Proyecto Adalid, Plataforma jee2
Utilizando Google reCAPTCHA

Tabla de Contenido

Generación y Refinación de la Aplicación

Para utilizar Google reCAPTCHA en aplicaciones generadas con Adalid es necesario:

- Obtener el par de claves de reCAPTCHA para su sitio. El par de claves consta de una clave de sitio y una clave secreta (en inglés: *site key* y *secret key*, respectivamente). La clave de sitio se utiliza para mostrar el *widget* en su sitio. La clave secreta autoriza la comunicación entre sus aplicaciones y el servidor de reCAPTCHA para verificar la respuesta del usuario. La clave secreta debe mantenerse protegida por motivos de seguridad. Para más información sobre cómo obtener las claves de reCAPTCHA, consulta la página de Google reCAPTCHA.

- Generar la aplicación indicando que requiere acceso a internet para su funcionamiento. Para ello, utilice el método **setInternetAccessAllowed** en el proyecto Maestro, como se muestra a continuación:

  ```
  setInternetAccessAllowed(true);
  ```

- Editar el archivo **Google.reCAPTCHA.js** y sustituir el valor que retorna la función **grecaptchaSiteKey** (`6LeIxAcTAAAAAJcZVRqyHh71UMIEGNQ_MXjiZKhI`) con la clave de sitio previamente obtenida para su sitio. El archivo **Google.reCAPTCHA.js** se encuentra en el subdirectorio **src\main\webapp\resources\js\base** del módulo Web de la aplicación de empresa generada y no se reescribe al regenerar la aplicación. La función **grecaptchaSiteKey** generada retorna la clave de sitio de prueba de reCAPTCHA, la cual se puede utilizar en combinación con la clave secreta de prueba (vea Configuración del Servidor de Aplicaciones más adelante). Con las claves de prueba el *widget* nunca presenta un desafío (CAPTCHA) y todas las solicitudes de verificación son aprobadas. Por favor utilice estas claves solo para pruebas. La función **grecaptchaSiteKey** generada se muestra a continuación:

  ```
  function grecaptchaSiteKey() {
      return '6LeIxAcTAAAAAJcZVRqyHh71UMIEGNQ_MXjiZKhI';
  }
  ```

Configuración del Servidor de Aplicaciones

Para utilizar Google reCAPTCHA en aplicaciones generadas con Adalid también es necesario configurar el servidor de aplicaciones en el que se ejecuta la aplicación. Esta configuración varía dependiendo del servidor utilizado (GlassFish o WildFly) y del dominio (*realm*) de autenticación de la aplicación (JDBC o LDAP), tal como se describe en las siguientes secciones.

Independientemente del servidor y el dominio de autenticación, siempre es necesario suministrar su clave secreta. Para ello debe escoger una de las siguientes opciones:

- Añadir la propiedad **google.recaptcha.secret.key** a las propiedades del sistema del servidor de aplicaciones; el valor de la propiedad sería su clave secreta.

- Almacenar su clave secreta en un archivo ubicado en un directorio al cual el servidor de aplicaciones tenga acceso y añadir la propiedad **google.recaptcha.secret.key.file** a las propiedades del sistema del servidor de aplicaciones; el valor de la propiedad sería la ruta absoluta del archivo que contiene la clave secreta.

- Almacenar su clave secreta en un archivo llamado **google.recaptcha.secret.key** en el directorio de trabajo del usuario (*user working directory*) del servidor de aplicaciones (el directorio de trabajo del usuario corresponde al valor de la propiedad user.dir de la plataforma Java).

Dado que la clave secreta debe mantenerse protegida por motivos de seguridad, es conveniente restringir el acceso al archivo que la contiene. Esto aplica a cualquiera de las opciones anteriores, ya que las propiedades del sistema del servidor de aplicaciones se almacenan en un archivo del directorio de configuración del servidor.

En el subdirectorio **setup/config/google** del directorio **management** de la aplicación generada se encuentra un archivo **google.recaptcha.secret.key** que contiene la clave secreta de prueba de reCAPTCHA, la cual se puede utilizar en combinación con la clave de sitio de prueba que retorna la función **grecaptchaSiteKey** generada en el archivo **Google.reCAPTCHA.js**. Para utilizar este archivo, especifique su ruta absoluta en la propiedad **google.recaptcha.secret.key.file** de las propiedades del sistema del servidor de aplicaciones o simplemente cópielo en el directorio de trabajo del usuario (*user working directory*) del servidor de aplicaciones. Con las claves de prueba el *widget* nunca presenta un desafío (CAPTCHA) y todas las solicitudes de verificación son aprobadas. Por favor utilice estas claves solo para pruebas.

Configuración de GlassFish

Lleve a cabo las siguientes acciones:

- Haga una copia de respaldo del archivo de configuración **login.conf** que se encuentra en el subdirectorio **config** del directorio del dominio GlassFish en el que se encuentra instalada la aplicación (usualmente el subdirectorio **domains/domain1** del directorio **HOME** de GlassFish).
- Copie al subdirectorio **lib** del directorio del dominio GlassFish en el que se encuentra instalada la aplicación el archivo **third-party-2.0/lib/adalid-jaas.jar** y todos los archivos **jar** contenidos en el directorio **third-party-2.0/lib/httpcomponents-client/lib**

Finalmente, lleve a cabo las acciones que se indican en la sección correspondiente al dominio de autenticación de la aplicación (JDBC o LDAP).

Dominio de autenticación JDBC

- En la sección **jdbcRealm** del archivo **login.conf** reemplace **com.sun.enterprise.security.ee.auth.login.JDBCLoginModule required;** con **adalid.jaas.glassfish.JDBCLoginModule required;**

Dominio de autenticación LDAP

- En la sección **ldapRealm** del archivo **login.conf** reemplace **com.sun.enterprise.security.auth.login.LDAPLoginModule required;** con **adalid.jaas.glassfish.LDAPLoginModule required;**

Configuración de WildFly

Lleve a cabo las siguientes acciones:

- Haga una copia de respaldo del archivo de configuración **standalone-full.xml** que se encuentra en el subdirectorio **standalone/configuration** del directorio **HOME** de WildFly.

Finalmente, lleve a cabo las acciones que se indican en la sección correspondiente al dominio de autenticación de la aplicación (JDBC o LDAP).

Dominio de autenticación JDBC

- En el archivo **standalone-full.xml**, ubique la sección **<security-domain>** correspondiente a la aplicación y reemplace **<login-module code="Database" flag="required">** con **<login-module code="adalid.jaas.jboss.JDBCLoginModule" flag="required" module="adalid.jaas.jboss">**

Dominio de autenticación LDAP

- En el archivo **standalone-full.xml**, ubique la sección **<security-domain>** correspondiente a la aplicación y reemplace **<login-module code="LdapExtended" flag="required">** con **<login-module code="adalid.jaas.jboss.LDAPLoginModule" flag="required" module="adalid.jaas.jboss">**