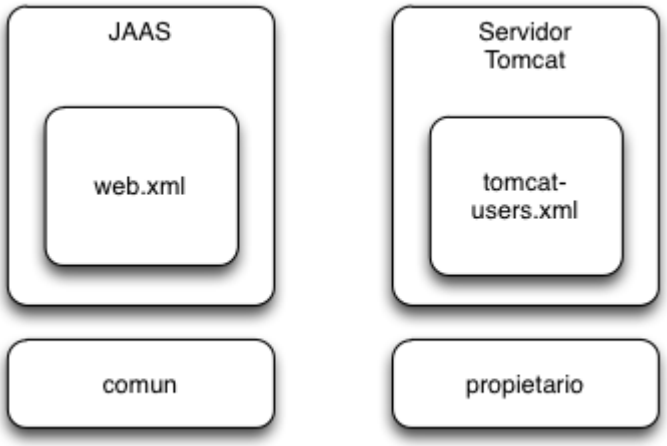
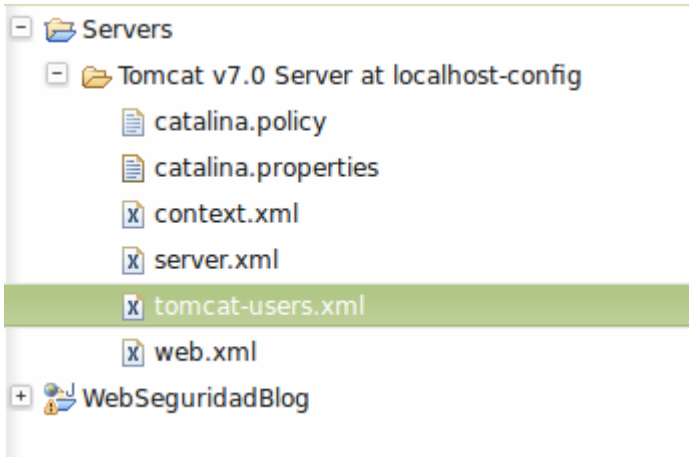
En el articulo anterior hemos configurado todo lo necesario de seguridad en cuanto a web.xml se refiere .Ahora nos queda integrar la seguridad de JAAS con nuestro servidor (Tomcat) .Algo que en cada servidor de aplicaciones se realiza de una forma distinta.



En el caso del Tomcat como la imagen indica deberemos apoyarnos en el fichero tomcat-users.xml . Este fichero lo podemos encontrar en la carpeta conf del propio Tomcat. En el caso de tener el Tomcat integrado con eclipse (nuestro caso) este fichero se encuentra en el proyecto servers.



Cuando abrimos el fichero nos encontramos con una serie de usuarios y roles comentados

por defecto que vienen de ejemplo . Podemos borrarlos y substituirlos por los siguientes roles y ususarios.

```
<tomcat-users>

<role rolename="ROLEA"/>
 <role rolename="ROLEB"/>
 <user username="cecilio" password="cecilio" roles="ROLEA"/>
 <user username="luis" password="luis" roles="ROLEB"/>
</tomcat-users>
```

La etiqueta <role> se encargara de definir cada uno de los usuarios posibles para la aplicación.

```
 <role rolename="ROLEA"/>
```

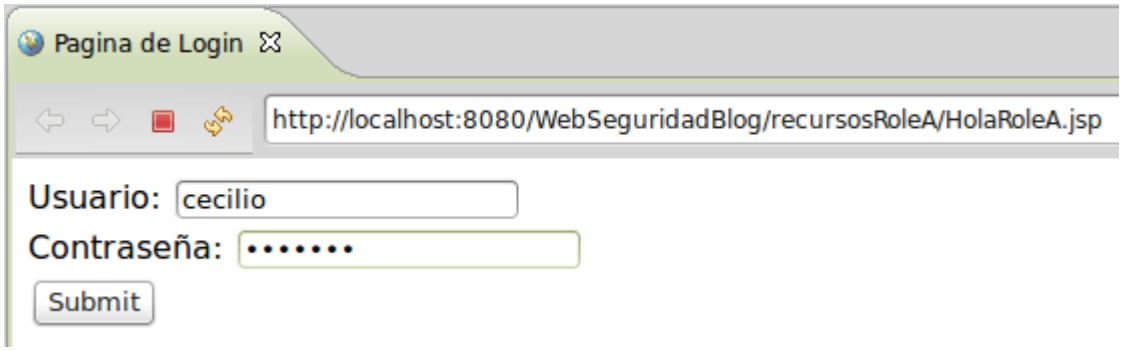
Mientras que la etiqueta <user> se encargara de dar de alta cada uno de los usuarios con nombre y clave y asignarles un rol.

```
 <user username="cecilio" password="cecilio" roles="ROLEA"/>
```

Una vez configurado el servidor podemos solicitar cualquiera de las páginas que tienen controlado el acceso via JAAS.



Nada mas solicitar acceso el navegador nos redirige a la página de Login en donde deberemos introducir usuario y clave.

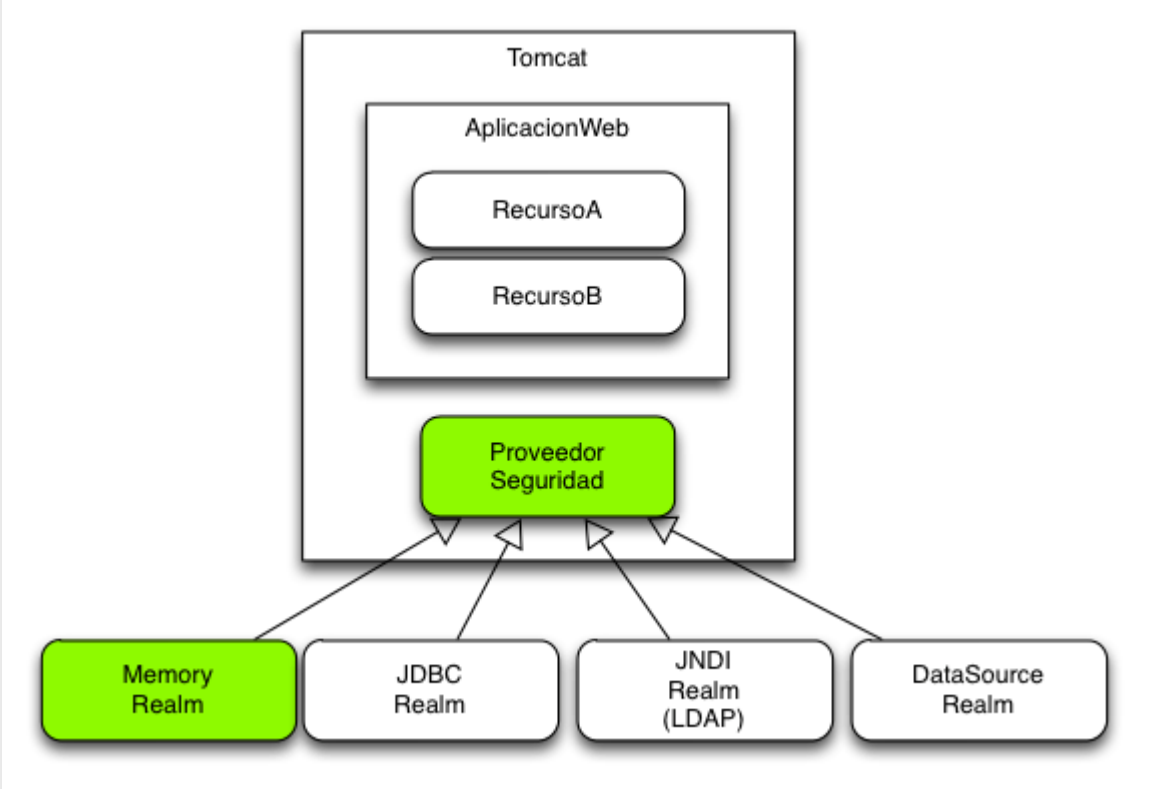


Una vez introducidos los datos el servidor nos validará y podremos acceder al contenido sin mayor problema.



En este caso hemos usado el proveedor de seguridad mas sencillo (por claridad) pero Tomcat como servidor soporta otros proveedores que son los habituales a utilizar en las

aplicaciones reales.



Los proveedores de JDBC y DataSource nos permiten ligar la seguridad contra una base de datos . Mientras que por el otro lado el proveedor de JNDI nos permite trabajar con LDAP.