Manual de configuración de SSL en Apache Tomcat 8.5

Autor: Iván E. Tinajero Díaz

Al publicar un servidor Tomcat en Internet es recomendable permitir sólo HTTPS y acceder a él mediante un certificado digital firmado por una CA. El proceso para activar SSL en Tomcat se divide en dos partes:

1. Crear un keystore funcional
2. Configurar los conectores para usar SSL.

Veamos primero como crear el keystore.

Crear un keystore funcional

Las claves que Tomcat usará para las transacciones SSL se almacenan en un fichero protegido por contraseña llamado "**keystore**". El formato de este fichero es el estándar de Java **JKS ("Java KeyStore")** y es creado por la utilidad keytool que incluye el JDK. Para crearlo debemos realizar lo siguiente:

- Escribir el siguiente comando en la terminal:
  # keytool -genkey -alias tomcat -keyalg RSA -keystore /home/ivan/servidor/certificado-ssl.jks
  Nota: aquí puede cambiar la ruta y nombre del archivo keystore. En este ejemplo se usará **/home/ivan/servidor/certificado-ssl.jks**

- Enseguida se solicitarán algunos datos. Hay que completar los datos.

Campo	Descripción
First & Last Name	Dominio para el que se genera el certificado
Organizational Unit	Campo opcional que se refiere al departamento dentro de la empresa
Organization	Nombre legal de la empresa
City / Locality	Localidad
State / Province	Provincia
Country Code	Código de dos letras del país

Ejemplo:

Enter keystore password: **key123**
Re-enter new password: **key123**
What is your first and last name?
[Unknown**]: www.example.com**
What is the name of your organizational unit?
[Unknown]: **IT**
What is the name of your organization?
[Unknown]: **My Company**
What is the name of your City or Locality?
[Unknown]: **My City**
What is the name of your State or Province?
[Unknown]: **My State**

What is the two-letter country code for this unit?
[Unknown]: **MX**
Is CN=www.example.com, OU=IT, O=My Company, L=My City, ST=My State, C=MX correct? [no]: **yes**
Enter key password for <tomcat>
(RETURN if same as keystore password): **Enter**

Nota: No olvidar keystore password. En este ejemplo se ingresó la clave **key123**

Configurar los conectores para usar SSL

Ahora que ya tenemos nuestro **keystore** creado localmente ya podemos configurar Tomcat para usar SSL. Este sería el procedimiento:

- Abrir el archivo de configuración de Tomcat: **apache-tomcat-8.5.23/conf/server.xml.** Buscar en este archivo el conector para el puerto 8443 por default que deberá estar comentado.

- Después de localizar el conector, agregar la siguiente configuración:

```
<Connector
        protocol="org.apache.coyote.http11.Http11NioProtocol"
        port="8443"
        maxThreads="200"
        scheme="https"
        secure="true"
        SSLEnabled="true"
        keystoreFile="/home/ivan/servidor/certificado-ssl.jks"
        keystorePass="key123"
        clientAuth="false"
        sslProtocol="TLS"/>
```

  Nota: Personalizar los valores para el atributo **keystoreFile** y **keystorePass**, dependiendo de los valores en el momento de crear el keystore.

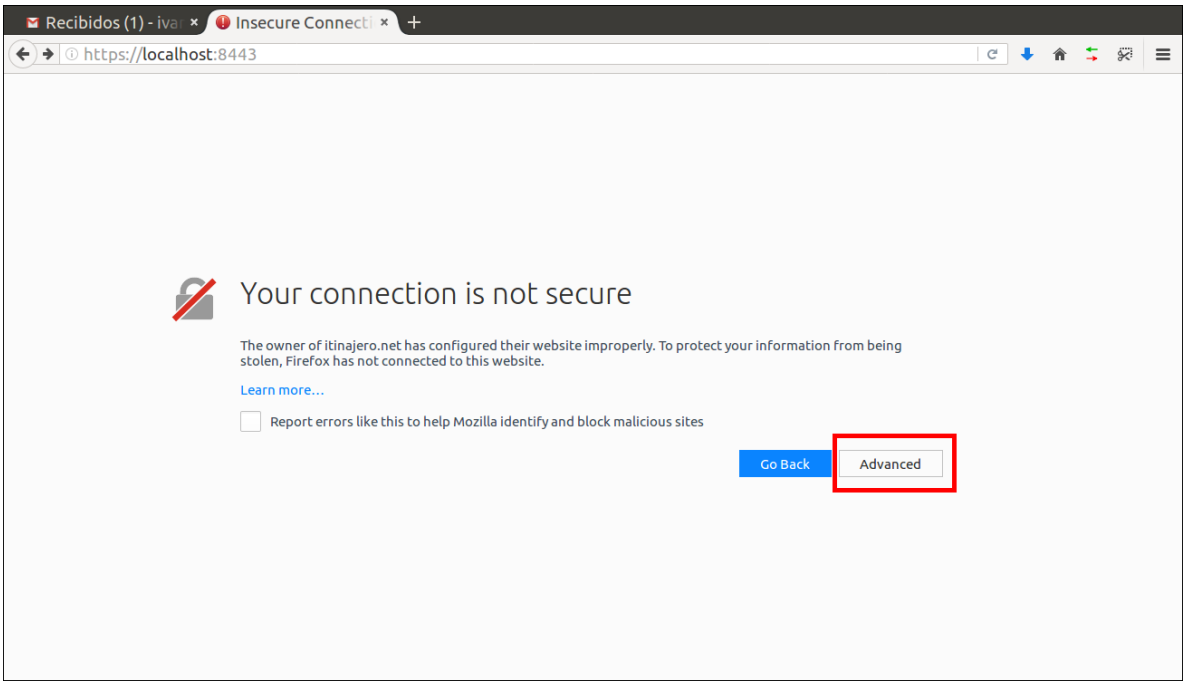
- Reiniciar Apache Tomcat.

- Despúes de reiniciar Tomcat, ya podríamos ver si el puerto 8443 está abierto en el servidor.

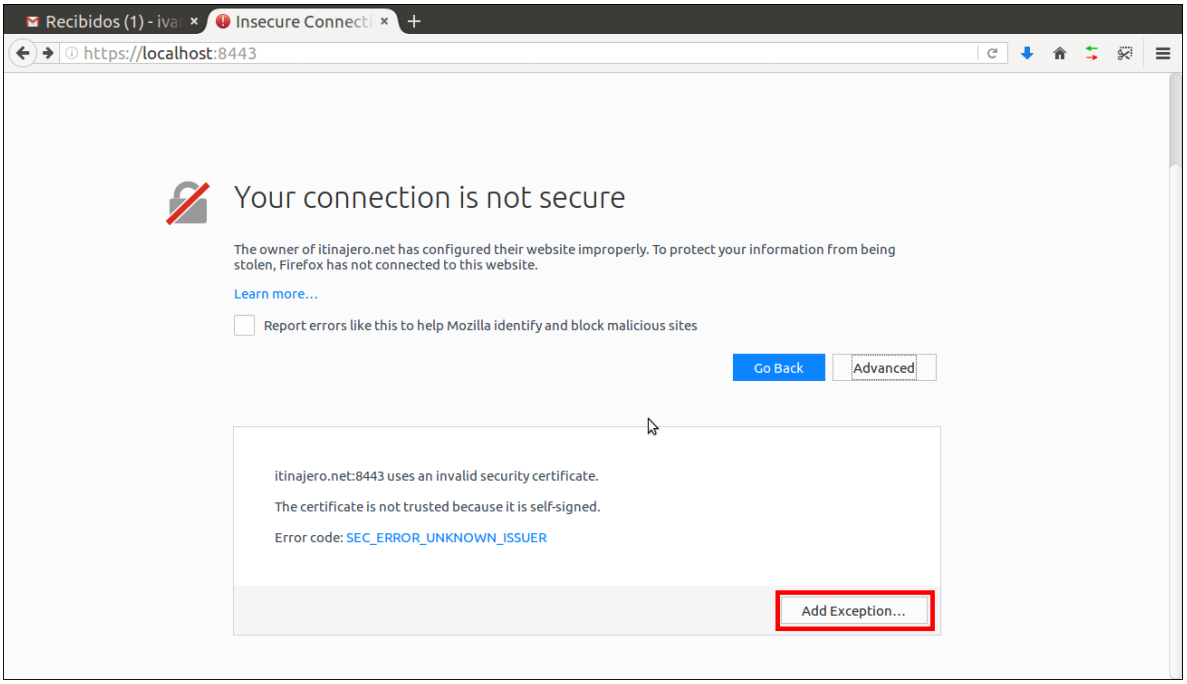
```
# netstat -lpn | grep :8443
tcp6       0      0 :::8443                 :::*                    LISTEN      5297/java
```

Probar la conexión Https desde Firefox.

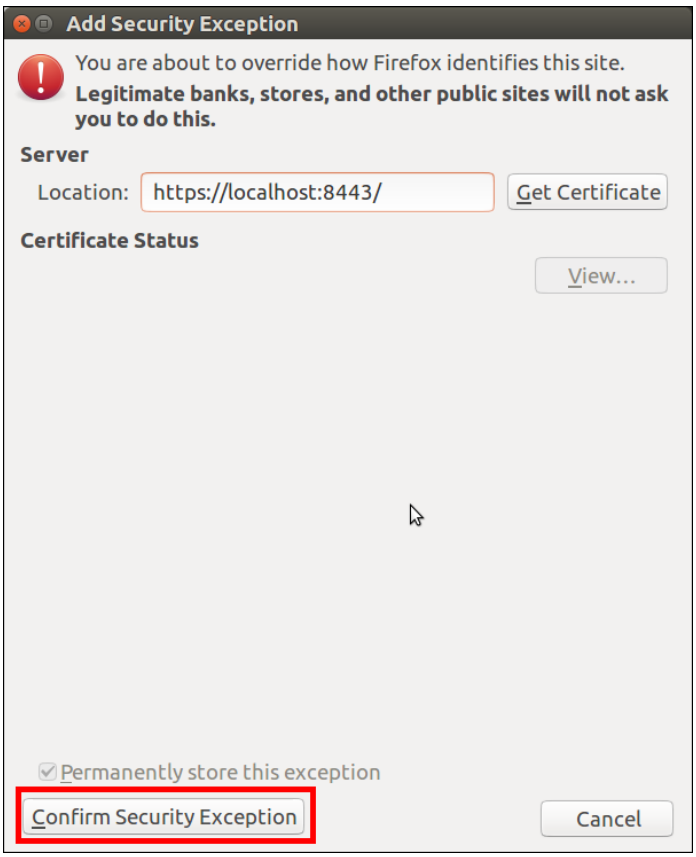
Abrir el navegador de internet y escribir la url https://localhost:8443. Aparecerá el mensaje de que la conexión no es segura. Dar clic en Advanced.



Enseguida, dar clic en el botón Add Exception.



Finalmente, dar clic en el botón Confirm Security Exception.



En este punto, ya debería aparecer la página principal de Apache Tomcat con https.