

t:Z Quickstart for Tomcat

T:Z QuickStart for Tomcat - User's Guide

V 7.0.0/6.0.2 Edition

Published May, 2012

Copyright © 2012 Dovetailed Technologies, LLC

Table of Contents

Revision History	iii
1. Introduction	4
1.1. Features	4
1.2. System Requirements	4
1.3. Trademarks	4
2. Installation	6
3. Basic Configuration and Operation	8
4. Using SAF Security in Tomcat	11
5. For More Information... ..	14
A. License	15

Revision History

T:Z QuickStart for Tomcat 7.0.0 - May 4, 2012

Initial release in support of Tomcat version 7. Note that this version of Tomcat requires Java 6 or later.

- Includes vanilla Tomcat 7.0.27 distribution
- SAFROLES JCL now includes entries for `manager-gui`, `manager-script`, `manager-jmx`, and `manager-status` roles.
- Fixed issue with `saf-roles.xml` being overwritten

T:Z QuickStart for Tomcat 6.0.2 - May 4, 2012

Release in support of Tomcat version 6:

- Updates to Tomcat 6.0.35 level distribution
- Fixed issue with `saf-roles.xml` being overwritten

T:Z QuickStart for Tomcat 1.0.1 - December 4, 2009

This release makes the following enhancements and fixes:

- Fixed a problem SAF Realm configuration.

T:Z QuickStart for Tomcat 1.0.0 - April 21, 2009

Initial release in support of Tomcat version 6

- Co:Z® is a trademark of Dovetailed Technologies LLC.
- Apache Tomcat™ and Tomcat™ are trademarks of The Apache Software Foundation.
- z/OS® is a trademark of IBM Corporation.
- Java® is a trademark of Sun Microsystems, Inc.

2. Installation

The following steps are required to install the T:Z Quickstart for Tomcat package.

1. Download the zip file to your workstation and extract the contents to a local directory.
2. Transfer the XMIT file from your workstation to the z/OS system. Please be sure that you upload the following files in binary (no translation).

If you are uploading using FTP, use the following commands (substituting your own dataset high-level qualifier for "HLQ"):

```
ftp myzos.myco.com
(Log in with your host name, user ID, and password.)
ftp> bin
ftp> quote site recfm=fb
ftp> quote site lrecl=80
ftp> quote site cyl
ftp> quote site pri=8
ftp> put tz.tomcat.xmit 'HLQ.TOMCAT.XMIT'
ftp> quit
```

If you are uploading using Personal Communications, then use the following commands to transfer the file. Be sure that you are logged on the host and within the READY mode (outside ISPF). Change the session string ("A:") and the destination "HLQ" as appropriate:

```
send tz.tomcat.xmit A:'HLQ.tomcat.xmit' recfm(f) lrecl(80)
space(8,3) cylinders
```

If you are uploading with an SSH sftp client like PuTTY with Co:Z SFTP on z/OS, you can use the following commands:

```
psftp myid@myzos.myco.com
psftp> ls /+mode=bin,recfm=fb,lrecl=80,space=cyl.8.3
psftp> put tz.tomcat.xmit //HLQ.TOMCAT.XMIT
```

3. To unload the XMIT dataset into a PDS, enter the following TSO command:

```
receive inda('HLQ.TOMCAT.XMIT')
```

When prompted with the message: Enter restore parameters..., enter the following, supplying

your own target dataset name:

```
da( 'HLQ.TOMCAT.INSTJCL' )
```



Note

If you get an error "Unable to issue message with prompt for reply", then enable prompting with the following TSO command:

```
profile prompt
```

4. Customize the `INSTALL` member of the `INSTJCL` PDS, following the comments included in the JCL. The `TCHOME` JCL symbol will reference an *empty* HFS or zFS directory that has 10MB of free space, plus any space that is required for your own web applications.

Run this job and verify that all steps complete with a condition code of zero.



Note

It is also possible to have a single common Tomcat home (aka "`CATALINA_HOME`") directory that is shared by many Tomcat instances that have their own "`CATALINA_BASE`" directories that contain web applications and work/temp space.

3. Basic Configuration and Operation

This section discusses the basic steps required to configure and run Tomcat using T:Z. You will only need to customize the sample JCL and configuration members distributed in the "SAMPJCL" PDS that you unloaded in [Chapter 2, Installation](#)



Note

For a really quick install, you might not need this documentation - just follow the SAMPJCL(\$README) instructions for customizing and starting TOMCAT

1. Edit the SAMPJCL(TCENV) member, which contains a shell script used to configure environment variables in order to run Java under the JZOS batch launcher. For now, just edit the section as shown below to match your installation:

```
# -----  
# $$$$ Often you will only need to customize this section:  
# -----  
export JAVA_HOME=/usr/lpp/java/J6.0 ❶  
CATALINA_HOME=/usr/local/tomcat      ❷  
CATALINA_BASE=/usr/local/tomcat      ❷  
DB2_JDBC_HOME=/usr/lpp/db2910_jdbc   ❸  
DB2_SSID=DSN9                        ❹  
IJO="-Xms64m -Xmx128m"               ❺
```

- ❶ Change to your Java SDK V5 or V6 home directory. See: [Section 1.2, "System Requirements"](#)
- ❷ Set both this an CATALINA_BASE should be set to the directory where you installed the Tomcat filesystem ("TCHOME" in the INSTALL JCL).
- ❸ If you have DB2, set this to the DB2 JDBC home directory which contains the JDBC driver jars. Otherwise this can be ignored.
- ❹ If you have DB2 and will be using JDBC type-2 connections, set this to your DB2 subsystem id. Otherwise this can be ignored.
- ❺ This is a reasonable starting point for min and max Java heap sizes, which you can update as necessary for your web applications.

2. Edit the SAMPJCL(TCPROC) member, which contains a sample stored procedure for running Tomcat using the JZOS Batch Launcher

```
//TCPROC PROC CNFGLIB=, < (RQD) PDS w/ config XML & env script  
// TCENV=TCENV, < Member of CNFLIB with STDENV script  
// JZOSLIB='SYS1.SIEALNKE', ❶ < JZOS launcher PDSE LIB  
// VERSION='60', ❷ < JZOSVM version: 50,56,60,66  
// LOGLVL=' ', < Debug LVL: +I(nfo) +D(ebug) +T(race)  
// REGSIZE='0M', < Max region  
// * DB2PRFX=DSN910, ❸ < Prefix for DB2 STEPLIBS, if used  
// LEPARM=' ',
```

```

//  JAVACLS='org.apache.catalina.startup.Bootstrap' ,
//  ARGS='start'
//JAVAJVM  EXEC  PGM=JVMLDM&VERSION,REGION=&REGSIZE,
//  PARM='&LEPARM/&LOGLVL &JAVACLS &ARGS'
//STEPLIB DD DISP=SHR,DSN=&JZOSLIB
//*❶      DD DISP=SHR,DSN=&DB2PRFX..SDSNEXIT < Uncomment for DB2
//*       DD DISP=SHR,DSN=&DB2PRFX..SDSNLOAD < type-2
//*       DD DISP=SHR,DSN=&DB2PRFX..SDSNLOD2 < JDBC
//STDENV  DD DISP=SHR,DSN=&CNFGLIB(&TCENV) < STDENV shell script
//TCCONFIG DD DISP=SHR,DSN=&CNFGLIB < Tomcat XML cnfig
//SYSPRINT DD SYSOUT=* < System stdout
//SYSOUT  DD SYSOUT=* < System stderr
//STDOUT  DD SYSOUT=* < Java System.out
//STDERR  DD SYSOUT=* < Java System.err
//CEEDUMP DD SYSOUT=*
//ABNLIGNR DD DUMMY
// PEND

```

- ❶ Set this to the PDSE library containing JVMLDM50/56/60/66, the JZOS batch launcher
- ❷ Set this to match the JAVA SDK that you are using (JAVA_HOME in TCENV)
- ❸❹ Uncomment these and set to your DB2 library prefix if you are using JDBC type-2 connections.

3. Edit the SAMPJCL(SERVVARS) member, which contains XML entity definitions (variables) that are used to parameterize the Tomcat configuration XML, which is contained in member SERVXML.
 - The `httpPort` variable should be set to an available port that Tomcat will listen on for normal HTTP connections.
 - The `sslPort` variable may be set to the port that you wish to use for HTTPS (SSL/TLS) connections. By default, HTTPS support is not enabled (in the SERVXML member).
 - Several variables are available to configure the DB2 parameters for type-2 and type-4 JDBC connections. They may be ignored if you won't be using DB2 in your web applications.
4. Edit the SAMPJCL(TCUSERS) member, which contains XML entity definitions that are used to define the users, passwords, and security roles for Tomcat *only if the Tomcat MemoryUserDatabase is configured in SERVXML*, which is the default.

Tomcat will only prompt browsers to logon if required by a given web application in its `web.xml` security specifications. The Tomcat Manager web application, which is shipped with Tomcat, requires that users logon and have the `manager` role.

If you will be using the default `MemoryUserDatabase`, update this file with the userids that you require and assign the `manager` role to at least one user so that you can manage your running Tomcat instance.

See [Chapter 4, Using SAF Security in Tomcat](#) for information on configuring Tomcat to use SAF (RACF) for userid/password authentication and role authorization. If you use SAF, then the TCUSERS member is not used. If you do use TCUSERS, then only allow read access to it by Tomcat and authorized personnel.

5. Customize the SAMPJCL(TCJOB) member, which contains sample JCL for running Tomcat as a batch job. You will only need to customize the jobcard for your installation and set the TCPROCLIB variable to refer to

the SAMPJCL PDS.

```
//TOMCAT JOB ( ), 'TOMCAT',MSGCLASS=H,NOTIFY=&SYSUID
//*****
//* Batch job to run Apache Tomcat using the JZOS Batch JVM launcher
//*   See: SAMPJCL($README) for customization info
//*****
//*
// SET TCPROCLB=TOMCAT.SAMPJCL      Proclib with TOMCAT PROC (this)
// SET TCCNFGLB=&TCPROCLB          Tomcat Config PDS (this)
//*
//PROCLIB JCLLIB ORDER=&TCPROCLB
//*
//TOMCAT EXEC PROC=TCPROC,
//   CNFGLIB=&TCCNFGLB,           < (RQD) PDS w/ config XML & env script
//   LOGLVL= ' '                 < Debug LVL: +I(nfo) +D(ebug) +T(race)
//
```

6. Submit the job!

After a bit, output in the STDOUT DD SYSOUT file should contain something like:

```
Apr 19, 2009 12:05:54 PM org.apache.coyote.http11.Http11Protocol init
INFO: Initializing Coyote HTTP/1.1 on http-8080
Apr 19, 2009 12:05:54 PM org.apache.catalina.startup.Catalina load
INFO: Initialization processed in 1347 ms
Apr 19, 2009 12:05:55 PM org.apache.catalina.core.StandardService start
INFO: Starting service Catalina
Apr 19, 2009 12:05:55 PM org.apache.catalina.core.StandardEngine start
INFO: Starting Servlet Engine: Apache Tomcat/6.0.18
Apr 19, 2009 12:06:00 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting Coyote HTTP/1.1 on http-8080
Apr 19, 2009 12:06:00 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 6202 ms
```

You should now be able to connect your browser to Tomcat at: `http://host:port`, substituting your host or ip address and the http port that you configured earlier.

To gracefully shutdown Tomcat, you may use the MVS STOP (P) console command. Under the SDSF DA panel, this command can be issued using the "Y" prefix command.

4. Using SAF Security in Tomcat

This document describes how to configure t:Z QuickStart for Tomcat to use SAF (RACF) for J2EE user Authentication and Authorization.



Note

Configuring Tomcat to use SAF for user authentication and authorization is different than running Tomcat under a Java security manager.

Support for using SAF to authorize users, passwords, and roles is provided by the Dovetailed Technologies Tomcat SAF Realm, which is included as Java classes in package `com.dovetail.zos.tomcat` in `lib/zos-tomcat.jar`.

The Tomcat SAF Realm uses SDK APIs in the `com.ibm.os390.security` package to validate userid/passwords and assign roles by checking associated SAF entities. These APIs use system services that require that the Tomcat job have the following system authorities:

- The userid executing Tomcat must have read access to the `BPX.SERVER` SAF entity (or be a superuser).
- The Tomcat address space must be "*program controlled*", which means that all of the load module libraries and DLLs that are loaded must be marked as program controlled. This is not the same as APF authorization, but is a system privilege required to check passwords and SAF entity access.

The following steps are required to configure t:Z QuickStart for Tomcat to use SAF:

1. Set the program controlled extended attribute on any DLLs that you added to the SDK runtime environment.

These would include any installation JNI libraries that you added to your `LIBPATH` in `TCENV`. If you configured `TCENV` to use an alphaWorks version of `JZOS`, rather than the SDK-supplied version, then the alphaWorks `JZOS` native libraries must also be program controlled. If neither of these apply, then you may ignore this step.

```
extattr +p libjzos*.so
```



Note

Your userid must be authorized for `READ` access to the `BPX.FILEATTR.PROGCTL` SAF entity to set this attribute.

2. All libraries with modules loaded by the Tomcat job must be *program controlled*. These include the `JZOS` Batch Launcher load module (`JVMLDMxx`) as well as the `c/c++` runtime libraries used by Java.

```
RALTER PROGRAM * ADDMEM ('<JZOS_PDSE_LOADLIB>' //NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('SYS1.LINKLIB' //NOPADCHK) UACC(READ)
```

```

RALTER PROGRAM * ADDMEM ('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('CEE.SCEERUN'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('CEE.SCEERUN2'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('CBC.SCLBDLL'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('SYS1.SEZALINK'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('SYS1.SEZALNKE'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('DSN910.SDSNEXIT'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('DSN910.SDSNLOAD'//NOPADCHK) UACC(READ)
RALTER PROGRAM * ADDMEM ('DSN910.SDSNLOD2'//NOPADCHK) UACC(READ)
SETROPTS WHEN(PROGRAM) REFRESH

```



Note

Many of these libraries may already be program controlled. The TSO command RLIST PROGRAM * ALL can be used to check the status of all libraries

3. Edit the SAMPJCL(SERVXML) member, which contains the Tomcat configuration XML. Near the bottom, locate and edit the Realm tag so that default UserDatabase Realm is commented out and the SafRoleDatabase is uncommented.

The result should be as follows:

```

<!-- This Realm uses the UserDatabase configured in the global JNDI
resources under the key "UserDatabase". Any edits
that are performed against this UserDatabase are immediately
available for use by the Realm. -->
<!--
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"/>
-->

<!-- For SAF(RACF) Authentication, replace the Realm above with: -->
<Realm className="com.dovetail.zos.tomcat.SafRealm"
resourceName="SafRoleDatabase"/>

```

4. Edit SAMPJCL(SAFROLES) and define the Tomcat (J2EE) roles and the SAF entities that will be used to grant them.

```

<role rolename="manager"
safclass="EJBROLE" safentity="TCAT.DEV.MANAGER" saflevel="READ"/>

<role rolename="myrole"
safclass="EJBROLE" safentity="TCAT.DEV.MYROLE" saflevel="READ"/>

```

5. Use the following TSO commands to define a new SAF entity and grant a user access to it:

```
RDEFINE EJBROLE TCAT.DEV.MANAGER UACC(NONE)
PERMIT TCAT.DEV.MANAGER CLASS(EJBROLE) ID(<user_id>) ACCESS(READ)
SETROPTS RACLIST(EJBROLE) REFRESH
```

6. Restart Tomcat and attempt to access a protected resource such as the Tomcat manager page:
`http://host:port/manager/html`

Supply your SAF userid and password when prompted to logon. If everything is setup and configured correctly, then the Tomcat manager page will display. If not, check the job's STDOUT and STDERR files for more information.



Note

If you receive an error message in the log indicating that the address space is not properly program controlled, check the system log for an IBM message that indicates which load module library or DLL is causing the problem.

5. For More Information...

Refer to the following sources for more information on using `t:Z QuickStart` for Tomcat on z/OS:

- <http://tomcat.apache.org/> for general information on Tomcat including documentation, source code, bug reports, FAQs, etc.
- <http://dovetail.com/forum> for free support forums, including a forum dedicated to using Tomcat on z/OS. Questions and problems on using `t:Z QuickStart` for Tomcat, especially those that are not general Tomcat questions should be posted here.
- <http://www.ibm.com/servers/eserver/zseries/software/java/products/jzos/overview.html> for more information on using the IBM JZOS batch launcher.
- <http://www.ibm.com/developerworks/> - the IBM developerWorks site which contains the experimental version of the JZOS Batch Toolkit which includes the ASM and COBOL record generations code. This site also contains the JZOS Batch Cookbook.

Appendix A. License

Contact us for information regarding consulting and support agreements for T:Z.

T:Z Quickstart for Tomcat is distributed free under the Apache 2 license.

```
Copyright (C) 2009 Dovetailed Technologies, LLC.  
Copyright (C) 1992-2008, The Apache Software Foundation
```

```
Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.
```

```
You may obtain a copy of the License at  
http://www.apache.org/licenses/LICENSE-2.0
```

```
Unless required by applicable law or agreed to in writing, software  
distributed under the License is distributed on an "AS IS" BASIS,  
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
```

```
See the License for the specific language governing permissions and  
limitations under the License.
```