# Examen del servidor de aplicaciones Tomcat9

1. **(2 puntos)** Se pide agregar dos nuevos hosts virtuales al servidor Tomcat9, con las siguientes características:
2. uno de ellos llevará por nombre “h1.tu\_nombre\_de\_pila.org” y su directorio de aplicaciones será “h1” (este directorio se debe crear dentro de /var/lib/tomcat9)

Texto

Descripción generada automáticamente

1. el otro llevará por nombre “h2.tu\_nombre\_de\_pila.org” y su directorio de aplicaciones será “h2” (también debe crearse dentro de /var/lib/tomcat9)

Texto

Descripción generada automáticamente

Texto, Carta

Descripción generada automáticamentea

Los dos hosts deben permitir auto desplegar aplicaciones empaquetadas en formato WAR dentro de su directorio de aplicaciones

1. **(1,75 puntos)** Ahora se pide configurar el fichero /etc/tomcat9/tomcat-users.xml de tal modo que el usuario “admin” y contraseña “naranco” pueda acceder a la parte web del manager de aplicaciones

Texto

Descripción generada automáticamente

Debe copiarse también el fichero manager.xml de la configuración del localhost en cada uno de los dos hosts virtuales para permitir el acceso a la parte web de gestión de aplicaciones

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Desde un equipo Windows se debe mostrar también capturas de pantalla del acceso correcto con el usuario y contraseña anterior a las URL’s

<http://h1.tu_nombre_de_pila.org:8080/manager> y <http://h2.tu_nombre_de_pila.org:8080/manager>

Texto, Carta

Descripción generada automáticamente

1. **(2 puntos)** Ahora desde la aplicación Eclipse se debe crear una aplicación “raiz” (ROOT) para el host h1.tu\_nombre\_de\_pila.org. Para ello:
2. Debe agregarse en el proyecto ROOT (dentro de la carpeta webapp) el fichero fuente JSP de nombre inicio.jsp que se adjunta en este examen
3. Ahora debe crearse automáticamente un fichero web.xml dentro de la carpeta WEB-INF, para ello seleccionamos el proyecto 🡪 botón derecho 🡪 Java EE Tools 🡪 Generate Deployment Descriptor y una vez creado el archivo debe editarse y modificarse para permitir que la página inicio.jsp se cargue por defecto, agregando otra etiqueta más de tipo <welcome-file></welcome-file>
4. Debe exportase el proyecto ROOT a fichero WAR y usando la interfaz web del manager de aplicaciones debe desplegarse en el host h1
5. Desde un navegador del equipo Windows se debe verificar que la página de inicio se carga correctamente, escribiendo la URL <http://h1.tu_nombre_de_pila.org:8080>
6. **(2,25 puntos)** Ahora debe crearse otra aplicación ROOT para el host h2 pero en este caso debe copiarse y auto desplegarse dentro de la carpeta “h2”. Para ello:
7. En la aplicación ROOT debe agregarse un fichero index.jsp y dentro de su etiqueta <body> debe agregarse el siguiente código JSP:

<%

out.print(“<h2>Host h1.tu\_nombre\_de\_pila.org</h2>”);

%>

1. Ajustar adecuadamente el grupo propietario y permisos del directorio “h2” de tal modo que se permita la escritura para un usuario a tu elección que pertenezca al grupo anterior
2. Una vez creado el fichero ROOT.war debe copiarse al directorio “h2” empleando la aplicación WinSCP desde la maquina Windows
3. Verificar el auto despliegue de la aplicación ROOT accediendo a <http://h2.tu_nombre_de_pila.org:8080> desde un navegador del equipo Windows
4. **(2 puntos)** Se pide activar el soporte SSL con certificado digital para el host localhost de Tomcat. Con las siguientes condiciones:
5. El alias del certificado será certificado1
6. El almacén de claves será /var/lib/tomcat9/mis\_claves
7. El algoritmo del certificado será RSA
8. La contraseña del almacén será “Naranco2023”
9. La contraseña del certificado será “Naranco2023”
10. Los demás valores solicitados: país, provincia, organización, etc.., se pueden rellenar a tu elección

Lógicamente debe agregarse un nuevo conector para el puerto seguro “8443” con los datos anteriormente configurados

Debe mostrarse una captura de pantalla de la conexión segura desde un navegador del equipo Windows accediendo a la URL <https://www.midominio.com:8443> así como otra captura donde se puedan visualizar los datos del certificado desde el propio navegador