链滴

生产环境 Tomcat 安全规范

作者：lbb4511

原文链接：https://ld246.com/article/1552209100939

来源网站：链滴

Tomcat的安全

生产环境tomcat规范

1. 更改服务监听端口

若 Tomcat 都是放在内网的，则针对 Tomcat 服务的监听地址都是内网地址

标准配置：<Connector port="10000" server="webserver"/>

2. telnet管理端口保护

修改默认的 8005 管理端口不易猜测（大于1024），但要求端口配置在8000~8999之间

修改SHUTDOWN命令为其他字符串

标准配置：<Server port="8578" shutdown="dangerous">

3. AJP连接端口的保护

修改默认的ajp 8009端口为不易冲突（大于1024），但要求端口配置在8000~8999之间

通过iptables规则限制ajp端口访问的权限仅为线上机器，目的在于防止线下测试流量被apache的mod jk转发至线上tomcat服务器

标准配置：<Connector port="8349" protocol="AJP/1.3"/>

4. 禁用管理端

删除默认$CATALINA_HOME/conf/tomcat-users.xml文件，重启tomcat将会自动生成新的文件

删除$CATALINA_HOME/webapps下载默认的所有目录和文件

将tomcat应用根目录配置为tomcat安装目录以外的目录

标准配置：

- server.xml配置

一种直接修改Host节点信息，表示全局配置

```
<Host name="localhost"  appBase="/data/www/tomcat_webapps" unpackWARs="true" autoeploy="false"></Host>
```

另一种直接在Host节点中新增Context节点，指定具体的项目

```
<Context path="" docBase="/usr/local/tomcat/webapps/jenkins" debug="0" reloadable="false" crossContext="true"> </Context>
```

- 在$CATALINA_HOME/conf/Catalina/locathost目录下新增文件 test##20160506172651.xml

```
<Context displayName="test" docBase="/data/www/tomcat_webapps/test##2016050617261.war" reloadable="false" />
```

5. 隐藏Tomcat的版本信息

针对该信息的显示是由一个jar包控制的，该jar包存放在$CATALINA_HOME/lib目录下，名称为 catalina.jar，通过 jar xf 命令解压这个 jar 包会得到两个目录 META-INF 和 org ,修改 org/apache/catalin/util/ServerInfo.properties 文件中的 serverinfo 字段来实现来更改我们tomcat的版本信息

```
$ cd $CATALINA_HOME/lib
$ jar xf catalina.jar
$ cat org/apache/catalina/util/ServerInfo.properties |grep -v '^$|#'
$ mkdir -p org/apache/catalina/util
$ vim ServerInfo.properties
```

原文链接：生产环境 Tomcat 安全规范

```
server.info=nolinux        # 把这个值改成其它值就行了
```

自定义错误页面：修改$CATALINA_HOME/conf/web.xml重定向 403/404/500等错误到指定的错页面

6. 降权启动

Tomcat启动用户权限必须非root权限，尽量降低tomcat启动用户的目录访问权限，如需直接对外使80端口，可通过普通账号启动后，配置iptables规则进行转发，为了防止 Tomcat 被植入 web shell 序后，可以修改项目文件。要将 Tomcat 和项目的属主做分离，即便被破坏也无法创建和编辑项目文件

7. 文件列表访问控制

$CATALINA_HOME/conf/web.xml文件中的default部分的listings的配置必须为false(默认)，表示列出文件列表

8. 访问限制

通过配置，限定访问的IP来源

全局设置限定IP和域名访问：

```
<Host name="localhost"  appBase="/data/www/tomcat_webapps"   unpackWARs="true" aut
Deploy="false">
  <Valve className="org.apache.catalina.valves.RemoteAddrValve"  allow="192.168.1.10,192
168.1.30,192.168.2.*" deny=""/>
  <Valve className="org.apache.catalina.valves.RemoteHostValve"  allow="www.test.com,*.t
st.com" deny=""/>
</Host>
```

9. 脚本权限回收

控制CATALINAHOME/bin目录下的start.sh、catalina.sh、shutdown.sh的可执行权限，chmod−R 44CATALINAHOME/bin目录下的start.sh、catalina.sh、shutdown.sh的可执行权限，chmod−R74 CATALINA_HOME/bin/*

10. 访问日志格式规范

开启tomcat默认访问日志中Referer和User-Agent记录

标准配置：

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
  directory="logs" prefix="localhost_access_log"
    suffix=".txt" pattern="%h %l %u %t "%r" %s %b %{Referer}i %{User-Agent}i %D"
    resolveHosts="false" />
```

11. Server header重写

在HTTP Connector配置中加入server的配置，server=” chuck-server”