

open suse

TOMCAT SSL

Zygimantas Sniurevicius

DAW 2°

Antes de empezar, el software que necesitamos es el siguiente:

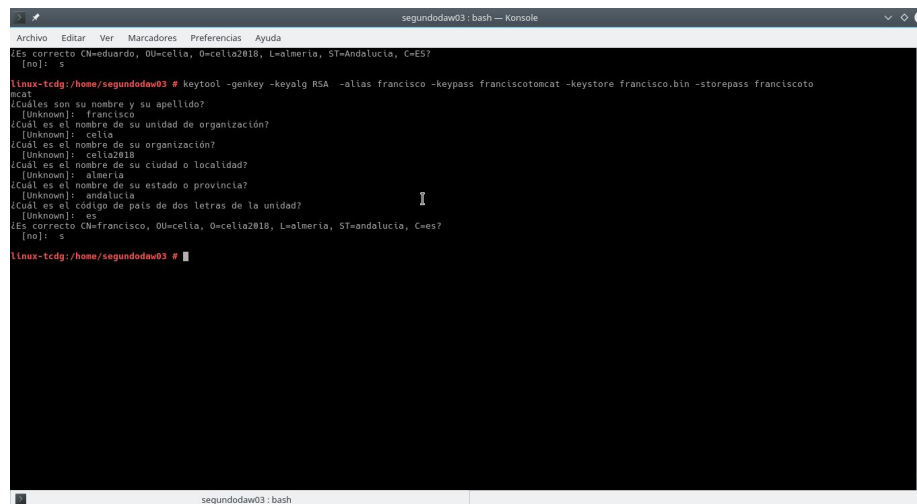
Tomcat 7.0.22 o mayor.

JDK 7ul

Una vez que tengamos todo lo necesario podemos empezar, abrimos la consola y escribimos el siguiente comando

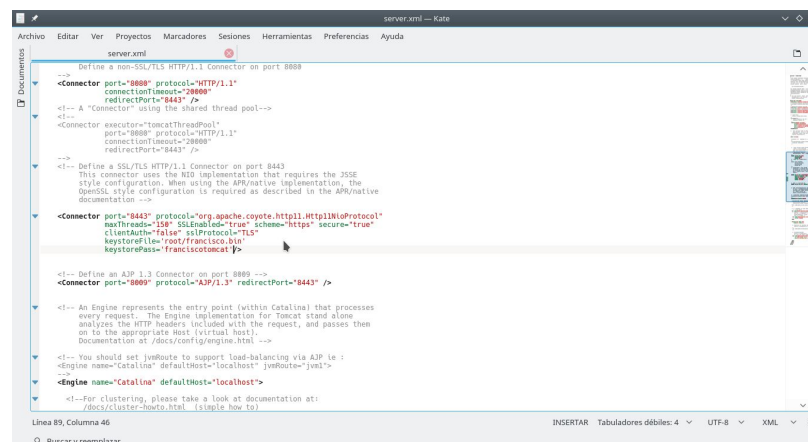
keytool -genkey -alias pepe -keypass pepetomcat -keystore /etc/pki/pepe.bin -storepass pepetomcat

NOTA: Si estamos usando firefox o Chrome debemos añadir la opción **-keyalg RSA**



```
segundodaw03: bash — Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
¿Es correcto CN=Eduardo, OU=celia, O=celia2018, L=almeria, ST=Andalucía, C=ES?
[no]: s
linux-tcdg:/home/segundodaw03 # keytool -genkey -keyalg RSA -alias francisco -keypass franciscotomcat -keystore francisco.bin -storepass franciscotomcat
¿Cuáles son su nombre y su apellido?
[Unknown]: francisco
¿Cuál es el nombre de su unidad de organización?
[Unknown]: celia
¿Cuál es el nombre de su organización?
[Unknown]: celia2018
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: almeria
¿Cuál es el nombre de su estado o provincia?
[Unknown]: andalucia
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: es
¿Es correcto CN=francisco, OU=celia, O=celia2018, L=almeria, ST=andalucia, C=es?
[no]: s
linux-tcdg:/home/segundodaw03 #
```

Ahora buscamos el archivo server.xml en /etc/tomcat/.



```
server.xml — Kate
Archivo Editar Ver Proyectos Marcadores Sesiones Herramientas Preferencias Ayuda
server.xml
<!-- Define a non-SSL/TLS HTTP/1.1 Connector on port 8080 -->
<Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
<!-- A "Connector" using the shared thread pool -->
<!-- Connector executor="tomcatThreadPool"
    port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
-->
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
    This connector uses the NIO implementation that requires the JSSE
    style configuration. When using the APR/native implementation, the
    OpenSSL style configuration is required as described in the APR/native
    documentation -->
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="/etc/pki/pepe.bin"
    keystorePass="pepetomcat" />
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
<!-- An Engine represents the entry point (within Catalina) that processes
    every request. The Engine implementation for Tomcat stand alone
    analyzes the HTTP headers included with the request, and passes them
    on to the appropriate Host (virtual host).
    Documentation at /docs/conf/engines.html -->
<!-- You should set jvmRoute to support load-balancing via AJP ie :
    <Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
-->
<!-- For clustering, please take a look at documentation at:
    /docs/cluster-howto.html (if you have it) -->
```

Miramos donde salga el puerto 8443 comentado y lo descomentamos o en el caso de que nos salga lo ponemos nosotros mismo.

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
```

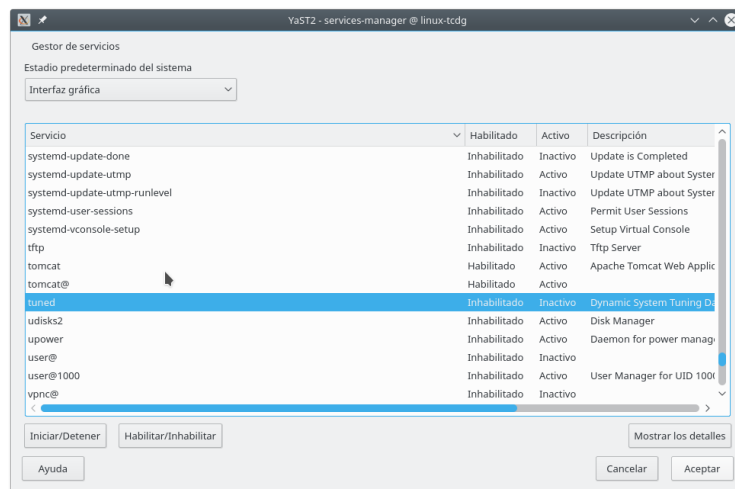
```
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
```

```
clientAuth="false" sslProtocol="TLS"
```

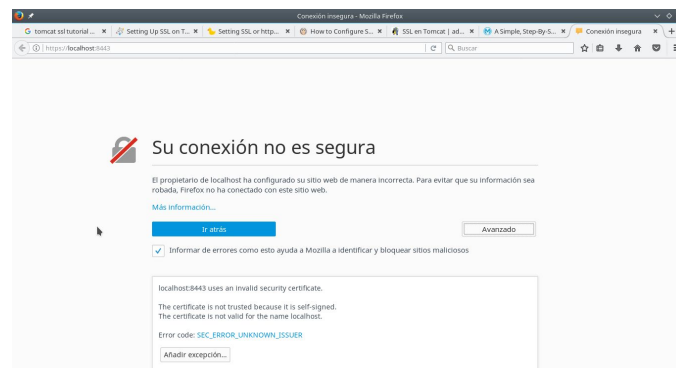
```
keystoreFile="/etc/pki/pepe.bin"
```

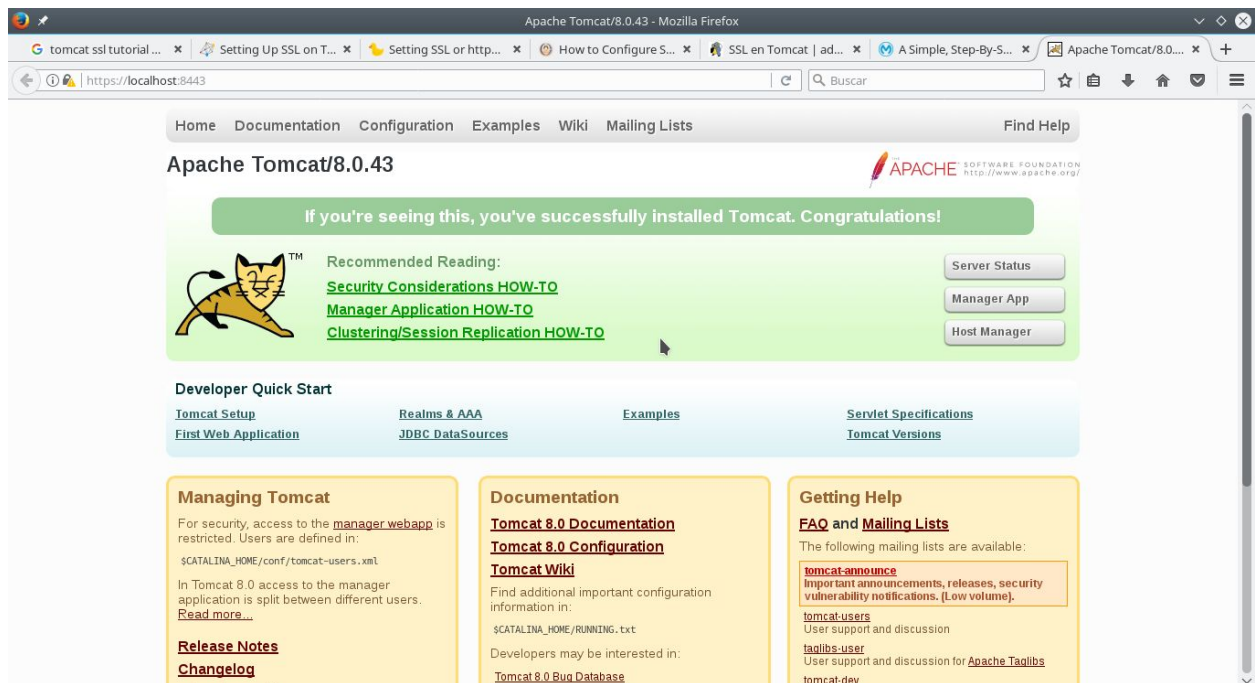
```
keystorePass="pepetomcat"/>
```

Guardamos los cambios y procedemos a reiniciar el servicio de tomcat en Yast.



Nos dirá que la conexión no es segura a la hora de comprobar la dirección, añadimos como excepción y aceptamos.





FIN.