Tomcat安全加固

（1）补丁安装

关注tomcat官方发布的最新漏洞及补丁（httpd.tomcat.org）

（2）删除文档和实例程序

到tomcat的家目录下的webapps文件夹，删除默认存在的docs和examples文件夹

（3）检查控制台口令

打开http://IP:8080/manager/html可以访问tomcat manager页面，一般不需要通过web页面的manager来管理tomcat，删除webapps目录下的manager和host-manager文件夹，如果需要使用tomcat manager 到tomcat\_home/conf/tomcat-user.xml 修改用户名和密码

打开http://IP:8080/admin可以访问tomcat admin页面 删除admin的文件夹

没有特殊的使用需求 删除webapps下的所有文件夹

（4）设置SHUTDOWN字符串

防止恶意用户telnet到8005端口后，发送shutdown命令关闭tomcat服务

打开tomcat\_home/conf/server.xml，查看是否设置了负责的字符串

<Server port="8005" shutdown="复杂的字符串">

（5）设置运行身份

以tomcat用户运行服务，增强安全性

创建apache组 创建apache用户加入到apache组，以tomcat身份启动服务

（6）禁止列目录

防止直接访问目录时由于找不到默认的主页而列出目录下所有的文件

到web.xml下查看listings是否设置为false

（7）日志审核

通过nginx的upstream模块获取

（8）自定义错误信息隐藏Tomcat信息

编辑conf/web.xml，在</web-app>标签上添加以下内容：

<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>