【应用安全】浅谈 LINUX 系统 JBOSS 安全配置

文/EmmaDai

0x00 JBoss 应用介绍

JBoss 是一个基于 J2EE 的开放源代码的应用服务器。 JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用。JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB3 的规范。但 JBoss 核心服务不包括支持 servlet/JSP 的 WEB 容器，一般与 Tomcat 或 Jetty 绑定使用。

0x01 为什么要做安全配置

JBoss 的默认配置中存在一些安全问题，例如弱密码、未配置使用 SSL 协议等。因此安全配置 JBoss 服务器能有效的减少安全威胁，下面将对 JBoss 的安全配置进行讨论。因 JBoss 版本较多，本期加固方法以 JBoss 6 为例。

0x02 如何进行安全配置

1. 设置 jmx-console 登录的用户名和密码，并且密码复杂度符合要求

JBoss 应配置 jmx-console 登录的用户名和密码，并且密码长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。

加固方法：
1）启用密码保护
修改 Jboss 目录下 server/$CONFIG/deploy/jmx-console.war/WEB-INF/jboss-web.xml ，去 掉<security-domain>节点的注释。 其中$CONFIG 表示用户当前使用的 JBoss 服务器配置路径。修改 jboss-web.xml 同级目录下的 web.xml 文件，去掉<security-constraint>节点的注释，在这里可以看到为登录配置了角色 JBossAdmin。
2） 设置复杂口令
jmx-console 的安全域和运行角色 JBossAdmin 都是在 login-config.xml 中配 置 ， 在 Jboss 的 安 装 目 录 server/$CONFIG/config 下 找 到 。 在 login-config.xml 中查找 jmx-console 的 application-policy 可以看到登录的角色 、 用 户 等 信 息 分 别 在 server/$CONFIG/config/props 的 jmx-console-roles.properties 和 jmx-console-users.properties 文件中配置。
3)重新启动 Jboss 服务。

2. 设置 web service 密码，并且密码复杂度符合要求

JBoss 应配置 web service 登录的用户名和密码，并且密码长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类。

加固方法：
1）启用密码保护
先修改配置文件
${home}$/common/${server_name}$/jbossws-console.war/WEB-INF/web.xml ， 将 <security-constraint> </security-constraint>部分的注释取消

然后修改配置文件${home}$/common/${server_name}$/jbossws-console.war/WEB-INF/jboss-web.xml，将<security-domain> </security-domain>部分的注释取消。
2）设置复杂口令
为 jbossws 设置复杂的口令，修改配置文 server/$CONFIG/conf/props/jbossws-users.properties 将其中 kermit=thefrog 修改为 kermit=复杂的密码。
3)重新启动 Jboss 服务。

3. Jboss 进程的用户不是超级用户

JBoss 进程的用户应该是非超级用户。查看当前系统的 JBoss 进程，确认程序启动时使用的身份。禁用超级用户启动 JBoss。

加固方法：
1) 创建 jboss 组： groupadd Jboss
2) 创建 jboss 用户并加入 jboss 组： useradd Jboss -g Jboss
3) 以 Jboss 身份启动服务

4. 设置支持加密协议

JBoss 应开启 HTTP 加密协议，使用 https 方式登录 Jboss 服务器管理页面。对于通过 HTTP 协议进行远程维护的设备，设备应支持使用 HTTPS 等加密议。

加固方法：
1)使用 JDK 自带的 keytool 工具生成一个证书 JAVA_HOME/bin/keytool -genkey -alias tc-ssl -keyalg RSA -keystore /opt/keystore (/opt/keystore 为存储证书得位置) 。
2) 编辑${jboss_path}/server/${jboss_server}/deploy/jbossweb.sar/server.xml 文件，取消 SSL/TLS 节点的配置，并设置 keystoreFile="/opt/keystore" keystorePass="nsfocus". 修改后内容如下（是具体情况而定）：

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector protocol="HTTP/1.1" SSLEnabled="true" port="8443"
address="${jboss.bind.address}" scheme="https" secure="true"
clientAuth="false" keystoreFile="/opt/keystore"
keystorePass="nsfocus" sslProtocol = "TLS" />
```

其中 keystoreFile 的为存储证书的路径 keystorePass 为生成 keystore 时输入的密码 。
3)重新启动 Jboss 服务。

5. 修改默认端口

为防止恶意的攻击，使得攻击者难以找到数据库并将其定位，使用 HTTP 协议的设备， 应更改 JBoss 服务器默认端口。

加固方法：
编辑${jboss_path}/server/${jboss_server}/deploy/jbossweb.sar/server.xml 配置文件，修改 8080 端口为 8100 端口. 参考配置如下：

```
<!-- A HTTP/1.1 Connector on port 8080 -->
<Connector protocol="HTTP/1.1" port="8100" address="${jboss.bind.address}"
redirectPort="${jboss.web.https.port}" />
```

6. 设置超时登出

对于具备字符交互界面的设备，应支持定时账户自动登出。登出后用户需再次登录才能进入系统。登录 jboss 默认页面 ，使用管理账号登录，闲置 30 分钟后，用户自动登出。

加固方法：
编辑${jboss_path}/server/${jboss_server}/deploy/jbossweb.sar/server.xml 文件， 修改 Connector 节点的 connectionTimeout 值 1800 秒。

7. 设置错误页面重定向

Jboss 应配置错误页面重定向，URL 地址栏中输入 http://ip:8100/manager12345 后，跳转至指向指定错误页面。

加固方法：
1)编辑${jboss_path}/server/${jboss_server}/deploy/jbossweb.sar/web.xml 文件:

```
<welcome-file-list>
   <welcome-file>index.html</welcome-file>
   <welcome-file>index.htm</welcome-file>
   <welcome-file>index.jsp</welcome-file>
</welcome-file-list>
```

2)重新启动 Jboss 服务

8. 限制目录列表访问

应禁止 Jboss 列表显示文件，当 WEB 目录中没有默认首页如 index.html,index.jsp 等文件时，不会列出目录内容。

加固方法：
1) 编辑${jboss_path}/server/${jboss_server}/deploy/jbossweb.sar/web.xml 配置文件：

```
<init-param>
   <param-name>listings</param-name>
   <param-value>false</param-value>
</init-param>
```

2)重新启动 Jboss 服务

9. 屏蔽状态信息

在配置文件中应删除或屏蔽状态页面，防止服务器信息泄露。访问 http://ip:port/status，不能看到状态信息。

加固方法：
编辑${jboss_path}/server/${jboss_server}/deploy/ROOT.war/WEB-INF/web.xml 文件， 注释如下内容

```
<!-- Uncomment to enable the status Servlet
<servlet>
   <servlet-name>Status Servlet</servlet-name>
   <servlet-class>org.jboss.web.tomcat.service.StatusServlet</servlet-class>
```

```
</servlet>
<servlet-mapping>
   <servlet-name>Status Servlet</servlet-name>
   <url-pattern>/status</url-pattern>
</servlet-mapping> -->
```

10. 记录用户登录行为

设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，使用的 IP 地址。

加固方法：
日志输出格式应为 %d %-5p [%t] [%c{1}] %l %m%n 配置文件路径：${jboss_path}/server/${jboss_server}/deploy/jboss-logging.xml 修改 periodic-rotating-file-handler 节点的 pattern 值。

0x03 总结

对 JBoss 进行安全配置可以有效的防范一些常见安全问题，按照基线标准做好安全配置能够减少安全事件的发生。国内常见的基线标准有中国信息安全等级保护、电信网和互联网安全防护基线配置要求及检测要求，不同的企业也可以根据自身企业业务制定符合自己企业的安全基线标准。

0x04 参考链接

- 国家信息安全等级保护制度要求
- 电信网和互联网安全防护基线配置要求及检测要求