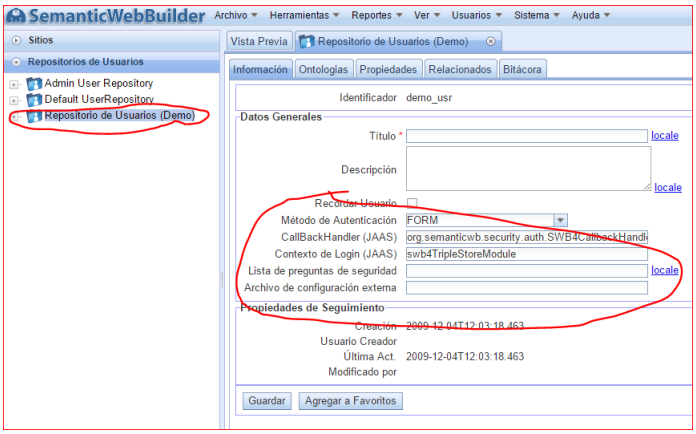


El repositorio mostrado en "Repositorio de Usuarios" es el que ocupa nuestro portal actualmente para validar a los usuarios, este podría pertenecer de manera predeterminada (Exclusivo) al portal o haberlo asignado de manera manual (externo).

Ya identificado el Repositorio, es necesario configurar los parámetros para que tome la configuración de LDAP.
Para realizar esto abrimos la pestaña de Repositorio de Usuarios



Se nos mostraran los repositorios que tiene nuestra instancia de SWB y damos doble clic en el repositorio a configurar, esto nos abrirá la ventana de información y configuración del repositorio.



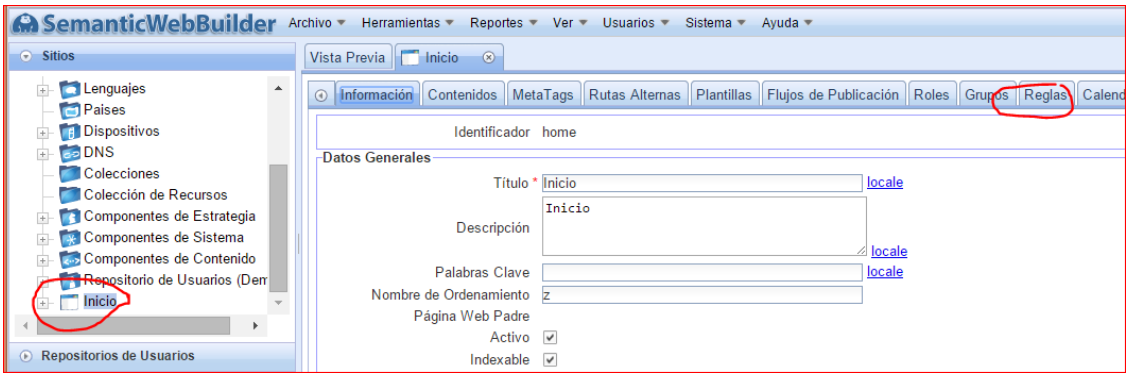
Configuraremos nuestro repositorio con los parámetros siguientes:

CallBackHandler (JAAS) = org.semanticwb.security.auth.SWB4CallbackHandlerLoginPasswordImp
Contexto de Login (JAAS) = LDAPModule
Lista de preguntas de seguridad = (no es necesario configurar esta opción)
Archivo de configuración externa = /genericLDAP.properties

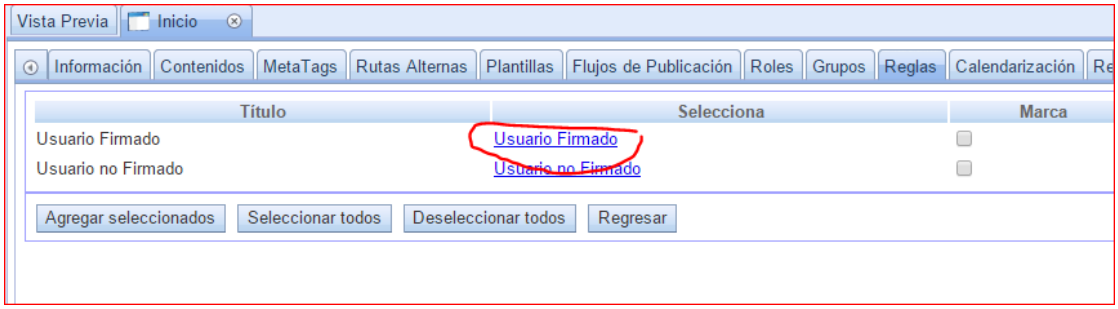
Después damos clic en guardar.

Asignamos la una regla de Firmado a nuestro Home del portal

Abrimos las pestañas de propiedades de nuestra página de inicio (Home) del portal dando doble clic en esta.



En la pestaña de Reglas, seleccionamos agregar de Lista y damos clic en Usuario firmado, para que se asigne la regla a nuestro portal.



Activamos la regla asignada para que nuestro sitio quede protegido con la verificación de un usuario firmado (con login)

Configuración de los Modulos (classes) de validación de Logueo en nuestro Application Server

NOTA: Es posible que ya se haya realizado este pasó durante la instalación inicial de SWB
IMPORTANTE: Algunos Application server com Jetty o versiones de Tomcat no requieren este paso debido a sus características, por lo que podremos omitirlo

Es necesario agregar las clases que ocupa SWB para validar nuestro acceso al Application server que estemos ocupando

Editamos el archivo web.properties de SWB ubicado en WEB-INF/classes desactivando la configuración siguiente:

```
#Ruta relativa a classes donde esta la configuraci\u00f3n del JAAS
wb/security.auth.login.config=/wb_jaas.config
```

De manera que quede como se muestra a continuación:

```
#Ruta relativa a classes donde esta la configuraci\u00f3n del JAAS
wb/security.auth.login.config=ignore
```

Guardamos los cambios

Abrimos en modo lectura el archivo jaas.config ubicado en WEB-INF/classes, para poder copiar las líneas (modulos) siguientes:

```
swb4TripleStoreModule {
   org.semanticwb.security.auth.TripleStoreLoginModule required;
};

LDAPModule {
   org.semanticwb.security.auth.LDAPLoginModule required;
};
```

Estas líneas deberán ser agregadas a nuestros archivos de configuración de nuestro Application Server en la parte de los Modulos de Logueo conforme los manuales de configuración de estos.

Ejemplos:

En GlassFish se edita el archivo login.conf del dominio que tiene nuestro SWB agregando las líneas a este.

En JBoss se edita el archivo login-conf.xml dentro de <policy> </policy> agregando los parámetros para cada modulo:

```
<application-policy name="swb4TripleStoreModule">
 <authentication>
 <login-module code="org.semanticwb.security.auth.TripleStoreLoginModule"
flag="required">
 </login-module>
 </authentication>
 </application-policy>
```

Reinicio y Pruebas

Después de verificar y guardar todos cambios realizados, es necesario realizar un reinicio de nuestro completo de nuestro Application Server, para que tome todas las configuraciones nuevas.

Una vez que todo haya cargado de manera correcta, intentaremos acceder a nuestro portal con un usuario valido en el Directorio Activo, esto nos debe de dar acceso a nuestro sitio.

De igual manera es necesario intentar acceder con un usuario o contraseña invalida para verificar que las validaciones del LDAP sean correctas.