

## Actividad Tomcat. Conexiones seguras HTTPS

1. Se pide activar el soporte SSL en el sitio localhost de Tomcat. Para ello:

- a) Usando la herramienta keytool vamos a generar el certificado digital que empleará Tomcat con la orden:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore /var/lib/tomcat8/almacen_claves
```

donde alias (tomcat) es el nombre creado para este certificado digital y /var/lib/tomcat8/almacen\_claves es el fichero de almacen del certificado y clave privada

Se nos pedirá la contraseña del almacén y la del alias (que pueden ser la misma) y se solicitan también los datos habituales del certificado: organización, país, provincia, etc..

- b) Una vez generado se debe editar el fichero /etc/tomcat9/server.xml y añadir un conector para las conexiones seguras al puerto 8443. Se muestra captura del bloque de configuración:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="/var/lib/tomcat8/almacen_claves"
    keystorePass="naranco"
    keyAlias="tomcat" keyPass="naranco"/>
```

Es importante fijarse en que el valor de keystorePass es el valor de la contraseña del almacén anterior y keyPass es la contraseña del alias del certificado anterior (en este ejemplo son "naranco")

- c) Una vez reiniciado el servicio tomcat9 debemos probar el acceso a las aplicaciones con conexión segura, accediendo desde el equipo Linux o Windows a <https://www.midominio.com:8443/aplicacion>
- d) Para forzar una aplicación del tal modo que se redirija automáticamente a la conexión segura debemos editar el descriptor del despliegue web.xml que se encuentra dentro de la carpeta de la aplicación, bajo el directorio WEB-INF y agregar el siguiente bloque:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Viewpoint Secure URLs</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
</security-constraint>
<user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

dentro del bloque <web-app></web-app>

Finalmente se debe reiniciar tomcat9

Se debe elegir una aplicación cualquiera que ya tengamos desplegada y modificarla para que redirija a la conexión segura

Verificarlo en el navegador, accediendo a  
<http://www.midominio.com:8080/aplicacion>

## Resolver

Lo primero es crear la carpeta en la cual almaceno las claves

```
alumno@debian11:~$ su -
Contraseña:
root@debian11:~# cd /var/lib/tomcat9
root@debian11:/var/lib/tomcat9# ls
conf lib logs policy tomcat1 tomcat2 webapps work
root@debian11:/var/lib/tomcat9# mkdir almacen_claves
root@debian11:/var/lib/tomcat9# ls
almacen_claves conf lib logs policy tomcat1 tomcat2 webapps work
root@debian11:/var/lib/tomcat9#
```

La contraseña es naranco

```
root@debian11:/var/lib/tomcat9# keytool -genkey -alias tomcat -keyalg RSA -keystore almacen_claves
Introduzca la contraseña del almacén de claves:
Olvolver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
[Unknown]: fabricio
¿Cuál es el nombre de su unidad de organización?
[Unknown]: naranco
¿Cuál es el nombre de su organización?
[Unknown]: DAW
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: Oviedo
¿Cuál es el nombre de su estado o provincia?
[Unknown]: Asturias
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: ES
¿Es correcto CN=fabricio, OU=naranco, O=DAW, L=Oviedo, ST=Asturias, C=ES?
[no]: si
error de herramienta de claves: java.io.FileNotFoundException: almacen_claves (Es un directorio)
```

```
[3]+ Detenido          service tomcat9 status
root@debian11:/var/lib/tomcat9# service tomcat9 restart
root@debian11:/var/lib/tomcat9# █
```

```

// ...
</>

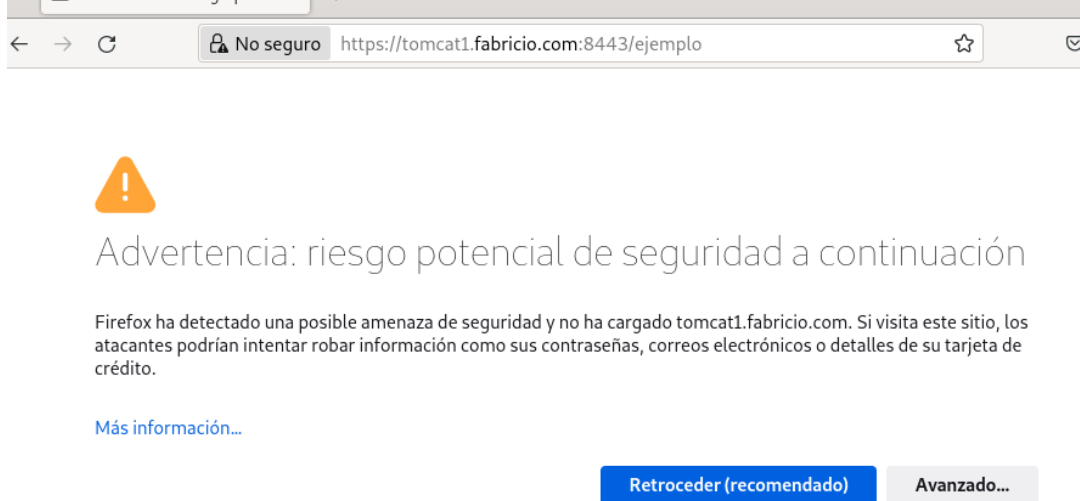
```

```

6         <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
7             maxThreads="150" scheme="https" secure="true"
8             clientAuth="false" sslProtocol="TLS"
9             keystoreFile="/var/lib/tomcat9/almacen_claves"
10             keystorePass="naranco"
11             keyAlias="tomcat" keyPass="naranco"/>
12     <!-- A "Connector" using the shared thread pool-->
13     <!--

```

⚠ Advertencia: riesgo poten × +



```

<servlet>
  <servlet-name>HelloServlet</servlet-name>
  <servlet-class>mypackage.Hello</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>HelloServlet</servlet-name>
  <url-pattern>/hello</url-pattern>
</servlet-mapping>
  <security-constraint>
<web-resource-collection>
  <web-resource-name>Viewpoint Secure URLs</web-resource-name>
  <url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
</web-app>

```

Y ahora redirige a la pagina indicada en conexión segura

**Gestor de Aplicaciones Web de Tomcat**

Mensaje: OK

**Gestor**

[Listar Aplicaciones](#) [Ayuda HTML de Gestor](#) [Ayuda de Gestor](#) [Estado de Servidor](#)

Aplicaciones					
Ruta	Versión	Nombre a Mostrar	Ejecutándose	Sesiones	Comandos
/	Ninguno especificado	ROOT	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
/ejemplo	Ninguno especificado	Hello, World Application	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar ≥ 30 minutos
...	...	...	...	...	Arrancar Parar Recargar Replegar

