Tomcat:

Tomcat is a lightweight java Servlet container.

But we can use tomcat as HTTP Server + Servlet container.

Popular combination is Apache HTTP Server + Tomcat

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards. Some common language interfaces support [Perl](https://en.wikipedia.org/wiki/Mod_perl), [Python](https://en.wikipedia.org/wiki/Mod_python), [Tcl](https://en.wikipedia.org/wiki/Tcl" \o "Tcl) and [PHP](https://en.wikipedia.org/wiki/PHP).

<Http://mydomain.com:80/a/b/1.html>

Modules PHP

[Http://mydomain.com:80/a/\*](Http://mydomain.com:80/a/*) route towards php runtime

JSP/Serverlet

Module Tomcat

[Http://mydomain.com:80/b/\*](Http://mydomain.com:80/b/*) route towards tomcat runtime

The Apache Tomcat® software is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies.

Normally in the development mode download zip file. Extract somewhere into your system.

To run tomcat : browse bin directory and run startup.bat file.

To stop tomcat : run shutdown.bat file or simply close tomcat command window.

How to change tomcat port.

|  |  |
| --- | --- |
| <Server port="8005" shutdown="SHUTDOWN"> |  |
| <Connector port="8080" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8443" /> | Webshpare : 9080 |
| <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> |  |
| <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="150" SSLEnabled="true">  <SSLHostConfig>  <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"  type="RSA" />  </SSLHostConfig>  </Connector> | 9043 / |

How to increate tomcat heap memory

Step 1

Create a batch file setenv.bat in the bin folder with following contents

|  |
| --- |
| set JAVA\_OPTS=-Xms1024m -Xmx2048m -XX:MaxPermSize=1024m  echo ambrish setting java env with %JAVA\_OPTS% |

Step 2

Save and restart your tomcat.

**Increase Tomcat Upload File Size Limit**

webapps/manager/WEB-INF/web.xml

<multipart-config>

<max-file-size>52428800</max-file-size>

<max-request-size>52428800</max-request-size>

<file-size-threshold>0<</file-size-threshold>

</multipart-config>

**Increase Tomcat Request Size Limit**

Edit into server.xml file from conf directory of tomcat

<Connector port="80" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443"

maxPostSize="67589953" />

Setup tomcat users to use manage application for uploading war files and monitoring tomcat server.

Edit tomcat-users.xml file from conf directory of tomcat.

|  |
| --- |
| <role rolename="manager-gui"/>  <role rolename="manager-script"/>  <user username="tomcat" password="tomcat" roles="manager-gui,manager-script"/> |

## SSL/TLS Configuration HOW-TO

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

One problem when you administer a network is securing data that is being sent between applications across an untrusted network. You can use TLS/SSL to authenticate servers and clients and then use it to encrypt messages between the authenticated parties.

The Transport Layer Security (TLS) protocol, Secure Sockets Layer (SSL) protocol, versions 2.0 and 3.0, and the Private Communications Transport (PCT) protocol are based on public key cryptography. The Security Channel (Schannel) authentication protocol suite provides these protocols. All Schannel protocols use a client/server model.

In the authentication process, a TLS/SSL client sends a message to a TLS/SSL server, and the server responds with the information that the server needs to authenticate itself. The client and server perform an additional exchange of session keys, and the authentication dialog ends. When authentication is completed, SSL-secured communication can begin between the server and the client using the symmetric encryption keys that are established during the authentication process.

For servers to authenticate to clients, TLS/SSL does not require server keys to be stored on domain controllers or in a database, such as the Microsoft Active Directory directory service. Clients confirm the validity of a server’s credentials with a trusted root certification authority’s (CA’s) certificates, which are loaded when you install Microsoft Windows Server 2003. Therefore, unless user authentication is required by the server, users do not need to establish accounts before they create a secure connection with a server.

* + What you send and receive from the website is encrypted, which makes it difficult for anyone else to get to this info.
  + The website is verified, which means the company running the site has a certificate proving they own it. Click the lock button to see who owns the site and who verified it. ﻿
  + While a gray lock means that the website is encrypted and verified, a green lock means that Microsoft Edge considers the website more likely to be authentic. That's because it's using an Extended Validation (EV) certificate, which requires a more rigorous identity verification process.

What is trust store / key store

C:\

|  |
| --- |
| How to list list certificates from cacerts keystore file |
| Change directory to your jre]lib\security folder  And run following command  keytool –list -v -keystore cacerts |

default password password is changeit

|  |
| --- |
| How to add certificate file into keystore |
| Change directory to your jre]lib\security folder  And run following command  keytool –keystore cacerts –import –file <XXX.cer> -alias <alias name> |

Note: if it is added successfully cacerts file size will increase by 1 kb.

|  |
| --- |
| How to generate a fresh certificate / self signed certificate using keytool command |
| keytool -genkey -keyalg RSA -alias tomcat -keystore cacerts -validity 120 -keysize 2048 |
| This will ask few question and then will add certificate into cacerts |

|  |
| --- |
| How to export certificates from cacerts keystore |
| keytool -exportcert -keystore cacerts -alias tomcat -file shivani.cer |

|  |
| --- |
| Setting certificate into tomcat conf\server.xml file. |
| <Connector  protocol="org.apache.coyote.http11.Http11NioProtocol"  port="8443" maxThreads="200"  scheme="https" secure="true" SSLEnabled="true"  keystoreFile="C:\\Progra~1\\Java\\jdk1.8.0\_45\\jre\\lib\\security\\cacerts" keystorePass="changeit"  clientAuth="false" sslProtocol="TLS"/> |
|  |