**Tomcat安全配置规范**

# 概述

## 范围

本规范适用于数字广东所有服务器上部署Tomcat程序的安全配置

## 目的

本规范旨在数字广东同事在安装配置Tomcat时进行必要的安全限制，最大化减少安全漏洞的产生，保障公司信息资产的安全

# 下载

## 下载位置

Tomcat程序的下载，应该从Tomcat官方提供的页面下载：

<http://tomcat.apache.org/>

建议下载最新稳定版本（目前最新稳定版本是9.0.7），注意不要下载beta版本

## 下载后校验

下载的同时，需记录下官方提供的文件hash（推荐MD5）

下载完毕后立即判断下载的文件hash是否与官网提供一致。

# 安装

## 安装

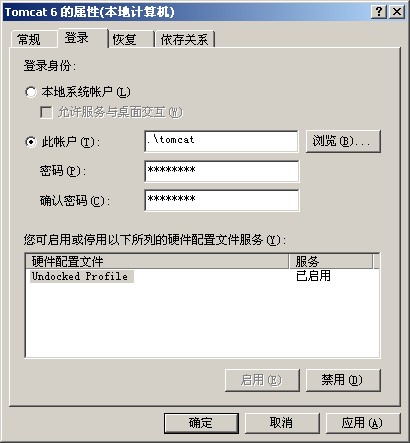
tomcat安装时，建议不引入不必要的模块

# 安全配置

## Window平台使用非管理员账号启动Tomcat

1)Tomcat禁止以系统system账户启动，需新建普通用户用于启动Tomcat。

2) 操作系统新建一个普通用户（如tomcat） , 设置 tomcat 用户对 tomcat\_home 的相关权限，在服务管理器 (service.msc) 中找到 tomcat 服务，右键选择属性，设置登录身份为 tomcat 用户



## Linux平台使用使用非root启动Tomcat

Tomcat禁止以系统root账户启动，需新建普通用户用于启动Tomcat。检查tomcat启动进程账户可以通过ps aux | grep tomcat命令查看。

**方案一**： 使用jsvc启动tomcat，适用tomcat6/7/8，可以监听1024以下的端口，如80端口。

root权限执行tomcat自带脚本daemon.sh，该脚本使用jsvc以普通用户权限去启动Tomcat，这是官方最推荐的方法，原理是root用户fork非root进程，好处是可以监听80端口。操作步骤如下：

**第一步：新建用户**

useradd -s /sbin/nologin tomcat

**第二步：修改tomcat目录属主并赋予权限**

chown -R tomcat:tomcat apache-tomcat-\*

chmod -R 770 apache-tomcat-\*

注：apache-tomcat-\* 为tomcat目录名。

**第三步：生成jsvc**

cd apache-tomcat-\*/bin/

tar zxvf commons-daemon-native.tar.gz

cd commons-daemon\*/unix

./configure --with-java={%JDKpath%}

make

cp jsvc ../.. #将jsvc二进制文件拷贝到tomcat的bin目录中

cd ../..

注： {%JDKpath%}为JDK安装路径，请根据实际情况设置，如

./configure --with-java=/usr/lib/jvm/java-1.6.0-openjdk-amd64/

**第四步：修改tomcat的./bin/daemon.sh脚本文件**

如果业务正在使用的版本没有daemon.sh，可下载同系列最新的版本，拷贝daemon.sh即可。

1）设置JAVA\_HOME路径

JAVA\_HOME={%JDKpath%}

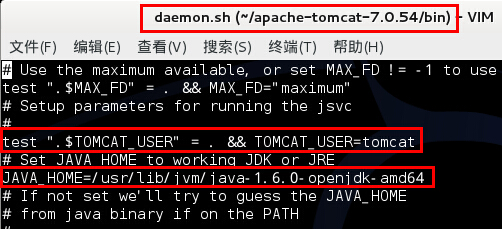
注：取消JAVA\_HOME 注释，{%JDKpath%} 需要修改为JDK安装路径。

2）设置TOMCAT\_USER=tomcat

test ".$TOMCAT\_USER" = . && TOMCAT\_USER=tomcat

注：我们第一步新建的用户名就是tomcat，所以这里不用修改，否则需要修改成对应的用户名，这里仅当做脚本参数说明。

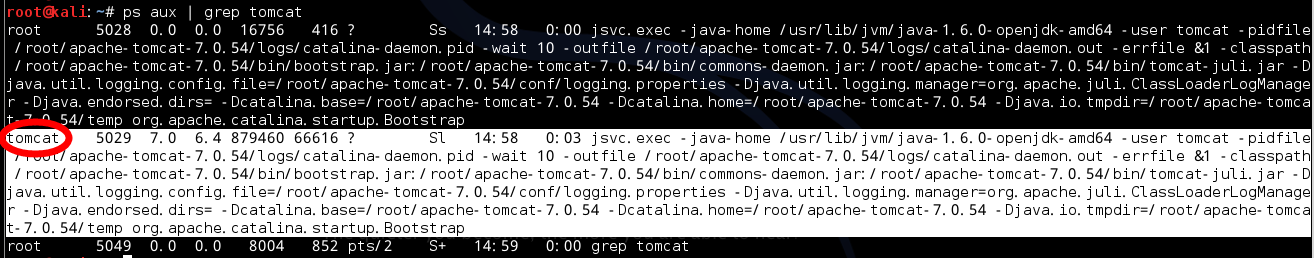
最后的效果如下图所示：



**第五步：启动tomcat**

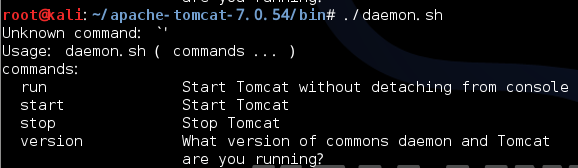
启动前确保该tomcat已经停止，启动命令为./daemon.sh start

启动成功后，可以看到tomcat现在已经以tomcat用户权限运行，如下图所示：



注：正常情况下有两个进程，参数都是一样的，但属主不一样，1个是root用户，1个是tomcat用户。

另外，停止/重启tomcat也是通过daemon.sh执行，命令参数如下：



**方案二**： 直接使用非root用户启动tomcat，适用tomcat5/6/7/8，只能监听1024以上的端口，如8080。操作步骤如下：

**第一步：新建用户**

useradd tomcat

**第二步：修改tomcat目录属主并赋予权限**

chown -R tomcat:tomcat apache-tomcat-\*

chmod -R 770 apache-tomcat-\*

注：apache-tomcat-\* 为tomcat目录名。

**第三步：启动tomcat**

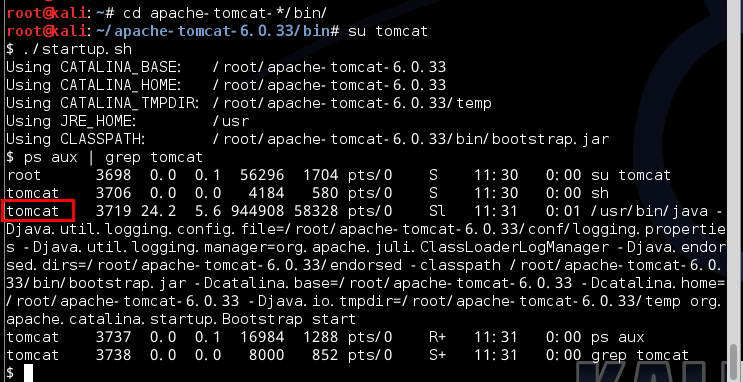
切换到系统普通用户tomcat去启动tomcat，启动前确保该tomcat已经停止。

cd apache-tomcat-\*/bin/

su tomcat

./startup.sh

启动成功后，可以看到tomcat现在已经以tomcat用户权限运行，如下图所示：



方案二的弊端是非root权限只能监听大于1024的端口，所以若想tomcat监听80/443端口并对外，则需要使用iptables或apache/nginx作转发。如iptables规则为：

iptables -A FORWARD -p tcp --destination-port 443 -j ACCEPT

iptables -t nat -A PREROUTING -j REDIRECT -p tcp --destination-port 443 --to-ports 8443

iptables -A FORWARD -p tcp --destination-port 80 -j ACCEPT

iptables -t nat -A PREROUTING -j REDIRECT -p tcp --destination-port 80 --to-ports 8080

## 删除tomcat默认页面

删除tomcat/webapps/目录下的所有文件及目录。目前已知webapps有以下目录：

Tomcat/webapps/docs/

tomcat/webapps/examples/

tomcat/webapps/host-manager/

tomcat/webapps/manager/

tomcat/webapps/ROOT/ （Linux 系统）

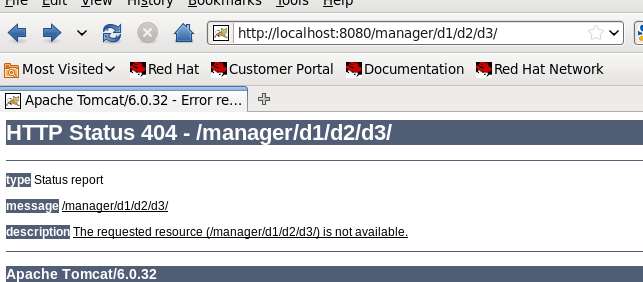
tomcat/webapps/admin/ (windows系统)

## Tomcat目录浏览

Tomcat服务器不允许目录遍历，以防止泄漏系统信息及服务器信息。配置项在tomcat/webapps/conf/web.xml文件中，具体配置为：

|  |
| --- |
| <param-name>listings</param-name>  <param-value>false</param-value>  注：默认配置为禁止目录浏览 |

效果截图如下



## Tomcat日志记录

编辑server.xml配置文件，确保在<HOST>标签中有记录日志功能，配置如下：

|  |
| --- |
| <valve classname=”org.apache.catalina.valves.AccessLogValve”  Directory=”logs” prefix=”localhost\_access\_log.” Suffix=”.txt”  Pattern=”common” resloveHosts=”false”/>  注：默认tomcat已经开启日志记录功能 |

## 启动安全模式

为了限制脚本的访问权限，防范webshell木马，建议启动时增加安全参数启动，如采用如下方式启动Tomcat

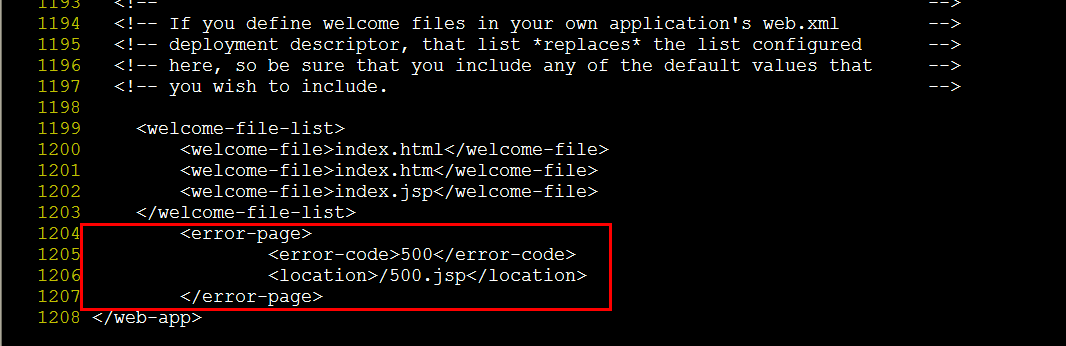
|  |
| --- |
| Tomcat/bin/startup.sh -security |

注：该选项可以极大的提高web服务器的安全性，但是可能会导致程序因权限不足运行出错的问题，请业务斟酌使用。

## 禁止显示错误信息

Tomcat在程序执行失败时会有错误信息提示，可能泄漏服务器的敏感信息，需要关闭错误提示信息。可以通过指定错误页面的方式不将错误信息显示给用户，修改tomcat/conf/web.xml,增加如下配置项：

|  |
| --- |
| <error-page>  <error-code>500</error-code>  <location>/500.jsp</location>  </error-page>  注：可以根据需要自行增加相应的错误码，常见的如500，404等，location选项为指定跳转的页面，该jsp文件需要自己生成。 |



## 删除jspx文件解析

Tomcat默认是可以解析jspx文件格式的后缀，解析jspx给服务器带来了极大的安全风险，若不需要使用jspx文件，建议删除对jspx的解析，具体操作为修改conf/web.xml文件：将如下代码注释掉：

|  |
| --- |
| <url-pattern>\*.jspx</url-pattern> |

## 文件目录权限配置

Web目录和文件属主不能与tomcat启动用户属主相同。如tomcat是以tomcat账号权限启动，则web文件和目录的属组必须是非tomcat账号。

Web目录权限统一设置为755，web文件权限统一设置为644。只有上传目录这类可读可写目录权限统一设置为777 。

# 简明Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 检查点 | 检查方法 | 检查结果 |
| 下载 | 下载 | 是否从官方渠道<http://tomcat.apache.org/>下载,当前最新的安全版本是9.0.7 |  |
| 校验 | 是否在下载完成后校验文件hash |  |
| 编译和安装 | 编译和安装 | 是否安装时引入不必要的组件 |  |
| 配置 | Tomat启动账户 | Linux系统Tomcat是否以非root账户启动  Windows系统Tomcat是否以非system权限或admin账号启动 |  |
| 删除Tomcat默认目录 | 删除tomcat/webapps/manager目录  删除tomcat/webapps/docs目录  删除tomcat/webapps/examples目录  删除tomcat/webapps/host-manager目录  删除tomcat/webapps/ROOT目录  删除tomcat/webapps/admin目录 |  |
| 关闭Tomcat目录浏览 | 查看conf/web.xml确认listings配置为false。 |  |
| Tomcat日志记录 | 查看conf/server.xml配置文件，确保在<HOST>标签中有记录日志功能 |  |
| 启动安全模式 | Tomcat启动脚本命令中增加security的启动参数 |  |
| 禁止显示错误信息 | 检查conf/web.xml确保自定义了错误页面转向，防止泄漏敏感信息 |  |
| 删除jspx后缀文件解析 | 检查conf/web.xml，确保jspx解析的代码已经注释掉 |  |
| 文件目录权限配置 | web目录755权限，web文件644权限，上传目录等可读可写目录777权限 |  |