**Tomcat Installation and Hardening on Windows Environment**

Link: <https://drive.google.com/drive/folders/1Ibw8ci1URERzBT7aqqy5xm2WRyvns3XS?usp=sharing>

1. Download Tomcat v10.1.34

<https://archive.apache.org/dist/tomcat/tomcat-10/v10.1.34/bin/>

1. Install JDK 11 from

<https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html> on Default Path: C:\Program Files\Java\jdk-11

1. Install Tomcat 10.1.34 on C:\Program Files\Apache Software Foundation\Tomcat 10.1

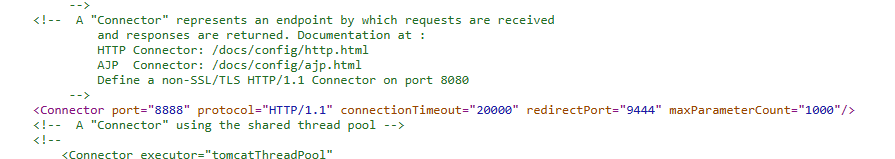
With JDK Path as specified above

1. Remove docs, examples and host-manager folders from webapps
2. Changes in $TOMCAT\_HOME /conf/server.xml
3. Change the default ports of

HTTP -> 8080 to 9080

HTTPS -> 8443 to 9444

AJP -> 8009



b. Also add jvmRoute variable in

<Engine name="Catalina" defaultHost="localhost" jvmRoute="server1">

c. And enable the AJPCommunication

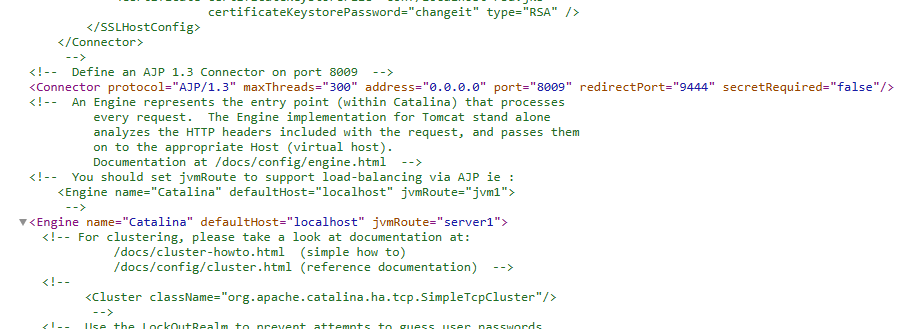
<Connector protocol="AJP/1.3"

maxThreads="300"

address="0.0.0.0"

port="8009"

redirectPort="9444" secretRequired="false"/>



d. Redirecting to 400 bad request custom error page – Add the below configuration in $TOMCAT\_HOME /conf/server.xml

<Valve className="org.apache.catalina.valves.ErrorReportValve"

errorCode.400="webapps/ROOT/400.jsp"

errorCode.0="webapps/ROOT/errorOthers.jsp"

showReport="false"

showServerInfo="false" />

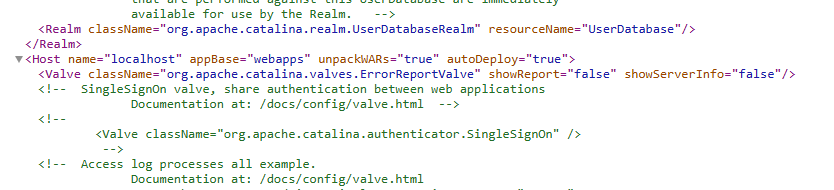
Note: Not exist in MLos config server.xml file.

e. Tomcat Version Disclosure

Open Server.xml from path $TOMCAT\_HOME /conf/server.xml

Find the Host section and add the below line immediately after it:

<Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false" showServerInfo="false" />



1. Change the following files in $Tomcat\_HOME/webapps/ROOT
2. Backup the original file of index.jsp as [index.jsp.bk](http://index.jsp.bk)
3. Swap the contents of index.html by below mentioned files

Copy files from Downloaded ROOT Directory to this ROOT Directory

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<title>404 Error</title>

</head>

<body>

<img src="404.jpg" width="100%" height="100%">

</body>

</html>

1. Add the following in $Tomcat\_HOME/webapps/ROOT

400.html

400.jpg

401.html

403.html

404.html

404.jpg

405.html

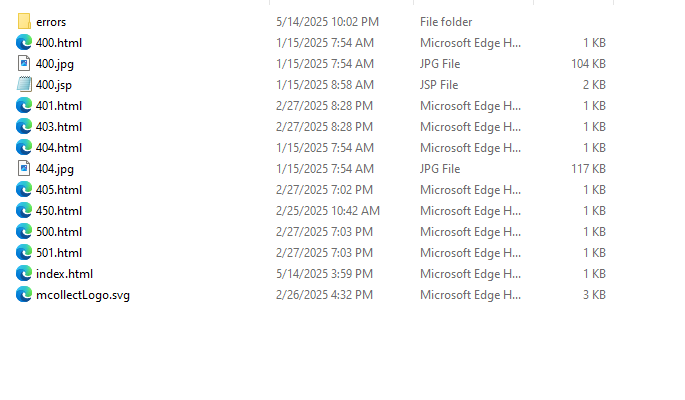
450.html

500.html

501.html

mcollectLogo.svg

errors directory from ROOT



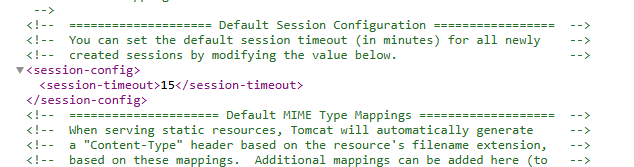
7. Changes in $TOMCAT\_HOME /conf/web.xml

1. Change the session timeout for inactivity from the application side. Default value is 30 minutes in $TOMCAT\_HOME /conf/web.xml to 15 min

<session-config>

<session-timeout>15</session-timeout>

</session-config>



b. To enable HSTS headers to add the below configuration in / Missing Security Headers in $TOMCAT\_HOME /conf/web.xml

<filter>

<filter-name>httpHeaderSecurity</filter-name>

<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>

<async-supported>true</async-supported>

<init-param>

<param-name>antiClickJackingOption</param-name>

<param-value>SAMEORIGIN</param-value>

</init-param>

<init-param>

<param-name>hstsEnabled</param-name>

<param-value>true</param-value>

</init-param>

<init-param>

<param-name>hstsMaxAgeSeconds</param-name>

<param-value>31556927</param-value>

</init-param>

<init-param>

<param-name>hstsIncludeSubDomains</param-name>

<param-value>true</param-value>

</init-param>

<init-param>

<param-name>xssProtectionEnabled</param-name>

<param-value>true</param-value>

</init-param>

</filter>

c. Change the default error pages in $TOMCAT\_HOME/conf/web.xml

<error-page>

<error-code>400</error-code>

<location>/400.html</location>

</error-page>

<error-page>

<error-code>401</error-code>

<location>/401.html</location>

</error-page>

<error-page>

<error-code>403</error-code>

<location>/403.html</location>

</error-page>

<error-page>

<error-code>404</error-code>

<location>/404.html</location>

</error-page>

<error-page>

<error-code>500</error-code>

<location>/500.html</location>

</error-page>

<error-page>

<error-code>501</error-code>

<location>/501.html</location>

</error-page>

<error-page>

<error-code>405</error-code>

<location>/405.html</location>

</error-page>

<error-page>

<error-code>450</error-code>

<location>/450.html</location>

</error-page>



d. Restrict HTTP methods

Add the tags below in web.xml file

$TOMCAT\_HOME /conf/web.xml

<security-constraint>  
    <web-resource-collection>  
      <web-resource-name>restricted methods</web-resource-name>  
      <url-pattern>/\*</url-pattern>         
      <http-method>OPTIONS</http-method>  
      <http-method>DELETE</http-method>  
    </web-resource-collection>  
    <auth-constraint/>  
  </security-constraint>



8. Change the default error pages (401.jsp, 403.jsp, 404.jsp) from manager on path $TOMCAT\_HOME/webapps/manager/WEB-INF/jsp -----------No Need

<error-page>

<error-code>400</error-code>

<location>/400.html</location>

</error-page>

<error-page>

<error-code>401</error-code>

<location>/401.html</location>

</error-page>

<error-page>

<error-code>403</error-code>

<location>/403.html</location>

</error-page>

<error-page>

<error-code>404</error-code>

<location>/404.html</location>

</error-page>

<error-page>

<error-code>500</error-code>

<location>/500.html</location>

</error-page>

<error-page>

<error-code>501</error-code>

<location>/501.html</location>

</error-page>

<error-page>

<error-code>405</error-code>

<location>/405.html</location>

</error-page>

<error-page>

<error-code>450</error-code>

<location>/450.html</location>

</error-page>

9. Create new tomcat user in $TOMCAT\_HOME /conf/tomcat-users.xml

<role rolename="admin-gui"/>

<role rolename="admin-script"/>

<role rolename="manager-status"/>

<role rolename="manager-script"/>

<role rolename="manager-gui"/>

<user username="KotakGLOS" password="M0b1cu!e123" roles="manager-gui,admin-gui" />

If login error occurs then comment above 5 rolenames.

10. Limit Catalina.out logs (Not required for Windows installation)

CATALINA\_BASE"/logs/catalina.out

Replace with new path.

Restart tomcat.

And as suggested in comments, to block writing to catalina.out entirely, **set CATALINA\_OUT=/dev/null in**[**catalina.sh**](http://catalina.sh)