Unidad Educativa
“CAPITAN PEDRO OSCAR SALAS BAJAÑA”

SAIN
Sistema Académico Institucional

Guía de Despliegue para la aplicación, a continuación se mostrará de manera detallada todos los requerimientos que el software necesita para poder ser levantado en cualquier computador.

FIEC

Requisitos

- Apache Tomcat 7.0

- Java Development Kit (JDK) versión 7 o superior.

- Sistema Operativo Windows

Para la instalación de cada uno de estos softwares se adjunta el respectivo link para su descarga:

Apache Tomcat: http://tomcat.apache.org/download-70.cgi

JDK: http://www.oracle.com/technetwork/java/javase/downloads/index.html

Creación del certificado

El Software SAIN necesita indispensablemente un certificado seguro para poder ser desplegado por lo que a continuación se mostrara este proceso:

1. Crear un almacén de claves auto-firmado.

Abrimos una ventana de comandos (cmd.exe) y nos ubicamos en el siguiente directorio:

cd %JAVA_HOME%\bin

Escribimos el siguiente comando:

keytool -genkey -alias <key name> -keypass <key password> -keyalg RSA

Para efecto de ejemplo, se usaran los siguientes datos (Sin el menor y mayor que):

<key name> = tomcat

<key password> = changeit

Presionamos enter y se mostrarán algunas preguntas para poder generar el certificado, y las respuestas que deberá colocar:

Enter keystore password: changeit

What is your first and last name?

[Unknown]: grupoF

What is the name of your organizational unit?

[Unknown]: Software

What is the name of your organization?

[Unknown]: ESPOL

What is the name of your City or Locality?

[Unknown]: Guayaquil

What is the name of your State or Province?

[Unknown]: Guayas

What is the two-letter country code for this unit?

[Unknown]: EC

Is CN=compA, OU=Information Systems, O=Pacific Disaster Center, L=Kihei, ST=HI, C=US correct?

[no]: si

Nota: Cabe recalcar que el dato que se coloque como nombre y apellido, será el nombre del dominio que más adelante utilizaremos para usar la conexión segura HTTPS, por lo que una vez entregada la aplicación estos datos se tomaran en consideración con el cliente.

Ahora lo que hacemos es exportamos el certificado generado del almacén de clave.

keytool -export -alias tomcat -keypass changeit -file server.crt

Finalmente, agregamos el certificado al archivo cacerts del JDK.

keytool -import -file server.crt -keypass changeit -keystore ..\jre\lib\security\cacerts

Respondemos: si y cerramos la ventana de comandos.

2. Modificar el archivo host de Windows

La ubicación del archivo host es la siguiente:

C:\Windows\System32\drivers\etc

Abrimos el archivo con un editor de texto cualquiera y agregamos un nuevo dominio al final del archivo, en nuestro caso sería el siguiente.

127.0.0.2 grupoF

Guardamos los cambios y cerramos el archivo.

3. Habilitar la conexión HTTPS en Apache Tomcat

Para habilitarla es necesario abrir el archivo server.xml que se encuentra en la siguiente dirección dentro de la carpeta de Apache Tomcat:

C:\<Directorio de Tomcat Server>\conf\server.xml

Reemplazamos la sección **<!-- Define a SSL HTTP/1.1 .... -->**

Por la siguiente:

```
<Connector port="8443" maxHttpHeaderSize="8192" SSLEnabled="true"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:/Users/<Mi usuario>/.keystore"
keystorePass="changeit"
truststoreFile="C:/Program Files (x86)/Java/jdk1.8.0_05/jre/lib/security/cacerts" />
```

Una vez realizado esto, guardamos lo cambios del archivo y procedemos a reiniciar el servidor de Apache Tomcat.

Nota: No olvidar de cambiar las rutas del almacén de claves de keystoreFile por la ruta donde está alojada su almacén, de igual forma debe cambiar la ruta de truststorefile por la ruta donde está alojada su versión del JDK.

Para más información, puede consultar en: **https://wiki.jasig.org/display/CASUM/Demo**

4. Verificar de la conexión HTTPS

Una vez levantado el servidor, entramos a la siguiente URL haciendo uso del puerto para conexión segura: **https://grupof:8443/**

Despliegue de CAS Server

Descargamos el archivo ZIP de la versión CAS Server 3.5.2.1, luego se descomprime el archivo y buscamos la carpeta modules. Dentro de esta carpeta se encuentra un archivo llamado cas-server-webapp-3.5.2.1.war (http://www.jasig.org/cas_server_3_5_2_1_release), hacemos una copia del mismo y la renombramos con el nombre cas.war.

Entramos a la página principal del servidor Apache Tomcat, luego nos damos clic sobre Manager App. Una vez dentro, en la sección archivo WAR a desplegar presionamos sobre el botón Seleccionar archivo, buscamos y seleccionamos el archivo cas.war y damos click en abrir.

Finalmente damos clic en desplegar, actualizamos la página y damos clic en la lista de aplicaciones a la página CAS. Una vez que nos redireccione, nos debe mostrar la página de login de CAS. Y listo, para probar que funciona correctamente debemos ingresar el mismo valor dentro del campo NetID y contraseña.

Instalar la base de datos PostgreSQL

Descargamos la base de datos desde esta página;

http://www.postgresql.org/download/

Una vez instalado PostgreSQL se procederá a la creación de la base de datos usada en el proyecto

Vamos a Inicio -> Todos los programas -> PostgresSQL 9.3 -> Abrimos pgAdmin III.

-En Object Browser, entramos a PostgresSQL 9.3 (localhost:5432) damos clic derecho sobre Databases y escogemos New Database.

-La nombramos usuarios y luego clic en OK.

-Una vez ya creada nuestra base de datos, damos clic derecho sobre ella y escogemos la opción Create script.

Añadimos el script adjunto a este documento, luego de esto procedemos a ejecutarlo para asi tener lista nuestra base de datos.

Agregar el Bean y haciendo uso de la base de datos PostgreSQL

Descargamos el archivo postgresql-9.3-1100-jdbc41.jar y validadorCAS.jar y los agregamos en la siguiente ruta dentro de la carpeta del CAS Server:

C:\<Directorio de Tomcat Server>\webapps\cas\WEB-INF\lib

Una vez realizado esto dentro de la carpeta WEB-INF, abrimos el archivo deployerConfigContext.xml y comentamos la siguiente línea:

<bean class="org.jasig.cas.authentication.handler.support.SimpleTestUsernamePasswordAuthenticationHandler" />

Debajo de la línea que acabamos de comentar, colocamos la siguiente:

<bean class="com.software.validadorcas.Validador" />

Guardamos los cambios y cerramos el archivo.

Desplegar la aplicación SAIN

Para desplegar la aplicación se realiza los mismos pasos del despliegue que se realizó con el CAS Server en el paso 5 con la diferencia que la ubicación del archivo WAR está en la SAIN\target bajo el nombre de SAIN-1.0-SNAPSHOT.war el cual debemos renombrarlo con SAIN.war y lo desplegamos en el servidor de Apache Tomcat.

Probamos la aplicación SAIN

Entramos a la siguiente URL:

https://grupof:8443/SAIN

Inmediatamente antes de entrar a la aplicación, seremos redireccionados a la página de login del CAS Server del cual para hacer uso de la misma, debemos entrar con el usuario y contraseña que ingresamos a la base de datos.