## **1 删除默认目录**

     安装完tomcat后，删除$CATALINA\_HOME/webapps下默认的所有目录文件  rm -rf /srv/apache-tomcat/webapps/

## **2 隐藏tomcat版本信息**

修改$CATALINA\_HOME/conf/server.xml,在Connector节点添加server字段，示例如下  
<Connector port="8080" protocol="HTTP/1.1"  
               connectionTimeout="20000"  
               redirectPort="8443" />  
               server="No Version"  
    <!-- A "Connector" using the shared thread pool-->

## **3 启用cookie的HttpOnly属性**

这个修改要注意，会导致登录获取不到cookie，导致登录不成功，如果不是https访问的情况下。

如：由于非 HTTPS Cookie 无法设置“secure”属性，已拒绝 Cookie “JSESSIONID”。

修改$CATALINA\_HOME/conf/context.xml，添加<Context useHttpOnly="true">

配置cookie的secure属性，在web.xml中sesion-config节点配置cooker-config，此配置只允许cookie在加密方式下传输。

<session-config>

<session-timeout>30</session-timeout>

<cookie-config>

<secure>true</secure>

</cookie-config>

</session-config>

## **4.禁用8005端口（一般不禁用）**

telnet localhost 8005 然后输入 SHUTDOWN 就可以关闭 Tomcat，为了安全我们要禁用该功能

默认值:

<Server port="8005" shutdown="SHUTDOWN">

修改为:

<Server port="8015" shutdown="sfasffdfdfmh">

在新版的 Tomcat 中该端口仅监听在127.0.0.1上，因此大家也不必担心。除非黑客登陆到tomcat本机去执行关闭操作

## **5.隐藏或修改 Tomcat 版本号**

# cd /usr/local/tomcat/lib/

# vim catalina.jar

# org/apache/catalina/util/ServerInfo.properties 选择

server.info=Apache Tomcat/8.5.16

server.number=8.5.16.0

server.built=Jun 21 2017 17:01:09 UTC

将以上去掉或修改版本号即可。

**6去除其他用户对tomcat的bin目录下的shutdown.sh startup.sh catalina.sh的执行权限**chmod -R 744 tomcat/bin/\*

## **7 应用程序安全&关闭自动部署**

<Host name="localhost" appBase="webapps"

unpackWARs="true" autoDeploy="true">

autoDeploy="true" server.xml改为autoDeploy="false"

**8访问日志格式规范**

打开access log  
按小时或按天记录。prefix/fileDateFormat/pattern可自定义，但必须记录关键信息，例如：源IP，Host、时间、 请求、状态码、数据大小、UA等。注意：如果前端是NG做反向代理，默认的pattern="combined"和pattern="common"不能 记录用户的真实IP，必须自定义pattern，记录客户端真实IP（X-Real-IP）

引用

|  |
| --- |
| <Valve className="org.apache.catalina.valves.AccessLogValve"      directory="logs"  prefix="xx" suffix=".log"      fileDateFormat="yyyy-MM-dd-HH"      pattern="%a %l %u %t "%r" %s %b "%{Referer}i" "%{User-Agent}i" " %{X-Real-IP}i"      resolveHosts="false"/> |

2.2 配置tomcat 写出更详细的日志

通过对 2.1 示例中 pattern 项的修改，可以改变日志输出的内容。

该项值可以为： common 与 combined ，这两个预先设置好的格式对应的日志输出内容如下：

common 的值： %h %l %u %t %r %s %b

combined 的值： %h %l %u %t %r %s %b %{Referer}i %{User-Agent}i

pattern 也可以根据需要自由组合, 例如 pattern="%h %l"

将记录访问源IP、本地服务器IP、记录日志服务器IP、访问方式、发送字节数、本地接收端口、访问URL地址等相关信息在日志文件中

对于各fields字段的含义请参照 :

<http://tomcat.apache.org/tomcat-8.0-doc/config/valve.html>  中的 Access Log Valve 项

|  |
| --- |
| 该pattern属性的值由文字文本字符串组成，结合以“%”字符为前缀的模式标识符，以导致替换为来自当前请求和响应的相应变量值。支持以下模式代码：  %a - 远程 IP 地址  %A - 本地 IP 地址  %b - 发送的字节数，不包括 HTTP 标头，如果为零则为“-”  %B - 发送的字节数，不包括 HTTP 标头  %h - 远程主机名（或 IP 地址，如果 enableLookups连接器为 false）  %H - 请求协议  %l - 来自 identd 的远程逻辑用户名（总是返回“-”）  %m - 请求方法（GET、POST 等）  %p - 接收此请求的本地端口。另见%{xxx}p下文。  %q - 查询字符串（如果存在，则以 '?' 开头）  %r - 请求的第一行（方法和请求 URI）  %s - 响应的 HTTP 状态代码  %S - 用户会话 ID  %t - 日期和时间，采用通用日志格式  %u - 已通过身份验证的远程用户（如果有），否则为“-”  %U - 请求的 URL 路径  %v - 本地服务器名称  %D - 处理请求所花费的时间，以毫秒为单位  %T - 处理请求所用的时间，以秒为单位  %F - 提交响应所花费的时间，以毫秒为单位  %I - 当前请求线程名称（可以稍后与堆栈跟踪进行比较）  还支持写入信息传入或传出标头、cookie、会话或请求属性以及特殊时间戳格式。它以[Apache HTTP Server](https://httpd.apache.org/)日志配置语法为模型 。它们中的每一个都可以使用不同的xxx键多次使用：  %{xxx}i 用名称写入传入标头的值 xxx  %{xxx}o 用名称写入传出标头的值 xxx  %{xxx}c 用名称写入 cookie 的值 xxx  %{xxx}r 用名称写入 ServletRequest 属性的值 xxx  %{xxx}s 用名称写入 HttpSession 属性的值 xxx  %{xxx}p写入本地（服务器）端口 ( xxx==local) 或远程（客户端）端口 ( xxx=remote)  %{xxx}t 在使用增强的 SimpleDateFormat 模式格式化的请求结束时写入时间戳 xxx  SimpleDateFormat 支持的所有格式在%{xxx}t. 此外，还添加了以下扩展：  sec - 自纪元以来的秒数  msec - 自纪元以来的毫秒数  msec\_frac - 毫秒分数  这些格式不能与 SimpleDateFormat 格式混合使用相同的格式标记。  此外，可以定义是否记录请求开始时间或响应结束时间的时间戳：  begin或前缀begin:选择请求开始时间  end或前缀end:选择响应完成时间  通过向%{xxx}t模式添加多个令牌，还可以记录两个时间戳。  速记模式pattern="common" 对应于由'%h %l %u %t "%r" %s %b'定义的通用日志格式 。  速记模式pattern="combined" 将Referer和User-Agent 标题的值（每个都用双引号）附加到common模式中。 |

**9目录权限**  
默认情况下，tomcat启动用户对WEB目录下所有文件及子目录应无写权限。标准配置：文件属主为root.root，权限为755。  
日志文件及cache文件应放在WEB目录之外

**10关闭war自动部署**

默认 Tomcat 是开启了对war包的热部署的。为了防止被植入木马等恶意程序，因此我们要关闭自动部署。

<Host name="localhost" appBase="" unpackWARs="false" autoDeploy="false">

appBase值为新路径。另外docBase为根路径