# 服务器安全加固

目录

[服务器安全加固 1](#_Toc21697952)

[一、操作系统加固 2](#_Toc21697953)

[1. 账号和口令 2](#_Toc21697954)

[2. 服务 3](#_Toc21697955)

[3. 文件系统 5](#_Toc21697956)

[4. 日志 5](#_Toc21697957)

[5. 更新系统安全补丁 6](#_Toc21697958)

[二、MySQL服务安全加固 7](#_Toc21697959)

[1. 帐号安全 7](#_Toc21697960)

[2. 口令 7](#_Toc21697961)

[3. 开启日志审计功能 8](#_Toc21697962)

[4. 安装补丁 8](#_Toc21697963)

[5. 设置可信 IP 访问控制 8](#_Toc21697964)

[6. 连接数设置 9](#_Toc21697965)

[7. 数据库备份 9](#_Toc21697966)

[三、Tomcat服务安全加固 9](#_Toc21697967)

[1. 网络访问控制 9](#_Toc21697968)

[2. 开启 Tomcat 访问日志 9](#_Toc21697969)

[3. Tomcat 默认帐号安全 10](#_Toc21697970)

[4. 修改默认访问端口 10](#_Toc21697971)

[5. 重定向错误页面 10](#_Toc21697972)

[6. 禁止列出目录 10](#_Toc21697973)

[7. 删除文档和示例程序 11](#_Toc21697974)

[8. 普通账号运行tomcat 11](#_Toc21697975)

[四、应用软件安全加固 11](#_Toc21697976)

[1. 版本选择 11](#_Toc21697977)

[2. 授权访问 11](#_Toc21697978)

[3. 规范化配置 11](#_Toc21697979)

[4. 最小权限运行 12](#_Toc21697980)

[5. 访问控制 12](#_Toc21697981)

# 一、操作系统加固

1. 账号和口令

**1.1 禁用或删除无用账号**

减少系统无用账号，降低安全风险，如games用户

**操作步骤**

* 使用命令 userdel <用户名> 删除不必要的账号。
* 使用命令 passwd -l <用户名> 锁定不必要的账号。
* 使用命令 passwd -u <用户名> 解锁必要的账号。

**1.2 检查特殊账号**

检查是否存在空口令和root权限的账号。

**操作步骤**

查看空口令和root权限账号，确认是否存在异常账号：

* 使用命令 awk -F: '($2=="")' /etc/shadow 查看空口令账号。
* 使用命令 awk -F: '($3==0)' /etc/passwd 查看UID为零的账号。
* 加固空口令账号：
* 使用命令 passwd <用户名> 为空口令账号设定密码。
* 确认UID为零的账号只有root账号。

**1.3 添加口令策略**

加强口令的复杂度等，降低被猜解的可能性。

**操作步骤**

1. 使用命令 vi /etc/login.defs 修改配置文件。

* PASS\_MAX\_DAYS 90 #新建用户的密码最长使用天数
* PASS\_MIN\_DAYS 0 #新建用户的密码最短使用天数
* PASS\_WARN\_AGE 7 #新建用户的密码到期提前提醒天数

1. 使用chage命令修改用户设置。  
   例如，chage -m 0 -M 30 -E 2020-01-01 -W 7 <用户名>

表示将此用户的密码最长使用天数设为30，最短使用天数设为0，密码2020年1月1日过期，过期前七天警告用户。

1. 设置连续输错三次密码，账号锁定五分钟。

使用命令 vi /etc/pam.d/common-auth修改配置文件，在配置文件中添加

auth required pam\_tally.so onerr=fail deny=3 unlock\_time=300

**1.4 限制用户su**

限制能su到root的用户。

**操作步骤**

使用命令 vi /etc/pam.d/su修改配置文件，在配置文件中添加行。例如，只允许test组用户su到root，

则添加 auth required pam\_wheel.so group=test

**1.5 禁止root用户直接登录**

限制root用户直接登录。

**操作步骤**

1. 创建普通权限账号并配置密码,防止无法远程登录;
2. 使用命令 vi /etc/ssh/sshd\_config修改配置文件将

PermitRootLogin的值改成no，并保存，然后使用service sshd restart重启服务。

**1.6 锁定用户信息文件**

避免账号信息被恶意串改，添加等。

**操作步骤**

1. 对password shadow group三个文件进行加锁禁止修改

chattr +i /etc/passwd /etc/shadow /etc/group

1. 文件解锁

chattr -i /etc/passwd /etc/shadow /etc/group

2. 服务

**2.1 关闭不必要的服务**

关闭不必要的服务（如普通服务和xinetd服务等），降低风险。

**操作步骤**

使用命令systemctl disable <服务名> 设置服务在开机时不自动启动。

使用命令systemctl stop <服务名> 关闭正在运行的服务。

**说明**： 对于部分老版本的Linux操作系统（如CentOS 6），可以使用命令chkconfig --level <init级别> <服务名> off 设置服务在指定init级别下开机时不自动启动。

**2.2 SSH服务安全**

对SSH服务进行安全加固，防止暴力破解成功。

**操作步骤**

使用命令 vi /etc/ssh/sshd\_config 编辑配置文件。

* 不允许root账号直接登录系统。  
  设置 PermitRootLogin 的值为 no。
* 修改SSH使用的协议版本。  
  设置 Protocol 的版本为 2。
* 修改允许密码错误次数（默认6次）。  
  设置 MaxAuthTries 的值为 3。
* 修改SSH服务监听端口
* 设置Port 的值为50022

配置文件修改完成后，重启sshd服务生效。

**2.3 防火墙规则**

严格控制服务器进出流量，防火墙规则粒度要求至端口级别。

**操作步骤**

* 对所有IP开放80端口服务

firewall-cmd --zone=public --add-port=80/tcp --permanent

firewall-cmd --reload

iptables写法：

iptables -I INPUT -p tcp --dport 80 -j ACCEPT

service iptables save

* 对IP地址1.2.3.4开放6379端口

firewall-cmd --add-rich-rule="rule family="ipv4" source address="1.2.3.4" port protocol="tcp" port="6379" accept" --permanent

firewalld-cmd --reload

iptables写法：

iptables -I INPUT -s 1.2.3.4 -p tcp --dport 6379 -j ACCEPT

service iptables save

* 关闭服务器ping包响应

firewall-cmd --permanent --add-rich-rule='rule protocol value=icmp drop'

firewall-cmd --reload

iptables写法如下：

iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -j DROP

* 封禁恶意IP：11.22.33.44

firewall-cmd --permanent --add-rich-rule="rule family=ipv4 source address=11.22.33.44 reject"

firewall-cmd --reload

iptables写法如下：

iptables -I INPUT -s 11.22.33.44 -j DROP

service iptables save

3. 文件系统

**3.1 设置umask值**

设置默认的umask值，增强安全性。

**操作步骤**

使用命令 vi /etc/profile 修改配置文件，添加行 umask 027， 即新创建的文件属主拥有读写执行权限，同组用户拥有读和执行权限，其他用户无权限。

**3.2 设置登录超时**

设置系统登录后，连接超时时间，增强安全性。

**操作步骤**

使用命令 vi /etc/profile 修改配置文件，将以 TMOUT= 开头的行注释（没有则在最后行添加），设置为TMOUT=180，即超时时间为三分钟。

4. 日志

**4.1 syslogd日志**

启用日志功能，并配置日志记录。

**操作步骤**

Linux系统默认启用以下类型日志：

* 系统日志（默认）/var/log/messages
* cron日志（默认）/var/log/cron
* 安全日志（默认）/var/log/secure

**注意**：部分系统可能使用syslog-ng日志，配置文件为：/etc/syslog-ng/syslog-ng.conf

**4.2 记录所有用户的登录和操作日志**

通过脚本代码实现记录所有用户的登录操作日志，防止出现安全事件后无据可查。

**操作步骤**

1. 运行vi /etc/profile打开配置文件。
2. 在配置文件中输入以下内容

history

HISTFILESIZE=2000  
HISTSIZE=2000  
HISTTIMEFORMAT='%F %T '  
export HISTTIMEFORMAT

USER=`whoami`

USER\_IP=`who -u am i 2>/dev/null| awk '{print $NF}'|sed -e 's/[()]//g'`

if [ "$USER\_IP" = "" ]; then

USER\_IP=`hostname`

fi

if [ ! -d /var/log/history ]; then

mkdir /var/log/history

chmod 777 /var/log/history

fi

if [ ! -d /var/log/history/${LOGNAME} ]; then

mkdir /var/log/history/${LOGNAME}

chmod 300 /var/log/history/${LOGNAME}

fi

export HISTSIZE=4096

DT=`date +"%Y%m%d\_%H:%M:%S"`

export HISTFILE="/var/log/history/${LOGNAME}/${USER}@${USER\_IP}\_$DT"

chmod 600 /var/log/history/${LOGNAME}/\*history\* 2>/dev/null

运行source /etc/profile 加载配置生效  
**注意**： /var/log/history 是记录日志的存放位置，可以自定义

通过上述步骤，可以在 /var/log/history 目录下以每个用户为名新建一个文件夹，每次用户退出后都会产生以用户名、登录IP、时间的日志文件，包含此用户本次的所有操作

5. 更新系统安全补丁

关注系统、软件安全资讯，对存在安全漏洞软件及时安装补丁修复，防止新漏洞被恶意利用

使用yum命令检查是否有相应软件安全补丁

yum --security check-update

安装全部安全补丁

yum update --security

安装tomcat安全补丁可使用如下命令

yum update tomcat --security

# 二、MySQL服务安全加固

1. 帐号安全

* + **禁止 Mysql 以管理员帐号权限运行**

以普通帐户安全运行 mysqld，禁止以管理员帐号权限运行 MySQL 服务。在 /etc/my.cnf 配置文件中进行以下设置。

[mysqld]

user=mysql

* + **修改mysql端口**

修改/etc/my.conf监听端口，降低被攻击可能性

[mysqld]

port=10066

* + **避免不同用户间共享帐号**

为不同类型用户创建不同账号，参考以下步骤

* + 1. 创建mysqladmin 超级用户

mysql> insert into mysql.user(Host,User,Password,ssl\_cipher,x509\_issuer,x509\_subject) values("localhost","mysqladmin",password("123!@#!admin"),'','','');

创建test用户，该用户只拥有test数据库所有权

mysql> create user 'test'@'localhost' identified by 'admin!@#!@3'; grant all privileges on test\* to 'test localhost';

* + **删除无关帐号**

DROP USER 语句可用于删除一个或多个 MySQL 账户。使用 DROP USER 命令时，必须确保当前账号拥有 MySQL 数据库的全局 CREATE USER 权限或 DELETE 权限。账户名称的用户和主机部分分别与用户表记录的 User 和 Host 列值相对应。

mysql> DROP USER test;

2. 口令

检查账户默认密码和弱密码。口令长度需要至少八位，并包括数字、小写字母、大写字母和特殊符号四类中的至少两种类型，且五次以内不得设置相同的口令。密码应至少每 90 天进行一次更换。

可以通过执行以下命令修改密码。

mysql> update user set password=password('test!p3') where user='root';

mysql> flush privileges;

3. 开启日志审计功能

数据库应配置日志功能，便于记录运行状况和操作行为。

MySQL服务有以下几种日志类型：

* + **错误日志**： -log-err
  + **查询日志**： -log （可选）
  + **慢查询日志**： -log-slow-queries （可选）
  + **更新日志**： -log-update
  + **二进制日志**： -log-bin

找到 MySQL 的安装目录，在 my.conf 配置文件中增加上述所需的日志类型参数，保存配置文件后，重启 MySQL 服务即可启用日志功能。例如:

log-error=/var/log/mysql/error.log  
log=/var/log/mysql/mysql.log  
log-slow-queries=/var/log/mysql/slowquery.log

log-update=/var/log/mysql/update.log

log-bin=/var/log/mysql/mysql-bin-log

**日志查询操作说明**

* + 1. 执行show variables like 'log\_%';命令可查看所有的 log。
    2. 执行show variables like 'log\_bin';命令可查看具体的 log。

4. 安装补丁

确保系统安装了最新的安全补丁。

**注意**： 在保证业务及网络安全的前提下，并经过兼容性测试后，安装更新补丁。

**如果不需要，应禁止远程访问**

禁止网络连接，防止猜解密码攻击、溢出攻击、和嗅探攻击。

**注意**： 仅限于应用和数据库在同一台主机的情况。

如果数据库不需要远程访问，可以禁止远程 TCP/IP 连接，通过在 MySQL 服务器的启动参数中添加--skip-networking参数使 MySQL 服务不监听任何 TCP/IP 连接，或修改监听地址bind-address=127.0.0.1增加安全性

可以使用 iptables、firewall 进行内外网访问控制，建议不要将数据库高危服务对互联网开放。

5. 设置可信 IP 访问控制

通过数据库所在操作系统的防火墙限制，实现只有信任的 IP 才能通过监听器访问数据库。

mysql> GRANT ALL PRIVILEGES ON \*.\* TO 'wwdt'@'1.2.3.4' IDENTIFIED BY 'ad1@#!12345' WITH GRANT OPTION;

6. 连接数设置

根据机器性能和业务需求，设置最大连接数。

在 MySQL 配置文件my.conf的 [mysqld] 配置段中添加

max\_connections = 1000，保存配置文件，重启 MySQL 服务后即可生效。

7. 数据库备份

定时对数据库进行异地全量备份、增量备份，可预防数据库误操作、数据恢复等操作

使用定时器配置每小时对test数据库进行备份导出

crontab -e

00 \* \* \* \* mysqldump -test -ptestpasswd test > /backup/test\_$(date +%F-%T).sql

# 三、Tomcat服务安全加固

Tomcat服务默认启用管理后台功能，使用该后台可直接上传 war 文件包对站点进行部署和管理，可能导致管理后台存在空口令或者弱口令的漏洞，使得黑客或者不法分子可以利用该漏洞直接上传 Webshell 脚本导致服务器沦陷，由于此类型漏洞可能对业务系统造成比较严重的危害，建议针对 Tomcat 管理后台进行以下安全加固配置。

1. 网络访问控制

* 如果不需要使用 Tomcat 管理后台管理业务代码，直接将 Tomcat 部署目录中 webapps 文件夹中的 manager、host-manager 文件夹全部删除，并注释 Tomcat 目录中 conf 文件夹中的 tomcat-users.xml 文件中的所有代码。
* 如果确实需要使用 Tomcat 管理后台进行业务代码的发布和管理，建议为 Tomcat 管理后台配置强口令，并修改默认 admin 用户，且密码长度不低于10位，必须包含大写字母、特殊符号、数字组合。

2. 开启 Tomcat 访问日志

修改 conf/server.xml 文件，将下列代码取消注释：

<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"

prefix="localhost\_access\_log." suffix=".txt" pattern="common" resolveHosts="false"/>

启用访问日志功能，重启 Tomcat 服务后，在 tomcat\_home/logs 文件夹中就可以看到访问日志。

3. Tomcat 默认帐号安全

修改 Tomcat 安装目录 conf 下的 tomcat-user.xml 文件，重新设置复杂口令并保存文件。重启 Tomcat 服务后，新口令即生效。

4. 修改默认访问端口

修改 conf/server.xml 文件把默认的 8080 访问端口改成其它端口。

如不使用ajp连接器则注释代码段

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

5. 重定向错误页面

修改访问 Tomcat 错误页面的返回信息，在 webapps\manger 目录中创建相应的401.html、404.htm、500.htm 文件，然后在 conf/web.xml 文件的最后一行之前添加下列代码：

<error-page>

<error-code>401</error-code>

<location>/401.htm</location>

</error-page>

<error-page>

<error-code>404</error-code>

<location>/404.htm</location>

</error-page>

<error-page>

<error-code>500</error-code>

<location>/500.htm</location>

</error-page>

6. 禁止列出目录

防止直接访问目录时由于找不到默认页面，而列出目录下的文件的情况。

在 web.xml 文件中，将

<param-name>listings</param-name>改成<param-name>false</param-name>

7. 删除文档和示例程序

删除 webapps 目录下的 docs、examples、manager、ROOT、host-manager 文件夹。

8. 普通账号运行tomcat

使用普通账号运行tomcat服务，即使web服务被入侵，入侵者只具有操作系统普通权限

新建无home目录权限，且无法登录的普通用户，使用tomcat账号运行tomcat服务

useradd -M -s /sbin/nologin tomcat

runuser -l tomcat -c '/usr/local/tomcat/bin/startup.sh'

# 四、应用软件安全加固

1. 版本选择

在安装软件时应选官网提供的最新稳定版本进行部署，可避免安装已知漏洞版本

2. 授权访问

软件提供授权访问功能，需配置相应账号信息，使用高复杂度密码并定期修改，未授权访问漏洞可导致敏感信息泄露、系统被破坏等

例如Redis 因配置不当存在未授权访问漏洞，在特定条件下，如果 Redis 以 root 身份运行，黑客可以给 root 账号写入 SSH 公钥文件，直接通过 SSH 登录受害服务器，从而获取服务器权限和数据。一旦入侵成功，攻击者可直接添加账号用于 SSH 远程登录控制服务器，给用户的 Redis 运行环境以及 Linux 主机带来安全风险，如删除、泄露或加密重要数据，引发勒索事件等。

**Redis漏洞修复步骤：**

1. 指定 Redis 服务使用的网卡，监听地址修改为127.0.0.1
2. 设置防火墙策略，只允许指定IP地址访问
3. 配置账号认证，在配置文件中设置requirepass 值
4. 服务运行权限最小化，创建普通账号并使用该账号运行redis服务

3. 规范化配置

配置文件以及软件安全设置容易被忽略，不规范的配置可为黑客提供可趁机会

例如Jenkins早期版本的默认配置下没有安全检查。任何人都可以以匿名用户身份进入Jenkins，执行build操作，设置可使用jenkins的script执行linux命令，黑客可利用这一特性植入webshell，从而获得服务器操作权限，

**Jenkins配置规范：**

1. 在jenkins配置页面上勾选**Enable security**复选框
2. 使用安全域和授权配置
3. 定期关注Jenkins官方安全公告，使用或更新到官方最新版本的Jenkins，防止部署存在安全漏洞的版本。

4. 最小权限运行

在应用软件被入侵时, 如果该软件使用root账号在服务器上运行时，相当于为黑客敞开root权限大门

1） 创建普通账号：useradd -M -s /sbin/nologin user

2) 使用该账号运行程序：runuser -l user -c <服务启动命令>

5. 访问控制

服务开放访问时，应考虑服务访问者身份，非必要情况重要高危服务不开放公网访问，确定要开放访问需结合iptables、firewalld配置相应访问策略

如只针对IP地址12.12.12.12开放3306服务

iptables -I INPUT -s 12.12.12.12 -p tcp --dport 3306 -j ACCEPT

service iptables save