Configuración de un LDAP para control de Acceso a la Administración de SWB

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

Procedimiento

IMPORTANTE: Es necesario realizar de manera previa un respaldo completo (Full Backup) de la Base de datos de SWB con el objetivo de poder realizar un RollBack en caso de ser necesario

IMPORTANTE: Es necesario realizar un respaldo completo del FileSystem de nuestra instancia de SWB el mismo día y hora que se realizó en respaldo de la BD, para que en caso de que se requiera realizar un RollBack no existan inconsistencias.

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 (módulos) 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 Módulos 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 módulo:

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

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
```

Habilitar Acceso al sitio de Administración

Es necesario activar el acceso desde SWB al sitio de Administración (ambiente de administración) para poder asignar el LDAP como repositorio de Usuarios

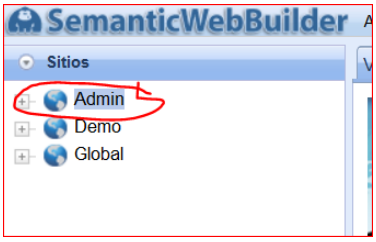
Esto se realiza modificando en el archivo web.properties con cualquier editor de texto, este se encuentra ubicado en la carpeta /WEB-INF/classes ,
La variable swb/adminShow de "false" a "true" de manera que nos quede así:

swb/adminShow=true

Guardamos los cambios y realizamos un reinicio del Application Server para que se carguen los cambios.

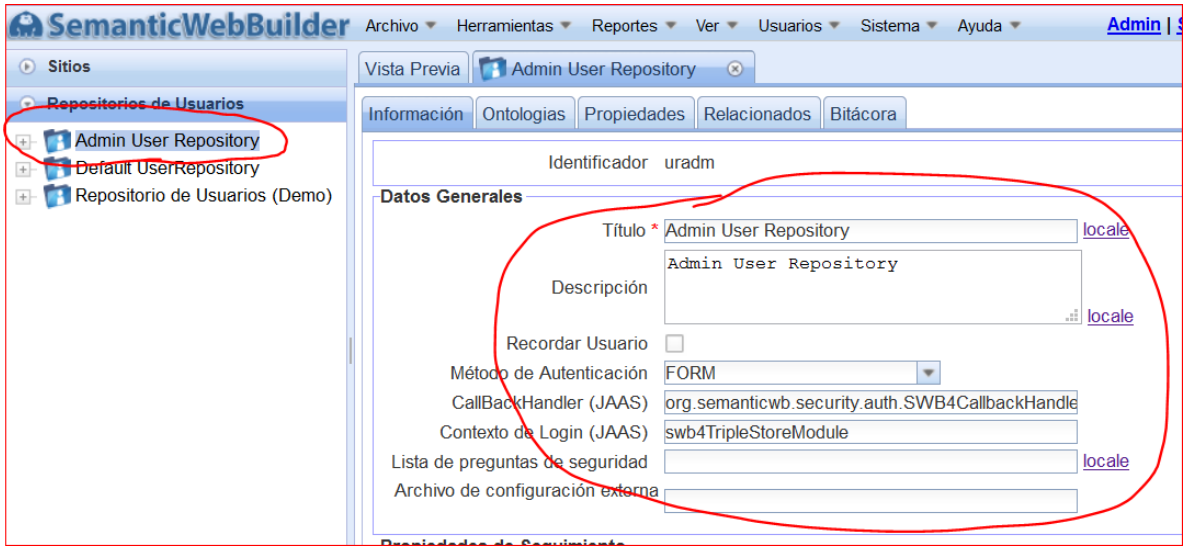
Configurar el repositorio con LDAP del sitio de Administración (Admin) de SWB

Una vez activado el sitio de administración, podremos ver este dentro de nuestra pestaña de sitios así como todas sus características y configuraciones.



Para configurar el repositorio para que ocupe el LDAP en lugar del repositorio de Usuarios de SWB 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 de Admin User Repository, 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 y Reiniciamos el Application Server para que cargue los cambios.

Acceder con el usuario candidato a ser SuperUsuario

Necesitamos conocer el usuario y contraseña del usuario en el Directorio Activo que se encargara de ser SuperUsuario de nuestro SWB. Con este usuario realizamos 2 intentos de acceso, estos serán fallidos, pero nos permitirán que SWB realice el copiado de la información de este a su BD. En ambos intentos se nos mostrara la página de que no se tiene permiso al portal.

Una vez realizado esto, es necesario ejecutar el script “setadmin.jsp” el cual debe ser copiado al servidor en la ruta de instalación de nuestro SWB dentro de la carpeta “work” (swb/work).
Este script se ejecuta de la siguiente manera:

http://<dirección ip>/work/setadmin.jsp?login=<loginusuario>

Donde `loginusuario` es el user (id) del usuario, al ejecutarlo se nos mostrara el mensaje “Usuario encontrado y modificado”, en caso negativo, revisar si el usuario es correcto y volver a intentar.

Reiniciamos el Application Server

Una vez iniciado probamos de nuevo entrar a la administración con el SuperUsuario, este logueo debe ser correcto.

Últimos Pasos y pruebas

Después de acceder con el SuperUsuario y verificar que nuestra administración funciona correctamente, es necesario realizar lo siguiente:

- Ocultar nuevamente el sitio de Administración, modificando el web.properties: swb/adminShow=false
- Eliminar el archivo “work/setadmin.jsp” del servidor de SWB

Después de esto realizar un reinicio de nuestro completo de nuestro Application Server, para que tome todas las configuraciones nuevas.

Cada que un usuario realice un intento de accedo será copiado a nuestro Repositorio de Admin de SWB, con esto podrá nuestro SuperUsuario darles los Grupos y Roles necesario para el uso de las administración.
De igual se recomienda intentar acceder con un usuario o contraseña invalida para verificar que las validaciones del LDAP sean correctas.