Manual de instalación y configuración Apache Tomcat para el uso del Portfolio SCSP J2EE

Proyecto: Librerías SCSP v4.22.0

Título: Manual de instalación y configuración Apache Tomcat para el uso del Portfolio SCSP J2EE

Revisión: 2.10

Fecha: Abril de 2020

Ficha del documento

Fecha	Revisión	Autor	Verificado por
20/06/2012	1.0	Oficina Técnica	

Documentos relacionados

Fecha	Revisión	Titulo
23/03/2020	1.17	Manual de instalación configuración y uso herramienta de test del Portfolio SCSP J2EE.pdf

Lista de distribución del documento

Fecha	Nombre
20/06/2012	Administraciones Públicas

Control de versiones

Fecha	Revisión	Descripción del cambio
20/06/2012	1.0	Versión inicial.
27/05/2013	1.1	Adaptación a las librerías 3.3.0
04/04/2014	1.2	Adaptación para la última versión del Portfolio SCSP J2EE
19/09/2019	1.3	Adaptación para la última versión del Portfolio SCSP J2EE
22/01/2015	1.4	Adaptación para la última versión del Portfolio SCSP J2EE
12/01/2016	1.5	Adaptación para la última versión del Portfolio SCSP J2EE
10/04/2016	1.6	Adaptación para la última versión del Portfolio SCSP J2EE
10/08/2016	1.7	Adaptación para la última versión del Portfolio SCSP J2EE
12/01/2017	1.8	Adaptación para la última versión del Portfolio SCSP J2EE
30/01/2017	1.9	Corrección de erratas
03/07/2017	2.0	Adaptación para la última versión del Portfolio SCSP J2EE
16/10/2017	2.1	Adaptación para la última versión del Portfolio SCSP J2EE

06/11/2017	2.2	Adaptación para la última versión del Portfolio SCSP J2EE
30/01/2018	2.3	Adaptación para la última versión del Portfolio SCSP J2EE
19/03/2018	2.4	Corrección de erratas
07/05/2018	2.5	Adaptación para la última versión del Portfolio SCSP J2EE
13/07/2018	2.6	Adaptación para la última versión del Portfolio SCSP J2EE
09/11/2018	2.7	Adaptación para la última versión del Portfolio SCSP J2EE
04/07/2019	2.8	Adaptación para la última versión del Portfolio SCSP J2EE
23/03/2020	2.9	Adaptación para la última versión del Portfolio SCSP J2EE
24/04/2020	2.10	Corrección de erratas

Contenido

1 Introducción

El presente manual describe el procedimiento de instalación y configuración de Apache Tomcat para el uso del Portfolio SCSP.

El manual se divide en 2 secciones.

La primera sección presenta la configuración de Apache Tomcat para el uso del servidor de aplicaciones a través de https, y la configuración para el acceso a servicios que requieran autenticación de cliente

La segunda sección describe mediante pasos el proceso de configuración de los certificados necesarios para el correcto funcionamiento del Portfolio SCSP.

1.1 Propósito

Este documento pretender ser una guía de referencia para una configuración simple de Apache Tomcat para el uso del Portfolio SCSP.

1.2 Alcance

Este documento nos indica el procedimiento para una instalación y configuración del servidor de Aplicaciones Apache Tomcat para el uso de del Portfolio SCSP.

1.3 Resumen

En este documento, trataremos de explicar paso a paso la instalación y configuración simple del servidor de aplicaciones Apache Tomcat para el uso del Portfolio SCSP. Abordaremos igualmente la configuración de certificados necesarios para el consumo de servicios y para el acceso a las aplicaciones.

2 Requisitos para la instalación

A continuación se enumeran los requisitos para la instalación y configuración del servidor de aplicaciones Apache Tomcat.

- Paquete de instalación de Apache Tomcat 6, utilizaremos la última versión disponible de esta versión que es la 6.0.37 pudiéndose obtener de la siguiente URL http://tomcat.apache.org/download-60.cgi en el manual se utilizará el paquete que viene comprimido en .zip el cual no necesita instalación. http://apache.rediris.es/tomcat/tomcat-6/v6.0.37/bin/apache-tomcat-6.0.37.zip
- JRE 1.8.x instalado, se puede obtener desde la siguiente URL https://www.oracle.com/java/technologies/javase/javase-jdk8-downloads.html
- Librerías JCE (Java Cryptographic Extension) para utilizar certificados de mas de 1024bits y longitudes de clave de 256bits, se pueden obtener desde la URL https://www.oracle.com/java/technologies/javase-jce8-downloads.html
- Certificado de usuario para el acceso con autenticación de cliente. **
- Certificado de servidor para el acceso vía https a las aplicaciones. **
- Partes públicas de los certificados necesarios para el acceso a las aplicaciones y para consumir los servicios. ***
- Aplicación de testeo de la configuración de las Librerías SCSP, está disponible en la carpeta ***Software_Portfolio-SCSP-v4.X.X\AplicacionesTest\TestConfiguracion.war*** del software distribuido.
- Driver de la Base de Datos utilizada, se pueden obtener de la carpeta de recursos del software distribuido o de las siguientes URLs para cada una de las bases de datos
    - MySQL http://dev.mysql.com/downloads/connector/j/
    - Oracle http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html
    - PostgreSQL http://jdbc.postgresql.org/download.html
    - SQLServer http://go.microsoft.com/fwlink/?LinkId=144633&clcid=0x409
    - MariaDB: https://mariadb.com/kb/en/library/about-mariadb-connector-j/

** No se distribuyen los certificados de servidor y usuario, puesto que deben ser propios de cada usuario
*** No se distribuyen las partes públicas usadas en el establecimiento SSL de las comunicaciones con los servicios utilizados a través de las librerías, deberán ser descargadas desde cada URL correspondiente.

3 Obtención de recursos

Antes de empezar a realizar la configuración es necesario descargar la aplicación de Test de la configuración. Esta aplicación se puede descargar del CTT a través de la URL http://administracionelectronica.gob.es/es/ctt/scsp en la cual deberá estar registrado para poder realizar la descarga.

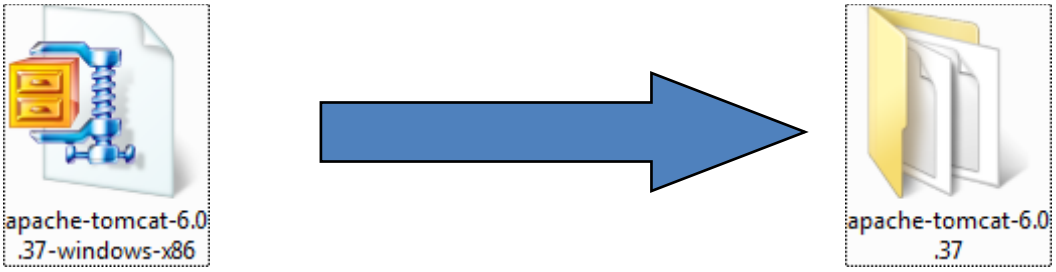
La aplicación se encuentra en la ruta ***Software_Portfolio-SCSP-v4.22.0 \AplicacionesTest*** del paquete de software descargado.

Los demás recursos se pueden obtener de las URLS indicadas en el punto 2.

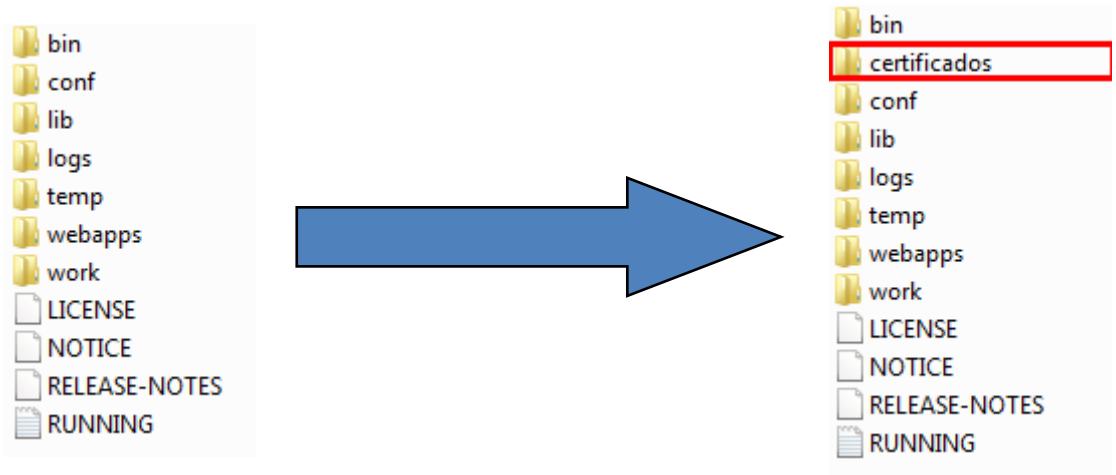
4 Procedimiento de instalación

La instalación de Tomcat la realizaremos bajo un entorno Windows, si la instalación se realiza sobre un entorno Linux, las rutas de instalación serán diferentes.

Una vez descargado el paquete de instalación de Apache Tomcat, para su instalación, únicamente debemos descomprimir ese mismo paquete en la ruta en la que queramos que quede instalado.



A continuación si entramos a *apache-tomcat-6.0.35* veremos la estructura de directorios de tomcat, en la que crearemos la carpeta *certificados* **, donde vamos a incluir todos los certificados usados.



** La carpeta certificados puede encontrarse en cualquier parte del sistema de archivos, pero por comodidad se ha puesto dentro del mismo servidor de aplicaciones.

5 Configuración Apache Tomcat

A continuación se describirá como se debe configurar Apache Tomcat para el uso del Portfolio SCSP.

5.1 Configuración autenticación de cliente

Tanto para el uso del cliente ligero como del administrador de las librerías, es requerida la autenticación de cliente para el acceso, así como para la comunicación con algunos servicios externos a la plataforma de intermediación.

Desde versiones 4.6.0 es posible realizar la configuración de autenticación de cliente desde el Administrador SCSP

5.2 Configuración librerías APR

Al activar el conector https se han encontrado conflictos con estas librerías preconfiguradas en Apache Tomcat, unicamente debemos deshabilitar el uso de estas librerías.

En el archivo ***apache-tomcat-6.0.37\conf\server.xml*** debemos comentar el uso de estas librerías de la siguiente forma.

Librerías habilitadas

```
<!--APR library loader. Documentation at /docs/apr.html -->
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
<!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
```

Librerías deshabilitadas

```
<!--APR library loader. Documentation at /docs/apr.html -->
<!--Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" /-->
<!--Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto.html -->
```

5.3 Configuración conector https

Para el acceso a las aplicaciones es necesario establecer un conector https en tomcat, así como para securizar todas las comunicaciones entre los posibles clientes emisores y las Librerías SCSP. A continuación configuraremos este conector en tomcat para poder acceder a las aplicaciones vía https.

En el archivo ***apache-tomcat-6.0.35\conf\server.xml*** debemos añadir un conector como el siguiente, este conector se añade en la parte de conectores entre los tags ***<Service name="Catalina"></Service>*** por comodidad y orden lo añadiremos justo debajo del conector existente del puerto 8080

```
<Connector
        port="8443"
        protocol="HTTP/1.1"
        SSLEnabled="true"
        maxThreads="150"
        scheme="https"
        secure="true"
        clientAuth="true"
        sslProtocol="TLS"
        keystoreFile="\certificados\self_signed_ssl.p12"
        keystoreType="pkcs12"
        keystorePass="changeit"
        truststoreFile="\certificados\truststore.jks"
        truststoreType="JKS"
        truststorePassword="changeit"/>
```

A continuación se muestra una imagen de cómo quedaría configurado.

```
<Connector
    port="8443"
    protocol="HTTP/1.1"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https"
    secure="true"
    clientAuth="true"
    sslProtocol="TLS"
    keystoreFile="\certificados\self_signed_ssl.p12"
    keystoreType="pkcs12"
    keystorePass="changeit"
    />
```

** El certificado **self_signed_ssl.p12** debe ser sustituido por un certificado propio de servidor

Dónde:

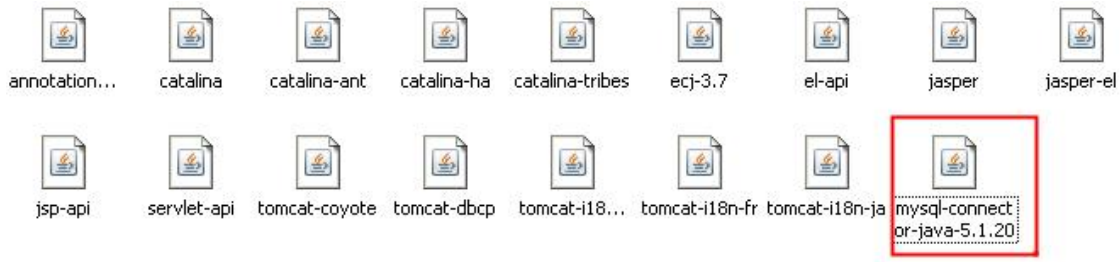
- […] → Es la ruta de apache tomcat.
- self_signed_ssl.p12 → Debe ser sustituido por un certificado de servidor propio
- truststore.jks → debe ser creado con las partes públicas de las CA de los certificados que se utilizarán para acceder al servidor de aplicaciones.

  Ejecutando:
  keytool -importcert -file {ruta a la CA a importar} -alias {nombre de alias a incluir} -keystore {ruta al servidor de aplicaciones}\certificados\truststore.jks -storetype JKS -storepass changeit
  Con el primer certificado a importar se creará dicho almacén

5.4 Configuración drivers Base de Datos

Con las aplicaciones del Portfolio SCSP no se distribuyen los drivers de Base de Datos, esto es debido a que estos drivers deben ir en el directorio lib de tomcat ***apache-tomcat-6.0.37\lib*** debido a que así se recomienda.

A continuación se muestra un ejemplo de un driver correspondiente a MySQL en el directorio indicado, para el uso de este gestor de Base de Datos.



Estos drivers se pueden encontrar en las páginas correspondientes de cada gestor de Base de Datos, *véase punto 2* o por el contrario en la distribución que se realiza de las librerías.

5.5 Configuración usuarios Apache Tomcat

Para tener acceso al manager de tomcat y poder desplegar aplicaciones a través de este, es necesario que se configuren los usuarios para tal fin.

En el fichero ***-tomcat-6.0.37\conf\tomcat-users.xml*** vamos añadir el usuario admin con los roles correspondientes.

En primer lugar se debe descomentar todos los roles y usuarios, y posteriomente añadir las líneas.

```
<role rolename="admin"/>
<user username="admin" password="admin" roles="admin,manager"/>
```

Una imagen de como quedaría la configuración final, se puede ver a continuación

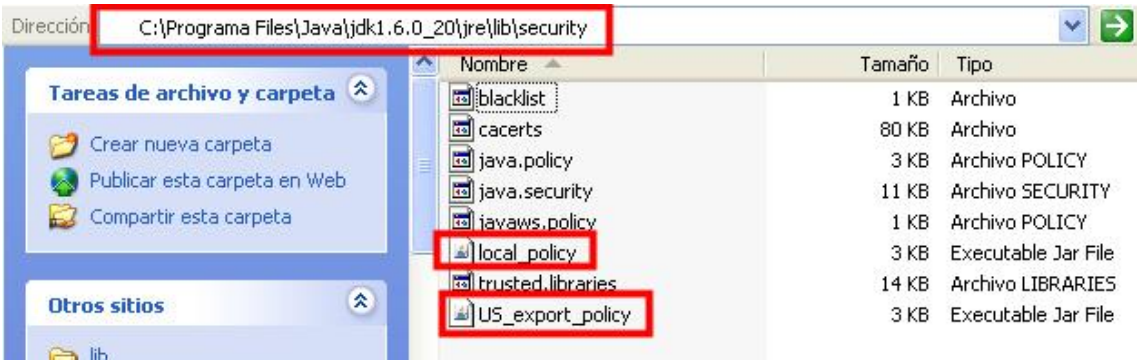
```
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename="root"/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
<user username="root" password="root" roles="admin,manager"/>
```

5.6 Configuración librerías JCE

Debido a una restricción de JRE para manejar certificados con una longitud de clave de más de 1024 bits y métodos de encriptación/firma con una longitud de clave de 256bits o mayor, se deben modificar dos librerías de la JRE, las librerías JCE (Java Cryptograpihc Extension).

Las librerías descargadas ***local_policy.jar*** y ***US_export_policy.jar*** (Véase punto 2) se deben sustituir en la ruta ***jre\lib\security*** sobrescribiendo las librerías existentes.

Se puede ver como quedaría la sustitución a continuación.



5.7 Importación de claves públicas en keystore

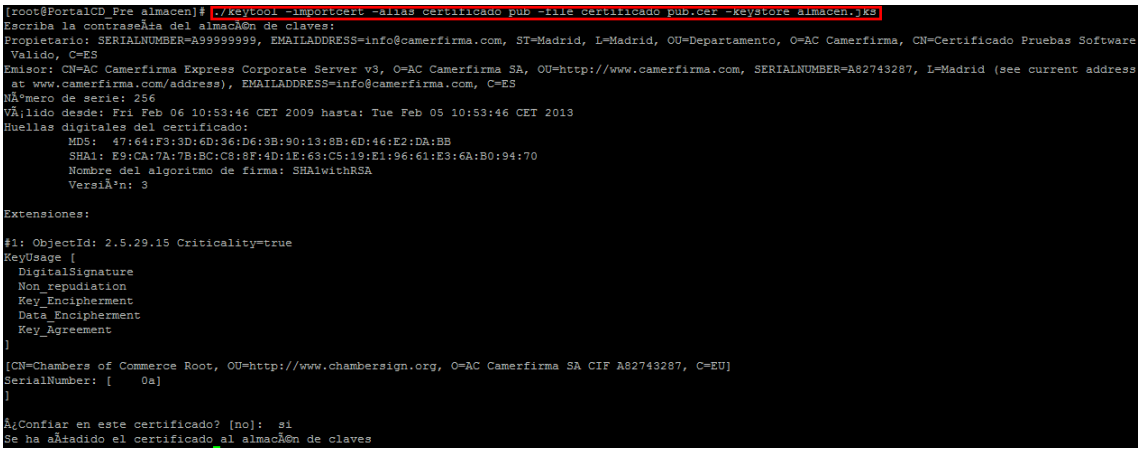
En el almacén de claves debemos tener importadas las partes públicas de los certificados que exponen los servicios vía https, así como las Cas de los certificados con los que nos conectaremos a nuestro propio servidor para autenticarnos como clientes.

Para añadir una clave pública al almacén utilizaremos el siguiente comando.

El almacén de claves por defecto se encuentra en ***jre/lib/security/cacerts***
Las claves públicas de los servicios comunes se encuentran en la carpeta de recursos distribuida

./keytool -importcert -alias **[cert_alias]** -file **[cert_file]** -keystore **[keystore]**

Al ejecutarlo nos pedirá la clave del almacén de certificados. Podemos verlo en la siguiente pantalla.



Dónde:

- **[cert_alias]** es el alias con el que guardaremos el certificado
- **[cert_file]** es el certificado a importar
- **[keystore]** es el almacén de claves

6 Testeo de configuración

A continuación vamos a testear la configuración que hemos realizado, para ello vamos a instalar una aplicación de test y a testear esta configuración siguiendo el manual "*Manual de instalacion, configuracion y uso herramienta de test del Portfolio SCSP J2EE.pdf*"

7 Definiciones, acrónimos y abreviaturas

Acrónimo	Significado
SCSP	Sustitución Certificados Soporte Papel
CTT	Centro de Transferencia tecnológica
BBDD	Bases de Datos
Keytool	Herramienta de manejo de certificados
JKS	Java KeyStore
@Firma	Plataforma de validación de certificados
PKCS12	Formato de un almacén de certificados de clave privada y pública
CA	Autoridad Certificadora