

PRÁCTICA 3.1

INSTALACIÓN Y CONFIGURACIÓN DE TOMCAT



Contenido

PRÁCTICA 3.1 2

 INSTALACIÓN Y CONFIGURACIÓN DE TOMCAT 2

 OBJETIVOS..... 2

 ENUNCIADO 2

 CREACION USUARIO 2

 PRIMERA PARTE - Configuracion de SSL 4

 SEGUNDA PARTE - Desplegar una aplicación 4

 DOCUMENTACIÓN 4

 PARTE 1: Configuración de SSL..... 4

 PARTE 2: Despliegue de la Aplicación 9

 Comprobación desde otro equipo 12

PRÁCTICA 3.1

INSTALACIÓN Y CONFIGURACIÓN DE TOMCAT

RA ASOCIADO: RA2. Implanta aplicaciones web en servidores de aplicaciones evaluando y aplicando criterios de configuración para su funcionamiento seguro

CEs ASOCIADOS: d, e, f, g, h, i.

OBJETIVOS

- Aprender a implantar aplicaciones web en servidores de aplicaciones.
- Habituarse a la descripción del proceso.

ENUNCIADO

Se desarrollará la práctica en un Ubuntu Server que disponga de un servidor de Tomcat instalado.

Se utilizará como nombre de dominio: segundo.daw.iesagl.fic.

El servidor tendrá al menos una de sus interfaces en MODO PUENTE, de forma que se pueda acceder

desde cualquier equipo del aula.

En Tomcat habrá un usuario con capacidad de gestión de aplicaciones a través de la interfaz web, con

credenciales: useradmin / 4321.

CREACION USUARIO

Añadiremos un usuario a el fichero de: tomcat-users.xml

```
adrian@ubuntuserver-adrian: X + v
GNU nano 7.2 /opt/tomcat/conf/tomcat-users.xml *
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->

<tomcat-users xmlns="http://tomcat.apache.org/xml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
  version="1.0">

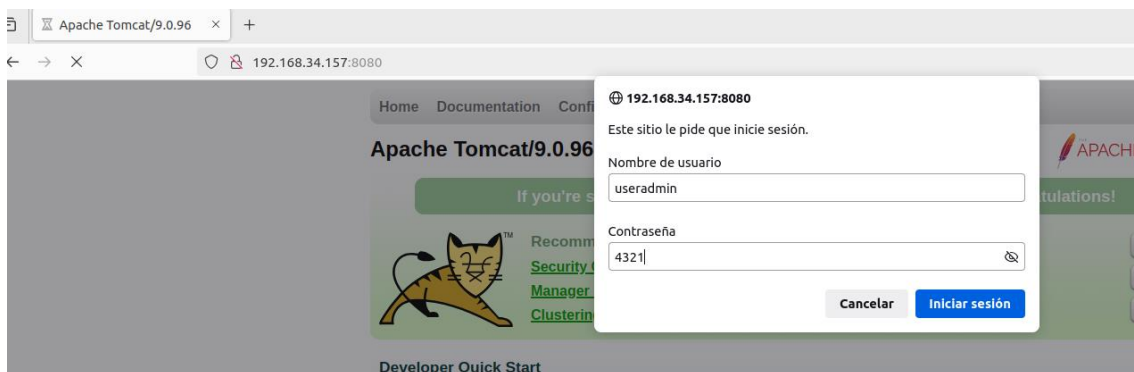
  <user username="useradmin" password="4321" roles="manager-gui,admin-gui"/>

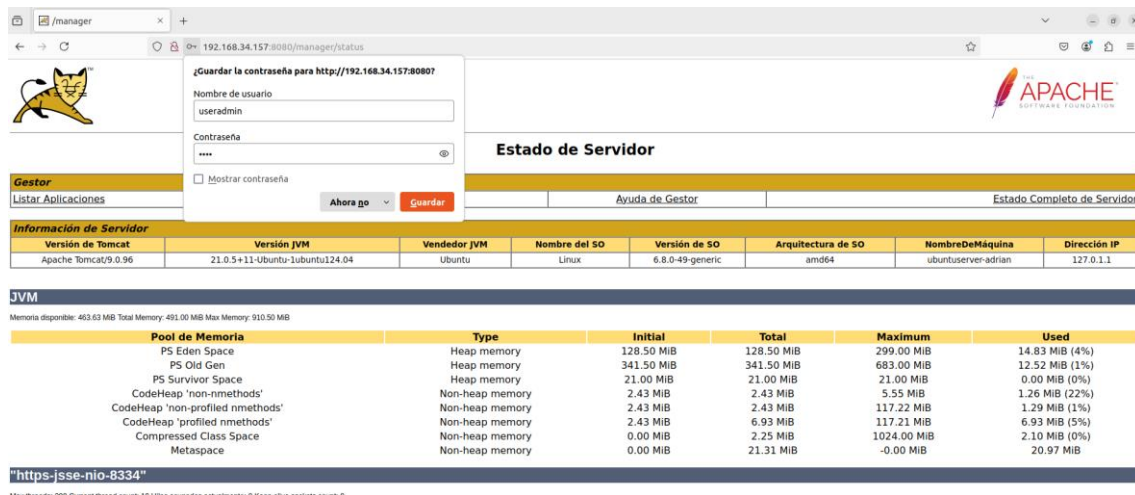
  <user username="admin" password="1234" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

Después para el correcto funcionamiento reiniciaremos el servicio de TomCat:

```
adrian@ubuntuserver-adrian: X + v
adrian@ubuntuserver-adrian:~$ sudo systemctl restart tomcat.service
adrian@ubuntuserver-adrian:~$
```

Comprobación de que el usuario esta añadido correctamente:





The screenshot shows the Apache Tomcat Manager web interface. On the left, there is a login form with fields for 'Nombre de usuario' (username) and 'Contraseña' (password). The username is 'useradmin'. Below the password field is a checkbox for 'Mostrar contraseña' (show password). To the right of the login form is the 'Estado de Servidor' (Server Status) section. Below this, there is a table titled 'Información de Servidor' (Server Information) with columns: Versión de Tomcat, Versión JVM, Vendedor JVM, Nombre del SO, Versión de SO, Arquitectura de SO, NombreDeMáquina, and Dirección IP. The table shows the following data:

Versión de Tomcat	Versión JVM	Vendedor JVM	Nombre del SO	Versión de SO	Arquitectura de SO	NombreDeMáquina	Dirección IP
Apache Tomcat/9.0.96	21.0.5+11-Ubuntu-1ubuntu124.04	Ubuntu	Linux	6.8.0-49-generic	amd64	ubuntuserver-adrian	127.0.1.1

Below the table, there is a section titled 'JVM' showing memory usage statistics. The table has columns: Pool de Memoria, Type, Initial, Total, Maximum, and Used. The data is as follows:

Pool de Memoria	Type	Initial	Total	Maximum	Used
PS Eden Space	Heap memory	128.50 MIB	128.50 MIB	299.00 MIB	14.83 MIB (4%)
PS Old Gen	Heap memory	341.50 MIB	341.50 MIB	683.00 MIB	12.52 MIB (1%)
PS Survivor Space	Heap memory	21.00 MIB	21.00 MIB	21.00 MIB	0.00 MIB (0%)
CodeHeap 'non-nmethods'	Non-heap memory	2.43 MIB	2.43 MIB	5.55 MIB	1.26 MIB (22%)
CodeHeap 'non-profiled nmethods'	Non-heap memory	2.43 MIB	2.43 MIB	117.22 MIB	1.29 MIB (1%)
CodeHeap 'profiled nmethods'	Non-heap memory	2.43 MIB	6.93 MIB	117.21 MIB	6.93 MIB (5%)
Compressed Class Space	Non-heap memory	0.00 MIB	2.25 MIB	1024.00 MIB	2.10 MIB (0%)
Metaspace	Non-heap memory	0.00 MIB	21.31 MIB	-0.00 MIB	20.97 MIB

PRIMERA PARTE - Configuración de SSL

Configura Tomcat para que responda a peticiones HTTPS a través del puerto 8334. Para ello, genera un certificado autofirmado.

SEGUNDA PARTE - Desplegar una aplicación

Realiza una aplicación, que desplegarás en Tomcat, en la que se introduzca un número en una caja de

texto y, pulsando un botón, te diga si el número introducido es divisible entre 13.

Se adjunta un fichero WAR de otra aplicación, por si no diera tiempo a modificar y crear la que se

indica.

DOCUMENTACIÓN

PARTE 1: Configuración de SSL

Generar el certificado autofirmado:

- Crea un directorio para almacenar el certificado:

sudo mkdir /opt/tomcat/ssl

```
adrian@ubuntuserver-adrian:~$ sudo mkdir /opt/tomcat/ssl  
[sudo] password for adrian:  
adrian@ubuntuserver-adrian:~$
```

- Genera el certificado autofirmado utilizando keytool:

```
sudo keytool -genkey -alias tomcat -keyalg RSA -keystore  
/opt/tomcat/ssl/keystore.jks -keysize 2048
```

(A mí con ese comando me daba problemas entonces lo creo por parámetros directamente)

Utilizaremos este comando para poder realizarlo:

```
sudo keytool -genkey -alias tomcat -keyalg RSA -keystore  
/opt/tomcat/ssl/keystore.jks -keysize 2048 \  
-dname "CN=segundo.daw.iesagl.fic, OU=Despliegue, O=IES, L=Santander,  
ST=Cantabria, C=ES" \  
-storepass changeit -keypass changeit
```

Configurar el conector SSL en server.xml:

- Abre el archivo de configuración:

```
sudo nano /opt/tomcat/conf/server.xml
```

- Busca la sección <Service name="Catalina"> y añade el siguiente conector SSL para el puerto 8334:

```
<Connector port="8334" protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
        maxThreads="200" SSLEnabled="true">  
    <SSLHostConfig>  
        <Certificate certificateKeystoreFile="ssl/keystore.jks"  
            certificateKeystorePassword="changeit"  
            type="RSA" />  
    </SSLHostConfig>  
</Connector>
```

```
<Service name="Catalina">  
    <Connector port="8334" protocol="org.apache.coyote.http11.Http11Ni"  
        maxThreads="200" SSLEnabled="true">  
        <SSLHostConfig>  
            <Certificate certificateKeystoreFile="ssl/keystore.jks"  
                certificateKeystorePassword="changeit"  
                type="RSA" />  
        </SSLHostConfig>  
    </Connector>
```

Reiniciar Tomcat:

- Apaga y enciende Tomcat para aplicar los cambios:

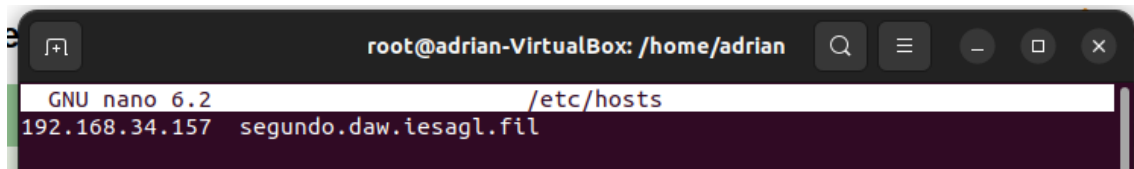
```
sudo /opt/tomcat/bin/shutdown.sh
```

```
sudo /opt/tomcat/bin/startup.sh
```

```
adrian@ubuntuserver-adrian:~$ sudo /opt/tomcat/bin/shutdown.sh
sudo /opt/tomcat/bin/startup.sh
Using CATALINA_BASE:   /opt/tomcat
Using CATALINA_HOME:   /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/
juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL
--add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/ja
=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --
ens=java.rmi/sun.rmi.transport=ALL-UNNAMED
Using CATALINA_BASE:   /opt/tomcat
Using CATALINA_HOME:   /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/
juli.jar
Using CATALINA_OPTS:
Tomcat started.
adrian@ubuntuserver-adrian:~$
```

Verificar el acceso HTTPS:

- Abre un navegador y accede a <https://segundo.daw.iesagl.fic:8334>.



- Si aparece un mensaje sobre el certificado no confiable, es normal debido a que es autofirmado.

Advertencia: riesgo pote: x

← → ↻

No seguro https://segundo.daw.iesagl.fic:8334



Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado **segundo.daw.iesagl.fic**. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

Retroceder (recomendado)

Avanzado...



Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado **segundo.daw.iesagl.fic**. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

Retroceder (recomendado)

Avanzado...

segundo.daw.iesagl.fic:8334 usa un certificado de seguridad no válido.

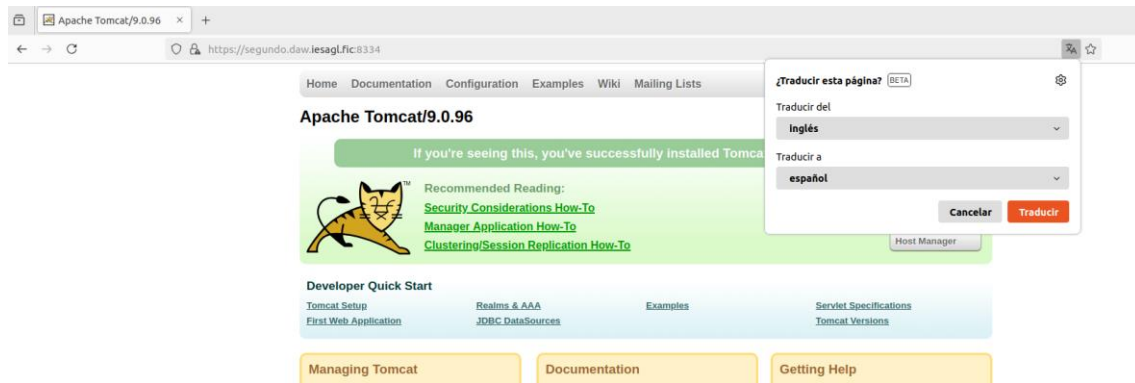
No se confía en el certificado porque está autofirmado.

Código de error: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[Ver certificado](#)

Retroceder (recomendado)

Aceptar el riesgo y continuar



PARTE 2: Despliegue de la Aplicación

Copiar el archivo .war al directorio de despliegue:

- Copia tu archivo .war al directorio webapps de Tomcat:

```
sudo cp tu_aplicacion.war /opt/tomcat/webapps/
```

Para pasarle el archivo de descargas a Ubuntu Server utiliza scp:

Con este comando pasaremos el archivo de mi ordenador al servidor Ubuntu:

```
connection to 192.168.34.157 closed.  
PS C:\Users\Adrián Peña Carnero> scp "C:\Users\Adrián Peña Carnero\Downloads  
BisiestoApp-1.0.war" adrian@192.168.34.157:/opt/tomcat/webapps/  
adrian@192.168.34.157's password:  
BisiestoApp-1.0.war 100% 5270 5.0MB/s 00:00
```

```
PS C:\Users\Adrián Peña Carnero> scp "C:\Users\Adrián Peña  
Carnero\Downloads\BisiestoApp-1.0.war"  
adrian@192.168.34.157:/opt/tomcat/webapps/
```

adrian@192.168.34.157's password:

BisiestoApp-1.0.war 100% 5270 5.0MB/s 00:00

PS C:\Users\Adrián Peña Carnero>

Después como se nos ha añadido directamente a la carpeta /otp/tomcat/webapps simplemente reiniciamos y esperamos a que se despliegue:

```
adrian@ubuntu-server-adrian:/$ sudo systemctl restart tomcat
[sudo] password for adrian:
adrian@ubuntu-server-adrian:/$
```

Verificar el despliegue:

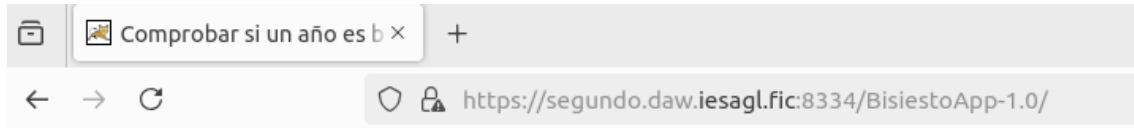
- Espera unos segundos mientras Tomcat despliega la aplicación automáticamente.
- Accede a la aplicación a través de la URL:

http://segundo.daw.iesaglfic:8080/tu_aplicacion



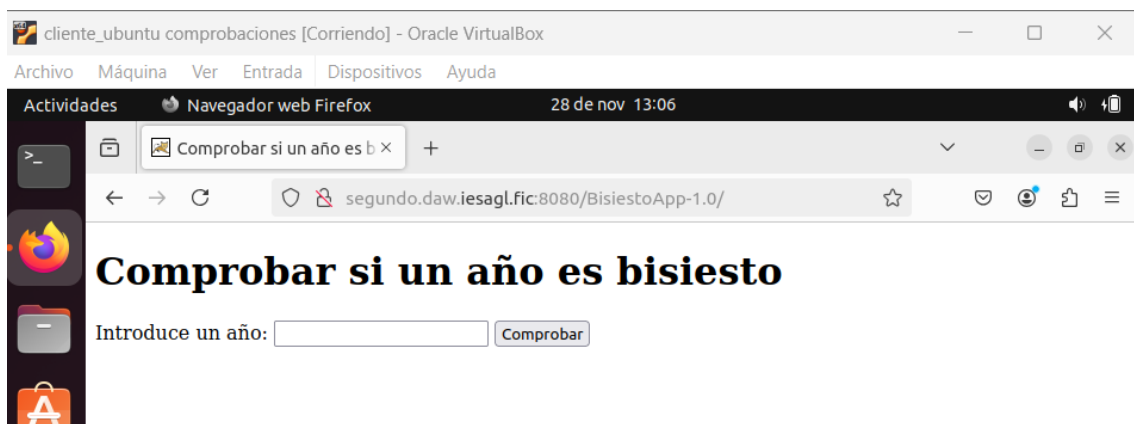
- Si configuraste SSL, también podrás acceder mediante HTTPS:

https://segundo.daw.iesaglfic:8334/tu_aplicacion



Comprobar si un año es bisiesto

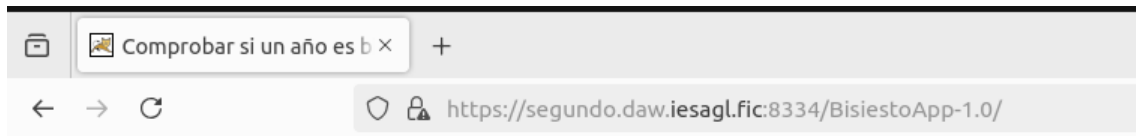
Introduce un año:



Probar la funcionalidad de la aplicación:

En mi caso he utilizado el archivo .war que nos facilitas. Aun así, te muestro la comprobación del .war adjunto:





Comprobar si un año es bisiesto

Introduce un año:

10 no es un año bisiesto.

Comprobación desde otro equipo

Desde el ordenador de mi compañero Alejandro Pila, funciona correctamente:

