Optimizing Tomcat for Web Applications

Tomcat Security and Optimization Document

© PlanetJ Corporation 1821 Kelson Place, Escondido CA 92029 Phone 760-432-0600 • Fax 760-432-0600

Table of Contents

Introduction to Tomcat	3
Increase Maximum Memory Used	3
Changes to web.xml configuration file	5
Administering Tomcat:	8
Changing Port Settings	11
Secure Application Files in Tomcat	12
SSL:	15
Other Security Considerations	15
References	15



INTRODUCTION

Introduction to Tomcat:

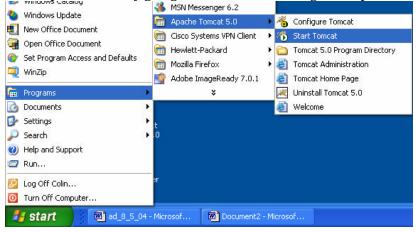
WebSphere has gained significant market share in Web application development space. A powerful, easy to use, and free alternative to WebSphere is Apache's Tomcat. Tomcat is open source and is the reference implementation for Sun' servlet standard. Tomcat has proven itself as production quality and is used by many companies. Tomcat installation on Window servers is an automated and easy process however the default installation places Tomcat into development mode. The advantage of development mode is that changes to JSPs, class, and JAR files are automatically incorporated at runtime without the need to restart the application server. The drawback is that performance suffers in development mode. Once you have created your WOW application and are ready to serve it to the public, the following steps should be taken to optimize Tomcat.

STEP 1

Increase Maximum Memory Used

Tomcat ships with the maximum amount of memory set to 64MB, which is not large enough to operate most large web applications. We recommend increasing the maximum amount of memory to 80% of the total RAM available on your server. This can be done as shown below.

First, open Tomcat by going to the Start Menu-Programs-Apache Tomcat-Start Tomcat.



After Tomcat has started you should see the Tomcat icon in the lower right hand corner as shown below.

🔇 🀔 4:10 PM

To access the Tomcat properties allowing changes to the maximum memory, right click on the icon and select properties. This is also the way to stop the server by clicking on Shutdown: Tomcat instead of properties.



The properties screen below has the Java VM tab selected. Inside the Java Options we will add the increased min and max memory allocation settings.

💑 Apache To	omcat 5.0.19 Server - http://jakarta.apache.org/tomcat/ Service 🗙
Service Java	a VM Standard Streams
– Java Virtual	Machine
Auto	
Java VM	1: java
Java Op	tions : -Dcatalina.home="C:\Program Files\Apache Software Foundation Apache Software Foundati Apache Software Foundation Apache Software Foundati Apache S
Start cla	ss : org.apache.catalina.startup.Bootstrap;main;start
Stop cla	ss : org.apache.catalina.startup.Bootstrap;main;stop
	OK Cancel Apply

The minimum value can be anything but should start with at least 64-100MB. The maximum memory should be up to 80% of your computers RAM. For example, if you have 512MB of RAM then you should set the maximum memory to around 400MB. To change the memory specifications you need to add this code to the Java Options text area:

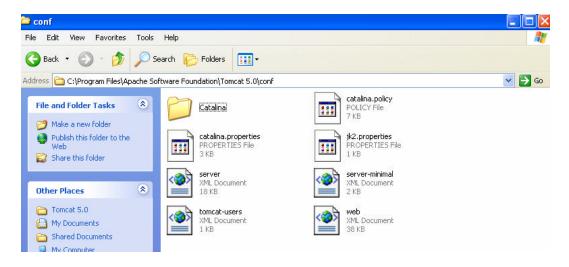
-Xms100m -Xmx400m

lava Virtual Mach	ine	
Auto	Г	
Java VM :	java	
Java Options :	-Xms100m -Xmx400m	4
		~
Start class :	org.apache.catalina.startup.Bootstrap;main;start	
Stop class :	org.apache.catalina.startup.Bootstrap;main;stop	

STEP 2

Changes to web.xml configuration file:

The web.xml is the document that defines default values for **all** web applications loaded into each instance of Tomcat. As each application is deployed, this file is processed, followed by the "/WEB-INF/web.xml" deployment descriptor from your own applications. The web.xml is located in Apache Software Foundation-Tomcat-conf folder shown below.



Open the web.xml by right clicking and select open with (NotePad or Wordpad or any text editor.) Now in the document we want to find the JSP Servlet Tag. This is located a quarter of the way down the page. Add two initial parameters - the reloading parameter and the development parameter.

innua paran	neters the reloading parameter and the developine	in puiu
by add<br If you</th <th>dding the above to your CATALINA_OPTS environment variable ou get an error reporting that jikes can't use UTF8 encoding, -</th> <th>> > ></th>	dding the above to your CATALINA_OPTS environment variable ou get an error reporting that jikes can't use UTF8 encoding, -	> > >
<pre><servit <init- pi <pi </pi </init- <init- <pi <pi <pi <td>baram-name>fork baram-value>false -param> param=name> baram-name>xpoweredBy baram-value>false -param> on-startup>3</td><td></td></pi </pi </pi </init- </servit </pre>	baram-name>fork baram-value>false -param> param=name> baram-name>xpoweredBy baram-value>false -param> on-startup>3	

The reloading and development parameters are automatically set to true when Tomcat is installed. The development init-parameter will check for JSP modification on every access and reload. Set both of these parameters in the web. xml document to false so Tomcat will not look for or reload changes to JSPs on every access.

D web -	Notepad			E E
File Edit	Format View Help			
</td <td>It you get an</td> <td>above to your CATALINA_OPTS environment variable. error reporting that jikes can't use UTF8 encoding, e init parameter "javaEncoding" to "ISO-8859-1".</td> <td>> > ></td> <td>2</td>	It you get an	above to your CATALINA_OPTS environment variable. error reporting that jikes can't use UTF8 encoding, e init parameter "javaEncoding" to "ISO-8859-1".	> > >	2
<5 <i>6</i>	<pre><servlet-class2 <init-param=""></servlet-class2></pre>	sp org.apache.jasper.servlet.JspServlet >fork e>false		
	<pre></pre>	>xpoweredoy e>Talse e>Talse e>Talse		
c/s	<pre><init-paramo <param-name <param-valu< pre=""></param-valu<></param-name </init-paramo </pre>	ezhansek, panam-oardez ezhansek/panam-names ps3k/load-on-stantups		
</td <td>directives in HT servers like Apa URL pattern "°.s</td> <td>udes processing servlet, which processes ssi ML pages consistent with similar support in web .che. Traditionally, this servlet is mapped to html". This servlet supports the following arameters (default values are in square brackets):</td> <td>****</td> <td></td>	directives in HT servers like Apa URL pattern "°.s	udes processing servlet, which processes ssi ML pages consistent with similar support in web .che. Traditionally, this servlet is mapped to html". This servlet supports the following arameters (default values are in square brackets):	****	
</td <td>buffered</td> <td>Should output from this servlet be buffered? (0=false, 1=true) [0]</td> <td></td> <td></td>	buffered	Should output from this servlet be buffered? (0=false, 1=true) [0]		
<	debug	pebugging detail level for messages logged by this convict [0]	>	

To add the init-parameters you will add this code: <init-param>

In summary, Tomcat is a cost-efficient tool to hosting Web applications. Now that you have made the above simple changes, Tomcat will run much faster and handle more complex workloads.



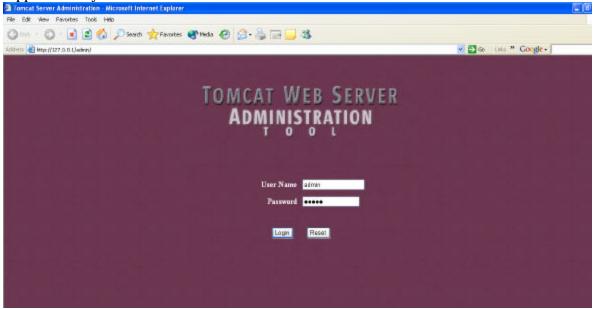
TOMCAT ADMINISTRATOR AND MANAGER APPLICATIONS

Administering Tomcat:

Tomcat also has its own administration, which can be helpful and accessed through the Tomcat server. Now we are going to show some of the helpful and powerful administration applications that Tomcat ships with such as Tomcat Administrator and Tomcat Manager.

To access both of these you can either go through the start menu under Apache Tomcat folder or you can open a browser and type go to the localhost such as <u>http://localhost:80</u> with the port that you specified in the installation of Tomcat.

Tomcat allows administration (start, stop, destroy, manage, create etc) via a web application. The Tomcat Administration Application allows you to see the server information, edit connections, edit users, groups, resources and change the main settings of the webserver. This application runs using the userid and password supplied when you installed Tomcat.



			i 🕹 🖂 🖵 🚳	
aldreiz 🛃 Hitp: (127.0.0.1/advir/Francest.pp				💌 🔁 Go 🛛 tide * Google - 🛛
IOMCAT WEB SERVER				
ADMINISTRATION TOOL				Central Changes Lig D
Tomost Server	EditE	disting User Propert	lies	User Actions
●₩ Senic# (Catalina) (©Resources				Save Des
Data Sources Mail Sensions	-		-	
Environment Entres.		Properties Name:	admin	
Cuer Definition	Past	sword:		
them troups	Full	Name:		
🕈 Fibles		Group Name	Description	
	the second s	Role Name	Description	
		admin manazar		
		rolel		

The userid and pwd are defined in tomcat at:

..../config/tomcat_users.xml as shown below.

```
<?xml version="1.0" encoding="utf-8" ?>

_ <tomcat-users>

<role rolename="tomcat" />

<role rolename="role1" />

<role rolename="admin" />

<user username="tomcat" password="tomcat" roles="tomcat" />

<user username="role1" password="tomcat" roles="role1" />

<user username="both" password="tomcat" roles="role1" />

<user username="both" password="tomcat" roles="tomcat,role1" />

<user username="admin" password="tomcat" roles="tomcat,role1" />

<user username="admin" password="tomcat" roles="tomcat,role1" />

<user username="admin" password="tomcat" roles="admin,manager" />

</tomcat-user>
```

These are set when you first install Tomcat on to your machine when the installation asks for username and password. You can also change the username and password and add new users in Tomcat Administration Application.

Tomcat also ships with the Tomcat Manager. This is an application that will allow you to edit, start, and stop applications dynamically without restarting the Tomcat. It also shows current applications and a few other options, which you can learn about by clicking on the Manager Help Link Shown below.

	http://ja	arta Project karta.apache.org/						X
		Tomcat We	b Application M	lanager				
Nessage:	OK .							
Manager		95						
List Application	085	HTML Manager	Help	Manag	ar Help			Server Statu
Applications		A 5						
Path	Display Name Walcome to Te		Romaing	Sessions		2ma Reland	Commands	
Satraio		istration Application	true	1		Stop Related	the set of the set of the local	
balancar	Turnual Admin	randorsopheann	the	0	and the second dependence of	Stop Related		
(sp-examples	JSP 20 Exam	in lies	true	0		Stas Related	a minimum of the later of the l	
manager		er Application	true	0		Shan Reland	and and the second s	
(cerdets-examp			true	0	-	Shap Reland		
formatidana	Torneat Docum		true	0		Stan Reland		
Avaities	Watday Conte	nt Management	true	Q	and the second second	Stap Related		
	WDW		true	Q		Stan Roland		
(wowed)						24024	S. A.S.S.	
<u>iwaw60</u>								
Deploy								
<u>liiovi60</u> Deploy Depley dirocte	ry er WAR filo lecated en sorvor							
Deploy	S	Context Path (optional)						

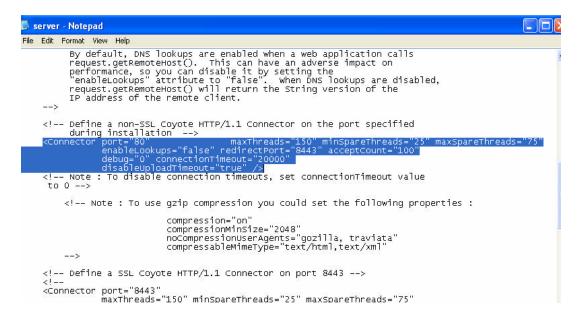
These are a few more tools to help you understand and optimize Tomcat for your Web Applications and to use WOW.

Chapter 3

CHANGING TOMCAT PORT SETTINGS

Changing Port Settings:

When you install Apache Tomcat it defaults the port to 8080. The ports are set in the ..Tomcat/conf/server.xml document. To adjust the port being used right click and open with notepad or any other text editor. After the document is open scroll down around half way looking for the connecter tag shown below and change the port number to a new port number (Usually either 8080 or 80). Then save the newly changed server.xml file and restart Tomcat.





SECURING APPLICATIONS FILES IN TOMCAT

Secure Application Files in Tomcat:

When installing a new web application such as WOW to Tomcat, Tomcat automatically allows people to view the directory listing of all files inside of the webapps folder. An example of this is the *sharedFiles* folder in the webapps folder on the hard drive shown below.

🔁 webapps			
File Edit View Favorites	Tools Help		
😋 Back 🔹 🕥 🖌 🏂 🍃	🔍 Search 🛛 🌔 Folders 🛛 🖾 🎯	× 🍤 💷-	
Address 🗁 C:\Program Files\Apa	che Software Foundation\Tomcat 5.0\w	ebapps	
Name 🔺	Size Type	Date Modified	
🚞 balancer	File Folder	7/2/2004 3:07 PM	
🚞 jsp-examples	File Folder	7/2/2004 3:07 PM	
🛅 ROOT	File Folder	7/2/2004 3:07 PM	
🚞 servlets-examples	File Folder	7/2/2004 3:07 PM	
🚞 sharedFiles	File Folder	8/25/2004 8:36 PM	
🛅 tomcat-docs	File Folder	7/2/2004 3:07 PM	
🚞 webdav	File Folder	7/2/2004 3:07 PM	
🚞 wow60	File Folder	7/2/2004 3:08 PM	

By Default the *sharedFiles* folder includes three directories: one directory contains sample images and another directory contains sample MS Word Documents. These folders are for example purpose only and may be deleted or added upon. There is also a directory labeled *WEB-INF*. This folder contains a file called web.xml. Web.xml allows WOW to be set up to show its contents over the Internet or to be set so that those files cannot be seen over the Internet. Below is an example of connecting to the *sharedFiles* directory through Tomcat.

Directory Listing For /

Filename	Size	Last Modified
HollyCow2.html	0.1 kb	Fri, 09 Apr 2004 18:46:34 GMT
<u>QueryBuilder.hta</u>	0.3 kb	Wed, 21 Apr 2004 22:08:18 GMT
QueryBuilder.html	0.3 kb	Wed, 21 Apr 2004 21:56:42 GMT
Thumbs.db	10.0 kb	Tue, 24 Aug 2004 00:00:52 GMT
<u>images/</u>		Fri, 20 Aug 2004 22:06:26 GMT
<u>ic/</u>		Sun, 22 Aug 2004 01:31:08 GMT
tomcat-power.qif	2.2 kb	Sat, 14 Feb 2004 10:21:44 GMT
<u>tomcat.qif</u>	1.8 kb	Sat, 14 Feb 2004 10:21:44 GMT

Apache Tomcat/4.1.24

This creates a security problem, as the whole Internet will be able to see our code and mess around with our files. To disable this feature you need to go in Apache Tomcat file structure <Apache Tomcat>/conf/web.xml file. In this web.xml file shown below there is an initial parameter called listing that is automatically set to true. We want to change that to false so that your files cannot be directly accessed and seen over the Internet.

Edit	F <u>o</u> rmat <u>V</u> iew <u>H</u> elp			
(!		contents. [null]	>	
(!			>	
(!		ing customization. Checks local×sltFile, then	>	
	global×sltFile, th	en defaults to original behavior.	>	
		and a second second second second second second second	>	
!	local×sltFile Make directory listings an XML doc and	>		
		pass the result to this style sheet residing in that directory. This overrides	>	
			>	
		global×sltFile[null]	> >	
1	qlobal×sltFile	Site wide configuration version of	>	
i	localxstrile This argument is expected	>		
i		to be a physical file. [null]	>	
i		to be a physical file. [hairi]	>	
			>	
	 <init-param> <param-name>de <param-value>de </param-value></param-name></init-param> <init-param> <param-name>li <param-value>f </param-value></param-name></init-param>	ina.servlets.DefaultServlet bug > stings false		
.1-	ervlet>	.		

Now that listings has been set to false users will not be able to see our files by connecting through Tomcat.



TOMCAT SECURITY AND SSL

SSL:

To set up SSL and other security features for Tomcat refer to the Apache's Tomcat site for SSL setup and optimization, <u>http://jakarta.apache.org/tomcat</u>

Other Security Considerations:

1. Make sure your have set proper userids and passwords for your Tomcat user file. This file is located at:/config/tomcat_users.xml

References

Tomcat: <u>http://jakarta.apache.org/tomcat</u> PlanetJ's WOW: http://<u>www.planetjavainc.com</u>