

Ejercicios de seguridad en JBoss y LDAP

Índice

1 Autenticación en JBoss.....	2
2 LDAP.....	3

1. Autenticación en JBoss

Vamos a configurar ahora JBoss para que use autenticación basada en BD para la aplicación de comentarios. La configuración de la aplicación propiamente dicha en el web.xml no es necesario cambiarla, ya que es portable, pero sí tendremos que crear un módulo de login para que use la BD comentarios.

Lo primero es crear la fuente de datos en JBoss para poder conectar con la BD:

1. Copiar el .jar con el driver de MySQL, incluido en las plantillas de la sesión, al directorio `default/lib` de JBoss. El driver es exactamente el mismo que usábamos con Tomcat
2. Crear el DataSource propiamente dicho. Simplemente tendréis que copiar el fichero `mysql-comentarios-ds` incluido en las plantillas de la sesión al directorio `deploy` de JBoss. Comprobar en la consola (solapa "Console") que JBoss la detecta (mensaje *Bound ConnectionManager* `'jboss.jca:service=DataSourceBinding,name=comentariosDS'...`)
3. El nombre JNDI en JBoss es ligeramente distinto al que se usaba en Tomcat. Por ello, en el código de `FuenteDatos.java` que es el que obtiene el DataSource con JNDI hay que cambiar el nombre actual por `java:/comentariosDS`
4. Ejecutar la aplicación en JBoss y comprobar que funciona con la BD

Ahora vamos a añadirle la autenticación:

1. Parar JBoss, ya que vamos a cambiar la configuración.
2. Insertar un nuevo `application-policy` en el `login-config.xml` de la carpeta `conf` con el siguiente módulo de login.

```
<application-policy name="comentarios">
  <authentication>
    <login-module
code="org.jboss.security.auth.spi.DatabaseServerLoginModule"
      flag="required">
      <module-option
name="dsJndiName">java:/comentariosDS</module-option>
      <module-option name="principalsQuery">
        select password from usuarios where login=?
      </module-option>
      <module-option name="rolesQuery">
        select rol, 'Roles' from roles where login=?
      </module-option>
    </login-module>
  </authentication>
</application-policy>
```

Cuando se re arranque el servidor, comprobar en la consola que no se genera ninguna excepción, por si hemos introducido mal el nuevo módulo de login.

3. En el proyecto de Eclipse crear un nuevo fichero descriptor de despliegue: `jboss-web.xml`, dentro de `WEB-INF` con el siguiente contenido:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE jboss-web PUBLIC
    "-//JBoss//DTD Web Application 2.4//EN"
    "http://www.jboss.org/j2ee/dtd/jboss-web_4_0.dtd">
<jboss-web>
  <security-domain>java:/jaas/comentarios</security-domain>
</jboss-web>
```

4. Ejecutar la aplicación de nuevo en JBoss y comprobar que la seguridad funciona exactamente igual a como lo hacía con Tomcat (para insertar comentarios hay que tener rol "registrado").

2. LDAP

En las plantillas de la sesión se incluye un servidor LDAP (ApacheLDAP) y JXExplorer, un programa para explorar el árbol LDAP.

Para instalar ApacheLDAP basta con descomprimirlo en cualquier carpeta. Para ponerlo en marcha, ejecutar el archivo `apacheds.bat` contenido en el directorio `bin`.

Lo mismo ocurre con JXExplorer, simplemente descomprímelo en cualquier directorio. Para arrancarlo, ejecutar el archivo `.bat`. Tenemos que configurar la conexión con el servidor LDAP e insertar datos.

1. Elegimos la opción `File > Connect`
2. En el cuadro de diálogo "Open LDAP/DSML connection" el host debe ser **localhost**, el puerto el **10389**, el Base DN vacío, el User+DN **uid=admin,ou=system** y el password **secret**.
3. Para insertar nuestros datos en LDAP elegimos la opción `LDIF > Import File` e importamos el archivo `ayuntamientoEjemplo.ldif` de las plantillas de la sesión.

Una vez insertados los datos, podemos verlos a través de la solapa "Explore" del programa.

Usando el *login module* visto en la sesión, configurar JBoss para que la autenticación se lleve a cabo contra el servidor LDAP en lugar de contra la BD. **Dejad comentado el módulo de login que se usaba en el ejercicio anterior e insertad uno nuevo. Valdrá el código de los apuntes, cambiando el nombre por "comentarios" en vez de "seguridadLDAP"**. Comprobar que la autenticación LDAP funciona, entrando por ejemplo como "acuena" con password "cuena".

