阿里云

云市场·镜像市场

镜像产品安全审核标准

文档版本：2.0（20170320）

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

前言

概述

本文档用于对阿里云云市场（镜像市场）中镜像类商品安全审核进行规范。

每一章节的“基本要求”项为审核必需，如有不符将在安全审核中被驳回。

每一章节的“操作建议”项为安全加固建议，非必需，但强烈建议服务商按照此标准制作镜像。

应用范围

阿里云云市场（https://market.aliyun.com）镜像类商品安全审核

获取更新

文档更新请从以下地址获取：

https://help.aliyun.com/document_detail/30500.html

目录

1. 系统组件安全

1.1 基本要求

1）不允许使用任何盗版或者破解版程序

2）不允许存在任何木马后门、挂机、挖矿等恶意程序

3）不允许存在已公开的、可利用的且已存在修复方案的安全漏洞

4）保证安骑士已安装且开机自启（特殊网关类、安全类镜像产品以及国际站产品可以不用安装安骑士）

5）原则上不允许使用停止维护的发行版本，如 Debian6、CentOS4、Win2003

6）镜像制作时必须安装所有官方安全更新，具体参阅 1.2.1 安装安全更新

7）已上架镜像会定期被扫描，存在较大安全风险者，将会下架并重新制作

1.2 操作建议

1.2.1 安装安全更新

1）Windows： 开启 *Windows Update* 定期检查，并保证最新更新已安装

2）Debian 系： 包括 Debian、Ubuntu 等 Linux 发行版，在配置好正确的 APT 镜像源地址的情况下，使用 *apt update && apt upgrade* 命令进行更新

3）红帽系：包括 RHEL、CentOS、AliOS（Aliyun Linux）、OpenSUSE 等，请使用 *yum update* 命令自动进行更新

4）其他发行版包括 BSD 衍生版，请使用相应的命令进行更新

1.2.2 检查安骑士状态

1）Windows：任务管理器 => 进程，检查是否有 AliYunDunUpdate.exe 和 AliYunDun.exe 两个进程

2）Linux：ps –ef |grep AliYunDun，检查是否有 AliYunDunUpdate 和 AliYunDun 进程

1.3 重要组件列举

以下列出的组件必须保证无可被利用漏洞，更新方法请见 1.2.1 安装安全更新

1）引导、内核层面：grub、kernel、initramfs、sysvinit、systemd、efistub 等

2）运行依赖库：libc6、glibc、libssl（openssl）、libgnutls、OpenJDK、SunJDK、libtomcat、libxml、libgd、libpng、zlib、libpython、libnet、libkrb、libcup、libfuse、libdbus 等

3）常见用户态程序：openssh、sshfs、shell（bash、zsh、csh、dash...）、ftp、wget、curl、tar、gzip、

sudo、su、ppp、rsync、fcitx、exim、apt、dpkg、rpm、yum、dnf 等

2. 第三方组件安全

2.1 基本要求

1）不允许存在已公开的、可利用的且已存在修复方案的安全漏洞

2）不允许使用停止维护的软件版本系列，比如 PHP 5.2、5.3、5.4、5.6 系列，Mysql 5.1 系列、Tomcat 6 系列（特殊情况请和负责镜像接入同学说明）

3）镜像制作时，第三方组件请使用当时最新的稳定版本

4）请通过官方渠道下载软件，切勿通过非官方站点下载，以防被植入后门

2.2 操作建议

2.2.1 Web 容器

注：以下示例版本仅为该文档制作时的最新数据，服务商制作镜像时请通过官网查询最新版本信息

1）PHP：目前维护中的稳定版本包括：、

- 5.6.*
- 7.0.*
- 7.1.*

PHP 官网： http://php.net/

2）Mysql：目前维护中的稳定版本包括：

- 5.5.*
- 5.6.*
- 5.7.*

Mysql 官网： http://dev.mysql.com/downloads/mysql/

3）Apache：目前维护中的稳定版本包括：

- 2.2.*
- 2.4.*

Apache HTTP Server 官网：https://httpd.apache.org/

4）Nginx：目前维护中的稳定版本包括：

- 1.10.*
- 1.11.*

Nginx 下载官网：http://nginx.org/en/download.html

5）Tomcat：目前维护中的稳定版本包括：

- 9.0.*
- 8.5.*

- 8.0.*
- 7.0.*

Tomcat 下载地址：https://tomcat.apache.org/whichversion.html

6）Nodejs：目前维护中的稳定版本包括：

- V4（维护到期时间：2018-04-01）
- V6（维护到期时间：2019-04-18）

Nodejs 下载地址：https://nodejs.org/en/download/

7）Jetty：目前维护中的稳定版本包括：

- 9.4.*
- 9.3.*
- 9.2.*
- 8.1.*（EOL，仅有少量安全更新）
- 7.6.*（EOL，仅有少量安全更新）

Jetty 下载地址：http://www.eclipse.org/jetty/download.html

8）ProFTPD：目前维护中的稳定版本包括：

- 1.3.5*
- 1.3.6*

下载地址：http://www.proftpd.org/

2.2.2 Web 应用

1）Web 程序不允许存在任何已知的高危漏洞， 譬如任意文件上传、SQL 注入、命令执行、远程包含等漏洞
2）开源 CMS、BBS、Blog 等应用必须是最新的安全版本
3）Web 应用预装的插件保证为最新的安全版本
4）web 应用后台强制用户首次登陆后修改密码

3. 系统安全配置

3.1 基本要求

1）合理配置系统安全更新（镜像源的配置，ECS 默认配置即可）
2）禁止使用弱密码，请使用随机字符串作为各种程序的默认密码
3）系统密码要有一定长度、复杂度要求（ECS 默认即可）
4）不允许出现非必须的 SUID 特权程序
5）合理配置系统关键目录的权限，比如/etc、/bin、 ~/.ssh 等
6）除了/tmp 目录，其他目录不允许出现 777 权限
7）默认日志服务保证正常运行，如 dmesg、syslog、wtmp、btmp、sudo 等
8）设置合理的防火墙策略，屏蔽不安全的端口（如 redis 6379、mongodb27017 等），仅开放需要的端口；建议使用 iptables 默认屏蔽所有端口， 单独开放需要的端口， 比如 HTTP 80、SSH 22、RDP 3389、HTTPS 443 等

3.2 操作建议

3.2.1 常见 Linux 镜像源配置

此处列出相关配置供自定义镜像使用：

- **Debian 8**

  以 root 权限编辑文件/etc/apt/sources.list，添加以下内容：

```
deb http://mirrors.aliyun.com/debian jessie main contrib non-free
deb http://mirrors.aliyun.com/debian jessie-proposed-updates main contrib non-free
deb http://mirrors.aliyun.com/debian jessie-updates main contrib non-free
deb http://mirrors.aliyun.com/debian-security/ jessie/updates main non-free contrib
```

- **Debian7**

  以 root 权限编辑文件/etc/apt/sources.list，添加以下内容：

```
deb http://mirrors.aliyun.com/debian wheezy main contrib non-free
deb http://mirrors.aliyun.com/debian wheezy-proposed-updates main contrib non-free
deb http://mirrors.aliyun.com/debian wheezy-updates main contrib non-free
deb http://mirrors.aliyun.com/debian-security/ wheezy/updates main non-free contrib
```

- **CentOS，先备份原有配置：**

```
mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup
```

CentOS 5

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-5.repo
```

CentOS 6

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-6.repo
```

CentOS 7

```
wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-7.repo
```

- **Ubuntu 14.04**
  以 root 权限编辑文件/etc/apt/sources.list，添加以下内容

```
deb http://mirrors.aliyun.com/ubuntu/ trusty main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-security main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-updates main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-proposed main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ trusty-backports main restricted universe multiverse
```

- **Ubuntu 16.04**
  以 root 权限编辑文件/etc/apt/sources.list，添加以下内容

```
deb http://mirrors.aliyun.com/ubuntu/ xenial main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-security main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-updates main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-proposed main restricted universe multiverse
deb http://mirrors.aliyun.com/ubuntu/ xenial-backports main restricted universe multiverse
```

3.2.2 Linux 密码策略配置

为了能够使用 pam_quality ，须在/etc/pam.d/passwd 文件下的 password 配置中添加以下参数：

```
password    required    pam_pwquality.so retry=3
```

要求一个密码的长度至少有 8 个字符，包含全部四种字符，添加以下参数到
/etc/security/pwquality.conf ：

```
minlen=8
minclass=4
```

- **设置密码强度检查**
  检测是否有连续或重复的字符，在 /etc/security/pwquality.conf 中添加

```
maxsequence=3
maxrepeat=3
```

- **将用户的密码设定为 90 天内有效**

```
chage -M 90 <username>
#要禁用密码过期功能，通常在 -M 选项后使用值 99999（这相当于 273 年多一点）
```

- **要迫使密码即刻到期：**

```
chage -d 0 username
# 这个命令会将密码上次作出改动的日期设定为（1970 年 1 月 1 日）这个时间。这样，无论有什么密码到期政策，它都会迫使密码作出即时到期这一行动。这样在用户初次登录时，则立即会提示输入新密码
```

- **失败登录尝试限制**

  对任何非 root 用户进行锁定，并在十分钟后对该用户解锁，则须添加以下命令行到/etc/pam.d/system-auth 文件和/etc/pam.d/password-auth 文件中的 auth 区段：

```
auth        required      pam_faillock.so preauth silent audit deny=3 unlock_time=600
auth        sufficient    pam_unix.so nullok try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3 unlock_time=600
```

- **查看每个用户的尝试失败次数**

```
faillock
```

- **解锁一个用户的账户**

```
faillock --user <username> --reset
```

3.2.3 SSH Server 配置

- **Root 仅允许使用公钥登录**

```
# vi /etc/ssh/sshd_config
PermitRootLogin without-password
```

- **仅使用 SSH Protocol 2：**

```
# vi /etc/ssh/sshd_config
Protocol 2
```

- **不要支持闲置会话，并配置 Idle Log Out Timeout 间隔：**

```
# vi /etc/ssh/sshd_config
ClientAliveInterval 600       # (Set to 600 seconds = 10 minutes)
ClientAliveCountMax 0
```

- **禁用用户的 .rhosts 文件：**

```
# vi /etc/ssh/sshd_config
IgnoreRhosts yes
```

- **配置防火墙以接受仅来自已知网段的 SSH 连接：**

```
Update /etc/sysconfig/iptables (Redhat specific file) to accept connection only
from 192.168.100.0/24 and 209.64.100.5/27, enter:

-A RH-FW-1-INPUT -s 192.168.100.0/24 -m state --state NEW -p tcp --dport 22 -j ACCEPT
-A RH-FW-1-INPUT -s 209.64.100.5/27 -m state --state NEW -p tcp --dport 22 -j ACCEPT
```

- **限制 SSH 将侦听和绑定到的可用接口：**

```
# vi /etc/ssh/sshd_config
ListenAddress 192.168.100.17
ListenAddress 209.64.100.15
```

- **使用 Chroot SSHD 将 SFTP 用户局限于其自己的主目录：**

```
# vi /etc/ssh/sshd_config
ChrootDirectory /data01/home/%u
X11Forwarding no
AllowTcpForwarding no
```

- **禁用空密码：**

```
# vi /etc/ssh/sshd_config
PermitEmptyPasswords no
```

- **通过配置增加 SSH 日志记录的详细度：**

```
# vi /etc/ssh/sshd_config
LogLevel DEBUG
```

- **删除 rlogin 和 rsh 二进制程序，并将其替代为 SSH 的一个 symlink：**

```
# find /usr -name rsh
/usr/bin/rsh
# rm -f /usr/bin/rsh
# ln -s /usr/bin/ssh /usr/bin/rsh
```

3.2.4 Linux 防火墙配置

- **Syn-flood 防护:**

```
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

- **端口扫描防御:**

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
```

- **ICMP 包限速:**

```
iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

- **不返回 ping 包**

```
# vim /etc/sysctl.conf
# 添加：net.ipv4.icmp_echo_ignore_all = 1
# sysctl –p
```

- **检查开放端口**

```
# 查看所有开放的 TCP 端口
netstat –nlp | grep tcp

查看所有开放的 UDP 端口
netstat –nlp |grep udp
```

3.2.5 Linux 特殊权限文件查看

- **查找系统中所有含"s"位的程序**
  把不必要得"s"位去掉,或者把根本不用的直接删除

```
find / -type f ( -perm -04000 -o -perm -02000 ) -exec ls -lg {}
```

- **系统中没有属主的文件:**

```
find / -nouser -o -nogroup
```

- **任何人都有写权限的文件和目录:**

```
find / -type f ( -perm -2 -o -perm -20 ) -exec ls -lg {}
find / -type d ( -perm -2 -o -perm -20 ) -exec ls -ldg {}
```

3.2.6 Windows 系统加固

- **系统事件审核策略配置**

```
“开始” --> ”运行” --> secpol.msc ->安全设置->本地策略->审核策略
建议设置：
```

审核策略更改：成功

审核登录事件：成功，失败

审核对象访问：成功

审核进程跟踪：成功，失败

审核目录服务访问：成功，失败

审核系统事件：成功，失败

审核帐户登录事件：成功，失败

审核帐户管理：成功，失败

- **增大日志文件大小上限**

  避免由于日志文件容量过小导致日志记录不全

“开始” --> ”运行” --> eventvwr.msc -> “windows 日志” ->查看“应用程序”“安全”“系统”的属性

建议设置：日志上限大小：20480 KB

- **检查 Everyone 权限**

鼠标右键系统驱动器（磁盘）-> “属性” -> “安全”，查看每个系统驱动器根目录是否设置为 Everyone 有所有权限，删除 Everyone 的权限或者取消 Everyone 的写权限

- **增强口令的复杂度及锁定策略**

“开始” --> ”运行” --> secpol.msc （本地安全策略）->安全设置

1，账户策略->密码策略

密码必须符合复杂性要求：启用

密码长度最小值：8 个字符

密码最短使用期限：0 天

密码最长使用期限：90 天

强制密码历史：1 个记住密码

用可还原的加密来存储密码：已禁用

2，账户设置->账户锁定策略

帐户锁定时间：30 分钟

帐户锁定阀值：5 次无效登录

重置帐户锁定计数器：30 分钟

3，本地策略->安全选项

交互式登录：不显示最后的用户名：启用

- **减少系统无用账号，降低风险**

“开始” --> ”运行” --> compmgmt.msc（计算机管理）->本地用户和组，查看是否有不用的账号，系统账号所属组是否正确以及 guest 账号是否锁定

使用“net user 用户名 /del”命令删除账号

使用“net user 用户名 /active:no”命令锁定账号

3.2.7 Windows 网络加固

- **不需要 IPv6 的用户可以选择关闭 IPv6**

控制面板-> 网络与共享中心->更改适配器设置->本地连接->属性->Internet 协议版本 6 (TCP/IPv6)，请取消选中复选框，禁用 ipv6

- **网络访问限制**

“开始” --> ”运行” --> secpol.msc ->安全设置->本地策略->安全选项

网络访问: 不允许 SAM 帐户的匿名枚举：已启用

网络访问: 不允许 SAM 帐户和共享的匿名枚举：已启用

网络访问: 将 Everyone 权限应用于匿名用户：已禁用

帐户: 使用空密码的本地帐户只允许进行控制台登录：已启用

- **关闭默认共享**

“开始” --> ”运行” --> cmd.exe->net share，查看共享

“开始” --> ”运行” -->->regedit->

找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters ，

新建 AutoShareServer（REG_DWORD），键值为 0

- **不需要 RPC 的用户可以选择关闭 135 端口**

1、“开始”—>“运行”，输入“dcomcnfg”，单击“确定”，打开组件服务。

2、在弹出的“组件服务”对话框中，选择“计算机”选项。

3、在“计算机”选项右边，右键单击“我的电脑”，选择“属性”。

4、在出现的“我的电脑属性”对话框“默认属性”选项卡中，去掉“在此计算机上启用分布式 COM”前的勾。

5、选择“默认协议”选项卡，选中“面向连接的 TCP/IP”，单击“删除”按钮。

6、单击“确定”按钮，设置完成，重新启动后即可关闭 135 端口。

- **关闭 Netbios 相关服务（137、138、139 等端口）**

1、控制面板-> 网络与共享中心->更改适配器设置->本地连接->属性->Internet 协议版本 4->属性->高级->WINS->禁用 TCP/IP 上的 NetBIOS

2、关闭打印机共享服务（关闭 139 端口）

4. Web 容器安全配置

4.1 基本要求

1）Web 容器必须降权运行
2）禁用一些危险函数
3）禁用 HTTP 目录索引
4）禁用 Tomcat 等容器附带的管理功能
5）不允许使用弱密码，请使用随机字符串作为默认密码
6）设置合理的目录权限，防止未授权跨目录访问，比如 .git/.svn 等目录
7）设置合理的错误信息输出，防止泄漏敏感信息

4.2 操作建议

4.2.1 PHP 安全配置

- **安全模式：修改 php.ini 文件**

```
safe_mode = on
safe_mode_gid = off
```

- **禁用危险函数：**

```
disable_functions=exec,passthru,popen,proc_open,shell_exec,system,phpinfo,assert
# 有特殊需求除外
```

- **其他配置：**

```
# 关闭错误信息提示
display_errors = off
display_startup_errors = off
# 关闭全局变量
register_globals = off
# 不允许调用 dl
enable_dl = off
# 关闭远程文件
allow_url_fopen = off
allow_url_include = off
# 开启 http only
session.cookie_httponly = 1
cookie domain
```

```
# 开启 https secure
session.cookie_secure = 1
# 适当的 PHP redirects
cgi.force_redirect = 0
# SQL 的安全模式
sql.safe_mode = on
```

4.2.2 Jboss 安全配置标准

禁止目录浏览

修改 deploy\jbossdomain\deploy\jbossweb-tomcat55.sar\conf\下面的 web.xml 文件 以下内容为修改后的内容：

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

将“param-value”的值默认是 true，改为 false

删除危险服务

- 删除 Jboss 的/web-console 控制台(web-console 存在远程代码执行漏洞)
- 删除 jboss/server/default/deploy/jbossweb-tomcat55.sar 目录下的 root.war
- 删除 jboss/server/default/deploy/management/console-mgr.sar/web-console.war
- 删除 Jboss 的/jmx-console 控制台(jmx-console 存在远程代码执行漏洞)
- 删除 jboss/server/default/deploy/jmx-console.war 以及其他目录下的 jmx-console.war 文件
- 删除 jboss/server/default/deploy/jbossws.sar/jbossws-context.war 以及其他目录下的 jbossws-context.war 文件
- 删除 Jboss 的 http-invoker(http-invoker 存在远程代码执行漏洞)
- 删除 jboss/server/default/deploy/http-invoker.sar 目录

限制危险服务

- 设置 Jboss 的 Bootstrap JNP、RMI naming service 服务只允许本地访问（存在远程代码执行漏洞）
- 修改 server/default/conf 下的 jboss-service.xml 文件内容以及其他目录下的 jboss-service.xml 文件
- 修改 Bootstrap JNP(端口 1099)和 RMI naming service(1098)只允许本地访问

以下内容为修改后的内容：

```
<mbean code="org.jboss.naming.NamingService"
name="jboss:service=Naming"
xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
<attribute name="CallByValue">false</attribute>
<attribute name="Port">1099</attribute>
<attribute name="BindAddress">127.0.0.1</attribute>
<attribute name="RmiPort">1098</attribute>
<attribute name="RmiBindAddress">127.0.0.1</attribute>
<depends optional-attribute-name="LookupPool"
 proxy-type="attribute">jboss.system:service=ThreadPool</depends>
<depends optional-attribute-name="Naming"
proxy-type="attribute">jboss:service=NamingBeanImpl</depends>
</mbean>
```

其中“BindAddress”的值默认是“${jboss.bind.address}”，改为“127.0.0.1”；“RmiBindAddress”的值默认是“${jboss.bind.address}”，改为“127.0.0.1”

- 设置 Jboss 的 RMI/JRMP invoker 服务只允许本地访问（存在远程代码执行漏洞）
- 修改 server/default/conf 下的 jboss-service.xml 文件内容以及其他目录下的 jboss-service.xml 文件
- 修改 RMI/JRMP invoker(4444)只允许本地访问

以下内容为修改后的内容：

```
<mbean code="org.jboss.invocation.jrmp.server.JRMPInvoker"
name="jboss:service=invoker,type=jrmp">
<attribute name="RMIObjectPort">4444</attribute>
<attribute name="ServerAddress">127.0.0.1</attribute>
<depends>jboss:service=TransactionManager</depends>
</mbean>
```

其中“RMIObjectPort”的值默认是“${jboss.bind.address}”，改为“127.0.0.1”

4.2.3 Jetty 安全配置标准

禁止目录浏览

修改 etc/webdefault.xml

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

```
</init-param>
```

将“param-value”的值默认是 true，改为 false

异常页面的处理

修改 etc/webdefault.xml，此文件默认没有这些东西，需要添加

```
<error-page>
<error-code>500</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>501</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>502</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>503</error-code>
<location>/</location>
</error-page>
<error-page>
<error-code>404</error-code>
<location>/</location>
</error-page>
```

限定文件解析的类型

修改 etc/webdefault.xml，只保留 jsp 相关解析：

```
<servlet-mapping>
<servlet-name>jsp</servlet-name>
<url-pattern>*.jsp</url-pattern>
<url-pattern>*.JSP</url-pattern>
</servlet-mapping>
```

禁止显示服务器版本

修改 etc/jetty.xml,此处默认是 true，修改为 false：

```
<Set name="sendServerVersion">false</Set>
```

禁止 CGI

- 删除 webapps/目录下的 test.war 文件
- 删除 contexts/test.d 这个和下面那个不删也行，启动会报错，但是不影响使用。
- 删除 contexts/test.xml

文件权限控制

*#chmod 755 jetty/etc/**

4.2.4 tomcat 安全配置

- 删除 Tomcat 的 admin 控制台软件:删除{Tomcat 安装目录}\webapps 下 admin.xml 文件
- 删除 Tomcat 的 Manager 控制台软件:删除{Tomcat 安装目录}\webapps 下 manager.xml 文件

4.2.5 Apache 配置

- **确保只有 root 用户才有权限写入含脚本或者 CGI 的任何目录。要做到这一点，则须作为 root 用户运行以下命令：**

```
chown root <directory_name>
chmod 755 <directory_name>
```

- **其他一些配置说明**

```
FollowSymLinks
# 此指令为默认启用，因此在创建符号链接到网页服务器的文档 root 目录时，请慎重行事。# 例如，请勿为“/”提供符号链接。

Indexes
# 虽然此指令为默认启用，但并非必要。要防止访问者浏览在服务器上的文件，
# 则须删除这个指令

UserDir
# 因为此指令可确认系统中用户帐户是否存在，所以要默认禁用 UserDir 指令
# 要在服务器上启用用户名目录浏览，则须使用以下指令：
UserDir enabled
 UserDir disabled root
# 这些指令用于 /root/ 之外的所有用户目录，可激活其用户目录浏览这一功能
# 在禁用帐户列表中添加用户，要在 UserDir disabled 命令行添加以空格分隔的用户列表

ServerTokens
# ServerTokens 指令控制着服务器响应标题头信息，这信息会传送回给客户
```

它包括不同的信息，通过使用下列参数，可以对其进行自定义操作：

4.2.6 IIS 配置

- **删除 IIS 默认站点**

删除 c:\Inetpub 以及其他默认站点目录

- **IIS 访问权限配置**

如果 IIS 中有多个网站，建议为每个网站配置不同的匿名访问账户。

1.新建一个账号，加入 Guests 组

2.“网站属性”--->“目录安全性”--->“身份验证和访问控制”，把“启用匿名访问”处，用刚新建的账户代替默认账户

- **禁用不必要的 Web 服务扩展**

打开 IIS 管理器，检查是否有不必要的“Web 服务扩展”，如果有则禁用掉

- **网站目录权限配置**

原则：

目录有写入权限，一定不要分配执行权限

目录有执行权限，一定不要分配写入权限

网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限

其他目录一般只分配“读取”和“记录访问”权限即可

- **不显示详细的 ASP 错误信息**

“IIS 管理器”--->“属性”--->“主目录”--->“配置”--->“调试”，选择“向客户端发送下列文本错误消息”项，自定义出错时返回的错误信息

- **修改默认错误页面**

“IIS 管理器”--->“属性”--->“自定义错误”，用自定义的错误页面替换默认的默认页面

- **自定义 IIS Banner 信息**

修改默认 HTTP 头信息

“IIS 管理器”--->“属性”--->“HTTP 头”，在“自定义 HTTP 头”选中默 认的 HTTP 头信息，进行编辑，或者删除掉默认的，自己添加一个新的 HTTP 头信息

4.2.7 Nginx 配置

- **禁用 autoindex**

```
cat /etc/nginx/nginx.conf
# 配置文件上禁用 autoindex，即 autoindex off 或者没有配置 autoindex
```

- **关闭服务器标记**

```
cat /etc/nginx/nginx.conf
# 添加这行配置：  server_tokens off
```

- **设置缓存限制**

```
http{
    … …
    server{
        … …
        client_body_buffer_size  16K;
        client_header_buffer_size  1k;
        client_max_body_size  1m;
        large_client_header_buffers  4  8k;
        … …
```

- **设置 timeout 抵御一些 DDoS 攻击**

```
http {
    … …
        client_body_timeout   10;
        client_header_timeout  30;
        keepalive_timeout     30  30;
        send_timeout          10;
```

4.2.8 vsFTPd 配置

- **更改 vsftpd 登录信息**

  在 /etc/vsftpd/vsftpd.conf 文件中添加

```
ftpd_banner=<insert_greeting_here>
```

- **要允许匿名用户上传文件，那么建议在 /var/ftp/pub/ 中生成只写目录**

```
mkdir /var/ftp/pub/upload
```

- **更改权限以防止匿名用户查看该目录中的内容：**

```
chmod 730 /var/ftp/pub/upload
```