SSL en Tomcat

1. Crear un almacén de claves con un certificado SSL
1.1 Inicia sesión en la máquina virtual con un usuario con privilegios de administración
1.2 Utiliza la herramienta keytool para crear un certificado autofirmado y almacenarlo en un almacén de claves JKS. Durante la generación del certificado se tienen que introducir dos claves, la del almacén de claves (daw1keystore) y la de las claves asociadas a alias (tomcat) creado. En ambos casos pondremos como clave tomcat.

```
root@sriserver:~# keytool -genkey -alias tomcat -keyalg RSA -keystore /var/lib/tomc
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  Victor Sanchez Garcia
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  tomcat
¿Cuál es el nombre de su organización?
  [Unknown]:  daw01.net
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  Collado Villalba
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  Madrid
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  ES
¿Es correcto CN=Victor Sanchez Garcia, OU=tomcat, O=daw01.net, L=Collado Villalba,
```

2. Configurar un conector SSL en Tomcat
2.1 En La máquina virtual edita el fichero /var/lib/tomcat9/conf/server.xml y realiza la configuración que se muestra a continuación dentro de la etiqueta (por encima del)

```
<Connector
    port="8443"
    protocol="HTTP/1.1"
    SSLEnabled="true"
    maxThreads="150"
    scheme="https"
    secure="true"
    ClientAuth="false"
    sslProtocol="TLS"
    keystoreFile="/var/lib/tomcat9/daw01keystore"
    keyAlias="tomcat"
    keystorePass="tomcat"
    keyPassword="tomcat"
/>

<Engine name="Catalina" defaultHost="localhost">
```

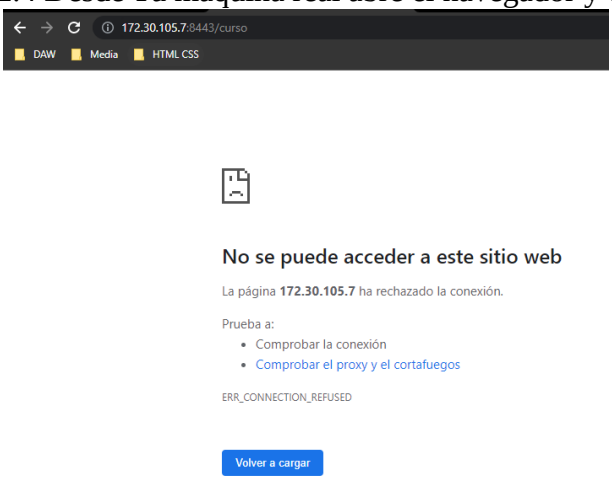
2.2 Reinicia Tomcat

```
root@sriserver:~# service tomcat9 restart
```

2.3 Comprueba que el servidor está iniciado y escuchando en los puertos 8080/TCP y 8443/TCP

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::8443                 :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

2.4 Desde Tu máquina real abre el navegador y establece una conexión a la máquina virtual



2.4 ¿Qué mensaje de advertencia te da el navegador? ¿Por qué?

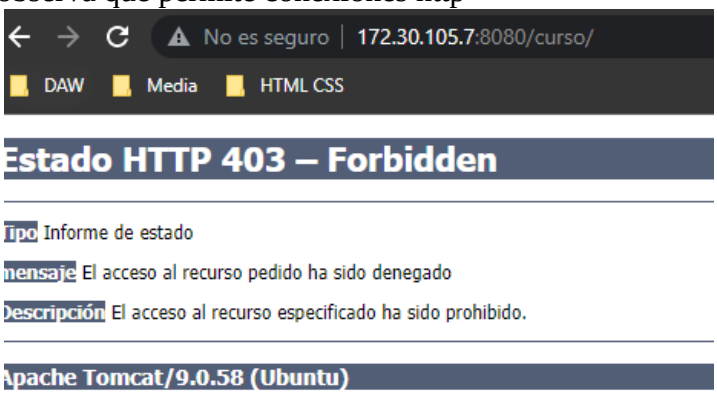
Me dice que no puedo acceder al sitio, el motivo es que el https no está configurado.

2.5 Muestra un pantallazo desde tu máquina real del certificado del servidor Tomcat. ¿Con qué algoritmo se generó la clave?

*Nota para Benito: Sale el nombre de Alberto porque tuve que importa su máquina virtual

2.6 ¿Para qué crees que sirve la información de la huella digital del certificado?

3 Configurar la aplicación curso para que sólo permita conexiones https
3.1 Desde tu máquina real abre el navegador y establece una conexión a http://IPMV:8080/curso y observa que permite conexiones http

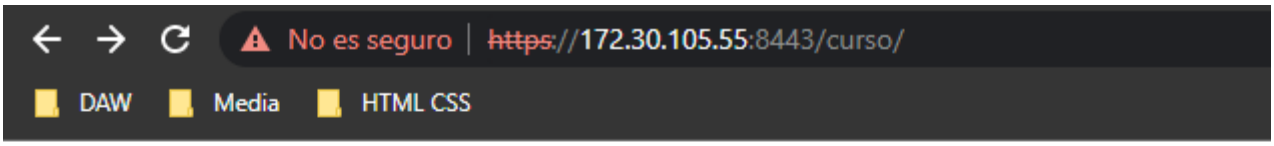


*Nota para Benito: le echaste un ojo conmigo y me dijiste que subiese este pantallazo y saltase al siguiente punto.

3.2 Edita el descriptor de despliegue de la aplicación curso y realiza la siguiente configuración

```
 </Connector>
 -->

<security-constraint>

     <user-data-constraint>
             <transport-guarantee>CONDIFENTIAL</transport-guarantee>
     </user-data-constraint>

</security-constraint>


 <!-- Define an AJP 1.3 Connector on port 8009 -->
```

3.3 Desde tu máquina real abre el navegador y establece una conexión a http://IPMV:8443/curso y observa la petición se redirige a https://IPMV:8443/curso



Curso de despliegue de aplicaciones web

- Hola (Servlet)
- Buenas (JSP)

3.4 ¿Qué dos formas hay de realizar es cambio en el descriptor de la aplicación? ¿Qué ventajas e inconvenientes tiene cada una?

Desde *var*/lib/tomcat9/conf/server.xml

o

var/lib/tomcat9/webapss/curso/WEB-INF/web.xml